

UNIVERSITÀ DELLA CALABRIA



UNIVERSITA' DELLA CALABRIA

Dipartimento di INGEGNERIA MECCANICA ENERGETICA E GESTIONALE

Dottorato di Ricerca in

INGEGNERIA CIVILE E INDUSTRIALE

CICLO

XXX

RISCHIO E SICUREZZA NELLE FILIALI BANCARIE.

TECNOLOGIE IoT A SUPPORTO DEI PROCESSI ORGANIZZATIVI E DEI MODELLI DECISIONALI

Settore Scientifico Disciplinare ING-IND/35

Coordinatore:

Ch.mo Prof. FRANCO FURGIUELE

Firma

Supervisore/Tutor:

Ch.mo Prof. SALVATORE AMMIRATO

Firma

Dottorando:

Dott./ssa CINZIA RASO

Firma

Sommario

Abstract.....	7
INTRODUZIONE	10
Il Metodo della ricerca	16
Il focus group.....	17
CAPITOLO 1. Il problema della gestione della sicurezza fisica delle dipendenze bancarie.....	19
1.1 La banca e le dipendenze bancarie	19
1.2 I modelli distributivi bancari.....	20
1.3 Il problema della sicurezza delle dipendenze bancarie: le dimensioni del fenomeno	30
CAPITOLO 2. Opportunità per il miglioramento nei processi di gestione della sicurezza nelle dipendenze bancarie	33
2.1 La gestione dei processi aziendali	33
2.1.1. Approcci al Business Process Management: Reingegnerizzazione vs. miglioramento incrementale. Metodologie il miglioramento dei processi aziendali	35
2.2 Strumenti per la modellazione dei processi aziendali.....	49
2.3 La leva per il cambiamento: l’impatto dell’Internet of Things nella reingegnerizzazione dei processi.....	58
2.4. Nuovi paradigmi IoT-based per la gestione “intelligente” della sicurezza delle dipendenze bancarie	62
2.4.1. Introduzione al concetto di “internet-of-things”	62
2.4.2 Gli elementi costitutivi dell’IoT: gli Smart Objects	67
2.4.3 Smart Environments e Ambient Intelligence	73
2.4.4 Smart Environments: dal Cyberspace al Cyber-physical social space	76
CAPITOLO 3. Ottimizzazione dei processi di sicurezza delle dipendenze bancarie: una proposta di reingegnerizzazione.....	85
3.1 La metodologia adottata.....	85
3.2 Analisi della situazione attuale: Uno stato dell’arte della Letteratura Scientifica	87
3.2.1 Modelli e tecnologie per la protezione dei luoghi fisici	87
3.2.2 Stato dell’arte sulla sicurezza delle dipendenze bancarie.....	97
3.2.3 La protezione delle dipendenze bancarie: Layout tipici delle Dipendenze Bancarie.....	119
3.2.4 Misure di protezione adottate nelle dipendenze bancarie.....	130
3.3 Analisi della situazione attuale: La percezione della sicurezza dei clienti. Un’indagine campionaria.....	135
3.3.1 La percezione della sicurezza	138
3.3.2 I reati subiti.....	140
3.3.3 Le rapine in banca	141

3.3.4 Prevenzione e mitigazione del rischio rapina.....	145
3.4 Focus group sui sistemi e le misure di sicurezza bancaria	148
3.4.1. La selezione dei partecipanti.....	150
3.4.2 Realizzazione discussione e metodo di analisi	151
3.4.3 Analisi dei risultati del focus group: La percezione della sicurezza.....	151
3.5 Analisi della situazione attuale.....	160
3.5.1 I processi e gli attori della sicurezza fisica in banca	160
3.5.2 Rappresentazione AS-IS dei processi di gestione della sicurezza fisica	163
3.5.3 Limiti negli attuali approcci alla gestione della sicurezza e proposte di miglioramento. ..	167
CAPITOLO 4: Verso un modello innovativo per la valutazione del rischio di filiale	171
4.1 Il concetto di rischio: un'analisi della letteratura scientifica.....	171
4.1.1 La gestione del rischio	176
4.2 Fase 1: L'identificazione del rischio.....	185
4.2.1 Il concetto di safety	185
4.2.2 Il concetto di Security.....	187
4.2.3 Identificazione dei reati ai danni delle dipendenze bancarie.....	191
4.3 Fase 2: Valutazione del rischio	213
4.3.1 L'impatto	214
4.3.2 Andamento delle serie storiche	215
4.3.4 Vulnerabilità dell'area in cui si colloca la filiale, rispetto a ciascun reato.....	224
4.4 Fase 3: Individuazione delle azioni correttive intese a ridurre il rischio di incidenti	229
4.5 Fase 4: Definizione del modello di rischio di Filiale.....	239
CAPITOLO 5: Una proposta risolutiva per la reingegnerizzazione della gestione della sicurezza nelle dipendenze bancarie	245
5.1 Elementi per la reingegnerizzazione della gestione della sicurezza nelle filiali bancarie.	245
5.2 Le dipendenze bancarie secondo una prospettiva di Cyber Physical Space	247
5.3 Verso un Intelligent Protection Systems per la gestione della sicurezza di filiale	250
5.3.1 L'utilizzo di Synthetic Sensors per la trasformazione della filiale in "ambiente intelligente"	253
5.4 Implicazioni organizzative derivanti dalla reingegnerizzazione del processo	260
5.5 Focus group: alcune considerazioni sulle proposte to-be.....	264
5.6 Intelligent Protection System: Architettura funzionale e Scenari di Utilizzo	273
5.6.1 Interfacce piattaforma	291
5.7 Performance Analysis: un confronto tra la situazione attuale e la soluzione proposta	302
Considerazioni Conclusive	309

Indice delle figure

<i>Figura 1. Struttura logica della tesi</i>	15
Figura 2. Processo di analisi delle fonti derivate dalla letteratura scientifica	16
Figura 3. Evoluzione del modello di servizio (Fonte: Elaborazione KPMG Advisory, 2013).....	21
Figura 4. Cambiamenti in atto nel settore bancario	22
Figura 5. Integrazione processi direzionali ed operativi nella gestione del rischio bancario	23
Figura 6. Evoluzione degli approcci organizzativi nella gestione del rischio bancario.....	24
Figura 7. Approccio integrato alla sicurezza e alla security governance	25
Figura 8. Scenari evolutivi per le strategie distributive (Fonte: CeTiF, 2014)	27
Figura 9. La prospettiva sistemica del Business Process Management.....	35
Figura 10. Approccio ciclico nella gestione dei processi di produzione	39
Figura 11. Ruota PDCA.....	40
Figura 12. Ciclo PDSA.....	41
Figura 13. Model for Improvement	42
Figura 14. BPR vs. BPI.....	43
Figura 15. I due differenti approcci al BPR (Valiris and Glykas, 1999)	44
Figura 16. Il processo di Reingegnerizzazione (Eftekhari e Akhavan, 2013)	48
Figura 17. Classificazione delle metodologie di rappresentazione dei processi aziendali (Vergidis, 2008)	49
Figura 18. La convergenza tra approcci organizzativi ed innovazioni in ambito ICT	60
Figura 19. Le dimensioni dell'IoT	63
Figura 20. Numero di papers indicizzati nel Database Scopus con la parola chiave "Internet of Things" negli ultimi dieci anni	64
Figura 21. Il paradigma dell'"Internet of things" come risultato della convergenza di visioni diverse. ..	66
Figura 22. Rappresentazione schematica dell'Internet Of Things (Gubbi et al., 2013)	67
Figura 23. Classificazione dell'intelligenza basata sulla teoria di Meyer	73
Figura 24. Il concetto di CPSS (elaborazione propria).....	83
Figura 25. La "società delle cose" vs la "società delle persone"	84
Figura 26. La protezione dei beni aziendali.....	88
Figura 27. Modello di simulazione dell'attaccante.....	97
Figura 28. Flusso Logico del sistema proposto (Sujith, 2014)	101
Figura 29. Esempi di traiettorie plottate sulla planimetria della filiale (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010).....	104
Figura 30. Esempio di scenario di rischio rilevato. Un soggetto si muove velocemente (corre) all'interno della dipendenza (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010)	104
Figura 31. Esempio di rilevazione di soggetti con stima dell'altezza e dettaglio del viso (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010)	105
Figura 32. Pattern di una rapina commessa da un solo rapinatore (De Gregorio, 2011)	107
Figura 33. Pattern di una rapina commessa da un solo rapinatore quando si verifica un incidente imprevisto (De Gregorio, 2011).....	108
Figura 34. Pattern di una rapina commessa da una coppia di rapinatori (De Gregorio, 2011)	108
Figura 35. Architettura per la sicurezza degli ATM proposta in (Jaiswal & Bartere, 2014).....	109
Figura 36. Rete Bayesiana relativa alla simulazione della Rapina in Banca (Ronsivalle G. B., 2007).....	114
Figura 37. Fase dell'identikit nella Simulazione della Rapina in Banca (Ronsivalle G. B., 2007).....	115
Figura 38. Rappresentazione della Rete Neurale Artificiale OSSIF (Guazzoni & Ronsivalle, 2008)..	116
Figura 39. Rappresentazione della Rete Bayesiana adottato da ABI per il modello di analisi del rischio rapina (Ronsivalle G. , 2011)	117
Figura 40. Esempio di Layout di una dipendenza bancaria (Messina, 2002)	123
Figura 41. Layout a banca aperta WWD2002 (Messina, 2002)	126
Figura 42. Layout a tre porte	127
Figura 43. Sistema integrato con area self banking.....	128
Figura 44. Sistema integrato con area self banking e sportello	129
Figura 45. Sistema sliding doors interbloccato.....	130

Figura 46. Locale esclusivo self banking H24	130
Figura 47. Ripartizione del campione per sesso ed età del campione. Valori percentuali	137
Figura 48. Ripartizione del campione per area geografica. Valori percentuali	137
Figura 49. Ripartizione del campione per condizione professionale. Valori percentuali	138
Figura 50. Ripartizione del campione per titolo di studio. Valori percentuali	138
Figura 51. E' stato/a vittima di reato nella sua città nell'ultimo anno?	140
Figura 52. Quali reati ha subito nella sua città negli ultimi tre anni?	141
Figura 53. Percezione dell'adeguatezza dei sistemi di sicurezza e protezione	142
Figura 54. Percezione dell'adeguatezza del personale addetto alla sicurezza	143
Figura 55. Percezione dell'adeguatezza del personale di filiale	143
Figura 56. I processi di gestione della sicurezza. Situazione AS IS	167
Figura 57. Fattori di rischio	178
Figura 58. Lo skimmer "contraffatto" è anteposto all'originale	203
Figura 59. Un esempio di come i ladri nascondono una mini telecamera in un porta-brochure contenente materiale promozionale dell'istituto di credito dell'Atm	203
Figura 60. La tastiera originale è coperta da un finta per ingannare il cliente	204
Figura 61. Tassonomia delle minacce.....	212
Figura 62. TIPOLOGIA DEGLI EVENTI CRIMINOSI orizzonte temporale 2009-2011	216
Figura 63. Esito delle rapine.....	216
Figura 64. Esito degli attacchi all'atm.....	217
Figura 65. Esito degli eventi di danneggiamento	217
Figura 66. Esito degli eventi di furto	217
Figura 67. Impatto/perdita delle rapine compiute	219
Figura 68. Danno subito/Perdita economica derivante da azione di danneggiamento.....	219
Figura 69. Danno subito/Perdita economica derivante da azioni di furto.....	220
Figura 70. Danno subito/Perdita economica derivante da attacchi agli atm	220
Figura 71. ATTACCO ATM COMPIUTO: Giorni della settimana	221
Figura 72. La tripla Minaccia, Asset, Contromisura	240
Figura 73. Approcci all'environmental sensing	256
Figura 74. Funzionalità di general purpose sensor disponibili commercialmente o in letteratura	257
Figura 75. I processi di gestione della sicurezza. Situazione TO BE	263
Figura 76. Struttura logica della piattaforma	273
Figura 77. Schema logico e possibili scenari	273
Figura 78. Architettura della piattaforma	274
Figura 79. Schema Attori - Use Case Diagram	277
Figura 80. Operatore Tecnico - Use Case Diagram.....	277
Figura 81. Operatore Manager - Use Case Diagram	278
Figura 82. Sensori - Use Case Diagram	278
Figura 83. Gestione avvisi per Operatore Tecnico - Use Case Diagram.....	279
Figura 84. Schema di Deployment della piattaforma	279
Figura 85. Schema Attori.....	280
Figura 86. Class Diagram.....	281
Figura 87. Use Case Diagram Complessivo	282
Figura 88. Caratteristiche funzionali della console operatore	284
Figura 89. Attività di un PSIM.....	288
Figura 90. Mock-up piattaforma operatore	293
Figura 91. Mock-up videosorveglianza.....	294
Figura 92. Mock-up visualizzazione interattiva pianta.....	295
Figura 93. Esempio di scenario reale	296
Figura 94. Esempio di Control Room	296
Figura 95. Esempio pannello operatore	297
Figura 96. Flusso logico segnalazione allarme	298
Figura 97. Flusso logico - Classificazione della segnalazione	299
Figura 98. Flusso logico decision manager.....	300
Figura 99. Sequence Diagram	302
Figura 100. Scenario Smart Face Recognition	305
Figura 101. Scenario Gesture Recognition	307

Indice delle tabelle

Tabella 1. Identificazione e Classificazione dei modelli di filiale (Fonte: PwC, 2016).....	29
Tabella 2. Principali differenze tra BPR e BPI (Costantini e Cassaro, 2001).....	38
Tabella 3. Le 4 fasi del ciclo PDCA.....	39
Tabella 4. Il ruolo dell'IT nel processo di Reingegnerizzazione.....	46
Tabella 5. Principali patterns di processo (Hovey, 2005).....	52
Tabella 6. Patterns di processo supportati dagli approcci di modellazione.....	53
Tabella 7. Rappresentazione grafica di flow object di tipo Event.....	55
Tabella 8. Rappresentazione grafica di flow object di tipo Activity.....	56
Tabella 9. Rappresentazione grafica di flow object di tipo Gateway.....	56
Tabella 10. Rappresentazione grafica della categoria DATA.....	57
Tabella 11. Rappresentazione grafica dei CONNECTING OBJECTS.....	57
Tabella 12. Rappresentazione grafica delle SWIMLANES.....	58
Tabella 13. Rappresentazione grafica degli ARTIFACTS.....	58
Tabella 14. Definizioni di cyber space nella letteratura scientifica.....	81
Tabella 15. Fasi, obiettivi e modalità di protezione di una "infrastruttura critica".....	94
Tabella 16. Matrice della sicurezza fisica delle infrastrutture critiche (O'Rourke, 2007).....	94
Tabella 17. Misure per la sicurezza degli ATM (Fonte: Guerette & Clarke, 2003).....	99
Tabella 18. Differenze tra professionisti e rapinatori improvvisati secondo (Weisel, 2007).....	112
Tabella 19. Sistemi di protezione delle dipendenze bancarie (Messina, 2002).....	121
Tabella 20. Qual è la sua percezione sull'andamento dei reati negli ultimi anni?.....	139
Tabella 21. In particolare si è mai trovata a subire e/o assistere ad una rapina o tentata rapina in banca?.....	142
Tabella 22. In generale si poteva evitare la rapina o la tentata rapina?.....	144
Tabella 23. In generale secondo la sua opinione si possono evitare le rapine o i tentativi di rapina?.....	145
Tabella 24. Quanto ritiene importanti i seguenti interventi al fine di evitare il rischio rapina nel territorio?.....	145
Tabella 25. Quanto ritiene importanti i seguenti interventi al fine di evitare il rischio rapina nel territorio? (per area geografica).....	146
Tabella 26. Quanto ritiene importanti i seguenti interventi ai fini della prevenzione dei rischi e delle eventuali conseguenze connessi al verificarsi dell'evento rapina?.....	148
Tabella 27. Principali task relativi ai processi della gestione della sicurezza nelle dipendenze bancarie.....	163
Tabella 28. Configurazioni minime di sicurezza.....	169
Tabella 29. Definizioni di rischio.....	173
Tabella 30. Approcci metodologici al Risk Management.....	184
Tabella 31. Tabella Asset-Minaccia.....	209
Tabella 32. Matrice Minaccia-Asset per il calcolo dell'impatto.....	215
Tabella 33. Importo derubato/Danno economico derivante da rapine.....	219
Tabella 34. Ranking Reati-Serie storiche.....	223
Tabella 35. Tabella dei punteggi per ciascun reato.....	224
Tabella 36. Fattori vulnerabilità area.....	225
Tabella 37. Vulnerabilità specifiche della filiale.....	229
Tabella 38. Tecnologie analizzate in letteratura.....	233
Tabella 39. Descrizione tecnologie di protezione.....	239
Tabella 40. Esempio Tabelle di rilevanza.....	242
Tabella 41. Mappatura di esempio tra Configurazioni Minime di Sicurezza e Controlli di Sicurezza.....	244
Tabella 42. Funzionalità di general purpose sensor.....	258
Tabella 43. Confronto Situazione AS IS (valori medi) e TO BE (stima).....	304

Abstract.

Negli ultimi anni le filiali bancarie hanno subito un forte processo di cambiamento, prevalentemente lungo due direzioni. La prima ha riguardato l'evoluzione tecnologica che ha reso disponibili piattaforme di comunicazione (internet & mobile banking) sempre più complete in termini di numero di servizi a personalizzazione elevata. La seconda riguarda il mutamento delle politiche commerciali degli istituti bancari che danno un significato nuovo alle filiali: da luoghi in cui i clienti si recano per effettuare transazioni monetarie (depositi, pagamenti e prelievi) a punti commerciali di vendita in cui consulenti professionali offrono prodotti finanziari articolati e diversificati. Nelle filiali operatori specializzati si occupano di gestire le relazioni con i clienti erogando informazioni e consulenza per accrescere la fidelizzazione ed aumentare il cross selling. Le transazioni monetarie vengono delegate a strumenti automatici (ATM, totem, ecc.)

In entrambi i casi, le problematiche relative alla sicurezza rappresentano un aspetto critico. Benché la ricerca scientifica abbia prodotto risultati significativi relativamente alla definizione di modelli decisionali, processi organizzativi, e tecnologie per la protezione dei canali remoti (information and cyber security), poco o nulla è stato realizzato per migliorare i sistemi di protezione "fisica" degli asset presenti nelle filiali bancarie. La letteratura scientifica si è focalizzata prevalentemente su approcci di natura econometrico-statistica o criminologica.

Eppure i reati contro le filiali bancarie rappresentano un fenomeno in costante crescita nel mondo e tale fenomeno assume maggiore valenza nel territorio italiano, dove si registra il 60% dei reati su scala europea ed una fra le più capillari reti di filiali d'Europa (27903 filiali presenti sul territorio nazionale). Inoltre, la gestione dei processi di protezione fisica delle filiali rappresenta un onere significativo nei bilanci dei gruppi bancari che poco hanno fatto, negli ultimi 20 anni, per adeguare i loro sistemi di protezione alle forti innovazioni commerciali. Il crescente interesse dei criminali verso gli sportelli bancari è direttamente correlato al persistente uso di tecnologie di protezione obsolete che, peraltro, sono fonte di inefficienze organizzative, costi elevati, tempi di reazione lunghi e benefici, in termini di performance, tutti da dimostrare.

La ricerca oggetto del dottorato ha voluto approcciare il problema della sicurezza delle filiali bancarie in maniera sistemica al fine di coniugare le esigenze di una gestione integrata dei processi di sicurezza con le opportunità derivanti dai recenti sviluppi nell'ambito dell'*Internet of Things*. L'oggetto di studio diviene quindi l'intero sistema di protezione delle filiali con l'obiettivo di renderlo uno strumento efficace ed efficiente a disposizione dei gruppi bancari che consenta loro di:

- Aumentare l'efficienza dei processi decisionali e operativi di protezione, attraverso l'ottimizzazione delle risorse tecnologiche e la riduzione dei costi operativi.
- Aumentare l'efficacia del sistema di protezione verso gli attacchi criminali.
- Individuare una piattaforma tecnologica innovativa, basata sui recenti sviluppi dell'Internet of Things, per la gestione dell'intero processo di protezione di filiale.

Per raggiungere questi scopi, è stata utilizzato un approccio di *BPM, Business Process Management*. In quest'ottica, è stata utilizzata una metodologia di *BPR, Business Process Reengineering*, in accordo con quanto proposto da Hammer and Champy (2009)¹. Tale metodologia consente di dare risposta alle tre domande fondamentali poste da Roberts (1994)² per un progetto di BPR:

1. *How are things currently?*
2. *How should things be?*
3. *How can the gaps be reconciled between what is and what should be?*

La metodologia si compone di 4 passi:

1. **Modellazione della situazione attuale**, basata su un'approfondita analisi della letteratura scientifica e tecnica di settore, per la rilevazione dei dati secondari, e un'indagine qualitativa (*qualitative survey research*) per raccogliere dati primari dai process owner della sicurezza di gruppi bancari italiani.
2. **Analisi della situazione attuale**, per evidenziare ulteriori debolezze nell'attuale sistema di protezione delle filiali bancarie fornendo linee guida per riprogettare un *Intelligent protection system (IPS)* in grado di migliorare le prestazioni aziendali e individuare nuove opportunità dall' IoT.
3. **Modellazione della situazione target**. Considerando i risultati dello step 2, viene proposto un IPS in grado di sfruttare le opportunità offerte dal paradigma IoT. Il livello tecnologico della dipendenza bancaria può essere visto come un *Cyber Physical Space* in cui le misure di protezione (sia quelle basate sugli smart object che quelli tradizionali) sono in grado di interagire tra loro e con gli esseri umani attraverso una piattaforma digitale. Le componenti fondamentali dell'IPS vengono quindi descritte nel dettaglio:
 - a. Un modello di processo di gestione della sicurezza delle filiali reingegnerizzato, modellato tramite tecniche di *BPMN (Business Process Management Notation)*
 - b. Un modello innovativo per la valutazione dei rischi di filiale
 - c. Un modello di una piattaforma tecnologica a supporto della gestione della sicurezza basato sul paradigma dell'IoT. La piattaforma definisce le

¹ Hammer, M. and Champy, J. (2009), *Reengineering the Corporation: Manifesto for Business Revolution*, Harper Business Essentials

² Roberts, L. (1994), *Process reengineering: The key to achieving breakthrough success*. Asq Press

componenti necessarie per realizzare un *CPS (Cyber-Physical System)* in grado di trasformare il tradizionale problema della sicurezza fisica in uno di *Cyber-Physical Security*. A supporto della modellazione verranno utilizzati diagrammi *UML (Unified Modeling Language)*.

4. **Analisi delle prestazioni.** Si propone una discussione sui benefici dovuti all'introduzione dell'IPS in termini di efficienza (risparmio di tempo, riduzione dei costi) ed efficacia (sicurezza migliorata). L'analisi è stata validata da un campione rappresentativo di process owner della sicurezza bancaria, ed esperti IoT e operatori della sicurezza (forze dell'ordine e agenzie di sicurezza private).

INTRODUZIONE

Negli ultimi anni le filiali bancarie sono state investite da un forte processo di cambiamento, prevalentemente lungo due direzioni. La prima ha riguardato l'evoluzione tecnologica in ambito internet che ha reso disponibili piattaforme di comunicazione (internet & mobile banking) sempre più complete in termini di numero di servizi e più personalizzate; la seconda invece riguarda il mutamento delle politiche commerciali degli istituti bancari, con l'obiettivo di trasformare le filiali sempre più in un punto di vendita, dove proporre offerte diversificate e gestire le relazioni con i clienti erogando informazioni e consulenza per accrescere la fidelizzazione ed aumentare il cross selling. Negli ultimi anni, gli sportelli bancari stanno gradualmente modificando il loro aspetto. Da luoghi in cui i clienti di solito si recano per effettuare transazioni economiche (come deposito, pagamenti e prelievi) a punti commerciali di vendita in cui consulenti professionali offrono prodotti e servizi finanziari diversificati e complessi. Sta dunque cambiando il concept della filiale, che si sta trasformando nel tempo in un luogo sempre più accogliente, dove il cliente dialoga con il personale bancario per essere aggiornato sui nuovi prodotti, e per acquistare le soluzioni più adatte alle proprie esigenze. Per raggiungere questo obiettivo le filiali bancarie stanno cambiando aspetto fisico, gli ambienti diventano sempre più accoglienti e confortevoli; è importante diminuire le "barriere" all'ingresso, avere aree diversificate per le diverse attività e soprattutto postazioni dove l'operatore bancario possa dialogare in maniera conviviale con il cliente. L'idea di rendere più confortevole l'interazione del cliente trova realizzazione nell'eliminazione dal campo visivo del cliente quegli elementi di sicurezza antifurto (sbarre, scanner per persone, porte girevoli, uomini armati, telecamere a vista, ecc.) che, pur necessari per prevenire le rapine e garantire l'incolumità delle persone, contribuiscono ad aumentare il senso di ansia e di pericolo negli utenti e quindi spingono ad evitare la permanenza nella filiale stessa.

Il problema della sicurezza delle filiali bancarie (dette in gergo, dipendenze) è complesso ed investe diversi aspetti. Innanzitutto, bisogna considerare che gli incidenti impattano su due diversi concetti di sicurezza. Il primo è quello identificato come "*security*", riferito alla sicurezza del luogo e quindi alla protezione delle transazioni economiche che in esso si svolgono; il rischio è sia diretto, inteso come danno economico, che indiretto, nel senso di perdita d'immagine aziendale. Il secondo va sotto la voce "*safety*", intendendosi la sicurezza fisica dei dipendenti e dei clienti della banca presenti in filiale al momento dell'evento. È ormai dimostrato da diverse analisi del settore che l'unico modo per proteggere e salvaguardare adeguatamente sia la *security* dei luoghi che la *safety* dei dipendenti, è quello di concentrarsi sulla prevenzione dell'incidente; una volta che l'evento accade, l'obiettivo della banca è unicamente quello di evitare ogni tipo di reazione da parte dei presenti in modo da far cessare l'evento (rapina, furto, attacco al bancomat) nel più breve tempo possibile al fine di limitare i danni alla *security* e assicurare la *safety* degli utenti.

Alla luce di ciò, le attuali tendenze nelle esigenze degli istituti bancari si scontrano con la necessità di garantire la sicurezza nelle attività di filiale sia in termini di “sicurezza fisica”, nei due sensi di security e safety, intesa come protezione da rapine e furti con garanzie per l’incolumità di clienti e personale, sia come “sicurezza operativa”, relativa alla minimizzazione delle situazioni di rischio tipiche nell’esecuzione dei processi operativi (sequenza di operazioni bancarie sospetta, frodi allo sportello, furto di identità agli ATM, ecc.)

Capire quale sia il modo migliore per proteggere un luogo pubblico dove tante attività finanziarie sono disponibili su base giornaliera è estremamente difficile. Le banche si stanno facendo carico della sfida di lavorare a stretto contatto con le forze dell'ordine per individuare tendenze e modelli. Esse quindi pongono in atto questo bagaglio di conoscenze unitamente ai sistemi tecnologici per contrastare queste minacce con modalità nuove e creative. È proprio la disponibilità di nuove tecnologie che ha cambiato sostanzialmente volto alle banche negli ultimi 10 anni. In un primo tempo, le tecnologie sono state utilizzate per blindare le filiali, con le bussole automatiche all’ingresso, spesso dotate di metal detector e di lettore di impronte digitali. Recentemente, con l’adozione delle casseforti temporizzate, dei roller cash e dei cash-in/cash-out alle casse, la diminuzione del contante circolante e la maggiore importanza delle funzioni di consulenza, si tende a realizzare “filiali aperte”, senza bussole all’ingresso e con un contatto più diretto tra clienti e impiegati della banca, favorito anche dalla maggiore quantità di informazioni e di servizi disponibili online. Con la diffusione delle reti geografiche a banda larga (cablate e wireless), delle reti IP e di dispositivi in grado di collegarsi alle reti locali Ethernet e alle reti IP, la dotazione tecnologica delle filiali ha cambiato volto ed è diventata molto più complessa e rappresenta ormai l’aspetto critico per la gestione della sicurezza nonché la leva fondamentale per la riduzione dei costi operativi e l’aumento di valore del brand aziendale.

Negli ultimi 15 anni, sia la ricerca scientifica che gli istituti bancari hanno manifestato un notevole interesse verso la definizione di processi e tecnologie per il miglioramento della sicurezza dei canali remoti, a vantaggio della clientela e a protezione di dati e applicazioni della banca, concentrando la maggior parte degli investimenti nella sicurezza in ambito informatico. Tuttavia l’interesse verso la cybersecurity ha distolto l’attenzione dal concetto tradizionale di sicurezza intesa come sicurezza di filiali all’interno della quale si svolgono le transazioni fisiche.

Le principali agenzie ed autorità di pubblica sicurezza evidenziano come i reati contro le filiali bancarie rappresentano un fenomeno in costante crescita sia negli USA che in Europa. Inoltre, è necessario evidenziare come il tema della sicurezza delle filiali bancarie è di fondamentale importanza per il territorio italiano, dove si registra il 60% dei reati su scala europea.

Pertanto il crescente interesse dei criminali verso gli sportelli fisici e l'esistenza di sistemi di sicurezza obsoleti comporta la necessità di superare questi limiti introducendo sistemi in grado di garantire un livello di sicurezza che sia equiparabile al livello raggiunto per la sicurezza informatica.

Nella letteratura scientifica si evidenzia uno scarso numero di ricerche nell'ambito di sistemi innovativi a supporto della sicurezza nelle dipendenze bancarie, focalizzandosi prevalentemente su approcci di natura statistica o criminologica. Si tratta di un ambito in cui le informazioni disponibili sono estremamente ridotte e che quando accessibili sono coperte da riserbo in quanto di proprietà di aziende private o organizzazioni governative. Dal punto di vista tecnologico, i sistemi adottati finora si basavano su tecnologie automatizzate di prevenzione tuttora basate sull'analisi di filmati tramite videosorveglianza classica, con lo vantaggio di poter intervenire solo a posteriori per ricostruire le dinamiche dell'incidente ed individuare l'autore. Anche nel caso di sistemi di sorveglianza attiva, quelli attualmente in uso risultano essere scarsamente efficienti in quanto generano un numero di falsi allarmi eccessivamente elevato tale da rendere l'utilizzo di tali tecnologie inutile e antieconomico, mentre accade molto spesso che le situazioni di vero allarme non vengano segnalate o sfuggano al controllo. Un approccio sistemico di coniugare le esigenze di una gestione integrata dei processi di sicurezza e le opportunità che derivano dai recenti sviluppi nell'ambito del cosiddetto Internet of Things.

Questo lavoro di ricerca si concentra dunque sulle tematiche relative alla sicurezza delle filiali bancarie con l'obiettivo di individuare modelli per l'ottimizzazione delle performance del processo di gestione della sicurezza che consentano di aggregare e sfruttare in maniera sistemica tutte le tecnologie presenti all'interno della filiale, consentendo agli istituti bancari di raggiungere i seguenti scopi:

- Aumento dell'efficienza attraverso ottimizzazione delle risorse tecnologiche una riduzione dei costi operativi.
- Aumento dell'efficacia delle misure di prevenzione e protezione da attacchi fisici.

Nello specifico, i risultati che si intendono ottenere sono riassumibili come segue

I risultati ottenuti da questo lavoro di ricerca sono riassumibili come segue:

- **Definizione di un modello reingegnerizzato dei processi di sicurezza delle dipendenze bancarie.** Al fine di ottimizzare in termini di performance di efficienza il processo di gestione della sicurezza, si intende proporre un approccio metodologico basato sul paradigma del Business Process Reengineering che, applicato alle filiali bancarie, contribuisce a rendere più "intelligenti" i processi di gestione della sicurezza. In particolare, viene presentata un'approfondita analisi dell'attuale sistema di protezione fisica delle banche per evidenziare le sue debolezze organizzative e tecnologiche ed è stato proposto un sistema di protezione intelligente che sfrutta le opportunità che l'introduzione di IoT può dare al processo di gestione della sicurezza

in termini di efficienza (risparmio di tempo, riduzione dei costi) e efficacia (sicurezza migliorata). Per superare le limitazioni della scarsa disponibilità di informazioni necessarie per la modellazione delle attività, è stato adottato un approccio multi-metodo alla raccolta dei dati e alla convalida dei risultati. L'approccio si basa su una revisione completa della letteratura e un'indagine qualitativa che coinvolge un campione di process owners.

- **Definizione di un modello innovativo per la valutazione del rischio di filiale.** L'analisi della letteratura scientifica, dei report professionali ed i colloqui con i process owner evidenziano che i sistemi di protezione attualmente utilizzati non sono integrati e sono di dubbia efficacia. Inoltre i modelli di valutazione attualmente adottati sono in grado di fornire un indice di rischio della filiale ma non un profilo di rischio, con la possibilità di suggerire opportune contromisure di protezione adatte alla specifica filiale. Inoltre tali modelli sono intrinsecamente statici e non predittivi, non tenendo conto dell'alta dinamicità degli eventi in questo dominio di applicazione e ponendo scarsa attenzione ai cosiddetti fattori endogeni.

Al fine di raggiungere i suddetti obiettivi, il documento è così articolato:

Nel primo capitolo si proporrà di contestualizzare il problema della gestione della sicurezza fisica nelle dipendenze bancarie e quindi giustificare le ragioni di questo studio. In particolare andremo a descrivere l'evoluzione delle filiali bancarie che nel corso degli anni hanno cambiato il loro assetto trasformandosi sempre più in luoghi "aperti" e accoglienti, dove il cliente può dialogare con il personale bancario per essere aggiornato sui nuovi prodotti, e per acquistare le soluzioni più adatte alle proprie esigenze.

L'idea di rendere più confortevole l'interazione del cliente trova realizzazione nell'eliminazione dal campo visivo del cliente quegli elementi di sicurezza antifurto (sbarre, scanner per persone, porte girevoli, uomini armati, telecamere a vista, ecc.) che, pur necessari per prevenire le rapine e garantire l'incolumità delle persone, contribuiscono ad aumentare il senso di ansia e di pericolo negli utenti e quindi spingono ad evitare la permanenza nella filiale stessa.

Verrà messo in evidenza come l'evoluzione della natura delle filiali bancarie secondo una prospettiva di "apertura al cliente", unitamente alle problematiche relative all'incidenza dei reati (che rappresentano tutt'ora un fenomeno in costante crescita sia negli USA che in Europa), rappresenta una sfida per la gestione della safety e della security delle filiali. Il crescente interesse dei criminali verso gli sportelli fisici e l'esistenza di sistemi di sicurezza obsoleti spinge verso un cambiamento nei processi di gestione della sicurezza.

Nel secondo capitolo verranno descritte le modalità, gli strumenti e le leve per attuare questo cambiamento.

Andremo a studiare, dunque, i principali approcci al BPM, effettuando una review della letteratura scientifica in merito alle metodologie di BPR e BPI con l'obiettivo di definire un opportuno approccio metodologico per la nostra ricerca.

Per ciò che concerne gli strumenti di rappresentazione dei processi verrà effettuato uno studio della letteratura al fine di identificare il modello di rappresentazione più adeguato alle nostre esigenze. Si andrà inoltre a verificare l'esistenza della convergenza tra cambiamenti organizzativi e il ruolo dell'IT, con particolare attenzione all'Internet of things, per il miglioramento dei processi.

Nel terzo capitolo verrà effettuata la rilevazione e l'analisi della situazione attuale relativa ai processi di gestione della sicurezza della safety e security delle dipendenze bancarie. Questa attività verrà realizzata secondo l'approccio metodologico definito nel capitolo due. Nello specifico per l'identificazione della situazione attuale si utilizzeranno fonti secondarie quali analisi della letteratura scientifica e report sulla sicurezza e fonti primarie ovvero focus group con esperti della sicurezza bancaria e indagine statistiche sulla percezione della sicurezza da parte dei clienti.

Gli ultimi due capitoli si concentreranno sulla definizione della situazione to be a seguito dell'identificazione dei limiti e dei punti di debolezza che emergeranno nel capitolo tre. In particolare il quarto capitolo riguarderà gli aspetti decisionali relativi al processo di gestione della sicurezza ed è finalizzato alla definizione di un nuovo modello di rischio

Nel quinto ed ultimo capitolo verranno presentate le soluzioni migliorative dal punto di vista organizzativo e tecnologico, grazie all'introduzione di un Intelligent Protection System caratterizzato da smart object all'interno dei quali sono inseriti sensori capaci di individuare ed interpretare segnali di tipo diverso.

Il flusso logico di questo lavoro può essere rappresentato con la seguente immagine.

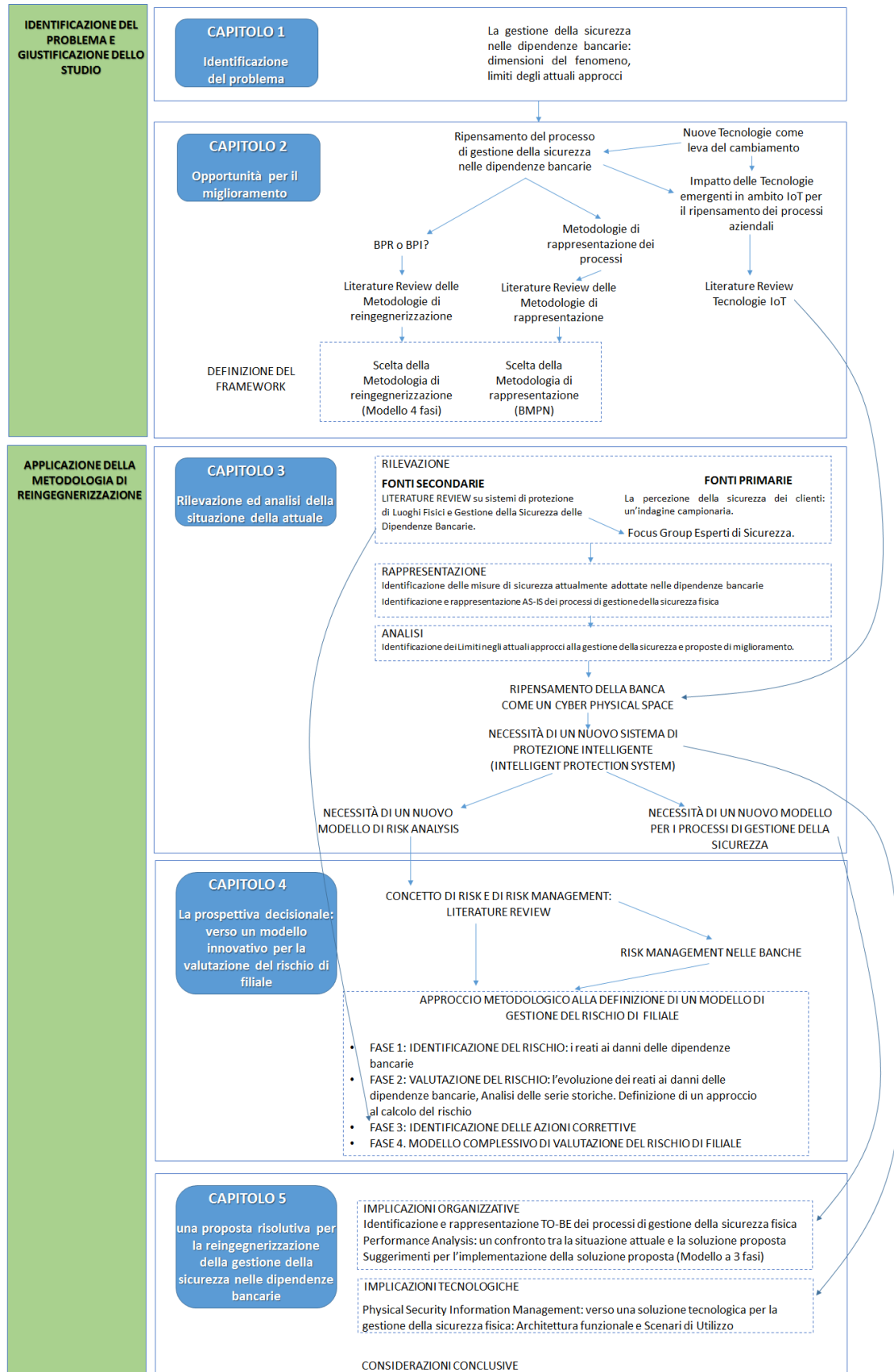


Figura 1. Struttura logica della tesi

Il Metodo della ricerca

La metodologia proposta in questo lavoro è stata derivata dalla letteratura scientifica attualmente disponibile. Il processo di ricerca adottato è rappresentato dal seguente diagramma.

- Step 0. Inizializzazione. Abbiamo selezionato le principali basi di dati utilizzate in ambito accademico, tra cui EBSCO, SCOPUS e Web of Science, e anche Google Scholar. Successivamente è stata inizializzata una lista L di termini di ricerca in lingua inglese, relativi ai domini di ricerca investigati. A titolo esemplificativo, si riportano le seguenti keywords inizialmente utilizzate: *Business Process Management, Business Process Reengineering, Internet-of-Things, smart objects, computer vision, artificial intelligence, security management, protection systems, criminal attacks, risk and safety*
- Step 1. Ricerca: Abbiamo effettuato la ricerca delle parole chiavi appartenenti alla lista L. I termini sono stati accoppiati anche alla keyword “bank branch”.
- Step 2. Screening dei paper rilevanti: Abbiamo analizzato gli abstract dei papers trovati per verificare se erano in linea con le nostre esigenze di ricerca. Durante questo processo, è stato aggiornato il set di parole chiave (ad esempio, aggiungendo termini quali “Cyber Physical Systems”, “Smart Environment”, “Synthetic Sensors”), ritornando al passo 1 della metodologia.
- Step 3. Analisi della letteratura scientifica. È stata effettuata una review esaustiva della letteratura recuperata, per ciascun dominio di riferimento investigato (Business Process Management, IoT, Security and Safety, Risk Management).

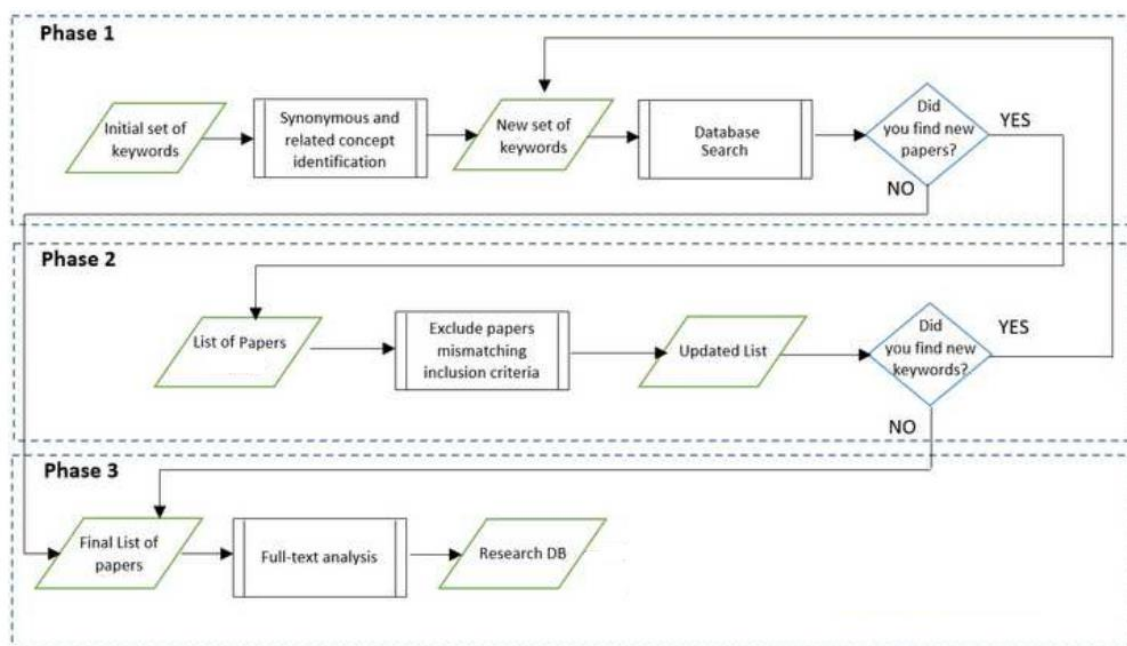


Figura 2. Processo di analisi delle fonti derivate dalla letteratura scientifica

Il focus group

L'ambito della sicurezza bancaria è caratterizzato da un elevato grado di riservatezza, con pochi documenti pubblicamente disponibili. Ciò è dovuto essenzialmente al fatto che la conoscenza in quest'ambito è posseduta da un numero ristretto di società che si occupano di security e che fondano il loro business sulla consulenza di procedure e tecnologie per la preservazione degli asset strategici delle dipendenze bancarie.

Quello che dunque si intende fare è superare queste limitazioni ricorrendo ad un approccio qualitativo alla ricerca basato sulla metodologia del Focus Group.

Nella letteratura compaiono varie definizioni di focus group, ma la maggior parte condivide elementi comuni, cioè piccoli gruppi di persone che possiedono determinate caratteristiche e che si incontrano per fornire dati di natura qualitativa in una discussione focalizzata (Krueger, 1994). L'intervista di focus group consiste in un colloquio di approfondimento guidato di un piccolo gruppo di individui relativamente omogeneo selezionato appositamente dal ricercatore per affrontare un argomento specifico.

Per dare una definizione più formale il focus group è una tecnica non standardizzata di rilevazione dell'informazione, basata su una discussione, che è solo apparentemente informale, tra un gruppo omogeneo di persone per approfondire un tema o particolari aspetti di un argomento. Si svolge come un'“intervista di gruppo” guidata da un moderatore che, seguendo una traccia (griglia) più o meno strutturata, propone degli “stimoli” ai partecipanti. Gli stimoli possono essere di tipo verbale (domande dirette, frasi, definizioni, associazioni) oppure visivo (fotografie, disegni, vignette, filmati). Dalle risposte a questi stimoli scaturisce (o dovrebbe scaturire) di volta in volta la discussione. La caratteristica, che poi è anche il grande pregio del focus group, sta proprio nell'interazione che si crea tra i partecipanti, interazione che produce idee in misura assai maggiore rispetto all'intervista singola sia a livello di quantità sia a livello di qualità di approfondimento.

La premessa da cui molti autori partono per “giustificare” l'utilizzo di tecniche basate sugli esperti è che esse rappresentano una risposta “alternativa” in contesti caratterizzati da tempi e risorse a disposizione limitati oppure da particolare incertezza. Quando infatti le informazioni non sono reperibili, o come accade nel nostro caso i dati e le informazioni sono coperti da riserbo e, quindi, la possibilità di accedervi direttamente è estremamente complessa se non impossibile, il focus group è una buona tecnica di rilevazione per superare l'ostacolo. Si parte dall'idea che il giudizio informato degli esperti offra un valido supporto alla ricerca. I focus group possono essere usati nelle fasi preliminari o esplorative di uno studio (Kreuger 1988), parliamo in tal caso di **Focus group Esplorativo**; durante uno studio, forse per valutare o sviluppare un particolare programma di attività (Race et al., 1994) o dopo che un programma è stato completato, per valutare il suo impatto, per confermare e validare le ipotesi fatte all'inizio della ricerca (**Focus group Confermativo**) o per generare ulteriori percorsi di ricerca. Possono essere utilizzati come metodo a sé stante o come complemento di altri metodi, in particolare per la triangolazione (Morgan 1988) e il controllo

di validità. I focus group possono aiutare a esplorare o generare ipotesi (Powell & Single 1996) e sviluppare domande o concetti per questionari e guide di interviste (Hoppe et al 1995; Lankshear 1993). Solitamente questa tecnica viene usata in integrazione con altre. Una modalità piuttosto comune prevede l'uso combinato di focus group per l'indagine esplorativa (volta a individuare le ipotesi da sondare) e questionario per la successiva verifica statistico-quantitativa. La tecnica del focus group ha subito cambiamenti e innovazioni nel tempo, al punto che oggi ne esistono diverse varianti. Il modello più diffuso e conosciuto prevede le seguenti procedure:

- **DEFINIZIONE DELL'OBIETTIVO DELLA RICERCA.** Si tratta, a monte, di definire i bisogni conoscitivi e le domande d'indagine a cui la ricerca intende rispondere, nonché di decidere se il problema rientra tra quelli affrontabili con la tecnica del focus group.
- **SCELTA DEI PARTECIPANTI.** La composizione del gruppo è cruciale. E' necessario bilanciare due esigenze contrapposte: da una parte il gruppo deve risultare omogeneo al proprio interno, per facilitare lo scambio di opinioni e la reciproca comprensione concettuale e linguistica, dall'altra deve essere quanto più possibile eterogeneo, per consentire un ventaglio di opinioni il più ampio possibile.
- **COSTRUZIONE DELLA TRACCIA D'INTERVISTA.** Non si tratta di una traccia rigida, ma di una guida per la discussione. Contiene in genere poche domande. Con temi che richiedono una discussione mediamente approfondita.

In questo lavoro la tecnica del focus group è stata utilizzata due volte. Nel primo caso è stata necessaria per sopperire alla mancanza di un numero sufficiente di dati e informazioni dovute al fatto che i processi di gestione della sicurezza e le informazioni ad essi connesse sono coperti da riserbo data la natura estremamente sensibile dell'argomento.

Nel secondo caso, invece, questo metodo di analisi è stato utilizzato a scopo confermativo. Considerando la mancanza di esempi di best practices e, non potendo implementare il sistema poiché i tempi di esecuzione risulterebbero elevati e l'accettazione di cambiamenti radicali da parte dei manager della sicurezza, nonché dei sindacati risulterebbe molto difficile, è stata effettuata una valutazione qualitativa su quelle che dovrebbero essere le potenzialità derivanti dall'adozione dello IoT nei processi di gestione della sicurezza coinvolgendo gli esperti di sicurezza che hanno preso parte al primo focus group.

In particolare gli esperti coinvolti sono stati 9 soggetti scelti tra opinion leader altamente qualificati del settore della sicurezza pubblica e privata e altri soggetti sensibili alle tematiche oggetto d'indagine:

- il vicequestore di Cosenza con delega all'anticrimine,
- il responsabile del Cyber Security Competence Center di NTT DATA S.p.A
- il caporedattore di una TV locale responsabile della cronaca nera,
- il responsabile del maggiore gruppo di vigilanza privata calabrese,
- i responsabili sicurezza di alcuni gruppi bancari italiani.

CAPITOLO 1. Il problema della gestione della sicurezza fisica delle dipendenze bancarie

1.1 La banca e le dipendenze bancarie

La banca può essere definita come un *“istituto che compie operazioni monetarie e creditizie, e la cui funzione principale, oltre alla custodia di valori e ai pagamenti, è quella di farsi intermediario nella circolazione della moneta, raccogliendo il risparmio e concedendolo in prestito”* (Treccani, 2011). Questa definizione mette in evidenza quella che la Banca d'Italia (2009) individua come la principale funzione economica svolta dalla banca ovvero l'intermediazione che *“consiste nel trasferire risorse finanziarie (ossia, moneta) dai soggetti che ne dispongono a quelli che invece ne difettano, ponendosi come controparte di ciascuno di essi”*. Tuttavia, pur contraddistinguendo l'attività bancaria, la funzione di intermediazione nell'ambito del credito monetario non è l'unica svolta. Un ventaglio di diverse funzioni le si sono affiancate da quando, in tempi recenti, il Testo Unico bancario³ ha sancito che: *“le banche esercitano, oltre all'attività bancaria, ogni altra attività finanziaria, secondo la disciplina propria di ciascuna, nonché attività connesse o strumentali”*. Questo intervento legislativo, che ricalca il dettato della seconda direttiva comunitaria⁴, consente di mettere da parte la legge bancaria del 1936 che sanciva una separazione tra credito a breve termine, affidato alle banche di credito ordinario, e credito a medio-lungo termine, responsabilità degli istituti di credito speciale. La nuova normativa offre, perciò, alle banche vasti spazi di diversificazione operativa; si va da banche la cui diversificazione è ai livelli minimi, *retail bank*, le cui attività sono unicamente quelle di raccolta di risparmio tra il pubblico e dell'attività di concessione del credito, a banche in cui si è operata la più ampia diversificazione, le cosiddette *universal bank*, che il Financial Times (2011) definisce conglomerati finanziari che offrono congiuntamente e con diverse combinazioni i servizi di retail, di wholesale⁵ e di investment⁶ banking; a livelli di diversificazione intermedia, vi sono poi banche con un diverso grado di specializzazione lungo le dimensioni relative alla tecnologia adottata, al tipo di prodotto ed al segmento di clientela (Onado, 2000). Partendo proprio dalla combinazione di queste tre dimensioni, Caparvi (2006) individua le distinte aree di business diversamente rappresentate in ordine alla maggiore o minore

3 Art. 10 del Testo unico bancario, d.lgs. 1 settembre 1993, n. 385 e successive modificazioni e integrazioni.

4 Seconda direttiva 89/646/CEE del Consiglio, del 15 dicembre 1989, relativa al coordinamento delle disposizioni legislative, regolamentari e amministrative riguardanti l'accesso all'attività degli enti creditizi e il suo esercizio e recante modifica della direttiva 77/780/CEE.

5 Il wholesale banking è quell'attività di banca che concentra i suoi rapporti con una clientela ristretta e qualificata, composta prevalentemente da grandi imprese, governi e grandi amministrazioni pubbliche.

6 L'investment banking è quell'attività di banca (o divisione di una banca) che si occupa principalmente di assistere individui, aziende e governi nella raccolta di capitale attraverso le sottoscrizioni e nell'emissione di titoli.

specializzazione dell'intermediario bancario. Si fa quindi riferimento alle seguenti principali aree di attività:

- Il *retail banking*, è l'attività di una banca (o sezione di una banca) che si focalizza su un target costituito da un gran numero di piccoli clienti privati (famiglie e piccole imprese) e che ha come principale funzione quella di intermediazione creditizia. Come sottolineato in (Caparvi, 2006), trattasi di servizi scarsamente personalizzabili, offerti con modalità distributive di tipo standardizzato su mercati altamente competitivi;
- Il *private banking*, è l'attività di una banca (o sezione di una banca) che, come evidenziato in (Grohmann & Vacca, 1994), si contraddistingue per la gestione estremamente personalizzata del rapporto bancario per via dell'elevata frazione del volume d'affari generata dal singolo cliente (in genere persone fisiche individuali e famiglie caratterizzate da un alto grado di reddito e/o ricchezza personale).
- Il *corporate & investment banking*, è l'attività di una banca (o sezione di una banca) che si occupa di offrire servizi finanziari ad aziende di grandi dimensioni, ad istituti finanziari, governi ed altro. Come messo in luce in (Caparvi, 2006), questa è un'area assai ampia e complessa di attività che necessita di servizi altamente personalizzati, comprendendo sia il reperimento e la gestione dei finanziamenti (*corporate finance*), sia il servizio di assistenza verso le imprese nel processo di emissione di titoli e nella ricerca di sottoscrittori (*underwriting*), che l'*intermediazione titoli* per conto proprio o per conto terzi; quest'ultima attività si differenzia dalle precedenti perché non è indirizzata soltanto alle imprese ma a tutto il mercato.

1.2 I modelli distributivi bancari

Le banche, come del resto la gran parte degli altri operatori economici, si trovano a fronteggiare un contesto socio-economico in profonda e continua evoluzione. Il mutamento dei fattori sociali e demografici, l'innovazione tecnologica ed i cambiamenti culturali stanno avendo importanti ripercussioni sul business bancario. La crisi che nell'ultimo decennio ha colpito un gran numero dei paesi sviluppati, si innesta su questo processo di trasformazione, accentuando, almeno in parte, alcuni trend (come ad esempio lo sviluppo dell'e-banking e la maggiore attenzione al prezzo da parte della clientela), in parte accelerando alcune evoluzioni regolamentari e di gestione di politica economica (la riduzione del contante effetto dei vincoli più stringenti per la tracciabilità dei pagamenti). L'insieme di questi fattori delinea un quadro di profonda trasformazione nella fruizione dei servizi bancari e di quelli allo sportello in particolare.

Le nuove evoluzioni del modello distributivo puntano a valorizzare la relazione con la clientela per costruire e mantenere un solido rapporto fiduciario: venire incontro ai

fabbisogni dei clienti, oggi molto più esigenti rispetto a qualche anno fa, passando quindi dall'offerta di servizi a valore aggiunto.



Figura 3. Evoluzione del modello di servizio (Fonte: Elaborazione KPMG Advisory, 2013)

Il consolidamento attraverso processi di fusione e acquisizione e la ricerca di efficienze sul fronte dei costi costringono le banche a pianificare e gestire l'integrazione, standardizzando le misure di sicurezza e le nuove normative in materia di gestione del rischio operativo impongono l'adozione di metodologie appropriate e lo sviluppo di applicativi per la sua gestione (Basilea III, 2010), regolamenti della Banca d'Italia e standard internazionali (Banca d'Italia, 2013) spingono le banche ad individuare gli impatti di possibili eventi catastrofici (*business continuity*) e ad adottare appropriati piani di contrasto. Nuovi progetti avviati a livello di sistema bancario (es. Carte Microcircuito e *Corporate Banking*) tendono a trasformare la sicurezza in un fattore abilitante per l'erogazione di servizi ad elevato valore aggiunto. Multicanalità e nuove tecnologie rendono infine la convergenza digitale una realtà, permettendo di fidelizzare maggiormente i clienti, ma al costo di un più elevato rischio di furto dell'identità digitale. L'esperienza dimostra che sono stati fatti molti passi in avanti per aumentare il livello di sicurezza del sistema, ma restano ancora diverse criticità. Si segnalano in particolare come aree di attenzione:

- l'esigenza di adottare sempre l'analisi dei rischi come prerequisito per l'impostazione di strategie della sicurezza;
- la necessità di applicare con rigore degli strumenti di pianificazione degli investimenti in sicurezza;
- l'esigenza di implementare sistemi di pianificazione *ex-ante* e controllo *ex-post* in merito all'efficacia e all'efficienza della contromisure di sicurezza;

- l'opportunità di aumentare il livello di integrazione della sicurezza a livello di processi e linee di business;
- l'esigenza di diffondere maggiormente il sapere tecnico e di attivare nel contempo le "comunità di *practice*" di sicurezza.

	Driver del cambiamento	Implicazioni in ottica Sicurezza
Consolidamento	<ul style="list-style-type: none"> •Fusioni/acquisizioni/dismissioni •Focus su efficienza •Integrazione organizzazione/sistemi 	<ul style="list-style-type: none"> •Pianificare e gestire l'integrazione •Condividere e standardizzare le misure di sicurezza
Basilea 2	<ul style="list-style-type: none"> •Valutazione e misurazione RO •Equity capital ratios •Readiness entro 2006 	<ul style="list-style-type: none"> •Definire le metodologie di calcolo del rischio e sviluppare applicativi per la gestione del rischio operativo (e IT)
Business Continuity	<ul style="list-style-type: none"> •Guidelines Banca d'Italia •Normative e standard internazionali •Maggior attenzione eventi impattanti 	<ul style="list-style-type: none"> •Individuare possibili eventi catastrofici •Definire un piano d'azione da rivedere a scadenze regolari
Nuovi progetti	<ul style="list-style-type: none"> •EMV/ Microcircuito •Corporate Banking Interbancario 	<ul style="list-style-type: none"> •Interpretare la sicurezza come fattore abilitante per i nuovi servizi •Predispone normative e processi organizzativi mirati
Multicanalità e nuove tecnologie	<ul style="list-style-type: none"> •Accesso ai servizi finanziari multicanale •Convergenza digitale •Servizio e fidelizzazione cliente 	<ul style="list-style-type: none"> •Gestire la sicurezza, anche quando affidata a partner esterni •Negoziare contratti basati su SLA

Figura 4. Cambiamenti in atto nel settore bancario

Per rispondere alle nuove sfide sollevate dall'evoluzione tecnologica e dai nuovi scenari normativi e di business, le banche devono fare lo sforzo per completare la transizione da un approccio alla sicurezza di taglio tecnologico ad uno realmente manageriale, capace d'integrare aspetti tecnologici, organizzativi e culturali. *Corporate Security*, in particolare, deve sapersi proporre come centro servizi che supporta le altre funzioni aziendali e le aiuta a ridurre i rischi collegati ai processi di business. *Corporate Security* deve perciò assicurare un approccio esaustivo, coprendo le tematiche di sicurezza informatica, fisica e di *business continuity*: dalla fase di progettazione, all'implementazione, sino all'esercizio. L'esperienza e *benchmarking* internazionali dimostrano con chiarezza che l'efficacia della gestione della sicurezza tende a migliorare se vengono implementati adeguati meccanismi e processi organizzativi e se *Corporate Security* tende ad assumere un ruolo proattivo e prossimo ai processi di business della banca. In un contesto di forte cambiamento è sempre più importante riuscire ad integrare i processi di sicurezza con la "macchina organizzativa" bancaria (Lorini, 2005).

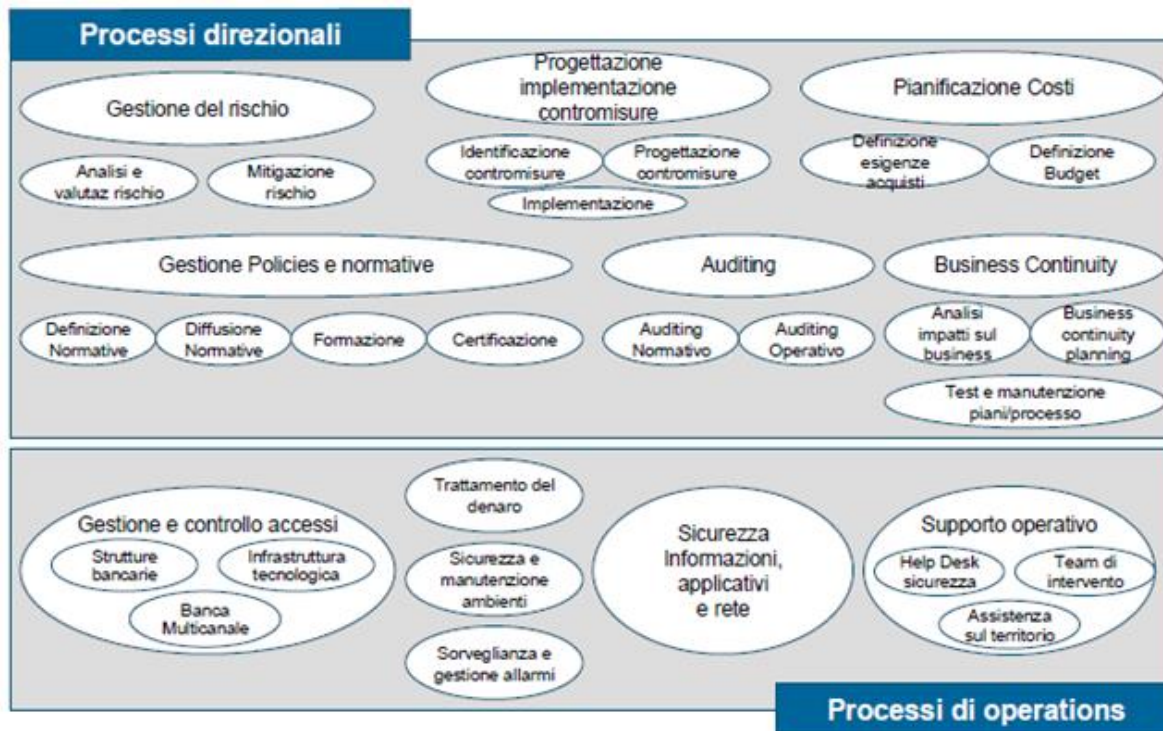


Figura 5. Integrazione processi direzionali ed operativi nella gestione del rischio bancario

Da un punto di vista organizzativo, il presidio efficace delle tematiche di sicurezza richiede sempre più la capacità di coniugare visione d'insieme e soluzioni organizzative innovative. Mentre in passato le organizzazioni bancarie erano caratterizzate da una gestione separata delle funzioni di security, negli ultimi anni si sta assistendo ad un vero e proprio processo di integrazione dei processi entro una direzione centrale, sotto il controllo diretto del CEO.

Le funzioni di sicurezza tipiche di un istituto bancario, mirate a garantire la continuità dei processi operativi e dei servizi (business continuity), la privacy dei clienti, l'incolumità delle persone (safety) e la preservazione degli assets materiali ed immateriali della banca (sicurezza fisica e sicurezza logica) tendono ad essere concentrate in un'unica funzione (Direzione Sicurezza) al fine di creare sinergie e integrazioni tra processi, strumenti, competenze e risorse presenti nella banca in modo da perseguire un'efficace Pianificazione e controllo della strategia di gestione del rischio e del piano integrato di Sicurezza e di Comunicazione in maniera integrata risultati e obiettivi di Sicurezza verso il top management e le altre direzioni aziendali

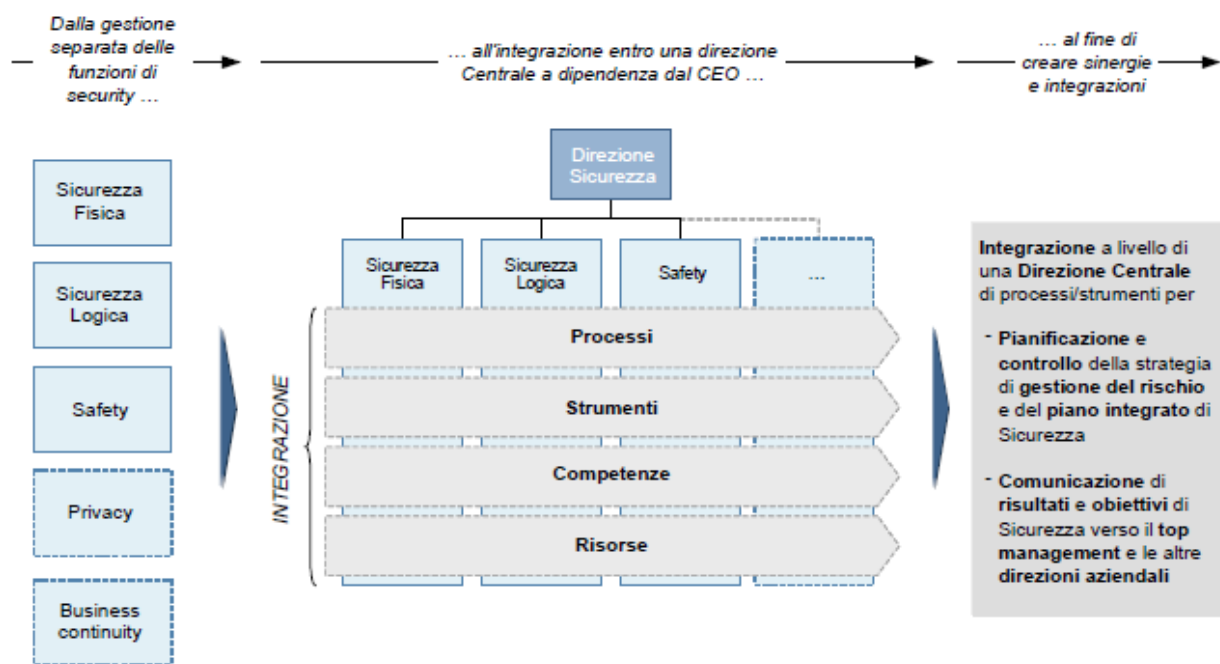


Figura 6. Evoluzione degli approcci organizzativi nella gestione del rischio bancario

Oltre ai meccanismi di tipo organizzativo, le banche possono migliorare il proprio profilo in termini di sicurezza adottando strumenti di *governance* quali il *Security Tableau de Bord* e il *Security Knowledge Management*, con evidenti benefici in termini di capacità di tracciare l'efficacia delle contromisure adottate, comunicazione delle informazioni, migliore reportistica di sicurezza e maggiore sensibilizzazione del personale. Soluzioni avanzate di sicurezza quali i *Security Operation Center (SOC)* permettono inoltre di gestire in modo centralizzato e in tempo reale le problematiche di sicurezza, riducendo i tempi di reazione e aumentando la capacità di risposta della banca rispetto alle minacce a cui è esposta. E' il caso di ricordare, infine, come *Corporate Security* possa svolgere un ruolo centrale nel rendere più sicuro il business aziendale attraverso la predisposizione di efficaci misure di *business continuity* e *disaster recovery*, nonché di integrazione delle iniziative e delle tecnologie di contrasto al rischio di furto dell'identità digitale degli utenti di servizi di banca multicanale.

Per rispondere alle sfide di un contesto in continua evoluzione le banche devono adottare un approccio integrato alla sicurezza e alla security governance.

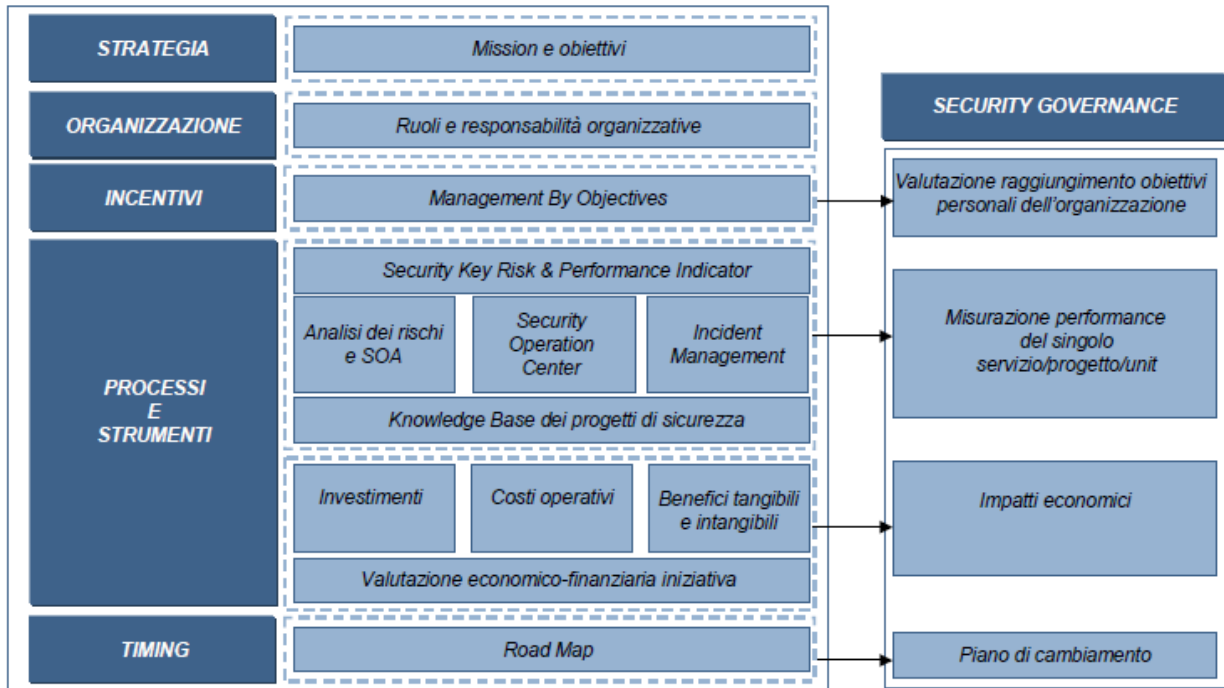


Figura 7. Approccio integrato alla sicurezza e alla security governance

Per molti anni Il paradigma del retail banking è stato basato sul concetto di prossimità fisica come leva per raggiungere obiettivi di business e per la diffusione della brand awareness sul territorio. Le dipendenze bancarie (o filiali) sono spazi fisici che tradizionalmente rappresento il punto di contatto tra gli istituti bancari ed i propri clienti.

Storicamente, la filiale ha sempre svolto sia un ruolo transazionale e di credito (legato al sistema dei pagamenti e alla gestione del contante/liquidità dei Clienti) che relazionale (flagship), rappresentando l'elemento predominante (se non l'unico) del sistema distributivo. Le filiali vengono distribuite sul territorio in modo da ottenere la massima penetrazione del mercato evitando, al contempo, fenomeni di cannibalizzazione tra dipendenze bancarie geograficamente vicine.

Recentemente, diversi fattori quali il calo di redditività, trasformazioni di carattere socio demografico, cambiamenti nelle abitudini dei consumatori e sviluppo della tecnologia, ha modificando il modello distributivo, secondo una prospettiva di multicanalità. Ne consegue un ripensamento del ruolo della Filiale: a causa del superamento del paradigma della prossimità fisica è, cioè, possibile l'esecuzione in via remota delle operazioni che hanno tipicamente costituito il core business della Filiale, rendendo operativo il concetto di "Banca comoda". Questo non significa però che la Filiale, intesa come punto di contatto fisico con la clientela, sia destinata a scomparire del tutto. Come sottolineato da una recente survey di

PwC (2016) tra i senior executives delle principali banche, sebbene in passato si è assistito ad un calo del numero di clienti delle dipendenze bancarie, si prevede che negli anni futuri la filiale rimarrà comunque uno dei canali più utilizzati, preceduto solo dall'online banking. Si va dunque affermando un modello in cui la Filiale si configura non più solo come spazio fisico legato all'offerta di servizi ma anche come luogo di incontro per le comunità di cui vuol rappresentare il punto di riferimento e come punti commerciali di vendita in cui consulenti professionali offrono prodotti e servizi finanziari diversificati e complessi. In questa nuova logica, viene ripensato l'intero modello di servizio, nelle dotazioni, nella struttura fisica/layout; andrà ridefinito il ruolo, necessariamente diverso da quello tradizionale di solo presidio del territorio o di sola operatività transazionale. Mentre le figure professionali legate all'esecuzione e al settlement delle transazioni andranno progressivamente scomparendo, si affermerà sempre più il ruolo del consulente della propria clientela, che trova una ragion d'essere proprio nelle motivazioni e quindi nelle tipologie di operazioni che spingono ad entrare in Filiale. Le evoluzioni organizzative prospettate, anche a livello di maggiore flessibilità nei ruoli e nell'organizzazione del lavoro in Filiale, dovranno necessariamente essere accompagnate da strumenti normativi e contrattuali di sistema che supportino questo cambiamento, ovvero da un framework normativo comune che consenta alla Banche di gestire con maggiore flessibilità l'attribuzione delle mansioni del personale in base al servizio da erogare al Cliente.

Le principali strategie distributive degli istituti bancari sono di seguito riassumibili (CeTiF, 2014):

- **SINGOLO CANALE.** Il cliente utilizza un unico canale o punto di contatto per tutte le attività dispositive e informative. La banca gestisce un'unica modalità di relazione con il cliente, prevedendo l'operatività dei correntisti unicamente presso la filiale bancaria.
- **MULTICANALITÀ** Il cliente utilizza diversi canali o punti di contatto (filiale, call center, sito web) gestiti in modo indipendente dalla banca, talvolta anche mediante brand differenti. Per quanto riguarda il modello di relazione, la gestione del cliente avviene attraverso silos funzionali e relazionali.
- **CROSS-CANALITÀ** Il cliente ha la possibilità di utilizzare diversi canali o punti di contatto (filiale, call center, sito web), in base alle proprie preferenze, in quanto gestiti in modo integrato dalla banca. L'approccio evolve verso una visione unica del cliente e della relazione, sebbene la gestione rimanga attraverso silos funzionali.
- **OMNICANALITÀ** Il cliente interagisce con diversi canali o punti di contatto nell'acquisto/fruizione di uno o più prodotti/servizi (filiale, call center, sito web, mobile banking, social media...). Da parte della banca c'è una visione olistica della relazione e nel governo dei percorsi del cliente che ha il massimo grado di autonomia nella scelta dei canali e nelle modalità con le quali relazionarsi con l'istituto bancario.

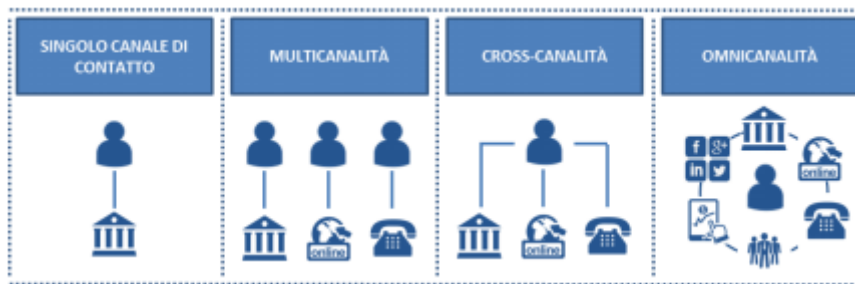


Figura 8. Scenari evolutivi per le strategie distributive (Fonte: CeTiF, 2014)

La banca, agli occhi del cliente, si è da sempre identificata attraverso la dipendenza bancaria, in grado di rispondere alle sue principali esigenze, quali la gestione del denaro, le operazioni transazionali e l'accesso al credito.

Queste strategie hanno determinato la proliferazione di reti distributive molto capillari sul territorio, con filiali "full service", ciascuna delle quali è in grado di fornire indistintamente tutti i prodotti/servizi dell'offerta commerciale. Questa tipologia di dipendenze si caratterizzano per la presenza completa dei ruoli tradizionali di filiale (direttore, vice-direttore, cassiere) e la presenza di personale con competenze specialistiche (gestore, consulente, promotore finanziario...) in grado di rispondere a tutti i bisogni finanziari del cliente. Ognuna di esse mantiene una propria autonomia sul territorio rispetto agli altri sportelli.

La perdita di redditività delle filiali tradizionali insieme al rapido diffondersi di nuove tecnologie e dei canali bancari diretti (contact center, web e mobile) ha reso necessario un ripensamento del tradizionale modello distributivo "filiale-centrico". Sulla base di queste premesse, gli istituti di credito stanno mettendo in atto negli ultimi anni, processi di riorganizzazione delle reti fisiche, passando dalle tradizionali filiali indipendenti (fullservice) verso modelli distributivi più efficienti come quello "Hub & Spoke", che permette di ridurre i costi operativi e allo stesso tempo di definire un modello di servizio più efficace secondo le logiche dell'omniscanaltà e in grado di generare un più alto valore aggiunto per il cliente. Il modello organizzativo "Hub & Spoke" permette di introdurre un assetto distributivo più efficiente e flessibile, capace di sfruttare appieno i diversi canali (contact center, ATM evoluti, promotori, internet e mobile banking) e le opportunità offerte dall'innovazione tecnologica, pur continuando a valorizzare la rete distributiva fisica, punto di riferimento per il presidio del territorio, la proposizione commerciale e le attività di branding della banca. La FILIALE HUB (filiale capofila) si configura come uno sportello situato in posizione centrale, che offre funzionalità di servizio completo, che coordina una rete di FILIALI SPOKE di più piccole dimensioni, che presentano un'offerta di prodotti/servizi specializzata e un elevato

tasso di automazione. Le filiali Hub hanno una propria autonomia organizzativa e decisionale. Al loro interno la presenza completa dei ruoli tradizionali di filiale (direttore, vice-direttore, cassiere), e di personale con competenze specialistiche (gestore, consulente, promotore finanziario...) anche a disposizione delle filiali Spoke. Le filiali Spoke, pur presentando una propria operatività, riportano alla filiale capofila (Hub) e non hanno la presenza completa dei ruoli tradizionali di filiale ma si avvalgono degli specialisti messi a disposizione dalla filiale capofila. Molteplici sono le configurazioni e le connotazioni che possono assumere le filiali nel modello "Hub & Spoke" (secondo il target di clientela servito, tipologia e numerosità del personale, prodotti e servizi offerti, orari di apertura, layout e suddivisione degli spazi). Le filiali Spoke sono caratterizzate da una maggiore flessibilità rispetto all'Hub, negli orari (apertura estesa) e nei giorni (apertura alternata, apertura in giorni festivi), per essere sempre vicine al cliente e garantire il presidio del territorio. Inoltre, si caratterizzano per un elevato tasso di automazione (ATM evoluti, totem, schermi interattivi) e aree self molto estese. Le filiali Spoke possono differenziarsi ulteriormente in sportelli Cash Light e sportelli Cash Less. Lo sportello Cash Light è caratterizzato da una limitata transazionalità assistita. L'attività di cassa con operatore è generalmente disponibile solo in alcuni orari o per specifiche operazioni. La filiale Cash Less offre massima autonomia operativa al cliente presentando un'area self molto estesa, casse automatiche, ATM evoluti, totem, schermi interattivi e postazioni innovative in grado di fornire consulenza attraverso gestori virtuali/da remoto. Essendo l'operatività di cassa completamente automatizzata, non sono presenti cassieri fissi, sostituiti dalla figura del cassiere polivalente. In aggiunta agli archetipi di filiale fino a qui descritti, emerge anche un quarto modello, la filiale Flagship. Questo sportello è disegnato per il presidio di zone strategiche, come i centri storici e le zone commerciali ad alta frequentazione, con l'obiettivo di fornire agli utenti (non necessariamente clienti) una customer experience esclusiva, creare engagement e generare nuovo business. Queste filiali presentano spazi destrutturati e layout particolarmente innovativi, consentendo di ospitare eventi di vario genere, come concerti e convegni, diventando dei veri e propri laboratori di esperienza e conoscenza per soddisfare sia i bisogni bancari sia quelli extrabancari di clienti e prospect. In termini di personale, la loro composizione è equiparabile a quella di una filiale Cash Less, tuttavia si registra la tendenza ad assumere personale "non bancario" che abbia maturato esperienze commerciali in altri settori (come l'abbigliamento e la telefonia) e in possesso di competenze e capacità relazionali molto forti. La seguente tabella illustra le principali caratteristiche relative ai suddetti modelli distributivi

	<i>Automatica</i>	<i>Light</i>	<i>Specializzata</i>	<i>Full-service</i>	<i>Flagship store</i>
Clientela Servita	<ul style="list-style-type: none"> Clientela fai da te con propensione medio alta alla tecnologia Prevalentemente clientela retail e small business 	<ul style="list-style-type: none"> Clientela che cerca supporto del personale per semplici operazioni Prevalentemente clientela retail e small business 	Particolari segmenti di clientela che necessitano di un'offerta dedicata	<ul style="list-style-type: none"> Clientela desiderosa di una relazione personalizzata Prevalentemente retail e small business 	<ul style="list-style-type: none"> Clienti prospect Clientela sofisticata, affascinata dalla tecnologia
Prodotti servizi	Offerta limitata di principali prodotti retail e small business (es. operazioni transazionali, prodotti maturi)	<ul style="list-style-type: none"> Offerta relativa ai principali prodotti retail e small business Può essere presente all'interno di store 	Offerta focalizzata su prodotti ad elevato valore aggiunto per segmenti di clientela definiti	<ul style="list-style-type: none"> Alta ampiezza di gamma e di servizi offerti Offerta completa per soddisfare tutti i bisogni del Cliente 	<ul style="list-style-type: none"> Alta ampiezza di gamma Prevalentemente servizi di vendita e consulenza dedicata
Modello di relazione	<ul style="list-style-type: none"> Prevalentemente di tipo informativo Filiale operativa 	Relazione di tipo supportiva e informativa	Relazione altamente personalizzata, basata su conoscenza del Cliente profonda (consulenziale)	<ul style="list-style-type: none"> Le operazioni semplici sono eseguite dal Cliente mediante aree self-service Relazione di tipo consulenziale con personale dedicato 	<ul style="list-style-type: none"> Relazione orientata a creare un'esperienza unica per il Cliente Relazione supportiva, informativa e consulenziale
Localizzazione	A presidio di aree con scarsa affluenza in cui il territorio è a bassa redditività o che non giustifica la presenza fisica di personale di rete	Aree urbane sub-urbane e rurali	Aree urbane facilmente accessibili dal Cliente con location strategiche	Aree urbane e sub urbane e rurali con dimensioni variabili in funzione della localizzazione	Aree urbane ad elevata affluenza di pubblico e visibilità (es. principali piazze in grandi città)
Intensità tecnologica/dotazione tecnologica	Intensità elevata (es. chioschi con funzionalità di web-conference) Utilizzo di ATM evoluti per gestione dell'operatività	Intensità varia: combinazione di strumenti tecnologici e ATM evoluti in funzione della localizzazione geografica, stili di consumo dei Clienti	<ul style="list-style-type: none"> Intensità medio bassa Utilizzo di ATM evoluti per gestione dell'operatività 	Intensità varia: combinazione di strumenti tecnologici e ATM evoluti in funzione della localizzazione geografica, stili di consumo dei Clienti	<ul style="list-style-type: none"> Forte intensità tecnologica per favorire customer experience e brand awareness Utilizzo di strumenti tecnologici innovativi
Competenze	Il personale ha solo l'obiettivo di controllare e garantire la corretta operatività (anche da remoto)	Il personale presente ha l'obiettivo di supportare il Cliente nelle operazioni	Il personale presente è specializzato per ambiti di prodotto e di servizio al Cliente	Il personale impiegato è misto, sia specializzato, sia con competenze generiche	Il personale presente è specializzato e focalizzato sulle competenze relazionali

Tabella 1. Identificazione e Classificazione dei modelli di filiale (Fonte: PwC, 2016)

1.3 Il problema della sicurezza delle dipendenze bancarie: le dimensioni del fenomeno

Alla fine del secolo scorso si era diffusa una visione comune sulla prossima fine del settore bancario "brick and mortar". L'ascesa della banca virtuale, che vedeva internet come fondamentale canale per accedere ai servizi bancari faceva dare per scontato il fatto che le filiali fisiche avrebbero avuto un valore residuale sul globale delle operazioni bancarie (Diebold Nixdorf, 2016). Tuttavia, ad oggi queste previsioni non si sono realizzate ed i clienti continuano a preferire le relazioni personali e dirette con il personale bancario per effettuare operazioni economiche e finanziarie (Patel e Brown, 2016) (Höbe, 2015).

Anche se l'introduzione di nuove tecnologie di automazione (ad es. sportelli ATM) e di servizi online (banking online, mobile banking e, più recentemente, smart banking) hanno cambiato le abitudini dei clienti nei confronti dell'utilizzo di servizi standard, un gran numero di consumatori continua ad essere resistente alla perdita del contatto interpersonale nell'effettuazione di operazioni bancarie (Martins et al., 2014; Al-Somali et al., 2009; Flavian et al., 2006). Recenti indagini dimostrano che è ancora attraverso filiali che i clienti svolgono la parte principale della loro attività a valore aggiunto e che le filiali bancarie rappresentano ancora il canale preferito indiscusso per il cliente (Höbe, 2015, Paradi e Zhu, 2013).

Di conseguenza, il numero di dipendenze bancarie in diversi paesi è comunque aumentato. Negli Stati Uniti, il numero delle filiali bancarie è aumentato del 87% nel periodo tra il 1985 ed il 2015 (FDIC, 2017). Trends simili sono osservabili anche in Europa: in Spagna, il numero totale delle filiali tra il 1986 ed il 2010 è aumentato drasticamente da 30.961 a 42.894 (Alamá et al., 2015). In Italia, il numero delle dipendenze bancarie è cresciuto da 24.421 del 1996 a 32.881 nel 2012, mostrando un elevato livello di prossimità del sistema bancario rispetto ai clienti finali (56 filiali ogni 100 mila abitanti (KPMG, 2013)

Il canale ATM, insieme a quello delle dipendenze bancarie, continua dunque a mantenere un ruolo centrale nella relazione con il consumatore, diventando parte integrante dell'esperienza multicanale della banca. La penetrazione degli sportelli ATM è cresciuta su scala globale, raggiungendo un volume di 44 sportelli ATM ogni 100 mila abitanti nel 2014, con incremento del 52% rispetto al 2010 (29 ATM ogni 100 mila abitanti) (Accenture; 2016).

In (Paradi and Zhu, 2013) è stato rilevato che il 61% dei clienti visita la filiale bancaria in media una volta al mese, il 52% dei clienti effettua transazioni attraverso gli sportelli bancari o i canali ATM ed 1/3 di essi utilizza i canali on-line.

La presenza locale e la vicinanza ai clienti continuano ad essere una risorsa strategica per i gruppi bancari. Le ragioni per cui i gruppi bancari continuano a investire nella creazione di punti di contatto fisici con i propri clienti, nonostante i loro elevati costi operativi, sono ricercabili sulla necessità dei consumatori per l'affidabilità, la garanzia dei contatti personali, i servizi personalizzati, soprattutto dopo il periodo di crisi economica iniziato nel 2008 (Walsh et al., 2010). Dopo aver tentato di spingere i clienti all'utilizzo di Internet e contact center per controllare le spese, le banche stanno dando una seconda opportunità alle proprie reti di filiali, investendo pesantemente su di esse (Brunier et al., 2016).

Inoltre, nonostante la costante crescita del numero di transazioni economiche in formato elettronico, il denaro contante è ancora ampiamente utilizzato. Secondo il report G4S (2016) il volume di contanti in circolazione su scala mondiale è aumentato dell'11% annuo fino al 2015, con il denaro contante che costituisce il 60% di tutte le transazioni di pagamento. I prelievi presso gli sportelli ATM sono aumentati del 14,6% tra il 2009 e il 2014, con un incremento di 2.188 miliardi di euro; la quota di persone che ritirano almeno una volta al mese da sportelli bancomat supera il 70% in tutti i paesi (Bagnall et al., 2014). Secondo il data warehouse reso disponibile dalla Banca Centrale Europea (<http://sdw.ecb.europa.eu>), il valore dei prelievi di contanti è stato di 1.523,95 € miliardi nel 2015.

Il crescente numero di dipendenze bancarie e sportelli ATM, unitamente all'utilizzo estensivo di denaro contante, rappresentano le ragioni principali per le quali in differenti paesi gli attacchi criminali nei confronti delle banche stanno crescendo. Secondo il Federal Bureau of Investigation degli Stati Uniti, i reati contro le banche (ad es. rapine, furti, attacchi ATM) rappresentano un problema che continua a gravare sulle istituzioni finanziarie in giro per il mondo. Nel 2015 sono state rilevate 4030 rapine, con un incremento del 3,8% (3879 nel 2014) rispetto all'anno precedente (FBI, 2016). In Europa, un'analisi dettagliata sulle statistiche relative ai reati nei confronti delle banche è effettuato dall'European Banking Foundation (EBF, 2016) mettendo in evidenza alcune tendenze generali. Nonostante il trend nel numero delle rapine in banca nel 2015, le perdite totali continuano a crescere (27.608.147 € rispetto ai 24.002.526 € del 2014, con un incremento del 15%). Gli attacchi all'ATM sono incrementati da 2.657 del 2015 a 2.974 nel 2016 (+12%). La perdita media degli attacchi agli ATM arriva a 15,905 \$, per un attacco esplosivo a 18.589 \$ e per una rapina è di 21.676 \$.

Questi valori non tengono conto dei danni collaterali a attrezzature o edifici, che possono essere significativi e spesso superano il valore dei soldi persi in un attacco riuscito. Molti degli attacchi fisici agli ATM vengono perpetrati tramite esplosivi oppure legando l'ATM ad una catena, trainandola con un camion o un altro veicolo di grandi dimensioni. (Geetha et al., 2016). I danni collaterali provenienti da questi tipi di attacchi sono facili da immaginare.

Il numero di furti bancari commessi in Europa è diverso da un paese all'altro (da zero in diversi paesi a più di 772 in Italia, che da sola rappresenta il 60% degli attacchi totali sul territorio europeo. In alcuni paesi, il numero di attacchi con esito positivo rimane particolarmente elevato (69% degli incidenti totali). Gli attacchi hanno generalmente più successo in Portogallo (83%), Slovacchia (82%) Spagna (80%) e Grecia (79%). I dati evidenziano inoltre che il 58% del valore deriva da furti effettuati in Italia.

Gli attacchi bancari rappresentano una sfida ancora aperta, che ha un impatto non solo economico (in termini di perdite, costi aggiuntivi di sicurezza e consumo di risorse) ma implica anche i costi sociali (Dolan e Peasgood, 2007). Inoltre, gli attacchi possono portare a gravi danni fisici e psicologici a personale e dipendenti di front-end. Oltre alle ovvie implicazioni per la sicurezza delle persone, questi attacchi hanno gravi conseguenze economiche per le istituzioni bancarie: ad esempio, in Bunn e Guthrie (2009) viene segnalato un caso di attacco ATM (ammontare rubato 200k \$) dove un dipendente è stato trattenuto dagli autori del reato con la minaccia di ucciderla se

avesse dato loro l'accesso al contante contenuto nell'ATM. La dipendente ha sofferto di lesioni psicologiche e ha richiesto circa tre settimane di astensione dal lavoro, formulando una richiesta di risarcimento danni. La banca è stata condannata a risarcire un importo di 162.500 dollari al proprio dipendente.

Dopo un evento criminoso, oltre a danni collaterali rilevanti ad attrezzature ed edifici, le banche subiscono ulteriori perdite indirette a seguito di un peggioramento della reputazione e dell'immagine e della perdita di fiducia per conto dei propri clienti e degli stakeholders (Penz e Sinkovics, 2013)

Inoltre, dopo un delitto, le banche subiscono altre perdite dirette a causa di danni collaterali rilevanti a attrezzature ed edifici (EAST, 2017) e perdite indirette a seguito di un peggioramento della reputazione e dell'immagine e perdita di fiducia per conto dei propri clienti e delle controparti (Penz e Sinkovics, 2013). In questo senso, vale la pena sottolineare che nel caso della banca commerciale, un numero rilevante di reati non viene segnalato a causa della paura del danno del marchio, della perdita di attività e della pubblicità negativa (Kabay, 2014).

CAPITOLO 2. Opportunità per il miglioramento nei processi di gestione della sicurezza nelle dipendenze bancarie

2.1 La gestione dei processi aziendali

Gli ultimi anni sono stati caratterizzati dall'accelerazione del processo di globalizzazione che ha fortemente contribuito a ridurre la rilevanza del fattore spaziale accentuando allo stremo quello temporale. In tale contesto, risulta essere sempre più evidente ed elevato il grado di competitività al quale sono soggetti i sistemi organizzativi, allo scopo di garantire la propria sopravvivenza.

In aggiunta a tutto ciò, l'emergere di tecnologie sempre più innovative, pone l'accento sull'importanza strategica di fattori quali tecnologie e conoscenza ai fini della determinazione del vantaggio competitivo delle aziende. L'ambiente competitivo degli anni recenti è stato infatti caratterizzato da un certo grado di turbolenza, dovuta ad una serie variegata ed interdipendente di fattori, tra i quali la tecnologia. In poche parole l'emergenza di cambiamenti tecnologici repentini rappresenta sempre più evidentemente la principale causa di instabilità. A fronte di una tale configurazione ambientale, la formulazione di scelte precise ai fini di un'efficiente gestione della risorsa tecnologica e della capacità di anticipare il mercato sembrano affermarsi come imperativo per il successo aziendale.

Proprio allo scopo di preservare il vantaggio competitivo del quale si parlava in precedenza, le organizzazioni devono essere progettate in maniera opportuna al fine di garantire il giusto grado di coerenza tra le variabili organizzative che entrano in gioco.

Le mutevoli condizioni del mercato e il conseguente aumento della concorrenza sono solo alcuni dei motivi alla base della crescente attenzione delle imprese alle modalità organizzative che meglio agevolano le strategie d'impresa.

A fronte di una scelta strategica di crescita dimensionale piuttosto diffusa all'interno del settore, ciò che sembra comunque essere differenziante è la capacità di predisporre le condizioni affinché i sistemi, i processi e i meccanismi organizzativi cambino e trovino una configurazione stabile nel minor tempo possibile.

Definire la struttura aziendale secondo una visione per processi può rivelarsi, in tal senso, un intervento strategico rilevante e opportuno; l'organizzazione per processi, infatti, è in grado di fornire adeguato supporto alle necessità strategiche dell'impresa, in termini di capacità di formalizzazione delle attività aziendali, possibilità di definizione di indici di misurazione delle performance di processo e la conseguente facilità di misurazione e controllo delle stesse.

Le attività di trasformazione dei processi non possono però prescindere da considerazioni legate alle caratteristiche intrinseche di variabilità, che inducono le risorse a operare in modo diverso a seconda delle eccezioni, e al concetto di standardizzazione del processo, con l'obiettivo di recuperare efficienza nello svolgimento delle attività, producendo l'output in tempi ridotti e con minore impiego di input.

La struttura per processi si configura infatti come trasversale alle funzioni aziendali e l'attenzione rispetto all'oggetto dell'organizzazione si focalizza sull'intero processo di creazione del valore

aziendale, dall'input delle risorse all'output di prodotto, consentendo di legare l'operatività dell'azienda alla visione strategica degli obiettivi aziendali. La visione funzionale dell'organizzazione aziendale, al contrario, pone l'accento sulle relazioni di tipo gerarchico che caratterizzano l'azienda, e non consente di avere una visione univoca delle attività che consentono l'erogazione del prodotto o servizio. Sebbene quanto detto sia condiviso in modo pressoché unanime dal sistema bancario, è doveroso precisare che, all'atto pratico, la variabilità dei processi e la loro intrinseca complessità generano una difficoltà oggettiva nel determinare e formalizzare gli step operativi, commerciali e di controllo nei quali si articolano gli stessi e ottenerne una mappa precisa e puntuale.

Un processo può essere definito come *“un insieme organizzato di attività e di decisioni, finalizzato alla creazione di un output effettivamente domandato dal cliente, e al quale questi attribuisce un valore ben definito”* (Davenport e Stoddard, 1994)

In Trkman (2010) l'approccio alla gestione dei processi di business (Business Process Management) viene definito come l'insieme degli sforzi di un'organizzazione per analizzare e migliorare continuamente attività fondamentali quali la produzione, il marketing, le comunicazioni ed altri elementi principali delle attività aziendali. Un processo aziendale è un insieme completo di attività dinamiche coordinate o compiti logicamente correlati che devono essere eseguiti per fornire valore ai clienti o per adempiere ad altri obiettivi strategici (Guha & Kettinger, 1993; Strnadl, 2006).

Il BPM riguarda in maniera sistemica tutto l'ecosistema aziendale, coinvolgendo la supply chain a monte (partners e suppliers) e a valle (clienti). Richiede inoltre un elevato coinvolgimento interno da parte dei dipendenti dell'organizzazione (impiegati, managers e specialisti in ambito IT). I sistemi informativi giocano un ruolo cruciale nel mantenere forte questo legame. L'integrazione tra sistemi informativi interni ed esterni consente lo svolgimento ed il continuo monitoraggio dei processi end-to-end anche al di fuori dei confini organizzativi, con un sensibile impatto sulle performances dell'intera organizzazione.

Secondo l'Association of Business Process Management Professionals il “Business Process Management (BPM) è un approccio disciplinato per identificare, progettare, eseguire, documentare, misurare, monitorare e controllare processi aziendali automatizzati e non automatizzati per ottenere risultati coerenti e mirati, in linea con gli obiettivi strategici di un'organizzazione”. Van der Aalst (2004) definisce invece il BPM come *l'insieme di metodi, tecniche e software che consentono di individuare, disegnare, eseguire, controllare, monitorare e analizzare i processi di business, grazie alla combinazione coordinata di persone, unità organizzative, applicazioni, documenti e altre fonti informative.*

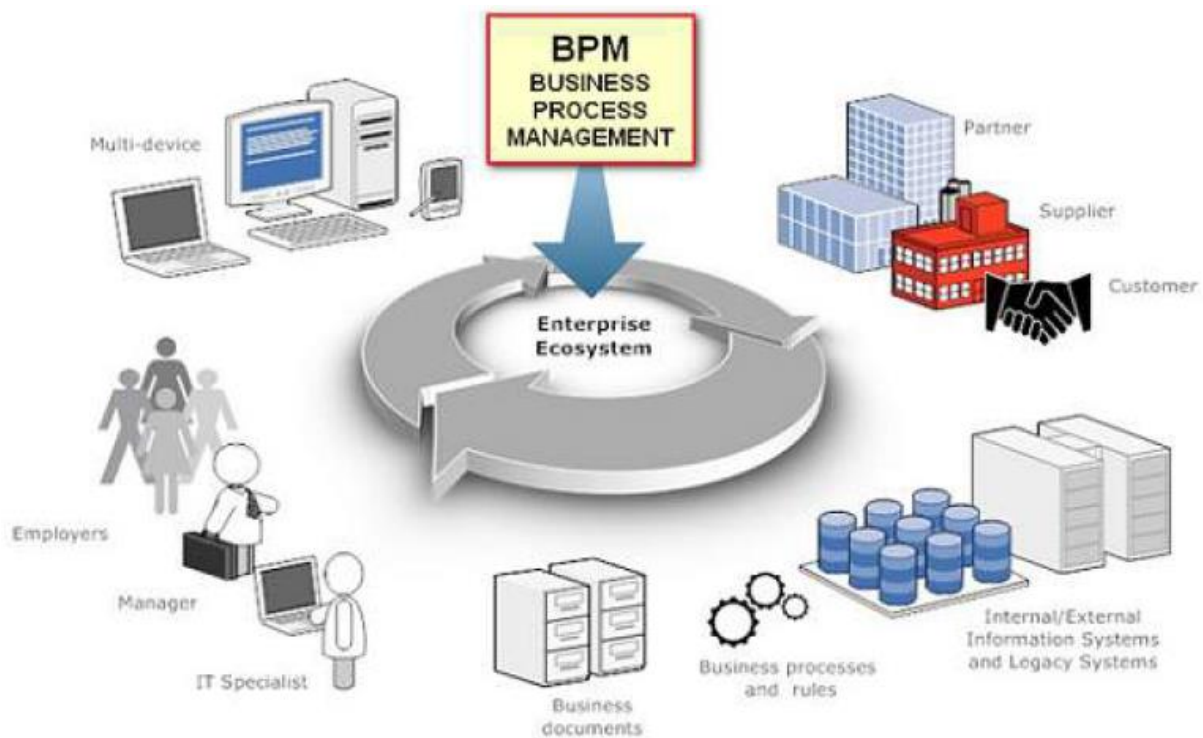


Figura 9. La prospettiva sistemica del Business Process Management

2.1.1. Approcci al Business Process Management: Reingegnerizzazione vs. miglioramento incrementale. Metodologie il miglioramento dei processi aziendali

Il BPM coinvolge la definizione, il miglioramento, l'innovazione e la gestione dei processi aziendali end-to-end deliberati, collaborativi e sempre più tecnologicamente assistiti. Tali processi guidano i risultati di business, creando valore e consentendo di raggiungere i propri obiettivi di business con più agilità. IL BPM permette alle imprese di allineare i propri processi di business con la propria strategia, portando ad un'efficienza delle prestazioni complessive dell'azienda attraverso il miglioramento di attività lavorative sia all'interno di un reparto specifico, che in tutta l'azienda, o tra le organizzazioni."

Smith e Fingar (2003) vedono il BPM come una via intermedia fra la gestione d'impresa e l'information technology. Secondo i due autori il Business Process Management è riferito a processi operativi, che interessano variabili quantitative e sono ripetuti su grandi volumi quotidianamente.

In realtà il BPM non riguarda soltanto le fasi di scoperta, disegno e sviluppo dei processi di business, ma anche i controlli di supervisione, amministrativi e direzionali che verificano e assicurano la conformità rispetto agli obiettivi di business. A differenza quindi di quanto previsto dal BPR, l'obiettivo non consiste nella ricerca di un miglioramento radicale dei processi che si completa in tempi predefiniti ma, piuttosto, in un'evoluzione incrementale, guidata da un continuo sforzo di comprensione e di interpretazione dei processi, che interagiscono con persone e sistemi entro e fuori dai confini organizzativi dell'azienda.

Il BPM rappresenta dunque una strategia finalizzata al miglioramento dei processi di business. Esistono due approcci diversi per la gestione dei processi:

- Business Process Reengineering (BPR)
- Business Process Improvement (BPI)

Il concetto di BPR nasce come una radicale riprogettazione dei principali processi di una organizzazione tesa al raggiungimento di fortissimi miglioramenti nei risultati

Esposto per la prima volta da Hammer all'inizio degli anni '90 (Hammer, 1990), è stato successivamente ripreso da altri esperti, come Davenport ed Harrington (1995), che hanno mitigato questi concetti generando ipotesi e approcci che si differenziano principalmente per la profondità del cambiamento, per l'ampiezza dell'intervento e per il diverso peso degli obiettivi di efficacia o efficienza. La caratteristica di radicalità del BPR nel puntare ad obiettivi di forte discontinuità nei livelli di prestazione, non consente di limitare l'attenzione ai soli flussi operativi, ma obbliga ad una profonda analisi in cui si mettano in discussione gli aspetti organizzativi, le responsabilità, le strutture, le competenze, i sistemi tecnologici ed informatici. Di conseguenza il BPR rappresenta un approccio complesso e pieno di rischi, che richiede forte leadership, attenzione ai problemi di gestione del cambiamento e una visione di medio e lungo periodo.

Reingegnerizzare i processi di business significa abbandonare i processi esistenti e ricominciare. In Hammer e Champy (1993), la riprogettazione dei processi aziendali è definita come "il ripensamento fondamentale e la riprogettazione radicale dei processi per ottenere miglioramenti drammatici (sensibili, notevoli) nelle misure critiche di prestazioni contemporanee come i costi, la qualità e la velocità". Questa definizione contiene quattro parole chiavi: -

- **Fondamentale.** Rivalutare gli obiettivi primari della società, ignorando le regole e le ipotesi formulate in passato.
- **Radicale.** Non cercare di migliorare la situazione esistente, ma inventare nuovi modi di realizzare il lavoro.
- **Drammatico.** Non utilizzare la riprogettazione dei processi aziendali per ottenere miglioramenti marginali, ma mirare a miglioramenti di "su larga scala".
- **Processo.** Focus sui processi aziendali invece delle strutture organizzative. Quindi, in poche parole, il BPR è un approccio ambizioso e regolare che si concentra sui processi aziendali invece che sui confini organizzativi.

Le definizioni di riprogettazione e reingegnerizzazione dei processi aziendali sembrano concentrarsi su aspetti operativi, mentre in alcuni casi prendono in considerazione i punti di vista organizzativi. In modo evidente, diversi termini vengono utilizzati in modo intercambiabile con focus leggermente diverso dagli obiettivi. Tuttavia, in sostanza, si occupano dello stesso fenomeno; radicale ripensamento di processi importanti e cruciali per ottenere miglioramenti drammatici in diverse operazioni misurabili.

Short e Venkatraman(1992) affermano che il BPR si concentra quasi esclusivamente sul miglioramento delle operazioni interne dell'impresa, vale a dire in una prospettiva operativa. Anche se l'efficienza interna è importante, sostengono che la riprogettazione della rete commerciale, vale a dire riconcettualizzare il ruolo dell'impresa e i suoi processi aziendali chiave

nella grande rete aziendale, è di maggiore importanza strategica. Infatti, l'obiettivo del BPR è generalmente l'ottimizzazione di un singolo processo piuttosto che la trasformazione dell'impresa stessa (Davidson, 1993)

Il Business Process Improvement si caratterizza invece attraverso il concetto di gradualità al cambiamento, il quale presume che si parta dai processi attuali per apportare miglioramenti di valore, individuandone punti di debolezza ed applicando i debiti interventi correttivi. L'applicazione del BPI prevede, infatti, una prima fase di valutazione del processo attuale («as is»), con la quale si cerca di comprendere se il processo in analisi sia adeguato alle esigenze del cliente e rispetto alle performance conseguite dalla concorrenza. Qualora il processo vada migliorato, inizia la seconda fase, quella cioè in cui viene impostato un lavoro di miglioramento. Il BPI viene spesso attuato in una situazione caratterizzata dall'assenza di emergenze particolari e, nella maggior parte dei casi, esso è indipendente dal cambiamento strategico. Proprio per questa ragione la gestione incrementale dei processi è atta al conseguimento anche di piccole opportunità di miglioramento, pur potendone conseguire anche di notevoli. I processi coinvolti in un progetto di BPI sono spesso di ampiezza contenuta ed in numero elevato, proprio grazie alla gradualità nel cambiamento sui medesimi; spesso accade che strada facendo vengano individuate nuove opportunità ed aree di miglioramento. È importante, per il buon esito di una gestione BPI, che vi sia un forte contributo degli operatori di processo (bottom-up), proprio perché fondamentali per individuare le aree critiche di miglioramento. In generale, tutta l'organizzazione deve essere disponibile al cambiamento graduale ed in effetti difficilmente si verificano situazioni di astio e resistenza.

Grazie all'adozione del BPI è possibile ridurre costi e tempi nel life cycle aziendale, migliorandone la qualità. Questa metodologia è stata descritta per la prima volta da Harrington (1991). Harrington utilizza il termine "Redesign" per sottolineare l'orientamento a soddisfare l'esigenza delle organizzazioni a procedere verso cambiamenti più contenuti e meno rischiosi, semplificando i processi e utilizzando tecniche IT per svolgere le attività di routine e ripetitive. In sintesi i benefici del processo di Redesign sono:

- Documentare e quantificare il processo in corso.
- Preparare un modello di simulazione dei processi statali attuali e futuri.
- Ridurre il tempo di costi e di durata del ciclo
- Migliorare la qualità.
- Aumentare la soddisfazione dei clienti.
- Ridurre il conflitto interno.

Le principali caratteristiche dei due approcci possono essere riassunti come segue:

Business Process Reengineering	Business Process Improvement
Riprogettazione del processo	Semplificazione del processo
Trasformazione radicale	Cambiamento graduale
Trasformazione guidata da una "visione"	Trasformazione guidata dal processo
Introduzione di nuove tecnologie	Migliora l'applicazione della tecnologica
Modifica atteggiamenti e comportamenti	Accetta atteggiamenti e comportamenti

Guidata dalla direzione	Guidata dai manager
Numero limitato di iniziative aziendali	Riguarda contemporaneamente più processi

Tabella 2. Principali differenze tra BPR e BPI (Costantini e Cassaro, 2001)

Il BPI si tratta dunque di un approccio caratterizzato dalla gradualità al cambiamento, la quale presume che si parta dai processi attuali per apportare miglioramenti di valore, individuandone punti di debolezza ed applicando i debiti interventi correttivi. L'applicazione del BPI prevede, infatti, una prima fase di valutazione del processo attuale («as is»), con la quale si cerca di comprendere se il processo in analisi sia adeguato alle esigenze del cliente e rispetto alle performance conseguite dalla concorrenza. Qualora il processo vada migliorato, inizia la seconda fase, quella cioè in cui viene impostato un lavoro di miglioramento. Il BPI viene spesso attuato in una situazione caratterizzata dall'assenza di emergenze particolari e, nella maggior parte dei casi, esso è indipendente dal cambiamento strategico. Proprio per questa ragione la gestione incrementale dei processi è atta al conseguimento anche di piccole opportunità di miglioramento, pur potendone conseguire anche di notevoli. I processi coinvolti in un progetto di BPI sono spesso di ampiezza contenuta ed in numero elevato, proprio grazie alla gradualità nel cambiamento sui medesimi; spesso accade che strada facendo vengano individuate nuove opportunità ed aree di miglioramento. È importante, per il buon esito di una gestione BPI, che vi sia un forte contributo degli operatori di processo (bottom-up), proprio perché fondamentali per individuare le aree critiche di miglioramento. Nell'ambito delle metodologie per il miglioramento dei processi aziendali, un paradigma ampiamente utilizzato è quello del cosiddetto "Ciclo di Deming" (conosciuto anche come ciclo PDCA – Plan, Do, Check, Act).

Il modello PDCA trae origine dai tradizionali modelli di sviluppo nell'ambito della produzione manifatturiera. Nello specifico il Ciclo di Deming rappresenta una evoluzione dello "Shewhart Cycle".

Shewhart era partito da una rappresentazione lineare costituita da 3 passi: specification, production, e inspection. Col tempo egli si rese conto che la vecchia versione (quella lineare) dovesse seguire un cerchio anziché una linea retta. Secondo Shewhart era utile pensare ai 3 passaggi del processo di produzione di massa come passi del metodo scientifico. In questo senso, dunque, secondo lui la specificazione, la produzione e l'ispezione avrebbero dovuto corrispondere rispettivamente a fare un'ipotesi, eseguire un esperimento e testare l'ipotesi. Le tre fasi costituiscono un processo dinamico scientifico di acquisizione di conoscenze.

Deming (1950) ha modificato il ciclo Shewhart con l'introduzione di un ulteriore passo ovvero - Riprogettare attraverso la ricerca di marketing. Deming ha sottolineato l'importanza di un'interazione costante tra la progettazione, la produzione, la vendita e la ricerca, avendo come obiettivi la qualità del prodotto e la qualità del servizio.

Il ciclo Shewhart di Deming è stato poi modificato leggermente nel 1951 ed è mostrato in Figura 9. Il ciclo prese dunque il nome di "ruota di Deming".

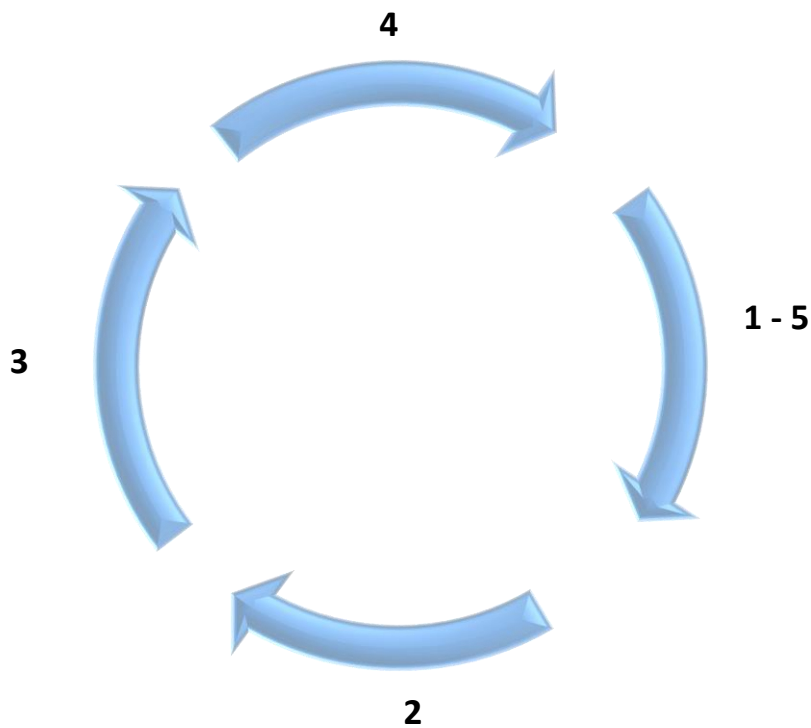


Figura 10. Approccio ciclico nella gestione dei processi di produzione

Le fasi erano:

1. Progettare il prodotto (con i test appropriati).
2. Realizzarlo; provarlo nella linea di produzione e nel laboratorio.
3. Metterlo sul mercato.
4. Testare in servizio, attraverso la ricerca di mercato, scoprire cosa l'utente pensa di esso e perché il un utente non lo abbia acquistato.
5. Riprogettare il prodotto, alla luce delle reazioni dei consumatori alla qualità e al prezzo.
Ripetere il ciclo

Successivamente alcuni dirigenti giapponesi hanno riformulato la ruota di Deming nel ciclo PDCA

Fase	Descrizione
1. Progettazione – Plan	La progettazione del prodotto corrisponde alla fase di gestione
2. Produzione – Do	La produzione corrisponde alla realizzazione del prodotto che è stato progettato
3. Vendita – Check	Le cifre di vendita confermano se il cliente è soddisfatto
4. Ricerca – Act	In caso di presentazione di una denuncia, deve essere inserita nella fase di pianificazione e le azioni devono essere intraprese nel prossimo ciclo di attività

Tabella 3. Le 4 fasi del ciclo PDCA

Il ciclo di PDCA risultante è mostrato in Figura 9. Il ciclo di risoluzione dei problemi a quattro fasi comprende la pianificazione (definizione di un problema e un'ipotesi sulle possibili cause e soluzioni), il fare (implementazione), il controllo (valutazione dei risultati) e l'azione (ritornare alla pianificazione se i risultati sono insoddisfacenti o standardizzare se i risultati sono soddisfacenti). Il ciclo PDCA evidenzia la prevenzione degli errori ripetuti stabilendo norme e la continua modifica di tali norme. Anche prima che si utilizzi il ciclo PDCA, è essenziale stabilizzare gli standard attuali. Il processo di stabilizzazione è spesso chiamato ciclo SDCA (standardize-do-check-action). Ishikawa (1985) ha affermato: "Se le norme e le regolamentazioni non vengono rivedute in sei mesi, è la prova che nessuno li sta usando seriamente".



Figura 11. Ruota PDCA

Ishikawa ridefinisce il ciclo PDCA per includere obiettivi, segmento target e metodi per raggiungere gli obiettivi della fase di pianificazione. Nello step DO, include la formazione e l'istruzione necessarie per la realizzazione del prodotto. Inoltre afferma che un buon controllo significa permettere che gli standard siano costantemente riveduti per riflettere le voci dei consumatori e le loro lamentele come requisiti del prossimo processo.

Nel 1993 Deming modifica nuovamente il ciclo Shewhart definendolo ciclo Shewhart per l'apprendimento e il miglioramento - il ciclo PDSA (figura 10) Lo descrive come un diagramma di flusso per l'apprendimento e per il miglioramento di un prodotto o di un processo.

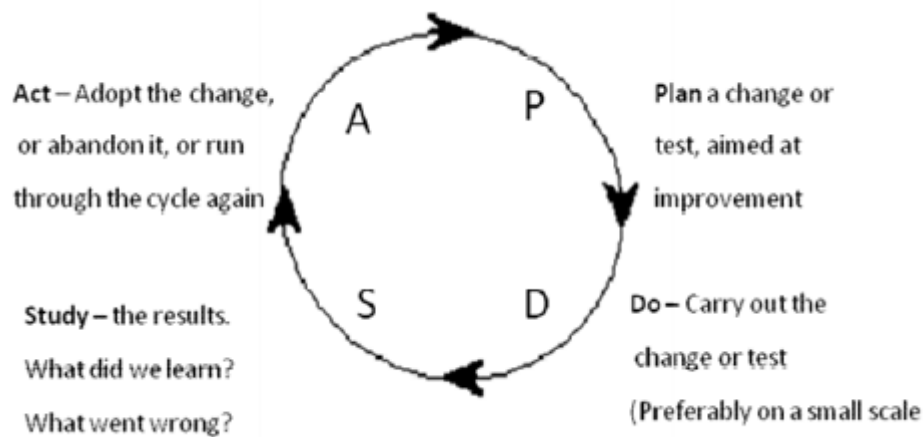


Figura 12. Ciclo PDSA

Secondo Langley et al. (1994) l'uso della parola "studio" sottolinea che lo scopo di questa fase è quello di costruire nuove conoscenze. Non è sufficiente determinare che un cambiamento ha portato ad un miglioramento durante un determinato test. Quando si sviluppano nuove conoscenze, si deve essere in grado di prevedere se una modifica provocherà un miglioramento alle diverse condizioni che si potrebbero affrontare in futuro. Inoltre, hanno aggiunto tre domande fondamentali per completare il ciclo PDSA:

1. Che cosa stiamo cercando di realizzare?
2. Come sapremo che un cambiamento è un miglioramento?
3. Quali cambiamenti possiamo fare per ottenere un miglioramento

Langley et al.(2009) hanno combinato le tre domande e il ciclo PDSA per formare la base del modello API per il miglioramento (vedi Figura 11). Le tre domande definiscono l'obiettivo, le misure e le possibili modifiche. Il modello può essere applicato al miglioramento di processi, prodotti e servizi in qualsiasi organizzazione, nonché a migliorare gli aspetti dei propri sforzi personali. Il modello tenta di bilanciare il desiderio e le ricompense delle azioni intraprese col buon senso di uno studio attento prima di intraprendere le azioni.

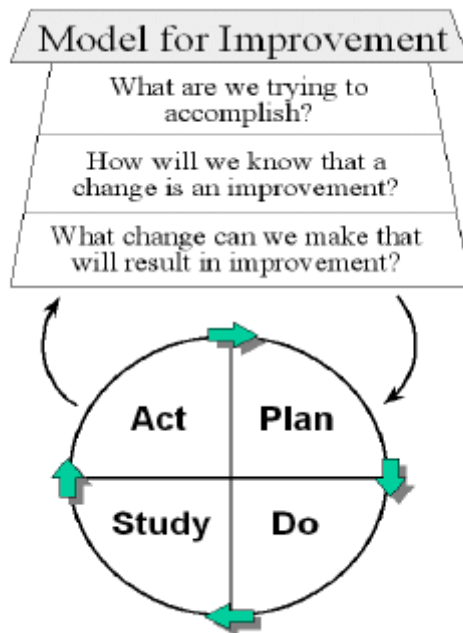


Figura 13. Model for Improvement

METODOLOGIA

Come già affermato in precedenza gli interventi di miglioramento incrementale, noti come Business Process Improvement BPI, partendo da un'analisi dettagliata dei processi esistenti, nota come mappatura dei processi as-is, puntano ad adattarli e migliorarli in maniera incrementale rispondendo alle richieste di clienti interni ed esterni senza stravolgere la struttura esistente.

Attraverso un'attenta analisi della situazione attuale si cerca, infatti, di individuare lacune e difetti per poterli risolvere con opportune nuove soluzioni. "Si tratta di sottoporre il processo ad una serie di verifiche per operare i cambiamenti necessari a garantire migliori performance, a restare al passo con i concorrenti e a sfruttare le offerte da eventuali nuove tecnologie" (Pierantozzi, 1998). Il paradigma da seguire con questi interventi di miglioramento, ma anche con la prima implementazione di un sistema BPM, è "Think Big, Start Small": nel senso che "è importante avere una visione complessiva del problema, la cosiddetta Big Picture, ma passare all'implementazione con gradualità, scegliendosi magari un progetto prototipale, generando consenso nell'organizzazione, affinando le metodologie e creando un Centro di Eccellenza interno, con persone con le competenze adeguate" (Sinibaldi, 2009)

Gli interventi di miglioramento radicale, noti come Business Process Reengineering, BPR, partono invece dal presupposto che non vi sia nulla di positivo nella situazione attuale ai fini della creazione di valore. Pertanto semplici provvedimenti di natura incrementale, volti alla correzione di alcuni elementi nei processi, non risultano essere sufficienti a garantire un cambiamento in termini migliorativi della situazione attuale, ma si rende necessario un intervento di natura radicale che porti al ridisegno completo dei processi, un radicale intervento di ristrutturazione

organizzativa facendo leva sulle potenzialità di coordinamento e controllo offerte dalle nuove tecnologie.

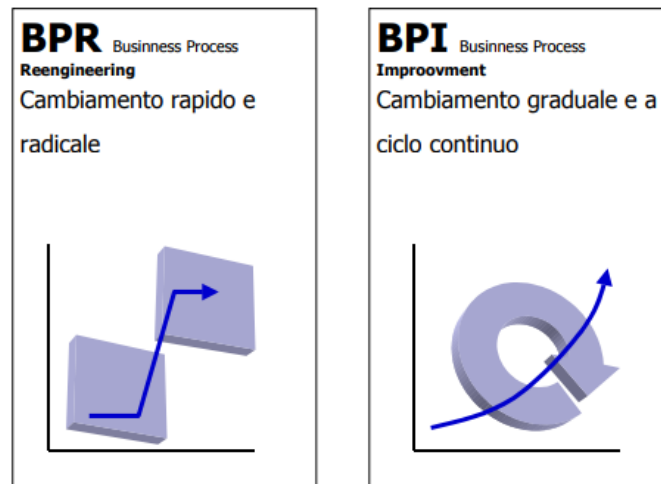


Figura 14. BPR vs. BPI

Dopo aver mappato i processi, definito i *process owners* ed identificato la necessità di una riprogettazione dei processi stessi attraverso il confronto tra gli standard definiti in fase di progettazione e le reali misure di performance del processo in atto, sarà necessario definire da dove partire con gli interventi di miglioramento, identificando quali processi sono i responsabili dell'insuccesso, quali sono critici per la creazione del valori e quali prioritari per le azioni di miglioramento

Sono definiti critici quei processi, sia primari sia di supporto, che devono essere gestiti con particolare attenzione secondo criteri definiti dall'azienda. Criteri utili per l'individuazione delle criticità possono essere collegati alla sicurezza, all'ambiente, ai clienti, alla qualità, ai costi e al clima interno (Cepas, 2006).

Sono definiti prioritari quei processi su cui è necessario intervenire prima rispetto ad altri processi. La definizione della priorità avviene solitamente tramite l'analisi delle priorità, definite a loro volta dalla singola realtà aziendale (Cepas, 2006).

Valiris e Glykas (1999) affermano che nella letteratura scientifica, viene proposta un'ampia gamma di metodologie di BPR. Secondo gli autori, queste metodologie possono essere raggruppate in due categorie principali, a seconda della prospettiva che prendono in considerazione: gestione contabile o sviluppo di sistemi informativi. Secondo la prospettiva della gestione contabile, gli analisti tentano di riorganizzare i processi aziendali, utilizzando l'Information Technology come un fattore abilitante per l'automazione dei processi. Nella prospettiva di sviluppo dei Sistemi Informativi, gli sviluppatori devono comprendere e eventualmente riorganizzare i processi aziendali in modo che l'introduzione di opportune tecnologie possa apportare un miglioramento nei processi di business.

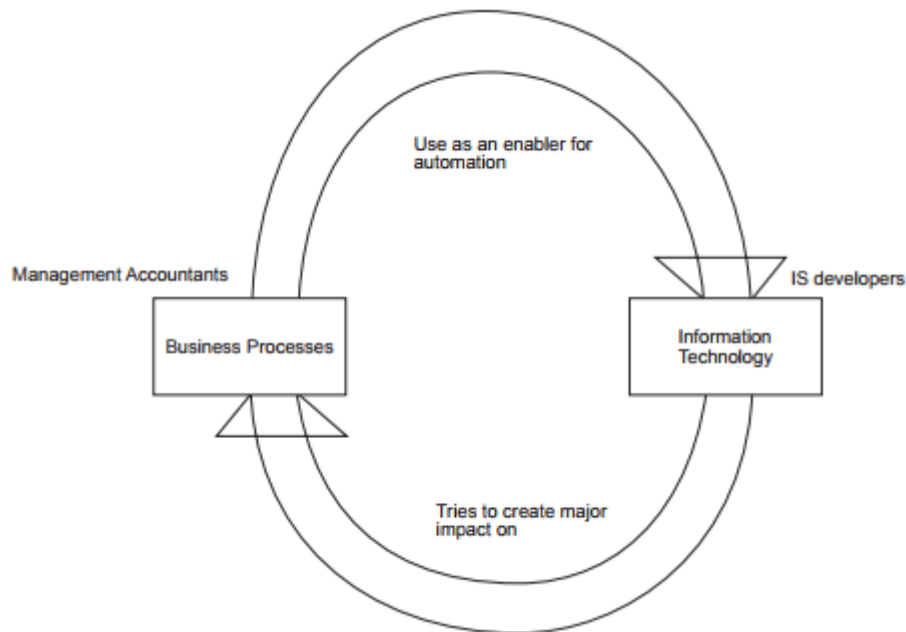


Figura 15. I due differenti approcci al BPR (Valiris and Glykas, 1999)

Indipendentemente dall'approccio adottato, gli step individuabili in un processo di reingegnerizzazione sono di seguito identificabili:

- (1) Identificazione della Vision e degli obiettivi aziendali.
- (2) Identificazione dei principali processi aziendali che li supportano.
- (3) Modellazione e analisi dell'ambiente di business.
- (4) Raffinamento.
- (5) Controllo continuo e miglioramento dei passaggi precedenti.

Il ripensamento dei processi di business trova le sue radici nell'industria manifatturiera (Davenport e Short, 1990). In ambito manifatturiero l'accento è di solito posto sulla descrizione del flusso di materiale attraverso i processi produttivi. In questo contesto la gestione dei processi è orientata a ridurre al minimo il ciclo di processo e i costi, massimizzando la qualità del prodotto finale (Hand, 1991). Gli approcci metodologici al BPR secondo una prospettiva economico/contabile mirano ad identificare i seguenti parametri per l'analisi dei processi:

1. Flusso: il metodo per trasformare gli input in output.
2. Efficacia: come le aspettative del cliente vengono rispettate.
3. Efficienza: come vengono usate le risorse al fine di produrre un output.
4. Tempo di ciclo. Il tempo necessario per la trasformazione degli input nell'output finale.
5. Economia. Le spese associate all'intero processo.

Attaran (2004) enfatizza il ruolo dell'Information Technology nella ri-progettazione dei processi aziendali, identificando tre differenti ruoli dell'IT, a seconda della fase che va a supportare: prima della progettazione, durante la progettazione, durante l'implementazione.

Fase 1: prima della progettazione del processo.

In questa fase l'IT funge da "abilitatore". Il BPR è un'azione strategica e richiede una chiara comprensione dei clienti, del mercato, dell'industria e del contesto competitivo. Inoltre, come qualsiasi altra azione strategica, richiede coerenza tra la strategia aziendale e la visione aziendale. In questa fase, l'IT offre l'opportunità di utilizzare una tecnologia più recente e migliore per sviluppare una nuova visione strategica e contribuire a migliorare il processo aziendale prima che sia stato progettato.

Fase 2: durante la progettazione del processo.

Questa fase prevede essenzialmente due attività: la progettazione "tecnica" (ripensamento dei processi) e la progettazione "sociale" (ripensamento dei ruoli, definizione delle competenze, identificazione delle esigenze del personale, progettazione degli incentivi). In questa fase l'IT assolve il ruolo di "facilitatore" del processo di reingegnerizzazione. Si pensi all'utilizzo di tools di project management, oppure tecnologie per la modellazione, rappresentazione e misurazione dei processi.

Fase 3: dopo la progettazione del processo.

In questa fase l'IT svolge un ruolo di "implementazione" in quanto consente di costruire il commitment, fornisce strumenti di supporto alla valutazione degli impatti e consente di ottimizzare i processi di comunicazione ed i flussi di informazione nello svolgimento dei processi.

Before the Process Design	During the Process Design	During the Implementation
<ul style="list-style-type: none"> • Create infrastructures and manage information that support evolving organization • Foster process thinking in organizations • Identify and select process for redesign • Participate in predicting the nature of change and anticipate the information needs to support that change • Educate IT staff in non-technical issues such as marketing, customer relationships, etc. • Participate in designing measures of success/ failures of reengineering 	<ul style="list-style-type: none"> • Bring vast amounts of information into the process • Bring complex analytical methods to bear on the process • Enhance employees' ability to make more informed decisions with less reliance on formal vertical information flows • Identify enablers for process design • Capture the nature of proposed change and match IT strategy to that change • Capture and disseminate knowledge and expertise to improve the process • Communicate ongoing results of the BPR effort • Transform unstructured processes into routinized transactions • Reduce/replace labor in a process • Measure performance of current process • Define clear performance goals and objectives to drive the implementation • Define the boundaries and scope of the process 	<ul style="list-style-type: none"> • Create a digital feedback loop • Establish resources for critical evaluation of the reengineered process • Improve IT processes to meet increasing needs of those divisions that have gone under reengineering processes • Institute a program of "cleanup" and damage control in case of failure • Communicate ongoing results of the BPR effort • Help to build commitment to BPR • Evaluate the potential investment and return of reengineering efforts

Tabella 4. Il ruolo dell'IT nel processo di Reingegnerizzazione

Eftekhari e Akhavan (2013) propongono una metodologia strutturata per la reingegnerizzazione dei processi basata sui seguenti passi:

STEP 1: Valutazione delle performances attuali

In questo step, l'alta direzione si occupa di valutare le performance dei processi al fine di identificare la necessità dell'attuazione del BPR. Questo step comprende le seguenti attività:

- Identificazione della vision
 - Interviste con il top management e con i quadri aziendali al fine di identificare gli obiettivi strategici, la struttura organizzativa ed i ruoli all'interno dell'organizzazione
 - Identificazione dei processi organizzativi.
 - Analisi dei dati e dei documenti interni (organigrammi, manuali, procedure)
- Identificazione del contesto competitivo.
 - Esplorare ed analizzare i concorrenti (attuali e potenziali) presenti sul mercato.

- Valutare le esigenze dei clienti e le modalità di soddisfare le richieste dei clienti e misurare la soddisfazione del cliente
- Identificazione dell'attuale dotazione IT dell'organizzazione.

Tutte le informazioni raccolte in questo primo step consentiranno di definire lo stato corrente dell'organizzazione ed identificare il gap tra le performance attuali dell'organizzazione ed il contesto competitivo. I risultati dell'attuazione della fase "prima di avviare il progetto BPR" sono:

- Identificazione completa della struttura organizzativa
- Analisi e valutazione delle prestazioni dei processi
- Riconoscimento della necessità di modifiche da parte dei dirigenti
- Individuazione di punti di forza e di debolezza organizzativi
- Valutazione delle prestazioni organizzative rispetto al contesto competitivo
- Selezione dell'approccio all'implementazione del progetto di reingegnerizzazione.

STEP 2: Identificazione del cambiamento

L'obiettivo principale di questo step è quello di organizzare un team di progetto BPR per pianificare l'implementazione del progetto e identificare i processi chiave dell'organizzazione. Questo passo può essere condotto attraverso le seguenti attività:

- organizzazione del team di progetto e pianificazione del progetto
Il team BPR è composto da diversi esperti con diverse specialità all'interno e all'esterno dell'organizzazione. È molto importante che i membri del team BPR siano selezionati da diverse parti dell'organizzazione e tutti hanno competenze nel loro campo. Il team BPR inizia il suo lavoro studiando le idee fornite dai top e middle managers. Al fine di identificare i processi chiave organizzativi e attuare il progetto, vengono tenute riunioni regolari affinché i membri possano ideare e presentare idee innovative. I fattori chiave di successo sono analizzati anche dalla squadra BPR in questa fase. Queste attività costituiranno la fase per la pianificazione dell'attuazione del progetto.
- esplorare le opportunità offerte dall'IT (strumenti informatici hardware e software).
Dopo la costituzione del team di BPR, vengono individuate le potenzialità delle tecnologie ICT, identificando il loro impatto sul successo del progetto
- individuare i processi chiave da riqualificare
Considerando i risultati della fase precedente e riconoscendo le strategie organizzative e le prestazioni, il team BPR utilizza tutti gli strumenti disponibili e documenti sui processi organizzativi per identificare i processi chiave (ad esempio strumenti IT e software, diagrammi di flusso dei processi di mappe e organizzativi). Tra i processi chiave organizzativi identificati, i processi vitali vengono estratti e classificati per essere ri-progettati

STEP 3: Implementazione del cambiamento

L'obiettivo principale di questo step è quello di scegliere il metodo migliore per ri-progettare, testare e finalmente stabilire i processi chiave. Questo step è costituito dalle seguenti attività:

- Riorganizzare i processi che devono essere modificati:
Dopo aver specificato i processi chiave da reingegnerizzare, vengono proposte una serie di soluzioni correttive.
- Testing e valutazione dei nuovi processi
I nuovi processi possono essere testati attraverso la simulazione e la prototipazione.
- Implementare i nuovi processi
Dopo la prototipazione e la simulazione dei nuovi processi, gli utenti sono formati per acquisire le competenze necessarie per implementare i nuovi processi. Durante la formazione vengono comunicate le necessità di tali miglioramenti nei processi organizzativi ed indicate le nuove modalità di implementazione dei processi.

STEP 4: Valutazione post-intervento

Lo scopo principale di questo step è quello di migliorare e controllare continuamente i nuovi processi e valutandone i miglioramenti introdotti. In altre parole, il nuovo sistema viene valutato e aggiornato regolarmente. Questo passaggio è costituito dalle seguenti attività:

- Misurare il miglioramento, confrontandolo rispetto alla situazione attuale. Bisogna valutare i miglioramenti in termini di efficienza ed efficacia dei processi, funzionalità del sistema e facilità di utilizzo per i process owners.
- Valutare il gap rispetto al contesto competitivo.
- Valutare la soddisfazione dei clienti.

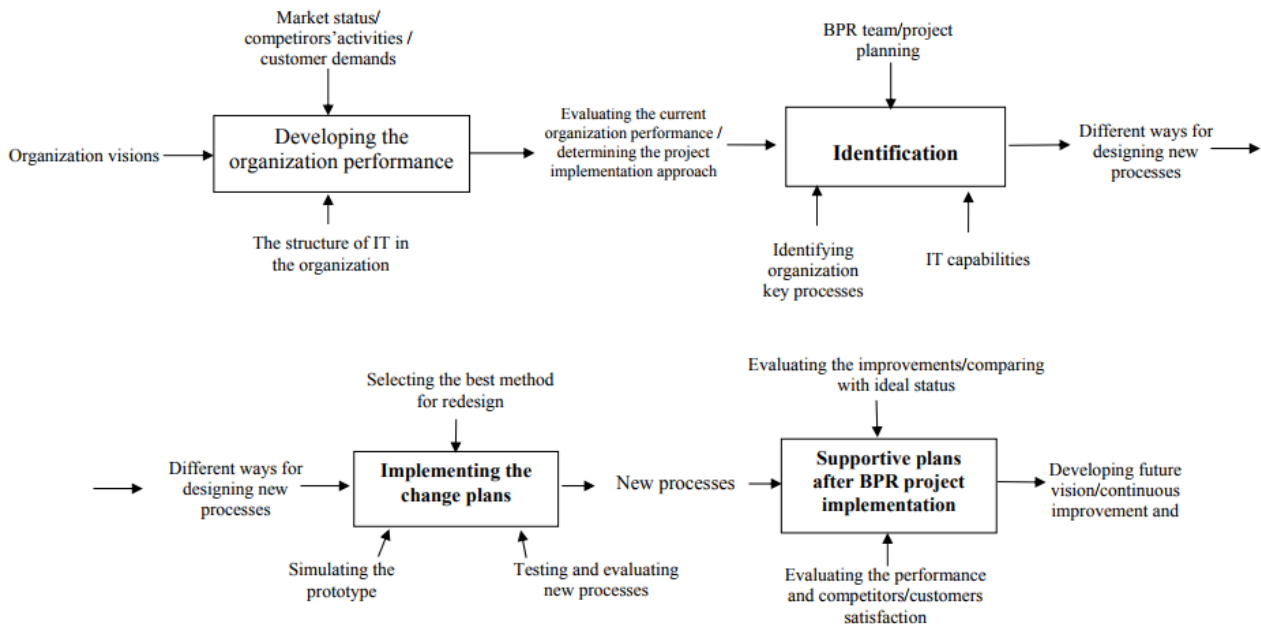


Figura 16. Il processo di Reingegnerizzazione (Eftekhari e Akhavan, 2013)

2.2 Strumenti per la modellazione dei processi aziendali

Nella letteratura scientifica esiste un'abbondanza di tecniche per la modellazione dei processi di business caratterizzate da approcci differenti che catturano diversi aspetti dei processi stessi (Vergidis et al., 2008).

Lindsay (2003) descrive la modellazione dei business process come una "fotografia istantanea" di quello che viene percepito osservando il business process.

L'obiettivo della modellazione dei processi di business, secondo Biazzo (2002), è la rappresentazione delle relazioni tra attività, persone, dati e oggetti coinvolti nella produzione di un output specifico. Così come rilevato da Volkner e Werners (2000) e Aguilar-Saven (2004), la modellazione dei processi di business risulta essere essenziale per l'analisi, la valutazione ed il miglioramento dei business process, fornendo la possibilità di analizzare in maniera sistematica e comprensibile le attività aziendali, diventando altresì un valido supporto per le attività di decision making e per lo sviluppo di software a supporto dei processi stessi.

Come già detto precedentemente, esistono differenti modalità per la modellazione dei business process.

In (Vergidis et al., 2008) viene proposta una classificazione delle metodologie per la modellazione dei business process secondo tre direttive:

- Diagrammatic Models
- Mathematical Models
- Business Process Languages

Il primo insieme include modelli di rappresentazione dei processi aziendali attraverso una rappresentazione grafica, il secondo insieme si riferisce ai modelli che hanno si basano su formalismi di origine matematica, infine, il terzo insieme contiene linguaggi software che supportano la modellazione dei processi aziendali. Il seguente diagramma racchiude le tecniche di modellazione più rappresentative riportate in letteratura:

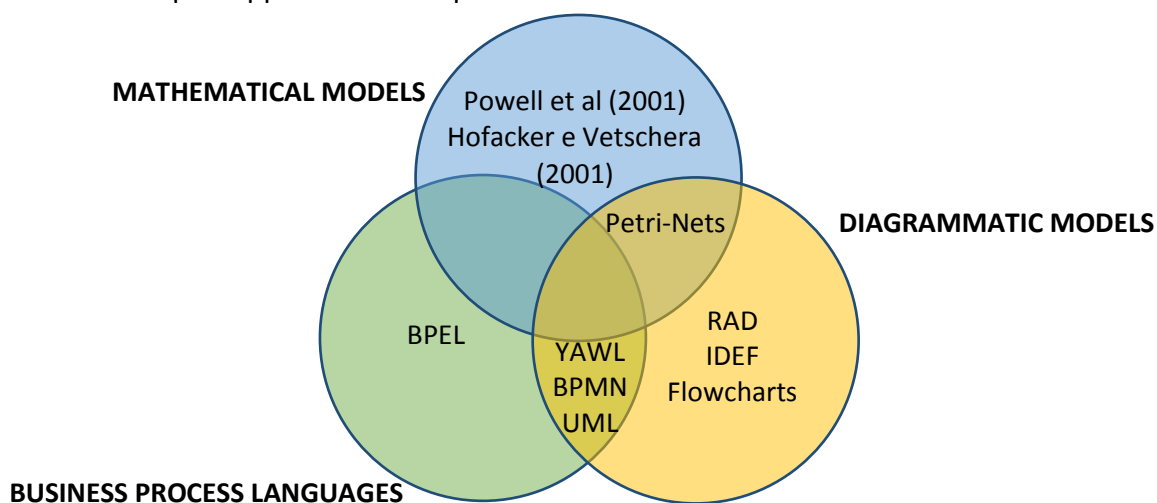


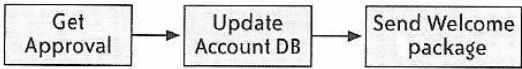
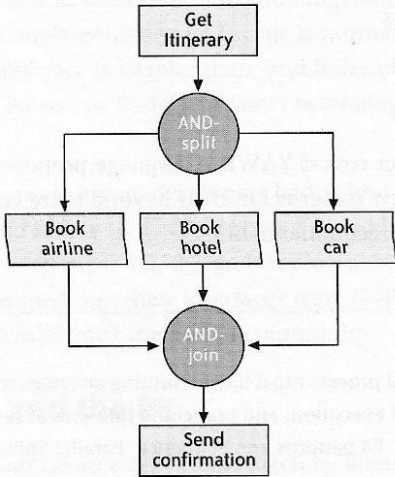
Figura 17. Classificazione delle metodologie di rappresentazione dei processi aziendali (Vergidis, 2008)

DIAGRAMMATIC MODELS: Le prime tecniche utilizzate per la modellazione dei processi aziendali erano semplici rappresentazioni grafiche (cioè diagrammi di flusso), inizialmente sviluppati per definire specifiche software (Chapin N., 1971). Questi schemi semplicistici rappresentavano un processo aziendale, ma molte delle volte senza ricorrere ad un linguaggio formale (Havey, 2005). Ciò ha portato allo sviluppo di metodologie standard come IDEF per la modellazione di processo e / o lo sviluppo del software. La modellazione dei processi aziendali ha beneficiato di questi approcci schematizzati standardizzati poiché sono semplici e facili da usare. Tuttavia, hanno anche ricevuto una serie di critiche da parte di diversi autori. Queste tecniche sono infatti utili per la rappresentazione rapida e informale del processo, ma mancano della semantica necessaria per sostenere i costrutti più complessi e standardizzati. Il punto centrale dell'argomentazione è che questi approcci di modellazione si basano solo su notazioni grafiche (Zakarian e Kusiak, 2001), mancando così la semantica formale (Valiris e Glykas, 1999).

MATHEMATICAL MODELS: La necessità di avere una semantica formale per la modellazione dei processi aziendali ha portato ad una seconda generazione di modelli. I modelli formali sono quelli in cui i concetti sono definiti rigorosamente e con precisione, in modo che la matematica possa essere utilizzata per analizzarle, estrarre conoscenza e motivarle. Van der Aalst et al. (2003) sottolineano che i modelli di processo aziendali "debbono avere una base formale" perché i modelli formali non lasciano alcun ambito di ambiguità e aumentano il potenziale di analisi. Tuttavia, accade spesso che gli elementi e i vincoli dei processi aziendali sono prevalentemente di natura qualitativa, spesso difficili da caratterizzare in modo formale tramite metodi puramente analitici (Tiwari, 2001). Ciò spiega la difficoltà di sviluppare modelli puramente formali dei processi aziendali e il fatto che solo alcuni esempi pratici si trovano nella letteratura. Un approccio che ha una base matematica è proposto da Hofacker e Vetschera (2001). Descrivono un processo aziendale che utilizza una serie di vincoli matematici (che definiscono i confini di fattibilità del processo aziendale) e un insieme di funzioni obiettivo (che consistono in diversi obiettivi per il processo di business process). Il loro approccio può gestire solo processi sequenziali e non può modellare complessi modelli di modellazione. Sono stati dunque sviluppati formalismi che uniscono una modellazione matematica con una rappresentazione diagrammatica. Le reti di Petri sono un esempio di una tecnica di modellazione dei processi aziendali che unisce la rappresentazione visiva usando la notazione standard con una rappresentazione matematica sottostante. Nonostante i loro vantaggi rispetto a semplici approcci schematici, sono state segnalate anche critiche per i modelli di processi aziendali / matematici. La costruzione di un modello di processo aziendale può risultare molto più complesso e esigente rispetto alle tecniche tradizionali in cui è sufficiente un diagramma di processo e l'uso di notazioni matematiche complesse potrebbe scoraggiare l'analista aziendale (Koubarakis e Plexousakis, 2002).

BUSINESS PROCESS LANGUAGES: La terza e la più recente generazione di tecniche di modellazione dei processi aziendali nasce come un tentativo di affrontare la complessità dei modelli formali ma mantenere la loro coerenza e il potenziale per ulteriori analisi. Come la prima generazione di tecniche di modellazione di processi aziendali, anche in questo caso è stata fortemente influenzata da quelle utilizzate nello sviluppo del software. È proprio la natura dinamica, complessa e in rapida

evoluzione dei modelli di processi aziendali che li rende simili alle tecniche di sviluppo del software. Il terzo set prende il processo di business modeling un ulteriore passo avanti in quanto utilizza linguaggi di processo, in genere XML. Questi linguaggi eseguibili specifici per il contesto sono l'ultima tendenza che è la modellazione dei processi aziendali, una tendenza che ha già prodotto diversi pacchetti semantici, con Business Process Execution Language per i servizi Web (BPEL4WS - anche conosciuta come BPEL) e Business Process Modeling Language (BPML). BPML è un prodotto della Business Process Modeling Initiative (www.bpmi.org). È anche un linguaggio basato su XML che codifica il flusso di un processo aziendale in un modulo eseguibile. BPML è accompagnato da BPMN (Business Process Modeling Notation), un linguaggio di diagramma di flusso grafico che è in grado di rappresentare un processo aziendale in una forma visiva intuitivo (Havey, 2005). Ogni processo BPML ha un nome, un insieme di attività e un gestore; supporta anche i sottoprocessi. YAWL (Yet Another Workflow Language) è un altro - come dice il nome stesso - linguaggio di processo grafico creato da van der Aalst e ter Hofstede (2003). YAWL è un linguaggio basato su Petri-net che è stato costruito con l'obiettivo primario per supportare un'ampia gamma di modelli di processi aziendali. Ha ricevuto critiche per essere inadeguato in termini di espressività e di capacità di integrazione (Havey, 2005). In ogni caso, qualsiasi tecnica di modellazione dei processi aziendali dovrebbe essere in grado di supportare una vasta gamma di patterns, ovvero costrutti di base che permettono la standardizzazione di soluzioni ai problemi spesso ricorrenti nei processi aziendali, grazie al riutilizzo di queste parti di processo standardizzate nei vari modelli di processo. L'identificazione dei costrutti di processo di base è necessaria per qualsiasi approccio di modellazione dei processi aziendali per poter considerare diverse dipendenze complesse tra le attività (Scheer, 1994). I principali costrutti base di seguito riportati, sono ripresi da Havey (2005).

<p>1) SEQUENZA: i vari step sono eseguiti uno di seguito all'altro</p>	 <pre> graph LR A[Get Approval] --> B[Update Account DB] B --> C[Send Welcome package] </pre>
<p>2) SINCRONIZZAZIONE: da un'unica attività, devono essere effettuate più attività in parallelo, fino a convergere in un'unica attività, che attende il completamento di tutti i percorsi prima di iniziare.</p>	 <pre> graph TD A[Get Itinerary] --> B((AND-split)) B --> C[Book airline] B --> D[Book hotel] B --> E[Book car] C --> F((AND-join)) D --> F E --> F F --> G[Send confirmation] </pre>

<p>3) SCELTA ESCLUSIVA: da un'unica attività, si deve scegliere soltanto una alternativa sulla base della valutazione di una determinata condizione.</p>	<pre> graph TD A[Get approved] --> B((XOR-split)) B --> C[Send welcome package] B --> D[Send rejection letter] C --> E((XOR-join)) D --> E E --> F[Record in audit trail] </pre>
<p>4) SCELTA MULTIPLA: da un'unica attività, possono essere effettuate più attività in parallelo (ma al verificarsi di determinate condizioni) fino a convergere in un'unica attività, che attende il completamento di tutti i percorsi prima di iniziare.</p>	<pre> graph LR A[Evaluate damage] --> B((OR-split)) B -- Structural damage --> C[Contact fire department] B -- "> \$1000 damage" --> D[Contact insurance company] C --> E((OR-join)) D --> E E --> F[Submit report] </pre>
<p>5) DISCRIMINAZIONE: da un'unica attività, si possono effettuare più attività in parallelo, fino a convergere in un'unica attività che può partire quando N su M attività parallele sono concluse</p>	<pre> graph LR A[Initiate check] --> B((AND-split)) B --> C[No criminal record] B --> D[Natural citizen] B --> E[Good credit] C --> F((2 of 3)) D --> F E --> F F --> G[Grant security clearance] </pre>
<p>6) CICLI: Ripetizione di un flusso di attività fino al verificarsi di una determinata condizione.</p>	
<p>7) INTERRUZIONE: Fermare l'esecuzione di una particolare attività al verificarsi di un determinato trigger di interruzione.</p>	
<p>8) CANCELLAZIONE: Fermare l'esecuzione di un processo al verificarsi di un determinato trigger di cancellazione.</p>	

Tabella 5. Principali patterns di processo (Hovey, 2005)

La seguente tabella riporta invece i pattern di processo supportati dagli approcci di modellazione analizzati in questa trattazione.

	IDEF	UML	PETRI NETS	MATH. MODEL	BPEL	BPMN
Sequenza	X	X	X	X	X	X

Sincronizzazione	X	X	X		X	X
Scelta esclusiva	X	X	X		X	X
Scelta multipla	X		X			X
Discriminazione						
Cicli					X	X
Interruzione		X			X	X
Cancellazione		X			X	X

Tabella 6. Patterns di processo supportati dagli approcci di modellazione

BPMN

Il Business Process Modeling and Notation (BPMN) è uno standard di modellazione dei business process che ha l'obiettivo di fornire una notazione comprensibile a tutti gli utenti, dall'analista che progetta il processo, agli sviluppatori che implementano la tecnologia in grado di eseguire il processo, alle persone che gestiranno il processo. Inoltre assicura che i linguaggi XML, progettati per l'esecuzione dei processi di business, possano essere visualizzati secondo una notazione business-oriented, ovvero definisce un Business Process Diagram (BPD), che rappresenta un adattamento della tecnica di stesura di diagrammi di flusso alla descrizione dei processi di business. Gli elementi che si utilizzano per modellare i business process vengono classificati in 5 categorie di base:

- 1) **Flow objects (Events, Activities, Gateways)**
- 2) **Data;**
- 3) **Connecting objects;**
- 4) **Swimlanes;**
- 5) **Artifacts.**

I Flow objects sono gli elementi principali per definire il comportamento di un processo di business. Ce ne sono di 3 tipi:

- Events, indicano qualcosa che accade durante il corso del processo, influenzando il flusso del processo stesso, e solitamente hanno una causa (trigger) e un impatto (result). Gli eventi sono di 3 tipi a seconda del punto in cui influenzano il flusso: Start, Intermediate, End.
- Activities, indicano un compito che l'azienda deve svolgere all'interno del processo. Può essere atomica o complessa, ossia può essere un task oppure un sottoprocesso.
- Gateways, sono usati per controllare le divergenze e le convergenze del flusso del processo. Eventuali marker interni al simbolo indicano particolari comportamenti di controllo.

La categoria Data è composta dai seguenti elementi: Data object; Data store; Message.

I Connecting objects rappresentano tutti i differenti modi in cui i Flow objects sono collegabili tra loro. Per raggruppare gli elementi precedenti si utilizzano le Swimlanes, che possono essere pool (a

rappresentazione grafica di un partecipante ad una collaborazione) e lane (è una sottopartizione interna a un processo, qualche volta interna ad un pool)

Infine gli Artifacts vengono utilizzati per rappresentare informazione aggiuntive.

Di seguito vengono riportate le rappresentazioni grafiche ed i dettagli delle categorie sopra riportate.

START

Evento	Descrizione	Simbolo
Start event	indica il punto in cui il processo ha inizio	
Start message event	il processo verrà avviato nel momento in cui si riceve un messaggio	
Start timer event	il processo partirà alla scadenza di un timer, ad un dato istante oppure dopo un certo periodo di tempo	
Start signal event	il processo verrà eseguito in base alla ricezione di un segnale, lanciato da un processo esterno, che può essere rilevato anche più di una volta	
Start multiple event	indica che il processo ha inizio al verificarsi di uno tra un insieme di possibili eventi	
Start parallel multiple event	indica che il processo inizia al verificarsi di tutti gli eventi attesi	
Start escalation event	utilizzato solo all'interno di sottoprocessi, reagisce all'escalation a un altro ruolo dell'organizzazione	
Start error event	utilizzato solo all'interno di sottoprocessi fa partire il processo al verificarsi di un predefinito errore	
Start conditional event	il processo inizia al verificarsi di una data condizione	
Start compensation event	utilizzato solo all'interno di sottoprocessi gestisce l'arrivo di una "compensation"	

INTERMEDIATE

Evento	Descrizione	Simbolo	
		Catching	Throwing
Intermediate event	indica l'occorrenza di un particolare evento che non ritarda l'esecuzione del processo		
Intermediate message event	Reagisce all'arrivo di un messaggio		
Intermediate timer event	Rimanda l'esecuzione del processo ad un determinato momento oppure allo scadere di un timeout		
Intermediate escalation event	Deve essere attaccato al bordo di un'attività e reagisce all'escalation di un particolare caso		
Intermediate conditional event	L'esecuzione del processo è ritardata fino al verificarsi di una data condizione		
Intermediate link event	Porta direttamente ad un certo punto del processo. Due link corrispondenti equivalgono ad un sequence flow		
Intermediate error event	Dev'essere attaccato al bordo di un'attività. Reagisce al verificarsi di un errore provocato da un sottoprocesso		
Intermediate cancel event	Dev'essere attaccato al bordo di un'attività. Reagisce al verificarsi di una transazione interna ad un sottoprocesso		
Intermediate compensation event	Dev'essere attaccato al bordo di un'attività. Funge da compensazione in caso di parziale fallimento di un'operazione		
Intermediate signal event	Ritarda l'esecuzione del processo fino all'arrivo di un segnale		
Intermediate multiple event	Ritarda l'esecuzione del processo fino a che uno dei possibili eventi che possono essere causati non si verifica		
Intermediate parallel multiple event	Ritarda l'esecuzione del processo finché tutti i possibili eventi non si verificano		

END

Evento	Descrizione	Simbolo
End event	indica la fine del processo	
End message event	alla fine del processo viene inviato un messaggio di notifica	
End error event	il processo termina in maniera errata, inviando un particolare errore che dev'essere trattato	
End cancel event	il processo termina cancellando una particolare transazione attiva	
End compensation event	alla fine del processo viene eseguita una particolare sequenza di task come compensazione	
End escalation event	alla fine del processo viene eseguita una particolare sezione del processo	
End multiple event	Alla fine del processo viene eseguito uno tra un insieme di possibili eventi	
End signal event	Alla fine del processo viene lanciato un segnale che dev'essere catturato	
End terminate event	indica la terminazione immediata del processo, interrompendo tutti i task ancora in esecuzione	

Tabella 7. Rappresentazione grafica di flow object di tipo Event



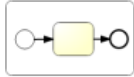

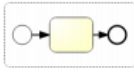
Attività	Descrizione	Simbolo
Task	Rappresenta l'attività da svolgere	
Collapsed subprocess	Rappresenta un'attività che può essere scomposta in più attività. Può essere collegata ad un altro diagramma di processo	
Expanded subprocess	Rappresenta un'attività decomponibile, e deve contenere un diagramma BPMN valido	
Collapsed event-subprocess	Attività decomponibile che deve essere inserita all'interno di un sottoprocesso. Si attiva quando il suo start event verifica la condizione. Può essere eseguito in parallelo al sottoprocesso in cui è contenuto oppure può interromperlo fino al termine della sua esecuzione. Può riferirsi ad un altro diagramma di processo	
Event-subprocess	Attività decomponibile che deve essere inserita all'interno di un sottoprocesso. Si attiva quando il suo start event verifica la condizione. Può essere eseguito in parallelo al sottoprocesso in cui è contenuto oppure può interromperlo fino al termine della sua esecuzione.	

Tabella 8. Rappresentazione grafica di flow object di tipo Activity






Gateway	Descrizione	Simbolo
Exclusive gateway	Instrada il flusso sul sequence flow che verifica la condizione d'uscita, quando divide ha funzione di splitting del flusso. Quando ha funzione di merging, attende un sequence flow in ingresso prima di far proseguire il flusso	
Event-based gateway	È sempre seguito da un catch event o da un receive task. Il flusso viene instradato verso il primo evento o task che si verifica.	
Parallel gateway	Quando viene usato per dividere il flusso, tutti i sequence flow d'uscita vengono attivati simultaneamente. Quando è usato per riunire più flussi, attende che tutti questi siano arrivati.	
Inclusive gateway	Quando viene usato per dividere il flusso, attiva tutti i sequence flow che soddisfano la loro condizione. Quando ha funzione di merging attende l'arrivo di tutti i sequence flow attivi.	
Complex gateway	Attiva uno o più flussi sulla base di condizioni complesse o descrizioni verbali.	

Tabella 9. Rappresentazione grafica di flow object di tipo Gateway

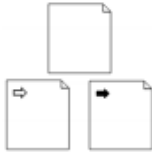


Data	Descrizione	Simbolo
Data object	può essere di due tipi: <i>Data Input</i> o <i>Data Output</i> . Rappresenta l'informazione che circola durante il processo, come ad esempio documenti o e-mail	
Data store	rappresenta il luogo dove il processo può leggere o scrivere dati (ad esempio un database). La sua esistenza non è limitata al periodo di esecuzione del processo	
Message	viene utilizzato per rappresentare il contenuto di una comunicazione tra due <i>Participant</i>	

Tabella 10. Rappresentazione grafica della categoria DATA



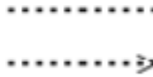
Object	Descrizione	Simbolo
Sequence flow	definisce l'ordine di esecuzione delle attività	
Message flow	utilizzato per mostrare il flusso di messaggi tra due partecipanti abilitati per l'invio e la ricezione di messaggi. In BPMN, due pool separati in un diagramma rappresentano due partecipanti	
Association	utilizzata per collegare un'informazione ad un Artifact. Le Text Annotation e altri Artifact possono essere associati con elementi grafici (ad esempio Task). L'Association, quando è appropriato, può essere indicata con una freccia per esprimere un flusso direzionale	

Tabella 11. Rappresentazione grafica dei CONNECTING OBJECTS



Swimlane	Descrizione	Simbolo
Pool	un pool è la rappresentazione grafica di un partecipante ad una collaborazione. Agisce anche da "swimlane" e da contenitore grafico per partizionamenti di insiemi di attività provenienti da altre pool (in contesto di situazioni B2B)	
Lane	è una sottopartizione interna a un processo, qualche volta interna ad un pool, utilizzata per organizzare e categorizzare le attività	

Tabella 12. Rappresentazione grafica delle SWIMLANES



Artifact	Descrizione	Simbolo
Group	è un raggruppamento di attività appartenenti alla stessa categoria. Un Group non influisce sul flusso del processo. Vengono utilizzati soprattutto per visualizzare graficamente le categorizzazioni di attività in un diagramma	
Text Annotation	utilizzata per fornire, a chi legge il diagramma, informazioni aggiuntive. Possono essere associate ad un Association	

Tabella 13. Rappresentazione grafica degli ARTIFACTS

2.3 La leva per il cambiamento: l'impatto dell'Internet of Things nella reingegnerizzazione dei processi

L'evoluzione del Business Process Management (BPM), come un approccio centrato sul cliente e sui processi per il miglioramento dei risultati di business, è avvenuto nel corso degli ultimi anni come convergenza di due principali domini di riferimento: da un lato l'evoluzione degli approcci organizzativi dell'innovazione, dell'aumento dell'attenzione diretta al cliente, mentre dall'altro lo sviluppo della tecnologia, in combinazione con i protocolli Internet-based, sta consentendo la separazione della gestione aziendale dalla gestione dei sistemi, quindi la separazione del processo dai sistemi, e lo sviluppo dei modelli di processo, guidati dal contesto, che sono essenziali per il BPM (Dumas, 2011)

Con riferimento ai nuovi sviluppi applicativi e tecnologici emerge la necessità di dotarsi di tecnologie e approcci che governino gli sviluppi in termini di velocità di realizzazione (time to market), maggiore automazione delle procedure, adeguatezza alle richieste dell'utente, efficienza dello sviluppo e agilità nel cambiamento. I progetti di Business Process

Management (BPM) hanno spesso l'obiettivo di introdurre visioni organizzative e sistemi informativi che permettano di governare, misurare e gestire il cambiamento di processo nel continuo, realizzando il corretto equilibrio nel trade-off sopra descritto

Intorno al 1950, i computer e le infrastrutture di comunicazione digitale hanno cominciato a influenzare i processi aziendali. Ciò ha determinato cambiamenti drastici nell'organizzazione del lavoro e ha permesso nuovi modi di fare business. Oggi il mondo è soggetto sempre più a repentini cambiamenti e tale andamento diventa col passare del tempo sempre più inarrestabile e incalzante. Le innovazioni nel campo dell'informatica e della comunicazione sono ancora i principali fattori di cambiamento in quasi tutti i processi aziendali.

I processi aziendali sono diventati più complessi, basandosi fortemente sui sistemi di informazione e includendo più organizzazioni. Pertanto, la modellazione di processo è diventata di fondamentale importanza.

I modelli di processo aiutano nella gestione della complessità fornendo informazioni e documentando procedure. I sistemi informativi devono essere configurati e guidati da istruzioni precise e i processi transorganizzativi possono funzionare correttamente solo se esiste un accordo comune sulle interazioni necessarie. Di conseguenza, i modelli di processo sono ampiamente utilizzati nelle organizzazioni odierne

Secondo Van Der Aalst (2013) il Business Process Management (BPM) è la disciplina che unisce le conoscenze della tecnologia dell'informazione alle conoscenze dalle scienze manageriali e le applica ai processi aziendali operativi. Soprattutto negli ultimi 20 anni, si è sviluppata una visione olistica dell'azienda, secondo la quale l'organizzazione come sistema è diventata più importante dell'esame delle sue singole parti. Ciò ha permesso alla "gestione aziendale" di iniziare a separarsi dalla "gestione dei sistemi" consentendo alla "gestione del processo" di esistere separata dai sistemi stessi.

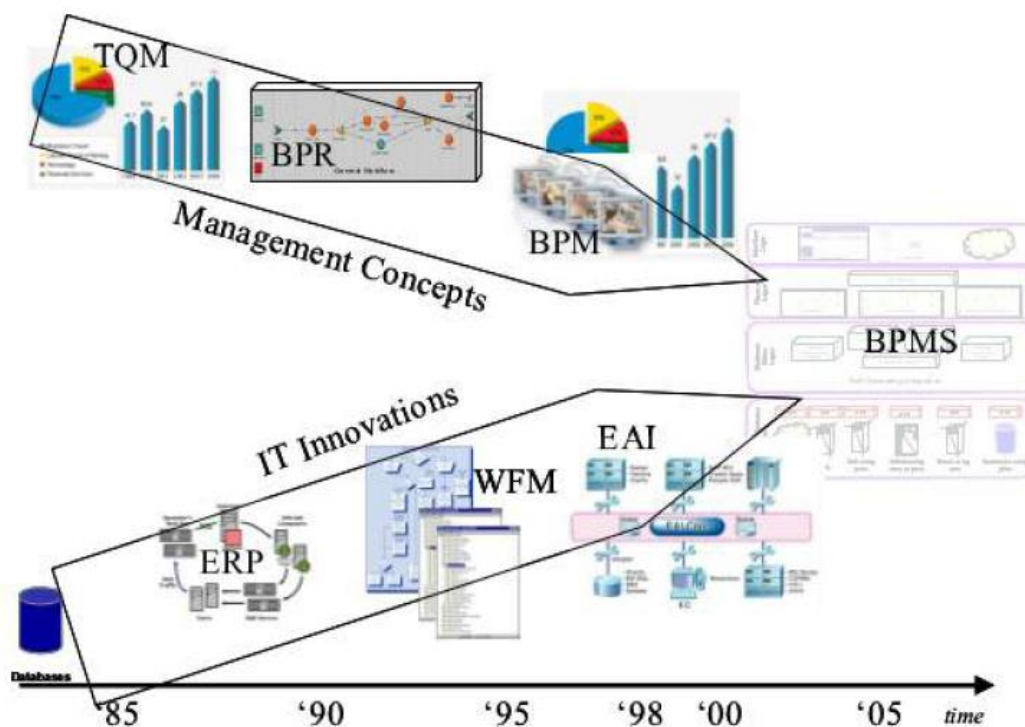


Figura 18. La convergenza tra approcci organizzativi ed innovazioni in ambito ICT

Goldman-Sachs (2014) afferma che l'Internet "sta emergendo come la terza ondata nello sviluppo di Internet. L'ondata di Internet fisso degli anni '90 ha connesso 1 miliardo di utenti mentre l'ondata mobile del 2000 ha collegato altri 2 miliardi di utenti. L'Internet ha il potenziale di far decuplicare questi valori, rendendo possibile la connessione di 28 miliardi di "oggetti" a Internet entro il 2020. La diffusione dell'Internet ha cambiato il modo in cui le persone e le aziende agiscono nella loro vita quotidiana. I settori chiave come la comunicazione, la sanità, la finanza, l'istruzione, il trasporto, la vendita al dettaglio, l'ospitalità, la produzione e l'agricoltura sono già supportati da Internet e altri progressi renderanno altri importanti settori economici del paesaggio di connettività digitale (EY, 2015).

La complessità e l'impatto dell'introduzione delle tecnologie Internet all'interno degli ambienti di business richiede alle aziende una strategia di gestione tecnologica efficace, fondamentale per andare oltre l'aspetto di automazione del processo (Forrester, 2015). Infatti, la combinazione di hardware, software, sensori di controllo, archiviazione dati e connettività consentono alle aziende moderne di generare e trasmettere grandi flussi di dati. Se elaborati correttamente, tali dati hanno il potenziale da un lato, di migliorare la produttività e ridurre i costi marginali, dall'altro, di agevolare e automatizzare i processi decisionali.

Prendendo in considerazione soltanto le aziende operanti nell'Internet, ovvero le società che sono direttamente coinvolte nella produzione di beni (quali dispositivi intelligenti, sensori,

attuatori, applicazioni) o servizi, si prevede che genereranno circa 900 miliardi di dollari di ricavi entro il 2020 (EY, 2015).

Oggi l' IoT ha abilitato nuove piattaforme che, collegando direttamente l'offerta e la domanda, eliminano completamente le industrie tradizionali. I "nativi digitali" (Uber, Airbnb e altri) hanno creato modelli di business completamente nuovi basati sulla fornitura di beni e servizi senza inventario o infrastruttura. Piuttosto, i nativi digitali offrono una piattaforma per collegare i consumatori con i venditori di prodotti e servizi, su richiesta e "a portata di schermo".

Per le aziende diventa di fondamentale importanza capire il potenziale dell' IoT al fine di gestire i loro processi di business e la loro strategia tecnologica (Del Giudice, 2016 a, p. 2). L'adozione di queste nuove tecnologie va al di là della semplice automazione di processo (Forrester, 2015). I dati generati dai processi di IoT hanno il potenziale sia per migliorare la produttività aziendale, per la riduzione dei costi marginali e la semplificazione ed automatizzazione dei processi decisionali. Infatti i grandi flussi di dati generati dagli Smart Objects non solo vengono trasmessi e trattati, ma anche gestiti e trasformati (Eftekhari e Akhavan, 2013).

Il BPM rappresenta il punto di unione tra le misure tecniche e organizzative e può trarre grande vantaggio dall'integrazione dell' IoT poiché il suo obiettivo principale è quello di integrare persone e sistemi automatizzati all'interno di flussi di lavoro strutturati per raggiungere migliori valori di performance (Yu et al., 2011).

Considerando che il Business Process Management si basa sulla gestione dei workflows, l'aggiornamento e la tracciabilità di dati ed informazioni, il modo migliore per ottenere prestazioni migliori è quello di portare il paradigma IoT ad uno stadio successivo, prevedendo una vera e propria interazione con i processi di business (Ozil, 2015). Il Business Process Management rappresenta il legame tra le misure tecniche e organizzative e può trarre grande vantaggio dall'integrazione dell' IoT, in quanto il suo obiettivo principale è quello di fondere persone e sistemi automatizzati in flussi di lavoro strutturati per raggiungere performance superiori (Del Giudice, 2016b). Il ruolo fondamentale del BPM è quello di definire il giusto livello di integrazione tra capacità umane e sistemi di automazione (Candra et al., 2016). La risoluzione di problemi complessi all'interno delle organizzazioni non può basarsi solo su servizi software dotati di capacità cognitive, ma richiede l'intervento umano, supportato da opportuni sistemi di supporto alle decisioni, al fine di fornire soluzioni più efficienti (Doan et al., 2011).

Questa ricerca propone un modello di un Intelligent Protection System (IPS) progettato per ottimizzare la sicurezza e migliorare le prestazioni del processo di gestione della sicurezza delle dipendenze bancarie (Bank Branches – BB). Il modello si basa sulla reingegnerizzazione del processo di gestione della sicurezza BB in corso e la caratterizzazione del Cyber Physical System (CPS) sottostante. La leva per il reengineering è dunque l'utilizzo delle tecnologie IoT,

la cui adozione può supportare la trasformazione di BB in ambienti intelligenti. Se correttamente introdotte e gestite, le tecnologie di IoT hanno il potenziale per migliorare le prestazioni del processo, in termini di efficacia per ridurre il rischio di attacchi criminali e aumentare l'efficienza operativa. In altri termini, è possibile dimostrare che l'introduzione di un IPS è giustificata da fini aziendali come richiesto da Noble (1991) per l'introduzione di un'innovazione "distruttiva" nei processi aziendali. Per raggiungere questo obiettivo, la metodologia si riferisce ad una tipica metodologia di BPR, come originariamente proposto in Hammer e Champy (2009). Tale metodologia è definita per rispondere alle tre domande precedenti poste da Roberts (1994). In particolare, affrontiamo il BPR da una prospettiva di sviluppo del sistema informativo in linea con quanto definito da Valiris e Glykas (1999, p. 446), i quali sottolineano la necessità di introdurre uno strumento metodologico "per comprendere e eventualmente riorganizzare i processi aziendali in modo che l'introduzione dell'IT abbia il massimo impatto possibile su di essi". Con questo obiettivo metodologico, analizziamo il ruolo dell'IT e in particolare dello IoT, come "enabler" della reingegnerizzazione del processo di gestione della sicurezza delle BB e si riferiscono alla ridefinizione per quanto riguarda il miglior utilizzo dell'infrastruttura IT aziendale che si ottiene attraverso la ridefinizione delle risorse esistenti (Attaran, 2004). L'effettiva introduzione del paradigma IoT in un progetto BPR ha il potenziale per migliorare gli effetti dell'introduzione di sistemi ICT già proposti da Eftekhari e Akhavan (2013). Gli effetti chiave dell'introduzione degli IoT sono riassumibili nei seguenti cinque punti:

- integrazione delle attività tra gli stakeholders
- supporto operativo ai workflows
- rafforzare l'efficacia dei processi di creazione e condivisione di dati;
- automatizzare i processi
- consentire il coordinamento.

2.4. Nuovi paradigmi IoT-based per la gestione "intelligente" della sicurezza delle dipendenze bancarie

2.4.1. Introduzione al concetto di "internet-of-things"

Fino a qualche anno fa, la maggior parte delle connessioni Internet in tutto il mondo avveniva solo grazie a dispositivi utilizzati dagli esseri umani, come computer e telefoni cellulari. La forma di comunicazione principale era semplicemente uomo-uomo. Adesso con l'avvento di quello che è definito Internet of Things (IoT) il mondo fisico e quello dell'informazione si mescolano. Il futuro non sarà fatto solo di persone che parlano con altre persone, o di persone che accedono alle informazioni, ma anche di dispositivi che comunicano con altri dispositivi a nome delle persone. Stiamo entrando nell'era in cui

qualsiasi oggetto sarà connesso e si potrà essere connessi in qualsiasi luogo e in qualunque momento.

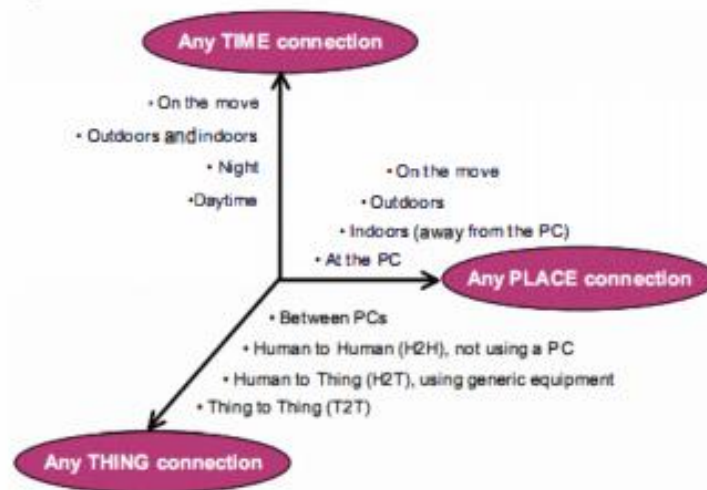


Figura 19. Le dimensioni dell'IoT

Negli ultimi dieci anni, il paradigma dell'“internet of things” (IoT) ha guadagnato sempre più popolarità, sia nella letteratura scientifica che tra gli operatori professionali.

Il termine fu introdotto per la prima volta da Kevin Ashton durante una presentazione a Procter & Gamble nel 1999, riferendosi con questo termine all'uso di sensori RFID nella gestione della supply chain (Ashton, 2009). Il concetto si è poi evoluto nel corso del tempo introducendo una nuova visione in cui Internet si estende al mondo reale e abbraccia oggetti di uso quotidiano i quali acquisiscono una loro identità nella rete.

Molteplici definizioni di Internet of Things, rintracciabili all'interno della comunità scientifica, testimoniano il forte interesse per questo topic e per la vivacità dei dibattiti su di esso.

Negli ultimi dieci anni, più di 14.000 documenti sono indicizzati nella banca dati Scopus con la parola chiave “internet of things”. La Figura seguente mostra l'evoluzione in termini di numero di paper indicizzati con quella parola chiave nell'ultima decade.

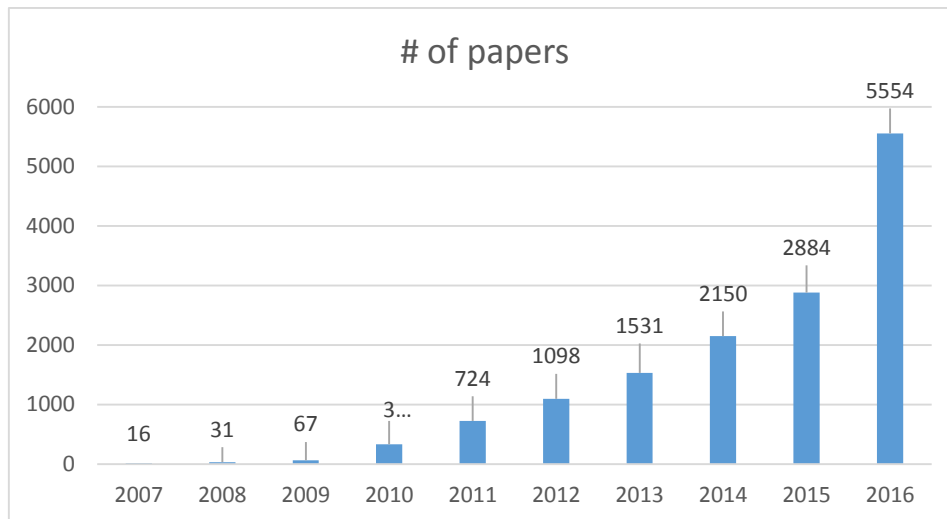


Figura 20. Numero di papers indicizzati nel Database Scopus con la parola chiave “Internet of Things” negli ultimi dieci anni

Analizzando la letteratura, un lettore interessato potrebbe avere difficoltà nel comprendere cosa si intenda realmente per Internet of Things, quali idee stanno alla base di questo concetto, e quali implicazioni sociali, economiche e tecniche avrà. La ragione dell’attuale apparente confusione relativa alla comprensione del concetto è una conseguenza del nome stesso che sintatticamente è composto da due termini “internet” e “things”. Il primo spinge verso una visione network oriented, mentre il secondo sposta l’attenzione su “oggetti generici” da integrare in un framework comune (Atzori et al, 2010). Inoltre le differenze, a volte sostanziali, nelle visioni IoT derivano dal fatto che i vari stakeholder affrontano l’argomento da un punto di vista “internet oriented” o “Things oriented” a seconda dei loro specifici interessi, delle finalità e del proprio background (Atzori et al, 2010).

“Internet of things” vuol dire semanticamente una “world-wide network” di oggetti interconnessi indirizzabili in modo univoco, sulla base di protocolli standard di comunicazione” (INFISO 2008). Ciò implica un enorme numero di oggetti (eterogenei) coinvolti nel processo.

L’IoT rappresenta una visione in cui Internet si estende nel mondo reale abbracciando oggetti di uso quotidiano. Questo significa che gli oggetti fisici non sono più scollegati dal mondo virtuale, ma possono essere controllati da remoto e agire come punti di accesso fisici ai servizi Internet (Mattern and Floerkemeier, 2010).

In Tan and Wang (2010) le “things hanno identità e personalità virtuali, operano in spazi intelligenti utilizzando interfacce intelligenti per connettere e comunicare in contesti sociali, ambientali e con l’utente”.

L'IoT è una tecnologia recente emersa grazie alla convergenza nell'ambito dei sistemi internet & mobile based e nel campo dell'elettronica.

La definizione di "things" comprende dunque una varietà di elementi fisici. Questi includono oggetti personali che generalmente portiamo con noi, come smartphone, tablet e fotocamere digitali, sia elementi che si trovano in ambienti quali la casa, l'auto, il posto di lavoro, sia oggetti dotati di tag (RFID o altro) che si collegano tramite un dispositivo di gateway (ad esempio uno smartphone). Sulla base di questa visione di "things", un numero enorme di dispositivi e oggetti sarà collegato a Internet, ognuno fornendo dati e informazioni e alcuni, anche i servizi (Coetzee et Eksteen, 2011).

Grazie a sensori e ad etichette elettroniche, tali oggetti assumono un ruolo attivo all'interno della rete, dal momento che possono inviare dati su se stessi e ricevere dati da altri dispositivi connessi, creando così un'infrastruttura di comunicazione che rende disponibili tali dati all'interno della rete e a dispositivi mobili, come smartphone e tablet, in modo da poter monitorare gli oggetti di interesse e fornire informazioni all'utilizzatore. In sintesi la Rete dà intelligenza agli oggetti d'uso quotidiano.

Diversi autori considerano il paradigma IoT come un'infrastruttura globale di rete di oggetti intelligenti e altri oggetti fisici di uso quotidiano unicamente indirizzabili, sulla base di protocolli di comunicazione standard (Atzori et al., 2010; Gubbi et al, 2013; Volpentesta, 2015).

Nello specifico in Atzori et al. (2010) si afferma che l'IoT può essere realizzato secondo tre paradigmi: internet-oriented (middleware), things-oriented (sensori) e semantic-oriented (conoscenza). Nonostante sia necessario questo tipo di distinzione a causa della natura interdisciplinare della materia, l'utilità dell'IoT può avere effetti solo in un dominio di applicazione in cui i tre paradigmi si intersecano come possiamo vedere dall'immagine sottostante.

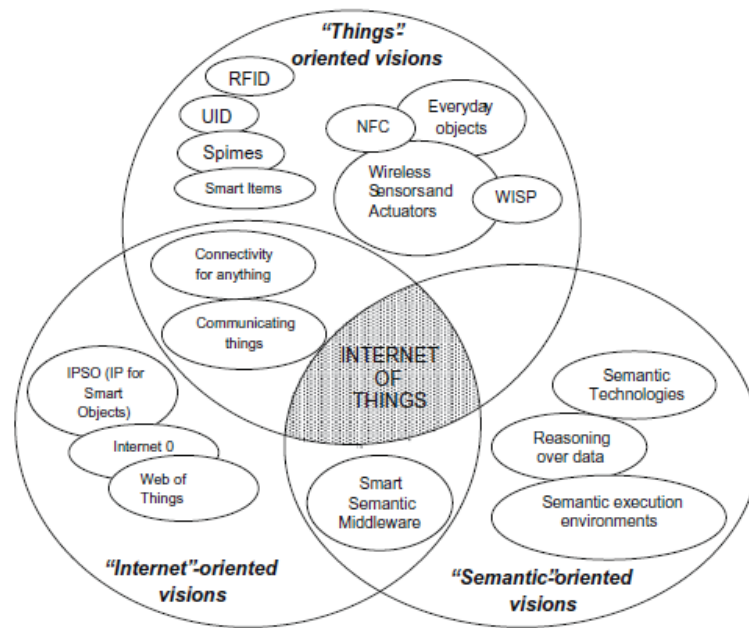


Figura 21. Il paradigma dell' "Internet of things" come risultato della convergenza di visioni diverse.

Secondo la definizione di Gubbi et al. (2013) l'IoT riguarda l'Interconnessione di dispositivi di rilevamento e di azionamento che forniscono la possibilità di condividere le informazioni tra piattaforme tramite un framework unitario, sviluppando un quadro operativo comune per abilitare applicazioni innovative.

L'Internet of things (IoT) è un fenomeno tecnologico che nasce da sviluppi e concetti innovativi nella tecnologia dell'informazione e della comunicazione associati a:

- comunicazione/connettività ubiqua,
- elaborazione pervasiva dei dati e
- Ambient Intelligence

La comunicazione ubiqua riguarda la capacità generale degli oggetti di comunicare dovunque e in qualsiasi momento; Il comportamento pervasivo riguarda il miglioramento di oggetti attraverso l'introduzione di potenza di elaborazione (rendendo gli oggetti intelligenti; Ambient Intelligence significa la capacità degli oggetti di registrare le modifiche nell'ambiente fisico e quindi interagire attivamente in un processo. (Dohr et al., 2010).

Pertanto grazie allo sviluppo che sta avendo la tecnologia wireless e agli studi sull'IoT, la comunicazione "anywhere, anytime by anything" non è più considerata un'utopia. Sempre più dispositivi, in qualsiasi momento, anche senza ricevere degli input da parte di una persona, possono accedere alla rete e interagire con i vari dispositivi connessi (Gubbi et al., 2013).

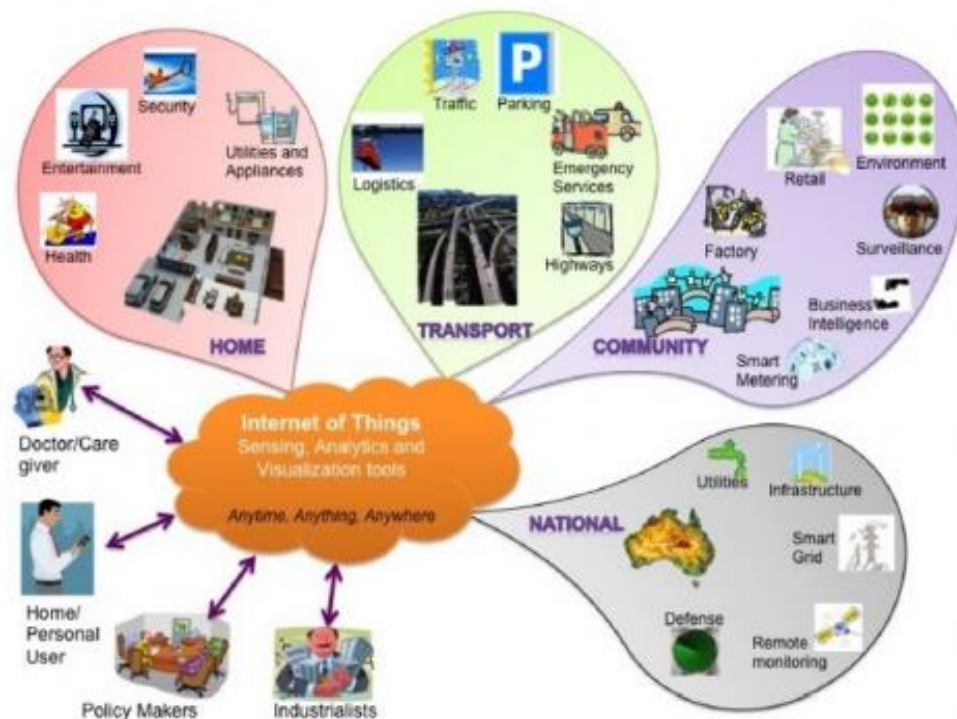


Figura 22. Rappresentazione schematica dell'Internet Of Things (Gubbi et al., 2013)

Goldman-Sachs (2014) afferma che l'IoT "sta emergendo come la terza ondata nello sviluppo di Internet. L'ondata di Internet fisso degli anni '90 ha connesso 1 miliardo di utenti mentre l'ondata mobile del 2000 ha collegato altri 2 miliardi di utenti. L'IoT ha il potenziale di far decuplicare questi valori, rendendo possibile la connessione di 28 miliardi di "oggetti" a Internet entro il 2020. La diffusione dello IoT ha cambiato il modo in cui le persone e le aziende agiscono nella loro vita quotidiana. I settori chiave come la comunicazione, la sanità, la finanza, l'istruzione, il trasporto, la vendita al dettaglio, l'ospitalità, la produzione e l'agricoltura sono già supportati da IoT e altri progressi renderanno altri importanti settori economici del paesaggio di connettività digitale (EY, 2015).

Prendendo in considerazione soltanto le aziende operanti nell'IoT, ovvero le società che sono direttamente coinvolte nella produzione di beni (quali dispositivi intelligenti, sensori, attuatori, applicazioni) o servizi, si prevede che genereranno circa 900 miliardi di dollari di ricavi entro il 2020 (EY, 2015).

2.4.2 Gli elementi costitutivi dell'IoT: gli Smart Objects

Nell'Internet of things, come già affermato, assumono grande importanza gli oggetti. In particolare utilizzando sensori, questi oggetti sono in grado di percepire il contesto in cui si trovano, e mediante funzionalità di rete incorporate sono in grado di comunicare gli uni con

gli altri, accedere ai servizi Internet e interagire con le persone (Mattern and Floerkemeier, 2010). La tecnologia fondamentale che permette di percepire il contesto e monitorarlo è la tecnologia WSN (wireless sensor networks) che, come già detto sopra, monitora l'ambiente tramite i sensori (Da Xu et al., 2014).

Come possiamo dunque dedurre, tutte le diverse definizioni del termine "Internet of things" hanno in comune che sono legate all'integrazione del mondo fisico con il mondo virtuale di Internet.

Tuttavia, come accennato all'inizio di questo capitolo, la prima vera definizione di IoT, nell'ottica del fautore del termine Ashton, è relativa all'utilizzo delle tecnologie Radio-Frequency Identification (RFID).

I tag RFID supportano un maggior numero di ID univoci rispetto ai codici a barre e possono incorporare dati aggiuntivi, come produttore, tipo di prodotto, e anche misurare i fattori ambientali come la temperatura. Inoltre, i sistemi RFID possono localizzare molti tag differenti situati nello stesso ambiente senza l'intervento dell'uomo (Want, 2006).

Uno **smart object**, noto anche come **Intelligent Product**, è un elemento fisico che può essere identificato in tutta la durata della sua vita e interagire con l'ambiente e con altri oggetti. (García et al., 2017)

Come già affermato precedentemente, ciò che permette agli smart objects di interagire con l'ambiente circostante è il sistema operativo in essi integrato e il fatto che sono dotati di attuatori, sensori, o entrambi (Hribernik et al., 2011).

I sensori sono elementi fisici specifici che permettono di misurare un parametro fisico concreto o rilevare qualcosa dell'ambiente prossimo al sensore stesso (García et al., 2017)

Si tratta di un dispositivo che rileva e risponde ad un certo tipo di input proveniente dall'ambiente fisico. Lo specifico input potrebbe essere la luce, il calore, un movimento, l'umidità, la pressione, o un qualsiasi altro gran numero di fenomeni ambientali. L'output è generalmente un segnale che viene convertito in un dato leggibile direttamente attraverso un display presente sul sensore o trasmesso elettronicamente attraverso una rete per la lettura o l'ulteriore elaborazione. (<http://whatis.techtarget.com/definition/sensor>).

I sensori sono, dunque, il legame tra mondo digitale e fisico. Infatti, l'acquisizione automatica del contesto è un prerequisito indispensabile per catturare situazioni del mondo reale. Come visto in (Goertz, 2004): "Un sensore è un dispositivo che percepisce una proprietà fisica e trasmette il risultato ad un misuratore. In parole semplici, associa il valore di qualche attributo ambientale a una misura quantitativa. Quindi i sensori forniscono l'intelligenza all'ambiente fisico.

Secondo Felicetti et al. (2015) i sensori permettono la rilevazione di dati ambientali (ad esempio, la presenza dell'utente, la temperatura, illuminazione, ecc) e l'invio dei dati a un'unità centrale. Gli attuatori riguardano, invece, l'esecuzione di azioni operative sui sottosistemi o apparecchiature in risposta ad un'unità centrale e/o richieste degli utenti.

Gli oggetti dell'IoT possiedono una o più funzionalità di self-awareness, di interazione con l'ambiente circostante ed elaborazione di dati, nonché capacità di connettersi e comunicare le informazioni possedute, raccolte e/o elaborate. L'innovazione principale dell'IoT consiste nell'introdurre una forma di interazione non più solo tra le persone, ma tra persone e oggetti e tra oggetti stessi. Internet connette tra di loro computer, router, server e altri dispositivi informatici. L'internet of things crea una rete più ampia in cui trovano posto anche gli oggetti di uso quotidiano. Questo è reso possibile mediante la loro tracciabilità. L'IoT per poter funzionare infatti necessita di un immenso database nel quale vengono tracciate e catalogate tutte le "cose" (gli oggetti) che appartengono alla rete stessa. Attraverso questi mezzi di riconoscimento e tracciabilità gli oggetti divenuti nodi della rete saranno in grado di comunicare informazioni agli altri nodi sfruttando la connettività senza fili.

Nel contesto dell'"Internet of things" un oggetto potrebbe essere definito come una entità reale/fisica o digitale/virtuale che esiste e si muove nello spazio e nel tempo ed è in grado di essere identificata. Gli oggetti sono comunemente identificati con numeri assegnati di identificazione, nomi e/o indirizzi di localizzazione.

L'IoT implica un'interazione simbiotica tra i mondi reali/fisici, digitali /virtuali: entità fisiche hanno controparti digitali e rappresentazione virtuale; gli oggetti diventano context aware (ovvero in grado di rilevare modifiche di stato nell'ambiente in cui si trovano) e possono percepire, comunicare, interagire, scambiare dati, informazioni e conoscenze. Attraverso l'uso di algoritmi decisionali intelligenti nelle applicazioni software, ai fenomeni fisici possono essere date risposte rapide appropriate sulla base delle più recenti informazioni raccolte circa entità fisiche e considerazione dei modelli nei dati storici, sia per la stessa entità o per simili entità.

Gli oggetti possiedono diverse caratteristiche che li rendono capaci di interagire con l'ambiente circostante. Secondo Mattern and Floerkemeier (2010) gli oggetti hanno diverse capacità che li rendono intelligenti:

- *Communication and cooperation.* Gli oggetti hanno la capacità di fare rete con le risorse di Internet o anche con altro, di fare uso di dati e servizi e aggiornare il loro stato
- *Addressability:* all'interno dell'internet of things gli oggetti possono essere indirizzati
- *Identification:* Gli oggetti sono univocamente identificabili. RFID, NFC (Near Field Communication) e codici a barre a lettura ottica sono esempi di tecnologie con le quali possono essere identificati anche oggetti passivi che non sono dotati di risorse energetiche (con l'aiuto di un "mediatore" come ad esempio un lettore RFID o cellulare). L' identificazione consente agli oggetti di essere collegati a informazioni associate al particolare oggetto e che possono essere recuperate da un server, purché il mediatore è collegato alla rete.

- *Sensing*: Gli oggetti raccolgono informazioni relative all'ambiente circostante con i sensori, le registrano, le trasmettono o reagiscono direttamente ad esso.
- *Actuation*: Oggetti contengono attuatori per manipolare l'ambiente. Tali attuatori possono essere utilizzati per controllare a distanza i processi del mondo reale via Internet
- *Embedded information processing*: Gli smart objects presentano un processore o microcontrollore, più capacità di immagazzinamento dati. Queste risorse possono essere utilizzate, ad esempio, per elaborare e interpretare le informazioni del sensore, o per dare ai prodotti "memoria" del modo in cui sono stati utilizzati.
- *Localization*: Smart things sono context aware ovvero consapevoli della loro ubicazione fisica, o possono essere localizzati. Le reti GPS o dei cellulari sono tecnologie adeguate per raggiungere questo obiettivo.
- *User interfaces*: Gli oggetti intelligenti possono comunicare con le persone in modo appropriato (direttamente o indirettamente, per esempio attraverso un cellulare). Paradigmi di interazione innovativi in questo caso risultano essere importanti, come le interfacce utente tangibili, visualizzazione e voce a base polimerica flessibile, metodi di riconoscimento delle immagini o dei gesti.

Secondo Miorandi et al. (2012) dal punto di vista concettuale, l'IoT si basa su tre pilastri, legati alla capacità degli oggetti intelligenti di essere identificabili, di comunicare e di interagire sia tra di loro, costruendo reti di oggetti interconnessi, o con gli utenti finali o altre entità nella rete. Gli autori definiscono gli smart object come entità che:

- hanno una realizzazione fisica e una serie di caratteristiche fisiche associate (per esempio, dimensione, forma, ecc).
- possiedono un set minimo di funzionalità di comunicazione, come ad esempio la possibilità di essere rintracciato e di accettare i messaggi in arrivo e rispondere ad essi.
- sono in possesso di un identificatore univoco
- sono associati ad almeno un nome e un indirizzo. Il nome è una descrizione leggibile dell'oggetto e può essere utilizzato per scopi di ragionamento. L'indirizzo è una stringa leggibile da una macchina che può essere utilizzato per comunicare con l'object.
- in possesso di alcune capacità di calcolo di base. Questo può variare dalla capacità di abbinare un messaggio in arrivo a una data impronta (come in RFID passivi) alla capacità di eseguire calcoli piuttosto complessi, tra cui il rilevamento dei servizi e le attività di gestione della rete.

- possono possedere mezzi per percepire fenomeni fisici (ad esempio, temperatura, luce, livello di radiazione elettromagnetica) oppure per attivare azioni di effetto sulla realtà fisica (attuatori).

Secondo Meyer et al. (2009) gli Smart Objects possono essere classificati in tre dimensioni. Con queste tre dimensioni, si può determinare l'intelligenza che un oggetto ha e il tipo di smart object di cui si tratta.

Le tre dimensioni a cui Meyer et al. Si riferiscono sono il livello di intelligenza, la posizione della intelligenza, e il livello di aggregazione dell'intelligenza.

1. **livello di intelligenza** dice quanto un oggetto può essere intelligente. È formato da:
 - gestione delle informazioni (*Information handling*), ovvero la capacità dell'oggetto di gestire le informazioni raccolte dai sensori, lettori RFID, o da qualsiasi altra tecnica. Meyer asserisce che senza questa capacità, difficilmente può essere chiamato intelligente.
 - notifica del problema (*Problem notification*) e processo decisionale, ovvero la capacità di un oggetto di avvisare il suo proprietario, in determinate condizioni o quando si verifica un evento insolito
 - decision making: Il processo decisionale è il più alto livello di intelligenza che un oggetto può avere. Il prodotto è in grado di gestire completamente la propria vita, ed è in grado di prendere tutte le decisioni relative a questa autonomamente, senza alcun intervento esterno.
2. La **posizione (collocazione) dell'intelligenza**

Secondo Meyer et al (2009) la seconda dimensione è formata da due categorie ovvero *l'intelligenza attraverso la rete* e *l'intelligenza nell'oggetto*. García et al. (2017) hanno introdotto in questa dimensione una terza categoria che hanno definito come *intelligenza combinata*. Quest'ultima unisce le altre due categorie.

L'intelligenza attraverso la rete (Intelligence through network) consiste nel fatto che l'intelligenza dipende totalmente da un agente esterno (generalmente una piattaforma) a causa della mancanza di intelligenza nell'oggetto stesso. L'intelligenza dell'oggetto, dunque, è completamente al di fuori dall'oggetto fisico. L'agente può essere una rete a cui è legato l'oggetto, questo agente è comunemente noto come *Portal Platform* (Ramparany et al., 2002) , un server o un altro oggetto che prende le decisioni o possiede l'intelligenza globale.

L'intelligenza nell'oggetto (Intelligence at Object) significa che gli oggetti sono in grado di elaborare le informazioni da soli, quindi, non hanno bisogno di alcun agente esterno per essere intelligenti. Hanno potere di calcolo e capacità di immagazzinamento e connessione alla rete. Le piattaforme che hanno gli oggetti con questo livello di solito sono chiamate **piattaforme embedded** (Ramparany et al., 2002)

L'intelligenza combinata (*Combined intelligence*) è un livello che Meyer et al., (2009) non includono nella loro classificazione, ma che comunque includono nella seguente rappresentazione grafica. In questo livello, l'oggetto ha entrambe le intelligenze. L'oggetto possiede la sua intelligenza ed è in grado di utilizzare l'intelligenza che si trova nella rete. Questo piattaforma sono di solito chiamate **piattaforme surrogata** (Ramparany et al., 2002)

3. Il **livello di aggregazione** dell'intelligenza (*Aggregation level of intelligence*). Il livello di aggregazione dell'intelligenza è formato da tre categorie. Questa dimensione è utile per descrivere gli oggetti che sono composti da più parti. A seconda del livello di aggregazione si potrebbe dire che un oggetto è indivisibile oppure ogni parte è indipendente. Le categorie sono: l'intelligenza nell'item, l'intelligenza nel contenitore, e l'intelligenza distribuita.

- L'intelligenza nell'item (*Intelligence in the item*). Questa categoria include gli oggetti che sono in grado di gestire informazioni, notifiche e/o decisioni. Inoltre, se questi oggetti sono composti da componenti diversi, questi componenti devono essere dipendenti gli uni dagli altri. Esempi di oggetti che appartengono a questa categoria sono gli smartphone. Essi sono costituiti da sensori e attuatori che non possono essere separati perché sono incorporati.
- La seconda categoria è l'*intelligenza nel contenitore (intelligence in the container)*. Gli oggetti di questa categoria devono essere in grado di gestire informazioni, notifiche e/o decisioni e devono conoscere i loro componenti al fine di lavorare come un proxy tra i loro componenti e Internet o l'intelligenza. Inoltre, questi oggetti sono in grado di lavorare come contenitori o Smart object nonostante la rimozione di alcuni dei loro componenti. Un Arduino con almeno due sensori appartiene a questa categoria. Se abbiamo rimosso un sensore dall'Arduino, esso sarebbe in grado di continuare a lavorare come contenitore. Un altro esempio potrebbe essere un ripiano intelligente (Meyer et al., 2009) che notifica quando un prodotto è esaurito.
- La terza categoria è l'*intelligenza distribuita (distributed intelligence)*. Questa categoria è la fusione delle altre due. Qui, item e contenitori sono intelligenti ma, in questo caso, essi possono negoziare tra loro per prendere decisioni migliori in base all'intero sistema e al resto degli elementi.

Un esempio di questa categoria è quando si ha uno smart object che è composto da altri smart objects, per esempio, una Raspberry Pi che è connessa a due schede Arduino. In questo caso, ogni Arduino ha la propria intelligenza e può prendere le proprie decisioni, ma a volte, deve chiedere alla Raspberry Pi alcuni dati o lo stato di un altro Arduino per poter eseguire alcune azioni.

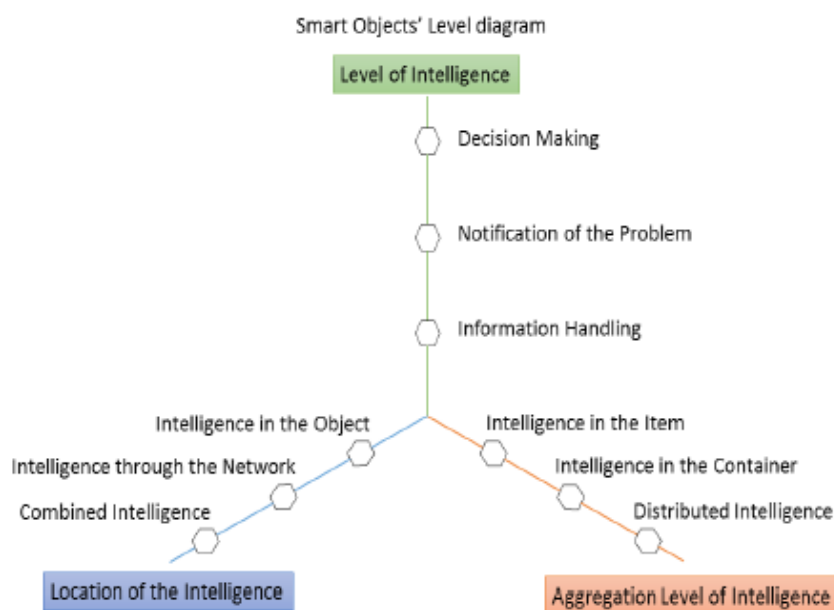


Figura 23. Classificazione dell'intelligenza basata sulla teoria di Meyer

Recenti sviluppi nell'ambito degli smart object, vanno nella direzione dei cosiddetti *indirect sensors* che permettono di nascondere sensori all'interno dell'ambiente (Lloret et al., 2015). Seguendo questo approccio, un unico sensore fisico può consentire di rilevare diverse caratteristiche da uno stesso segnale, invece di richiedere l'utilizzo di molti sensori.

Questa tecnologia si basa su un singolo sensore onnisciente in grado di digitalizzare interi ambiente fisici. Per realizzare tale approccio, sono disponibili due diverse tecnologie: *computer vision*, basata su telecamere intelligenti dotate di sensori multipli e *synthetic sensors*, capaci di integrare e sintetizzare diverse tipologie di segnali (Grill et al., 2015; Dimitrova, 2016; Laput et al., 2017). In questo secondo caso, un unico sensore è in grado di riassumere differenti segnali come vibrazioni, audio, temperatura dell'ambiente, umidità, pressione atmosferica, illuminazione, colore, movimento, interferenze elettromagnetiche. In entrambi i casi, i sensori utilizzano algoritmi di apprendimento macchina per elaborare i dati raccolti, in modo da poter essere riconfigurati per identificare vari tipi di attività.

2.4.3 Smart Environments e Ambient Intelligence

Gli Smart Object rappresentano gli elementi costitutivi dell'Internet-of-Things e offrono la possibilità di connettere persone e ambiente all'interno di un "ambiente intelligente". Gli oggetti dell'Internet of Things non sono altro che oggetti dell'ambiente fisico. L'ambiente fisico circonda le persone che vivono in esso e le persone portano con sé dispositivi mobile (oggetti). Gli oggetti possono essere dotati di sensori e a loro volta i sensori possono essere

installati nell'ambiente fisico. Dotare un oggetto di sensori che lo rendono capace di interpretare l'ambiente circostante rende a sua volta l'ambiente fisico un **ambiente intelligente**. L'intelligenza all'interno degli ambienti (interni ed esterni) permette quindi agli oggetti dotati di sensori di rilevare le condizioni a contorno dell'individuo.

Il campo di ricerca in cui vengono studiati i principi e la metodologia necessaria per la creazione di un ambiente intelligente, si chiama ambient computing. Partendo dall'ambiente fisico, l'ambient computing, infatti, consente di creare spazi in cui dispositivi eterogenei interagiscono tra loro, con le persone e con l'ambiente stesso, consentendo l'identificazione di servizi attinenti al contesto e adattandoli alla situazione e al profilo utente nonché alle sue preferenze. Questi tipi di ambienti sono detti **Smart Environments (SE)**.

Lo smart Environment fornisce una visione della Società dell'Informazione, dove si enfatizza la maggiore facilità d'uso dei servizi e degli oggetti. Le persone sono circondate da interfacce intelligenti intuitive che sono incorporate in tutti i tipi di oggetti e un ambiente capace di riconoscere e rispondere alla presenza di diversi individui in modo trasparente, discreto e spesso invisibile.

Analizzando la letteratura scientifica troviamo differenti definizioni di Smart Environment.

Uno smart environment può essere definito come la combinazione di spazio fisico, infrastruttura per la gestione dei dati (chiamata Smart Space), una collezione di sistemi embedded che raccoglie dati eterogenei dall'ambiente e una soluzione di connettività per trasmettere questi dati allo Smart Space.

Secondo Cook et al. (2005) un ambiente intelligente è “un mondo in cui tutti i tipi di dispositivi intelligenti lavorano continuamente per rendere più confortevole la vita degli utenti”. Anche secondo Augusto (2007) lo Smart Environment, che lui chiama Ambient Intelligence (Aml), è “un ambiente digitale che in modo proattivo, ma sensibilmente, sostiene le persone nella loro vita quotidiana.”

Gli SE mirano a soddisfare l'esperienza degli individui di ogni ambiente, sostituendo l'attività pericolosa, il lavoro fisico e le attività ripetitive con agenti automatizzati. L'obiettivo è quello di arricchire luoghi specifici (stanza, edificio, auto, strada) con sistemi di elaborazione che possano reagire alle esigenze delle persone e fornire assistenza. (Aarts et De Ruyter, 2009).

L'Aml è dunque un sistema sensibile perché dotato di intelligenza. Questa definizione porta Augusto ad effettuare un'analogia con un assistente addestrato.

L'assistente aiuterà, ma si limiterà ad intervenire se non quando necessario. Essere sensibili invece significa riconoscere l'utente, apprendere o riconoscere le sue preferenze nonché la capacità di mostrare empatia o reagire allo stato d'animo dell'utente stesso e alla situazione prevalente, cioè implicitamente richiede che il sistema sia in grado di rilevare ciò che avviene nell'ambiente. (Augusto et al., 2010). Lo smart environment interagisce in maniera user-friendly con le persone, è in grado di riconoscere e rispondere alle emozioni dei suoi abitanti ed è capace di anticiparne i comportamenti e i bisogni.

Lo smart environment riduce l'interazione uomo-computer poichè il sistema usa l'intelligenza per dedurre le diverse situazioni e soprattutto le esigenze dei suoi abitanti e interviene per facilitare l'esperienza dell'uomo con l'ambiente. Il sistema mira a ridurre l'interazione uomo-computer in quanto suppone di usare la sua intelligenza per dedurre le situazioni e le esigenze degli utenti dalle attività registrate, come se un assistente umano passivo osservasse le attività che si svolgono aspettando di intervenire quando (e solo se) necessario (Augusto, 2007)

Secondo Han et al. (2012) il concetto di smart environments o Ambient Intelligence si riferisce agli spazi fisici dotati di sensori di alimentazione in algoritmi adattivi che consentono all'ambiente di diventare sensibile e rispondere alla presenza di persone ed alle loro esigenze individuali. Lo smart environment secondo questi autori rappresenta, dunque, l'infrastruttura fisica (sensori, attuatori e reti) che supporta il sistema.

Gli spazi diventano intelligenti quando sono in grado di osservare ciò che sta accadendo al loro interno, costruire un modello di sé stessi, comunicare con i propri abitanti, e agire in base alle loro decisioni. Chiaramente, questo richiede la presenza di abitanti e un gran numero di sensori, attuatori, e altri dispositivi con processori integrati in grado di comunicare tra di loro, così come la costruzione di una rete informativa globale integrata. (Wang, 2010).

In uno smart environment, le persone svolgono le loro attività quotidiane in modo semplice e comodo utilizzando le informazioni e l'intelligenza nascosta nella rete che collega dispositivi e sensori. (Han et al., 2012).

Un ambiente intelligente sarà in grado di

- Circondare gli utenti in modo non invasivo.
- Riconoscere gli utenti e le loro circostanze (attività, stato d'animo, ecc.) e operare di conseguenza, cioè essere sensibili alla presenza umana.
- avere un comportamento predittivo basato sulla conoscenza dell'ambiente (consapevolezza del contesto), sulle abitudini di coloro che "serve" e sulle attività specifiche degli stessi quando agiscono.
- Realizzare in tempo reale nuovi servizi in ambiti quali intrattenimento, sicurezza, salute, lavori domestici, ambiente di lavoro, accesso alle informazioni, calcolo, comunicazioni, ecc., Per migliorare la qualità della vita creando atmosfere e funzioni adeguate.
- consentire l'accesso a quanti più servizi e funzionalità possono svolgere, indipendentemente da dove si trova l'utente e della posizione in cui l'utente richiede tali servizi (ubiquità).
- Relazionarsi, in modo naturale, agli utenti tramite interfacce vocali multi-modali; Leggendo movimenti e gesti; Generando, emettendo e proiettando immagini; Generando ologrammi, ecc. Gárate et al. (2005).

Lo SE deve essere location-aware, ovvero deve essere in grado di conoscere in qualsiasi momento la posizione delle entità mobili (persone o dispositivi). In esso deve essere rilevato il contesto degli occupanti. In questo modo le informazioni contestuali possono essere utilizzate per supportare e migliorare la capacità di eseguire azioni specifiche applicative, fornendo informazioni e servizi adattati alle esigenze immediate dell'utente (Ryan, 2005). I dispositivi intelligenti che lavorano insieme sono interconnessi tra di loro. Questi dispositivi intelligenti devono catturare informazioni contestuali e per tale ragione devono essere dotati di sensori che forniscono dati di basso livello. Se le informazioni contestuali sono quelle degli utenti, i dispositivi intelligenti sono dispositivi mobile utilizzati dall'utente stesso. Poslad (2009) introduce gli "smart environments", come ambienti capaci di acquisire ed applicare conoscenza al fine di migliorare l'esperienza dei suoi abitanti (Poslad 2009). All'interno di un ambiente intelligente, gli smart environment acquisiscono conoscenza ed agiscono facendo leva sugli smart objects, quali elementi costitutivi di un **cyber physical space**. Quest'ultimo è uno smart environment che fa leva su processi fisici e di rete e dispositivi intelligenti che sono in grado di acquisire ed applicare le conoscenze che provengono dal contesto in cui questi dispositivi sono localizzati.

2.4.4 Smart Environments: dal Cyberspace al Cyber-physical social space

Il concetto di *cyber physical space* rappresenta la naturale evoluzione del ben noto concetto di *cyberspace*, arricchito con nuove funzionalità del paradigma IoT. La parola "cyberspazio" è ampiamente usata in molti contesti a partire dagli anni novanta e rappresenta il concetto di base per molti altri termini (ad esempio cybersecurity, cybercrime, cyberterrorism) che sono stati sviluppati.

Secondo Martin C. Libicki il cyberspace non è altro che un medium virtuale diverso rispetto agli altri domini come la terra, l'acqua, l'aria e lo spazio extra-atmosferico.

Per comprendere la natura ibrida del dominio cibernetico, Libicki rappresenta questa realtà su tre livelli²:

- 1) Il livello fisico (costituito da elementi "materiali" del cyberspace come cavi a fibra ottica, i satelliti, i router, le antenne.
- 2) Il livello sintattico in posizione superiore a quello fisico è costituito dalle informazioni e dalle istruzioni che i progettisti e gli utenti danno allo strumento informatico, si tratta di protocolli operativi per mezzo dei quali i computer o le "macchine" interagiscono con le infrastrutture di riferimento. In questo strato si possono verificare operazioni di hacking, ovvero individui outsider che si introducono nel sistema.
- 3) Il livello semantico rielabora i dati contenuti nelle macchine.

Sotto l'aspetto ambientale il dominio cibernetico si distingue dagli altri ambiti militari. La geografia del cyberspace è molto più mutevole rispetto ad altri ambienti. Le parti del cyberspace possono essere attivate con dei semplici click.

Vale la pena dire che questo termine è spesso inteso in diversi significati. Al fine di fornire una visione più chiara, nel seguito, forniamo una tabella che mostra diverse definizioni di "cyberspazio", riportato dalla letteratura scientifica e le autorità ufficiali di sicurezza del governo. Abbiamo analizzato le definizioni che abbiamo reperito, al fine di individuare una serie di parole chiave che possono rappresentare. Successivamente, queste parole chiave sono state raggruppate per similarità semantica in nove categorie (vale a dire, infrastrutture fisiche, dispositivi IT, persone, software e servizi, dati e informazioni, attività, infrastrutture di rete, internet, connettività). Poi le definizioni sono state classificate secondo le categorie di cui sopra.

9	<u>Cyberspace</u> is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.		X	X	X	X		X	X	X
10	<u>Cyberspace</u> is "The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place"		X					X		X
11	<u>Cyberspace</u> is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.			X	X	X	X	X	X	
12	<u>cyberspace</u> : Word invented by the writer William Gibson in his play "le Neuromancien". It describes the virtual space in which the electronic data of worldwide PCs circulate		X			X			X	
13	The <u>cyber environment</u> include the software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyber environment	X	X		X	X	X			
14	<u>cyberspace</u> The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form		X	X	X			X	X	X
15	The " <u>cyberspace</u> dimension" refers to the middle layer—the information infrastructure—of the three realms of the information warfare battle- space. These three realms are the physical (facilities, nodes), the information infrastructure, and the perceptual.		X			X		X		
16	"The electronic medium of computer networks, in which online communication takes place. . . a metaphor for the non-physical terrain created by computer systems. . . the impression of space and community formed by computers, computer networks, and their users. . .		X	X		X		X		
17	"That intangible place between computers where information momentarily exists on its route from one end of the global network to the other. . . the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light. . . Cyberspace is borderless . . . [but also] think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world."		X			X		X	X	
18	"[National] cyberspace are distinct entities, with clearly defined electronic borders. . . Small-Cyberspaces consist of personal, corporate or organizational spaces. . . Big-Cyberspace is the National Information Infrastructure. . . add [both] and then tie it all up with threads of connectivity and you have all of cyberspace."		X							X
19	"The environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the WorldWideWeb."		X		X			X	X	
20	"The information space consisting of the sum total of all computer networks."		X			X		X		

21	“A physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place. . . . Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats. . . . Cyberspace consists of electronically powered hardware, networks, operating systems and transmission standards.”		X		X	X		X		
22	“The on-line world of computer networks.”							X	X	
23	“A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures.”	X	X			X		X		
24	“The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.”		X						X	X
25	“A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”		X					X	X	
26	“the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.		X	X	X				X	X
27	“Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”		X			X		X	X	

<ol style="list-style-type: none"> 1. Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In Proceedings of the 2011 conference on Information technology education (pp. 113-122). ACM 2. Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 26-28 3. Mesic, R., Hura, M., Libicki, M. C., Packard, A. M., & Scott, L. M. (2010). Air Force Cyber Command (Provisional) Decision Support. RAND PROJECT AIR FORCE ARLINGTON VA. 4. Gibson, William. Neuromancer. Ace Science Fiction Specials, Ace Books, 1984 5. Bryant, R. (2001). What kind of space is cyberspace. Minerva-An Internet Journal of Philosophy, 5, 138-155. 6. Germany, “Cyber Security Strategy for Germany.” Feb-2011. [Online]. Available: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf? 7. United States, “Cyberspace Policy Review.” Jan-2008. [Online]. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf 8. Dictionary, Oxford English Dictionary, 2009 Edition 9. Canada, “Canada’s Cyber Security Strategy.”2010. [Online]. Available: 	<ol style="list-style-type: none"> 15. Waltz, E. L. (1998). Information warfare principles and operations. Artech House, Inc.. 16. Kramer, F.D., Starr, S.H., Wentz, L.K. (2009). Cyberpower and National Security. Potomac Books Inc., Dulles, Virginia, USA. 17. Schwartz, W. (1994). Information warfare: Chaos on the electronic superhighway. Thunder's Mouth Press. 18. Schwartz, W. (2d ed., 1996). Information warfare: Chaos on the electronic superhighway. Thunder's Mouth Press. 19. Walter G. Sharp Sr. (February 1, 1999) Cyberspace and the Use of Force, Ageis Research Corp 20. Dorothy E. Denning , Information Warfare and Security, Addison-Wesley Professional; 1 edition (December 20, 1998) 21. Gregory J. Rattray, Strategic Warfare in Cyberspace, The MIT Press; 1 edition (April 16, 2001) 22. Merriam-Webster Third New International Dictionary (2002) 23. National Military Strategy for Cyberspace Operations (2006) 24. National Security Presidential Directive 54 (2008) 25. Deputy Secretary of Defense Gordon England(2008)
---	--

<p>http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf</p> <p>10. New Zealand, "Cyber security Ministry of Economic Development." Jun-2011. [Online]. Available: http://www.med.govt.nz/sectors-industries/technology-communication/cyber-security</p> <p>11. United Kingdom, "The UK Cyber Security Strategy." Nov-2011. [Online]. Available: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf</p> <p>12. European Union, "Help: Glossary Europa – Information Society 'C' (archived)."[Online]. Available: http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c (2004)</p> <p>13. ITU-T, "ITU-T Recommendations X.1205 (X.cso)," Apr-2008. [Online]. Available: https://www.itu.int/itu-t/recommendations/rec.aspx?id=9136</p> <p>14. ISO/IEC, ISO/IEC 27032 Guidelines for cybersecurity, 2011 -available at https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:e</p>	<p>26. International Standards Organization (ISO 2012)</p> <p>27. The US Joint Publication 3-13 (Information Operations 2012)</p>
--	---

Tabella 14. Definizioni di cyber space nella letteratura scientifica

L'integrazione tra cyberspace e processi fisici ha portato all'introduzione di un nuovo paradigma di ambiente intelligente, noto sotto il termine "Cyber-Physical Systems" (CPS) (Lee, 2008). Come si è detto in precedenza, il concetto CPS deriva da due termini (Ning et al., 2016):

- Cyberspace, che si riferisce alle risorse di informazioni generalizzate, comprese le astrazioni virtuali e digitali per ottenere interconnessioni tra le entità cyber.
- Spazio fisico, che si riferisce al mondo reale, in cui gli oggetti fisici vengono rispettivamente percepiti e controllati da sensori e attuatori per stabilire interazioni attraverso i canali di comunicazione, la collaborazione remota, la localizzazione in tempo reale e la manutenzione dell'autonomia.

Secondo questa prospettiva, un CPS si presenta come un'integrazione dei processi di calcolo, di networking e fisici, in cui gli smart object fisici vengono mappati nel cyberspazio per fornire servizi context-aware. Un CPS integra capacità di calcolo, comunicazione e spazio di archiviazione con il monitoraggio e/o il controllo delle entità nel mondo fisico, e deve farlo in modo affidabile, sicuro, efficiente e in tempo reale (Sanislav e Miclea, 2012).

Due elementi funzionali principali caratterizzano i CPS (Lee et al., 2015):

- Connettività avanzata che garantisce l'acquisizione in tempo reale dei dati dal mondo fisico e le informazioni dal cyber space;
- gestione intelligente dei dati, capacità di analisi e computazionale che costruisce il cyberspazio

Basandosi sul paradigma CPS, sono stati sviluppati diversi tipi di applicazioni per aiutare l'attività degli utenti in molti domini, ad esempio trasporti e logistica (Lee et al., 2015), smart buildings (Fan et al., 2015; Felicetti et al., 2015); sanità (Zhang et al., 2015).

In ogni caso, nei sistemi moderni è importante considerare non solo servizi (ad esempio software) e oggetti: anche gli esseri umani stanno diventando attori sempre più attivi nella fornitura di servizi context-aware. I nuovi approcci tendono a considerare i fattori umani come parte integrante del sistema invece di piazzarli al di fuori dei confini (Liu et al., 2011). In questo senso, molti autori concordano nell'impiego della nozione di Cyber-Physical-Social System (CPSS) (Smirnov et al., 2014; Zeng et al., 2016; Ning et al., 2016; Candra et al., 2016) . CPSS estende il concetto di CPS, includendo il cosiddetto dominio dello "spazio sociale", che include la partecipazione e l'interazione umana tra gli esseri umani e l'interazione uomo-computer. Di conseguenza, è possibile caratterizzare CPSS come un sistema che comprende i seguenti componenti interlacciati:

- Social Space (SS): lo spazio umano che contiene gli attori umani, le caratteristiche sociali, le relazioni e il dispositivo interconnesso dell'utente (Internet of People - IoP)
- Cyberspace (CS): sistemi basati su software, infrastrutture e piattaforme hardware forniscono servizi agli utenti (Internet of Services - IoS)
- Spazio fisico (PS): il mondo fisico di oggetti intelligenti interconnessi, compresi sensori, attuatori e gateway (Internet of Object – IoO)

Quando accoppiati, i suddetti componenti portano alla definizione dei seguenti sottosistemi che caratterizzano un CPSS:

- Human Computer Interaction (HCI): l'uomo non è solo un operatore in un ambiente intelligente, ma interagisce continuamente con oggetti/dispositivi intelligenti per ottenere servizi mobiqui. Volpentesta (2015) identifica due tipi di interazione: un'interazione esplicita si verifica quando un utente interagisce direttamente con un'interfaccia utente di oggetti intelligenti basandosi su input e output espliciti, mentre le interazioni implicite si verificano quando un oggetto intelligente implicitamente rileva l'azione di un utente senza richiedere un input esplicito.
- Cyber social space (CSS): mondi virtuali, reti sociali e servizi basati su internet, permettono una relazione sincrona e asincrona tra gli esseri umani.
- Cyber Physical Space (CPS): l'integrazione di sistemi basati su software, piattaforme, infrastrutture di rete e oggetti intelligenti e dispositivi interconnessi che forniscono servizi basati sul contesto.

Come affermato da Ning et al. (2016), il CPSS sembra essere una versione avanzata del paradigma IoT dove gli attributi sociali sono considerati per affrontare l'integrazione di calcolo, networking e processi fisici che riguardano l'interfaccia del cyber-fisico space e del social space.

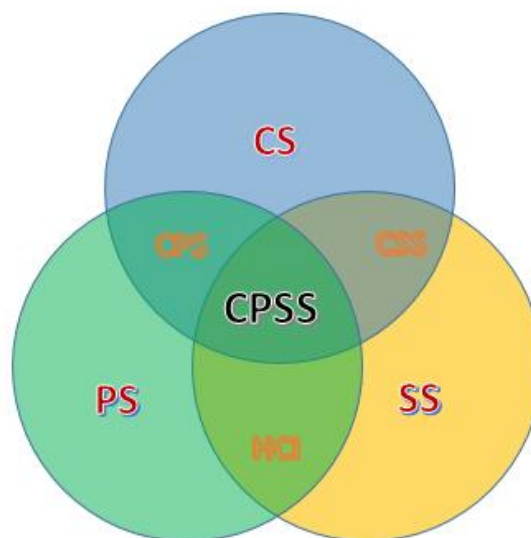


Figura 24. Il concetto di CPSS (elaborazione propria)

I CPSS si basano su infrastrutture di comunicazione, calcolo e controllo comunemente costituite da diversi livelli per i tre mondi (fisico, cyber e sociale) con varie risorse come sensori, attuatori, risorse di calcolo, servizi, persone, ecc. (Smirnov et al., 2014)

Come accennato sopra, I CPSS includono il *cyber space*, il *physical space* e *social space*, quest'ultimo definito da Smirnov et al. (2014) *Mental Space*. Mentre Cyber e Physical space sono stati discussi in precedenza, ora poniamo l'attenzione sul *Social (Mental) Space*.

Il *Social Space* è un'architettura logica, un'integrazione degli attributi sociali e delle intra ed interrelazioni proprie degli esseri umani e di altri oggetti fisici o delle entità cyber. Nel Cybermatics lo spazio sociale può essere formalmente descritto nelle rappresentazioni semantiche per affrontare questioni quali la gestione del controllo di proprietà, la modellazione delle relazioni di affiliazione, la valutazione della fiducia e la formalizzazione del comportamento umano. I principi dell'apprendimento umano (ad esempio, la psicologia cognitiva e la neuroscienza decisionale) e le regole sociali possono essere introdotte nell'esistenza umana, e lo spazio sociale considera sia la società che i suoi gli oggetti, che includono le modalità offline e online.

Si noti che la "thing" nella "società delle cose" si riferisce in senso stretto, a un dispositivo, un'apparecchiatura e un oggetto fisico. La modalità offline è la società nel mondo reale e la modalità online è la società basata sulle piattaforme di social network. (Ning et al., 2016)

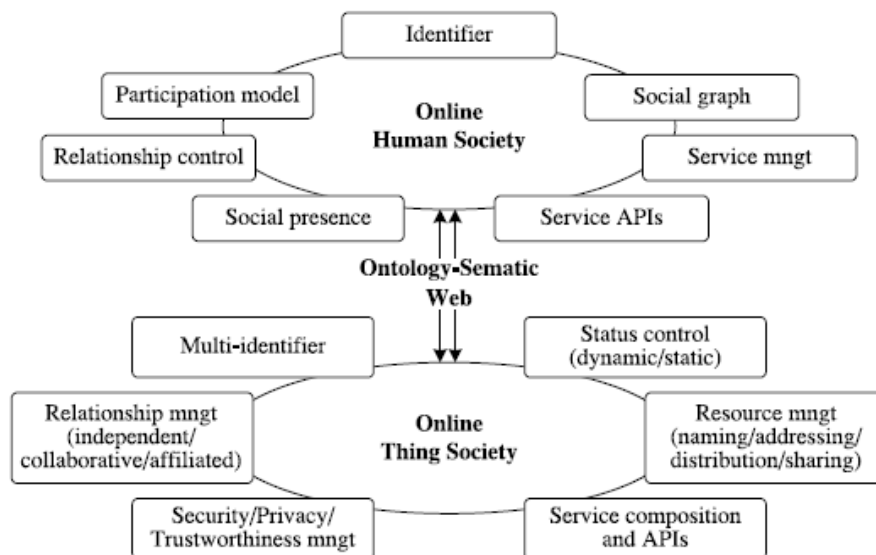


Figura 25. La "società delle cose" vs la "società delle persone"

Secondo Smirnov et al. (2014) lo *spazio mentale (Mental Space)* è rappresentato dagli esseri umani con le loro conoscenze, capacità mentali e elementi socioculturali e le informazioni dal cyberspazio interagiscono con lo spazio fisico (dispositivi fisici) e lo spazio mentale (umano).

Il contesto della risorsa è descritto da posizione, ora, individualità della risorsa e dall'evento. Le risorse eseguono una serie di attività in funzione dei ruoli che svolgono nel contesto attuale e in base al tipo di evento. D'altra parte, il tipo di attività che una risorsa esegue definisce il tipo di evento. Ad esempio, l'evento di una telefonata definisce l'attività umana di risposta al telefono. Ma quando una persona alza la mano al momento della lezione, questa attività definisce un evento come, ad esempio, l'interruzione della lezione. Ciò spiega la bidirezionalità della relazione "definisce" tra evento e attività.

CAPITOLO 3. Ottimizzazione dei processi di sicurezza delle dipendenze bancarie: una proposta di reingegnerizzazione

3.1 La metodologia adottata.

Così come in altri settori di business, per gli Istituti Bancari diventa di fondamentale importanza capire il potenziale dell'IoT al fine di gestire i loro processi di business e sviluppare in maniera integrata la loro strategia tecnologica (Del Giudice, 2016 a, p. 2). L'adozione di queste nuove tecnologie va al di là della semplice automazione di processo (Forrester, 2015), in quanto i dati generati dai processi sono in grado di semplificare e trasformare i processi decisionali, con sostanziali ripercussioni positive in termini di efficienza ed efficacia (Eftekhari e Akhavan, 2013). Considerando che il Business Process Management si basa sulla gestione dei workflows, l'aggiornamento e la tracciabilità di dati ed informazioni, il modo migliore per ottenere prestazioni migliori è quello di portare il paradigma IoT ad uno stadio successivo, prevedendo una vera e propria interazione con i processi di business (Ozil, 2015). La risoluzione di problemi complessi all'interno delle organizzazioni non può basarsi solo su servizi software dotati di capacità cognitive, ma richiede l'intervento umano, supportato da opportuni sistemi di supporto alle decisioni, al fine di fornire soluzioni più efficienti (Doan et al., 2011).

Questa ricerca propone un modello di un Intelligent Protection System (IPS) progettato per ottimizzare la sicurezza e migliorare le prestazioni del processo di gestione della sicurezza delle dipendenze bancarie (Bank Branches – BB). Il modello si basa sulla reingegnerizzazione del processo di gestione della sicurezza BB in corso e la caratterizzazione del Cyber Physical System (CPS) sottostante. La leva per il reengineering è dunque l'utilizzo delle tecnologie IoT, la cui adozione può supportare la trasformazione di BB in ambienti intelligenti. Infatti, se correttamente introdotte e gestite, le tecnologie di IoT hanno il potenziale per migliorare le prestazioni del processo, in termini di efficacia per ridurre il rischio di attacchi criminali e aumentare l'efficienza operativa. In altri termini, è possibile dimostrare che l'introduzione di un IPS è giustificata da fini aziendali come richiesto da Noble (1991) per l'introduzione di un'innovazione "distruttiva" nei processi aziendali. Per raggiungere questo obiettivo, la metodologia si riferisce ad una tipica metodologia di BPR, come originariamente proposto in Hammer e Champy (2009). La scelta dell'approccio metodologico da adottare è avvenuta in base all'analisi della letteratura scientifica riportata nella sezione precedente.

Tale metodologia è definita per rispondere alle tre domande precedenti poste da Roberts (1994). In particolare, affrontiamo il BPR da una prospettiva di sviluppo del sistema informativo in linea con quanto definito da Valiris e Glykas (1999, p. 446), i quali sottolineano la necessità di introdurre uno strumento metodologico "per comprendere e eventualmente riorganizzare i processi aziendali in modo che l'introduzione dell'IT abbia il massimo impatto possibile su di essi". Con questo obiettivo metodologico, analizziamo il ruolo dell'IT e in particolare dello IoT, come "enabler" della reingegnerizzazione del processo di gestione della sicurezza delle BB e si

riferiscono alla ridefinizione per quanto riguarda il miglior utilizzo dell'infrastruttura IT aziendale che si ottiene attraverso la ridefinizione delle risorse esistenti (Attaran, 2004).

La metodologia di reingegnerizzazione proposta in questo lavoro comprende i seguenti quattro steps

1. **RILEVAZIONE DELLA SITUAZIONE ATTUALE.** Per ricostruire il sistema di protezione, è fondamentale effettuare una review esaustiva della letteratura per ricostruire la conoscenza eterogenea nel dominio di sicurezza delle BB. La natura strettamente riservata delle informazioni trattate limita l'accesso a fonti dirette di dati secondari. La maggior parte della letteratura scientifica accessibile ai ricercatori include report statistici sugli attacchi contro la BB e misure di protezione o profilazione criminologica. Le fonti dirette di dati secondari sono difficili da individuare, ad esempio report ufficiali o i white papers prodotti dagli istituti bancari. Per superare questo limite sull'accesso ai dati, questo studio utilizza un approccio multimethod (Sommer e Sommer 1991) basato su:

- una review approfondita della letteratura scientifica e di documenti di terzi (report statistici e documenti di practitioners e società di consulenza), come fonte di dati secondari
- una survey qualitativa per la raccolta dei dati primari.

Nello specifico, l'indagine qualitativa effettuata nel nostro studio, fa riferimento ad un piccolo campione di membri di una popolazione (Fink, 2003), considerando un gruppo di esperti di sicurezza delle dipendenze bancarie, identificati tra security manager dei principali gruppi bancari italiani, il manager responsabile del centro di competenza della cybersecurity di NTT DATA Italia SpA (una delle principali società di consulenza informatica in materia di sicurezza cyber e fisica per i gruppi bancari) ed alcuni esponenti delle forze dell'ordine. L'obiettivo di questa indagine qualitativa non era quello di identificare e definire in maniera esaustiva un determinato dominio teorico, ma quello di raccogliere "fatti" e ottenere "intuizioni" per comprendere opinioni, atteggiamenti, esperienze, processi, comportamenti o previsioni (Guba et al., 1998). Per i nostri scopi, è stato fondamentale condurre interviste semi-strutturate di un piccolo campione di process-owners Rowley (2012). Considerando l'obiettivo dell'analisi causale abbiamo trattato l'indagine qualitativa come un multiple-case study (Yin, 2009).

Le interviste semi-strutturate sono state basate su un inventory progettato in quattro blocchi: le caratteristiche del contesto aziendale in evoluzione e le previsioni sulla sua evoluzione, il funzionamento dei sistemi di protezione attuali, le debolezze rilevate del sistema, i requisiti aziendali per il reengineering del processo di gestione della sicurezza. Le informazioni raccolte attraverso le interviste sono state protette da una "clausola di non divulgazione" riguardante l'utilizzo di informazioni riservate solo per scopi legati alle attività di modellazione. I risultati delle interviste analizzate e la ricerca della letteratura sono state fondamentali per condurre le quattro fasi della metodologia. I partecipanti hanno ricevuto in anticipo i risultati delle attività di modellazione e valutazione alla fine di

gennaio 2017 e hanno fornito loro un feedback entro un mese. I loro suggerimenti sono stati fondamentali per validare i risultati metodologici e le caratteristiche del IPS proposto.

2. **ANALISI DELLA SITUAZIONE ATTUALE.** La modellazione dell'attuale sistema di protezione delle BB comprende la caratterizzazione delle misure di protezione e la rappresentazione dell'attuale trattamento di gestione della sicurezza BB utilizzando le tecniche BPMN (Business Process Management Notation). Questa fase è volta ad evidenziare ulteriori debolezze nel sistema di protezione BB, fornendo linee guida per la ridefinizione di un IPS in grado di migliorare le prestazioni aziendali e di individuare nuove opportunità derivanti dall'IoT. Considerando la mancanza di esempi di best practices in quest'ambito, viene effettuata una valutazione qualitativa su quelle che dovrebbero essere le potenzialità derivanti dall'adozione dello IoT.
3. **MODELLAZIONE DELLA SITUAZIONE OBIETTIVO.** Secondo l'approccio BPR e considerando i risultati del passo 2, proponiamo di affrontare la tradizionale questione della sicurezza fisica secondo una prospettiva di natura "cyber-fisica". Il livello tecnologico di una BB può essere modellato come un CPS in cui le misure di protezione, basate o meno su Smart Objects, sono in grado di interagire tra loro e con l'uomo attraverso una rete digitale. Il modello IPS risultante comprende la rappresentazione del processo di gestione della sicurezza tramite le tecniche BPMN e la descrizione del CPS circostante.
4. **PERFORMANCE ANALYSIS.** Si propone una discussione su ciò che l'IPS può fornire in termini di efficienza (risparmio di tempo, riduzione dei costi) e efficacia (sicurezza migliorata). La soluzione proposta è stata validata da un campione di esperti opportunamente interrogati.

3.2 [Analisi della situazione attuale: Uno stato dell'arte della Letteratura Scientifica](#)

3.2.1 [Modelli e tecnologie per la protezione dei luoghi fisici](#)

Gli Smart Object rappresentano gli elementi costitutivi dell'Internet-of-Things e offrono la possibilità di verificarsi di eventi terroristici e criminosi a livello internazionale ha enfatizzato il ruolo della sicurezza e rafforzato il problema del controllo degli accessi in molte strutture pubbliche e private, con una particolare attenzione nei confronti della salvaguardia sia di beni fisici che delle persone. La sicurezza fisica è definita come il *complesso di misure che prevengono o dissuadono gli attaccanti dall'accedere a un locale, a una risorsa o a informazioni e delle linee guida su come progettare strutture in grado di resistere ad atti ostili* (Conrath, 1999).

Gli aspetti relativi alla sicurezza nelle organizzazioni pubbliche e private possono essere dunque delineati secondo tre prospettive principali:

Sicurezza Fisica: Fine della Sicurezza Fisica è quello di proteggere persone e beni coinvolti nel funzionamento del processo Aziendale. In particolare occorre definire le politiche di salvaguardia sia dei beni, che di tutti gli impianti coinvolti nel processo di produzione del business.

Sicurezza Logica: La Sicurezza Logica si occupa dell'integrità, disponibilità, e riservatezza delle informazioni Aziendali. Devono essere definite adeguate policy di autenticazione ai sistemi, in grado di garantire riservatezza ed integrità dei dati trattati. Inoltre, in merito alla eventuale perdita di dati, con conseguente indisponibilità delle informazioni e relativa interruzione nella "Business Continuity", devono essere definiti criteri e procedure per il salvataggio di dati e per il ripristino degli stessi (Disaster Recovery).

Sicurezza Organizzativa: Oltre all'adozione delle opportune misure tecnologiche connesse agli aspetti precedentemente illustrati, devono essere definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo medesimo (Management System). L'aspetto organizzativo principale riguarda la definizione di ruoli, compiti e responsabilità per la gestione del processo di Sicurezza.



Figura 26. La protezione dei beni aziendali

Nella letteratura scientifica si evidenzia un particolare interesse nei confronti delle misure di sicurezza fisica, sia in termini di salvaguardia dei beni strutturali e patrimoniali in senso stretto (concetto per il quale si utilizza il termine inglese *SECURITY*) che per ciò che concerne l'incolumità psico-fisica degli individui (concetto per il quale si utilizza il termine inglese *SAFETY*) (Burns, McDermid, & Dobson, 1992).

Diversi autori evidenziano la necessità di un approccio integrato alla gestione della sicurezza fisica, parlando spesso di Sistemi di Protezione Fisica (PPS – Physical Protection Systems) (Garcia, 2007).

Oggi sempre più i sistemi di controllo e di sicurezza sono rappresentati dal baricentro dell'integrazione tra applicazioni complementari, da quelle più strettamente connesse al settore della sicurezza - come l'antintrusione, la videosorveglianza, ma anche la rilevazione

delle presenze - a quelle di building automation, fino alle soluzioni di gestione e amministrazione del personale. Alle aziende fornitrici di soluzioni di sicurezza sono pertanto richieste elevate competenze ICT, sistemi innovativi (es. web based) e integrabili con le altre applicazioni aziendali e soluzioni che sappiano coniugare l'elevata tecnologia con le linee guida imposte dalla normativa sulla privacy.

Dal punto di vista della sicurezza, l'Italia si inserisce nel contesto europeo e internazionale (sia per la natura dei problemi che per le possibili risposte, compresa la cooperazione internazionale, sia europea che transatlantica), ed intende dedicare ai vari aspetti della sicurezza la necessaria attenzione e le imprescindibili risorse. Nel 2010 è stata creata SERIT (Security Research in ITaly) una Piattaforma Tecnologica Nazionale sulla Sicurezza promossa congiuntamente da CNR e Finmeccanica che raggruppa le aziende e gli enti che in Italia si occupano di ricerca in ambito Homeland Security, con l'obiettivo dello sviluppo di capacità e tecnologie volte ad individuare, prevenire, contrastare e gestire l'impatto di atti criminali e dolosi, inclusi quelli terroristici, che possano nuocere ai cittadini, alle organizzazioni, alle infrastrutture ed ai beni materiali ed immateriali. Si considerano inoltre tutte le attività di ricerca e sviluppo rivolte alla mitigazione dei rischi, alla gestione delle crisi e all'assicurazione della continuità operativa, a valle di eventuali attacchi/incidenti, in un'ottica all'hazards approach, che tenga conto anche di disastri naturali, antropici e industriali e rischi emergenti (SERIT, 2014). Da un punto di vista normativo, la stringente necessità di proteggere le cosiddette infrastrutture critiche da numerose minacce viene esposto anche all'interno del Decreto Legislativo 61/2011, con cui l'Italia ha recepito la Direttiva 114/08 CE, Direttiva che "stabilisce una procedura d'individuazione e designazione delle infrastrutture critiche europee e un approccio comune per la valutazione della necessità di migliorarne la protezione al fine di contribuire alla protezione delle persone" (COM, 2008).

Un sistema di protezione fisica non riguarda soltanto l'utilizzo di tecnologie, ma integra persone, procedure e attrezzature per la protezione di beni o servizi contro il furto, sabotaggio o qualsiasi intervento mirato a danneggiare cose o persone, implicando la necessità di un approccio metodologico integrato.

La sicurezza personale e degli spazi, intesi sia come luoghi di lavoro e privati sia come aree pubbliche, sta diventando un'esigenza sempre più rilevante, che ha bisogno di soluzioni complete e integrate, che siano in grado di verificare i transiti di persone e mezzi a qualunque varco e luogo secondo criteri di semplicità di configurazione e immediatezza di utilizzo. Alla luce degli eventi criminosi e terroristici degli ultimi anni, ha assunto una sempre maggiore enfasi il concetto di sicurezza personale e degli spazi, e più specificatamente delle cosiddette "infrastrutture critiche". Per infrastrutture critiche si intendono tutte quelle strutture (ad es. porti, aeroporti, siti istituzionali, banche) a rischio di atti vandalici, sabotaggi fisici ed informatici, attentati e minacce al patrimonio fisico quali potrebbero essere furti, rapine, incendi dolosi ed occupazioni (Anderson & Malm, 2006).

Contrariamente ad un passato in cui si necessitava di strumenti di sicurezza solo per proteggere i beni materiali, oggi aziende e istituzioni di qualsiasi settore e dimensione hanno sempre più bisogno di proteggere anche i beni immateriali, l'incolumità delle persone e la continuità della loro attività. Per questo un sistema integrato di sicurezza e controllo accessi deve essere progettato per coniugare le esigenze di sicurezza con quelle di libertà operativa (Bertocchi, Emanuele, Paoluzzi, & Zollo, 2008).

In base alla necessità dell'intervento umano nell'attivazione dei sistemi di protezione è possibile operare una distinzione in

- Sistemi di Protezione Passivi
- Sistemi di Protezione Attivi

Le misure di protezione passive propongono, a fronte dei rischi di effrazione, soluzioni statiche la cui funzione è principalmente quella di impedire o ostacolare fisicamente i tentativi di intrusione e di accesso non autorizzato ai beni protetti. I sistemi di protezione attivi invece richiedono l'attivazione (automatica o da parte dell'uomo) di una contromisura a seguito di un evento di rischio (Baker, 2012).

Per quello che riguarda le misure tecnologiche di protezione attiva, vengono proposte in letteratura differenti soluzioni. Liu e Silverman (2001) presentano una review sulle tecnologie biometriche per la sicurezza. Il settore della sicurezza utilizza tre diversi tipi di autenticazione: qualcosa che si sa (password, PIN, informazioni personali); qualcosa che si ha (smart card, Carta SecurID), qualcosa che si è (un dato biometrico). Tra queste alternative, la metodologia di autenticazione biometrica viene ritenuta dagli autori senz'altro la più sicura, in quanto si basa su caratteristiche che non possono essere prese in prestito, rubate e/o smarrite. Vengono identificate le seguenti tipologie di dati biometrici che possono essere utilizzate in un sistema di sicurezza:

- *Impronte digitali*: Una impronta digitale è un'impronta lasciata dai dermatoglifi dell'ultima falange delle dita delle mani. Un dermatoglifo è il risultato dell'alternarsi di creste e solchi. Esse presentano caratteristiche di immutabilità ed individualità. Per quanto riguarda la prima caratteristica, le impronte si formano definitivamente nel feto al settimo mese di gravidanza e non cambiano per tutta la vita (in caso di graffi o tagli, la pelle dei polpastrelli ricresce con le stesse caratteristiche). Per ciò che concerne la seconda caratteristica, l'individualità, essa viene ritenuta essere vera sulla base di risultati empirici. Il riconoscimento biometrico è effettuato confrontando caratteristiche come la tipologia globale dell'impronta, la posizione e la tipologia di alcuni punti distintivi, l'orientamento e frequenza delle creste, la posizione ed il tipo delle minuzie (terminazioni, biforcazioni delle creste) (Maltoni, Maio, Jain, & Prabhakar, 2009).
- *Riconoscimento del volto*: si tratta di un processo di acquisizione del tratto biometrico a scarsa invasività. I sistemi biometrici basati sul volto possono utilizzare caratteristiche globali o misurazioni locali. Esempi di caratteristiche globali sono le

autofacce, ottenute come le differenze tra l'immagine del volto acquisita ed il volto medio di una base di dati biometrica. Caratteristiche locali sono invece le informazioni geometriche, ottenute misurando le distanze relative tra punti distintivi come occhi, bocca e naso (Jain, Technology: Biometric recognition, 2007).

- *Iride*: l'iride è considerato il tratto biometrico più accurato. L'iride umana è infatti caratterizzata da un pattern casuale, stabile per l'intera durata della vita di un individuo e dotato di numerose caratteristiche distintive. Oltre ad un'elevata accuratezza, il processo di riconoscimento dell'iride è molto veloce. Ciò ha consentito una rapida diffusione dei sistemi di riconoscimento basati su questo tratto biometrico in contesti applicativi caratterizzati da un elevato numero di utenti, come frontiere o aeroporti. Un limite alla diffusione di questa tecnologia consiste nel fatto che il processo di acquisizione delle immagini iridee viene considerato invasivo e pericoloso per la vista da parte di numerosi utenti. I sistemi biometrici basati sull'iride sono inoltre relativamente costosi. La maggior parte di questi sistemi biometrici è basata sul calcolo di una stringa binaria che ne incorpora le caratteristiche distintive, chiamata *Iriscode* (Daugman, 2004).
- *Geometria della mano*: I sistemi biometrici basati sulla geometria della mano, forniscono sicuramente un'accuratezza inferiore a quella dei sistemi basati sull'analisi dell'iride o delle impronte digitali o iride. Tuttavia questa tecnica è particolarmente apprezzata in quanto è ritenuta come poco invasiva dagli utenti. Il metodo è basato sull'acquisizione di una fotografia della mano mentre essa è posizionata su un supporto (eventualmente con l'ausilio di pioli per aiutare il corretto posizionamento). Successivamente, sono effettuate misurazioni delle dimensioni della mano, come, ad esempio, la lunghezza e larghezza delle dita e del palmo (Sidlauskas & Tamer, 2008).
- *Retina*: I sistemi basati sulla retina sfruttano l'unicità dei pattern delle vene presenti sulla zona posteriore del bulbo oculare per effettuare il riconoscimento biometrico. La distribuzione dei vasi sanguinei sulla retina è infatti principalmente casuale ed univoca per ogni individuo. Tra i principali vantaggi, è da annoverare che questo tratto biometrico è difficilmente falsificabile, in quanto la parte esaminata si trova all'interno dell'occhio. Per lo stesso motivo, però, la scansione della retina viene vista come intrusiva e potenzialmente dannosa (Jain, Ross, & Prabhakar, 2004)

Altri sistemi biometrici di discreta diffusione sono basati sulle caratteristiche di voce, firma e camminata. Esistono inoltre sistemi biometrici in grado di sfruttare contemporaneamente informazioni inerenti a differenti tratti. Questa tipologia di sistemi biometrici consente di ottenere una maggiore accuratezza nel riconoscimento e risulta maggiormente robusta a tentativi di frode o intrusione rispetto ai sistemi basati su un unico tratto biometrico (Gamassi, Piuri, Sana, Scotti, & Scotti, 2006).

Per quanto riguarda altre tecnologie a supporto della protezione dei luoghi fisici, in (Bonfanti, 2014) si propone una review relativa alle nuove tecnologie di sniffer artificiali (conosciuti anche come “nasi elettronici” o “sniffer chimici” al fine di rilevare sostanze illecite, polvere da sparo o materiale esplosivo. Zyczkowski, et al., (2011) presentano un sistema mobile per la protezione di oggetti di grande superficie, che consiste in un radar e telecamere termiche e visive. Il radar è utilizzato per la rilevazione immediata e la localizzazione di un intruso e le telecamere con ristretto campo visivo sono utilizzati per l'identificazione e il tracciamento di un oggetto in movimento. Una tecnologia emergente nell'ambito dei meccanismi di protezione per i luoghi fisici è quella relativa ai cosiddetti body scanner. Si tratta di un dispositivo di imaging dell'intero corpo utilizzato per lo screening di sicurezza. Permette una ispezione corporale, finalizzata alla ricerca di armi e/o esplosivi, senza alcun contatto fisico con gli addetti alla sicurezza. È un'apparecchiatura ad onde millimetriche, ossia emissioni elettromagnetiche a bassa frequenza, che rileva presenza di oggetti addosso ad una persona. Il body scanner si presenta come una cabina, con ingresso e uscita aperti, che l'utente soggetto al controllo deve attraversare. Nel caso in cui il body scanner rilevi un oggetto, sul monitor posto sul lato di uscita dalla cabina si riproduce una sagoma stilizzata del corpo umano, con l'indicazione della zona ove effettuare un controllo manuale approfondito. Altrimenti viene dato il segnale di via libera di colore verde. Le risultanze del monitor costituiscono la guida operativa per l'addetto alla sicurezza. Ai fini della tutela della privacy, la macchina riproduce, esclusivamente in caso di rilevazione positiva, una sagoma stilizzata standard, non l'immagine della persona che si sta sottoponendo al controllo. In caso di rilevazione di un oggetto sospetto indosso al passeggero, il monitor indica la zona dove effettuare il controllo manuale approfondito. Vengono rilevati tutti i materiali, metallici e non metallici: liquidi, gel, plastica, ceramica ecc., nonché tutti i tipi di oggetti: armi, esplosivi sia standard che assemblati, sostanze stupefacenti, denaro, carta e così via (Neroth, 2011).

Una tecnologia di controllo molto diffusa nei sistemi di controllo e protezione dei luoghi fisici è senz'altro quella della Televisione a Circuito chiuso (TVCC) o Closed Circuit Television (CCTV), ovvero l'uso di telecamere che trasmettono il segnale verso specifici o limitati set di monitor e/o videoregistratori. Gli impianti CCTV sono usati per sorvegliare aree che devono essere controllate come aeroporti, banche e basi militari. Gli impianti TVCC sono utilizzati prevalentemente come sicurezza passiva, ossia sistemi che registrano 24 ore su 24 e al verificarsi di eventi vandalici, attentati o qualsiasi evento di questo tipo, le immagini registrate vengono analizzate per ricostruire il fatto (Matchett, 2003). Bisogna tuttavia sottolineare che nei sistemi di videosorveglianza tradizionale con elevati numeri di monitor da sorvegliare, soltanto il 3% delle immagini vengono effettivamente viste in tempo reale dagli operatori di sorveglianza e che inoltre tali operatori necessitano di una pausa fisiologica di circa 5 minuti ogni ora (Wallace & Diffley, 1988). Questi fattori limitano fortemente l'efficacia di questi sistemi di sorveglianza. Al fine di superare tali limiti, negli ultimi anni queste tecnologie sono state affiancate da sistemi intelligenti di supporto alle decisioni che consentono di rilevare in maniera

semiautomatica situazioni di rischio, comportamenti anomali (come la corsa, permanenza sospetta, persone a terra, Rilevazione movimenti umani veloci improvvisi) o individuazione di persone sospette (Chiu, Lu, & Wen, 2006) (Goya, Zhang, Kitayama, & Nagayama, 2009). Sul tema della modellazione dei comportamenti e della rilevazione automatica degli eventi di rischio, viene effettuata una review esaustiva in (Dee & Velastin, 2008).

Secondo una prospettiva di natura organizzativa e modellistica, in (Rinaldi, 2004) vengono individuati i principali elementi di un Sistema di Protezione Fisica:

- **Deterrenza.** Misure di sicurezza che consentono di mitigare il rischio ai danni di un'infrastruttura fisica in quanto invitato il malvivente a desistere dal compiere l'azione criminosa. Misure quali un'opportuna illuminazione, una struttura con ampi spazi senza ostacoli alla visuale, la presenza di un sistema TVCC (TV a Circuito chiuso) o la presenza di personale addetto al controllo (ad es. guardie giurate) possono dissuadere un malintenzionato ad attaccare un insediamento.
- **Rilevazione:** Lo scopo di misure di sicurezza attiva, quali i sensori, è di rilevare la presenza di un intruso. Un efficace sistema di rilevazione deve comprendere sia dispositivi elettronici, quali sensori e telecamere, sia l'osservazione visiva per la valutazione della validità dell'allarme. In funzione del tipo di sensori, un sistema di rilevamento può includere rilevatori di movimento, telecamere di monitoraggio, apparecchiature di controllo accessi, o altri dispositivi.
- **Ritardo:** I dispositivi di sicurezza passiva, come le barriere fisiche, devono essere progettati per ritardare l'azione del malintenzionato fino a quando una forza di risposta può contrapporsi alla stessa. Essi sono generalmente composti da apparati di elevata resistenza fisica, spesso dislocati su più livelli, per fornire una protezione in profondità. La loro azione è più efficace se collocati all'interno di una zona di rilevamento.
- **Contromisure.** Le contromisure si riferiscono alle azioni intraprese per interrompere le iniziative del malintenzionato. Il personale di staff, quello di security o le Forze dell'Ordine possono attuare le contromisure più appropriate in relazione al tipo di minaccia ed alle procedure di sicurezza dell'insediamento. La capacità del personale impiegato in un evento di sicurezza, il loro numero, l'autorità e le armi in dotazione dovrebbe essere superiore alla capacità percepita di una minaccia alla struttura. La squadra di risposta più adeguata dovrebbe essere identificata durante la fase di valutazione della vulnerabilità della struttura e di relativi requisiti operativi ed il protocollo da adottare chiaramente stabiliti nel piano di risposta alle emergenze.

La seguente tabella riassume fasi, obiettivi e modalità di un approccio integrato alla protezione fisica di una cosiddetta "infrastruttura critica".

FASE	SCOPO	COME
Deterrenza	<ul style="list-style-type: none"> • Scoraggiare facili accessi • Definire univocamente i confini 	<ul style="list-style-type: none"> • Recinzioni, mura • Barriere, cancelli, lucchetti • Vincoli fisici
Rilevazione	<ul style="list-style-type: none"> • Fornire un rapido allertamento di accessi non autorizzati 	<ul style="list-style-type: none"> • Sensori di rilevamento intrusioni
Ritardo	<ul style="list-style-type: none"> • Rallentare l'accesso ai beni primari • Ritardare l'intruso per le opportune verifiche 	<ul style="list-style-type: none"> • Recinzioni, barriere interne • Segnalazioni ottico/acustiche • Dispositivi di rallentamento
Verifica	<ul style="list-style-type: none"> • Accertare che si tratta di un vero evento di allarme 	<ul style="list-style-type: none"> • Illuminazione • Visione diretta • Sistemi TVCC
Risposta	<ul style="list-style-type: none"> • Intraprendere le contromisure più adeguate 	<ul style="list-style-type: none"> • Comunicazioni • Allertamento Vigilanza • Forze dell'Ordine

Tabella 15. Fasi, obiettivi e modalità di protezione di una "infrastruttura critica"

O'Rourke (2007) concettualizza il concetto di sicurezza fisica delle infrastrutture critiche secondo quattro caratteristiche:

- *Robustezza*: la forza di resistenza intrinseca o in un sistema di sopportare sollecitazioni esterne senza degradazione o perdita di funzionalità.
- *Ridondanza*: proprietà di sistema che consentono opzioni alternative.
- *Risorse*: la capacità di mobilitare risorse e servizi necessari in caso di emergenza.
- *Rapidità*: la velocità con cui l'interruzione dovuta all'attacco può essere affrontata e superata.

Queste caratteristiche riguardano diverse dimensioni dell'infrastruttura da un punto di vista tecnico, organizzativo, sociale ed economico. L'autore utilizza la seguente matrice per esprimere la correlazione tra le sopracitate categorie.

	Technical	Organizational	Social	Economic
Robustness	Building codes and construction procedures for new and retrofitted structures	Emergency operations planning	Social vulnerability and degree of community preparedness	Extent of regional economic diversification
Redundancy	Capacity for technical substitutions and "work-arounds"	Alternate sites for managing disaster operations	Availability of housing options for disaster victims	Ability to substitute and conserve needed inputs
Resourcefulness	Availability of equipment and materials for restoration and repair	Capacity to improvise, innovate, and expand operations	Capacity to address human needs	Business and industry capacity to improvise
Rapidity	System downtime, restoration time	Time between impact and early recovery	Time to restore lifeline services	Time to regain capacity, lost revenue

Tabella 16. Matrice della sicurezza fisica delle infrastrutture critiche (O'Rourke, 2007)

Diversi autori si sono concentrati sulla definizioni di approcci di natura modellistica all'analisi della protezione delle infrastrutture critiche. In (Brown, Carlyle, Salmerón, & Wood, 2006) gli autori propongono un modello di ottimizzazione orientato a rendere le infrastrutture critiche più resistenti agli attacchi, applicando modelli di tipo “attacker-defender” ed altri modelli di ottimizzazione a due e tre livelli. Il concetto chiave di un modello di questo tipo risiede nella minimizzazione dei costi per il “defender” in riferimento a potenziali attacchi. In particolare, il modello che viene proposto dagli autori consta nei seguenti componenti.

- k generico asset che il “defender” intende preservare (e l’attacker vuole attaccare)
- c_k valore del generico asset k (danno subito, nel caso in cui l’asset non venga protetto)
- p_k riduzione del valore del danno subito, nel caso in cui l’asset venga protetto
- x_k variabile binaria: 1 se viene adottata una misura di protezione dell’asset k , 0 altrimenti.
- y_k variabile binaria: 1 se viene attaccato l’asset k , 0 altrimenti.

$$\min_{x \in X} \max_{y \in \{0,1\}^M} \sum_{k=1}^M (c_k + x_k p_k) y_k$$

Dudenhofer, Permann, e Manic (2006) hanno analizzato invece il problema dell’interdipendenza, in termini fisici, logici e geografici, nella sicurezza delle infrastrutture critiche. Gli autori propongono una piattaforma di simulazione denominata CIMS basata sull’approccio di tipo “war game” che consente di modellare e visualizzare le interdipendenze, costruire un modello virtuale utilizzando mappe, foto satellitari ed altre immagini digitali. CIMS fornisce un ambiente visuale e interattivo per osservare gli effetti a cascata e conseguenza di perturbazioni delle infrastrutture. L'utilizzo di sistemi di visualizzazione tuttavia, date le dimensioni e la complessità delle reti rende necessarie ulteriori analisi per identificare le relazioni causa-effetto utilizzando tecniche di Intelligenza Artificiale (AI) per aiutare a raffinare lo spazio di ricerca e di identificare sottogruppi di possibili interazioni. La piattaforma consente di identificare la “sotto-rete” critica (ovvero insieme di asset coinvolti nella relazione causa-effetto), i punti di debolezza della rete e le possibili contromisure.

In (Ezell, 2007) viene invece proposto un modello di valutazione delle vulnerabilità delle infrastrutture, denominato I-VAM (Infrastructure Vulnerability Assessment Model). Il modello di valutazione pone le sue basi sulla teoria matematica del valore multi-attributo (Grabisch, Kojadinovic, & Meyer, 2008). Le componenti di protezione del sistema vengono definite secondo le dimensioni di *deterrenza*, *rilevazione*, *ritardo* e *contromisure* alle quali si è accennato in precedenza. In questo lavoro tali parametri vengono definiti come segue:

- *Deterrenza*: probabilità che una determinata misura venga percepita dal malintenzionato come difficile da superare.
- *Rilevazione*: probabilità che un’azione non autorizzata venga rilevata da un sistema di controllo.
- *Ritardo*: tempo, misurato in minuti, per il quale un elemento del sistema di protezione fisica impedisce al malintenzionato di penetrare o fuoriuscire dall’area protetta.

- *Risposta*: tempo, espresso in minuti, necessario per reagire all'attacco.

Un altro modello di simulazione basato sulla presenza di due agenti "intelligenti" (attaccante e difensore) è illustrato in (Weiss, 2008). Da un punto di vista logico, il difensore è modellato come una serie di sensori (sistemi di protezione attiva) e barriere (sistemi di protezione passiva) accoppiati secondo la logica di limitare e reagire agli attacchi. Viene presentato uno scenario di simulazione relativo alla protezione fisica di un aeroporto. Nel modello, il sensore ha una certa probabilità di rilevare una delle seguenti situazioni:

- Nessun pericolo rilevato.
- Possesso di armi
- Comportamento Sospetto
- Persona di interesse (ad es. Ricercato).

Una volta che un sensore (automatico o persona) ha rilevato una situazione di rischio (in maniera corretta o errata) e quindi l'informazione passa nel "defense action block", è possibile intraprendere una delle seguenti azioni:

- Nessuna azione
- Ripetere la rilevazione (ad es. una persona passa nuovamente attraverso il metal detector dopo aver rimosso alcuni oggetti personali).
- Effettuare un controllo ulteriore (ad es. manuale)
- Bloccare il sospetto

La seguente figura illustra (in blu) le decisioni che un attaccante deve fare quando si confronta con un sensore o barriera. (Si noti che, se un sensore presente nella simulazione, ma non può essere individuato da un aggressore, il blocco attaccante azione viene omesso e l'attaccante non fa decisioni) In primo luogo, un utente malintenzionato deve decidere se avanzare o ritirarsi. Se l'attaccante decide di ritirarsi, può decidere di lasciare la sua arma per ridurre al minimo le sue probabilità di rilevamento. Il livello di sicurezza dell'area circostante influenza questa decisione. E se lascia la sua arma, può decidere di nascondersela e recuperarla per un futuro attacco. Se l'attaccante decide di continuare, ma non ha armi, egli può prendere un'arma qualora sia stata lasciata e nascosta da un attaccante precedente. Se l'attaccante decide di non ritirarsi e ha un arma, poi decide se utilizzare la sua arma: i fattori che incidono su questa decisione comprendono, tra gli altri anche le caratteristiche ambientali e la dimensione della folla, ovvero la numerosità di persone presenti. Se l'attaccante decide di continuare, avanza al sensore successivo o barriera presenti sul suo cammino. Il modello di simulazione consente di tenere in considerazione anche la possibilità di coordinamento tra più attaccanti (ad es. azioni congiunte, oppure trasporto di componenti di un arma che può essere assemblata in seguito) nonché un approccio dinamico che consente di modificare le strategie dell'attaccante basate sulle azioni di difesa intraprese in risposta agli attacchi precedenti.

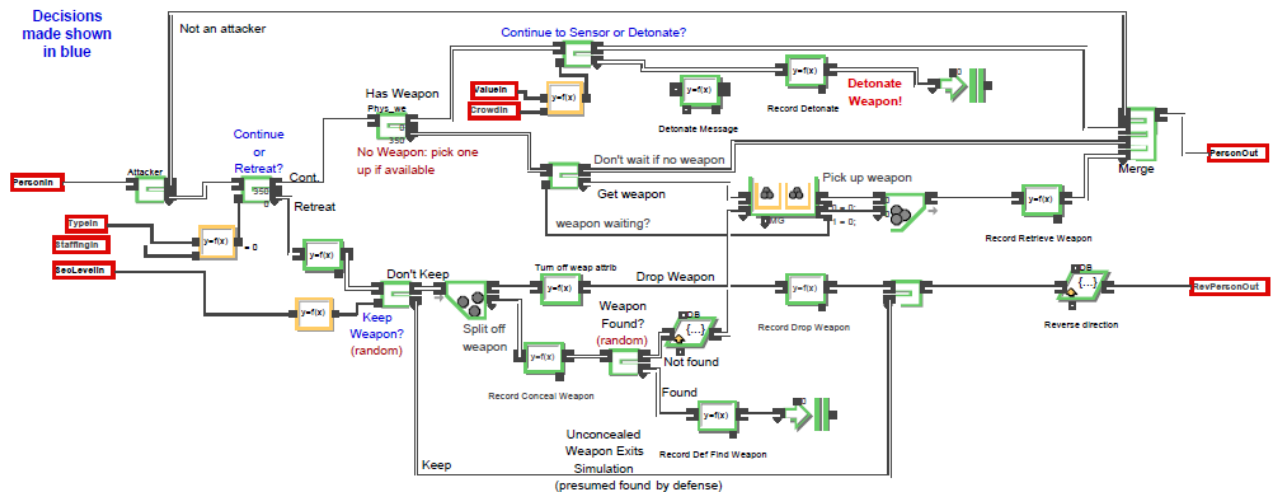


Figura 27. Modello di simulazione dell'attaccante

Nel seguito del documento, l'attenzione si concentrerà sulle misure di natura organizzativa e tecnologica di protezione adottate all'interno delle dipendenze bancarie.

3.2.2 Stato dell'arte sulla sicurezza delle dipendenze bancarie

La sicurezza nelle banche è connessa a problematiche di natura diversa, contemplando e integrando lo studio e l'attuazione di strategie nuove volte a prevenire, fronteggiare e superare eventi di natura dolosa e/o colposa che possono danneggiare le risorse materiali e immateriali, organizzative e umane di cui la banca dispone.

Quello della protezione delle dipendenze bancarie è un problema di notevole interesse. Le dipendenze bancarie infatti possono essere soggette a diverse tipologie di attacco, così come dettagliato nella sezione riguardante i delitti commettabili contro il patrimonio di una dipendenza bancaria. Il problema della sicurezza delle dipendenze bancarie è molto complesso e articolato e si combatte, come nel caso generale delle infrastrutture critiche, sui due fronti della *security* e della *safety*. Nel caso della dipendenza bancaria, il problema della *security* è connesso alla sicurezza fisica del luogo e quindi alla protezione delle transazioni economiche che in esso si svolgono e dell'intero patrimonio bancario. In questo senso il rischio dell'incidente è sia diretto, inteso come danno economico alla specifica dipendenza che si ribalta come danno all'istituto bancario, che indiretto, nel senso di perdita d'immagine aziendale. Per ciò che invece concerne la *safety*, ci si riferisce alla necessità di preservare l'incolumità psico-fisica dei dipendenti e dei clienti della banca presenti in filiale al momento del verificarsi dell'evento criminoso. In particolare, per quanto riguarda la sicurezza dei dipendenti, bisogna tener presente che l'articolo 18 del "Testo unico in materia di salute e sicurezza sul lavoro" (TUSL, 2008) detta una serie di obblighi a carico del datore di lavoro e del dirigente rivolti proprio alla tutela della *safety* dei propri dipendenti rispetto al potenziale incidente.

Negli ultimi anni è accresciuta sempre più la sensibilità nei confronti delle problematiche connesse alla sicurezza delle dipendenze bancarie. Nel 2013 le prefetture e l'ABI (Associazione bancaria italiana) hanno firmato un protocollo di intesa per la prevenzione della criminalità in

banca (ABI, 2013). Con questo protocollo, le banche si impegnano a dotare ciascuna dipendenza di almeno 5 misure di sicurezza tra quelle di seguito elencate:

- Bussola
- metal detector
- rilevatore biometrico
- vigilanza
- videocollegamento/videosorveglianza
- sistema anticamuffamento
- videoregistrazione
- allarme antirapina
- sistema di protezione perimetrale attiva/passiva
- bancone blindato/area blindata ad alta sicurezza
- dispositivo di custodia valori ad apertura ritardata
- dispositivo di erogazione temporizzata del denaro
- gestione centralizzata dei mezzi forti
- sistema di macchiatura delle banconote
- sistema di tracciabilità delle banconote
- formazione anticrimine.

La videoregistrazione è da considerarsi obbligatoria e le banche si impegnano, per le nuove installazioni e per l'adeguamento delle preesistenti, ad utilizzare la tecnologia digitale, che gradualmente sostituirà quella analogica. Il protocollo di intesa pone l'attenzione anche nei confronti delle installazioni ATM, che le banche si impegnano a proteggere con almeno due sistemi di sicurezza tra quelli elencati:

- protezione con impianto di allarme locale e/o remoto connesso a sensori antiscasso/antintrusione
- blindatura del mezzo forte e/o rinforzo dei dispositivi di riferma
- rinforzo aggiuntivo della vetrina ove è installato il Bancomat o dello spazio antistante con difese passive quali putrelle, archetti, dissuasori atti ad impedire l'asportazione del mezzo.
- sensori presenza gas e/o dispositivi per impedire l'esplosione.
- dispositivi per localizzare/rintracciare le banconote rubate e/o dispositivi per rendere inutilizzabili le banconote rubate.
- dispositivi attivi per proteggere il locale contenente il mezzo forte e/o la vetrina ove è installato il mezzo forte.
- dispositivi atti ad impedire l'introduzione di esplosivo o gassoso nel mezzo forte.

Sempre secondo il suddetto protocollo, per aumentare la deterrenza delle misure di sicurezza, le banche sono invitate ad adottare strumenti di comunicazione (vetrofanie o similari), che pubblicizzino, alcune delle soluzioni di sicurezza presenti nelle proprie dipendenze.

Dal punto di vista della ricerca scientifica, il problema della sicurezza delle dipendenze bancarie è stato affrontato tenendo in considerazione differenti prospettive.

Molti autori analizzano la problematica secondo un punto di vista tecnologico. In Bhartilak, Kaur, & Khosla (2014) viene presentata una review sui sistemi di protezione di sorveglianza basati sull'analisi dei movimenti umani. Lo scopo principale di questa indagine è quello di fornire un quadro completo dei più recenti sviluppi in questo settore. Questo articolo seleziona una tassonomia basata su funzionalità, tra cui il rilevamento, il monitoraggio e la comprensione del comportamento all'interno dei sistemi di analisi del movimento umano.

In (Guerette & Clarke, 2003) viene presentato un excursus sulla storia degli ATM e gli approcci alla gestione della sicurezza per questi dispositivi. Successivamente viene effettuato un confronto sulle misure di sicurezza adottate per gli ATM di New York e Los Angeles (facendo distinzione tra le misure richieste per legge e quelle non richieste ma comunemente implementate).

Di seguito si riporta l'elenco di tali misure

MISURA	New York	Los Angeles
ATM all'interno delle porte di sicurezza	X	
Illuminazione aumentata	X	X
Vetri trasparenti	X	
Specchi retrovisori per gli utenti	X	XX
Vegetazione ridotta nei pressi dell'ATM		X
Videocamere di Sorveglianza	X	XX
Messaggi di sicurezza per gli utenti	X	X
Personale di Guardia	X	
Riduzione orario utilizzo in alcune aree		XX

X *Misura richiesta per legge*

XX *Misura facoltativa ma comunemente diffusa*

Tabella 17. Misure per la sicurezza degli ATM (Fonte: Guerette & Clarke, 2003)

Le problematiche relative ai sistemi di protezione di sorveglianza sono stati anche analizzate da Reynolds e Bank (2006). Secondo gli autori, la tecnologia di riconoscimento facciale risulta essere molto utile per risolvere problemi di identificazione ed autenticazione, tuttavia il suo utilizzo in questo senso è limitato al riconoscimento di soggetti precedentemente registrati ed in genere viene utilizzata per il controllo agli accessi del personale autorizzato. Ciò nonostante i nuovi sviluppi tecnologici consentono di utilizzare queste tecnologie per attività volte al controllo ed alla riduzione delle frodi agli sportelli bancari. In questo lavoro si propone un nuovo framework per il riconoscimento facciale integrato in un programma di gestione delle frodi. Tale tecnologia è stata installata in quindici sportelli bancari per testare l'affidabilità nell'identificazione delle persone. In particolare, sono stati utilizzati tre gruppi di persone:

truffatori, rapinatori di banche, e un gruppo di controllo. La sperimentazione ha condotto all'identificazione corretta in un numero elevato di casi, soprattutto nelle filiali bancarie caratterizzate da inquadrature con una buona messa a fuoco, ampio campo visivo e scarsi fenomeni di riflesso ottico.

Sempre in riferimento alle soluzioni architettoniche di protezione, in (Sujith, 2014) viene proposto un framework di rilevazione di "incidenti" all'ATM. In particolare, a partire dall'osservazione di casi reali di "incidenti" agli ATM, si propone un framework per la rilevazione tramite video di eventi criminosi ai danni degli ATM. Nell'articolo vengono identificati i possibili eventi criminosi ai danni degli ATM:

- Furto di numeri di identificazione personale;
- Furto da intercettazione dei dati elettronici;
- Furto da transazioni elettroniche fraudolente;
- Furto di denaro dal bancomat;
- Furto di bancomat;
- Vandalismo ai danni dell'ATM;
- Attacchi fisici.

L'autore propone un'architettura di sistema suddivisa in tre parti. La prima parte comprende una telecamera che cattura le immagini video. La seconda parte è il modulo di rilevamento di oggetti multipli che rilevano l'esistenza di più di una persona nei pressi dell'ATM. Se si rileva più di una persona, allora verrà visualizzato un prompt per l'utente. Se il cliente acconsente alla presenza delle altre persone, le informazioni vengono passate al modulo di riconoscimento delle attività che hanno il compito di analizzare il comportamento umano. Se l'interazione avviene normalmente allora la transazione vera e propria potrà avere luogo altrimenti viene prodotto un allarme nei confronti degli addetti alla sicurezza. Il seguente flowchart illustra il framework logico proposto in questo lavoro.

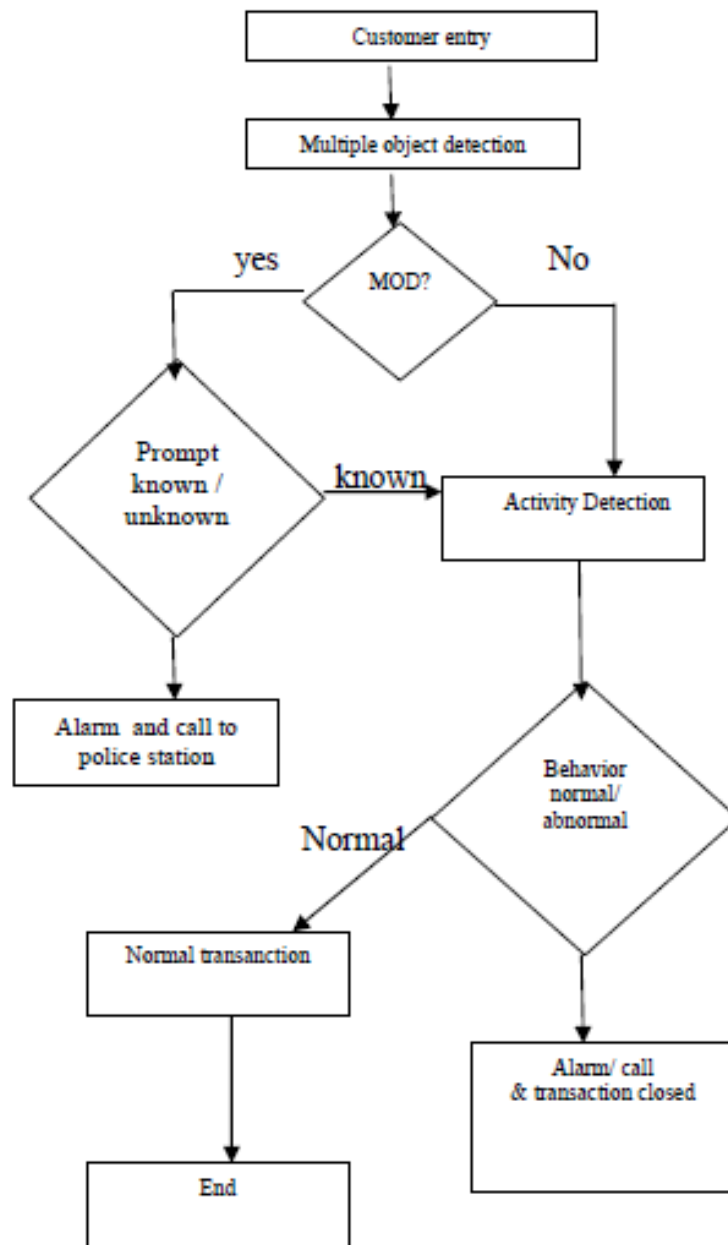


Figura 28. Flusso Logico del sistema proposto (Sujith, 2014)

In (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010) viene proposto un approccio integrato che tiene conto di ricerche nell'ambito della Computer Science e della sociologia al fine di definire nuovi sviluppi nelle tecnologie di sorveglianza. Negli ultimi anni, la sorveglianza e il monitoraggio sono diventati argomenti di maggiore interesse non solo per la ricerca nell'ambito di studio del computer vision, ma anche per molti studiosi nel campo delle scienze sociali e umanistiche. Un approccio congiunto alla ricerca diventa importante quando i sistemi di sorveglianza vengono utilizzati negli spazi pubblici. Questo documento si concentra sulla progettazione e sviluppo di un'applicazione di sorveglianza socio-tecnica in una delle infrastrutture critiche di sicurezza come una banca. Il sistema tecnico presentato è progettato per rilevare eventi specifici come comportamenti anomali o sospetti. Il paper fa riferimento al

contesto Austriaco. Le immagini rilevate dagli impianti di videosorveglianza a circuito chiuso rivestono elevata importanza sia per gli approcci finalizzati alla prevenzione di atti criminali come le rapine in banca ma anche ai fini delle indagini giudiziarie.

Gli esperti di sicurezza della banca e dell'Ufficio Federale di polizia austriaca concordano sull'ipotesi che praticamente tutti i rapinatori effettuano un'esplorazione preliminare della filiale della banca, al fine di ottenere informazioni circa il personale e la struttura spaziale. In aggiunta a ciò, vi è l'ipotesi che i potenziali ladri sceglieranno un'altra filiale della banca, se hanno un'interazione troppo diretta col personale della banca durante il sopralluogo, soprattutto se percepiscono la sensazione di aver destato un particolare sospetto.

Suscita particolare interesse la "capacità" di rilevare un potenziale sospettato da parte del personale della banca, una sorta di "istinto" che potrebbe essere utilizzato per la progettazione di un sistema intelligente che rileva automaticamente comportamenti sospetti. Gli autori hanno effettuato interviste con esperti di sicurezza e membri dello staff, frequentato seminari di formazione speciali di sicurezza dei membri del personale con simulazioni di rapine in banca, e parlato con diversi altri esperti nel campo della sorveglianza, protezione dei dati e dei diritti civili. È importante riuscire a catturare questa "conoscenza tacita" e trasformarla in conoscenza esplicita.

Innanzitutto è stato necessario pervenire all'identificazione dei comportamenti ritenuti "sospetti", quali ad esempio sostare presso il foyer banca senza utilizzare l'ATM, senza interagire con un membro del personale per un periodo di tempo prolungato, oppure permanenze insolitamente prolungati nei paraggi dell'ATM. Un ulteriore passo è stato effettuato analizzando il comportamento "normale" delle persone che soggiornano in una filiale della banca per conoscere il comportamento "solito" dei clienti delle banche. A questo scopo è stato adottato il metodo di osservazione non partecipante combinata con la video-analisi utilizzata nella "ricerca sociale". L'osservazione è volta a descrivere e analizzare lo spazio sociale, le azioni, le interazioni tra gli esseri umani e interattività tra l'uomo e le macchine in una filiale della banca. Nel giro di quattro sessioni di osservazione (due non partecipanti direttamente in due diversi sportelli bancari, e due sulla base di registrazioni video in un'altra filiale) gli autori hanno ottenuto un campione di 236 persone. Queste tre dipendenze bancarie hanno caratteristiche abbastanza in linea con gli standard austriaci, con foyer di circa 20 - 30 metri quadrati. I foyer sono dotati di 2 bancomat, stampanti di dichiarazioni per le banche, macchine per deposito contanti e bonifici bancari. Le macchine sono accessibili anche al di fuori degli orari di apertura. Per aprire la porta al di fuori dell'orario di apertura si deve inserire una carta bancomat. Naturalmente non è rara la possibilità di entrare seguendo un altro cliente. Durante l'orario di apertura, di solito un membro del personale è al servizio al banco. Le osservazioni delle filiali sono state condotte nel luglio 2009. La maggior parte dei clienti osservati è entrata nella filiale della banca da sola (86,4%). Dieci persone sono entrate indossando occhiali da sole e 35 persone indossando un copricapo (cappello, berretto, berretto, o velo). Le persone rimangono in media 3 min. 53 sec. All'interno di una filiale della banca,

mentre il tempo medio di persone che soggiornano solo nel foyer è 3 min. 08 sec. Ci sono state 38 su 236 persone (16%) che hanno soggiornato più di 5 minuti e 10 su 236 (4%) che hanno sostato più di 10 minuti. La percentuale outlier relativa di tempo di presenza in banca dei clienti è abbastanza alto, tale da poter concludere che una permanenza più lunga, presa da sola non può essere considerata come comportamento insolito o sospetto. In realtà, tutti i periodi più lunghi di tempo di presenza possono essere spiegati e appaiono come un comportamento usuale: Molti clienti della banca hanno dovuto aspettare in coda di fronte all'ATM o allo sportello bancario.

Un dato interessante riguarda le persone che sostano presso il foyer della banca senza l'utilizzo di una macchina (ad esempio, bancomat) o senza interagire con un membro del personale. 17 su 236 (7%) delle persone che entrano ed escono da una filiale della banca non ha fatto alcuna attività abituale: quasi il 50% di questi aveva accompagnato un'altra persona a svolgere un'attività abituale. L'altra metà è stata all'interno della hall bancaria per un brevissimo periodo di tempo. La maggior parte di questi è entrata giusto un attimo all'interno per notare molte persone in piedi in coda. Una conclusione principale dell'osservazione è che il comportamento usuale nel foyer della banca è molto vario. Esiste una vasta gamma di comportamenti, rendendo il rilevamento del comportamento insolito o sospetto molto difficile. Inoltre è stato visto che molti rapinatori di banche che esplorano una filiale della banca si comportano come clientela ordinaria o addirittura sono clienti delle banche. Alla luce di queste considerazioni può essere interessante realizzare un sistema di videosorveglianza intelligente capace di rilevare comportamenti e traiettorie anomale, quali:

- Vagare nella filiale senza utilizzare una macchina (ad esempio, l'ATM) o contattare un membro del personale per un periodo di tempo prolungato
- Interagire con l'ATM per un periodo di tempo insolito
- Presenza di più persone contemporaneamente nei pressi di un ATM
- Movimenti repentini nei pressi di un ATM (ad es. scasso).
- Persone che si spostano velocemente o in giro.

Al fine di analizzare le traiettorie per il comportamento di interesse, l'atrio della banca è stato suddiviso in diverse aree, in particolare zona periferica, zona bancone, zona tavolo; la restante superficie è stata definita come area aperta. Se una persona è in piedi all'interno di una zona designata, la persona è contrassegnata come operativo. Le persone nella zona aperta possono essere in fila, in piedi o in movimento. Per determinare se una persona è in coda viene definito un raggio di azione. Una persona è contrassegnata come "in coda", se un'altra persona all'interno di questo raggio di azione è a sua volta in coda o si trova allo sportello (o utilizza l'ATM).

Nella figura seguente vengono illustrate due traiettorie campione tracciate sulla planimetria della filiale. La linea verde continua mostra una traiettoria normale estratta durante il normale funzionamento del sistema. La linea rossa tratteggiata rappresenta una traiettoria di un comportamento di potenziale interesse, dal momento che non è stata rilevata alcuna

interazione con un dispositivo. In questo caso il dato è acquisito in una sessione speciale in cui il comportamento sospetto è stato nuovamente validato sotto la supervisione dell'esperto di sicurezza della banca.

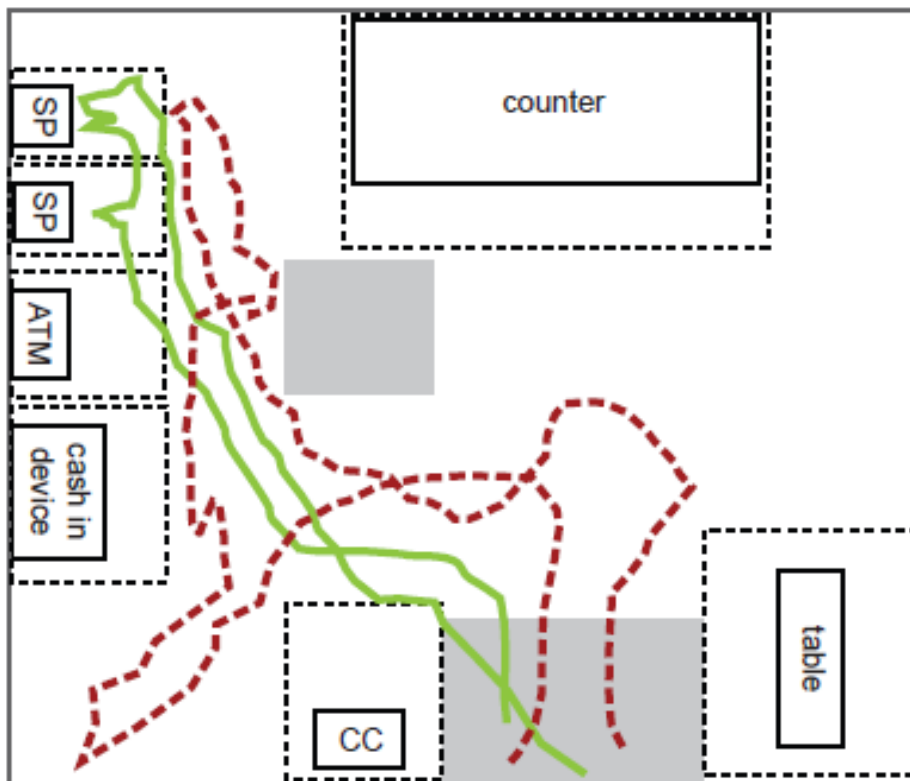


Figura 29. Esempi di traiettorie plottate sulla planimetria della filiale (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010)

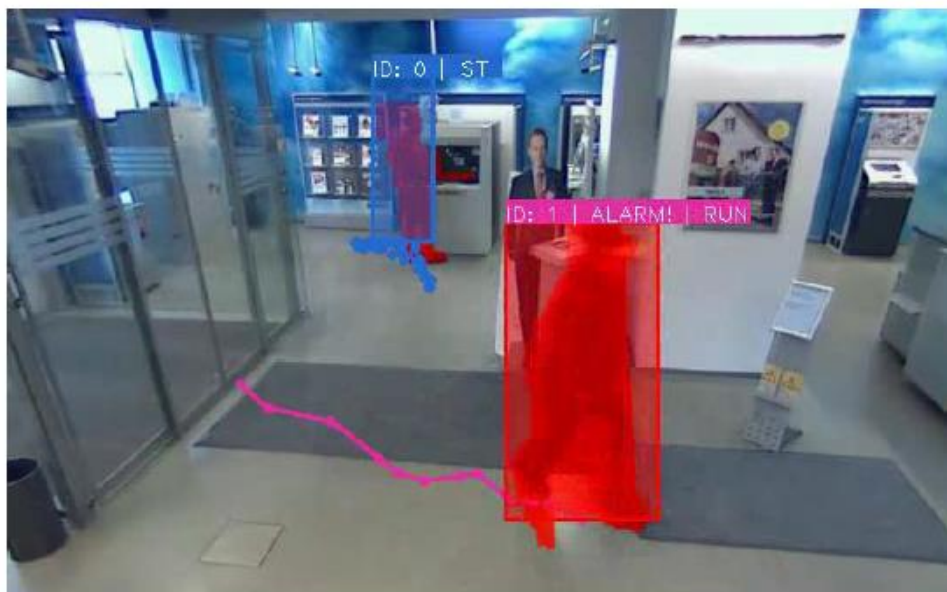


Figura 30. Esempio di scenario di rischio rilevato. Un soggetto si muove velocemente (corre) all'interno della dipendenza (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010)

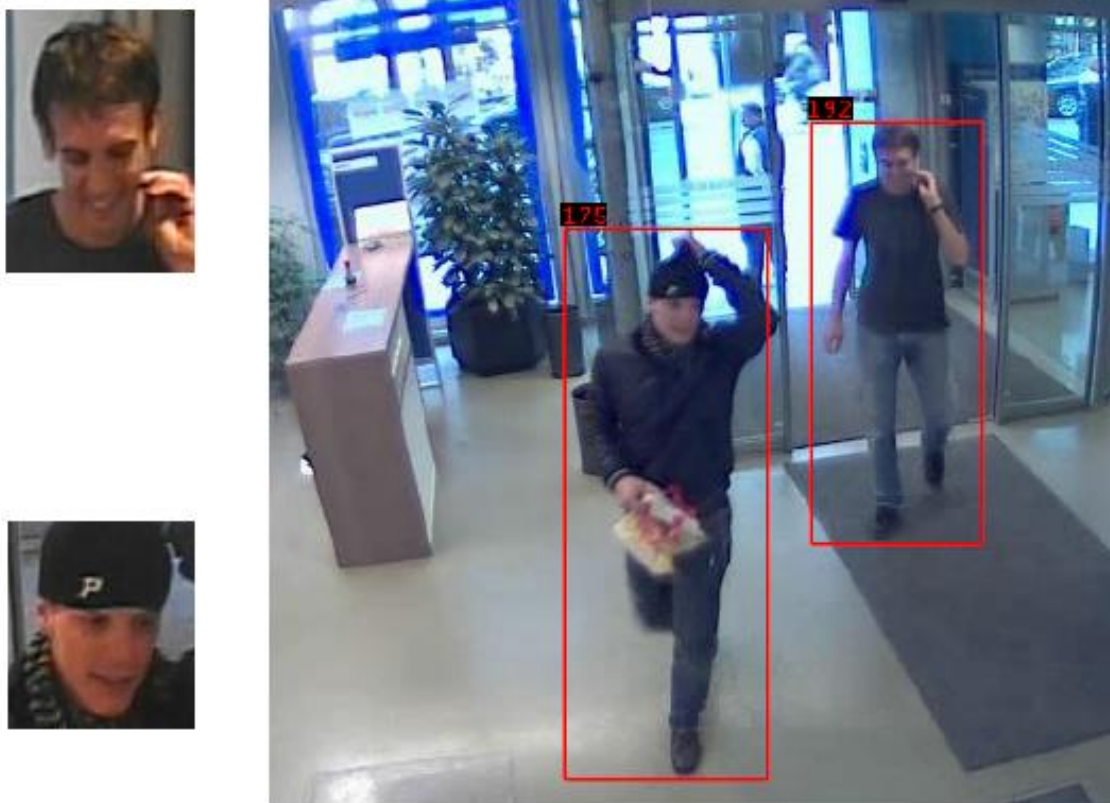


Figura 31. Esempio di rilevazione di soggetti con stima dell'altezza e dettaglio del viso (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010)

Per quanto riguarda l'analisi dei comportamenti attraverso sistemi di videosorveglianza a circuito chiuso, un interessante contributo è presentato in (De Gregorio, 2011). Questo articolo riassume i risultati di un'analisi effettuata a valle della visione di 23 filmati di videosorveglianza relativi a casi di rapine all'interno delle dipendenze bancarie. I filmati sono stati visionati al fine di identificare sequenze tipiche che siano comuni in queste situazioni. Lo studio mirava a stabilire se le azioni viste nei film seguono alcuni modelli di comportamento al fine di definire modelli teorici che descrivono tali azioni. I risultati mostrano che gli attori sociali seguono modelli comportamentali specifici in ambienti diversi. All'interno del lavoro viene analizzato inizialmente il fenomeno delle rapine in Italia e in Europa (DATI OSSIF). Dopo aver delineato la recente tendenza delle rapine, viene data una spiegazione criminologica del fenomeno. La Rapina è un atto complesso, una situazione che irrompe inaspettatamente nel contesto lavorativo dell'impiegato di banca. Rapinatore e vittima hanno ruoli molto definiti. Il rapinatore dirige il gioco, impartendo ordini che devono essere rispettati dalle persone presenti sulla scena (sia clienti che dipendenti). Questi tipi di interazioni implicano che:

- (1) tutti i partecipanti hanno aspettative reciproche sui comportamenti e sull'esito delle azioni;
- (2) interagiscono con le norme e i regolamenti che la banca impone ai suoi dipendenti;
- (3) interagiscono con le variabili strutturali dei sistemi di sicurezza;

(4) sia ladro che vittima sono in uno stato altamente emotivo.

Secondo l'autore, i rapinatori di banche sono in genere altamente 'professionalizzati': pianificano e organizzano la rapina, selezionando attentamente i loro complici ai quali assegnano compiti specifici, hanno familiarità con i sistemi di sicurezza e con le procedure bancarie; vogliono rubare quanto più denaro possibile nel minor tempo possibile. Incidenti imprevisti nella sequenza rapina possono aumentare il livello e la gravità della violenza utilizzata nell'azione. Gli eventi di violenza possono essere causati dal comportamento dei presenti sulla scena o dalla scarsa conoscenza del ladro di nuovi sistemi di sicurezza adottati dalla banca. Un maggior livello di violenza potrebbe essere attivato, per esempio, se è necessario un tempo maggiore per ottenere il denaro. Sulla base di queste premesse, l'autore ha condotto la ricerca analizzando le dinamiche di rapine in una zona coperta da videosorveglianza con tre obiettivi principali:

(1) Dal punto di vista criminologico, si sono volute studiare a fondo le principali tappe di una rapina, la gestione del flusso di comunicazione (in particolare la comunicazione non verbale), e gli incidenti imprevisti.

(2) È stata data particolare attenzione alla possibilità di identificare un "modus operandi" tipico per le azioni di rapina. Va chiarito che l'espressione 'modus operandi' in criminologia si riferisce specificamente ai reati violenti e indica lo stile di comportamento dei criminali seriali. In questo studio, tuttavia, il termine è usato nel suo senso più ampio, per indicare la dinamica dello stesso tipo di reati perpetrati da diversi criminali.

(3) Infine, l'autore ha cercato di individuare gli indicatori comportamentali che possono essere utilizzati per impedire una rapina e che dovrebbero far parte della formazione di impiegati di banca, le forze di polizia e le guardie di sicurezza.

Di seguito si riportano alcuni pattern comportamentali individuati nella ricerca.

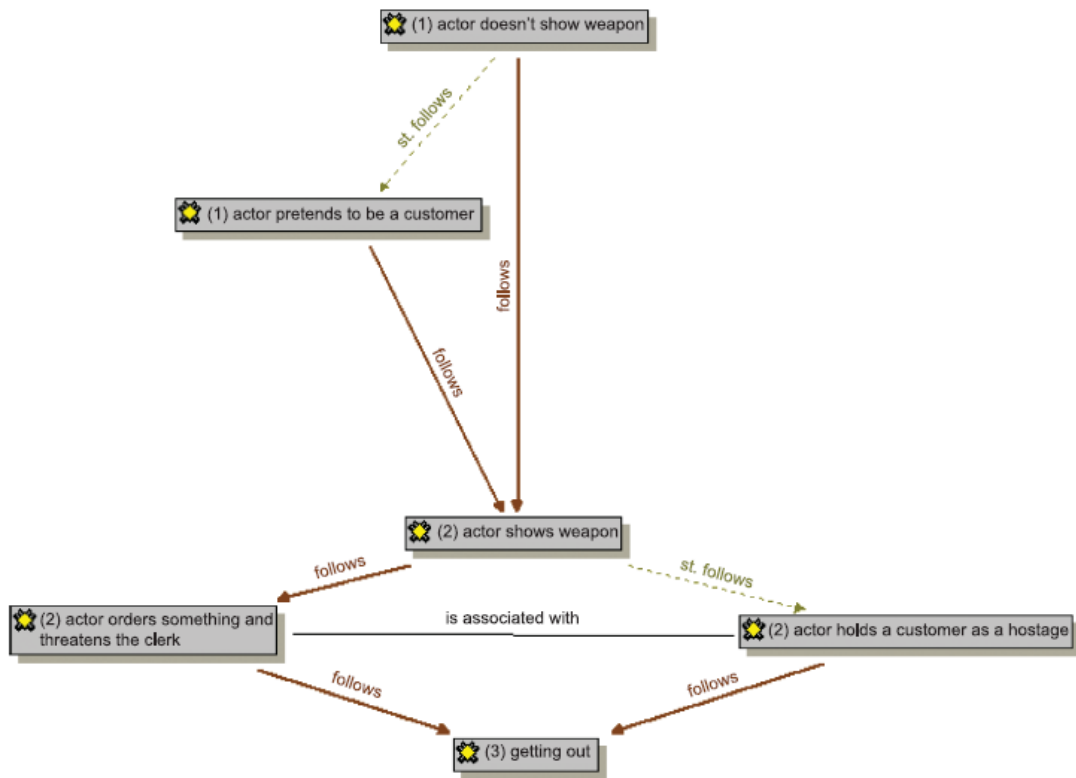


Figura 32. Pattern di una rapina commessa da un solo rapinatore (De Gregorio, 2011)

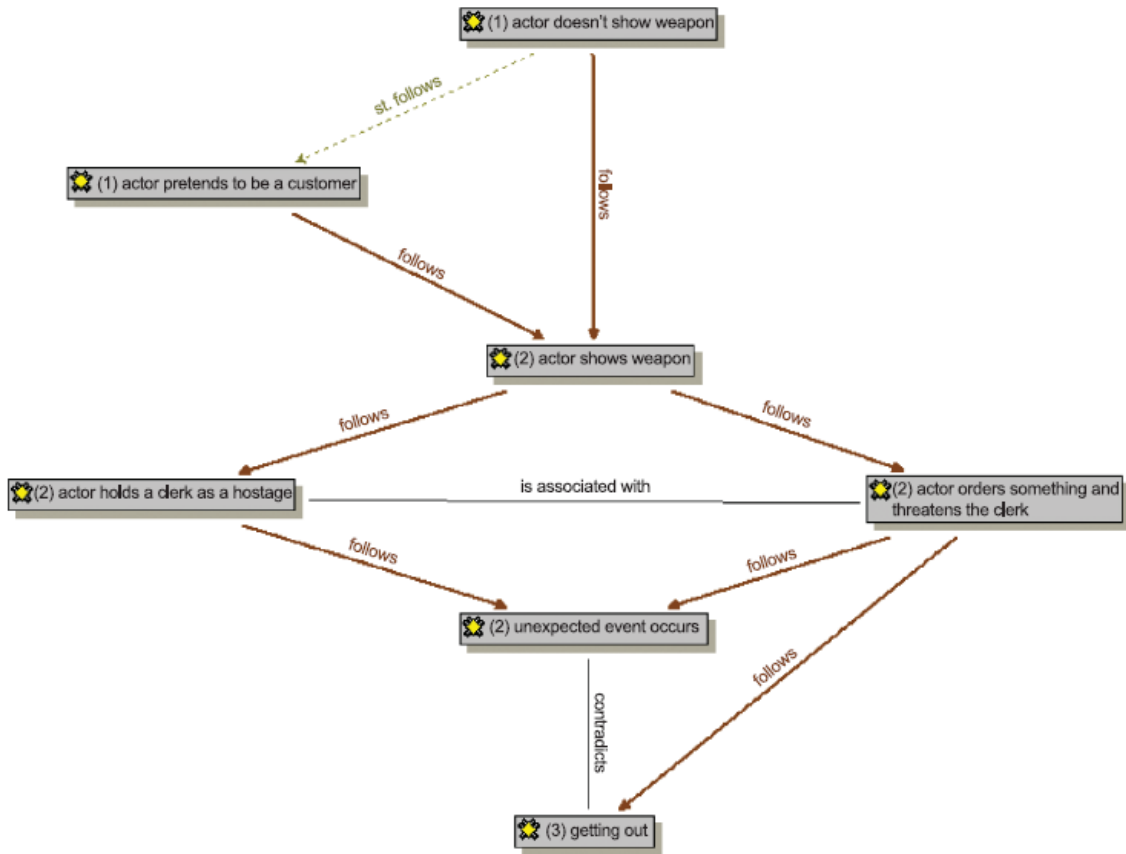


Figura 33. Pattern di una rapina commessa da un solo rapinatore quando si verifica un incidente imprevisto (De Gregorio, 2011)

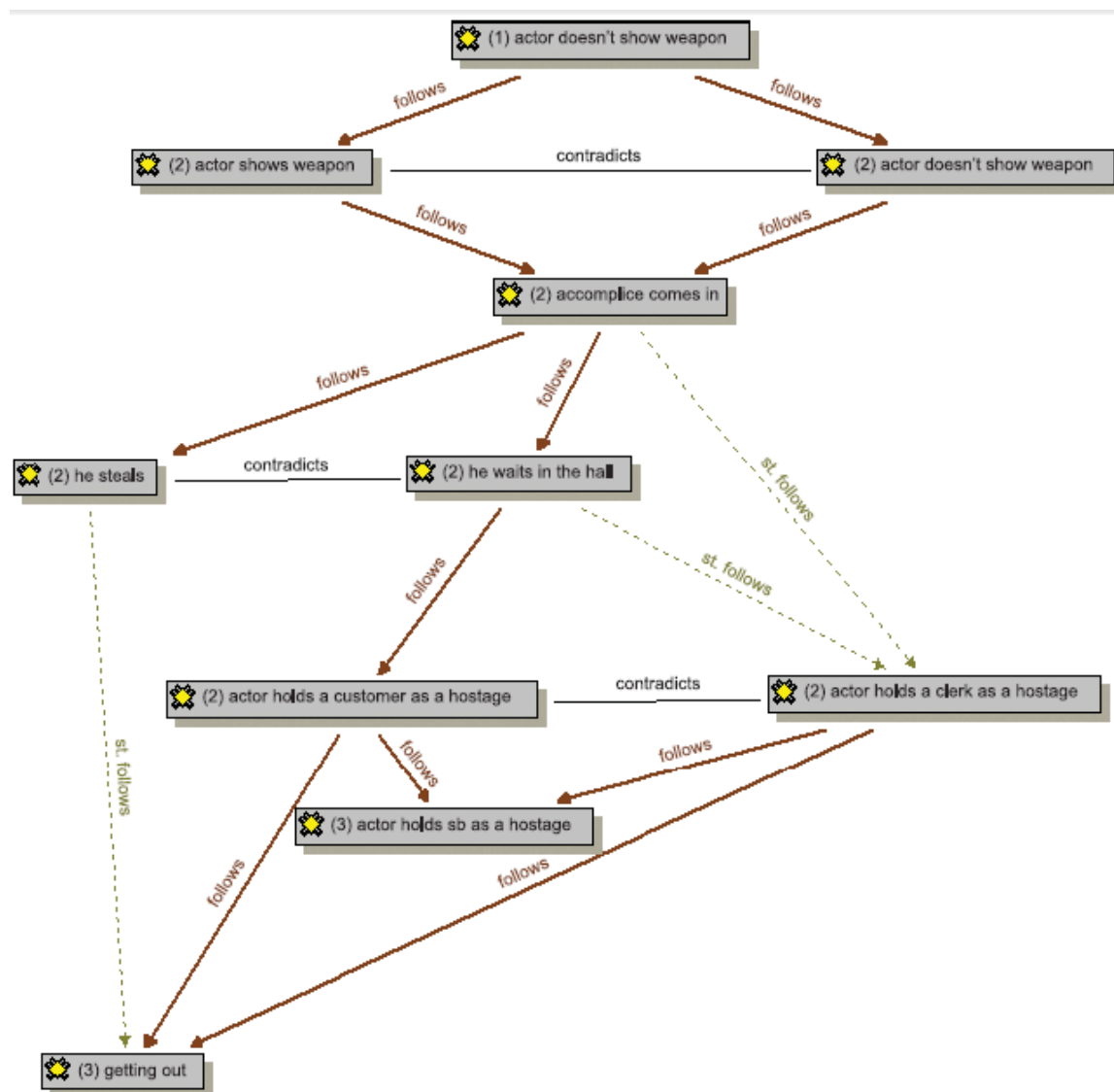


Figura 34. Pattern di una rapina commessa da una coppia di rapinatori (De Gregorio, 2011)

Negli ultimi anni è evidente la crescente attenzione nei confronti delle problematiche di sicurezza connesse agli ATM. In (Braz, Seffah, & M'Raihi, 2007) viene affrontata la problematica relativa alla definizione di un tradeoff nella progettazione di sistemi ATM tenendo in considerazione aspetti legati sia all'usabilità che alla sicurezza. Trovare il giusto compromesso tra la sicurezza e l'usabilità di un sistema non è mai un tentativo facile. In questo paper viene introdotto un modello basato sul paradigma dello "usability inspection method". Questo metodo, chiamato Security Usability Symmetry (SUS) sfrutta gli approcci teorici relativi alle macchine automatiche ed introduce il concetto di Multifunction Teller Machine (MTM). Viene

dimostrato, tramite un caso di studio applicato al Credit Lyonnaise (Banca Francese), come utilizzare questo modello durante la progettazione di sistemi interattivi utilizzabili e sicuri. Sempre in riferimento alla sicurezza degli ATM, un'architettura tecnologica innovativa viene presentata in (Jaiswal & Bartere, 2014). L'obiettivo principale di questo lavoro è quello di proporre un sistema, che viene utilizzato per applicazioni di sicurezza ATM. L'approccio proposto richiede che l'istituto bancario raccolga le impronte digitali dei clienti e il numero di cellulare al momento dell'apertura del conto. Quando il cliente immette la propria carta all'interno dell'ATM deve posizionare il dito sul modulo finger print, per poi ottenere automaticamente un codice a 4 cifre generato ogni volta attraverso un modem GSM collegato al microcontrollore ed inviato come messaggio al cellulare del cliente. Il codice deve essere inserito dal cliente premendo i tasti sul touch screen, e solo dopo egli sarà in grado di svolgere ulteriori azioni.

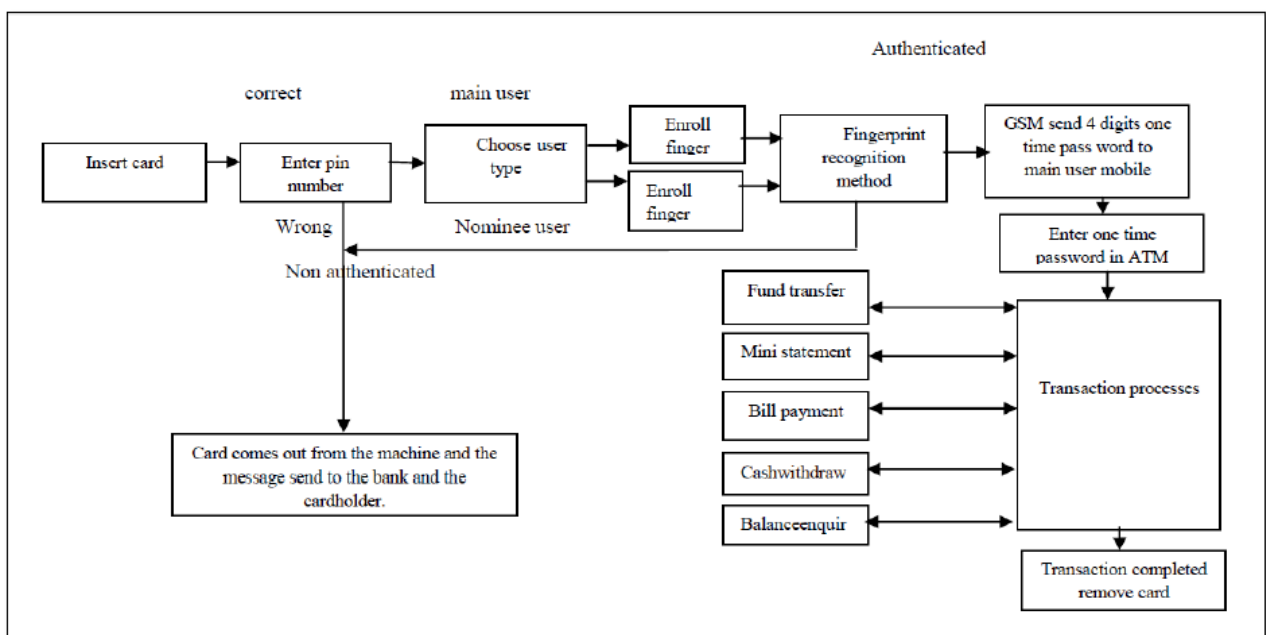


Figura 35. Architettura per la sicurezza degli ATM proposta in (Jaiswal & Bartere, 2014)

Molti autori si concentrano sull'analisi dei dati storici relativi agli eventi criminosi ai danni delle dipendenze bancarie. In (Borzycki, 2006) viene effettuata un'analisi delle serie storiche delle rapine in banca in Australia, in termini di numerosità degli eventi, utilizzo di armi, utilizzo di violenza (vittime, feriti, ostaggi), durata, numero di malviventi. Viene fatta un'analisi descrittiva delle serie storiche relative alle rapine in banca in Australia, a partire da dati aggregati forniti dall'ABA - Australian Bankers' Association. I risultati della ricerca suggeriscono che il fenomeno delle rapine nelle banche australiane è in declino e che le caratteristiche dei malviventi che commettono tale tipologia di reato sono cambiate negli ultimi due decenni: le rapine sono in genere meno programmate (meno progettate), con un impiego meno massiccio di armi, ed utilizzando approcci più semplici al fine di intimidire il personale della banca. Un dato importante è che dal raffronto con gli anni '80 le rapine in banca sono meno proficue. La ricerca

ha l'ambizione di migliorare gli approcci alla protezione dagli eventi criminosi in questo settore, tenendo conto di come sono cambiati i comportamenti dei malviventi che commettono tale tipologia di reato.

Le Rapine in banche australiane sembrano essere in declino perché è cambiata la tipologia di soggetto che compie il reato. In particolare, questi ladri nuovo stile:

- tendono ad operare in bande;
- hanno meno probabilità di essere armati;
- sembrano impegnarsi di meno in attività di pianificazione (ad esempio, travestimenti).
- registrano un maggiore numero di vittime

In (Weisel, 2007) viene analizzato il fenomeno delle rapine in banca negli Stati Uniti. Dopo aver introdotto il problema delle rapine in banca, viene effettuata una analisi sui trends relativi a tale fenomeno. E' interessante evidenziare come negli USA il fenomeno delle rapine in banca è in crescita (in controtendenza con quello che si rileva ad esempio in Europa ed Australia).

Successivamente l'analisi si sposta sui fattori che contribuiscono alle rapine in banca, ovvero:

- **INCREMENTO DELLE OPPORTUNITÀ:** Il numero di filiali è sempre più elevato. Il retail banking è altamente competitivo, e il consolidamento negli ultimi decenni, attraverso fusioni e acquisizioni ha portato ad una espansione in nuovi mercati. Molte filiali vengono aperte anche all'interno di supermercati e centri commerciali. Sebbene gli sportelli bancari nei supermercati potrebbero sembrare particolarmente vulnerabili alla rapina, la via di fuga è difficile da percorrere a causa di carrelli della spesa, cartelloni, passeggini e numerosi clienti.
- **ALTA REDDITIVITÀ:** Anche se molte banche limitano sia la quantità di denaro in cassa, sia il controllo di accesso al denaro per il personale della filiale, le banche, tuttavia, restano una fonte di denaro facile per i ladri. Negli Stati Uniti, le rapine in banca rappresentano il 10% del totale delle rapine, ma il bottino delle rapine in banca ammonta a circa il 60% rispetto al bottino totale delle rapine.
- **RISCHIO NON ELEVATO PER I RAPINATORI:** Per un ladro, ci sono due ragioni principali per cui gli sportelli bancari possono essere considerati prevedibili e obiettivi relativamente a basso rischio. Innanzitutto le filiali hanno un layout standard e quindi le azioni da compiere sono più facilmente prevedibili. Sebbene tale uniformità possa aiutare i clienti a sentirsi a proprio agio in qualsiasi dipendenza bancaria, offre anche grande prevedibilità per i ladri. Inoltre, i dipendenti della banca sono disarmati. In particolare, nel corso di una rapina, le pratiche bancarie sono altamente standardizzate, e di conseguenza, i ladri sanno che possono contare su un comportamento standard dei dipendenti. I cassieri in genere non oppongono resistenza nello svuotare le casse in seguito alla semplice dichiarazione di rapina, specie se viene minacciato con un'arma. Ciò non avviene in altre attività commerciali, magari gestite direttamente dal titolare il cui obiettivo è salvaguardare il proprio patrimonio. (Nota: Da tenere in considerazione anche la normativa sull'utilizzo delle armi negli USA, spesso vendute anche nei

supermercati). L'obiettivo primario della banca è quello di proteggere la safety dei propri dipendenti e clienti, riducendo il rischio di violenza. Pertanto, il rischio di "resistenza" che un ladro incontrerà è estremamente basso. Questa è anche uno delle ragioni che rendono le rapine veloci ed efficienti: più di due terzi delle rapine in banca sono state completate in tre minuti o meno. In molte rapine, l'evento viene gestito in modo talmente discreto che altri clienti e anche altri dipendenti non sono neanche a conoscenza che un crimine è avvenuto fino a dopo che il rapinatore ha lasciato i locali.

- **PROCEDURE DI SICUREZZA DELLE BANCHE:** Le banche hanno rigide procedure di sicurezza e di solito sono considerate le più sicure di tutte le imprese commerciali. Le pratiche di sicurezza bancaria sono altamente standardizzate, e la sicurezza elettronica è una misura comunemente adottata, anche tra le filiali derubate. Il 98% delle filiali derubate fino al 2000 aveva sia le telecamere di sicurezza che i sistemi di allarme. Tuttavia, la diffusa adozione di pratiche di sicurezza della banca ha ridotto le perdite medie di rapina e potrebbe aver ridotto la violenza in rapine. Molti studi dimostrano che le filiali che hanno subito una rapina, hanno una maggiore probabilità di subirne nuovamente altre rispetto a quelle che non sono mai state derubate (fenomeno della repeat victimisation). Attualmente i sistemi di sorveglianza aumentano la probabilità che un colpevole venga arrestato, tuttavia si sottolinea la necessità di adottare strategie di sicurezza più proattive che sono progettati per contrastare rapine prima che si verifichino.

La ricerca infine analizza le caratteristiche delle rapine in banca facendo una distinzione tra rapine effettuate da professionisti e rapinatori improvvisati sulla base dei seguenti parametri:

- Caratteristiche del Rapinatore
- Durata dell'evento
- Violenza
- Successo
- Selezione dell'obiettivo
- Modalità di fuga

	Professional	Amateur
Offenders	<ul style="list-style-type: none"> • Multiple offenders with division of labor • Shows evidence of planning • May be older • Prior bank robbery convictions • Travels further to rob banks 	<ul style="list-style-type: none"> • Solitary offender • Drug or alcohol use likely • No prior bank crime • Lives near bank target
Violence	<ul style="list-style-type: none"> • Aggressive takeover, with loud verbal demands • Visible weapons, especially guns • Intimidation, physical or verbal threats 	<ul style="list-style-type: none"> • Note passed to teller or simple verbal demand • Waits in line • No weapon
Defeat Security	<ul style="list-style-type: none"> • Uses a disguise • Disables or obscures surveillance cameras • Demands that dye packs be left out, alarms not be activated, or police not be called 	
Robbery Success	<ul style="list-style-type: none"> • Hits multiple teller windows • Larger amounts stolen • Lower percentage of money recovered • More successful robberies • Fewer cases directly cleared • Longer time from offense to case clearance 	<ul style="list-style-type: none"> • Single teller window victimized • Lower amounts stolen • Higher percentage of money recovered • More failed robberies • Shorter time from offense to case clearance, including more same-day arrests • Direct case clearance more likely
Robbery Timing	<ul style="list-style-type: none"> • Targets banks when few customers are present, such as at opening time • Targets banks early in the week 	<ul style="list-style-type: none"> • Targets banks when numerous customers are present, such as around midday • Targets banks near closing or on Friday
Target Selection	<ul style="list-style-type: none"> • Previous robbery • Busy road near intersection • Multidirectional traffic • Corner locations, multiple vehicle exits 	<ul style="list-style-type: none"> • Previous robbery • Heavy pedestrian traffic or adjacent to dense multifamily residences • Parcels without barriers • Parcels with egress obscured
Getaway	<ul style="list-style-type: none"> • Via car 	<ul style="list-style-type: none"> • On foot or bicycle

Tabella 18. Differenze tra professionisti e rapinatori improvvisati secondo (Weisel, 2007)

Un altro studio (Matthews, Pease, & Pease, 2001) esamina tutte le rapine in banca (registrate dalla Metropolitan Police del Regno Unito), compiute e tentate in Inghilterra su un orizzonte temporale di tre anni. Questo lavoro cerca di analizzare le ragioni del repeat victimisation. In particolare il lavoro mostra come sia elevato il tasso di ripetizione di questi eventi criminosi contro le stesse dipendenze bancaria: tra le filiali che hanno subito almeno una rapina nel periodo di osservazione, si registra una media di 1,54 rapine, con picchi fino a sei. Si evidenzia nella ricerca come in genere le rapine successive alla stessa dipendenza bancaria abbiano un tasso di successo inferiore, presumibilmente a causa di miglioramenti nei sistemi di sicurezza o formazione del personale in seguito all'evento precedente. La rapina "ripetuta" tende ad accadere poco dopo il furto precedente. In totale, ci sono stati 734 furti (compresi i tentativi)

distribuiti tra 508 filiali. Circa il 35% degli sportelli ha subito più di una rapina, con quarantacinque filiali che ne hanno subito 3, quattordici ne hanno subite 4, sei filiali con 5 rapine ed infine una filiale con ben 6 rapine all'attivo. Prestando attenzione alle "prime" rapine delle banche che non sono state derubate di nuovo, il 38% non hanno avuto successo in quanto non è stato sottratto denaro. Questo dato contrasta con il 27% delle prime rapine di coloro che sono stati derubati di nuovo. La differenza è statisticamente affidabile (Chi-quadro = 6.15 p <.025). Per quanto riguarda le filiali che hanno subito un furto, si registra in media un importo inferiore tra quelle che non hanno subito ripetizioni (una media di £ 2.200) rispetto alla prima rapina di quelli che hanno sofferto ripetizioni (una media di £ 2.800). (z = 2.67, p <.01). Presi insieme, questi risultati suggeriscono che una seconda rapina è più spesso una risposta al successo della prima piuttosto che una risposta ad un attacco che era stato precedentemente vanificato. La domanda di ricerca successiva riguarda il successo della prima e delle rapine successive. Il 40% di seconde rapine non hanno avuto successo, contro il 27% delle prime rapine delle stesse banche. I dati mostrano anche che le banche che hanno subito una prima rapina senza sottrazione di denaro, tendono a non subire sottrazione di denaro anche in quella successiva: quando non sono stati sottratti soldi nel primo caso, si registra un 70% di situazioni senza sottrazione anche nell'evento successivo; al contrario, quando il denaro è stata preso in occasione della prima rapina, nel 71% dei casi di denaro è stato perso anche al secondo (Chi-quadro = 24.38, p <.0001).

Per quanto concerne l'Italia, il fenomeno del repeat victimization relativo ad eventi di rapine in banca viene affrontato anche da Dugato (2014). Questo lavoro analizza il database dell'OSSIF, secondo il quale si sono verificate 15744 rapine in Italia tra il 2005 ed il 2010. L'analisi evidenzia un decremento del numero delle rapine in Italia di circa il 49% rispetto al 2007. La riduzione delle rapine in banca si contrappone al crescere dei furti ai danni di ATM e rapine ai danni di altri esercizi commerciali. Il fattore che sembra caratterizzare questo tipo di crimine è l'incidenza della vittimizzazione ripetuta (repeat victimization). Il 32% di tutti i 34.722 sportelli bancari in esame ha subito almeno una rapina nei 6 anni considerati, tuttavia quasi la metà dei furti registrati (48% del totale) ha riguardato un attacco alla stessa filiale. Viene effettuata un'analisi quantitativa degli eventi criminosi nell'area della città di Milano, utilizzando la "Getis-Ord G*" una tecnica statistica utilizzata per analizzare la distribuzione spaziale degli eventi in un dato spazio. Questo metodo è utile non solo per identificare l'esistenza di concentrazioni inusuali di reati, ma anche per determinare quanto questi pattern sono significativamente differenti dalla distribuzione generale del fenomeno in tutta l'area. In particolare, questo studio divide la città di Milano con una griglia quadrata regolare (500 × 500 m) e assegna ad ogni cella il numero di rapine e di sportelli situati nella zona corrispondente. Il metodo Getis-Ord G * applica la definizione dei punteggi Z per le distribuzioni di criminalità e obiettivi.

Mastrobuoni (2014) invece effettua un'indagine sulle rapine in banca, prendendo in considerazione i dati forniti dall'European Banking Federation e dall'OSSIF. L'autore presenta inoltre un approccio al calcolo della "funzione di utilità" per i rapinatori. I Rapinatori di banche

affrontano un trade-off: più a lungo rimangono all'interno della banca più soldi sono in grado di raccogliere, ma al contempo aumenta il rischio di essere fermati. La funzione di utilità del criminale $V(t)$ è quindi una funzione della durata della rapina in banca. Altri fattori che incidono sono la ricchezza iniziale del criminale (W), l'avversione al rischio (r), così come il trade-off tra il bottino e il rischio, che dipende dalla sua abilità, nonché dalle caratteristiche della filiale scelta, entrambi i quali sono predeterminati una volta che inizia la rapina.

Per quanto concerne infine gli approcci computazionali alla definizione del rischio sicurezza nelle dipendenze bancarie, vengono proposti diversi approcci. In (Ronsivalle G. B., 2007) viene presentata una piattaforma di simulazione delle rapine in banca. Il modello si basa su una rete Bayesiana ed è finalizzato a calcolare il rischio totale. Vengono definite variabili che impattano sul rischio nel corso di una rapina e le fasi di una rapina in banca. La simulazione propone tre casi che rappresentano tre tipi di rapine, ciascuna caratterizzata da diverse sequenze ed elementi ed un diverso numero di criminali. L'utente ha varie opzioni di risposta e queste non sono mai completamente giuste o sbagliate. Esse invece rappresentano diversi livelli di priorità che il lavoratore può scegliere. Ogni volta che l'utente effettua una decisione, il sistema subisce un "disturbo locale" che comporta una revisione globale della rete e la sua riorganizzazione in merito allo stato di equilibrio.

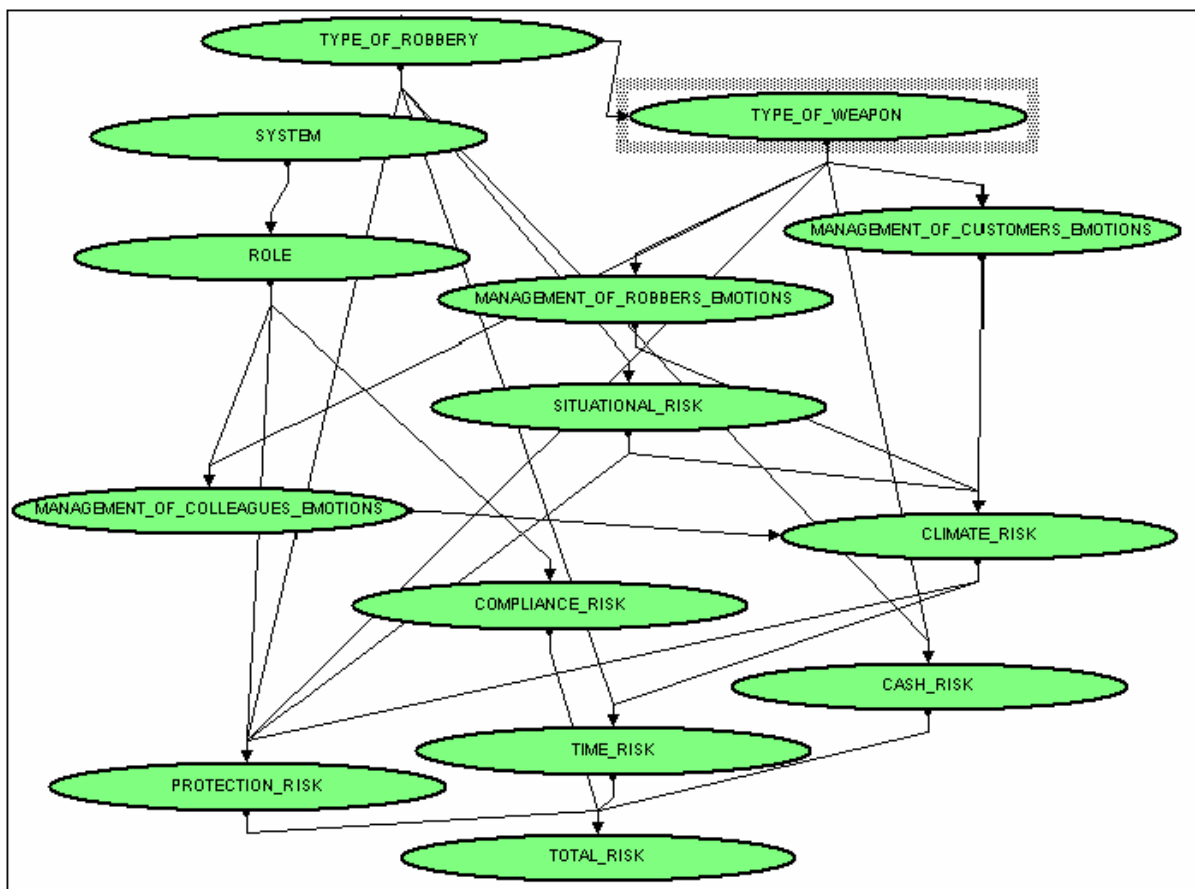


Figura 36. Rete Bayesiana relativa alla simulazione della Rapina in Banca (Ronsivalle G. B., 2007)

Come nella situazione reale in cui le decisioni devono essere prese entro un breve lasso di tempo, nella simulazione gli utenti hanno un tempo limitato (10 secondi) in cui fare le loro scelte. Se l'utente non riesce a decidere entro 10 secondi, il sistema assegna a caso una delle opzioni presentate, mentre non ci sono limiti di tempo per le risposte da fornire alle forze dell'ordine o agli agenti di sorveglianza. L'alterazione dello stato della rete è visibile attraverso la presenza dell'icona rischio globale. L'icona "rischio globale" identifica il risultato della rapina in termini di gestione complessiva da parte dell'utente, e indica la probabilità che il rischio globale è elevato (rosso), medio (giallo) o basso (verde); può quindi essere visto come un "Termometro" che misura il progresso della rapina. Inoltre, l'utente può aprire in ogni momento una finestra in cui è possibile osservare lo stato delle quattro variabili da cui dipende il rischio globale:

- Rischio di protezione;
- Risk Compliance;
- Rischio Tempo;
- Rischio "Cash".



Figura 37. Fase dell'identikit nella Simulazione della Rapina in Banca (Ronsivalle G. B., 2007)

L'ABI (Associazione Bancaria Italiana), il dipartimento Anti-crimine Dipartimento, l'OS.SI.F (Centro di Ricerca dell'ABI per la Sicurezza Anticrimine) hanno creato una rete neurale artificiale

(Artificial Neural Network - ANN) per la gestione del rischio rapina nel settore bancario italiano (Guazzoni & Ronsivalle, 2008).

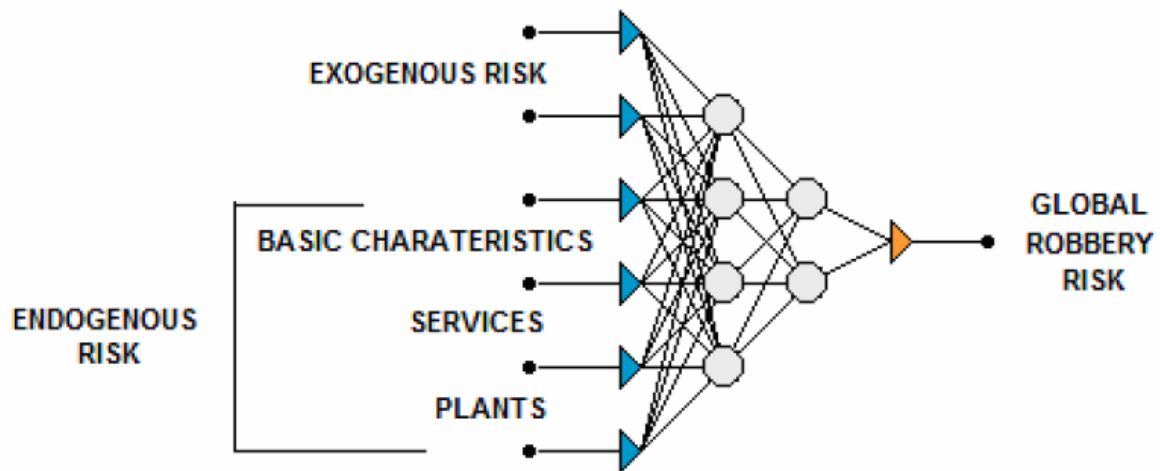


Figura 38. Rappresentazione della Rete Neurale Artificiale OSSIF (Guazzoni & Ronsivalle, 2008)

Il modello di analisi si basa sull'indice di rischio rapina globale relativo ad una filiale bancaria. Tale indice globale è composto da: il rischio esogeno, relativo all'area geografica in cui si trova la filiale e il rischio endogeno, collegato alle variabili specifiche della filiale stessa. La realizzazione di una rete neurale per la gestione del rischio rapina prevede 5 vantaggi:

- 1) rappresenta, in modo coerente, la complessità dell'evento "rapina";
- 2) il database che supporta la rete neurale artificiale si basa su una rappresentazione storica esaustiva relativa al fenomeno delle rapine in banca in Italia;
- 3) il modello è rappresentativo dello stato dell'arte relativo agli approcci per la gestione del rischio;
- 4) la rete neurale artificiale garantisce il massimo livello di flessibilità, dinamicità e adattabilità;
- 5) la rete neurale artificiale permette una efficace integrazione tra un modello di calcolo solido e il buon senso del responsabile della gestione della safety e della security all'interno delle dipendenze bancarie.

Sulla base di questi due lavori appena illustrati, Ronsivalle (2011) propone un nuovo approccio modellistico volto ad analizzare, descrivere e spiegare il fenomeno delle rapine in banca. Esso fornisce un pannello di controllo online per analizzare lo stato attuale di tutte le filiali italiane e scientificamente sostenere la gestione del rischio rapina in tempo reale.

L'obiettivo specifico di questo strumento è quello di fornire ai responsabili della sicurezza della banca italiana con un modello operativo in grado di:

1. "Descrivere" le variabili che caratterizzano il fenomeno "rapina";
2. "Spiegare" le modalità per il calcolo (i) della componente "esogena", (ii) della componente "endogena", e (iii) gli indici di rischio globali per ogni singola dipendenza bancaria;
3. "Prevedere", tramite un modulo di simulazione, le variazioni delle componenti di rischio in relazione ai diversi sistemi di sicurezza adottati nelle dipendenze bancarie.

In particolare, in questo lavoro viene sviluppato un meta-modello incentrato esclusivamente sulla fenomenologia criminale, denominato NBNC (Neural and Bayesian Network to fight Crime - Rete Neurale e bayesiana per combattere il crimine). Tale meta-modello integra appunto le Reti Neurali Artificiali e le reti bayesiane per analizzare efficacemente molti tipi di rischi operativi legati alla criminalità organizzata, come anti-terrorismo e le tecniche di indagine penale.

Il lavoro comprende:

- una premessa sui concetti di "complessità" e "risk management" applicato alla fenomenologia criminale;
- una presentazione analitica della struttura logica e le principali caratteristiche del meta-modello NBNC;
- una breve discussione sul metodo utilizzato per una rete bayesiana derivata dal database OSSIF, attraverso una Rete Neurale Artificiale ANN;

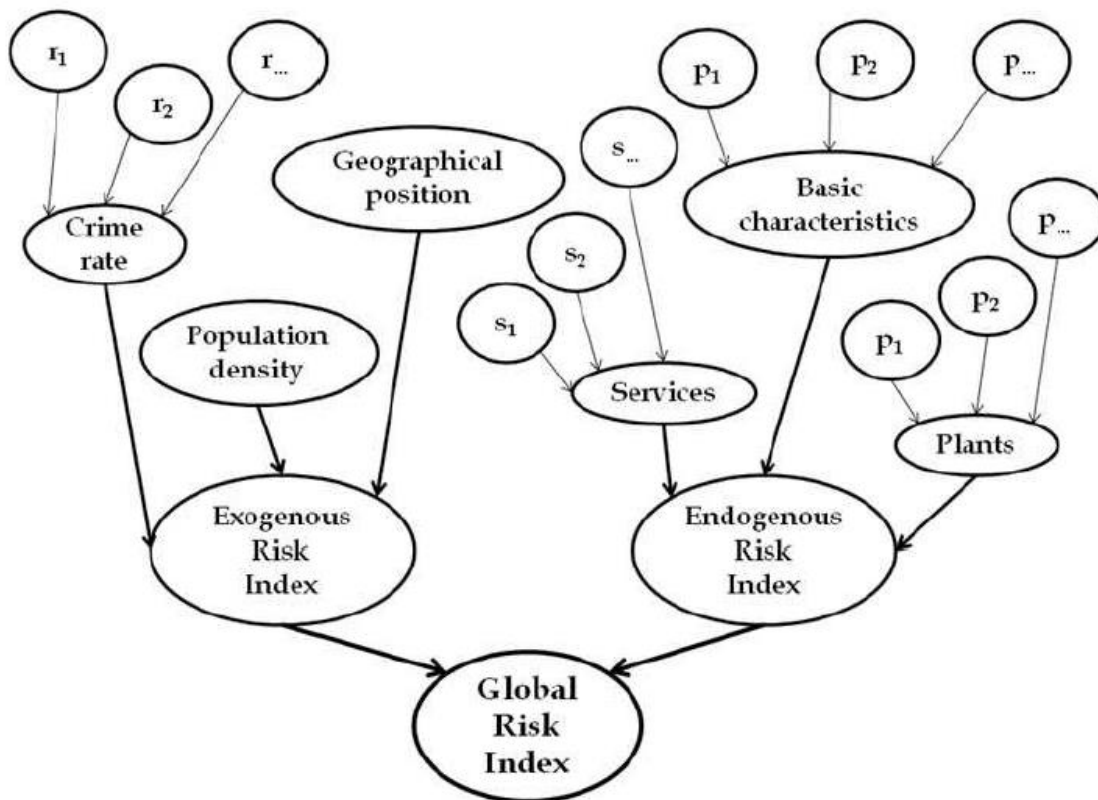


Figura 39. Rappresentazione della Rete Bayesiana adottato da ABI per il modello di analisi del rischio rapina (Ronsivalle G. , 2011)

Per ciò che concerne la sicurezza delle dipendenze bancarie, alcuni autori si sono concentrati su fattori di deterrenza dal compiere una rapina. Uno studio condotto a Victoria, in Australia, da Clarke, Field, e McGrath (1991), tra il 1979 e il 1987, mostra come l'introduzione di una serie di apprestamenti di sicurezza all'interno delle filiali delle banche abbia portato alla diminuzione considerevole del numero di rapine. L'installazione di telecamere, la presenza di guardie

giurate, la protezione degli addetti allo sportello, costituivano un deterrente per l'autore di reato. Infatti, esse sono tutte misure rivolte ad aumentare i controlli di accesso, gli sforzi percepiti (e quindi maggiori difficoltà di perpetrare il reato), ad aumentare i rischi percepiti e la sorveglianza formale. Gli studiosi hanno rilevato che un programma intenso di rinforzo dell'obiettivo in queste banche australiane condusse anche ad una generale riduzione delle rapine di tutti gli obiettivi commerciali. I rapinatori iniziarono a credere che questa forma di crimine non fosse più una attività remunerativa, per la diminuzione del contante alla mano presente all'interno delle filiali delle banche.

La visibilità rende il potenziale autore di reato maggiormente a rischio rispetto al contesto circostante in cui decide di agire, nonché rispetto alla presenza di "guardiani capaci". Questo perché limita la sua capacità di azione, di controllo della situazione e del territorio. Essa costituisce, quindi, una forma di limitazione, di rischio non calcolato. Uno dei problemi di sicurezza che le banche devono affrontare è quello di implementare una serie di misure che riducano il numero di reati di rapina. Per raggiungere questo importante obiettivo, le banche operano, attraverso specifiche attività, una attenta valutazione del rischio rapina, nonché una analisi di quelle che sono le vulnerabilità del sistema bancario, gli apprestamenti di sicurezza anti-rapina più adeguati alle diverse filiali della banca, in base ad una serie di parametri che identificano i differenti livelli di rischio. La sorveglianza naturale è un obiettivo primario della prevenzione situazionale. L'incremento dell'illuminazione delle strade, dello spazio difendibile, l'installazione di TVCC sono tutte misure dirette non solo a creare una maggiore visibilità dello spazio, ma anche del potenziale autore di reato (Ramsay & Newton, 1991).

Da diversi anni si discute e si disquisisce in merito alle vetrate che sono presenti nelle agenzie bancarie. All'interno di questo importantissimo argomento di sicurezza, nella fattispecie di prevenzione delle rapine, si inserisce anche l'aspetto estetico, dove architetti, arredatori, esperti di marketing, che hanno cura dell'immagine e dell'impatto sui clienti della banca, hanno esigenze particolari, non sempre allineate con quelle della sicurezza. Infatti, la soluzione ideale elaborata dagli esperti di sicurezza è quella di tenere le vetrate completamente scoperte, libere. Si presuppone che durante i sopralluoghi effettuati da un rapinatore, per stabilire quale agenzia sia più idonea a compiere un attacco, un elemento importante sia rappresentato dalla presenza o meno di strutture che impediscano di vedere attraverso le vetrate. Il motivo di individuare un'agenzia con le vetrate non trasparenti è che la copertura impedisce ai passanti, i potenziali 'guardiani capaci', e agli impiegati e clienti della filiale di rendersi conto di quanto accade all'interno, di lanciare eventualmente l'allarme, e quindi di impedire il compimento della rapina (innescando, così, un processo di sorveglianza informale). Si afferma sempre più l'idea che la trasparenza delle vetrate delle filiali sia una componente fondamentale della diminuzione del rischio rapina, in accordo anche con le Forze dell'ordine. Il focus dell'analisi è che il potenziale autore di reato, nel suo processo decisionale (ammesso che egli sia un autore professionista), prenderà fortemente in considerazione il fatto di essere visto dall'esterno dei locali delle banche. Ecco che si inizia a parlare di sorveglianza naturale (o informale o di

vicinato) come strumento di deterrenza. Tale concetto deriva appunto dalla teoria della prevenzione situazionale. La sorveglianza naturale si inserisce nella teoria delle attività abituali e della scelta razionale, e costituisce uno degli elementi fondamentali che il potenziale autore di reato prende in considerazione nel processo decisionale che caratterizza la commissione di un reato.

Intervenendo sul tema della sicurezza degli sportelli bancari, il Questore di Torino (28 gennaio 2005) riferisce di essere rimasto colpito da una serie di agenzie bancarie le cui vetrine sono coperte da una pellicola non trasparente (le bande satinare), che impedisce di vedere dall'esterno ciò che avviene all'interno dei locali. Ciò è risultato incomprensibile, quasi all'interno si svolgessero attività molto riservate, anziché semplici attività consulenziali, commerciali e di sportello. Tale occultamento, secondo il Questore di Torino, non può che favorire il compimento di atti criminosi, in quanto i rapinatori preferiscono agire senza essere visti, mentre, al contrario, l'interscambio visivo con l'esterno può consentire a chiunque di scorgere una rapina in corso e dare l'allarme. Il Questore di Torino non auspica una trasparenza completa, in quanto gli appare necessario mantenere qualche angolo di riservatezza, non al punto, però, da oscurare alla vista del pubblico l'intero salone, il quale dovrebbe essere in gran parte liberamente osservabile dall'esterno.

In data 30 novembre 2005 è stato sottoscritto il Protocollo di intesa in materia di sicurezza delle banche, con l'intento di prevenire i fenomeni criminali in banca nella provincia di Verona, in collaborazione istituzionale in materia di sicurezza degli Istituti di Credito. In particolare, è stata affrontata la questione riguardante l'affissione di manifesti sulle vetrine degli Istituti di Credito. È stato, a tale riguardo, osservato che i manifesti o altri avvisi di tipo pubblicitario, sovente affissi sui vetri di detti Uffici, non consentono un'ottimale visione di quanto accade all'interno degli stessi, rendendo così difficoltosa l'attività di vigilanza e di contrasto ad opera degli Organi di Polizia, soprattutto in caso di intervento determinato da una rapina in atto. Al fine, pertanto, di facilitare il delicatissimo compito delle Forze dell'ordine nell'azione di controllo, a salvaguardia anche della sicurezza pubblica, è stata rappresentata la possibilità che tale documentazione venga posizionata, ove possibile, in altri siti. Questa esigenza nasce anche dalla necessità di avere una sorta di "trasparenza" nei rapporti con il cliente, di eliminare, quindi, tutte le barriere che si interpongono tra la banca e il cliente. Il cliente sembra volere sempre più un comportamento vicino, rassicurante, "trasparente" con la sua banca, quindi la scelta ricade su quelle che soddisfano maggiormente queste esigenze nascenti, invece di una banca "fortezza".

3.2.3 La protezione delle dipendenze bancarie: Layout tipici delle Dipendenze Bancarie

Il controllo degli accessi risponde all'esigenza di una azienda di consentire, in modo automatico o assistito, l'accesso dei dipendenti o di soggetti terzi che la frequentano, ai propri locali. Lo stesso tipo di esigenza è presente nelle banche, soprattutto per le grandi sedi e/o aree di particolare interesse. Per le sedi e/o edifici vi sono diverse soluzioni. In ogni caso quando

parliamo di sistemi di protezione/sicurezza agli accessi ci riferiamo a sistemi che si basano su individui “censiti”, e quindi conosciuti, registrati e autorizzati. Quando invece parliamo di sistema di controllo agli accessi dedicato ad uno sportello bancario aperto al pubblico, ci si riferisce ad un filtro in grado di contrastare l’accesso di individui (censiti e non censiti) con intenzioni criminali.

Verranno presentate qui di seguito alcune tipologie di layout che serviranno a comprendere quali sono le diverse esigenze di sicurezza di uno sportello bancario e quali sono le possibili soluzioni atte a soddisfare tali esigenze, indicando anche gli elementi tecnologici principali. Sono evidenziate agenzie con diverse complessità sia per diverse aree in esse presenti (area sportello, area self-banking e area tecnica valori) e sia per diversi modi di gestione delle agenzie stesse nelle ore di apertura e chiusura degli sportelli. Per questo tipo di difesa le soluzioni possibili vanno da quelle puramente deterrenti a quelle che svolgono un’azione attiva in grado di impedire l’accesso con armi da fuoco. Di particolare importanza sono gli spazi contenenti valori come i caveau, i mezzi forti ecc. Per questi spazi si dovrà garantire un elevato livello di protezione/sicurezza derivante dalla combinazione di misure fisiche passive ed elettroniche attive, sempre abbinate al sistema di controllo degli accessi. Un altro aspetto da tenere in dovuta considerazione riguarda il controllo accessi alle aree self-service. In queste aree è necessario effettuare un controllo volto a contrastare la clonazione dei bancomat e a segnalare situazioni anomale come una permanenza lunga. Come si potrà evincere dai sottoparagrafi che sono riportati nel seguito di questa trattazione ogni tipologia di layout esprime una o più specifiche esigenze di sicurezza di uno sportello bancario. Sono evidenziate agenzie con differenti complessità, sia per le differenti aree in esse presenti (area sportello, area self banking ed area tecnica valori) sia per i diversi modi di gestione delle agenzie stesse nelle ore di apertura e chiusura degli sportelli. Per andare incontro alle esigenze commerciali delle banche e dovendole proteggere da un rischio che purtroppo è ancora elevato è necessario trovare soluzioni che siano confacenti a questa esigenza. Le funzioni di marketing e commerciali delle banche “spingono per rendere gli sportelli bancari sempre più simili alle altre attività commerciali. Al fine di arrivare a questa configurazione e proporre alle funzioni interne delle banche improntate al business qualcosa che non sia “pesante” in termini di protezione, in (Messina, 2002) vengono identificate le seguenti categorie

La protezione degli accessi e perimetrale	Bussole motorizzate con o senza metaldetector, porte interbloccate, biometrici, uscite di emergenza con o senza magnete e/o segnalazione d’allarme, finestre e vetrine, dissuasori antisfondamento, rinforzi alle opere murarie)
Le misure per disincentivare il rapinatore	Mezziforti con time-lock, timebination, time-delay, sistemi di frazionamento del denaro, cash in - cash out, posta pneumatica, sistemi di colorazione delle banconote
Le misure di ricostruzione di eventi	Impianti TVCC analogici o digitali
Le misure di segnalazione di evento	Allarme antirapina, videosorveglianza, sensibilità all’esterno

I servizi di vigilanza	Piantonamento antirapina, guardia itinerante, guardia multibanca, videosorveglianza
-------------------------------	---

Tabella 19. Sistemi di protezione delle dipendenze bancarie (Messina, 2002)

Quali sono le esigenze commerciali delle banche? Rispondere effettivamente ai bisogni della clientela, ridistribuire gli spazi. Non ci sono più ormai sportelli bancari disposti su più piani per centinaia o migliaia di metri quadri, si va su soluzioni tipicamente da negozio, da 100–180 metri quadri, che oltretutto non vengono costruiti ad hoc per lo sportello bancario, ma sono soluzioni che sono anche abbandonabili quando la quota di mercato non sia sufficientemente interessante.

La funzione di sicurezza all'interno di un'azienda ovviamente non è avulsa da ciò che l'azienda fa. C'è un *core business* che è la funzione di vendita, e nel caso delle banche parliamo di vendita finanziaria, quindi con dei rischi, ma la funzione di security deve adattare le proprie scelte in funzione delle finalità del proprio *core business*, e non diventare un limite a questo. Come facciamo ad aumentare la facilità di accesso ai nostri sportelli visto che questo apre, oltre che alla clientela, anche a maggiori rischi? Un approccio è quello di ridurre il livello di protezione perimetrale e aumentare il livello di protezione per qualcos'altro, tipicamente il denaro. Le apparecchiature *cash in-cash out* sono soluzioni ormai abbastanza diffuse, e si stanno evolvendo. Ce ne sono di varie tipologie, più o meno costose e automatizzate e sono un vincolo forte per la riduzione del bottino della rapina. Ci sono poi strumenti che servono affinché le forze di polizia conseguano il loro obiettivo, che è quello di reprimere, se non si riesce a prevenirlo, il crimine. Reprimere significa che, se le batterie di rapinatori vengono assicurate alla giustizia si riducono anche le rapine. Quindi, sistemi di videoregistrazione o, dove è possibile e dove il rischio li giustifica, sistemi di videosorveglianza. Considerando che le statistiche affermo che nella maggiorparte dei casi le rapine vengono perpetrate da rapinatori "occasionalmente", Messina (2002), propone dei sistemi di ingresso basate su *sliding doors*, con una logica di interblocco che consenta di interromperne il funzionamento laddove ci sia un travisamento del rapinatore che accede; quindi fare in modo che comunque questa soluzione, anche se presenta una bella luce ed è automatica nell'apertura della porta, consenta un minimo di protezione da parte dell'operatore di sportello. Questa stessa porta può consentire anche l'utilizzo della stessa come porta di emergenza, evitando quindi di occupare altre vetrine che invece tipicamente le funzioni di marketing desiderano utilizzare per il merchandising, cioè di messaggi commerciali. La valorizzazione dell'area self, quindi delle macchine di erogazione del denaro e di più recente applicazione nel mercato italiano anche quelle di deposito, consente da una parte di ridurre il carico degli operatori di cassa che, come ho già detto, è personale che svolge attività esecutiva e non ha nessuna possibilità di vendita. È possibile, cioè, spostare gradualmente le attività, compatibilmente con quello che il cliente sarà disposto ad accettare, perché non ci potrà essere identico comportamento sull'intero territorio nazionale nell'operare di fronte ad una macchina. Può esserci un innalzamento del "rischio furto" con queste

apparecchiature, perché contengono cifre assolutamente rilevanti e quindi dobbiamo individuare delle soluzioni di protezione piuttosto forti. Però, bisogna constatare che in questo tipo di evento viene a mancare quella situazione di emergenza che è l'attacco in presenza di persone e, quindi, l'assenza di rischio fisico. Il furto è indubbiamente dannoso, provoca l'aumento dei premi assicurativi le polizze assicurative e così via, però certo non ci pone in condizioni, in primo luogo, di grandi rischi per il dipendente e per la clientela e, poi, di contenzioso sindacale per un'ovvia pretesa, da parte di chi rappresenta il lavoratore, di proteggere adeguatamente il personale.

I "nuovi" obiettivi della security bancaria spingono verso l'utilizzo di sistemi di protezione soltanto dove effettivamente serve:

- ottimizzazione degli spazi con conseguente contenimento delle aree dedicate alla sicurezza o, comunque, non utilizzabili per la "vendita";
- miglioramento dell'equilibrio fra investimenti e risultati attesi;
- adeguamento delle misure di sicurezza alle reali esigenze (implicite, esplicite e cogenti) di tutte le parti interessate

Nella seguente figura viene rappresentato una possibile configurazione di dipendenza bancaria, al quale si è arrivato, nel tempo, attraverso diversi momenti, adeguamenti ed integrazioni. Ripercorrendo velocemente lo sviluppo di questa tipologia di sportello durante gli anni, per la "rincorsa" delle misure di sicurezza alle mutate esigenze operative ed all'evoluzione dei fenomeni criminosi. Tali evoluzioni, a partire dallo sportello tipo degli anni '70, sono identificabili nei seguenti punti:

- Al perimetro vengono aggiunte inferriate, vetrate antiproiettile e/o antisfondamento, dissuasori contro lo sfondamento sulla base della tipologia e della "magnitudo" degli eventi criminosi (nascono contrasti con gli uffici preposti all'immagine aziendale, con le autorità locali e con le amministrazioni di condominio per l'occupazione di spazi pubblici o condominiali, con gli uffici tecnici per le difficoltà realizzative e per le modifiche agli impianti, con i dipendenti perché si sentono "chiusi in gabbia").

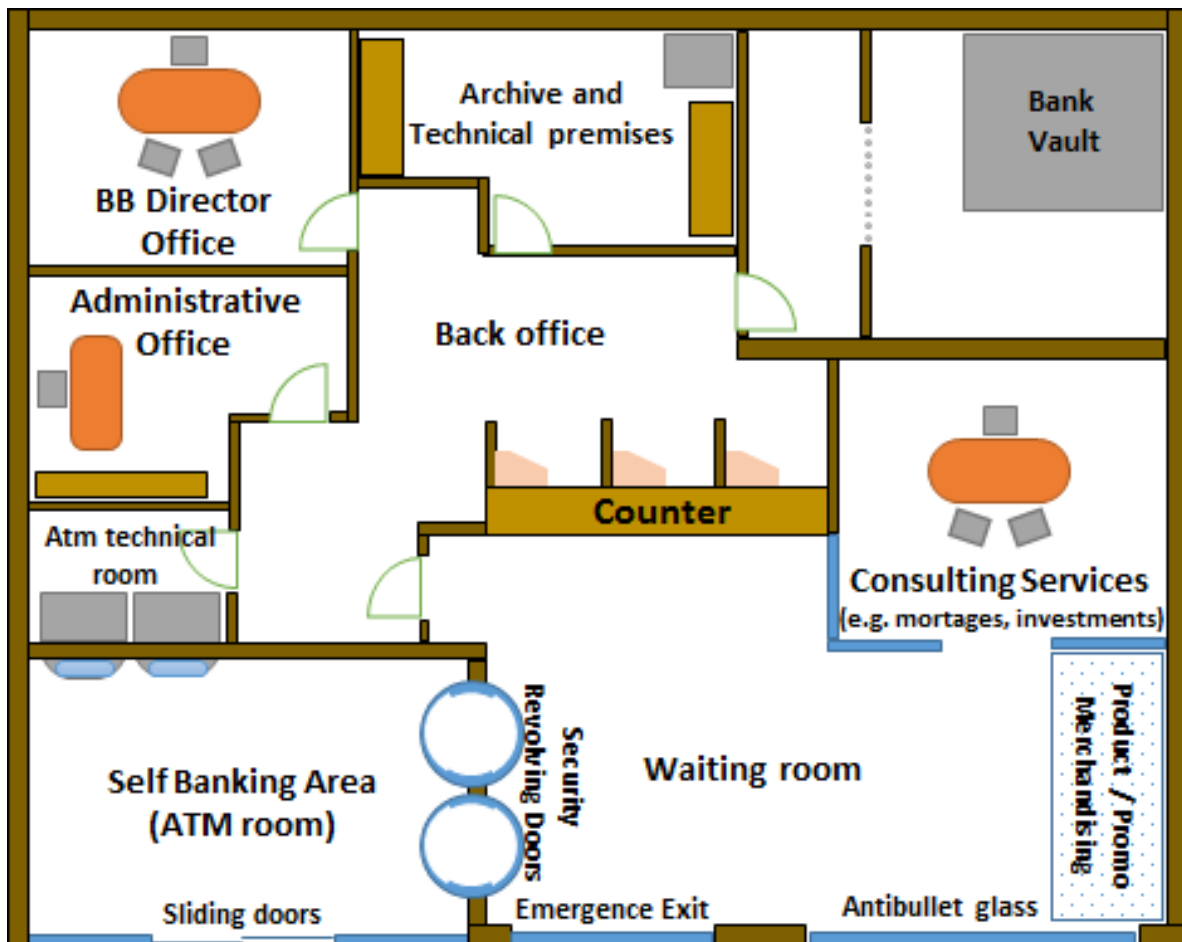


Figura 40. Esempio di Layout di una dipendenza bancaria (Messina, 2002)

- All'interno si ha una suddivisione fra "sala pubblico" e "locali ad ufficio", costituita da banconi o da posti di lavoro più o meno continui.
- La superficie destinata al "pubblico" è tale da soddisfare le esigenze operative nel breve periodo.
- La superficie destinata alla "clientela" ricerca sempre nuovi spazi in quanto le nuove tecniche di vendita richiedono un maggior contatto interpersonale (vengono utilizzati anche locali interni non sempre funzionali - "oscuramento" di telecamere con conseguente creazione di aree non protette).
- La superficie destinata ad uffici interni, a locali tecnici, ad archivi non può venir compressa oltre certi limiti tecnici e funzionali.
- Per garantire un miglior rapporto con il pubblico, i banconi antiproiettile vengono "sostituiti" da bussole più o meno sofisticate (proporzionalmente al livello di sicurezza offerto dalle bussole aumentano le occasioni di attrito/contrasto con gli uffici commerciali, con la clientela e con i dipendenti) e munite di apparati per il controllo degli accessi sempre in evoluzione (dal mutuo consenso al sistema "biometrico").

- L'installazione di bussole comporta (quasi sempre) la creazione di agevoli uscite di sicurezza (con conseguente necessità di adeguamento alle disposizioni di legge e alle prescrizioni degli Organi di Vigilanza preposti e con i problemi tecnici che tutti conosciamo).
- Le "CASSE": erano il "cuore" e la "bandiera" di un sportello bancario. Non più. Vengono relegate in secondo piano e senza una visione diretta delle bussole (mancata assistenza della clientela durante il transito attraverso le bussole).
- Il "LOCALE VALORI – ex CAVEAU" ubicato sempre in posizione decentrata, ma sempre "in mezzo" (risulta ora nelle vie di transito, più lontano dalle casse e facilmente raggiungibile anche da malintenzionati).
- I bancomat e le casse continue devono affacciarsi sulla strada o su ambienti accessibili anche fuori orario (solo nelle regioni maggiormente colpite da attacchi criminosi i valori sono protetti da locali).
- Gli allarmi sono localizzati a protezione dei valori e degli accessi. Sino a modifiche sostanziali del lay-out non si ravvisano particolari problemi per la sicurezza.
- La fornitura di buone immagini "video" alle Forze dell'Ordine sta fornendo risultati apprezzabili, ma non basta: si devono fornire immagini certe e utilizzabili. Ciò comporta un ampliamento delle aree di ripresa con conseguente aumento dei costi di installazione, di esercizio e di manutenzione.

Nella prossima figura invece lo stesso sportello bancario è allestito con il modello **WWD 2002**. L'accesso allo sportello potrà essere configurato nel modo più consono alla "mission" dello sportello senza dimenticare però le opportune sicurezze.

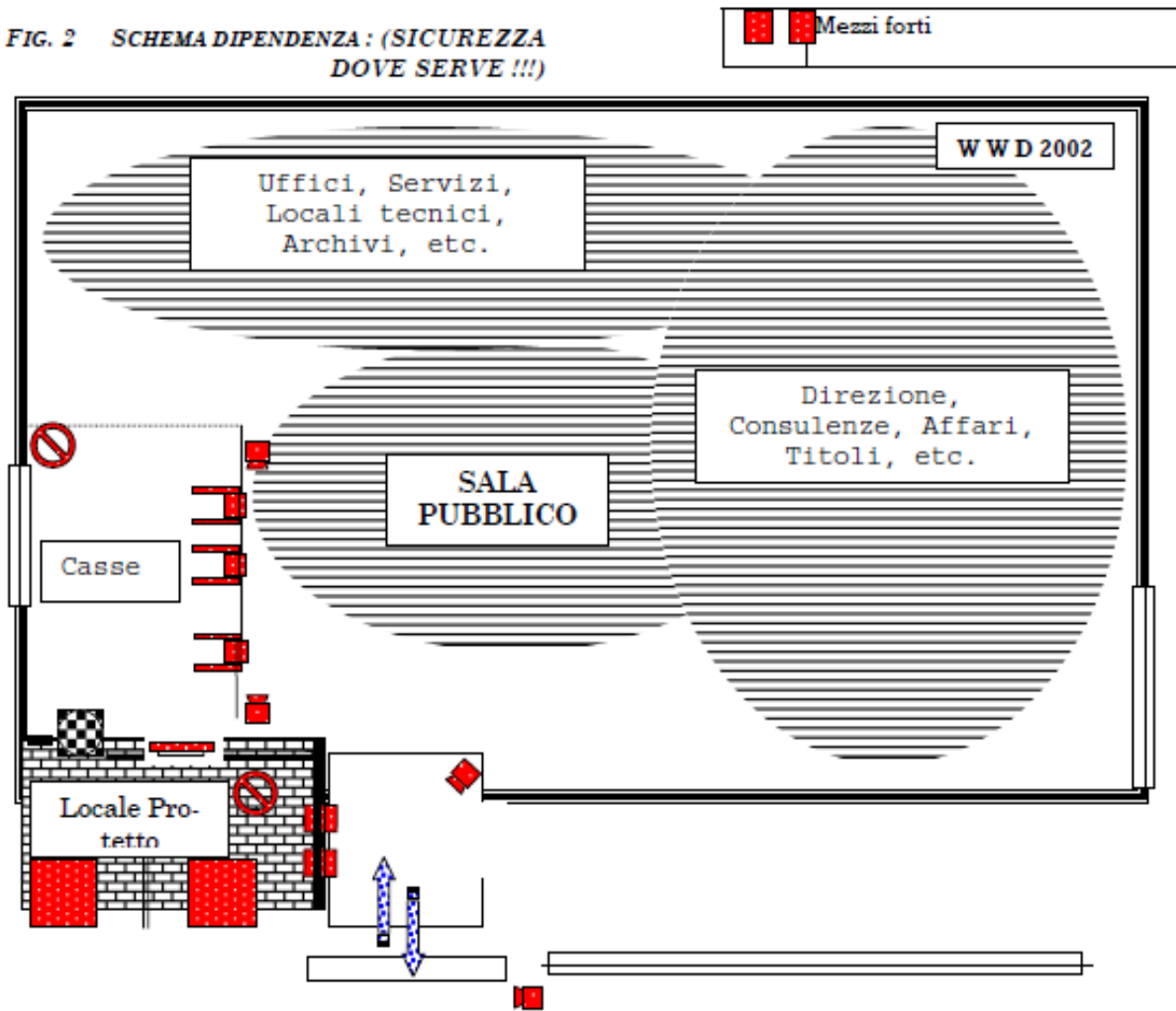
Si potrà notare:

- le aree in sicurezza sono state ridimensionate e concentrate;
- maggior spazio risulta disponibile per le attività di vendita (e servizi accessori);
- gli accessi sono agevoli;
- non sono necessarie strutture fisiche perimetrali antisfondamento;
- l'impianto di allarme (e l'impianto di rilevazione fumi collegato) risulta concentrato solo in presenza di valori;
- l'impianto di televisione in circuito chiuso è stato ridimensionato;
- la bussola (con "biometrico") è prevista all'ingresso del "Locale Protetto" dotato anche di "Uscita d'emergenza";
- le casse sono dotate di sistemi "cashin/cash-out ON LINE", per consentire la conservazione dei valori durante l'intero arco della giornata (e – se blindate - di ragionevoli somme di denaro anche durate le ore notturne)

Esaminiamo in dettaglio questo modello di sportello bancario:

- Le CASSE (in numero adeguato alle esigenze operative dello sportello): non necessariamente a bancone, se del tipo “cash-in/cash-out ON LINE”. Non è questa la sede adatta per approfondire la tipologia della attrezzatura, peraltro il mercato ha già fornito una risposta (rimango a disposizione personalmente per eventuali approfondimenti e scambio di esperienze). Sull’argomento mi rimane da suggerire che, per garantire una maggior sicurezza di carattere generale ed una migliore funzionalità, è opportuno che le CASSE risultino contigue al “LOCALE PROTETTO”.
- Il “LOCALE PROTETTO” sarà di dimensioni adeguate alle dimensioni e alla tipologia dello sportello bancario con pareti ad alta sicurezza. Al suo interno troveranno posto la cassaforte “uso banca”, la cassaforte “cassette di sicurezza”, eventuali altri mezziforti a tempo, il tesoretto del bancomat e della cassa continua. Meglio se l’utilizzo di questi ultimi sistemi automatici (e degli altri che verranno) avverrà in un’area riservata dalla quale non risulti possibile accedere allo sportello “fuori orario” (in alcune realtà bancarie europee quest’area viene collocata al termine del percorso della clientela, per evitare che il cliente si “innamori” delle macchine perdendo di vista gli altri servizi offerti dallo sportello). L’accesso al locale sarà regolato da una bussola con sistema “biometrico” od altro sistema ad alta sicurezza (sulla base della cultura aziendale in materia e ... del budget a disposizione). Tenuto conto delle sicurezze all’accesso, sarà necessario prevedere un’uscita di sicurezza adeguatamente accessoriata.

FIG. 2 SCHEMA DIPENDENZA: (SICUREZZA DOVE SERVE !!!)



Legenda	
	Aree di Sicurezza
	Aree aperte al pubblico/clientela
	Impianto di allarme (volumetrici, sismici, etc.) e di rilevamento
	Impianto di televisione in circuito chiuso
	Bussole all'ingresso con "biometrico"
	Uscita di sicurezza
	Strutture fisiche antisfondamento/intrusione (inferriate)
	Posto cassa con cassettera antirapina "on line"

N.B.: La dislocazione delle diverse aree funzionali e degli apprestamenti di sicurezza è da ritenersi indicativa.

Figura 41. Layout a banca aperta WWD2002 (Messina, 2002)

- L'impianto di allarme sarà concentrato sul "LOCALE PROTETTO" e, tenuto conto delle ridotte dimensioni, potrà essere, se del caso, agevolmente aggiornato tecnologicamente (anche come interfaccia con l'utenza).
- Anche l'impianto TVCC risulterà concentrato dove sono i valori e, tenuto conto delle ridotte dimensioni, le immagini potranno essere trasmesse a distanza presso centrali di sorveglianza.

SISTEMA TRE PORTE SLIDING DOORS

Modalità di funzionamento

- Fascia oraria sportello aperto
 - **Area self-banking:** accesso **libero**
 - **Area sportello:** accesso **controllato** a porte interbloccate
- Fascia oraria sportello chiuso
 - **Area self banking:** accesso **controllato** da lettore
 - **Area sportello:** accesso **riservato** tramite Bussola

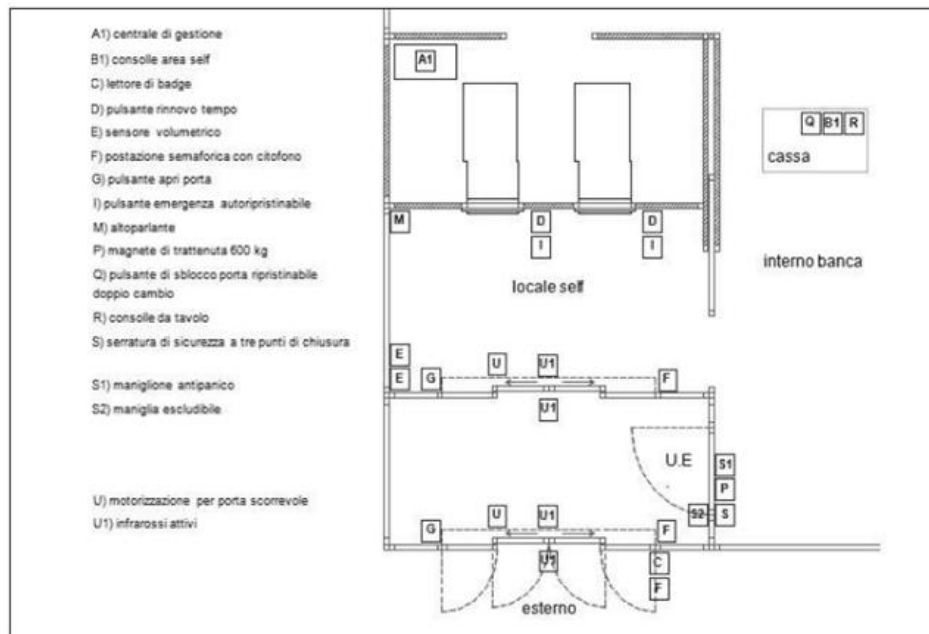


Figura 42. Layout a tre porte

SISTEMA INTEGRATO AREA SELF-BANKING E BUSSOLA

- Fascia oraria sportello aperto
 - **Area self banking:** accesso **libero**
 - **Area sportello:** accesso **controllato** tramite **Bussola**
- Fascia oraria sportello chiuso
 - **Area self banking:** accesso **controllato** da lettore
 - **Area sportello:** accesso **riservato** tramite Bussola

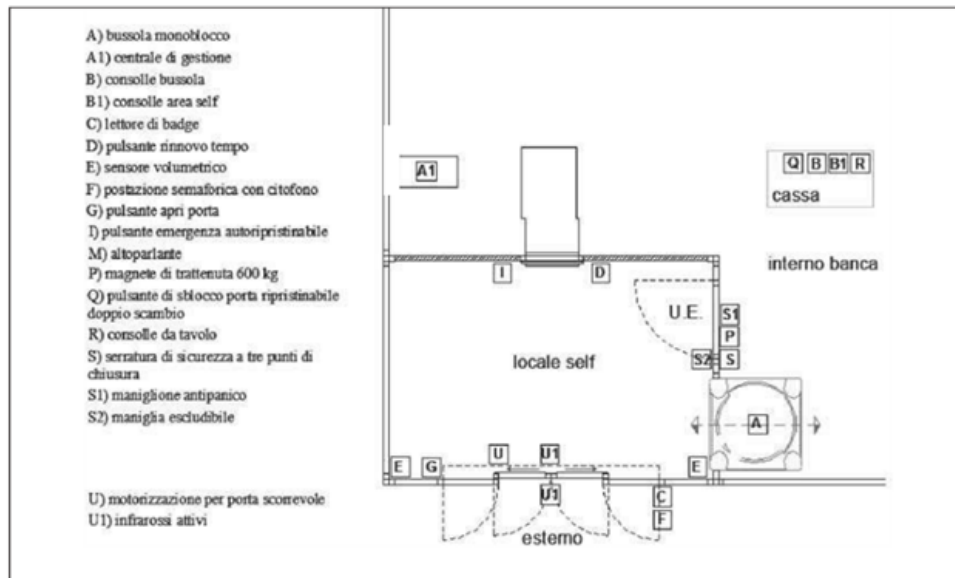


Figura 43. Sistema integrato con area self banking

SISTEMA DI CONTROLLO AREE INTEGRATO: SELF BANKING, SPORTELLO, TECNICA VALORI

Modalità di funzionamento

- Fascia orario sportello aperto
 - **Area self banking:** accesso **libero**
 - **Area sportello:** accesso **controllato** tramite Bussola
 - **Area tecnica valori:** accesso **controllato** personale sportello
- Fascia oraria sportello chiuso
 - **Area self banking:** accesso **controllato** da lettore
 - **Area sportello:** accesso **riservato** tramite Bussola
 - **Area tecnica valori (non accessibile al pubblico):** accesso **riservato e controllato** Portavalori Via Area self-banking e Bussola

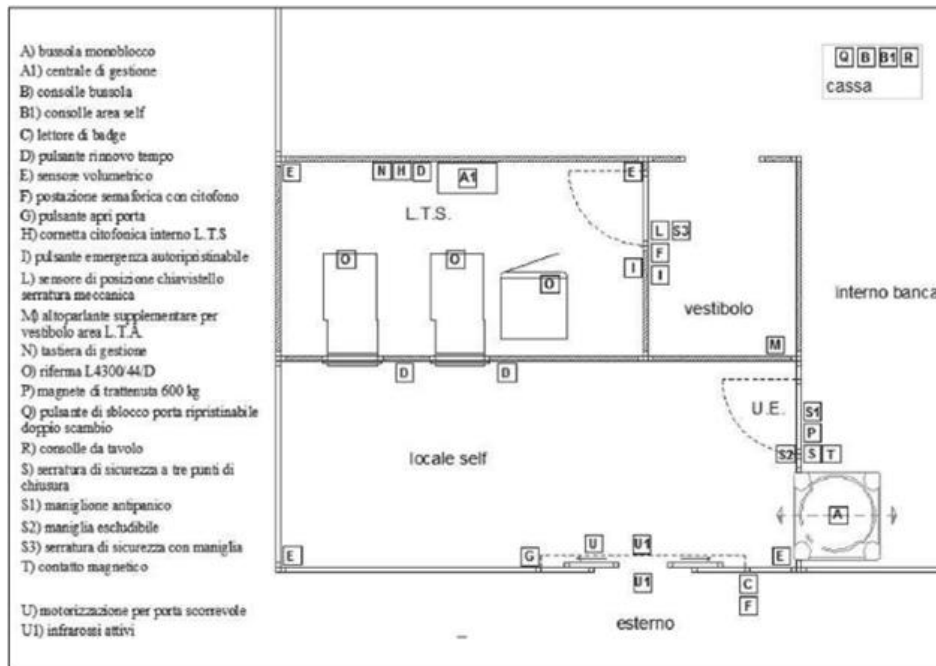


Figura 44. Sistema integrato con area self banking e sportello

3.2.3.1 SISTEMA-SLIDING DOORS INTERBLOCCATO CON FUNZIONE AREA SELF-BANKING

Sistema di controllo accesso area Self-Banking e area sportello

- Fascia oraria sportello aperto
 - **Area self-banking:** accesso **libero**
 - **Area sportello:** accesso **controllato** tramite Bussola
- Fascia oraria sportello chiuso
 - **Area self-banking:** accesso **controllato** da lettore
 - **Area sportello:** accesso **riservato** tramite Bussola

- C) lettore di badge
 - D) pulsante rinnovo tempo
 - E) sensore volumetrico
 - F) postazione semaforica con citofono
 - G) pulsante apri porta
 - I) pulsante emergenza autoripristinabile
 - M) altoparlante
 - P) magnete di trattenuta 600 kg
 - Q) pulsante di sblocco porta ripristinabile doppio scambio
 - R) consolle da tavolo
 - S) serratura di sicurezza a tre punti di chiusura
 - S1) maniglione antipanico
 - S2) maniglia escludibile
- U) motorizzazione per porta scorrevole
U1) infrarossi attivi

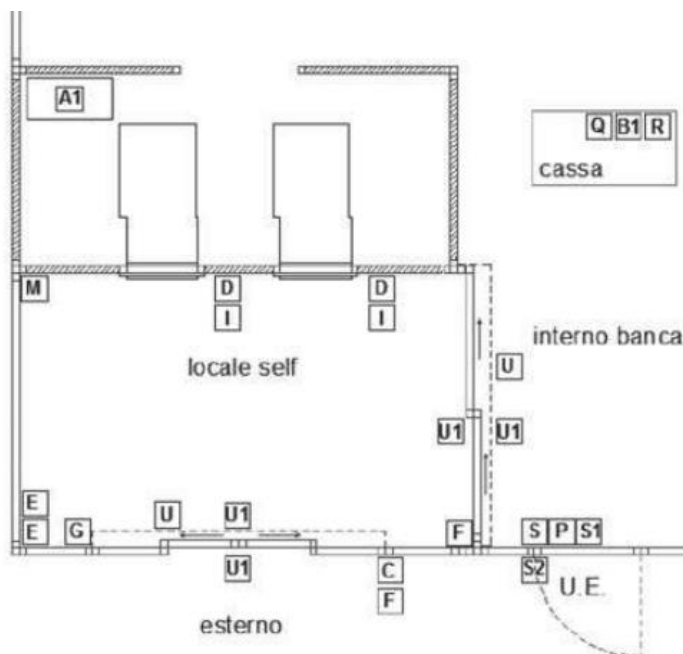


Figura 45. Sistema sliding doors interbloccato

3.2.3.2 LOCALE ESCLUSIVO PER AREA SELF-BANKING DI TIPO 24 ORE

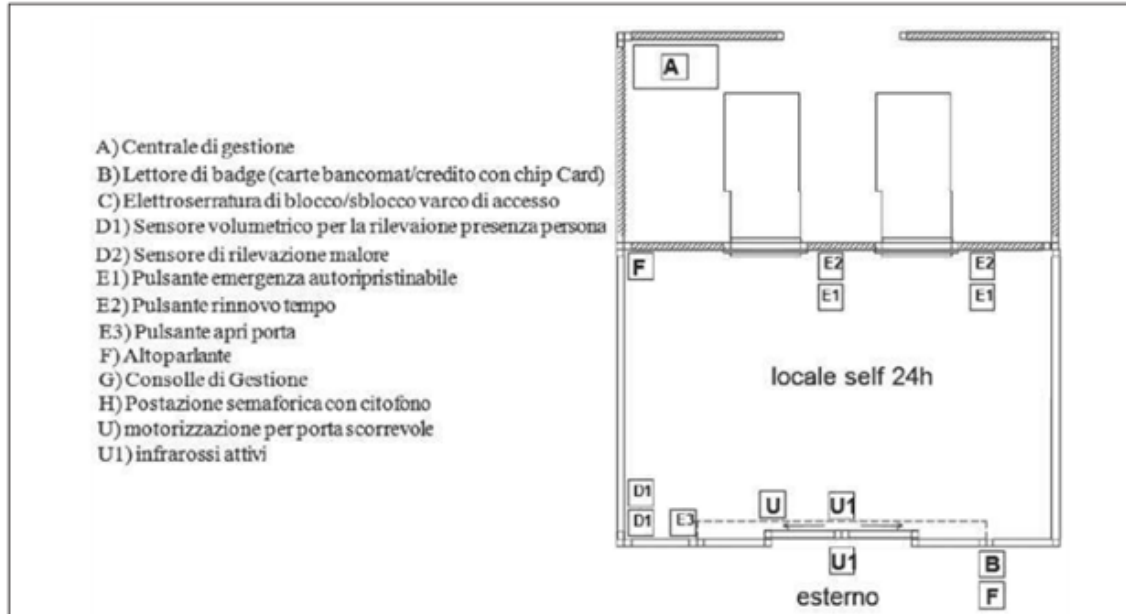


Figura 46. Locale esclusivo self banking H24

3.2.4 Misure di protezione adottate nelle dipendenze bancarie

Per ciò che concerne le misure di protezione (o soluzioni difensive) che una banca può adottare, come si è potuto evincere dalle trattazioni precedenti, la tecnologia gioca senza dubbio un ruolo importante. Di seguito verranno trattate e spiegate con maggiore attenzione le misure difensive che la banca può adottare per impedire o quantomeno arginare i fenomeni criminali. Le seguenti misure, come affermato in precedenza, fanno parte dei protocolli d'intesa per la prevenzione della criminalità in banca sottoscritti dall'ABI con le Prefetture, le banche firmatarie e le Forze dell'ordine.

La vigilanza

La vigilanza è stata una delle maggiori strategie di sicurezza adottate dalle banche in passato, soprattutto perché altri dispositivi di sicurezza non erano ancora molto diffusi in commercio.

Oggi questa strategia di protezione, seppur presente, risulta essere utilizzata in misura minore rispetto a prima. Il vantaggio di questa misura è quella di fungere da deterrente per il rapinatore. Tuttavia c'è da dire che l'efficacia della deterrenza dipende dalla tipologia di rapinatore. Essa infatti risulta essere più efficace nel caso in cui si tratti di rapinatore dilettante, mentre nel caso in cui ci si trovi davanti ad un rapinatore professionista l'efficacia diminuisce perché il rapinatore, contando sull'effetto sorpresa, può aggirare l'ostacolo, disarmando la guardia e impedendole qualsiasi possibilità di intervento.

La guardia giurata generalmente è utilizzata all'esterno della dipendenza, proprio in prossimità dell'ingresso principale in questo caso si parla di piantonamento fisso.

Nel caso invece di vigilanza mobile le dipendenze sono soggette a controlli saltuari da parte di pattuglie di guardie che operano in aree di grandi dimensioni e cambiano di volta in volta gli orari con lo scopo di generare un effetto deterrente nel rapinatore e dunque ridurre la sua propensione a commettere atti criminali.

Le difese perimetrali

Le difese perimetrali sono rappresentate da tutte quelle misure che dovrebbero impedire, o perlomeno scoraggiare, l'accesso dei rapinatori nella dipendenza bancaria.

La bussola antirapina risulta essere lo strumento più diffuso tra le difese perimetrali. Si tratta di un vano blindato omogeneamente in tutte le sue parti, attraverso il quale il transito è bloccato da porte interbloccate (che non si aprono contemporaneamente).

Esistono tre differenti tipi di bussole antirapina:

- Porte semplici, a una o due ante girevoli, senza interblocco;
- Porte doppie interbloccate pluripersona: questa tipologia di misura di protezione impedisce l'apertura delle seconde porte se le prime non si sono richiuse completamente, ma nel vano tra le due possono entrare più persone;
- Bussole monopersona, a doppia anta, a cilindro rotante o altro, ma in questo caso nel vano non può entrare più di una persona per volta.
- Porte scorrevoli interblocco.

Le bussole monopersona possono essere abbinare ad altre misure di sicurezza, come i metal-detector e i sistemi biometrici.

I **metal-detector** usano l'induzione elettromagnetica per rilevare la presenza di metalli. Nonostante si possa eludere il controllo, questo strumento di sicurezza ha comunque contribuito a ridurre il numero delle rapine perpetrate con le armi.

L'utilizzo dei **sistemi biometrici**, come descritto in precedenza, si basano sulla lettura dei parametri biologici. Essi hanno la funzionalità e lo scopo di identificare una persona sulla base di una o più caratteristiche biologiche e /o comportamentali (biometria). Il vantaggio che ne risulta è dunque determinato dalla possibilità di fornire alle Forze dell'ordine un dato di identificazione sicuro in caso di rapina.

Questi sistemi di controllo agli accessi sono realizzati in modo tale da non dover ricorrere all'intervento dei dipendenti, se non i casi particolari.

Negli ultimi anni inoltre si stanno diffondendo i **sistemi anticamuffamento**, i quali si basano sull'analisi dei video per impedire l'accesso in filiale ai soggetti non chiaramente identificabili.

Ogni dipendenza deve inoltre poter garantire un'uscita di sicurezza che, all'occorrenza, potrà essere utilizzata come ingresso per persone con neonati in carrozzina, disabili su sedie a rotelle e portatori di pacemaker. Molto importanti risultano essere anche le vie di accesso conosciute come "improprie", ovvero le vetrine e le finestre anch'esse utilizzate dai criminali come punto

di accesso all'interno della dipendenza. Per tale ragione è opportuno garantire degli accorgimenti di natura tecnica:

- Per quanto riguarda le vetrine è necessario che i vetri siano blindati, i telai siano robusti e i componenti di tali attrezzature siano saldamente ancorati tra loro.
- Mentre in riferimento alle finestre, è consigliabile che i vetri siano antisfondamento, i telai siano ben ancorati al muro e infine sia presente un'adeguata protezione, meglio se all'interno.

Sia le vetrate che le finestre possono inoltre essere ulteriormente protette inserendo impianti di allarme 24 h su 24.

Il videocollegamento/la videosorveglianza

Gli impianti video, oltre che registrare le immagini, possono trasmetterle in diretta alla centrale operativa remota. La trasmissione può essere di tipo continuo o su evento.

Poiché il grado di attenzione dell'operatore non può rimanere elevato per tutto il tempo, le banche hanno deciso di concentrarsi sempre più verso la trasmissione su eventi anomali.

All'interno della filiale, normalmente all'ingresso e nel salone, sono presenti alcuni monitor sui quali viene visualizzata in maniera continuativa oppure su "evento anomalo" l'immagine dell'addetto alla sicurezza presente nella sala operativa che sta controllando la filiale. A fronte di una situazione anomala viene attivata una procedura di controllo ed eventuale gestione dell'emergenza.

La videoregistrazione

Come già affermato in precedenza, i sistemi di videoregistrazione sono da considerarsi obbligatori poiché costituiscono una risorsa preziosa per le Forze dell'ordine e le banche si devono perciò impegnare, per le nuove installazioni e per l'adeguamento delle preesistenti, ad utilizzare la tecnologia digitale, che col tempo sostituirà quella analogica in modo da garantire una migliore qualità delle immagini.

All'inizio degli anni Ottanta, l'uso di sistemi di videoregistrazione avevano condotto a degli inconvenienti poiché i delinquenti a seguito della rapina pretendevano che gli venissero consegnate le cassette registrate, impedendo così di riuscire a risalire all'attore del crimine. Per ovviare a tale inconveniente, le banche hanno deciso di custodire i videoregistratori in armadi di sicurezza dotate di serrature a tempo.

I sistemi di allarme

La maggior parte delle dipendenze bancarie è dotata di allarme antirapina e antifurto. Questi sistemi non sono altro che dei pulsanti o delle pedaliere che, in caso di attivazione, inviano un segnale di allarme alla Centrale Operativa delle Forze dell'ordine oppure di un Istituto di Vigilanza privata o della banca stessa; in questi ultimi due casi la segnalazione viene a sua volta indirizzata alle Forze dell'ordine.

L'opportunità di segnalare in tempo reale una rapina attraverso questi sistemi rappresenta un deterrente per i rapinatori. L'impianto di allarme, in orario extra lavorativo, oltre a proteggere i mezzi forti può avere una funzione antiintrusione, proteggendo i varchi perimetrali e le aree interne della banca. Tali dispositivi vengono generalmente collocati nell'ufficio del direttore, nei bagni, negli archivi e in tutti quei locali nei quali ci si potrebbe rifugiare in caso di emergenza.

Sistemi anticamuffamento

La maggior parte delle rapine viene eseguita da rapinatori col volto travisato già all'ingresso della filiale. Per tale ragione sono stati sviluppati dei sistemi anticamuffamento che rappresentano delle tecnologie di videoregistrazione dotate però di funzionalità speciali note come "funzionalità anticamuffamento".

Tale tecnologia consente, dunque, di impedire l'accesso in filiale a soggetti non chiaramente identificabili. Una volta avvenuto l'ingresso nella bussola la persona viene invitata a voltarsi per permettere l'inquadratura da più angolazioni da parte di una o più telecamere. Tale dispositivo consente di escludere la necessità dell'acquisizione del consenso scritto degli interessati in quanto effettua un trattamento dei "dati personali comuni" teso ad evitare un "camuffamento" del volto, senza richiedere il "riconoscimento" dell'identità della persona stessa. Si tratta di una tecnologia che a differenza del sistema biometrico non richiede la preventiva autorizzazione dell'Autorità Garante.

I banconi blindati/area blindata ad alta sicurezza

Solo un numero ristretto di dipendenze bancarie adotta questa particolare tipologia di protezione perché ritenuta meno agevole per l'esecuzione delle attività. L'apprestamento difensivo richiede soltanto che il personale tenga chiusa a chiave dall'interno la porta che mette in comunicazione il retroportello con il salone del pubblico. L'area blindata ad alta sicurezza invece non è altro che un'area protetta in cui effettuare le operazioni a maggior rischio rapina quali caricamento ATM, apertura bossoli cassa continua, ecc..

I sistemi per la gestione del contante

Esistono tre tipologie di strumenti per la gestione del contante:

1. Cassettiere semplici temporizzate, con un solo scomparto ad apertura ritardata
2. Cassettiere multiple temporizzate dotate di più scomparti ad apertura ritardata
3. Erogatori automatici per cassieri: verificano e immagazzinano automaticamente le banconote e, sempre in modo automatico, provvedono a erogarlo in caso di prelievo.

I dispositivi a tempo possono essere a loro volta distinti in:

- ritardatori di apertura (time-delay), che consentono l'apertura dei mezzi forti solo dopo

un lasso di tempo predeterminato dal momento dell'attivazione dei relativi congegni. I ritardatori di apertura trovano applicazione in orario di lavoro;

- serrature a tempo (time-lock), che impediscono l'apertura dei mezzi forti fino a quando non sia trascorso un lasso di tempo impostato di volta in volta o programmato in precedenza. Essi sono utilizzati in orario di chiusura delle banche.

La centralizzazione dei mezzi forti

Generalmente questa tipologia di misura difensiva viene utilizzata in combinazione con la centralizzazione degli allarmi video. Il sistema consente di monitorare i mezzi forti da una postazione remota, monitorarne lo stato, inviarne comandi, modificare parametri ed effettuare attività di diagnostica in tempo reale. La connessione tra i sistemi (mezzi forti) facenti parte dell'impianto e la postazione remota, avviene utilizzando il protocollo TCP/IP su rete dedicata ethernet.

Le mazzette fumogene o sistema di macchiatura delle banconote

Si tratta di banconote false all'interno delle quali vengono inserite delle microcariche che si attivano automaticamente una volta portate fuori dalla dipendenza bancaria, rendendo quindi i valori rapinati inutilizzabili. Questa tipologia di misura risulta essere un buon deterrente per i rapinatori.

La tracciabilità delle banconote

Si tratta di un dispositivo di localizzazione e tracciabilità satellitare ultraminiaturizzato che viene nascosto all'interno di una falsa mazzetta di banconote. Quest'ultima appare identica ad una vera mazzetta. Il dispositivo di localizzazione è in grado di tracciare la posizione geografica in maniera puntuale e segnalarla ad una Centrale Operativa.

Il funzionamento è il seguente: una volta definita l'ubicazione della mazzetta (cassetto, ripiano, ecc.) questa non deve essere più spostata. Un semplice spostamento causa l'invio di un segnale di allarme ad una Centrale Operativa delle Forze dell'ordine oppure di un Istituto di Vigilanza privata o della banca stessa. L'uscita dall'agenzia garantisce la tracciatura in continuo tramite sistemi satellitari, pertanto la sua posizione geografica è costantemente disponibile.

La formazione anticrimine

Si tratta di una misura di carattere "organizzativo". Ha l'obiettivo di prevenire, contrastare e, qualora la rapina sia consumata, di limitare i danni dell'evento criminoso. La formazione è rivolta ai responsabili della filiale e della gestione dei valori. I contenuti della formazione riguardano i comportamenti da adottare prima, durante e dopo un evento criminoso.

Ulteriori interventi riguardano la specifica normativa in materia di sicurezza e una panoramica sulle aree a maggior rischio rapina evidenziando i dati statistici sul numero di rapine tentate e consumate in una determinata area.

3.3 Analisi della situazione attuale: La percezione della sicurezza dei clienti. Un'indagine campionaria.

L'indagine sulla sicurezza e sul rischio rapina è stata realizzata somministrando un questionario strutturato ad alternative fisse predeterminate tramite metodologia C.A.T.I. (Computer Assisted Telephone Interviewing) ad un campione di 857 cittadini italiani maggiorenni. L'indagine è stata condotta su un campione rappresentativo della popolazione residente nazionale, ed ha riguardato l'analisi del sentiment (opinioni e atteggiamenti) dei cittadini italiani sulle condizioni di sicurezza connesse alla situazione sociale ed ambientale locale, l'analisi delle esperienze dirette di criminalità predatoria, ossia furti, estorsioni, ed in particolare delle rapine in banca, per poi focalizzarsi sui temi della security e safety bancaria.

Gli aspetti metodologici hanno assunto un'importanza strategica al fine di raggiungere pienamente gli obiettivi proposti dal piano della ricerca. Lo strumento d'indagine è un questionario anonimo che ha consentito a ciascun intervistato di esprimersi liberamente, formulando giudizi e fornendo opinioni in merito alle tematiche trattate. L'indagine è stata strutturata in moduli, è concepita come insieme di sezioni tematiche autonome, trovando compimento nell'unità metodologica, nell'omogeneità e nella complementarità delle tematiche affrontate negli stessi.

La ricerca, nello specifico, è stata articolata nelle seguenti fasi:

- Desk analysis
- Piano di campionamento
- Progettazione e costruzione del questionario
- Pretest, correzione, eventuale revisione e aggiornamento del questionario
- Somministrazione dei questionari
- Elaborazione, interpretazione e analisi dei risultati

Desk analysis - Questa fase preliminare di studio, ci ha consentito di delineare e valutare la situazione generale relativa al fenomeno oggetto di indagine. A tal fine è stata presa in esame la rassegna stampa dei principali quotidiani specializzati relativa all'ambito della ricerca, circoscritta agli ultimi anni e una grande quantità di dati secondari forniti dai principali istituti di ricerca, le principali fonti statistico-documentali, i volumi Istat, una serie di fonti Internet da cui estrapolare il maggior numero di informazioni possibili. Si è trattato di reperire e analizzare materiali prodotti da studi recenti condotti aventi per oggetto l'analisi dei fenomeni oggetto di studio. Si precisa che tale attività di studio preliminare è stata strumentale alla progettazione, testing e redazione finale dello strumento di rilevazione (questionario).

Piano di campionamento - Nell'obiettivo di analizzare la situazione in tempi brevi, si è reso necessario il ricorso dell'estrazione di un campione rappresentativo della popolazione italiana. Per questo tipo di indagine è stato estratto un campione probabilistico di tipo casuale stratificato, che consente l'inferenza campione-popolazione. Questo sottoinsieme dovrebbe rappresentare adeguatamente la popolazione globale, nel senso che l'informazione ottenuta esaminando lo stesso dovrebbe possedere lo stesso grado di accuratezza di quella che avremmo ottenuto esaminando l'intera popolazione. L'universo di riferimento è rappresentato dai cittadini italiani maggiorenni (50.624.663) residenti nel territorio italiano secondo gli ultimi dati ISTAT 2014. Il campione estratto è stato pari a 857 cittadini e stratificato per le principali variabili ritenute fondamentali per una ricerca di tipo esplorativo–descrittivo, ossia:

- Sesso,
- Età, attraverso le fasce: giovani (18-35 anni), adulti (36-64 anni) ed anziani (65 anni e oltre).
- Area di residenza dei cittadini. Per mantenere una congrua dimensione dei sottocampioni indagati, è stata prevista una disaggregazione del campione nelle 5 aree principali geografiche della popolazione italiana secondo la classificazione ufficiale ISTAT: Nord ovest, Nord est, Centro, Sud, Isole. Inoltre, tra le variabili strutturali è stata prevista anche la condizione occupazionale e professionale e il titolo di studio che ha consentito ulteriori utili approfondimenti sull'orientamento e la percezione dell'universo di riferimento.

Margine di errore - Con il campione utilizzato (857 casi) si calcola un margine di errore massimo sul totale dei casi del + 3,3%, al livello di confidenza del 95%.

Progettazione e costruzione del questionario - Lo strumento di rilevazione, un questionario per l'appunto, dopo essere stato opportunamente strutturato sulla base delle indicazioni raccolte in fase preliminare e testato (fase pilota), è stato articolato in diverse aree tematiche, per ognuna delle è stato possibile raccogliere numerose informazioni.

Somministrazione dei questionari - La somministrazione dei questionari è avvenuta con la tecnica "CATI" (Computer Aided Telephone Inquiry) che utilizza il computer per guidare l'intervista, effettuata telefonicamente. Tale tecnica ha consentito in effetti un notevole sveltimento dei tempi di intervista ed una minimizzazione della caduta di risposta. Occorre precisare che sebbene tali metodologie di rilevazione non offrano garanzie assolute su eventuali azioni di condizionamento nel fornire le risposte (eventualità scongiurata da un'adeguata formazione degli intervistatori), molto spesso assicura una maggiore polarizzazione dei risultati rispetto alle altre modalità di somministrazione.

Elaborazione, interpretazione e analisi dei risultati - L'elaborazione, l'analisi e interpretazione dei risultati, costituisce la fase culminante e finale della ricerca. I dati raccolti attraverso la somministrazione del questionario, sono stati immessi ed elaborati per mezzo del package statistico SPSS

Di seguito l'identikit del campione d'indagine:

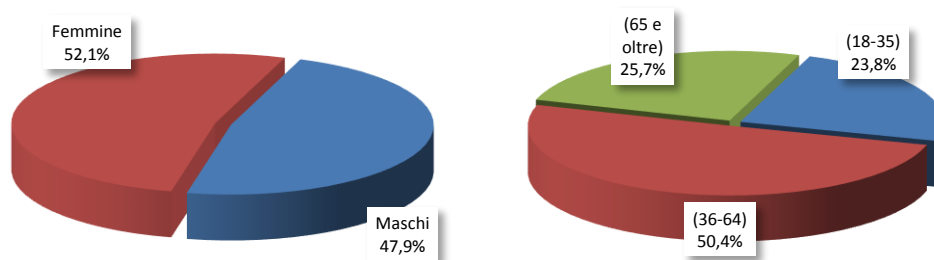


Figura 47. Ripartizione del campione per sesso ed età del campione. Valori percentuali

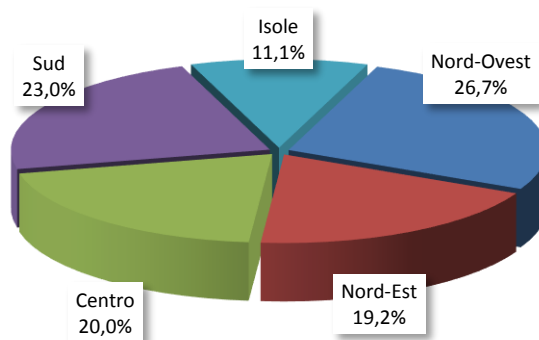


Figura 48. Ripartizione del campione per area geografica. Valori percentuali

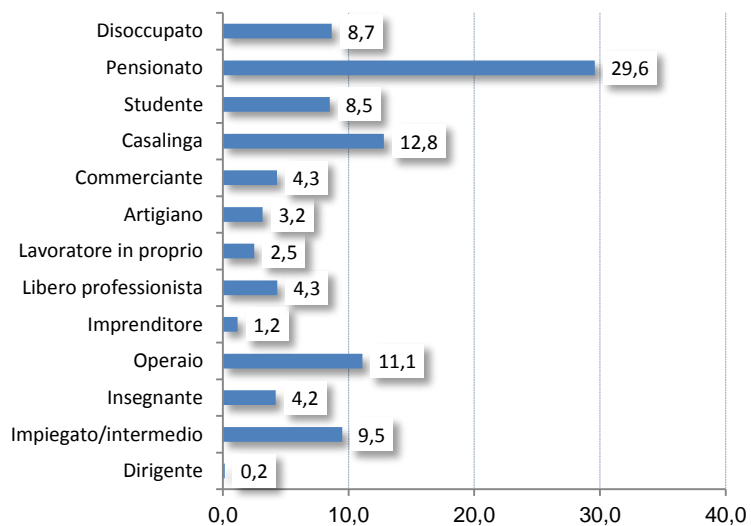


Figura 49. Ripartizione del campione per condizione professionale. Valori percentuali

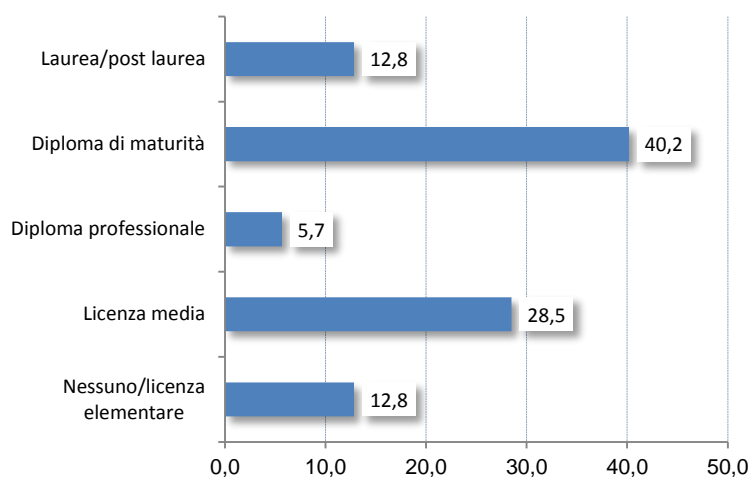


Figura 50. Ripartizione del campione per titolo di studio. Valori percentuali

3.3.1 La percezione della sicurezza

La percezione di sicurezza può essere interpretata come uno stato dell'anima individuale che risente degli atteggiamenti e dei sentimenti diffusi tra la popolazione e che non necessariamente risultano coerenti con l'andamento dei reati. In altre parole, può succedere che, in un determinato periodo o in un determinato territorio, i reati crescano ma la paura rimanga stazionaria e in un altro che l'allarme sociale aumenti pur essendo in presenza di una riduzione nel numero dei reati. Quali che siano le determinanti dell'allarme sociale, in questo momento il problema della sicurezza urbana è tra le preoccupazioni più sentite dalla

popolazione, per cui la paura rischia di diffondersi, trascinando con sé sfiducia nelle istituzioni, vittimismo esasperato, pessimismo che investe anche altre sfere della vita quotidiana ⁷.

Come premesso l'indagine parte con una prima batteria di domande tesa a rilevare la percezione del livello di sicurezza o insicurezza connesse alla situazione sociale ed ambientale locale.

Il primo dato che emerge è relativo all'andamento percepito dei reati negli ultimi anni, rispetto al quale il campione di soggetti intervistato appare quasi diviso tra quanti ritengono ci sia stato un incremento della criminalità (47,8%) e quanti, invece, segnalano una situazione di sostanziale stabilità (46,5%) con nessun cambiamento degno di nota, mentre sul fronte opposto una quota poco rilevante, appena il 5,7%, è del parere che c'è stato un miglioramento ravvisando una contrazione del fenomeno.

Modalità di risposta	ITALIA	Nord	Centro	Sud	MASCHI	FEMMINE	GIOVANI	ADULTI	ANZIANI
I reati sono molto diminuiti	2,0	1,1	0,8	3,9	2,4	1,6	2,1	2,6	0,6
I reati sono diminuiti	3,7	2,9	2,5	5,4	4,2	3,2	3,5	3,3	4,5
I reati sono rimasti stabili	46,5	48,4	43,0	46,1	44,8	48,1	44,1	48,0	45,8
I reati sono aumentati	42,5	41,8	47,9	40,2	44,8	40,4	48,3	40,4	41,3
I reati sono molto aumentati	5,3	5,8	5,8	4,4	3,8	6,7	2,1	5,6	7,7
Totale	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0

Tabella 20. Qual è la sua percezione sull'andamento dei reati negli ultimi anni?

A livello territoriale si nota che è nel Centro Italia che si avverte in maniera significativa un aumento dei fatti delittuosi (53,7%) rispetto alle altre 2 aree due macroaree, Nord con il 47,6% e Sud, che con il 44,6% presenta il valore più contenuto di persone che avvertono un peggioramento. Il genere non differenzia in modo significativo queste percezioni, mentre per la variabile età, la percezione di un peggioramento del grado di sicurezza sociale viene avvertito in particolare dalle classi più giovani (50,4%) e più anziane (49%) mentre gli adulti non segnalano particolari cambiamenti in atto (48%). Allo stesso modo gli abitanti con un medio (49,3%) e basso (47,9%) status professionale e livello di reddito ritengono in aumento i reati in modo più consistente, mentre quelli appartenenti al livello alto enfatizzano maggiormente una situazione di sostanziale stabilità (55,9%). Si riscontrano, infine, maggiori quote di soggetti preoccupati per l'aumento della criminalità tra i laureati (49,4%) (livello alto) e tra quanti hanno più bassi gradi di istruzione (49,2%). Approfondendo ulteriormente il dato sulla percezione della sicurezza alla domanda "...si sente sicuro in città quando è da solo", il 16,8% dichiara di sentirsi

⁷ Cfr. Università Cattolica del Sacro Cuore di Piacenza – Facoltà di Economica, in Laboratorio di Economia Locale, *Diagnosi locale di Sicurezza, Indagine sui bisogni di sicurezza di Piacenza*, Comune di Piacenza, 2009.

“sempre insicuro” mentre una quota analoga, il 17,5% dichiara di sentirsi non sicuri ma solo di notte e solo in alcune zone ritenute pericolose.

3.3.2 I reati subiti

Il tema della sicurezza è da sempre oggetto di dibattito all'interno della letteratura scientifica internazionale. I ricercatori hanno trovato accordo nel definire due dimensioni principali nel senso di insicurezza: il *fear of crime*, riferibile alla paura personale della criminalità, ed il *concern about crime*, ovvero la preoccupazione sociale per la criminalità. Le diverse forme di criminalità si possono distinguere, in linea teorica, tra quelle legate alla persona (ad es. omicidio, aggressione) e quelle legate al patrimonio (ad es. furto, borseggio). Quest'ultima viene anche classificata come criminalità predatoria. Essa sembra incidere, secondo diversi studi (es. Hough, 1985; Maguire, 1980), sulle variazioni del *fear of crime*. Infatti, ricerche svolte da Maguire (1980), sui furti in appartamento, hanno dimostrato: "...che il danno psicologico derivante dal furto è percepito dalle vittime come più grave rispetto alla perdita della proprietà o al danno economico, e che le donne risentono delle conseguenze di questo reato più degli uomini" (Bandini et al., 1991, p.342). Passando dai dati di percezione e *sentiment* a quelli oggettivi sui reati effettivamente subiti, emerge come il 13,7% dei cittadini nell'ultimo anno sia stato vittima di un reato e il 3% anche di più di uno. Non si osservano particolari differenze di genere e di età ma l'analisi per lo status lavorativo e professionale e il grado di istruzione evidenzia delle differenziazioni. Così mentre nel primo caso risultano vittime di reati in misura relativamente maggiore i soggetti che si collocano in un alto status professionale e lavorativo (35,3% contro il 14,5% del livello basso), nel secondo caso sono i cittadini con alto livello di istruzione ad essere maggiormente penalizzati (27,3% vs l'8,4% del livello basso). Ancora una volta incide anche la residenza, con i cittadini del centro Italia più colpiti, circa il 20% a fronte del 15,3% del Nord e del 16,7% del Sud.

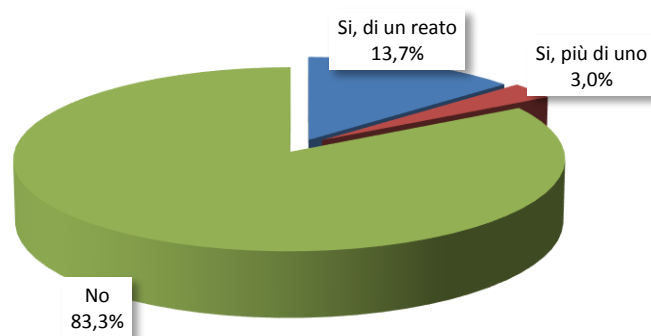


Figura 51. E' stato/a vittima di reato nella sua città nell'ultimo anno?

Allargando l'orizzonte temporale, è stato chiesto al nostro campione di cittadini italiani di elencarci i reati, principalmente di natura predatoria, che ha subito negli ultimi tre anni. Ai soggetti intervistati, è stata data la facoltà di indicare più di un reato pertanto il totale delle modalità di risposta è diverso da cento. Il primo dato rilevante che emerge è relativo alla quota

di soggetti che è stata vittima di reati nell'ultimo triennio che è pari al 27,3%, in linea con i dati precedenti tale quota tende a crescere tra i gli abitanti residenti nelle regioni del centro Italia, attestandosi al 36,4%. Dall'osservazione delle tabelle seguenti, si evince subito che rispetto alle diverse tipologie di reati, il più diffuso è il furto in casa (14,8%) in tutte le aree di residenza degli intervistati, con il picco maggiore (19,8%) nel centro Italia, e che vede ancora come vittime privilegiate principalmente gli anziani con il 20,6% dei casi. A seguire i borseggi e gli scippi con il 7,7% e i furti con la presenza di persone in casa, il 6,8%, anche in questo caso si rilevano percentuali maggiori fra le classi più anziane, soprattutto per la seconda tipologia di reato, l'11%. Meno rilevanti i reati più gravi che costituiscono vere minacce fisiche per coloro che ne risultano vittime (rapine a mano armata, aggressioni, estorsioni).

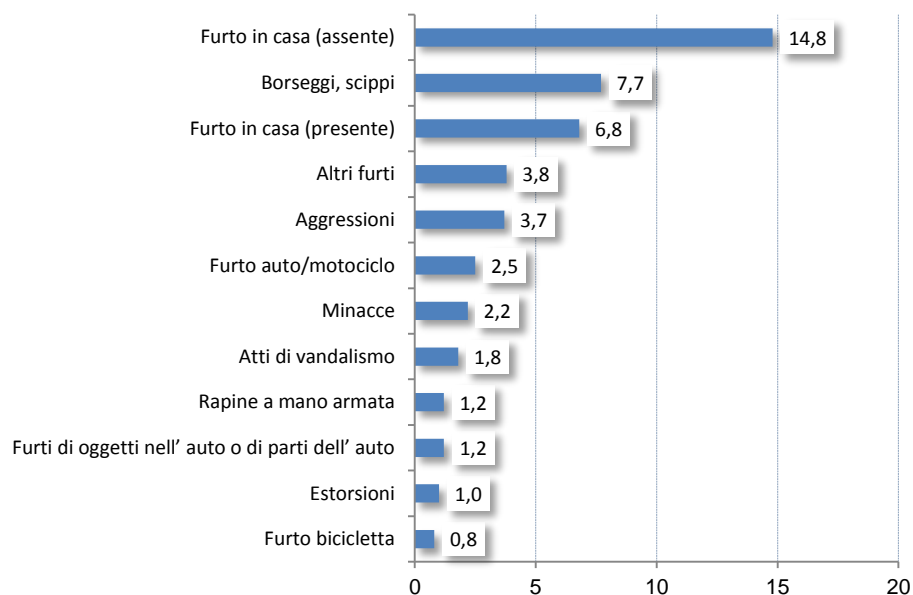


Figura 52. Quali reati ha subito nella sua città negli ultimi tre anni?

3.3.3 Le rapine in banca

Dopo avere analizzato i reati di natura principalmente predatoria subiti dagli italiani negli ultimi anni, in questo paragrafo l'attenzione si focalizza più specificatamente sull'analisi delle esperienze dirette di rapina e tentata rapina subite presso le dipendenze bancarie, ponendo

particolare attenzione alle opinioni e alle percezioni dei soggetti intervistati sull'adeguatezza ed efficienza dei sistemi e i servizi di sicurezza adottati dalle banche.

In linea con il dato quantitativo generale del numero dei reati più gravi che costituiscono vere minacce fisiche per coloro che ne risultano vittime (rapine a mano armata, aggressioni, estorsioni) che come abbiamo appena evidenziato è poco rilevante, si evidenzia che anche quello delle rapine e tentate rapine in banca ha riguardato un numero ridotto di casi, vale a dire il 2% del totale campione. Suddividendo le risposte per le principali variabili strutturali e socio-anagrafiche, area, sesso ed età, del campione intervistato non si registrano differenze degna di nota.

Modalità di risposta	ITALIA	Nord	Centro	Sud	Maschi	Femmine	Giovani	Adulti	Anziani
Si	2,0	2,2	0,8	2,5	1,7	2,2	0,7	2,6	1,9
No, mai	98,0	97,8	99,2	97,5	98,3	97,8	99,3	97,4	98,1
Totale	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0

Tabella 21. In particolare si è mai trovata a subire e/o assistere ad una rapina o tentata rapina in banca?

Al sottocampione dei soggetti che ha dichiarato di essere stato vittima o "spettatore" di una rapina o tentata rapina in banca è stato chiesto di formulare un giudizio sul livello di efficienza ed efficacia dei sistemi di sicurezza e di protezione in dotazione e sull'intervento e le azioni di difesa posti in essere dal personale addetto alla sicurezza per sventare l'evento criminoso. Rispetto ai primi il parere degli intervistati è per lo più negativo: il 41,7% ha difatti evidenziato che i sistemi antirapina sono risultati "poco adeguati" a cui sommando il 16,7% di chi li ha ritenuti "poco adeguati" si arriva ad un valore del 58,4%, minori, dunque, le percentuali di quanti esprimono soddisfazione ritenendoli "abbastanza" (24,2%) e "molto" adeguati (9,2%).

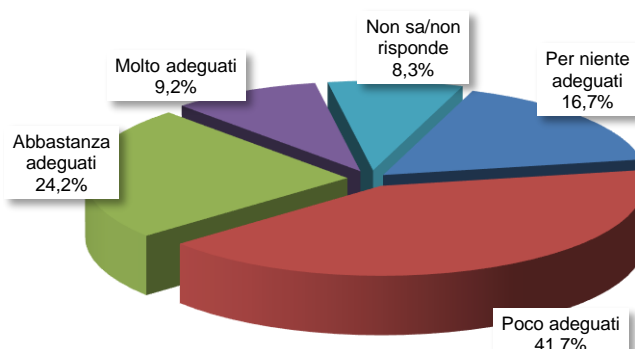


Figura 53. Percezione dell'adeguatezza dei sistemi di sicurezza e protezione

Giudizio più bilanciato è stato espresso per il personale addetto alla sicurezza, per il quale comunque la parte maggiore degli intervistati ha riservato una valutazione di insufficienza, ossia di totale assenza (25%) o poca 17,1% preparazione (25%) nel gestire gli eventi e

fronteggiare il pericolo derivante dall'azione criminosa. Non mancano anche in questo caso i giudizi positivi: il 32,8% è del parere che gli addetti alla vigilanza hanno dimostrato abbastanza (16,5%) e molta (16,3%) preparazione nel contrastare i rapinatori e più in generale a gestire l'evento delinquenziale.

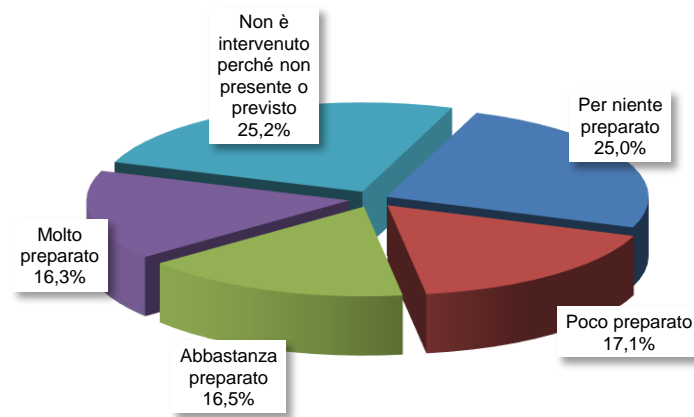


Figura 54. Percezione dell'adeguatezza del personale addetto alla sicurezza

Infine, le valutazioni espresse nei confronti del personale della banca, anche in questo caso c'è una prevalenza di giudizi negativi, quasi il 60% delle vittime di rapina è convinto della totale mancanza (25,6%) e della scarsa preparazione (33,3%) del personale della banca, mentre solo un terzo è certo invece che il 34,2% del personale era abbastanza e il 6,8% molto preparato.

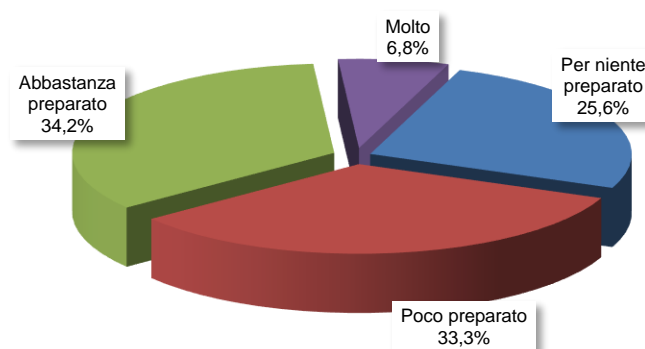


Figura 55. Percezione dell'adeguatezza del personale di filiale

Infine, con l'ultima domanda si è cercato di comprendere se, secondo l'opinione degli intervistati, al di là dell'evento subito, i sistemi di protezione e di sicurezza attuali, adottati dalla

banche, siano in grado di scongiurare o prevenire il rischio rapina o al contrario siano considerati scarsamente efficaci e comunque non idonei ad evitare che tali eventi criminosi accadano. Dalla distribuzione delle percentuali di risposta si evince che, nonostante il campione appare diviso sui sistemi di difesa da adottare, la gran parte degli intervistati (oltre i due terzi, il 67,3%) è del parere che comunque questi, se correttamente ed adeguatamente utilizzati, hanno la loro efficacia e sono in grado di impedire o quantomeno di prevenire le rapine presso le dipendenze bancarie. In particolare il 33,1% è convinto della validità ed efficacia dei sistemi di sicurezza e video sorveglianza, mentre il 34,2% è dell'avviso che era possibile sventare la rapina attraverso un maggiore preparazione e/o maggiore impiego di personale addetto alla sorveglianza della banca. Sul fronte opposto troviamo gli scettici, che rappresentano il 32,7%, convinti che nessun sistema, sarebbe stato in grado di evitare l'azione dei rapinatori.

Modalità di risposta	%
Si, soprattutto se ci fossero stati adeguati sistemi di sicurezza (es. all'entrata) di video sorveglianza e altri strumenti di protezione antirapina	33,1
Si, soprattutto attraverso personale addetto alla sicurezza e vigilanza all'entrata della banca (guardia giurata)	34,2
No, non si poteva evitare	32,7
Totale	100,0

(*) Valori riferiti al sottocampione di soggetti che hanno subito la rapina

Tabella 22. In generale si poteva evitare la rapina o la tentata rapina?

La stessa domanda è stata rivolta anche al sottocampione più numeroso, di soggetti che hanno dichiarato di non essere mai stati vittima o spettatori di rapine in banca. Anche in questo caso si registra una prevalenza (71,3%) di quanti sono del parere che prendendo le dovute precauzioni e adottando sistemi più adeguati (29,3%) e soprattutto personale addetto alla sicurezza più preparato (42%) è possibile fronteggiare efficacemente questi eventi criminosi. Ad esserne maggiormente convinti sono i cittadini del centro Italia (80%), i maschi (73,9%) e i le persone più anziane d'età (76,3%). Più contenute, dunque, ma non per questo non rilevanti, le percentuali di quanti sono del parere contrario che rappresentano in questo caso il 28,7% dei rispondenti.

Modalità di risposta	%
----------------------	---

Modalità di risposta	%
Si, soprattutto con adeguati sistemi di sicurezza (es. all'entrata) di video sorveglianza e altri strumenti di protezione antirapina	29,3
Si, soprattutto attraverso personale addetto alla sicurezza e vigilanza all'entrata della banca (guardia giurata)	42,0
No, non si possono evitare comunque	28,7
Totale	100,0

(*) Valori riferiti al sottocampione che non ha mai subito alcuna rapina.

Tabella 23. In generale secondo la sua opinione si possono evitare le rapine o i tentativi di rapina?

3.3.4 Prevenzione e mitigazione del rischio rapina

L'ultima batteria di domande aveva l'obiettivo di rilevare sia gli interventi diretti sia quelli indiretti che secondo gli intervistati sarebbero stati necessari per prevenire e mitigare il rischio rapina nel proprio territorio. Emerge subito un dato rilevante, ossia che oltre un terzo, il 35,3%, si concentra sulla tipologia di intervento "indiretto", ritenendo come provvedimento necessario e dunque prioritario, aumentare il presidio del territorio da parte delle forze dell'ordine, solo agendo in questa direzione si potrà contrastare con forza il fenomeno.

Pochi invece sono convinti, appena l'8,1%, sull'adozione di un altro provvedimento indiretto molto importante, ovvero la limitazione dell'uso del contante, che se applicato e diffuso in tutte le transazioni monetarie potrebbe scoraggiare e combattere definitivamente questo tipologia di reati. Sul fronte opposto i fautori dei provvedimenti "diretti" che sono invece dell'avviso che occorre in ogni caso potenziare i sistemi di sicurezza e di videosorveglianza (28,5%) e aumentare o prevedere laddove non presenti personale addetto alla sicurezza e sorveglianza (27,1%).

Modalità di risposta	%
Potenziare i sistemi di sicurezza (es. all'entrata) di video sorveglianza e altri strumenti di protezione antirapina	28,5
Aumentare o prevedere (laddove non presente) personale addetto alla sicurezza e sorveglianza all'entrata della banca (guardia giurata)	28,1
Limitare al massimo l'uso del contante	8,1
Aumentare in generale il presidio del territorio da parte delle forze dell'ordine	35,3
Totale	100,0

Tabella 24. Quanto ritiene importanti i seguenti interventi al fine di evitare il rischio rapina nel territorio?

Non si osservano particolari differenze di genere e di età e per area geografica e come pure l'analisi per lo status lavorativo e professionale e il grado di istruzione non evidenzia delle grandi divergenze di opinione almeno per quanto concerne la suddivisione tra interventi diretti che indiretti. Tuttavia è interessante osservare alcune differenziazioni all'interno delle due macro categorie individuate. Considerando la variabile geografica, i cittadini del Sud e del Centro propendono maggiormente per interventi diretti a rafforzare ed aumentare il personale addetto alla sicurezza e sorveglianza (guardie giurate), mentre i cittadini del Nord sono più convinti che occorre limitare l'uso del contante, così come gli intervistati più giovani e quanti si trovano in uno status professionale e lavorativo alto, mentre gli anziani e coloro che possiedono un basso grado di istruzione sono più propensi a rafforzare il presidio del territorio da parte delle forze dell'ordine.

Modalità di risposta	Nord	Centro	Sud
Potenziare i sistemi di sicurezza (es. all'entrata) di video sorveglianza e altri strumenti di protezione antirapina	28,1	26,9	29,9
Aumentare o prevedere (laddove non presente) personale addetto alla sicurezza e sorveglianza all'entrata della banca (guardia giurata)	25,9	29,3	30,2
Limitare al massimo l'uso del contante	10,2	6,6	6,4
Aumentare in generale il presidio del territorio da parte delle forze dell'ordine	35,8	37,2	33,5
Totale	100,0	100,0	100,0

Tabella 25. Quanto ritiene importanti i seguenti interventi al fine di evitare il rischio rapina nel territorio? (per area geografica)

Un altro aspetto molto importante da considerare riguarda le gravi conseguenze subite o che possono subire le persone, sia i dipendenti della banca sia la clientela, presenti durante e dopo la rapina.

Sappiamo che ogni gesto di reazione ai rapinatori può comportare pericoli gravissimi non solo per chi reagisce, ma anche per tutti gli altri presenti; non bisogna dimenticare come ogni rapina rappresenti di per se un evento potenzialmente mortale. Dunque, l'evento criminoso, può avere degli effetti e dei risvolti psichici e fisici gravissimi per tutti i soggetti coinvolti.

È stato, inoltre, dimostrato da più studiosi che tale tipologia di eventi provoca notevoli danni psicologici ed emotivi alla vittima che possono permanere anche per lungo tempo, da qui l'importanza degli aspetti e degli effetti non solo economici di tali tipo di reati ma soprattutto sociali e psicologici che spesso hanno un'incidenza ben più rilevante che non bisogna assolutamente sottovalutare.

C'è da dire che lo studio di tali problematiche, ossia degli effetti che produce la rapina nelle persone che la subiscono e quali siano le misure e gli interventi attivati dalle banche per affrontare l'evento e la loro efficacia, e più in generale il tema della sicurezza, sono già da tempo oggetto di attenzione da parte del sistema bancario. Una recente ricerca realizzata nell'ambito di OSSIF, il Centro di Ricerca dell'ABI sulla sicurezza, in collaborazione con esperti del settore, ha fornito alcune interessanti risposte ai quesiti, ponendo l'accento sulla necessità di perseguire, nel futuro, l'obiettivo di armonizzare, ove possibile, le procedure e le strategie messe in campo dalle banche sul tema del rischio rapina. Il lavoro ha fatto riferimento alle Linee di indirizzo per prevenire o ridurre i danni fisici e psichici dei lavoratori bancari correlati alle rapine, elaborate dal Coordinamento tecnico interregionale (organismo tecnico della Conferenza delle regioni e delle province autonome).

La ricerca nel ribadire la complessità di approccio multidisciplinare necessario per affrontare le problematiche della sicurezza e del rischio rapina, conferma l'importanza della stretta collaborazione tra le funzioni di security e di safety, talvolta percepite - ancora in molti ambiti - distinte e separate. Si legge nella ricerca che, infatti, il rischio del verificarsi di una rapina è di competenza della funzione security, per il rischio di traumi/danni fisici e psichici a seguito dell'evento rapina la competenza è dei servizi aziendali di prevenzione e protezione, cioè della funzione safety.

Sulla scorta di queste considerazioni è stato chiesto agli intervistati di esprimere un parere sull'importanza degli interventi attuati o da attuare ai fini della prevenzione dei rischi e delle eventuali conseguenze connesse al verificarsi dell'evento rapina. Dall'analisi delle risposte fornite dal nostro campione emerge con evidenza una rilevante importanza per tutti gli interventi proposti, tuttavia viene posto l'accento su un intervento in particolare: intraprendere e attivare azioni formative più mirate ai dipendenti delle banche sulle dinamiche psicologiche e comportamentali da adottare nel caso in cui si subisca l'evento criminoso, ben l'87,3% degli intervistati reputa tali tipologie di intervento "abbastanza" e "molto importanti". A seguire, il 75,9% indica come rilevanti e necessarie ai fini della prevenzione, attività informative più mirate da rivolgere ai clienti attraverso diverse modalità e strumenti diversi (sito internet, e-mail, news, guide informative, ecc.), sui comportamenti da tenere durante la rapina, mentre meno importante ma non per questo poco rilevante, il 63,9%, è la quota di quanti insistono sulle attività informative in questo caso indirizzate ai dipendenti delle banche, attraverso le diverse modalità disponibili (rete intranet aziendale, e-mail aziendali, news, guide informative, ecc.). Non si osservano particolari differenze di genere e di età e per area geografica e come pure l'analisi per lo status lavorativo e professionale e il grado di istruzione non evidenzia rilevanti divergenze di opinione sull'importanza delle azioni di prevenzione del rischio rapina.

Modalità di risposta	Per niente	Poco	Abbastanza	Molto	Totale
Formare adeguatamente il personale addetto delle banche sulle dinamiche psicologiche e comportamentali da	3,8	8,8	37,5	49,8	100,0

Modalità di risposta	Per niente	Poco	Abbastanza	Molto	Totale
adottare nel caso in cui si subisca l'evento criminoso					
Fornire maggiori informazioni ai dipendenti attraverso diverse modalità e strumenti diversi (rete intranet aziendale, e-mail aziendali, news, guide informative, ecc.)	8,2	28,7	36,5	26,7	100,0
Fornire informazione anche ai clienti sui comportamenti da tenere durante la rapina attraverso diverse modalità e strumenti diversi (sito internet, e-mail, news, guide informative, ecc.)	6,8	17,3	30,7	45,2	100,0

Tabella 26. Quanto ritiene importanti i seguenti interventi ai fini della prevenzione dei rischi e delle eventuali conseguenze connessi al verificarsi dell'evento rapina?

3.4 Focus group sui sistemi e le misure di sicurezza bancaria

Le azioni di ricerca mirano ad analizzare in profondità il fenomeno dei reati ai danni delle dipendenze bancarie (rapine, furti, danneggiamenti, frodi, ecc.) indagando sull'evoluzione dei sistemi di protezione e di sicurezza in linea con il fine ultimo della ricerca che è l'individuazione di un pacchetto integrato di strumenti tecnologici e misure organizzative in grado di mitigare e contrastare il rischio dell'accadimento di tali eventi criminosi. Nel rispetto di queste finalità, il *Focus Group* realizzato presso la sede del Liason Office dell'Università l'Università della Calabria a Rende, aveva come scopo principale quello di raccogliere le opinioni e gli orientamenti e giudizi di opinion leader ed esperti del settore sulla bontà, efficacia ed efficienza di tali misure, strumenti e interventi integrati. In quest'ottica, l'approccio progettuale ha consentito di chiarire, attraverso una logica comparativa tra gli interlocutori, i punti di forza e di debolezza oltre a possibili linee correttive di intervento. In particolare sono state esplorate le conoscenze che i partecipanti hanno nei confronti del mondo della sicurezza bancaria, esperienze, orientamenti prevalenti.

In particolare il focus era diretto principalmente a:

- ✓ Raccogliere opinioni e orientamenti dei partecipanti rispetto alle tematiche «sensibili» quali la sicurezza e prevenzione dei reati a danno delle banche anche alla luce anche dei risultati delle indagini desk e campionaria
- ✓ Individuare punti di forza e debolezza del pacchetto degli strumenti proposti
- ✓ Verificare adeguatezza, efficienza ed efficacia dei sistemi di sicurezza proposti alla luce delle considerazioni degli esperti
- ✓ Raccogliere eventuali suggerimenti e indicazioni utili ai fini di un corretta applicazione degli strumenti e misure organizzative proposte

- ✓ Definire gli eventuali correttivi alla luce delle considerazioni e delle critiche mosse dagli esperti ai fini dell'implementazione di azioni di miglioramento

Il Focus Group ha previsto la partecipazione di 9 soggetti scelti tra opinion leader altamente qualificati del settore della sicurezza pubblica e privata e altri soggetti sensibili alle tematiche oggetto d'indagine, che ha consentito di raccogliere un significativo numero di informazioni sugli item oggetto dell'osservazione. I soggetti sono stati selezionati in base a determinate caratteristiche in comune che li mettessero in relazione alla tematica della ricerca. Le risultanti del focus potranno essere utilizzate in una fase preliminare di ricerca come attività esplorativa per generare o mettere alla prova nuove ipotesi, oppure per individuare argomenti e concetti da adottare in un secondo momento come ausilio alla progettazione e all'utilizzo di altre tecniche di ricerca. Ad ogni modo, il processo di realizzazione del focus group si è svolto attraverso tre fasi:

- 1) progettazione della discussione;
- 2) realizzazione della discussione;
- 3) analisi dei dati raccolti.

L'indagine è stata, nel dettaglio, caratterizzata da una prima parte della discussione in cui si è rilevato l'approccio conoscitivo e la percezione che i partecipanti hanno in generale della sicurezza del territorio e dell'andamento e diffusione dei reati di natura predatoria ed in particolare di quelli a danno delle banche (rapine, furti, danneggiamenti, frodi, ecc.). Una seconda parte che ha rappresentato il nucleo centrale della discussione mirata ad indagare il livello di conoscenza dei sistemi e misure di sicurezza adottate dalle banche e in particolare a rilevare il parere e l'opinione dei partecipanti sull'efficacia, livello di fattibilità, criticità e vantaggi (punti di forza e debolezza) del pacchetto integrato di sicurezza che verrà proposto. La seconda parte del focus invece è stata orientata a valutare le soluzioni tecnologiche ed organizzative che vengono proposte in questa iniziativa. La fase di progettazione per la buona riuscita del focus è molto importante per cui è stata condotta con cura soprattutto per quanto riguarda la definizione degli obiettivi di ricerca. Tale attenzione ha permesso infatti di identificare l'argomento portante dell'incontro, stabilendo un accurato taglio tematico e consentendo in questo modo un'adeguata partecipazione dei soggetti e una buona qualità dei risultati. Pertanto in fase di pianificazione del focus gli obiettivi attesi sono stati definiti effettuando un'analisi del contesto e costruendo delle ipotesi di lavoro, nella successiva definizione dell'intervento è stata individuato il pubblico di riferimento, delineata la struttura dell'intervista e la composizione del gruppo rispetto alla numerosità e alle variabili prese in considerazione. Per quanto riguarda la struttura dell'intervista è stata adottata una traccia pianificata con una serie di argomenti predeterminati e sequenziali. Il testo guida è stato strutturato definendo innanzitutto alcune domande chiave che sono state utilizzate con ampia

flessibilità in quanto il suo obiettivo è stato quello di approfondire gli argomenti oggetto della ricerca. La tecnica di costruzione utilizzata è stata quella delle domande «*a imbuto*»: si è partiti da uno schema generale per arrivare ad uno specifico, da domande meno strutturate a quelle più strutturate. Le domande sono formulate in modo da permettere un'immediata comprensione e l'intervento spontaneo dei partecipanti seguendo un flusso logico che facilitasse la discussione. L'obiettivo è stato quello di sottoporre ai partecipanti domande il più possibili spontanee e semplici tali da non suggerire alcuna potenziale risposta.

3.4.1. La selezione dei partecipanti

Per quanto riguarda la scelta dei partecipanti fondamentalmente era possibile seguire due *modalità di selezione*:

- i) il campionamento ragionato
- ii) e il campionamento casuale.

Per la tipologia di ricerca e per l'argomento trattato e per un efficace raggiungimento degli obiettivi dell'indagine si è preferito scegliere la prima modalità. Nella prassi, difatti, la maggior parte dei ricercatori confida nel *campionamento ragionato*, poiché permette l'intervento di persone in base agli scopi della ricerca e al contributo atteso. Per questo motivo, ad esempio, si preferisce coinvolgere testimoni qualificati e appartenenti a particolari categorie sociali, considerando variabili come la professione, l'età, il genere, lo status socio-economico e la scolarità. In misura minore ci si affida al *campionamento casuale* (o *random*) che potrebbe essere utilizzato, ad esempio, per studiare piccoli gruppi, scegliendo casualmente un numero di partecipanti per un focus group. A tal proposito del metodo di campionamento è importante ribadire che i focus group non producono risultati statisticamente significativi.

Il livello di *omogeneità o eterogeneità* è un altro aspetto che è stato considerato nella fase di selezione e reclutamento dei partecipanti.

i) Un *gruppo omogeneo* permette una migliore trattazione degli argomenti, prevenendo deviazioni dal tema scelto e favorendo una libera espressione di soggetti che potrebbero altrimenti essere inibiti dalla presenza di attori con cui si vivono rapporti di potere e asimmetria sociale.

ii) D'altro canto, un gruppo eterogeneo consente di raccogliere una maggiore varietà di informazioni proprio facendo leva sulla diversità dei partecipanti e rilevando un vasto panorama di considerazioni sull'oggetto di discussione. Nel nostro caso si è scelto di selezionare e comporre un gruppo più omogeneo in considerazione anche della sua ridotta numerosità (9 persone). A tal proposito occorre sottolineare che nonostante sia impossibile stabilire il numero ideale dei partecipanti ad un focus group, così come il numero massimo di incontri da realizzare, la comparazione di vari studi in materia permette di affermare che il numero adeguato si colloca tra i 6 e i 12 componenti, tenendo presente che un gruppo omogeneo potrà essere meno numeroso di un gruppo eterogeneo. La numerosità solitamente deve essere stabilita mantenendo un corretto equilibrio tra la necessità di avere abbastanza persone per una discussione proficua e i limiti di un gruppo eccessivamente numeroso e dispersivo.

I soggetti sono stati selezionati in base a determinate caratteristiche in comune che li mettessero in relazione alla tematica della ricerca. All'interno di ogni categoria, la scelta degli interlocutori è avvenuta tenendo in considerazione diversi criteri, come l'ampiezza delle conoscenze, l'obiettività con cui queste conoscenze potevano essere messe a disposizione durante la fase di discussione, la predisposizione alla collaborazione, ecc.

3.4.2 Realizzazione discussione e metodo di analisi

La fase introduttiva ha riguardato l'esposizione degli scopi della convocazione e la presentazione ai partecipanti della tematica generale e degli obiettivi della ricerca. Per la tutela della riservatezza sono state illustrate brevemente le garanzie di privacy sul trattamento anonimo dei dati raccolti chiedendo il consenso all'uso per le finalità della ricerca per quanto riguarda la documentazione raccolta mediante audio registrazione.

Nel corso dell'incontro sono state poste domande aperte (precisando ai partecipanti che non esistono risposte giuste o sbagliate ai quesiti proposti) in forma verbale (quesiti diretti, frasi, definizioni, associazioni) e anche in forma visiva (disegni, foto, filmati) attraverso l'ausilio di video proiettore che è stato a molto utile per favorire un'immediata visualizzazione dei contenuti espressi e seguire l'evoluzione del dibattito.

Grazie a questi strumenti è stato possibile anche realizzare man mano delle sintesi provvisorie, evidenziando punti di vicinanza e divergenza tra le opinioni dichiarate. Talvolta durante la discussione è stato necessario utilizzare domande sonda per approfondire questioni sollevate dagli interventi dei partecipanti e per stimolare ulteriormente la discussione su una specifica problematica; in altri momenti è stato necessario ricondurre la discussione nell'ambito delle tematiche rilevanti per la ricerca, gestendo eventuali *fughe dal compito* che si verificano del resto comunemente nei gruppi di discussione. Il team di ricerca dopo un'accurata fase di analisi ha prodotto un report finale che contiene l'esposizione dei contenuti emersi, le citazioni salienti degli interventi e l'interpretazione dei risultati. Nella redazione del report finale i risultati, espressi in forma anonima, sono stati analizzati con un resoconto supportato dalle verbalizzazioni del gruppo concentrandosi sulla ricostruzione del dibattito, analizzando il flusso della discussione e identificando gli argomenti chiave con l'uso di mappe tematiche assieme alle citazioni dei partecipanti. L'intera discussione è stata registrata per poter disporre di una trascrizione integrale che consentisse di analizzare in modo fedele e accurato quanto emerso, e permettesse una facile identificazione dei partecipanti e osservarne le interazioni.

3.4.3 Analisi dei risultati del focus group: La percezione della sicurezza

La prima fase del focus prende l'avvio con l'introduzione della tematica oggetto di studio, aprendo il confronto e la discussione di gruppo con la presentazione ai partecipanti dei risultati dell'indagine campionaria sulla sicurezza. I partecipanti sono stati stimolati con alcune domande dirette a rilevare la loro opinione e le loro percezioni sulla sicurezza del territorio e sull'andamento e la diffusione dei reati di natura predatoria per poi focalizzarsi sul tema

specifico chiedendo di esprimersi sul trend nell'ultimo periodo dei reati che colpiscono le dipendenze bancarie (rapine, furti, danneggiamenti, frodi, ecc.).

L'obiettivo era quello di rilevare le eventuali "divergenze" di percezione acquisendo un'opinione più qualificata dal lato degli esperti in veste di osservatori privilegiati al fine anche di approfondire e integrare i risultati dell'indagine campionaria. La rilevazione di tali opinioni è importante perché nel modello di sicurezza elaborato nell'ambito del progetto BA.S.S. la percezione di insicurezza e vulnerabilità del territorio e nello specifico anche delle dipendenze bancarie è una delle variabili importanti che spiega e influenza il rischio dell'accadimento del fenomeno.

È stato dimostrato che se una filiale bancaria viene facilmente attaccata aggirando i sistemi di sicurezza, aumenta la percezione della sua vulnerabilità e di conseguenza i tentativi di rapina e il rischio e la probabilità che quella filiale venga nuovamente violata.

- Realtà e percezione della realtà

La prima domanda "guidata" del focus era a diretta a capire se ci fossero delle opinioni divergenti tra il comune sentire o *sentiment* del cittadino, in merito alla sicurezza del territorio e il parere più "qualificato" degli opinion leader intervenuti al focus.

Ricordiamo che i dati dell'indagine campionaria avevano evidenziato per la maggiore parte dei casi un aumento della criminalità mentre solo una piccola percentuale aveva ravvisato un miglioramento, ancora, una percentuale rilevante, quasi un cittadino su tre evidenziava in modo chiaro condizioni e situazioni di insicurezza.

Ci si chiedeva dunque se i reati nella realtà e non nell'immaginario collettivo fossero davvero aumentati in maniera significativa e le condizioni di sicurezza peggiorate così come evidenziato dalla ricerca.

Dalle osservazioni dei partecipanti emerge che non è sicuramente semplice stabilirlo a priori affidandoti solo alla percezione del territorio. Un dato comunque è certo: è che spesso la percezione della realtà è diversa dalla realtà e il più delle volte, come è stato osservato dai più, spesso la percezione di insicurezza è più elevata di quanto lo sia in realtà. Sono non pochi i casi in cui le statistiche ufficiali evidenziano un calo dei reati mentre il dato di percezione rileva un incremento del fenomeno. Ma il fatto che il dato sia sovradimensionato non è da sottovalutare. Si vuole dire che molte volte la percezione è in grado di condizionare la realtà, alimentare il senso di insicurezza creando un circolo vizioso. In questo, giocano un ruolo fondamentale anche l'informazione e i media che possono amplificare il fenomeno con allarmismo e condizionare in maniera rilevante il dato percettivo. Su quest'ultimo punto sono molte le osservazioni che confermano tale tendenza:

"...nell'immaginario collettivo non c'è il singolo episodio c'è una condizione di insicurezza...si crea e si ingenera nell'opinione pubblica questa difficoltà di vivere, questa recrudescenza criminale...poi se è un caso due casi importa poco..."

“...altro fenomeno che contribuisce a far crescere la percezione dell'insicurezza è quella legata alla tipologia del reato. Quando succede un fatto eclatante che occupa le prime pagine dei giornali e mobilita anche le testate televisive poi in sequenza si verificano un serie di casi che hanno la stessa dinamica e lo stesso svolgimento che riguardano la stessa categoria di attori ...i media e i giornalisti per questione di sintesi restituiscono al lettore e al telespettatore una condizione particolare che incute nella gente il timore di rimanere vittima di un reato e cominciando a guardarsi intorno anche dal vicino di casa, dal collega di lavoro, per paura di rimanere vittima di questo o questo o quello episodio...”

“In realtà i numeri non contano nulla le analisi fatte dagli esperti che evidenziano come vi sia una recrudescenza o meno di fatti criminali... per l'informazione contano poco o nulla perché poi è quello che il giornalista restituisce o il mezzo di informazione restituisce all'opinione pubblica che spesso conta veramente...”

Sono molti gli esempi che i soggetti portano per avvalorare la tesi che l'opinione pubblica è fortemente influenzata dai media che sono in grado di condizionare in maniera rilevante il giudizio dei cittadini e aumentare l'allarme sociale

“...durante in un colloquio avuto con il questore questi evidenziava un aumento dei reati, la città era in fibrillazione perché diventata insicura...c'è stato dunque un allarme generale tra commercianti, le associazioni di categoria, gli industriali...sono andato a verificare le statistiche e questi erano in calo. Per cui c'è spesso un eccessivo allarmismo, se succedono 2 reati nella stessa giornata, 3 o 4 nell'arco della settimana scatta l'emergenza criminale

Quindi la percezione spesso diverge dalla realtà ma ciò non significa che si può abbassare la guardia e non tenerne conto, la percezione è comunque un sentore, può essere una spia di un malessere sociale che può diffondersi.

...la percezione è una cosa diversa dall'effettiva sicurezza molto spesso basta uno scippo per ritenere la città insicura perché si legge la notizia della vecchietta scippata e tutte le vecchiette si ritengono potenziali vittime si diffonde nell'immaginario collettivo questa fobia dello scippo, pertanto la percezione della sicurezza è importante fino ad un certo punto. Però ciò non vuol dire che percezione non sia importante noi dobbiamo fare in modo che il cittadino abbia una percezione positiva della sicurezza indipendentemente dal fatto che il titolo dei giornali abbia amplificato il fenomeno e ingenerato paura e timore per questi fatti criminosi.

...la percezioni in effetti dell'aumento dei reati va forse oltre l'aumento in termini reali degli stessi a conferma forse che spesso questi fenomeni sono sovradimensionati...dunque questo aumento del senso e della percezione di insicurezza è dettato spesso dall'accadimento di questi piccoli reati che si possono vedere o sentire nel quotidiano vicini a noi che non fanno che amplificare in modo rilevante e spropositato la preoccupazione e alimentare questo senso di insicurezza...ci sentiamo spesso insicuri nelle nostra case...quindi questa percezione di insicurezza è fondata anche se non è tanto grave come appare...ma comunque siamo preoccupati di quanto avviene fuori...

- *Il fenomeno dei reati sommersi*

Non manca tra i partecipanti chi invece evidenzia un aumento degli episodi di microcriminalità al di là del condizionamento dei media e degli altri fattori che possono in qualche modo alterarne la percezione, ponendo l'accento su un altro fattore importante che sicuramente non è da sottovalutare quando si cerca di analizzare il fenomeno: e cioè che molte volte questi reati rimangono sommersi perché non denunciati. I motivi sono diversi ma spesso sono da imputare alla lentezza e alla scarsa efficienza dell'amministrazione della giustizia che rende poco conveniente denunciare questi reati che sfuggono alle statistiche ufficiali, rimanendo tra le altre cose impuniti.

...ho notato che di recente, nell'ultimo o negli ultimi due anni, i piccoli reati sono aumentati ciò molto probabilmente a causa anche della crisi economica...mi riferisco soprattutto ai piccoli furti che non hanno a che vedere con le rapine...ma sicuramente e realmente al di là della percezione o della stampa che in alcuni casi può amplificare il fenomeno posso affermare che se un anno fa o due anni fa c'erano due furti al giorno, oggi se ne verificano cinque e non denunciati a livello ufficiale presso le autorità pubbliche, Carabinieri, Polizia. Consideriamo che molti di questi reati non vengono rilevati perché non denunciati e quindi non entrano nelle statistiche a causa di lungaggini burocratiche della giustizia che non rende conveniente e agevole la denuncia, quindi molti di essi sfuggono alle statistiche...in ogni caso ho avvertito un aumento dei reati vi posso testimoniare perché sono sul campo...quindi al di là di quello che dicono i giornali che possono amplificare un fenomeno che può essere in realtà sottodimensionato i numeri ci sono...si rileva un aumento dei fenomeni di criminalità predatoria

- *Il fenomeno del cyber crime: diminuiscono le rapine "classiche" e aumentano le rapine e le frodi telematiche*

La discussione si sposta gradualmente sui sistemi di sicurezza bancaria e sui reati, rapine, furti e frodi compiuti ai danni delle banche. In questo caso le opinioni sono più circostanziate ed evidenziano che se da un lato si registra un ridimensionamento e flessione del fenomeno delle "classiche" rapine compiute all'interno delle filiali dall'altro c'è un'evoluzione di questa tipologia di azioni criminali che diventano sempre più sofisticate e specializzate. Si parla in questo caso del fenomeno del *cyber crime* e dunque dell'aumento delle rapine e delle frodi di natura informatica compiute da hacker esperti della rete internet che riescono a insinuarsi nei sistemi telematici e di pagamento delle banche.

...per quanto riguarda la sicurezza bancaria e quello che avviene nei locali della banca da quello che ho potuto constatare i nostri clienti si sentono più sicuri se hanno ben visibile i sistemi di videosorveglianza, ossia video camera, il personale addetto alla sicurezza che è all'esterno della filiale che indossa il giubbotto antiproiettile li rassicura di più se ha il mitra li rassicura di più...ma posso dire che oggi come oggi i reati all'interno della banca non sono più rilevanti...non esiste più l'assalto alla diligenza...ma i più rilevanti sono i reati di natura informatica...è lì che l'attività criminale incide maggiormente... si tratta principalmente di persone e criminali che operano anche fuori dall'Italia specialmente dall'Est Europa persone che sono molto attrezzate per questo genere di reati...

...la sicurezza rispetto agli eventi criminosi sta migliorando e anche la percezione sta migliorando...ciò soprattutto dopo il 2008, anno in cui è incominciata la famosa inversione di tendenza per cui dopo un trend in costante crescita fino al 2008, si è rilevato una riduzione delle rapine bancarie probabilmente perché come sostengono in molti abbiamo ridotto il contante che era presente nelle agenzie che sono

state trasformate in luoghi che sembrano sempre più negozi... la tendenza futura è che le banche pensano di risparmiare sulla sicurezza perché gli eventi rapina si stanno riducendo

La presente indagine, costituisce un primo passo importante per iniziare a delimitare e misurare in considerazione della complessità ed eterogeneità dei fenomeni osservati alcuni tratti specifici propri della sicurezza bancaria e del rischio rapina. Un impianto di questa natura può fornire un supporto utile ai responsabili della sicurezza sia nell'individuazione delle principali necessità dei sistemi in uso che in quelli di nuova applicazione, selezionare i principali nuclei di criticità, rappresentare una base per formulare le ipotesi più valide di intervento e di soluzione tale da consentire una corretta pianificazione di attività ed interventi legati ai servizi di prevenzione e protezione dal rischio rapina.

Dalle due linee di analisi, indagine campionaria e focus group, la prima di tipo quantitativo e la seconda di tipo qualitativo, emergono dei suggerimenti utili per la definizione delle linee guida del piano dell'innovazione, dal duplice punto di vista rispettivamente degli utenti/clienti ed esperti partecipanti al focus. Mentre l'indagine campionaria ci ha consentito di ricavare degli orientamenti e dei suggerimenti di ordine più generale, attraverso il focus sono emerse invece delle indicazioni più specifiche entrando nel merito degli aspetti tecnici dei sistemi e misure organizzative della sicurezza bancaria.

L'importanza della percezione della vulnerabilità e del livello di sicurezza bancaria

L'indagine campionaria ha consentito di rilevare il punto di vista degli utenti sul livello di affidabilità dei sistemi di sicurezza, la percezione del livello di sicurezza delle dipendenze bancarie e la loro vulnerabilità potenziale agli attacchi criminali.

In prima battuta è stata esplorata una variabile importante del modello che è la percezione del livello di sicurezza e le difficoltà intrinseche di una sua misurazione e rappresentazione "oggettiva", perché fortemente legata alle esperienze e condizioni personali del soggetto, nonché all'ambiente circostante. Il tema della sicurezza è frequentemente mal posto per tanti motivi. Il primo è che raramente si distingue tra la realtà e la sua percezione. Perciò, può benissimo accadere che il numero di furti o di rapine diminuisca costantemente nel corso del tempo ma, al contrario, la credenza diffusa tra la popolazione è che tali reati aumentino e si diffondano in maniera incontrollata.

Le statistiche giudiziarie, pertanto, possono essere del tutto slegate dal clima di opinione che è alimentato, invece, principalmente dall'allarmismo dei mezzi di comunicazione di massa.

Studiare le opinioni diffuse tra i cittadini/utenti, come si è fatto in questa ricerca, è dunque il primo passo per affrontare in maniera adeguata questo effetto distorto della realtà.

Una ricerca empirica così strutturata ha consentito di rilevare non solo le rappresentazioni sociali nel loro insieme, ma di entrare più in dettaglio per comprendere se vi siano a questo proposito differenze significative tra segmenti diversi della popolazione. È infatti plausibile che i timori della fascia anziana della popolazione siano diversi da quelle dei giovani; che le paure delle donne siano differenti rispetto a quelle degli uomini, e così via.

Anche se la percezione può essere diversa dalla realtà spesso è in grado di condizionare la stessa realtà e condizionare in particolare il comportamento dei soggetti atti a delinquere: è il caso del soggetto o criminale che ha la percezione che quella filiale è facilmente aggredibile e che i sistemi di sicurezza sono facilmente superabili o che sono insufficienti e quindi vale la pena tentare la rapina. Dalla ricerca è emerso che è in aumento il fenomeno dei reati compiuti non da criminali professionisti ma di soggetti che spesso si improvvisano tali, in quest'ottica è stata molto importante conoscere l'opinione dei cittadini/utenti dei servizi bancari al fine di avere un'idea di massima sulla sicurezza bancaria, un punto di partenza per comprendere, quali siano i fattori che possono aumentare e migliorare la percezione di vulnerabilità della filiale. Ciò suggerisce che sarebbe necessario concentrare maggiormente l'attenzione sulle dinamiche e sugli aspetti che caratterizzano questo genere di reati, studiando anche gli aspetti comportamentali del criminale comune e non solo quelli dei criminali professionisti.

Approfondendo il dato sul livello di sicurezza bancaria la percezione generale della maggior parte degli utenti è che le banche siano abbastanza vulnerabili e i sistemi di sicurezza non adeguati per scongiurare tale tipo di fenomeni, ciò viene evidenziato sia dai soggetti che hanno avuto esperienze dirette di rapina sia da quanti non ne hanno mai avute. Il giudizio non proprio positivo riguarda sia il personale addetto alla sicurezza valutato nella maggior parte dei casi poco preparato ad affrontare e gestire tale tipologia di eventi criminosi, sia i sistemi di sicurezza e di protezione antirapina in dotazione consideranti scarsamente adeguati o insufficienti; ancora più negativo il giudizio sul personale bancario anch'esso giudicato poco preparato.

Ciò ovviamente suggerisce un miglioramento e un potenziamento dei sistemi e delle misure di sicurezza sia tecnologiche che tradizionali ponendo particolare attenzione alle attività di prevenzione, di informazione e formazione a beneficio del personale addetto alla vigilanza e del personale della banca.

La rapina è, infatti, un evento criminoso che può comportare un rischio per la sicurezza e per la salute dei dipendenti e dei clienti. La prevenzione richiede l'attenzione dei responsabili della sicurezza di tutto il personale bancario. Diventa molto importante in quest'ottica far conoscere le best practice di prevenzione e gestione degli eventi criminosi: per contribuire efficacemente alla sicurezza antirapina è infatti necessario integrare le misure di difesa con comportamenti adeguati da adottare quotidianamente nel corso dell'attività lavorativa. Per tale ragione, le banche stanno potenziando l'attività di informazione del personale, strumento essenziale per lo sviluppo della cultura della sicurezza e della prevenzione. Dall'indagine infatti emerge che è necessario intraprendere e attivare azioni formative e informative più mirate attraverso diverse modalità e strumenti diversi (sito internet, e-mail, news, guide informative, ecc.), non solo al personale addetto alla vigilanza ma anche ai dipendenti delle banche sulle dinamiche psicologiche e comportamentali da adottare nel caso in cui si subisca l'evento criminoso.

Altro elemento importante che è stato possibile rilevare attraverso l'indagine è che il reato di rapina è un fenomeno complesso nella rappresentazione sia degli utenti che degli esperti:

sono tante le variabili che intervengono e che occorre tenere in considerazione. Sono in molti che concordano sul fatto che non esiste un sistema infallibile, sia materiale che umano, che sia in grado di scongiurare ed evitare in tutto e per tutto questo genere di eventi. Dal lato delle soluzioni, comunque, la maggiore quota di soggetti confida che solo attraverso un miglioramento dei sistemi di sicurezza, considerati come appena evidenziato, poco efficaci, si può evitare e contrastare questa tipologia di fenomeni. Tali interventi superano anche se non di molto gli interventi di tipo indiretto come la limitazione nell'uso del contante e un maggiore presidio del territorio da parte delle forze dell'ordine.

Quest'ultimi, invece, raccolgono il consenso soprattutto degli esperti, partecipanti al focus, tutti all'unisono concordi nel ritenere che è importante attuare la "sicurezza partecipata" che vede una stretta collaborazione tra sicurezza pubblica, forze dell'ordine e sicurezza privata attraverso un modello PPP (*Public and Private Partnership*).

La limitazione nell'uso del contante rappresenterebbe sicuramente il migliore antidoto secondo il parere dei soggetti partecipanti al focus, in linea con le recenti politiche e provvedimenti, sistemi tecnologici e organizzativi adottati dalle banche che hanno sortito già il loro effetto, registrandosi una riduzione delle rapine. Ciò risolverebbe il problema alla radice, cosa che invece è scarsamente compresa da parte degli utenti che molto probabilmente, anche se ne percepiscono l'importanza non rinunciano alla libertà dell'uso del contante.

La necessità di controllare e limitare l'uso del contante quale forte deterrente per scongiurare il verificarsi di queste azioni criminali trova dunque pieno riscontro nei dati di trend del fenomeno che come abbiamo appena rilevato vede una riduzione delle rapine in banca a fronte di un contestuale e considerevole aumento, negli ultimi anni, degli attacchi e rapine agli ATM dove il criminale sa di poter trovare con maggiore probabilità denaro contante e dove è più facile e soprattutto meno rischioso agire il più delle volte indisturbati.

Suggerimenti e linee di intervento

I partecipanti al focus sono stati invitati e stimolati ad esprimere le loro idee, pareri e orientamenti sui sistemi e misure organizzative del modello di sicurezza. In sintesi, tutti i soggetti hanno espresso un elevato livello di apprezzamento, formulando nella maggior parte dei casi delle valutazioni positive per i sistemi proposti cogliendone gli aspetti altamente innovativi e tecnologici. Ognuno di essi ha preso parte attivamente alla discussione, molto costruttiva e con un ottimo livello di interazione, che ha consentito di generare molti spunti di riflessione e nuove idee sulle tematiche dibattute. I soggetti hanno espresso in maniera chiara le loro posizioni, evidenziando dal lato della loro esperienza, potenzialità, vantaggi ma anche criticità e formulando laddove possibili linee di intervento e correttivi in un'ottica di miglioramento del sistema.

Occorre rilevare che non tutti i sistemi e le misure illustrati del pacchetto di integrato di sicurezza hanno suscitato lo stesso livello di interesse per cui spesso la discussione si è orientata e focalizzata spontaneamente sulla valutazione di quelli maggiormente attenzionati. Si tratta

dei sistemi più conosciuti dai partecipanti più vicini o legati alle loro esperienze di tecnici ed esperti e sui quali i soggetti avendo una maggiore competenza hanno avuto la possibilità di argomentare maggiormente, andando più profondità ed esprimendo dei pareri più articolati. Tra questi è da rilevare il sistema di videosorveglianza biometrico di riconoscimento dei visi e i sistemi che rilevano le manomissioni degli ATM esterni delle banche al fine di scongiurare i fenomeni di *cash trapping*, ossia le tecniche di prelievo fraudolento del contante (attraverso ad esempio l'inserimento di una forcina metallica, detta "forchetta", nella fessura di erogazione delle banconote e di altri materiali esplosivi). I suggerimenti vanno in direzione di un approfondimento degli aspetti legati alla sostenibilità economica e fattibilità delle misure di sicurezza proposte. Gli orientamenti degli stakeholders suggeriscono delle linee guida da tenere presente per sviluppare e implementare correttamente i sistemi di sicurezza alla luce delle tendenze di mercato attraverso delle azioni di lungo e breve periodo. Qui di seguito sono riportati i principali orientamenti emersi.

- Verifica della sostenibilità economica dei sistemi di sicurezza alla luce dei cambiamenti ed evoluzione dei comportamenti criminali, del cyber crime, dei comportamenti dei clienti che si recano sempre meno in banca grazie alla diffusione dei servizi di home-banking. Si è di fronte a minacce sempre più sofisticate. Se, da una parte, diminuiscono gli atti criminali tradizionali, dall'altra però si sta registrando un incremento e uno spostamento dell'attenzione verso i crimini informatici, meno rischiosi e più remunerativi. L'evoluzione verso l'*ifinance*, attraverso l'interconnessione informatica diffusa richiede soluzioni di continuità di servizio e di sicurezza sempre più efficaci. L'esigenza di protezione delle banche evolve nel tempo coerentemente con l'evoluzione del contesto tecnologico, economico e sociale in cui operano. La notevole introduzione dell'Ict nell'interazione con il cliente, privato o impresa, fa sì che la garanzia di un adeguato livello di sicurezza diventi una componente essenziale dell'offerta..

Il peso crescente nelle strategie commerciali dell'innovazione nelle modalità di accesso ai servizi bancari implica di rivedere l'approccio/ la strategia per il presidio della sicurezza.

La strategia di protezione del sistema banca che obbliga ad una segregazione di ambienti, è in contrasto con una logica di marketing che va verso un'apertura di servizi con modalità e canali differenti e che è diretta a perseguire una facilità di fruizione degli stessi da parte del cliente.

- Realizzare, allo stesso tempo, una corretta pianificazione finanziaria e analisi dei costi del pacchetto di sicurezza alla luce di tale evoluzione (pianificazione degli obiettivi e dei risultati da raggiungere, investimenti, costi operativi, benefici tangibili e intangibili, valutazione economica e finanziaria del progetto, NPV)
- Concentrare una maggiore attenzione sulla valutazione del rischio e sulle dinamiche dei reati e delle rapine compiute dai delinquenti occasionali, che rappresentano un

fenomeno in forte aumento, e non solo sui reati compiuti dai criminali professionisti che invece, sembrerebbero essere in calo. Ciò in considerazione del fatto che al di là del danno economico e patrimoniale del denaro sottratto, occorre valutare l'impatto dovuto al danno di immagine subito dalla banca che avrebbe la stessa portata sia che la rapina viene effettuata da un rapinatore professionista che da un delinquente occasionale.

- Approfondire attraverso una nuova indagine gli aspetti che possono definire e influenzare la percezione sulla vulnerabilità di una filiale bancaria. Ciò consentirà di definire meglio gli asset di sicurezza del modello e agire su tutti gli aspetti e gli elementi di dissuasione del potenziale rapinatore comune e non solo professionista.
- Attuare un monitoraggio continuo del rischio rapina attraverso la costruzione di un data base degli eventi che possa in qualche modo dare dei suggerimenti in merito all'efficacia di tali sistemi e dunque apportare dei miglioramenti.
- Concentrare una maggiore attenzione al superamento dei problemi di privacy legati all'acquisizione di dati personali e altri dati sensibili necessari per la costruzione delle banche dati (fondamentali per il funzionamento del sistema) che se trascurati e non correttamente affrontati potrebbero costituire un serio ostacolo nell'applicazione di alcune misure di prevenzione innovative. Si fa riferimento in particolare ai sistemi di rilevazione biometrici: il sistema *Smart face recognition* che rileva e riconosce i volti dei soggetti e quello che rileva le impronte digitali. Oltre a studiare in profondità le implicazioni di ordine giuridico al fine di garantire il pieno rispetto della normativa sulla privacy, si rende necessario adottare un adeguato piano di comunicazione rivolto ai clienti della banca al fine di sensibilizzarli sulle misure di sicurezza adottate, aumentare così l'immagine sulla sicurezza della banca e rendere agevole l'acquisizione dei dati biometrici, personali e altri dati sensibili.
- Verifica della fattibilità tecnica e dei tempi di costruzione del database dei dati biometrici dei soggetti. Ricordiamo che una delle criticità di queste misure di sicurezza risiede nel fatto che attraverso tali tecnologie si stabilisce l'identità di un soggetto a partire anche da un insieme di persone registrate, per cui il problema è la costruzione e la continua implementazione di una valida, efficace ed affidabile banca dati. Si suggerisce dunque di attivare dei protocolli di collaborazione con le forze dell'ordine e con altre strutture pubbliche di sicurezza (es. questure) al fine di rendere agevole l'acquisizione e l'aggiornamento dei dati sensibili sui soggetti e potenziali criminali che hanno avuto dei precedenti penali e compiuto azioni criminali legati a reati di natura predatoria (rapina, furti, frodi, ecc).
- Porre maggiore attenzione al presidio del territorio intorno alla banca e ai reati molto frequenti di rapina e di scippo che avvengono fuori ma a distanza ravvicinata dalla filiale a danno di quell'utente che ha appena effettuato un'operazione di prelievamento. È stato osservato in proposito che tali tipi di reato anche se esulano dalla competenza

della banca e non è suo compito intervenire si ha comunque un danno di immagine se si diffonde la notizia che in quella zona e nei pressi di quella filiale c'è stata una rapina, ciò avrebbe produrrebbe lo stesso effetto di una rapina fatta direttamente nei locali della banca stessa. Per affrontare efficacemente questi fenomeni è utile consolidare la collaborazione con le forze dell'ordine e le strutture che si occupano di vigilanza pubblica.

- Attuare all'esterno della banca un modello di "sicurezza partecipata" PPP (*Public and Private Partnership*), che vede una stretta collaborazione tra forze di sicurezza pubbliche e private della banca. In quest'ottica potrebbe essere utile nel breve stipulare un protocollo d'intesa tra forze dell'ordine locali e banca.

L'integrazione delle risorse pubbliche e private sarà diretta ad intensificare gli impianti di video sorveglianza e la protezione soprattutto ai bancomat; ad aver un maggior dialogo tra polizia e banca con costanti informazioni e analisi degli eventi criminosi accanto una continua e specifica formazione degli operatori bancari. Sono gli aspetti principali su cui dovrà essere fondato il protocollo per prevenire efficacemente la criminalità e le rapine negli istituti bancari.

Per concludere sarà necessario far evolvere la sicurezza nella direzione di una creazione più concreta di valore attraverso azioni che soddisfino puntualmente le esigenze di sicurezza delle diverse funzioni della banca e dei clienti; tenendo in considerazione che nel sistema bancario è in atto un cambiamento radicale nella concezione della sicurezza, che diventa sempre più attiva e, tramite servizi avanzati di monitoraggio, tende a prevenire piuttosto che reprimere e gestire gli eventi criminosi. Si va in direzione di un modello di sicurezza integrata che consente di concentrare la responsabilità in un unico punto di raccordo e di gestione, portando alla costituzione di un'unica direzione centrale di sicurezza. Mentre gli investimenti tecnologici sono orientati verso nuovi sistemi di videosorveglianza intelligente e sistemi informatici integrati di sicurezza.

L'attivazione del circolo virtuoso "più sicurezza uguale maggiore qualità dell'offerta e maggiore fiducia della clientela" assumerà sempre più importanza strategica nell'attività finanziaria, che sul trattamento dei dati e delle informazioni e sulla costruzione di un rapporto di fiducia con i clienti fonda la propria operatività. Alla luce di ciò la sicurezza, nel lungo periodo, tenderà ad essere considerata sempre meno solo una voce di costo, ma una vera e propria leva di business in grado di creare valore.

3.5 Analisi della situazione attuale

3.5.1. I processi e gli attori della sicurezza fisica in banca

Secondo il framework proposto da Anthony (1965), i livelli organizzativi che si occupano del processo di gestione e mitigazione dei rischi all'interno di gruppi bancari possono essere rappresentati come segue.

A livello strategico sono emerse tre possibili configurazioni dalle interviste:

- Una funzione organizzativa ad hoc che dipende direttamente dal CEO. È gestito da un Chief Security Officer (CSO) (o Global Security Officer) che ha la responsabilità di tutti i processi di sicurezza (interno, esterno, fisico, logico, personale), dal livello strategico a quello operativo.
- Due funzioni organizzative separate per la sicurezza logica e fisica: Un responsabile della sicurezza dell'informazione (CISO), direttamente dipendente dall'amministratore delegato, responsabile della protezione delle informazioni e eventualmente di altri aspetti strettamente correlati come la pianificazione e lo sviluppo delle architetture di sicurezza e gli incidenti informatici. Un responsabile della sicurezza fisica (CPSO) che appartiene a una struttura organizzativa del personale (ad es. Risk Management). Il CPSO è responsabile di assicurare tutte le attività fisiche del gruppo bancario.
- Una funzione di Staff al livello del CEO, incaricata di definire le politiche di sicurezza, le priorità e le linee guida mediante un Comitato di Controllo responsabile della gestione dei rischi, delegando la parte operativa di CISO ad una funzione IT e ad altre strutture operative (ad esempio Logistics, Asset Gestione, appalti).

In ogni caso, in tutte le configurazioni sopra considerate, sono coinvolti i seguenti attori che svolgono attività legate alla sicurezza fisica.

- Livello manageriale (tattico):
 - CSO: responsabile dello sviluppo e dell'attuazione delle politiche di sicurezza fisica.
 - CFO: Definisce il bilancio globale per le attività di gestione della sicurezza per la rete delle dipendenze bancarie.
 - CPO: Gestisce i processi di approvvigionamento di soluzioni e servizi di sicurezza per la rete delle dipendenze bancarie.
 - Direttore BB: responsabile dell'attuazione della politica di sicurezza fisica nella sua BB.
- Livello operativo:
 - Dipendenti BB: hanno il compito di rispettare le politiche di sicurezza.
 - Fornitori di soluzioni di sicurezza: installare e mantenere le misure di protezione all'interno della rete BB
 - Fornitori di servizi di sicurezza: appaltatori esterni che si occupano delle attività di monitoraggio delle potenziali minacce alle BB, in loco (ad esempio guardie armate) oppure in remoto (guardie di sicurezza all'interno della sala di controllo)

La seguente tabella riassume i principali task relativi ai processi di gestione della sicurezza emersi dall'analisi della letteratura e dalla discussione con gli esperti effettuata nel corso del focus group

Actors	Security Related Task
<i>Chief Security Officer</i>	<ul style="list-style-type: none"> • Implementation of the bank security strategy, and the development of

	<p>policies and procedures to support the strategy.</p> <ul style="list-style-type: none"> • Be responsible for the operational delivery and communication of security policy. • Develop a culture of security awareness and practice throughout the whole bank institute. • Ensure that operational security decisions are correctly recorded and stored, with due regard to sensitivity and information security. • Assess security risks and ensure that proportionate measures are in place to protect: visitors, staff, buildings, assets and reputation. • Ensure that professional security staff and employees appropriately trained. • Align 'in house' and 'outsourced' security staff. • Ensure that contracts for security services and systems are efficiently and effectively managed. • Prepare analytical reports to the executive, to identify areas where Security be involved. • Definition of Security Key Risk and Performance Indicators. • Technological Scouting. • Define and distribute a Checklist for Physical Security Risk Assessments. • Identify current and potential legal and regulatory issues affecting information security and assess their impact on the Bank. • Manage the security budget in implementing the security programme.
Chief Information Security Officer	<ul style="list-style-type: none"> • Define and elaborate the information security strategy in support of the Bank's business strategy and direction. • Identify current and potential legal and regulatory issues affecting information security and assess their impact on the Bank. • Establish and maintain information security policies that support business goals and objectives. Risk Management: Identify and manage information security risks to achieve business objectives • Manage the information security budget in implementing the information security programme. • Lead the Bank's IT security team: plan, organize, assign, supervise and monitor the work of team members • • Develop response and recovery plans including organizing, training, and equipping teams.
Chief Financial Officer	<ul style="list-style-type: none"> • Define the overall budget for security management activities.
Chief Procurement Officer	<ul style="list-style-type: none"> • Manage sourcing and procurement of security solutions and services.
BB director	<ul style="list-style-type: none"> • Participate in continuing education programs on safety and security. • Observe security procedure related to the appropriate use of protection measures (e.g. sliding doors, safe deposit box).

		<ul style="list-style-type: none"> • Observe, report and call the police if a crime occurs in their presence • Report faults or shortcomings of protection measures. • Report exceptional risky situation (e.g. abnormal cash holdings); • Fill the Checklist for Physical Security Risk Assessments.
	BB employee	<ul style="list-style-type: none"> • Participate in continuing education programs on safety and security. • Observe security procedure related to the appropriate use of protection measures (e.g. sliding doors, safe deposit box). • Observe, report and call the police if a crime occurs in their presence.
Security Service Contractor	Armed Guards	<ul style="list-style-type: none"> • Guard the physical space of the branch • stay alert to watch for potential threats to the safety of employees and customers. • Observe, report and call the police if a crime occurs in their presence.
	Remote control	<ul style="list-style-type: none"> • Monitoring for potential threats through CCTV systems • Observe, report and call the police if a crime occurs.
	Hardware solution providers	<ul style="list-style-type: none"> • Install and maintain security measures within a bank branch

Tabella 27. Principali task relativi ai processi della gestione della sicurezza nelle dipendenze bancarie

3.5.2. Rappresentazione AS-IS dei processi di gestione della sicurezza fisica

Sono stati identificati 5 sottoprocessi legati alla sicurezza, nei quali i summenzionati attori eseguono i loro compiti. Tali sottoprocessi sono rappresentati graficamente tramite un diagramma BPMN.

P1 Definizione del modello di valutazione dei rischi (Risk Evaluation Model) ed applicazione alle dipendenze bancarie. A partire dalle linee guida sulla gestione della sicurezza fornite dall'Associazione Bancaria Italiana, nonché dalle precedenti relazioni sugli attacchi criminali contro le BB, una volta all'anno il CSO definisce le politiche di sicurezza per le BB e le caratteristiche del REM. Ogni gruppo bancario possiede un proprio REM; quando applicato ad una BB, viene calcolato il suo valore di indice di rischio. In base a questo, si determina il tipo di misure di protezione che saranno installate e il modo in cui devono essere gestite. Anche se ogni modello di valutazione dei rischi è originale per ogni Istituto, i componenti di base per la valutazione del rischio sono comuni tra tutti i REM:

- attacchi criminali (minacce) che possono danneggiare una BB: rapina, furto, attacco ATM, danni fisici volontari.
- Beni che possono essere colpiti da una minaccia: Clienti, dipendenti, cassa contante, cassette di sicurezza, beni strutturali, Atm, l'immagine aziendale e la competitività commerciale

Un REM rileva la presenza di vulnerabilità di BB e misura il grado di sicurezza di BB contro ogni vulnerabilità rilevata. Ad esempio, il grado di sicurezza della vulnerabilità "Posizione della BB" può avere i seguenti valori: 1 (area isolata), 2 (area periferica), 3 (zona semi-periferica), 4 (zona centrale).

Il CSO invia al direttore della filiale una Checklist come strumento per rilevare il grado di sicurezza per tutte le vulnerabilità. I direttori di BB sono tenuti a completare questa checklist. Questi documenti vengono raccolti dal CSO, il quale valuta la capacità globale di ogni BB di proteggere le proprie risorse dalle diverse minacce. La valutazione si basa sul calcolo dell'indice di rischio che è funzione dei livelli ponderati di sicurezza del BB contro tutte le vulnerabilità. I pesi, diversi per ogni REM, sono impostati per tener conto di risorse e minacce direttamente correlate a ciascuna vulnerabilità. Alla fine, minore è il livello di sicurezza, maggiore è il valore generale dell'indice di rischio BB e la conseguente necessità di proteggere la BB rispetto alle sue vulnerabilità.

Sulla base dell'indice di rischio, il CSO classifica ogni BB all'interno di una categoria di rischio (variabile da su una scala da 1 a 5 oppure da 1 a 7, a seconda del REM). A ciascuna categoria di rischio è assegnato un insieme minimo di misure di protezione volte a ridurre l'indice di rischio BB a meno della soglia desiderata. Il CSO è costantemente coinvolto in attività di scouting tecnologico per identificare nuove misure di protezione.

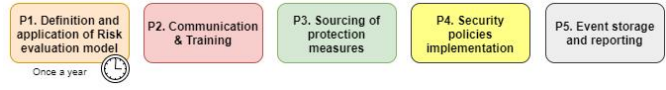
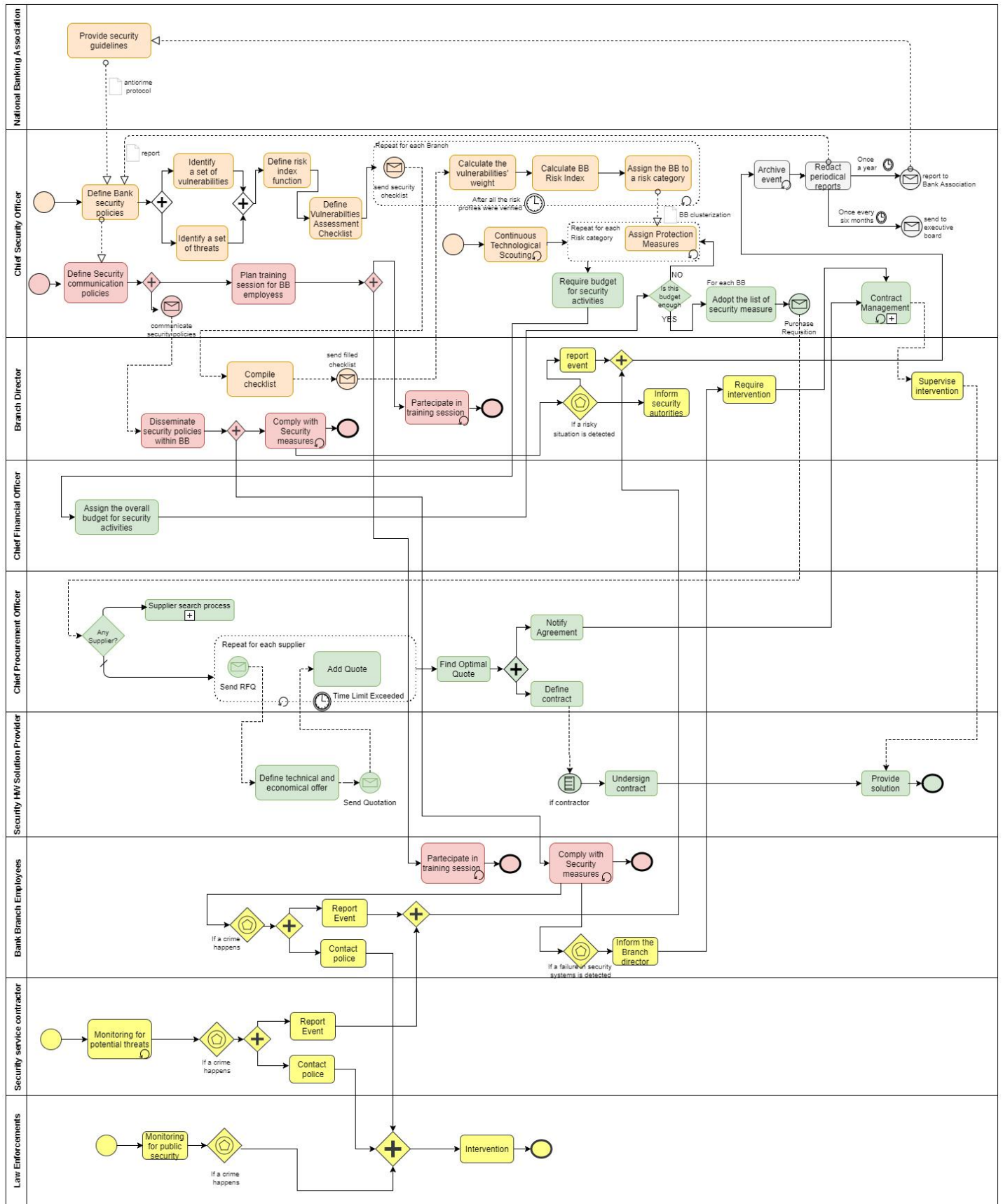
P2 Comunicazione e formazione: una volta individuate le politiche di sicurezza della banca, è necessario definire appropriate strategie di comunicazione in modo che queste politiche possano essere diffuse e capite in tutta l'organizzazione. Il CSO raggiunge questo scopo attraverso comunicazioni periodiche con i direttori delle BB (ad es. Newsletter), nelle quali spiega i requisiti e le prassi ottimali per garantire la safety e la security della Bank Branch, nonché le motivazioni che sottendono a determinate scelte. Il direttore della filiale si occupa di diffondere queste informazioni ai dipendenti della BB. Inoltre il CSO pianifica periodicamente sessioni di formazione su argomenti relativi alla sicurezza per i Direttori delle BB e per i dipendenti.

P3 Approvvigionamento delle misure di protezione. Il CFO definisce il budget da attribuire ad ogni categoria di rischio. In seguito, il CSO verifica se può implementare le soluzioni o ha bisogno di esaminare l'elenco delle misure di sicurezza alla luce del bilancio assegnato. Quindi, il CSO richiede al CPO di acquistare misure di protezione, stipulando contratti con fornitori di soluzioni tecnologiche.

P4 Implementazione delle politiche di sicurezza: durante le attività quotidiane, i dipendenti della BB devono rispettare le politiche di sicurezza definite dal CSO. Principalmente, queste politiche prevedono alcune procedure da seguire in caso di anomalie rilevate. Ogni volta che viene rilevata un'anomalia, i dipendenti delegati della BB informano il direttore che richiede un intervento per ripristinare il sistema di protezione. L'intervento è gestito alle condizioni definite in un "contratto di fornitura e manutenzione" di misure di protezione. Se si verifica invece un attacco criminale, le politiche di sicurezza richiedono ai dipendenti di rispettare le richieste dei

malfattori e di non intraprendere azioni che potrebbero mettere se stessi o altri in pericolo. Quando le condizioni di sicurezza lo consentono, possono attivare l'allarme e chiamare le forze dell'ordine. Subito dopo un evento criminoso, i dipendenti devono compilare un modulo specifico contenente informazioni descrittive sull'evento (ad esempio, data dell'evento, tipo di evento, descrizione del furto, direzione del viaggio, descrizione dell'auto, ecc.). Queste informazioni vengono fornite alle forze di polizia e comunicate al direttore della BB.

P5 Archiviazione e segnalazione di un evento: i dati sugli eventi criminali emessi in BB sono memorizzati in un repository e utilizzati per produrre report periodici. Questi rapporti vengono utilizzati dal consiglio d'amministrazione, per valutare le prestazioni della sicurezza BB e dal CFO per ridefinire le politiche di sicurezza. Inoltre, questi eventi criminali sono segnalati all'Associazione Bancaria Italiana al fine di aggiornare le linee guida per la sicurezza.



3.5.3. Limiti negli attuali approcci alla gestione della sicurezza e proposte di miglioramento.

La situazione che è stata possibile delineare attraverso le interviste si caratterizza essenzialmente per il fatto che attualmente le BB non dispongono di misure di protezione evolute (vale a dire non utilizzano piattaforme intelligenti), che hanno meccanismi di monitoraggio obsoleti e misure di protezione autonome.

Per ciò che concerne le misure di protezione, si evidenzia come seguito alla trasformazione del modello di business delle BB, la struttura fisica di queste ultime sta cambiando. In particolare, le misure di sicurezza di tipo "hard" (quali inferriate, guardie armate, telecamere visibili, metal detectors) vengono rimosse dalla vista dei clienti. Anche se tali misure sono considerate importanti per dare protezione agli asset bancari, possono dare ai clienti una sensazione di ansia e generare una cattiva sensazione di pericolo imminente che può persuadere i clienti ad evitare di entrare nella BB o comunque di restare al suo interno per il minimo tempo possibile. Purtroppo, l'obiettivo di ridurre il senso di ansia nei clienti si scontra con la necessità di garantire la protezione delle persone e di altri beni all'interno della filiale (Weisel 2007). Gli intervistati hanno sottolineato le debolezze delle misure di protezione che possono essere sintetizzate come segue:

- Le misure di protezione non sono ancora "intelligenti". Le misure fisiche più diffuse sono tradizionali nel senso che non presentano alcun livello di intelligenza embedded. In genere non possono monitorare costantemente l'ambiente, reagire e adattarsi a qualsiasi tipo di variazione, né comunicare con la control room o con altri dispositivi. L'unico canale di comunicazione riguarda i segnali di allarme provenienti da sistemi automatizzati o dagli esseri umani alla control room.
- Le misure di monitoraggio sono costose e di dubbia efficacia. Le sole misure in grado di monitorare l'ambiente e reagire alle condizioni mutevoli dell'ambiente circostante sono le misure basate esclusivamente sull'intervento umano: guardie armate e di sicurezza. Dall'analisi della letteratura e dalle opinioni degli esperti emerge che l'efficacia di queste misure non è evidente, nonostante il loro elevato costo. Le guardie armate coinvolte in attacchi possono solo avvertire la control room senza intervento diretto; il loro valore principale risiede nell'effetto psicologico dovuto alla loro presenza e visibilità per convincere i criminali a rinunciare ai loro pensieri criminali. La control room è spesso inefficace per individuare situazioni critiche. La parte principale del lavoro delle guardie di sicurezza consiste nel monitorare lo streaming video cercando di individuare comportamenti pericolosi o possibili attacchi criminali. Il numero di "falsi positivi" (ad esempio, l'interpretazione delle attività ordinarie come situazioni pericolose) e "veri negativi" (erronea interpretazione di situazioni pericolose come attività ordinarie) è elevato a causa di una sorta di "alienazione" che colpisce le guardie a causa della natura ripetitiva del lavoro. Inoltre, una control room è generalmente associata ad una singola

BB, generando costi elevati. Nel complesso, il bilancio della BB destinato alla sicurezza viene utilizzato principalmente per coprire il costo della sala di controllo e gli stipendi delle guardie.

- Le misure di protezione non sono integrate. Le misure di protezione sono incapaci di memorizzare e comunicare i dati sul loro stato al fine di analizzare fattori circostanti che caratterizzano l'ambiente in cui una BB è immersa. Se disponibili, le informazioni di contesto potrebbero essere utilizzate per supportare e migliorare la capacità di eseguire contromisure specifiche fornendo informazioni e servizi adattati alle esigenze di sicurezza. Un esempio tipico emerge da una delle interviste realizzate. Un addetto alle pulizie dimentica di richiedere l'autorizzazione ad entrare in una stanza; il sistema di allarme interpreta questo evento come un attacco in modo che l'allarme suona automaticamente e tutte le porte interne siano bloccate. La procedura di ripristino può durare un'ora, quindi la business continuity non è assicurata, con una conseguente perdita economica.

Per quanto riguarda il processo di gestione della sicurezza, le interviste consentono di evidenziare le seguenti debolezze dei sottoprocessi

P1:

- L'indice di rischio non è un profilo di rischio. Quando viene applicato ad una BB, il REM consente di calcolare il valore dell'indice di rischio che essenzialmente si riassume in un valore numerico. Questo rappresenta una forte debolezza perché il valore dell'indice non è in grado di rappresentare il profilo di rischio della BB e di suggerire eventuali misure di protezione che meglio soddisfino le attuali esigenze di sicurezza. Il problema risiede nel fatto che attualmente, ad ogni range di valore dell'indice è associato un insieme standard di misure di protezione. È possibile che due BB con caratteristiche e vulnerabilità differenti abbiano uguale punteggio degli indici di rischio (venendo classificate dunque nella stessa categoria di rischio). Verrà dunque richiesta l'installazione dello stesso insieme minimo di misure di protezione senza considerare il motivo per cui i valori dell'indice sono uguali. Ad esempio la prima BB potrebbe presentare vulnerabilità a causa delle misure di protezione ATM, mentre l'indice di rischio della seconda BB potrebbe essere dovuto alle caratteristiche dell'edificio BB.
- Durante il processo di trattamento del rischio, le banche organizzano generalmente le contromisure disponibili in una serie di *Configurazioni Minime di Sicurezza* da mettere rapidamente in campo in funzione dell'indice di rischio misurato per l'agenzia. Tali Configurazioni Minime dovranno consentire di ottenere un rischio residuo accettabile da migliorare, solo se necessario, con ulteriori interventi correttivi puntuali. Nell'ipotesi di avere un indice di rischio espresso con una scala a 10 livelli (cfr. Figura seguente), si possono organizzare ad esempio le agenzie in 5 gruppi e definire per ognuno di essi una configurazione minima di sicurezza da applicare per mitigare il rischio.

CONFIGURAZIONI MINIME DI SICUREZZA	GRUPPI AGENZIE									
	INDICE DI RISCHIO									
	1	2	3	4	5	6	7	8	9	10
D										Bussole (Metal detector attivo), Roller Cash, Vigilanza e Videosorveglianza
C								Bussole (Metal detector non attivo), Roller Cash e Vigilanza		
B						Bussole (Metal detector attivo), Roller Cash e Videosorveglianza				
A				Bussole (Metal detector non attivo), Roller Cash e Videosorveglianza						
BASE	Sliding Door, Roller Cash e Videosorveglianza									

Tabella 28. Configurazioni minime di sicurezza

- Il REM è intrinsecamente statico e non predittivo. Il REM non prende in considerazione l'elevato livello di dinamicità del dominio applicativo e presta scarsa attenzione ai rischi endogeni quali l'evoluzione del numero di attacchi nel tempo e tipologia degli attacchi a livello nazionale e locale; la disponibilità di nuovi sistemi di protezione; i cambiamenti nei modi in cui i criminali conducono attacchi criminali; ed il peggioramento della situazione del contesto socioeconomico che può portare ad un aumento generale dei reati predatori.
- Informazioni incoerenti e obsolete. i dati raccolti per la stima dei valori di rischio non sono automatizzati ma sono mediati dall'intervento umano, essendo così soggetti ad incoerenza interna, incompletezza, in genere pochi aggiornamenti nel tempo e altri tipi di errori. Gli errori dovuti al caricamento manuale dei dati sul sistema e sui sistemi di protezione in uso possono dare un'immagine errata dello stato di rischio a livello nazionale.
- Elevanti lead times nella definizione del REM. Dopo che il CSO completa la struttura della checklist, la compilazione della stessa da parte del direttore della filiale può durare parecchio tempo (anche settimane). Considerando il numero elevato di dipendenze bancarie per un istituto di credito, il processo può durare, in media, anche più di un mese. Il calcolo dell'indice di rischio e l'individuazione delle misure di protezione richieste per tutte le BB della rete possono dunque essere ulteriormente ritardate di oltre un mese.

P4: la rilevazione di anomalie durante le attività quotidiane ordinarie tende a non essere condotta con attenzione, in maniera tempestiva e con il giusto grado di dinamicità. Nei casi di

attacco in cui sono coinvolti i dipendenti, i direttori BB e gli appaltatori dei servizi di sicurezza, la compilazione del form per la segnalazione dell'evento può essere spesso errata o incompleta a causa del livello di conoscenza degli intervistati o del loro stato psicologico alterato dall'evento criminoso. Inoltre, quando un dipendente segnala un evento criminoso, potrebbe aver dimenticato dettagli rilevanti oppure potrebbe omettere volontariamente di riportare alcune informazioni al fine di ridurre il carico di lavoro richiesto nella compilazione della modulistica. Ciò può ritardare l'indagine dalle autorità preposte al contrasto della criminalità e l'aggiornamento tempestivo delle analisi statistiche periodicamente effettuate dal CSO.

P5: gli effetti della raccolta di dati inconsistenti e incompleti sugli attacchi hanno un impatto in larga misura sulla definizione delle politiche di sicurezza, all'istituzione del modello di valutazione dei rischi, alle categorie di rischio di calcolo dell'indice di rischio e alla definizione dell'insieme delle misure di protezione relative a le categorie di rischio.

CAPITOLO 4: Verso un modello innovativo per la valutazione del rischio di filiale

4.1 Il concetto di rischio: un'analisi della letteratura scientifica.

Il termine "rischio" è ampiamente utilizzato nella vita quotidiana e ampiamente dibattuto nella letteratura scientifica. A seconda del contesto ci sono molte definizioni accettate di rischio. Il concetto comune in tutte le definizioni è l'incertezza dei risultati (Berg, 2010).

Secondo Knight, infatti, per analizzare il concetto di rischio diventa importante partire dalla definizione d'incertezza. Nel suo libro, egli afferma che incertezza e rischio sono entrambi modellati dal fatto che il futuro non è noto. Tuttavia i termini non sono gli stessi, in circostanze di rischio, infatti, le probabilità sono calcolabili, secondo Knight, dunque **si può parlare di rischio soltanto quando è possibile calcolare oggettivamente la probabilità dell'evento futuro**; cioè la distribuzione degli esiti può essere espressa in termini probabilistici. L'incertezza manca, invece, di un calcolo: "All bets are off.". (Knight 1921).

Lindley (2006) ha fornito una spiegazione utile di incertezza:

"Ci sono alcune cose che sapete essere vere, e altre che sapete essere false; Eppure, nonostante si abbia questa vasta conoscenza, rimangono molte cose di cui la verità o la falsità non è nota. Diciamo perciò che non si è sicuri di queste cose. Si è incerti su tutto il futuro in varia misura; molto del passato è nascosto; e c'è molto del presente di cui non si dispone di informazioni complete. L'incertezza è ovunque e non si può rifuggire da essa" (p. XI).

Il concetto di incertezza è intrinsecamente correlato al concetto di rischio negli studi organizzativi. La differenza tra i due è stata a lungo dibattuta, soprattutto per le implicazioni sulla comprensione e sulle principali dinamiche aziendali. Un importante contributo a questo dibattito è stato fatto da Knight (1921) nel suo lavoro "Rischio, incertezza, e Profitto" dove ha stabilito una chiara distinzione tra rischio e incertezza:

...L'incertezza deve essere considerata in maniera radicalmente distinta dalla nozione familiare di rischio, da cui non è mai stata adeguatamente separata. Il termine "rischio", come liberamente usato nel linguaggio di tutti i giorni e in discussione economica, comprende in realtà due cose che, funzionalmente, almeno, nelle loro relazioni causali ai fenomeni di organizzazione economica, sono categoricamente diverseIl fatto essenziale è che concetto di "rischio", sia in alcuni casi suscettibile di misurazione mentre altre volte serve a rappresentare qualcosa di diverso, rendendo difficile la comprensione delle caratteristiche cruciali che contraddistinguono tale fenomeno.

Appare che un'incertezza misurabile, o "rischio" adeguato, come vedremo usare il termine, è tanto differente da una non misurabile che in realtà non si tratta affatto di incertezza. Abbiamo ... di conseguenza limitato il termine "incertezza" ai casi di tipo non-quantitativo.

In "More Than You Know", un libro sulla strategia di investimento, Mauboussin (2007) offre il seguente framework basato sul lavoro di Knight: "allora come possiamo pensare a rischio e incertezza? Un punto di partenza logico è la distinzione di Frank Knight: Rischio è un risultato sconosciuto, ma sappiamo a cosa somigli la distribuzione sottostante dell'esito.

Anche l'incertezza implica esito sconosciuto, ma non sappiamo a cosa somigli la distribuzione sottostante dell'esito. Perciò i giochi d'azzardo come roulette o blackjack sono rischiosi, mentre l'esito di una guerra è incerto. Knight ha detto che la probabilità oggettiva è la base per il rischio, mentre la probabilità soggettiva è alla base dell'incertezza".

La seguente tabella riporta alcune definizioni di rischio riportate nella letteratura scientifica:

Definizione	Fonte
<i>In business terms, a risk is the possibility of an event which would reduce the value of the business were it to occur. Such an event is called an "adverse event." Every risk has a cost, and that cost can be (more or less precisely) quantified. The cost of a particular risk during a particular period of time is the probability of an adverse event occurring during the time period multiplied by the downside consequence of the adverse event. The probability of an event occurring is a number between zero and one, with zero representing an event which will definitely not occur and one representing an event which definitely will occur.</i>	Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In <i>Proceedings of the 2001 workshop on New security paradigms</i> (pp. 97-104). ACM.
<i>The National Institute of Standards and Technology, NIST, defines risk as the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk is traditionally represented by the formula: R(risk) = P * C P: probability of occurrence C: consequence of occurrence either represented by some value or by a loss function</i>	Jennex, Murray E., "Assessing Knowledge Loss Risk" (2009). AMCIS 2009 Proceedings. Paper 446.
<i>"combination of probability or frequency of occurrence of a defined hazard and magnitude of the occurrence"</i>	Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). <i>Supply Chain Management: An International Journal</i> , 16(6), 474-483.
<i>'hazard, chance of bad consequences, loss, exposure to chance of injury or loss "' (Concise Oxford Dictionary). Such definitions illustrate one problem with the term 'risk'—its ambiguous use as a synonym of probability or chance in relation to an event or outcome, the nature of an outcome, or its cause. The US Project Management Institute (PMI) and the UK Association for Project Management (APM) have adopted a broad view of risk. Their definitions of risk are very similar, as follows: Risk—an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective. Risk— an uncertain event or set of circumstances that, should it occur, will have an effect on the achievement of the</i>	Ward, S., & Chapman, C. (2003). Transforming project risk management into project uncertainty management. <i>International Journal of Project Management</i> , 21(2), 97-105.

<i>project's objectives.</i>	
<i>Harland, Brenchley, and Walker (2003) define risk as a chance of danger, damage, loss, injury, or any other undesired consequences. Mitchell (1995) suggests risk contains different types of losses, and the risk of any particular type of loss is a combination of the probability of that loss, P (Loss_n), and the significance of that loss to the individual or organization, I (Loss_n). Therefore, for an event n: Risk_n = P (Loss_n) x I (Loss_n)</i>	Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. <i>Journal of Business Logistics</i> , 29(1), 133-155
<i>"Risk" is defined as the chance of an adverse event depending on the circumstances. The impact of a risk can be measured as the likelihood of a specific unwanted event and its unwanted consequences or loss: where:</i> <ul style="list-style-type: none"> • <i>RI = risk impact;</i> • <i>L = likelihood; and</i> • <i>C = consequence.</i> 	Mills, A. (2001). A systematic approach to risk management for construction. <i>Structural survey</i> , 19(5), 245-252.
<i>The common concept in all definitions is uncertainty of outcomes. Where they differ is in how they characterize outcomes. Some describe risk as having only adverse consequences, while others are neutral. One description of risk is the following: risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.</i>	Berg, H. P. (2010). Risk management: procedures, methods and experiences. <i>Risk Manage</i> , 1, 79-95.
<i>the possibility of experiencing an 'adverse event' – i.e., an 'incident' – and consequently, suffering harm or loss</i>	Volpentesta, A. P., Ammirato, S., & Palmieri, R. (2011). Investigating effects of security incident awareness on information risk perception. <i>International Journal of Technology Management</i> , 54(2/3), 304-320.

Tabella 29. Definizioni di rischio

Per semplificare, si può affermare che il rischio è una conoscenza imperfetta, dove sono note le probabilità dei possibili risultati, mentre esiste incertezza quando queste probabilità non sono note (Hardaker, 2004). Queste prospettive hanno qualche attinenza con l'approccio razionale al decision making. Sembrerebbe che il problema principale con l'approccio razionale dipende dalla difficoltà nel reperire tutte le informazioni necessarie, nel conoscere tutte le possibili alternative di una decisione e, in alcuni casi, acquisire piena comprensione delle conseguenze derivanti da ciascuna alternativa. Il focus dei decisori, prima di essere sul rischio delle alternative, deve essere sull'incertezza di soddisfare le fasi del processo decisionale. In altre parole le domande sono: "Sei sicuro di aver acquisito tutta la conoscenza necessaria per configurare le alternative? Sei in grado di valutare veramente tutte le conseguenze che derivano da ogni alternativa e, quindi, valutare il rischio di ogni decisione? "

L'incertezza è il principale problema che rende l'approccio razionale inutile in situazioni reali (Cravera, 2011).

Un'analisi approfondita sul concetto di rischio condotta da Canale, Leonardi, & Fabiano, (1998), definisce il rischio come "il danno incerto a cui un dato soggetto si trova esposto in seguito a

possibili eventi o concatenazione favorevole degli stessi". Gli autori sottolineano come l'incertezza che si ricollega alla condizione di danno potenziale è riconducibile due differenti dimensioni:

- gli incidenti (ovvero gli eventi sfavorevoli causativi di un danno) possono aver luogo con una probabilità più o meno grande ma che non è mai nulla;
- l'impatto dell'incidente (ovvero l'entità del danno associato all'evento avverso) può cambiare in relazione a circostanze esterne che, vista la loro natura aleatoria, non sono prevedibili in modo certo e univoco.

La definizione quantitativa adottata convenzionalmente, come riportato in (Volpentesta, Ammirato, & Palmieri, 2011), è di fatti la combinazione fra la frequenza (o probabilità) attesa di un certo incidente e la magnitudo (ampiezza dell'impatto) attesa delle conseguenze del verificarsi di tale evento in un dato periodo di tempo.

La frequenza è la probabilità che l'evento avvenga in un determinato intervallo di tempo ed è anche detta la conta delle occorrenze (ad esempio il numero di incidenti l'anno).

Per magnitudo si intende invece l'ampiezza del danno prodotto al verificarsi di un particolare evento negativo (quello che poco prima abbiamo chiamato impatto dell'incidente).

Naturalmente, come evidenziato in (Canale, Leonardi, & Fabiano, 1998), ridurre il rischio (per godere di un maggior grado di sicurezza) vorrà dire predisporre le azioni necessarie, a seconda del contesto di riferimento, che consentano di diminuire:

- l'impatto degli incidenti (tramite misure di protezione dall'incidente),
- la probabilità che l'incidente si verifichi (misure di prevenzione dell'incidente),
- entrambe le dimensioni.

Arlotta definisce il rischio come "qualsiasi evento capace di compromettere il raggiungimento di obiettivi aziendali" e, pertanto, nel suo articolo (Arlotta, 2006) evidenzia come gestire i rischi d'impresa non significa solo mettere in atto tutte le azioni ed i presidi in grado di neutralizzare gli eventi negativi o le attività di controllo derivanti da un'aspettativa contraria (*incertezza*), ma significa anche permettere all'impresa di trasformare le eventuali minacce in opportunità per la creazione di valore (*opportunità*). I rischi e gli eventi ad essi associati, possono dunque secondo Arlotta (Arlotta, 2006) essere:

- *rifiutati*, e cioè respinti sin dalla loro identificazione quali potenziali eventi non allineati al profilo desiderato di rischio dell'impresa (o alla propensione dell'imprenditore);
- *accettati*; in quanto ritenuti trascurabili in termini di frequenza di accadimento degli eventi negativi e di importanza del relativo impatto economico aziendale;
- *gestiti*, e cioè attivamente facenti parte di politiche di gestione attiva (operazioni di copertura totale o parziale e di natura speculativa), in funzione delle diverse fattispecie di evento e delle configurazioni di rischio individuate;
- *trasferiti*, in relazione alla pericolosità dell'evento o in relazione ad una precisa scelta aziendale di avversione al rischio con conseguente volontà di cedere a terzi rischi specifici o interi portafogli di rischi.

Da un punto di vista manageriale, come evidenziato in (Volpentesta, Ammirato, & Palmieri, 2011), il problema è quindi quello di prevedere quanto spesso e in quali casi potrebbe verificarsi un evento dannoso, quali sarebbero le conseguenze complessive di tale evento, e quali contromisure vanno prese per ridurre la possibilità che tale evento si verifichi.

// National Institute of Standards and Technology definisce il rischio come effetto netto negativo dell'esercizio di una vulnerabilità, considerando sia la probabilità che l'impatto del verificarsi (Jennex e Durcikova, 2013). Nella letteratura scientifica il concetto di rischio è spesso inteso come la possibilità di sperimentare un "evento avverso" e di conseguenza, di subire danni o perdite (Breakwell, 2014) (Volpentesta et al., 2011) (Alter e Sherer, 2004). Blakley et al. (2001). L'impatto degli eventi avversi riduce il valore delle attività aziendali che possono essere quantificate più o meno precisamente.

In questo senso, molti paper propongono funzioni matematiche volte a definire questo concetto e misurare il rischio nelle organizzazioni.

Il rischio contiene diversi tipi di perdite e il rischio di una perdita particolare è una combinazione della probabilità di tale perdita, $P(Loss_n)$, e il valore (o l'impatto) di tale perdita per l'individuo o l'organizzazione. La gestione e la mitigazione dei rischi rappresentano problemi cruciali per i gestori in modo da ridurre sia la probabilità che l'impatto degli eventi avversi indesiderati (Haimes, 2015).

In generale, il rischio è tradizionalmente modellato dalla funzione $R = P * C$, dove il rischio (R) è la probabilità (P) di un evento avverso che si verifica durante uno specifico intervallo di tempo moltiplicata per la conseguenza negativa (C) dell'evento negativo (Haimes, 2015). La probabilità che un evento si verifica è un numero tra zero e uno, con zero che rappresenta un evento che sicuramente non si verifica e uno che rappresenta un evento che sicuramente avverrà, mentre la conseguenza del verificarsi è rappresentata da un valore o da una funzione di perdita (Jennex, 2009) (Blakley et al. 2001).

Secondo Segal il rischio può essere suddiviso in tre componenti: l'incertezza, la volatilità e la deviazione rispetto a quanto previsto. L'incertezza si manifesta quando la probabilità è inferiore al 100%, vale a dire quando c'è meno del 100% di probabilità che un evento si verifichi esattamente come previsto. La volatilità ci dice di quanto può variare in termini percentuali il risultato finale mentre la deviazione di quanto varia in termini reali. La sua definizione di rischio è: "...consider risk as the possibility that results may not be exactly equal to expected, but rather are either lower or higher than expected." "Risk is generally thought of as the possibility of a loss." ovvero "...considerare il rischio come la possibilità che i risultati non siano esattamente uguali a quelli previsti, ma piuttosto sono inferiori o superiori ai risultati attesi". Il rischio è generalmente considerato come la possibilità di una perdita". (Segal, 2011).

Esistono diversi tipi di rischi: il **rischio per la sicurezza** che può essere anche definito rischio di natura infortunistica, in quanto si tratta di rischi responsabili di infortuni più o meno gravi in conseguenza di un impatto che può essere di natura fisica, chimica, biologica, meccanica o elettrica (ad esempio carenza di sicurezza degli impianti elettrici dovuta alla mancata attività di

manutenzione degli stessi o all'attività di manutenzione non effettuata correttamente); il **rischio per la salute**, definito anche rischio igienico, si tratta di rischi responsabili della compromissione dell'equilibrio biologico dei lavoratori (ad esempio rischi di esposizione correlati con l'impiego di sostanze chimiche che potrebbero risultare essere tossiche, rischi dovuti all'inalazione di microorganismi presenti nell'ambiente, all'inalazione di fumo, polveri pericolose e nocive); infine abbiamo i **rischi trasversali**, ossia quelli che impattano sia sulla salute che sulla sicurezza, in quanto derivano dal tipo di organizzazione. All'interno dei rischi trasversali troviamo il rischio di rapina.

Nel settore bancario, Van Greuning e Brajovic-Bratanovic (2009) hanno individuato tre categorie principali di rischio:

1. Finanziario: il rischio di incorrere in una perdita a causa di metodi di finanziamento che non si rivelano adeguati per fornire un rendimento positivo come credito, mercato, liquidità.
2. Operativo: il rischio di perdita dovuto a processi inadeguati o falliti, persone e sistemi inadeguati, o a eventi esterni.
3. Ambientale: il rischio associato all'ambiente bancario come fattori macroeconomici e regolatori, stabilità politica e infrastruttura del settore finanziario complessivo.

Secondo (Haines, 2015), possiamo modellare il rischio per la filiale bancaria con la seguente funzione:

$$R(ca) = P(ca) * I(ca)$$

significa che il rischio di un attacco criminale, $R(ca)$, dipende dalla probabilità che si verifichi l'attacco criminale, $P(ca)$, e che esiste un impatto dell'attacco, $I(ca)$. I tipi di attacchi criminali (minacce) che possono danneggiare una dipendenza bancaria includono rapine, furti agli sportelli bancari, furti agli ATM e danni fisici volontari. Ognuno di essi può ridurre il valore degli asset bancari come le persone (dipendenti e clienti della banca), bancomat, sportello, safedeposit boxes, beni strutturali.

Il rischio di rapina è il rischio rappresentativo più significativo nell'ambito del settore bancario. Si tratta di un rischio che ha assunto negli anni sempre più rilevanza destando sempre più l'interesse delle varie associazioni, in particolare esiste un'associazione che si occupa specificatamente di questa problematica, ovvero l'ABI (Associazione Bancaria Italiana).

Generalmente il verificarsi delle rapine in banca è dovuto a fattori socio-economici, alle caratteristiche dei luoghi in cui si trova la filiale bancaria e alle caratteristiche di quest'ultima che possono apparire ai rapinatori come favorevoli per il "buon esito" della rapina e della successiva fuga e soprattutto all'entità del bottino atteso.

4.1.1 La gestione del rischio

La gestione del rischio o Risk Management (RM) è definito come: "il processo che tende a salvaguardare il patrimonio dell'impresa contro le perdite che possono colpirla nell'esercizio della propria attività, attraverso l'uso di strumenti di varia natura (prevenzione, ritenzione, assicurazione, ecc.) e nelle migliori condizioni di costo" (Urciuoli & Crenca, 1989).

Il risk management non riguarda soltanto le imprese o gli enti pubblici, ma qualsiasi attività a breve o lungo termine. I vantaggi e le opportunità offerte non andrebbero valutate semplicemente nel contesto dell'attività in sé, ma in relazione ai molti diversi soggetti interessati sui quali può influire.

Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi positivi) o minacce al successo (elementi negativi). La concezione del risk management come attività legata sia agli aspetti positivi sia a quelli negativi del rischio è sempre più diffusa. Di conseguenza, questo standard valuta il rischio da entrambe le prospettive. Nel campo della sicurezza, si ammette in genere che le conseguenze sono esclusivamente negative e quindi la gestione di questo tipo di rischio si concentra sulla prevenzione e sulla riduzione del danno.

Il risk management fa parte integrante del management strategico di ogni organizzazione. È il processo attraverso il quale le organizzazioni affrontano i rischi legati alle loro attività con lo scopo di ottenere benefici durevoli nell'ambito di ogni attività, in generale e in particolare. La base di un buon risk management consiste nell'identificazione e nel trattamento di questi rischi. Il suo scopo è di conferire il massimo valore sostenibile ad ogni attività dell'organizzazione. Esso permette la comprensione dei potenziali aspetti positivi e negativi di tutti i fattori che possono influenzare l'organizzazione. Incrementa le probabilità di successo, mentre riduce sia le probabilità di fallimento sia l'incertezza sul raggiungimento degli obiettivi generali dell'organizzazione. Il risk management deve essere un processo continuo e graduale che coinvolge tutta la strategia dell'organizzazione e la sua implementazione. Deve affrontare sistematicamente tutti i rischi che circondano le attività dell'organizzazione nel passato, nel presente e, soprattutto, nel futuro. Deve essere integrato nella cultura dell'organizzazione attraverso una politica efficace e un progetto gestito dai massimi dirigenti. Deve trasformare la strategia in obiettivi tattici e operativi, assegnare responsabilità a ogni livello dell'organizzazione rendendo ogni manager e ogni impiegato responsabile della gestione del rischio come parte stessa dei doveri professionali. Favorisce le responsabilità, misura e premia le performance, promuovendo in tal modo l'efficienza operativa a tutti i livelli.

I rischi che minacciano un'organizzazione e la sua gestione possono aver origine da fattori sia esterni sia interni a essa. Il diagramma a tergo riassume esempi di rischi chiave presenti in queste aree e mostra come alcuni tipi di rischi possano avere fattori di stimolo sia esterni sia interni e quindi occupare entrambe le aree. È possibile distinguere ulteriormente le tipologie di rischio, per esempio strategico, finanziario, operativo, potenziale e via dicendo.

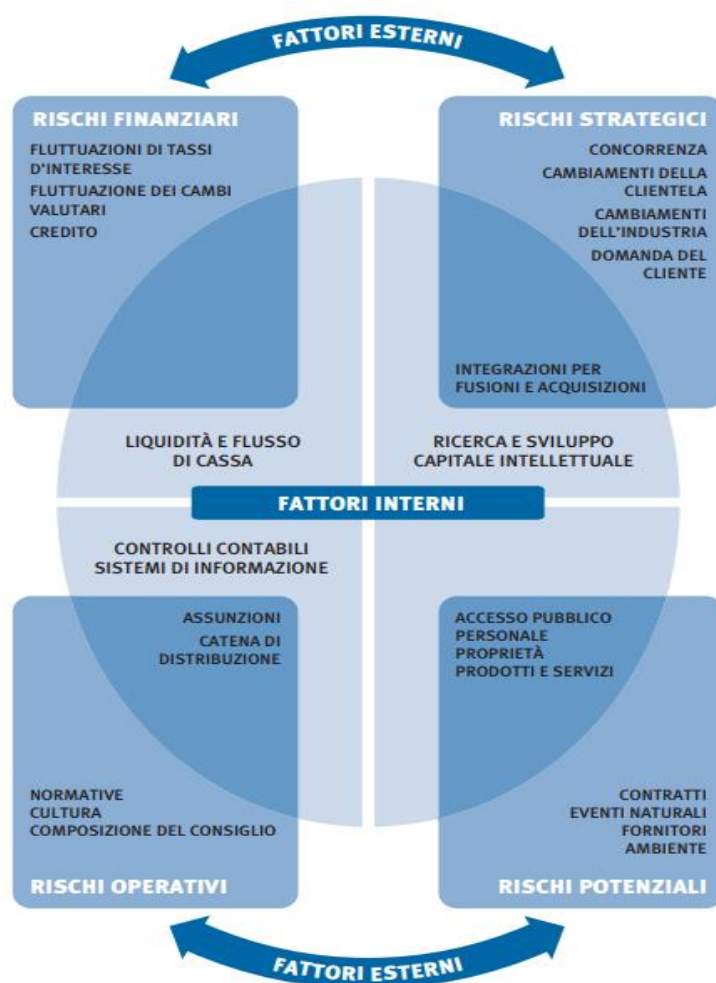


Figura 57. Fattori di rischio

Il risk management protegge e dà valore all'organizzazione e ai suoi stakeholder, sostenendo gli obiettivi dell'organizzazione con:

- la predisposizione di un quadro metodologico che consente uno svolgimento coerente e controllato di ogni futura attività
- il miglioramento del processo decisionale, della pianificazione e della creazione di priorità attraverso una comprensione esauriente e strutturata dell'attività commerciale, della volatilità e degli elementi positivi /negativi del progetto
- il contributo ad un utilizzo/allocazione più efficace del capitale e delle risorse all'interno dell'organizzazione
- la riduzione della volatilità nelle aree non essenziali dell'attività
- la protezione e il potenziamento del patrimonio e dell'immagine aziendale
- lo sviluppo e il sostegno delle persone e della base di conoscenza dell'organizzazione
- l'ottimizzazione dell'efficienza operativa

La letteratura presenta diversi approcci alla gestione del rischio, che si differenziano per la tipologia di rischio considerata rilevante, per la diversa importanza attribuita alle varie fasi del

processo, per gli strumenti utilizzati nel gestire i rischi. Già negli anni '70 emerge una visione «globale» per la quale il risk management ha la funzione di gestire, in un processo olistico, tutti i rischi di un'organizzazione; ma è solo all'inizio del nuovo millennio che la necessità di un ripensamento nei sistemi di gestione dei rischi diviene più concreta e strutturata. Fino alla fine degli anni '90, infatti, la disciplina si fonda ancora prevalentemente su una visione tradizionale del risk management:

DeLoach (2000) definisce l'enterprise risk management come un approccio disciplinato che allinea strategia, processi, persone, tecnologie e conoscenze al fine di stimare e gestire l'incertezza che l'azienda affronta per creare valore.

Gli approcci metodologici al risk management presenti in letteratura sono stati definiti in diversi ambiti di applicazione, tuttavia emergono alcuni aspetti in comune in riferimento agli obiettivi ed ai passi da adottare.

Di seguito, si propone una schematizzazione dei principali approcci metodologici rilevati in letteratura

Ambito di Applicazione	DESCRIZIONE DELLE FASI DELLA METODOLOGIA PROPOSTA	Riferimento
Information security	<ul style="list-style-type: none"> • MEASUREMENT: A common measure of the cost of risk is "Annualized Loss Expectation," or ALE. ALE is the expected cumulative cost of risk over a period of one year as estimated in advance. $ALE = POTENTIAL LOSS * PROBABILITY$ • IDEMNIFICATION: There are two major types of indemnification: pooling and hedging; In pooling schemes, several businesses share the cost of certain risks. Insurance policies are the most common type of risk-pooling scheme. In hedging schemes, a single business essentially places a bet that an adverse event will happen to it. Options are the best-known example of risk hedging scheme. • MITIGATION: A business can try to reduce the expected cost of a risk, either by reducing the probability of the adverse event occurring, or by reducing the consequences if it does occur. The probability of an adverse event can be reduced by redesigning systems or processes to eliminate the event's known or suspected causes. The consequences of an adverse event can be reduced by taking steps to limit the damage the event causes • RETENTION: If an adverse event is not very costly or not very likely to occur, or if the benefits to be realized from taking a risk are great, a business may choose to retain the risk which the adverse event creates. 	Blakley et al., 2001
Knowledge Management	<ul style="list-style-type: none"> • Conduct a Loss Risk Assessment: This is the impact to the organization caused by the loss of a human knowledge source, usually an expert, a knowledge worker, or a manager. The approach uses the following risk algorithm: $R(\text{knowledge loss}) = p(\text{loss of human knowledge source}) * C(\text{loss of perfect human knowledge source}) * Q(\text{quality of human knowledge source}).$ • Ranking Knowledge Loss Risks: Once values have been determined for each of the factors in the below algorithm, a knowledge risk value can be calculated that will be between 1 and 1000. The higher the knowledge loss risk value, the higher the priority for mitigating the risk and this value can be used to rank all knowledge loss risks. • Determining Appropriate Courses of Action: While the knowledge loss 	Jennex and Murray, 2009

	<p>risk value can be used to rank risk, it is not really the intent of the knowledge loss risk value. The more important use of the value is to classify the risk into knowledge capture action categories:</p> <ul style="list-style-type: none"> • ≥ 700: Urgent/immediate action category. • 300 to 699 High priority action category • < 300 Low priority action category 	
Supply Chain Risk Management	<ul style="list-style-type: none"> • RISK IDENTIFICATION: it involves a comprehensive and structured determination of potential SC risks associated with the given problem. • RISK MEASUREMENT: it involves the determination of the consequences of all potential SC risks, together with their magnitudes of impact. Consequences are defined as the manner in which or the extent to which the threat manifests its effects upon the resources. • RISK ASSESSMENT: is synonymous with the assessment of uncertainties (Raiffa, 1982), and is concerned with the determination of the likelihood (probability) of each risk factor. Uncertainties can be assessed by objective information, and probability distributions for relevant SC risks or consequences can be derived. • RISK EVALUATION: it involves the sub-steps of risk ranking and risk acceptance. Risk ranking is based on the determination of risk exposure values for each identified SC risk, and is defined as Risk Exposure Value of Risk Factor. $\text{Risk Exposure Value of Risk Factor} = \text{Risk Consequence Index} * \text{Risk Probability Index}$ <p>Once the SC risks are classified, acceptable levels of risk must be established. The ALARP (as low as reasonably practicable) principle can be used to classify SC risk as unacceptable, tolerable or acceptable"</p> • RISK MITIGATION: it involves the development of risk response action plans to contain and control the risks. • RISK CONTROL: it examines the progress made regarding the implemented risk response action plans; corrective actions can be taken if deviations occur in achieving the desired SC performance 	Tummala and Schoenherr, 2011
Project management	<ul style="list-style-type: none"> • RISK IDENTIFICATION: as a first step in the development of the model, all potential risk factors that would effect the project cost must be identified. At this stage, a broad view should be taken to ascertain without any constraint the risks that are likely to impede the project in meeting its cost target. To assist in this process it is proposed that the risks can be considered with respect to six categories (financial, economic, political, environmental, design, site construction, physical and acts of God) from which a potential list of risks factors are highlighted for reference purposes. In addition, we used the work breakdown structure (WBS) to identify potential risk factors by checklists. • RISK MEASUREMENT: Each cost component identified as a potential risk will have possible consequences, which tend to make the expected cost outcome have a range of possible cost values, rather than a single value. Therefore, in order to include more realistic information in the estimate, a range of values with an approximate probability distribution is determined for each cost element identified on the checklists. By adding all these costs with relevant fixed costs, we can determine the total project cost. • RISK ASSESSMENT: This phase requires an assessment of uncertainties associated with the risk factors that are identified in the form of subjective or objective probability distributions. If objective (historical) data is available, we can determine the most appropriate objective probability distributions by employing Bestfit with Chisquare test for goodness-of-fit or similar software systems. On the other hand, if we 	Tummala and Burchett, 1999

	<p>use experienced project staff, as mentioned earlier, we can generate subjective probability distributions. Either we use subjective or objective probability distributions for cost components; they determine the likelihood of occurrence of a cost estimate associated with each identified risk factor. The triangular distributions, which can be easily formed by three parameter estimates (minimum, most likely, maximum), and normal and logistic distributions, which can be determined by estimating two parameters (mean and standard deviation) are found useful in this study.</p> <ul style="list-style-type: none"> • RISK EVALUATION: it involves the sub-steps of risk ranking and risk acceptance. Risk ranking is based on the determination of risk exposure values for each identified SC risk, and is defined as Risk Exposure Value of Risk Factor. • RISK CONTROL AND MONITORING: we examine the targets set and contract strategies employed as a result of risk evaluation periodically and observe if any deviations would occur. If they occur, necessary corrective actions will be devised and evaluated using the risk evaluation phase of the model. Also, developing and distributing periodic reports on the progress of the project, including the milestones, to the concerned senior management and project personnel is carried out in this phase. At the end of every project life cycle and at the commissioning of the project, the person responsible should collect data and store it in risk data- bases for easy access. 	
Information Systems	<ul style="list-style-type: none"> • context analysis; • risk identification; • risk analysis; • risk evaluation; • risk treatment; • monitoring and review; • communication and consulting. 	Aloini et al., 2007
Supply Chain	<ul style="list-style-type: none"> • RISK IDENTIFICATION is undertaken at both domestic and global levels and in the context of supply, operational, demand, security, macro, policy, competitive, and resource risks. The global environment includes various supply chain partners, and how the environments in these different countries interact with the focal firm home country. In this first step of the risk management framework, the objective is to create what can be referred to as a "pro file" for each of the risks identified (<i>Supply Risks, Operational Risks, Demand Risks, Security Risks, Macro Risks, Policy Risks, Competitive Risks, Resource Risks</i>). The risk pro file contains elements of the specific risk within the broad category, whether the risk is atomistic or holistic, quantitative and/or qualitative, and affects domestic and/or global operations. • RISK ASSESSMENT AND EVALUATION: Not all risks affect all supply chains. A supply chain can be vulnerable to certain risks, but shielded from other risks. Hence, the next step is to determine which risks identified in Step I are critical for the supply chain. Those risks to which a supply chain is more vulnerable should be given more attention. • RISK MANAGEMENT STRATEGY SELECTION: After assessing and evaluating the risks, the next step is to select appropriate strategies to manage the risk. Risk management strategies are geared toward reducing the probabilities of losses associated with risk events. The assessment of risk in Step 2 provides the list of critical risks for which risk management strategies need to be devised. Risk management strategies should be in sync with the supply chain strategy, which in turn should fit with the SBU or corporate strategy. Based on supply and demand uncertainties, Lee (2002) suggests four types (quadrants) of 	Manuj and Mentzer, 2008

	<p>supply chains: efficient (high cost efficiency based on low demand and supply uncertainty), responsive (responsive and flexible to high demand uncertainty and low supply uncertainty), risk-hedging (pooling and sharing of resources in a supply chain with low demand uncertainty and high supply uncertainty), and agile (both hedging and responsive to high demand and supply uncertainty). The following table proposes risk management strategies depending on the quadrant in which the supply chain lies.</p> <ul style="list-style-type: none"> • MITIGATION OF SUPPLY CHAIN RISKS: Even after devising risk management strategies, all risks cannot be avoided. It is important to plan for situations that assume a risk that could be seriously detrimental may be realized. While risk management strategies are used to proactively address' the probability of expected (though uncertain) events, risk mitigation planning provides a firm with a more mature decision making process in facing potential unexpected losses caused by unexpected events. The key to risk mitigation is identifying the possible losses that may happen from an unexpected event. For example, if delivery issues are critical to a business, a risk mitigation plan should include identifying a back-up service provider, and developing a relationship with that provider to replace and/or pick up the capacity slack caused by the unexpected event. 	
Enterprise Risk Management	<ul style="list-style-type: none"> • EVENT IDENTIFICATION – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes. • RISK ASSESSMENT – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis. • RISK RESPONSE – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite. • CONTROL ACTIVITIES – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out. • INFORMATION AND COMMUNICATION – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity. • MONITORING – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both 	Ballou, 2005
Supply Chain	<ul style="list-style-type: none"> • ANALYSIS OF SUPPLY CHAIN. This step is finalized to an examination of the network structure, to define the most suitable performance measure and to delaine the responsibility inside the structure. • IDENTIFY UNCERTAINTY SOURCES. After studying the supply chain structure, in this step it is possible to underline the most important sources of uncertainty that can cause losses for the firm. • EXAMINE THE SUBSEQUENT RISK. In this step we select the risks in the production activities. • MANAGE RISK. At this point, with the aim to manage the risk, a preliminary analysis of risks inside the network and their damages is performed. • INDIVIDUALIZE THE MOST ADEQUATE REAL OPTION. After the risks analysis, it is possible to select the real options more suitable able to coverage against the risks under examination. • IMPLEMENT SUPPLY CHAIN RISK STRATEGY. The last step is finalized to 	Cucchiella and Gastaldi, 2006

	the implementation of the real option strategy defined in the previous steps	
Construction	<ul style="list-style-type: none"> • RISK IDENTIFICATION: Williams (1995) found that the identification of each risk is an essential first step in risk management and is possibly the most difficult. The identification of each source of risk and the components allows the risk item to be separated from others. Consideration of each influencing factor will simplify the analysis and management of the risk (Bajaj, 1997). In risk identification, the key question to ask is: What are the discrete features of the project (risk sources) which might cause such failure? (Godfrey, 1996). • RISK ANALYSIS: Williams (1995) defined the quantification of risk as the magnitude and frequency or time frame of each event. Each event may be a single incident or an aggregation of incidents. There are a number of analysis techniques that may be used as aids to quantify risks. Techniques which may be used in the evaluation of risk include: code optimisation (which is based on subjective estimation), sensitivity analysis, probabilistic analysis Monte Carlo simulation (Songer, 1997), and kinetic tree analysis (which allows the estimated probability of each alternative to be recorded and the probability of a sequence of events to be determined) (Mendenhall et al., 1986) • RISK RESPONSE: The greater the uncertainty associated with a project the more deliberate the response must be. There are ways to respond to risk, some of which may be used in combination: to avoid it, reduce it, transfer it, or absorb it. The most efficient response to risk is to allocate the risk to the party that is in the best position to accept it. This idea has long been part of the understanding of contract lawyers. The contract that the tender is awarded on becomes the instrument that defines the duties and responsibilities of each party. This means that invariably the owner allocates risks to one of the other contracting parties. Contractors, upon receiving a bid request, evaluate the cost of building the project, and will, consciously or not, add contingencies for risks. Very often, contingency premiums are added to the cost “intuitively”, because too often there is no formal risk analysis, so there can be no scientific premium calculation. Risk contingencies are a result of past experiences concealed or hidden within the bid process. 	Mills, 2001
	<ul style="list-style-type: none"> • ESTABLISH GOALS AND CONTEXT: The purpose of this stage of planning enables to understand the environment in which the respective organization operates, that means to thoroughly understand the external environment and the internal culture of the organization. The analysis is undertaken through: <ul style="list-style-type: none"> • establishing the strategic, organizational and risk management context of the organization, and • identifying the constraints and opportunities of the operating environment. <p>Methods to assess the environmental analysis are SWOT (Strength, Weaknesses, Opportunities and Threats) and PEST (Political, Economic, Societal and Technological) frameworks</p> • IDENTIFY THE RISKS: Using the information gained from the context, particularly as categorised by the SWOT and PEST frameworks, the next step is to identify the risks that are likely to affect the achievement of the goals of the organization, activity or initiative. • RISK ANALYSIS: Risk analysis involves the consideration of the source of risk, the consequence and likelihood to estimate the inherent or unprotected risk without controls in place. It also involves identification of the controls, an estimation of their effectiveness and the resultant level of risk with controls in place (the protected, residual 	Berg, 2010

	<p>or controlled risk). Qualitative, semi-quantitative and quantitative techniques are all acceptable analysis techniques depending on the risk, the purpose of the analysis and the information and data available. Using the consequence criteria provided in the risk matrix, one has to determine the consequences of the event occurring (with current controls in place). To determine the likelihood of the risk occurring, one can apply the likelihood criteria (again contained in the risk matrix). As before, the assessment is undertaken with reference to the effectiveness of the current control activities. To determine the level of each risk, one can again refer to the risk matrix. The risk level is identified by intersecting the likelihood and consequence levels on the risk matrix. Complex risks may involve a more sophisticated methodology. For example, a different approach may be required for assessing the risks associated with a significantly large procurement. Special approaches exist to analyse major risk in complex projects, e. g. described in (Cagno et al. 2007).</p> <ul style="list-style-type: none"> • EVALUATE THE RISK: Once the risks have been analysed they can be compared against the previously documented and approved tolerable risk criteria. When using risk matrices this tolerable risk is generally documented with the risk matrix. Should the protected risk be greater than the tolerable risk then the specific risk needs additional control measures or improvements in the effectiveness of the existing controls. The decision of whether a risk is acceptable or not acceptable is taken by the relevant manager. A risk may be considered acceptable if for example: <ul style="list-style-type: none"> – The risk is sufficiently low that treatment is not considered cost effective, or – A treatment is not available, e.g. a project terminated by a change of government, or – A sufficient opportunity exists that outweighs the perceived level of threat. If the manager determines the level of risk to be acceptable, the risk may be accepted with no further treatment beyond the current controls. Acceptable risks should be monitored and periodically reviewed to ensure they remain acceptable. The level of acceptability can be organizational criteria or safety goals set by the authorities. • TREAT THE RISK: An unacceptable risk requires treatment. The objective of this stage of the risk assessment process is to develop cost effective options for treating the risks. Treatment options, which are not necessarily mutually exclusive or appropriate in all circumstances, are driven by outcomes that include: <ul style="list-style-type: none"> – Avoiding the risk, – Reducing (mitigating) the risk, – Transferring (sharing) the risk – Retaining (accepting) the risk. <p>Avoiding the risk - not undertaking the activity that is likely to trigger the risk. Reducing the risk - controlling the likelihood of the risk occurring, or controlling the impact of the consequences if the risk occurs.</p> • MONITORING THE RISK This step requires the description of how the outcomes of the treatment will be measured. Milestones or benchmarks for success and warning signs for failure need to be identified. 	
--	--	--

Tabella 30. Approcci metodologici al Risk Management

Dall'analisi della letteratura emerge che gli approcci metodologici proposti, nonostante gli ambiti di applicazione differenti ed un numero di step che varia di volta in volta, presentano caratteristiche comuni.

Alla luce di tali considerazioni, la metodologia proposta in questo lavoro si compone delle seguenti fasi:

Il metodo adottato per definire un modello di rischio per le dipendenze bancarie è caratterizzato dai seguenti 4 passi:

- **Fase 1:** Identificazione del rischio
- **Fase 2:** Valutazione del rischio
- **Fase 3:** Individuazione delle azioni correttive atte a ridurre il rischio
- **Fase 4:** Definizione del modello di rischio di filiale

4.2 Fase 1: L'identificazione del rischio

La sicurezza è un concetto in continua evoluzione che ha costanti ripercussioni sull'ambiente socio-lavorativo. Le dimensioni su cui si fonda sono principalmente due: la dimensione esterna che è intesa come oggettiva e la dimensione interna, interpretata come soggettiva. Spaltro (Spaltro, 1996) ravvede in questa distinzione nella salvaguardia della vita e della salute dell'individuo e della società cui si appartiene (la *safety*) e nella tutela e salvaguardia dei propri beni materiali (la *security*).

4.2.1 Il concetto di safety

Tre dei principali dizionari della lingua inglese: American Heritage Dictionary of the English Language (American Heritage, 2000) , The Oxford Pocket Dictionary of Current English (Oxford dictionaries, 2010) e Merriam Webster's Collegiate Dictionary (Merriam-Webster, 2008) , concordano quasi perfettamente sulla definizione di *safety* come: "la condizione di essere al sicuro, la libertà dal pericolo, dal rischio, o dal danno." La *safety* è definita quindi da Misra, nel suo testo "Handbook of Performability Engineering" (Misra, 2008), come la condizione di essere protetti da conseguenze di tipo fisico, sociale, spirituale, finanziario, politico, emozionale, occupazionale, fisiologico, educativo o di qualunque altro tipo derivanti da guasti, danni, errori, incidenti o da qualunque altro evento che possa essere considerato *non desiderabile*. Ciò può avvenire sotto forma di protezione da un evento o dall'esposizione a qualcosa che può causare perdite economiche o di salute. Può includere la protezione di persone o beni.

La *safety* ha quindi un impatto reale e significativo sul rischio di morte, danni o danneggiamenti alle proprietà. In relazione ai rischi percepiti possono essere proposti diversi tipi di interventi, i due più comuni sono quelli di tipo ingegneristico e legislativo.

E' importante distinguere fra prodotti che rispondono agli standard di sicurezza, e prodotti che semplicemente appaiono sicuri. Misra (Misra, 2008), differenzia appunto i concetti di *safety* in:

- *normative safety* (sicurezza normativa) un concetto che descrive prodotti o progetti che corrispondono a standard progettuali applicabili

- *substantive safety* (sicurezza sostanziale) un concetto di sicurezza dato dalla consuetudine e rispettato, indipendentemente dagli standard adottati
- *perceived safety* (sicurezza percepita) che si riferisce al livello di sicurezza percepito dagli utenti. Ad esempio, il sistema dei semafori è percepito come sicuro, nonostante in alcuni casi possa favorire l'aumento del traffico o degli incidenti ad un incrocio.

In (Crescentini, Sada, & Giossi, 2007) gli autori definiscono la *safety* come: “ la salvaguardia o la protezione da eventi o circostanze generalmente indipendenti da precise volontà (eventi quindi accidentali) che comportano alta potenzialità lesiva in funzione del tipo di attività svolta.”

L'Encyclopædia Britannica (Encyclopædia Britannica, 2011) identifica in particolare la *safety* con tutte quelle attività che cercano al contempo di minimizzare e di eliminare le condizioni di pericolo che possono causare danni alle persone. Secondo il testo le precauzioni relative alla sicurezza fanno parte delle due categorie principali: sicurezza sul lavoro (*occupational safety*) e sicurezza pubblica (*public safety*). La *occupational safety* si occupa di tutti quei rischi che sono presenti nelle aree in cui la gente lavora: uffici, stabilimenti di produzione, aziende agricole, cantieri edili e strutture commerciali e di vendita al dettaglio. La *public safety* si interessa invece ai rischi che si incontrano a casa, in viaggio e nel tempo libero, ed in tutte le altre situazioni che non rientrano nell'ambito di applicazione della sicurezza sul lavoro.

Oggi la preoccupazione per la *safety* è diffusa a livello mondiale ed è competenza di numerosi enti governativi e privati a livello locale, nazionale e internazionale.

I tassi di frequenza e la gravità degli incidenti variano da paese a paese e da industria ad industria. Nelle nazioni industrializzate del mondo, gli incidenti in questo momento causano più morti di tutte le malattie infettive e più di ogni singola malattia, fatta eccezione per le malattie cardiache e il cancro. Gli incidenti in casa, nei trasporti pubblici e privati, e nelle aziende agricole e nelle fabbriche sono di gran lunga la causa predominante di morte nella popolazione dei paesi industrializzati sotto i 35 anni. Su base mondiale, gli incidenti su veicoli a motore tendono ad essere la prima causa di morte accidentale, seguita da quelle nel settore industriale ed in casa.

Artley e Stroh (2001), inseriscono la *safety* tra i sei principali indicatori delle prestazioni di un'organizzazione. Gli autori inquadrano la *safety* come la totalità delle misure approntate per la salute globale dell'organizzazione e dell'ambiente di lavoro dei suoi dipendenti.

Il discorso si fa più complesso quando si estende le responsabilità della *safety* anche alla realtà esterna all'organizzazione, associandola ai cosiddetti *rischi imprenditoriali*, che in (Vaccaro, 2005) sono definiti come: “il complesso dei rischi derivanti dall'attività imprenditoriale nei confronti delle persone, delle cose dell'impresa e del mondo esterno”.

In questo caso, per citare (Vaccaro, 2005), l'imprenditore è il primo responsabile di:

- salvaguardia della salute e della sicurezza dei lavoratori dell'impresa;
- dell'impatto ambientale dell'impresa sul mondo circostante;
- dell'impatto sociale dell'impresa sul mondo esterno (anche se quest'ultima responsabilità non è ancora completamente codificata).

L'imprenditore ha quindi una serie di incombenze da espletare in tema di *safety*, a cui non può sottrarsi senza rischiare di incorrere in reati civili e penali. Tuttavia, anche la società esterna ha il dovere di svolgere i suoi compiti di monitoraggio e prescrizione, con l'ausilio dei suoi rappresentanti legali.

Per proteggere l'asset più prezioso dell'organizzazione, ovvero le persone che vi lavorano, l'imprenditore ha la necessità di formulare ed implementare un programma che si occupi di *safety* e di salute (*health*) sul posto di lavoro. Ovviamente questo programma sarà tanto più complesso e corposo quanto più grande sarà la dimensione dell'organizzazione ed il livello di rischio legato al particolare settore di business. L'obiettivo di fondo resta comunque il raggiungimento e il mantenimento di un posto di lavoro sicuro e salubre; per poterlo centrare in pieno, bisogna tener conto dei quattro elementi citati sul sito del Dipartimento del Lavoro degli Stati Uniti, nella sezione "Occupational Safety & Health Administration" (Hodges, 2000):

1. Impegno del management e coinvolgimento dei dipendenti
2. Analisi del luogo di lavoro
3. Prevenzione e controllo dei rischi
4. Formazione rivolta alla *safety* ed alla salute

4.2.2 Il concetto di Security

La definizione di base di *security* può essere sintetizzata come "tutela e salvaguardia dei propri beni materiali". La *security* è stata associata, in (Vaccaro, 2005), ai *rischi non imprenditoriali*, cioè ai rischi originati sull'impresa dal mondo esterno (e sempre più spesso anche dall'interno dell'impresa).

La *security* può esser definita quindi come: "la condizione (oggettiva o percepita, di un individuo, una comunità, un'istituzione, uno Stato) di protezione da pericoli o minacce come attività criminali, terrorismo, altri atti deliberati o ostili, o disastri (naturali o di origine umana)" (Astarita, 2005).

E' evidente che i rischi legati alla sicurezza sul luogo di lavoro variano a seconda del business dell'organizzazione, della sua collocazione fisica e dei suoi orari di lavoro. L'elemento da cui partire, in qualsiasi iniziativa che desideri tutelare la sicurezza sul posto di lavoro, è pertanto l'individuazione dei rischi potenziali ed esistenti. Questa fase è fondamentale per poter poi stabilire le contromisure adeguate per prevenire, controllare o minimizzare ogni tipo di minaccia.

Nel testo di Vaccaro (Vaccaro, 2005), i rischi rilevanti generati dal mondo esterno possono essere distinti in varie categorie in funzione della loro causa scatenante:

A) Calamità

- ◆ Naturali – Terremoti, maremoti, uragani, eruzioni, inondazioni, ecc.
- ◆ Ambientali – Inquinamenti, epidemie, ecc.
- ◆ Di origine sociale – Insurrezioni, scioperi generali e selvaggi, blocchi, dimostrazioni, ecc.
- ◆ Di origine tecnica – Black out totali di erogazione utilities, comunicazioni, ecc.

B) Atti di danneggiamento diretto

- ◆ Terroristici – Attentati dinamitardi, chimici e batteriologici, attacchi armati, sabotaggi, ecc.
- ◆ Vandalici – Furti, incendi, intrusioni, irruzioni, produzione guasti, ecc.
- ◆ Di costrizione fisica o psicologica
- ◆ Minacce, aggressioni, percosse, sequestri, ricatti, pedinamenti, adescamenti, ecc.
- ◆ Di sottrazione o alterazione – Brevetti, marchi, procedure, documenti, know-how

C) Atti di danneggiamento indiretto

- ◆ Generazione di psicosi – Come conseguenza di atti di danneggiamento diretto o per informazioni non filtrate
- ◆ Sfruttamenti impropri – Di marchi, di pubblicità o per contraffazioni
- ◆ Infiltrazioni – Di virus su sistemi di telecomunicazione o infiltrazioni in canali commerciali, finanziari, tecnici e procedurali
- ◆ Attacchi su media

I rischi generati dall'interno dell'impresa possono essere identificati sostanzialmente in:

- Sottrazione o alterazione di brevetti, marchi, procedure, beni materiali, know – how
- Incompetenza delle persone
- Infedeltà delle persone
- Violenza delle persone.

La maggior parte dei rischi che vedono la luce all'interno delle organizzazioni sono correlati, in quello che in letteratura è noto come "Approccio basato sui costi di agenzia", al fatto che l'agire dei dipendenti è spinto da interessi individuali, oltre che dalla volontà di raggiungere gli obiettivi comuni dell'impresa.

In generale, possiamo quindi concludere che la *security* è notevolmente condizionata da due soggetti che sono chiamati ad agire insieme, affinché si arrivi ad un livello di "sicurezza socialmente accettabile" nel senso più ampio del termine:

- Il mondo esterno all'impresa, attraverso tutti i suoi responsabili politici, governativi, culturali, magistratura, forza dell'ordine, organi di sorveglianza, organi di pronto intervento, organismi sociali.
- L'imprenditore, attraverso tutti i mezzi dell'impresa.

Negli ultimi anni, l'ambito della *security* sul luogo di lavoro ha poi subito una notevole espansione, conquistando contestualmente maggiore visibilità. Questa crescente attenzione è legata a molteplici fattori, tra i quali si evidenziano: l'aumento della violenza sul posto di lavoro, le crescenti necessità di sicurezza legate all'utilizzo di Internet e della tecnologia, le minacce del terrorismo ed una più cospicua responsabilità legale attribuita alle imprese che non adottano misure adeguate per salvaguardare il luogo di lavoro dalle minacce alla sicurezza.

E' chiaro che, come per la *safety*, l'ampiezza e la complessità dell'intervento organizzativo in materia di *security* è legato alla natura del business ed ai rischi ad essa correlati. Prioritari, anche per la formulazione e la realizzazione di un programma di *security*, risultano: l'impegno profuso dal management, il coinvolgimento attivo e pro-attivo dei dipendenti, la fase di

identificazione, valutazione e gestione dei rischi, l'addestramento e la consapevolezza in tema di *security*. Tra le azioni maggiormente implementate all'interno dei programmi di *security* delle organizzazioni ricordiamo:

- La creazione di una funzione che si occupi formalmente di *security*.
- La formulazione di una serie di criteri e procedure da seguire per l'utilizzo dei computer e delle reti.
- Il coinvolgimento e l'empowerment dei dipendenti allo scopo di accrescerne la motivazione e la responsabilità nei riguardi degli obiettivi di sicurezza e ridurre contestualmente la tentazione di comportamento opportunistico.
- L'ideazione di contratti di lavoro nei quali siano inclusi accordi di non concorrenza ed altri tipi di clausole per la tutela delle informazioni riservate e della proprietà intellettuale.
- La creazione e lo sviluppo di piani per la gestione di crisi ed emergenze.
- La segnalazione degli incidenti indirizzata al responsabile o al gruppo che si occupa di *security* in quella particolare area e la conseguente apertura di indagini.
- La formulazione delle procedure atte a prevenire la violenza sul posto di lavoro.
- La disposizione di norme e metodi per la prevenzione di frodi, furti e rapine.
- L'installazione di sistemi di sicurezza locali.
- Lo sviluppo di politiche di protezione del perimetro aziendale e controllo degli accessi.
- La salvaguardia delle informazioni.

Bisogna infine tener conto che, per garantire un livello di *security* efficace, è necessario gestire sia gli aspetti tecnologici che le procedure operative e organizzative. Quindi la sicurezza dell'informazione non è un prodotto, ma un **processo globale** che richiede competenze specifiche e un'attenzione diffusa in tutto il personale; essa, come sottolineato in (Data Ufficio, 2006), racchiude ambiti diversi:

❖ *Sicurezza logica*

Si occupa principalmente di quello che è connesso con la memorizzazione e l'accesso ai dati:

- controlli e registrazione accessi
- controllo antivirus
- controllo dei software
- verifiche sui dati ed i trattamenti
- firma digitale
- cifratura dati trasmessi
- firewall e sicurezza reti di telecomunicazioni
- controllo traffico di rete, controllo instradamento

❖ *Sicurezza fisica*

Si occupa di proteggere quelle aree e zone aziendali dove l'informazione è custodita:

- vigilanza ed ingressi controllati

- sistemi di allarmi e antintrusione
- registrazioni accessibili
- custodia armadi
- dispositivi antincendio
- gruppo elettrogeno di continuità
- controllo manutenzione

❖ *Sicurezza organizzativa e procedurale*

Si occupa dell'analisi e dell'implementazione del sistema di gestione:

- definizione di ruoli, compiti e assegnazione delle responsabilità
- definizione di procedure per rafforzamento delle contromisure
- formazione
- definizione degli obiettivi

Perché un'organizzazione si esprima al massimo delle proprie potenzialità, è ormai acclarato che uno degli elementi chiave è l'adozione di misure che garantiscano la *safety* e la *security* per l'intero personale. Tra le due discipline esistono, come abbiamo visto, sia punti di contatto che divergenze. Entrambe si occupano essenzialmente di proteggere qualcosa: **la safety protegge il benessere fisico ed emotivo dei dipendenti, la security i beni materiali ed immateriali dell'organizzazione e i dipendenti da atti di violenza e sopraffazione.** Oltre all'oggetto/soggetto da salvaguardare, un'altra differenza tra *safety* e *security* si può ricercare nel fattore "**intenzionalità**", parte integrante delle azioni che rientrano nella sfera della *security* (se si escludono le cause legate alle varie calamità) ed assente invece negli incidenti di *safety* (correlati per lo più a carenze, omissioni, errori).

Nei paragrafi che si sono occupati della *safety* e della *security* a livello organizzativo, si è posto l'accento sull'importanza che, in questo ambito, riveste la realizzazione di un programma scritto per entrambe le problematiche, che affronti i particolari rischi operativi e le minacce alla sicurezza. La costruzione di un programma di questo tipo richiede ampia cura, impegno e l'utilizzo di pratiche adeguate. Molte tra **le pratiche più efficaci sono comuni ai programmi di safety e di security:**

- ❖ Una cultura organizzativa orientata alla sicurezza e al cambiamento ed un management che supporti visibilmente ed attivamente l'iniziativa sono i presupposti necessari per il successo di qualsiasi programma di *safety* e *security*.
- ❖ Gli obiettivi dei piani di *safety* e *security* sono entrambi collegati al piano strategico dell'organizzazione.
- ❖ I dipendenti sono attivamente coinvolti nel fornire un feedback e nel contribuire alla formazione e all'attuazione delle politiche.
- ❖ I compiti e le responsabilità sono attribuiti in modo chiaro e preciso in materia di *safety* e *security*.
- ❖ La performance aziendale è direttamente collegata ai risultati di entrambi i programmi.

- ❖ Un'ampia attenzione all'attività di formazione, per garantire il trasferimento di nuove conoscenze, esperienze e capacità in materia di *safety* e *security*.
- ❖ La risposta tempestiva alle emergenze, la gestione della crisi e la continuità del business sono tra i target prioritari sia dei programmi di *safety* che di *security*.
- ❖ I processi legati alla *safety* ed alla *security* sono inquadrati in un'ottica di miglioramento continuo; il fine ultimo è quello di arrivare a considerarli come un modo alternativo di vivere dell'intera organizzazione e non più come mere procedure da applicare per non incorrere in problemi di natura penale, civile, sociale o imprenditoriale.

Tra le pratiche che differenziano i programmi di *safety* e *security* possiamo invece annoverare:

- La gestione delle informazioni, improntata alla riservatezza ed alla discrezione in materia di *security*, volta invece alla più ampia diffusione nel caso della *safety*.
- La segnalazione degli incidenti, indirizzata a gruppi specifici e ristretti in tema di *security*, rivolta alla totalità dei dipendenti nel caso di *safety*.

Inoltre, è da evidenziare che sia la *security* che la *safety* possono trarre enormi vantaggi dalla tecnologia; un gran numero delle attività che sono svolte grazie o con l'ausilio della tecnologia sono comuni ad entrambi i programmi. Fra queste si possono annoverare l'elaborazione della documentazione, la gestione e la verifica delle performance, le comunicazioni elettroniche; altre attività sono invece peculiari della *safety*, come l'acquisizione e l'analisi dei dati legati ad infortuni o malattia, o della *security*, come la gestione dei dati delle telecamere di sicurezza.

In conclusione, ***safety* e *security* sono due facce della medesima medaglia: la sicurezza nelle organizzazioni.** Per questa ragione è necessario che il programma di *safety* e quello di *security* siano inquadrati come la continuazione l'uno dell'altro, come due entità che debbono non solo coesistere ma che è necessario integrare e coordinare, all'interno di una più ampia politica di *security and safety culture* che renda più sicura e più competitiva l'intera organizzazione.

4.2.3. Identificazione dei reati ai danni delle dipendenze bancarie

Come abbiamo constatato in precedenza, un'analisi approfondita del concetto di "*rischio*" è fondamentale per comprendere il concetto di sicurezza al fine di giungere ad una diffusa cultura della sicurezza all'interno delle organizzazioni.

Valutare il rischio significa quindi determinare la frequenza di un incidente ed il danno che può derivarne, allo scopo di approntare le opportune misure di sicurezza attraverso cui minimizzarne sia il numero di occorrenze che le conseguenze negative.

Lo stesso "Testo unico in materia di salute e sicurezza sul lavoro"⁸, emanato nel 2008, prescrive nell'articolo 2: la "*valutazione globale e documentata di tutti i rischi per la salute e sicurezza dei lavoratori presenti nell'ambito dell'organizzazione in cui essi prestano la propria attività,*

⁸ Per Testo unico in materia di salute e sicurezza nei luoghi di lavoro si intende, nell'ambito del diritto italiano, l'insieme di norme contenute nel Decreto legislativo 9 aprile 2008, n. 81 che - in attuazione dell'articolo 1 della Legge 3 agosto 2007, n. 123 - ha riformato, riunito ed armonizzato, abrogandole, le disposizioni dettate da numerose precedenti normative in materia di sicurezza e salute nei luoghi di lavoro succedutesi nell'arco di quasi sessant'anni, al fine di adeguare il corpus normativo all'evolversi della tecnica e del sistema di organizzazione del lavoro. Ad esso sono state apportate importanti modifiche e integrazioni dal d.lgs. 3 agosto 2009, n.106.

finalizzata ad individuare le adeguate misure di prevenzione e di protezione e ad elaborare il programma delle misure atte a garantire il miglioramento nel tempo dei livelli di salute e sicurezza”

Quanto detto è ancor più necessario in ambito bancario, nostro settore di interesse, per via dall’aumento della complessità della gestione aziendale che dà vita a nuovi fattori di rischio o che provoca l’acuirsi di problematiche già esistenti.

Il problema della sicurezza delle dipendenze bancarie è quindi complesso e articolato e si combatte, come sempre, sui due fronti:

- ❖ **della *security* che, nel caso della dipendenza bancaria, è connesso alla sicurezza del luogo e quindi alla protezione delle transazioni economiche che in esso si svolgono e, più in generale, dell’intero patrimonio bancario; il rischio dell’incidente è sia diretto, inteso come danno economico alla specifica dipendenza che si ribalta come danno all’istituto bancario, che indiretto, nel senso di perdita d’immagine aziendale.**
- ❖ **della *safety* che fa invece riferimento alla sicurezza fisica (salute psico-fisica) dei dipendenti e dei clienti della banca presenti in filiale al momento dell’evento. Bisogna tener presente che l’articolo 18 del “Testo unico in materia di salute e sicurezza sul lavoro” detta una serie di obblighi a carico del datore di lavoro e del dirigente rivolti proprio alla tutela della *safety* dei propri dipendenti rispetto al potenziale incidente.**

Una policy di sicurezza per dipendenze bancarie (obiettivo del presente progetto di ricerca) consiste in un insieme di principi, regole e linee guida di riferimento che, divenendo un “must known” all’interno delle dipendenze stesse, riesca ad individuare quali siano gli asset bancari critici per l’organizzazione, cosa possa essere considerato utile e cosa no, quale sia il loro uso accettabile e come possano essere protetti (Wiant, 2005). Questa policy dovrebbe essere approvata dal top management che la pubblica e diffonde all’interno dell’organizzazione al fine di testimoniare la volontà forte del management nell’intraprendere politiche di sicurezza perlomeno riferite agli aspetti critici dell’organizzazione.

Affinché questa policy possa essere efficace, la stessa deve essere formalizzata, sempre aggiornata e comunicata tempestivamente dal management in base ai cambiamenti principali del contesto di riferimento (cambi nella strategia aziendale, modifiche importanti sia nell’organizzazione che nella tecnologia in uso, nuovi tipi di incidenti scoperti o nuove indicazioni rispetto all’impatto di incidenti noti, ecc.)

Per poter identificare il rischio è necessario chiarirne la definizione che viene indicata nella “Direttiva Quadro” della Comunità Europea che ha formalizzato in ambito comunitario metodologie e procedure per la valutazione dei rischi nei luoghi di lavoro, e quindi preso come base per la formulazione del Decreto Legislativo 626/94 per quanto riguarda il sistema italiano. Il decreto distingue tra pericolo e rischio: mentre per pericolo si intende la potenzialità di un oggetto o di una condizione organizzativa di causare un danno, il rischio viene definito come “la

probabilità che sia raggiunto il livello potenziale di danno nelle condizioni d'impiego e/o esposizione, nonché il possibile peso del danno stesso" (Peruzzi, 2011).

Ne consegue che valutare il rischio significa sia stimare la probabilità che si verifichi un evento dannoso, sia stimare il danno che da quell'evento può derivare. Questo allargamento della valutazione porta con sé l'obbligo, da parte del Datore di Lavoro, di includere nel "classico" documento di valutazione dei rischi anche la valutazione dei cosiddetti "rischi psicosociali". I rischi psicosociali possono essere definiti come "quegli aspetti della progettazione del lavoro e dell'organizzazione e gestione del lavoro, nonché i rispettivi contesti ambientali e sociali, che possono arrecare danni fisici o psicologici." (Cox & Griffiths, 1995). I rischi di natura psicosociale sono stati identificati come stress, mobbing e burnout.

L'identificazione, dunque, risulta essere la fase più delicata, nonché la più importante per poter trattare il rischio in maniera corretta. I rischi a cui ci riferiamo sono quelli derivanti dai reati enucleati nel codice penale (rapina, furto, frode e danneggiamento). Tuttavia durante l'analisi dei dati statistici, presente nell'allegato 2, si parlerà di rapina, furto, attacco atm e danneggiamento. Per chiarire i dubbi che potrebbero nascere dai due differenti modi di identificare i rischi si vuole dare una spiegazione che permetta di conciliarne il significato. La rapina e il danneggiamento sono intese così come dichiarate nel codice penale. La definizione riportata nel codice penale va però limitata al solo contesto bancario. Per furto si definirà (riferito sempre all'ambito bancario) il reato di "furto in agenzia" o di "furto a danni di terzi" o di "furto con destrezza". Quest'ultimo coincide con il reato di "frode". Infine l'attacco all'Atm sarà il furto così come inteso nel codice penale limitatamente all'azioni criminose compiute ai bancomat. Questa scelta è dovuta all'esigenza di venire incontro agli aspetti tecnologici e organizzativi relative alle misure di contrasto per queste tipologie di reato.

Identificare i rischi è fondamentale per capire quali dovranno essere le misure sulle quali concentrarsi affinché si possa giungere alla riduzione degli stessi.

Per quanto riguarda le rapine il rischio non interessa unicamente il patrimonio ma soprattutto la salute del dipendente e delle persone che si trovano in filiale al momento del crimine. Proprio per tale ragione l'obiettivo del progetto è quello di individuare strumenti e tecnologie che siano in grado di preservare la safety delle persone e la security di persone e dipendenza bancaria.

OGGETTO DEL REATO: Una volta chiarito il concetto di rischio e le condizioni (reati) che lo provocano nel contesto bancario è necessario fare distinzione tra reati di natura fisica e reati di natura informativa, bisogna dunque dare una spiegazione dell'oggetto del reato.

L'oggetto del reato è di *natura fisica* quando vengono sottratti preziosi, banconote, beni strutturali e valori in genere.

Il caso in cui la sottrazione riguarda l'identità oppure si cerca eseguire azioni che "contaminino" l'immagine della banca ci troveremo a parlare di oggetto del reato di *natura informativa*.

- *Furto di denaro e/ o preziosi.* Sebbene i nuovi e sofisticati impianti di sicurezza ne abbiano reso più ardua e difficile la riuscita, il furto con scasso in banca e la spoliazione

della cassaforte e/o delle cassette di sicurezza all'interno del Caveau, resta una tipologia di crimine ancora assai temuta da banche e forze dell'ordine e non del tutto debellata. L'impatto di un furto con scasso è in realtà notevole poiché può comportare perdite non solo per la Banca e la sua immagine ma anche per i clienti stessi; esemplare in questo senso è il caso di un recente furto con scasso, citato in un articolo apparso sul portale on-line del Corriere del Mezzogiorno (Corriere del Mezzogiorno, 2011), avvenuto ai danni di una dipendenza bancaria a Foggia; qui i malviventi sembra abbiano forzato nottetempo con l'acido 250 cassette di sicurezza e rubatone gran parte del contenuto. In situazioni del genere, oltre al danno "affettivo" relativo alla perdita del contenuto delle cassette, i clienti potrebbero infatti trovarsi coinvolti in lunghe cause civili con la banca per ottenere un risarcimento per il danno subito. A tale proposito, in (Avvocati.it, 2011) troviamo spiegata la sentenza n. 19363/2011 con cui la Cassazione ha respinto la richiesta di risarcimento danni di una famiglia romana che, ben 22 anni fa, aveva perduto il contenuto della propria cassetta di sicurezza a seguito di un furto a danno della propria filiale. La motivazione della sentenza risiede nel fatto che l'istituto è riuscito a dimostrare che le misure di sicurezza adottate all'epoca erano adeguate e tecnologicamente al passo con i tempi. La riuscita del colpo è pertanto unicamente da attribuire all'estrema abilità dei ladri, motivo per cui i clienti non possono pretendere un risarcimento dalla banca per il maltolto, ma solo un piccolo rimborso. L'impatto sulla *security* perciò, sebbene in prima battuta riguardi la banca, può avere ripercussioni anche sulla *security* dei clienti. L'impatto sulla *safety* è trascurabile⁹.

- *Furto di beni mobili di proprietà della banca*. Questo tipo di furto prende di mira quelli che sono i beni mobili della banca, quali: computer, fax, stampanti, attrezzature di videosorveglianza e così via. E' chiaramente una tipologia di furto meno frequente delle altre analizzate poiché prende di mira oggetti con un valore relativamente ridotto. Ciononostante la cronaca ci informa di tanto in tanto relativamente a furti che rientrano in questa categoria e che se, come nel caso del furto di computer avvenuto alla Cassa di Risparmio di Padova a novembre dello scorso anno (Cronaca Live, 2011)), coinvolgono i computer aziendali, possono avere l'aggravante di mettere a rischio eventuali dati sensibili. In questo caso quindi l'impatto è principalmente sulla *security* della banca e solo in rari casi, quando sono messi a rischio i dati riservati dei clienti, può interessare anche la *security* dei clienti.
- *Attacco fisico (furto) agli Atm*¹⁰. Come evidenziato nell' e-book "Soluzioni innovative di sicurezza per le banche" (Iaconis, Limentanti, & Rossi, 2011) il problema della sicurezza

⁹ D'ora in avanti, se l'impatto sulla *safety* è trascurabile, non sarà citato.

¹⁰ Atm è l'acronimo di Automated Teller Machine. E' uno sportello per il prelievo automatico di denaro contante. L'ultima versione di Atm è abilitata anche per il versamento del contante.

degli Atm ha subito un notevole incremento negli ultimi anni a causa della diminuzione del contante¹¹ disponibile nelle dipendenze bancarie; questo ha fatto sì che i delinquenti si focalizzassero sui dispositivi, quali appunto gli Atm, che ancora custodivano notevoli somme di denaro.

“Il Rapporto sui Furti ai danni delle dipendenze bancarie” nel 2010, a cura dell’Ossif, evidenzia come la maggior parte degli attacchi sia stata rivolta verso gli Atm: con 410 episodi registrati e un incremento del 6,5% (Ossif, 2010) ; il rapporto mette altresì in luce come effettivamente, rispetto ad altre tipologie di furto, questa si sia dimostrata più redditizia.

Gli attacchi avvengono quasi sempre fuori dall’orario di lavoro con le tecniche più diverse, quali:

- Gas/esplosivi
- Fiamma ossidrica
- Arnesi da scasso
- Ruspa/automezzi
- Mezzi meccanici
- Mezzi tecnici
- Altro

Sovente questi attacchi determinano anche ingenti danni collaterali alle strutture edilizie delle dipendenze, come nel caso riportato in (Ossif, 2009) nel quale i malviventi, cercando di forzare l’Atm con un’eccessiva carica di gas, procurarono un’esplosione così violenta da devastare gli uffici dell’istituto di credito e far volare lo sportello automatico dall’altro lato della strada; altro caso emblematico di attacco scenografico e distruttivo è quello di tre malviventi che, utilizzando un escavatore rubato (come in Figura 7), asportarono letteralmente l’Atm dal muro esterno della dipendenza, dandosi poi alla fuga dopo averlo comodamente riposto in un furgone (Il Resto del Carlino, 2010).

Ovviamente in questo caso l’impatto è essenzialmente sulla *security* bancaria intesa sia come perdita economica, derivante dai danni alle apparecchiature e agli edifici, che come danno di immagine.

OGGETTO DELLA SICUREZZA: Nell’ambito della sicurezza bancaria, per ridurre i rischi che derivano da azioni illecite nei confronti degli istituti di credito, è importante preservare gli ASSET DIRETTI (oggetto della sicurezza) da uno specifico evento criminoso (minaccia). L’evento criminoso è, infatti, finalizzato a cagionare un danno nei confronti del patrimonio o delle persone presenti all’interno di una dipendenza bancaria al fine di trarne un indebito beneficio.

¹¹ La diminuzione del contante circolante nelle dipendenze bancarie è stata resa possibile grazie all’utilizzo delle casseforti temporizzate e delle macchine cash in/cash out a servizio dei cassieri.

Pertanto preservare tali asset implica la necessità di proteggere il luogo che li ospita (filiale e atm).

Gli incidenti bancari che andremo a classificare e valutare sono quindi tutti quei delitti che hanno come scopo primario la sottrazione illecita di qualcosa, sia essa: denaro, valori¹² o identità. Per tale motivo, all'interno della classificazione approntata, chiameremo gli incidenti bancari catalogati semplicemente “**reati**”. Per “reati” pertanto si intenderà qualsiasi tipo di illecito, perpetrato volontariamente da agenti esterni, che comporti la sottrazione illegittima di **denaro, valori o identità** all'interno del contesto bancario. I reati presi in considerazione nell'albero di classificazione comprenderanno buona parte delle minacce alle banche indicate dal Vice Presidente dell'Ossif¹³ durante l'ultimo convegno Bancasicura 2011 (Iaconis, 2011)

- le rapine;
- i furti;
- le frodi

Gli unici reati esclusi in toto sono quelli di natura terroristica, i reati di riciclaggio, di spionaggio industriale e di falso nummario, i quali esulano evidentemente dal nostro campo d'indagine

Bisogna altresì evidenziare che nel campo delle frodi, il più vasto in quanto a complessità e modalità di esecuzione, non è stato possibile annoverare la totalità delle varianti attuabili; in particolare si è tralasciato di analizzare molte delle cosiddette “frodi interne”, quel tipo di frodi in cui, come definito ne (Il Sole 24 Ore, 2009), “il soggetto che direttamente o indirettamente la commette è un dipendente della società anche attraverso la copertura di un suo familiare”, perché rappresentano una minaccia interna alla banca mentre il progetto è riferito alla protezione dai rischi di minaccia “esterni” alla banca.

Dalla definizione di “banca”, formulata dal Vocabolario Treccani (Vocabolario Treccani, 2011), è evidente come per essa la “*funzione principale, oltre alla custodia di valori e ai pagamenti, è quella di farsi intermediario nella circolazione della moneta, raccogliendo il risparmio e concedendolo in prestito*”.

Risulta quindi fondamentale stabilire se il reato commesso sia o meno legato ad una specifica transazione economica.

Il concetto di “*transazione*”, così come indicato in (Williamson, 1975) , può essere inteso come “lo scambio di beni, servizi o informazioni” fra organizzazioni, fra individui, fra organizzazioni ed

¹² Il termine “valori” è utilizzato sia come denominazione generica di gioielli e altri oggetti preziosi che, nel linguaggio di borsa, come sinonimo di tutto ciò che può essere oggetto di negoziazione nelle borse (dette appunto borse valori), e cioè divise estere, azioni, obbligazioni, cartelle fondiarie, titoli di stato

¹³ L'Ossif è il Centro di Ricerca dell'ABI (Associazione Bancaria Italiana) sulla Sicurezza Anticrimine; l'Ossif ha come mission il dare supporto alle banche nell'individuazione delle strategie di prevenzione più efficaci, la cui definizione tenga conto della normativa vigente, del grado di esposizione ai rischi predatori, delle innovazioni tecnologiche e delle esperienze maturate in ambito nazionale e internazionale

individui. Queste transazioni sono raggruppabili, in base all'oggetto dello scambio tra l'entità banca ed un'altra entità (persona, ente o banca), in:

Transazioni economiche che avvengono in modalità puramente elettronica: sono transazioni il cui oggetto di scambio è di tipo immateriale, ovvero dati e informazioni. Nel caso delle banche, i dati e le informazioni riguardano quasi sempre le credenziali bancarie degli utenti e le operazioni finanziarie svolte.

Transazioni economiche che avvengono in modalità mista, ovvero sia elettronica che fisica: sono transazioni economiche in cui la risorsa scambiata tra le due entità ha sia una componente fisica che una componente immateriale (flussi informativi tra le entità che accompagnano e certificano lo scambio della risorsa). In ambito bancario, ciò che si scambia in questo tipo di transazioni è essenzialmente denaro e/o beni di valore.

Ai fini dell'individuazione delle misure di salvaguardia da adottare per la sicurezza delle dipendenze bancarie, la dimensione temporale assume un peso fondamentale. Le misure di mitigazione dal rischio di incidente, infatti, devono tenere conto della grossa differenza operativa tra i reati che vengono commessi in funzione dell'esecuzione di specifiche transazioni bancarie, che prevedono l'interazione diretta fra clienti e dipendenti (impattando fortemente sui concetti di security & safety delle persone all'interno della banca), o indipendentemente da esse, e che quindi mirano al patrimonio (materiale o immateriale) presente in banca e il cui impatto sulla sicurezza risulta minore.

Introduciamo di conseguenza la variabile "tempo relativo", t , che rappresenta il tempo di esecuzione di una specifica *transazione economica*, sia essa puramente *elettronica* o *mista*. Nel dettaglio, indicheremo con:

- t : la durata dello svolgimento di una transazione economica;
- $t - \alpha$: l'intervallo di tempo precedente la transazione economica;
- $t + \alpha$: l'intervallo di tempo che segue la transazione economica.

In relazione alla modalità di esecuzione di uno specifico reato, l'intervallo di tempo immediatamente precedente o successivo alla transazione economica avrà durata variabile tra la frazione di secondo e pochi minuti.

I furti che si verificano nell'intervallo di tempo $t - \alpha$, hanno come "Oggetto del furto" due possibili specializzazioni: "Denaro" e "Identità"

Oggetto del furto: denaro

Rapina in banca. Per la rapina in banca vale quanto già scritto. L'unica considerazione da fare è che in questo caso, così come per le rapine che avvengono a t e $t+\alpha$, si presuppone che la rapina avvenga durante l'orario di lavoro, quando cioè sono attive le transazioni economiche

tra banca e clienti (nel caso di $t-\alpha$ e $t+\alpha$ potrebbe anche accadere pochissimo prima o pochissimo dopo la prima e l'ultima transazione della giornata).

In questo caso l'impatto sulla *safety* riguarda sia i clienti che i dipendenti dell'istituto di credito, mentre, per quanto riguarda la *security*, l'impatto ricade unicamente sulla banca se i clienti non subiscono il furto di oggetti personali. In realtà, recentemente gli istituti bancari si assicurano anche da eventuali danni fisici e/o economici subiti dai clienti all'interno dell'istituto di credito durante l'orario di ufficio. E' importante sottolineare come il maggior danno è quasi sempre quello relativo all'immagine della banca (*security*).

Oggetto del furto: identità

Rispetto a quanto già scritto, è necessario solo aggiungere che il furto di identità di cui si parla in questo paragrafo riguarda tutti gli incidenti che si verificano poco prima che una particolare transazione economica inizi, ovvero:

Rapina all'Atm. La rapina dinanzi all' Atm è un reato comune nel nostro paese. In particolare, le rapine che avvengono prima che la vittima abbia effettuato la transazione economica con lo sportello automatico sono i casi che la cronaca riporta con più frequenza; rientrano nella categoria dei furti di identità perché il criminale costringe la vittima a prelevare dal bancomat e poi gli sottrae il contante ritirato, sostituendosi così a lei. Di solito la minaccia avviene con l'ausilio di armi da fuoco o da taglio, ma può anche accadere, come nel caso avvenuto a Parma pochi mesi fa (la Repubblica , 2011), che si adoperino armi "non convenzionali", quali ad esempio una siringa, per obbligare il malcapitato a prelevare il massimo importo possibile dal bancomat e consegnarlo al rapinatore. Altre volte la vittima subisce un vero e proprio sequestro prima di esser forzato a ritirare il contante per i malviventi (PadovaOggi, 2012).

Nel caso della rapina all'Atm, l'impatto sulla *security* è in primo luogo sul cliente derubato e solo marginalmente sulla banca, relativamente ad un eventuale danno di immagine. Il contraccolpo sulla *safety* è a carico unicamente del cliente.

(Furto) Session riding (malware inoculation). Il session riding è una particolare pratica criminale che utilizza il malware precedentemente inoculato per manipolare la comunicazione con la banca direttamente sul computer della vittima, così come evidenziato dalla piattaforma online eBanking (eBanking, 2009). Quando la vittima si collega al sito dell'istituto di credito per effettuare un'operazione di e-banking, il malware manipola in tempo reale i dati relativi al pagamento ancor prima che essi siano trasmessi all'istituto di credito; questo è il motivo per cui questo tipo di furto è incluso nella categoria degli illeciti che avvengono a $t - \alpha$. Questa tipologia di attacco consente al malware di modificare, ad esempio, il numero di conto del destinatario del pagamento e la quantità di denaro da trasferire. Il programma utilizzato è così sofisticato da riuscire a cambiare anche la conferma inviata dalla banca e specificare i dettagli di

pagamento immessi originariamente. La vittima vedrà quindi sul suo schermo la conferma indicante i dati corretti, ragione per cui nella maggior parte dei casi impiegherà del tempo prima di rendersi conto di aver subito un attacco.

In linea di massima gli attacchi derivanti da malware dovrebbero impattare sulla *security* del cliente, dal momento che possono essere contrastati con un comportamento prudente e l'utilizzo dei più sofisticati strumenti di sicurezza (antivirus, antispyware e personal firewall). Le responsabilità della banca in merito alla *security* possono però riscontrarsi, come ricordato dall'Unione Nazionale Consumatori (Comitato Marano, 2011), nel caso non informi tempestivamente il cliente dell'avvenuto bonifico e se, rilevate delle irregolarità nell'utilizzo dell'internet banking, non proceda a bloccare immediatamente le transazioni correnti. La banca potrebbe inoltre dover dimostrare, in un eventuale giudizio, di aver realmente usato gli strumenti di sicurezza più d'avanguardia per la custodia dei dati e del denaro dei clienti (come ad esempio i dispositivi automatici per la generazione di password quali token, chiavette, digipass). L'impatto sulla *safety* riguarda il solo lato cliente.

Phishing con malware. Abbiamo già detto come funziona il phishing tradizionale. Nel caso del phishing con malware, come evidenziato in (eBanking, 2009), la vittima non arriva sul sito contraffatto dell'istituto di credito seguendo un finto messaggio di posta elettronica, ma vi è portato da un malware infiltratosi precedentemente suo PC. Quando entra nel sito Internet autentico, la vittima è reindirizzata automaticamente e in modo del tutto inosservato sul sito contraffatto.

Per *safety* e *security* vale quanto appena detto a proposito del session riding.

Pharming. Nel pharming la truffa consiste nel creare pagine web identiche ai siti originali (istituti di credito, softwarehouses,..) su cui reindirizzare l'ignara vittima attraverso la manipolazione del Domain Name System (DNS), un servizio Internet che ha un ruolo focale quando si stabilisce una connessione con un server web. Il nome "pharming" è riconducibile proprio al fatto che i cyber-criminali che adoperano questa tecnica dispongono di grandi "server farm" (ampi locali contenenti un gran numero di computer adibiti a server) in cui sono memorizzate diverse pagine Internet contraffatte. Rispetto al phishing, il potenziale di raccolta dati del pharming è di gran lunga superiore.

Come raccontato su (Norton, 2006), uno dei primi grandi attacchi di pharming utilizzò un difetto del software come punto di appoggio per scambiare centinaia di nomi di domini legittimi con quelli di siti Web contraffatti. Subito dopo si verificarono tre ondate di attacchi, due delle quali tentarono d'installare spyware e adware sui computer delle vittime, mentre la terza tentò di indirizzare gli utenti verso un sito web che vendeva pillole, in genere consigliate mediante e-mail di spamming.

Anche nel caso del pharming comprendere dove è che impatta in maggior misura la *security* è arduo. Se si analizza la tecnica criminale appare subito evidente che vi è un primo contraccolpo

sulla *security* della banca legato al danno indiretto di immagine. Per quanto riguarda però la perdita patrimoniale, legata in genere alle responsabilità nel danno, la situazione si fa complessa. Ettore Guarnaccia, esperto di information security, sul suo portale on-line (Guarnaccia, 2012) asserisce che nel caso di “attacchi di pharming, la responsabilità può non essere a carico né della banca né del cliente. La peculiarità di questo attacco, infatti, fa sì che esso possa essere agevolmente portato a termine sfruttando carenze di sicurezza dei server DNS di un Internet Service Provider (ISP) che può non essere né quello utilizzato dal cliente per accedere ad Internet, né quello cui la banca si appoggia per fornire i propri servizi di online banking”. D’altro canto, Lippi (2007) sostiene che numerosi episodi di pharming palesano la mancata sorveglianza da parte dell’istituto di credito nei riguardi del proprio sito e di eventuali siti cloni.

Inoltre molti tra consumatori e studiosi attribuiscono alle banche l’ulteriore responsabilità di non “bloccare”, una volta avvistate, con la giusta tempestività i conti delle vittime, causa “tempi tecnici”. Anche le sentenze civili non sono univoche e spesso anzi sono controverse. Per venire a capo di una questione così ambigua, si è deciso di considerare che il pharming abbia lo stesso grado di impatto sia sulla *security* della banca che su quella del cliente. L’impatto sulla *safety* è invece solo a danno del cliente.

Lebanese loop. Il Lebanese loop è un tipo di frode che interessa unicamente gli Atm. La modalità di esecuzione è abbastanza semplice: come indicato anche su (Monetos, 2009), i criminali applicano un particolare tipo di dispositivo allo sportello di prelievo automatico con il quale è possibile trattenere la carta inserita. L’ignara vittima è confusa, non può completare la transazione né riavere indietro la propria carta. E’ a questo punto che si fa avanti il truffatore: fingendosi un gentile passante, suggerisce alla vittima di digitare ancora una volta il pin, così da poterlo in segreto memorizzare. Non riuscendo ad estrarre la propria carta il titolare si allontanerà, lasciando in questo modo al criminale la possibilità di impossessarsene e utilizzarla per scopi illeciti. Il lebanese loop impatta sulla *security* della banca, responsabile dell’integrità del distributori automatico di banconote, e sulla *safety* della clientela.

Tipologia di furto al tempo t

Oggetto del furto: denaro

Rapina o scippo all’Atm. Come si è già sottolineato, le rapine davanti agli Atm sono reati di cui purtroppo la cronaca ci informa spesso. Il caso però in cui la rapina si verifichi durante la transazione economica con lo sportello automatico è il più raro. Solitamente i criminali costringono la vittima al prelievo “forzoso” di contante prima che la transazione sia effettivamente iniziata. Durante, e ancor di più dopo, la transazione economica (lo vedremo in seguito) è più usuale un altro reato: lo scippo della vittima.

Lo scippo che ha luogo quando ancora la transazione non è terminata, implica da parte del criminale una buona dose di inventiva per potersi avvicinare ai soldi e derubare la vittima senza attirare troppo l'attenzione. Un esempio di *modus operandi* è quello riportato sul sito del quotidiano La Repubblica (2011) da una donna che testimonia di esser stata avvicinata, durante la fase di prelievo dal bancomat, da un uomo con un cartello in mano (di quelli utilizzati per attirare l'attenzione nel domandare l'elemosina, del tipo: «aiutatemi sono povero») che le chiede un'indicazione stradale. Dopo averlo allontanato la donna si accorge però che le banconote, nel frattempo erogate dall'Atm, sono scomparse: senza dubbio sottratte dall'uomo che le si era accostato e nascoste, prima di andar via, dietro il cartello. Un altro esempio (ATnews, 2012), è quello di un cliente che, dopo aver richiesto l'erogazione di 200 euro dallo sportello automatico, distratto da una telefonata, non si accorge di esser stato nel frattempo derubato del denaro emesso dall'Atm. Come già illustrato in precedenza il pesante impatto sulla *safety* (in questo caso relativa ai danni psico-emozionali e talvolta fisici derivanti da un reato predatorio) e quello relativo alla *security* è a carico quasi esclusivamente del cliente. L'unico possibile danno alla *security* bancaria deriva dalla perdita di immagine che scaturisce dal crimine perpetrato.

Furto con destrezza all'Atm. Il furto con destrezza all'Atm è uno dei nuovi sistemi adoperati per frodare i malcapitati clienti dei bancomat. Generalmente, come spiega anche Anselmi (2011), il crimine si realizza mediante copertura della bocca erogatrice di banconote con un tappo impregnato di collante o con la sostituzione del frontalino di alluminio con uno del tutto simile cosparso di colla.

Lo scopo, in entrambi i casi, è trattenere le banconote del cliente all'interno della macchina. Nel 2011, i carabinieri hanno sgominato una banda di sabotatori di bancomat a Paullo che utilizzava proprio questa tecnica per defraudare le ignare vittime. I malcapitati clienti, vedendo che il denaro non usciva, pensavano ad un guasto e si allontanavano senza il denaro prelevato. In realtà la somma era poi estratta in un secondo momento dai rapinatori (Bruno C. , 2011).

Il furto con destrezza ha ripercussioni unicamente sulla *security* dell'istituto di credito, responsabile dell'integrità dei suoi bancomat.

Attacco al trasporto valori. La rivista Bancaforte (Zaurrini, 2012), , mette in luce gli ultimi numeri relativi a questo tipo di crimine: 57 gli attacchi a portavalori tentati in Italia nel 2011, conteggiando sia quelli sventati che quelli falliti, per un bottino di poco superiore ai 13 milioni di euro. Contestualmente, il Rapporto Intersettoriale sulla Criminalità Predatoria di ABI/OSSIF tratteggiava la situazione dei trasportatori di valori come "esposti alle attenzioni di bande specializzate, dotate di capacità organizzative e di tecniche non comuni, in grado di compiere imprese criminali che coniugano altissimo rischio ad una altrettanto elevata remunerazione. La pericolosità degli attacchi perpetrati da bande organizzate e dotate di vere e proprie capacità militari è testimoniata dal tipo di armi utilizzate. Non solo pistole, fucili ed armi da fuoco in genere, ma anche kalashnikov ed esplosivi rientrano nell'arsenale dei malviventi protagonisti di

tali attacchi". Ed effettivamente la grande preoccupazione con cui il settore della sicurezza in generale guarda a questo fenomeno criminale non è soltanto dovuto alle ingenti somme rubate, ma principalmente alla notevole minaccia che esso costituisce per l'incolumità innanzitutto delle guardie giurate e poi dei dipendenti di banca e raramente dei clienti.

Come evidenzia il rapporto dell'Ossif, i criminali sempre più spesso si organizzano in veri e propri commando che lavorano con freddezza e lucidità, non esitando a sparare se ostacolati nel loro agire. Tra i numerosi esempi di feroce determinazione che la cronaca racconta sempre più di frequente vi è l'assalto avvenuto a Casoria nell'ottobre 2010 (Cerino, 2010), dove perse la vita un vigilante e furono feriti un cliente ed un'altra guardia giurata.

In alcuni casi l'attacco assume i connotati "spettacolari" dell'action movie a stelle e strisce; è il caso dell'assalto avvenuto a settembre del 2011 sulla Firenze-Siena (Tani, 2011), dove un commando di banditi ha adoperato dei kalashnikov per incendiare sei macchine ed un camion, precedentemente rubati e posizionati in modo da bloccare da una parte l'avvicinamento delle forze dell'ordine o di altre vetture e dall'altra l'eventuale fuga del portavalori. Una volta sbarrata la strada, i criminali hanno aperto con una sega circolare la lamiera del tetto del veicolo blindato, riuscendo così ad accedere al contenuto della cassaforte: 350.000 euro destinato a banche e uffici postali della zona dell'Amiata verso cui il portavalori era diretto per le consegne.

Come abbiamo potuto notare dai pochi esempi fatti, sebbene la preoccupazione relativa alla *safety* sia preponderante per questo tipo di attacchi, è da sottolineare anche l'impatto notevole che essi hanno sulla *security*, legata in particolar modo alle ingenti perdite che essi producono. Juvara (2012) mette in risalto come effettivamente, nel 2010, siano stati segnalati 27 attacchi, di cui 21 riusciti che hanno generato una perdita complessiva di oltre 12 milioni di euro.

Ovviamente, in questa tipologia di attacco, la *safety* e la *security* intaccate sono nella gran parte dei casi quelle dell'agenzia che si occupa del trasporto valori per conto della banca. Di fatti la responsabilità dell'istituto di credito termina non appena i valori escono dai suoi locali.

Rapina in banca. Per la rapina in banca resta valido quanto scritto in precedenza.

Oggetto del furto: identità

Atm Skimming. Il vocabolo "skimming" proviene dal verbo inglese *to skim*, che significa "sfiorare, strisciare". Da questo termine deriva il nome del congegno elettronico impiegato negli Atm per registrare i contenuti delle bande magnetiche: lo skimmer. Come sottolineato in (D'Agata, 2012), l'utilizzo improprio di questi apparecchi, la loro manipolazione, fino ad giungere perfino alla sostituzione dello skimmer originale con uno contraffatto, sistemato di

proposito per leggere e memorizzare i contenuti delle carte magnetiche degli ignari clienti, ha reso possibile la nascita e l'affermarsi di una nuova tecnica criminale chiamata appunto skimming.

Le modalità di funzionamento sono ben spiegate in (Anselmi, 2011), che su un lavoro presentato per il convegno "Banche e Sicurezza, 2011" ha illustrato l'attacco in due distinte fasi:

- La cattura dei dati per la clonazione della carta: che avviene generalmente anteposto allo skimmer originale uno "manipolato" di uguale forma



Figura 58. Lo skimmer "contraffatto" è anteposto all'originale

La registrazione del Pin di convalida che può riuscire o attraverso:

- l'utilizzo di una telecamera nascosta (Figura 57)
- l'applicazione di una finta tastiera del tutto simile all'originale (Figura 58)



Figura 59. Un esempio di come i ladri nascondono una mini telecamera in un porta-brochure contenente materiale promozionale dell'istituto di credito dell'Atm



Figura 60. La tastiera originale è coperta da un finta per ingannare il cliente

Nel caso dello skimming, così come in tutte le altre circostanze in cui i malviventi perpetrano il crimine manomettendo l'Atm, esclusa ogni responsabilità del titolare nell'utilizzo fraudolento della carta, "gli importi relativi sono in genere riaccreditati dalla società emittente" (D'Agata, 2012), al limite previo pagamento della franchigia di 150 euro, come già sottolineato parlando di "Frodi mail not received". D'altronde, come riporta il portale di informazione giuridica Studio Cataldi (Matricardi, 2007), la Prima Sezione Civile della Corte di Cassazione ha stabilito che l'Istituto di Credito può essere ritenuto responsabile del malfunzionamento del Bancomat e dell'eventuale clonazione della carta da parte di terzi. Possiamo così esser certi che, in un buon numero di situazioni, l'impatto sulla *security* sia ad esclusivo appannaggio della banca. L'impatto relativo alla *safety*, trattandosi di un furto d'identità, sarà al contrario a carico del cliente.

Furto di credenziali di accesso ai servizi di e-banking allo scopo di sottrarre denaro (malware inoculation).

(Ludovini, 2010), riportava una serie di dati aggregati dalla Centrale d'allarme Abi Lab, relativi al 2009, su un campione di 162 istituti di credito «rappresentativi del 75% del sistema bancario italiano» e, in particolare, «dell'81,8% dei clienti on-line abituali». La notizia preoccupante che emergeva dalla lettura di questi dati era relativa al fatto che ben l'89% delle banche del campione affermava di aver individuato «tentativi fraudolenti mirati al furto delle credenziali di autenticazione all'home banking». E purtroppo il trend non sembra destinato a diminuire. Le minacce all'e-banking sono quindi una delle più grandi preoccupazioni degli istituti di credito italiani che si trovano a combattere contro "nemici" sempre più pervasivi e specializzati: i malware.

Come precedentemente delineato, una delle principali funzionalità del malware è proprio quella di carpire informazioni e dati strettamente riservati, come le credenziali bancarie. Nella

modalità di attacco più utilizzata, il cosiddetto “Man-In-The-Browser”, il malware (un trojan o un altro qualsiasi malware) si trova all'interno del browser web. Come spiega Andrea Bai, in un suo articolo pubblicato in rete (Bai, 2010), è un tipo di attacco organizzato appositamente per danneggiare le banche ed i loro clienti. Con un attacco Man-In-The-Browser, difatti, l'utente di un servizio di banking online è certo di interagire direttamente con il proprio istituto di credito, mentre in realtà il browser infetto intercetta e modifica le operazioni impartite. Il malware invia così le operazioni manipolate alla banca che a sua volta crede di interagire direttamente con il cliente, dal momento che ripone la sua fiducia nel canale di comunicazione; il canale è ritenuto sicuro principalmente per il fatto che il processo di autenticazione, effettuato a monte dall'utente, è andato a buon fine. Ed è proprio questa “fiducia mal riposta”, secondo Bai (Bai, 2010), la ragione del successo di questo tipo di attacco e il dogma da sfatare se si vuole debellare un nemico così insidioso.

Un'altra modalità di attacco è quella che utilizza i cosiddetti trojan banking come Mebroot, un software malefico altamente sofisticato che nel 2007-2008 infettò centinaia di pagine web tra le più insospettabili in tutto il mondo. I trojan come Mebroot sono in grado di rubare i codici di accesso e le password dei clienti per farle pervenire tramite la rete ai cyber-criminali. Come spiega Tonacci, (Tonacci, 2008), con questo sistema i creatori di Mebroot riuscirono a sottrarre solo dai conti italiani più di 8 milioni di euro. Il modus operandi era semplice: quando l'utente accedeva al conto on-line da un computer infetto, Mebroot inviava ciò che era digitato, ovvero il nome utente e le password, a server esteri, predisposti appositamente dai criminali e chiusi poche ore dopo l'attacco fraudolento. Ottenuti i dati riservati, i delinquenti eseguivano un bonifico di poche migliaia di euro sul conto di una terza persona, in Italia, la quale provvedeva poi a spostare il denaro all'estero usufruendo di uno dei tanti servizi di money transfert, quali ad esempio Western Union. Nella gran parte dei casi, coloro che trasferivano la somma erano i cosiddetti “soldatini” o “muli”, assunti in cambio di una piccola commissione con annunci del tipo "vuoi guadagnare 500 euro stando a casa?" e quasi sempre all'oscuro delle intenzioni criminali dei “datori di lavoro”.

Trattandosi sempre di malware inoculation, quanto detto nel paragrafo relativo al session riding riguardo a *safety* e *security* si applica anche qui.

Tipologia di furto al tempo $t + \alpha$

Oggetto del furto: denaro

Rapina o scippo all'Atm. Nella rapina o lo scippo dopo il prelievo dallo sportello bancomat capita spesso che i criminali si focalizzino sulle fasce più deboli della popolazione: anziani e donne. Caso esemplare quello accaduto a Lecce pochi anni fa (Il tacco d'Italia, 2009), quando uno

scippatore prese di mira le donne che prelevavano dai bancomat, riuscendo sempre a farla franca.

La valutazione in merito all'impatto su *safety* e *security* è identica a quella compiuta nei paragrafi precedenti per la stessa tipologia di reato.

Una volta individuati gli elementi che compongono l'insieme $R = \{r | r \text{ è un reato ai danni di un istituto bancario}\}$ e che sono stati descritti nel precedente paragrafo, in questo paragrafo definiremo la composizione del sottoinsieme

$RD = \{r \in R | r \text{ impatta direttamente sulla sicurezza di una dipendenza bancaria}\}$.

Al fine di specificare meglio quali reati siano compiuti bisogna considerare quei reati che hanno un impatto diretto su almeno una delle sue dimensioni caratterizzanti la sicurezza bancaria. Ciò comporta individuare quei reati il cui impatto è immediatamente verificabile su almeno una delle seguenti:

L'oggetto della sicurezza, che può essere il cliente, *c*, o il dipendente, *f*, di una specifica filiale.

La tipologia di sicurezza a cui facciamo riferimento: *security*, *sec*, (intesa come protezione del patrimonio e delle sue transazioni) o *safety*, *saf*, (intesa come incolumità psico-fisica delle persone che si trovano presso la dipendenza bancaria)

Siano quindi:

$RD_{sec,c} = \{r \in R | r \text{ impatta sulla security del cliente}\};$

$RD_{saf,c} = \{r \in R | r \text{ impatta sulla safety del cliente}\};$

$RD_{sec,f} = \{r \in R | r \text{ impatta sulla security di una dipendenza (filiale) bancaria}\};$

$RD_{saf,f} = \{r \in R | r \text{ impatta sulla safety di una dipendenza (filiale) bancaria}\};$

allora è possibile definire l'insieme RD in maniera più rigorosa:

$$RD = RD_{sec,c} \cup RD_{saf,c} \cup RD_{sec,f} \cup RD_{saf,f}$$

Nel seguito viene esplicitata la composizione singoli sottoinsiemi elencando gli elementi (reati) presenti in ogni insieme. Tali reati sono un sottoinsieme riclassificato dei reati elencati nel paragrafo precedente e costituenti il più generale insieme dei reati commettabili ai danni di un istituto bancario. L'obiettivo che viene perseguito nella riclassificazione è quello di avere un insieme finale RD che risponda, da un punto di vista insiemistico e matematico, ai criteri di completezza e consistenza.

$RD_{sec,c} = \{r \in R \mid r \text{ impatta sulla security del cliente} \}$

- rapina diretta al cliente immediatamente prima di entrare o appena uscito dalla filiale o dalla postazione ATM. Il fine della rapina è di acquisire denaro, valori o identità (carte, codici, ecc.) mediante minaccia con eventuale uso della forza.
- rapina diretta alla filiale durante la quale il cliente presente in banca viene derubato di denaro, valori o identità
- furto di identità del cliente (codici PIN, carte clonate, ecc.) durante l'operazione all'ATM (tramite telecamere nascoste, skimmer, ecc.) o alle porte di quelle dipendenze che necessitano di "strisciare" la carta bancomat per entrare.
- frode tramite operazioni allo sportello con falsa identità (identità di un cliente ignaro della banca)

$RD_{saf,c} = \{r \in R \mid r \text{ impatta sulla safety del cliente} \};$

- rapina diretta alla filiale durante la quale il cliente presente in banca non subisce alcun furto
- rapina diretta al cliente immediatamente prima di entrare o appena uscito dalla filiale o dalla postazione ATM. Il fine della rapina è di acquisire denaro, valori o identità (carte, codici, ecc.) mediante minaccia con eventuale uso della forza. N.B.: Già denominato come elemento **a** in $RD_{sec,c}$
- rapina diretta alla filiale durante la quale il cliente presente in banca viene derubato di denaro, valori o identità. N.B.: Già denominato come elemento **b** in $RD_{sec,c}$

$RD_{sec,f} = \{r \in R \mid r \text{ impatta sulla security di una dipendenza (filiale)bancaria} \};$

- frode tramite apertura di credito con false credenziali (inventate, non appartenenti a persona esistente) al fine di ottenere denaro o crediti/garanzie dalla banca.
- frode tramite falsificazione di titoli all'ordine e di proprietà cartacei presentati allo sportello al fine di ottenere denaro o crediti/garanzie dalla banca.
- furto all'ATM al fine di impossessarsi del denaro/valori in esso contenuti. Il furto può avvenire sia con scasso tramite la forze e l'ausilio di vari strumenti fisici, sia con false credenziali, sia tramite attacco logico (questa modalità si verifica per ATM evoluti in cui il protocollo di comunicazione è il TCP/IP)
- Rapina al portavalori
- rapina diretta alla filiale durante la quale il cliente presente in banca viene derubato di denaro, valori o identità N.B.: Già denominato come elemento **b** in $RD_{sec,c}$

- rapina diretta alla filiale durante la quale il cliente presente in banca non subisce alcun furto. N.B.: Già denominato come elemento **a** in $RD_{saf,c}$
- frode tramite operazioni allo sportello con falsa identità (identità di un cliente ignaro della banca) N.B.: Già denominato come elemento **d** in $RD_{sec,c}$

$RD_{saf,f} = \{r \in R \mid r \text{ impatta sulla safety di una dipendenza (filiale) bancaria } \};$

- Rapina durante le operazioni di carico/scarico di un ATM. Se l'ATM è di tipo tradizionale, il furto può riguardare sia denaro contanti che informazioni di base del cliente; qualora si tratti di ATM evoluto, dove il cliente può effettuare versamenti oltre che prelievi, il furto può riguardare anche assegni e altri valori versati dal cliente
- rapina diretta alla filiale durante la quale il cliente presente in banca viene derubato di denaro, valori o identità N.B.: Già denominato come elemento **b** in $RD_{sec,c}$
- Rapina al portavalori (intendendo gli operatori del portavalori come dipendenti della filiale) N.B.: Già denominato come elemento **d** in $RD_{sec,f}$
- rapina diretta alla filiale durante la quale il cliente presente in banca non subisce alcun furto. N.B.: già denominato come elemento **a** in $RD_{saf,c}$

Complessivamente l'insieme RD contiene 10 elementi (tipologie di reato che hanno impatto sulla sicurezza di una dipendenza bancaria e viene così individuato:

$$RD = RD_{sec,c} \cup RD_{saf,c} \cup RD_{sec,f} \cup RD_{saf,f} =$$

All'interno di questa trattazione bisogna tuttavia considerare un sottoinsieme di reati e di assets che interessano direttamente la filiale bancaria

L'*oggetto della sicurezza* è ciò che deve essere tutelato dalle minacce (i reati). Gli elementi che compongono l'oggetto della sicurezza sono stati citati precedentemente nella tabella omonima. La *tipologia di sicurezza* si riferisce, invece, alla safety e alla security. In particolare la safety riguarda l'incolumità della persona, mentre la security la protezione del patrimonio e delle sue transazioni.

ASSET (oggetto della sicurezza)
Cliente
Dipendente
Cassa contante
Cassette sicurezza
Beni strutturali
Atm
Immagine
Competitività commerciale

MINACCIA
Rapina
Furto
Frode
Danneggiamento

Tabella 31. Tabella Asset-Minaccia

Indichiamo a questo punto RD come il sottoinsieme di reati ai danni di un istituto bancario tale che il reato impatta direttamente sulla dipendenza bancaria.

$$RD = \{r \in R \mid r \text{ impatta direttamente sulla sicurezza di una dipendenza bancaria}\}.$$

Siano quindi:

$$RD_{sec,c} = \{r \in R \mid r \text{ impatta sulla security del cliente}\}$$

$$RD_{saf,c} = \{r \in R \mid r \text{ impatta sulla safety del cliente}\}$$

$$RD_{sec,d} = \{r \in R \mid r \text{ impatta sulla security del dipendente}\} = \{\emptyset\}$$

$$RD_{saf,d} = \{r \in R \mid r \text{ impatta sulla safety del dipendente della filiale}\}$$

$$RD_{sec,cc} = \{r \in R \mid r \text{ impatta sulla security della cassa contante della dipendenza}\}$$

$$RD_{saf,cc} = \{r \in R \mid r \text{ impatta sulla safety della cassa contante della dipendenza}\} = \{\emptyset\}$$

$$RD_{sec,cs} = \{r \in R \mid r \text{ impatta sulla security delle cassette sicurezza della dipendenza}\}$$

$$RD_{saf,cs} = \{r \in R \mid r \text{ impatta sulla safety delle cassette sicurezza della dipendenza}\} \\ = \{\emptyset\}$$

$$RD_{sec,atm} = \{r \in R \mid r \text{ impatta sulla security dell'atm}\}$$

$$RD_{saf,atm} = \{r \in R \mid r \text{ impatta sulla safety dell'atm}\} = \{\emptyset\}$$

$$RD_{sec,bs} = \{r \in R \mid r \text{ impatta sulla security dei beni strutturali presenti nella filiale}\}$$

$$RD_{saf,bs} = \{r \in R \mid r \text{ impatta sulla safety dei beni strutturali presenti nella filiale}\} \\ = \{\emptyset\}$$

$$RD_{sec,im} = \{r \in R \mid r \text{ impatta sulla security dell'immagine dell'agenzia}\}$$

$$RD_{saf,im} = \{r \in R \mid r \text{ impatta sulla safety dell'immagine dell'agenzia}\} = \{\emptyset\}$$

$$RD_{sec,co}$$

$$= \{r \in R \mid r \text{ impatta sulla security della competitività commerciale dell'agenzia}\}$$

$$RD_{saf,co}$$

$$= \{r \in R \mid r \text{ impatta sulla safety della competitività commerciale dell'agenzia}\} = \{\emptyset\}$$

allora è possibile definire l'insieme RD in maniera più rigorosa:

$$RD = RD_{sec,c} \cup RD_{saf,c} \cup RD_{saf,d} \cup RD_{sec,cc} \cup RD_{sec,cs} \cup RD_{sec,atm} \cup RD_{sec,bs} \cup RD_{sec,im} \\ \cup RD_{sec,co}$$

Nel seguito viene esplicitata la composizione dei singoli sottoinsiemi elencando gli elementi (reati) presenti in ogni insieme. Tali reati sono un sottoinsieme riclassificato dei reati R costituenti il più generale insieme dei reati commettabili ai danni di un istituto bancario. L'obiettivo che viene perseguito nella riclassificazione è quello di avere un insieme finale RD che risponda, da un punto di vista insiemistico e matematico, ai criteri di completezza e consistenza.

A partire dalle 4 tipologie di minacce presentate in precedenza (*Rapina, Furto, Frode, Danneggiamento*) e alla luce dei diversi reati trattati per ciascuna minaccia è possibile giungere ad una struttura tassonomica degli stessi. Questa struttura tassonomica consentirà di esprimere in maniera semplificata i principali eventi criminosi da cui una dipendenza bancaria dovrà proteggersi o che comunque dovrà cercare di evitare attraverso l'adozione di opportune misure di prevenzione.

MINACCIA 1: RAPINA

1. RAPINA include le seguenti sottocategorie

1.1. Rapina in filiale (diretta alla filiale)

- 1.1.1.** il cliente presente in banca viene derubato di denaro, di valori o identità
- 1.1.2.** rapina diretta alla cassa contante
- 1.1.3.** rapina diretta alla cassetta sicurezza
- 1.1.4.** rapina diretta ai beni strutturali della banca

1.2. Rapina fuori dalla filiale

- 1.2.1.** Rapina diretta al cliente di denaro, valori o identità all'ingresso/all'uscita della filiale
- 1.2.2.** Rapina al portavalori

1.3. Rapina all'ATM

- 1.3.1.** Rapina al cliente dalla postazione Atm con lo scopo di sottrarre denaro, valori o identità
- 1.3.2.** Rapina durante l'operazione di carico/scarico Atm

MINACCIA 2: FURTO

2. FURTO, che si suddivide in

2.1. Furto in filiale

- 2.1.1.** furto F.O.L.

- 2.1.1.1. Furto diretto alla cassa contante
 - 2.1.1.2. Furto diretto alla cassetta sicurezza
 - 2.1.1.3. Furto diretto ai beni strutturali della banca
 - 2.1.2. furto valori, denaro in O.L.
 - 2.2. furto all'ATM
 - 2.2.1. furto d'identità del cliente durante operazione all'Atm (tramite telecamere nascoste, skimmer, ecc.)
 - 2.2.2. furto con destrezza al cliente di denaro/valori o identità
 - 2.2.3. furto di denaro con danneggiamento Atm
 - 2.2.4. furto all'Atm di denaro/valori in esso contenuto tramite false credenziali
 - 2.2.5. furto all'Atm tramite attacco logico (questa modalità si verifica per ATM evoluti in cui il protocollo di comunicazione è il TCP/IP)

MINACCIA 3: FRODE

3. FRODE

- 3.1. **Frode in filiale (sportello) al fine di ottenere denaro o crediti/garanzie da parte della banca.**
 - 3.1.1. frode tramite operazioni allo sportello con falsa identità (identità di un cliente ignaro)
 - 3.1.2. Frode tramite apertura di credito con false credenziali (inventate, non appartenenti a persona esistente)
 - 3.1.3. Frode tramite falsificazione di titoli all'ordine e di proprietà cartacei presentati allo sportello

MINACCIA 4: DANNEGGIAMENTO

4. DANNEGGIAMENTO VOLONTARIO

- 4.1. Danneggiamento allo scopo di creare un danno di immagine per la banca
- 4.2. Danneggiamento allo scopo di creare un'interruzione di servizio
- 4.3. Danneggiamento finalizzato ad un'azione di furto

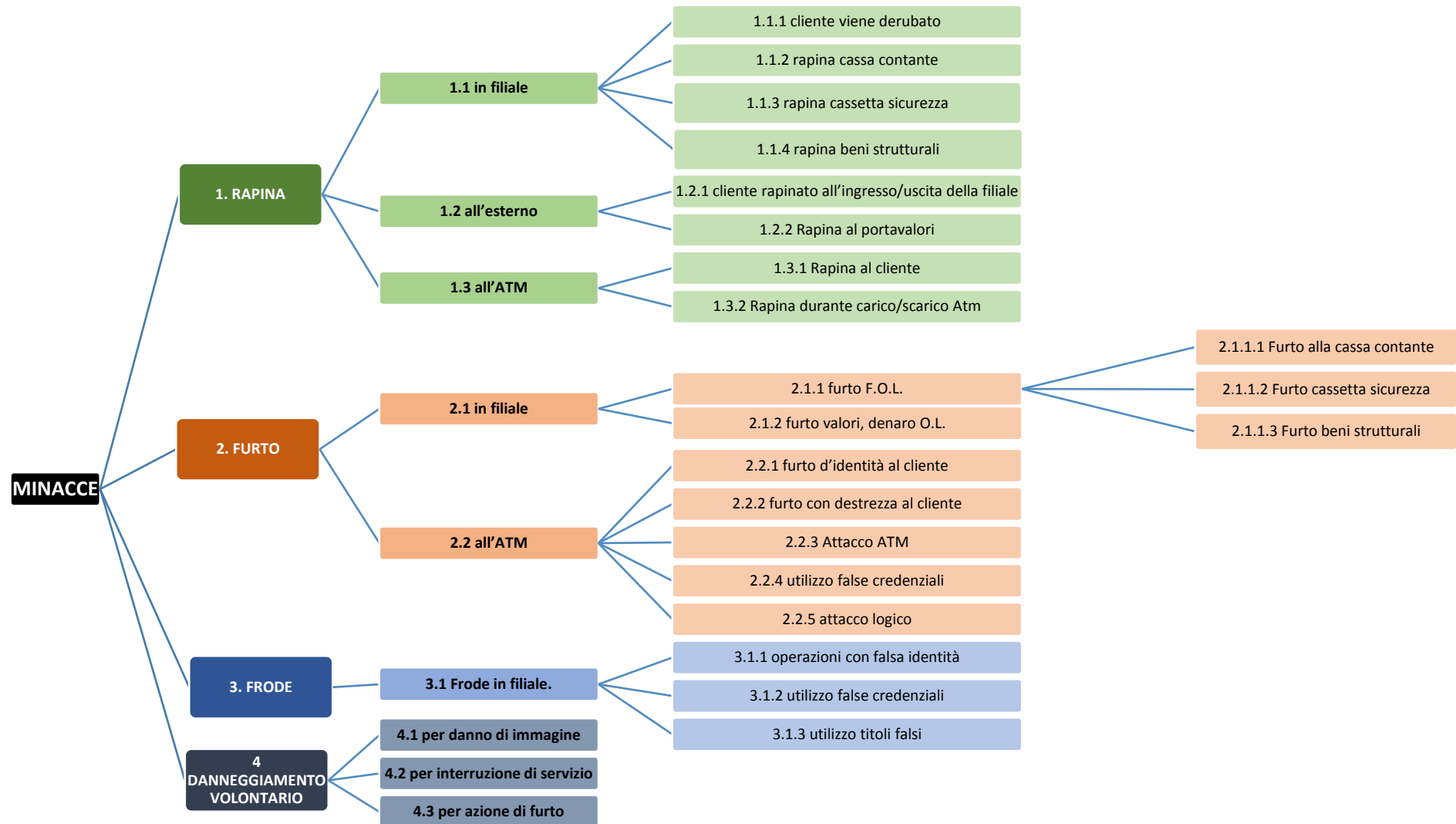


Figura 61. Tassonomia delle minacce

4.3 Fase 2: Valutazione del rischio

Sia l'indice di sicurezza BaSS (Bank Security and Safety) di filiale f_j definito come segue:

$$BaSS_{f_j} = \frac{1}{\sum_{r \in RD} Risk(r, f_j)}$$

Il fine del modello è individuare l'insieme delle azioni che consentano di massimizzare BaSS che, dal punto di vista analitico, rappresenta la funzione obiettivo del modello proposto.

$$\max BaSS = \max \frac{1}{\sum_{r \in RD} Risk(r)} = \min \sum_{r_i \in RD, f_j \in RD} Risk(r_i, f_j) = \min \sum_{r_i \in RD, f_j \in RD} P(r_i, f_j) \times I(r_i, f_j)$$

Dove:

- $P(r_i, f_j)$ = probabilità che il reato i venga compiuto sulla filiale j sarà
- F (vulnerabilità dell'area in cui si colloca f_j al reato r_i , andamento delle serie storiche di r_i , percezione della vulnerabilità di f_j al reato r_i)
- $I(r_i, f_j) = F(I(r_i), \text{vulnerabilità di } f_j \text{ al reato } r_i)$

Analizzando la formula del rischio si evince che per minimizzarlo è necessario intervenire o su probabilità e impatto contemporaneamente o su una delle due componenti. Considerando che la determinazione dell'impatto risulta essere estremamente difficile poiché l'entità del danno associato all'evento negativo può cambiare in relazione a circostanze esterne non controllabili a causa dell'incertezza che le caratterizza, allora si stima la funzione impatto $I(r)$ in base all'ampiezza che l'impatto dell'incidente ha sulle **due dimensioni caratterizzanti la sicurezza delle dipendenze bancarie**, ovvero l'oggetto della sicurezza (asset) e la tipologia di sicurezza (safety & security).

Si rende pertanto necessario agire sull'altra componente, ovvero la probabilità che si verifichi un particolare evento criminoso. Dal momento che per ridurre la probabilità occorre aumentare la protezione dei luoghi oggetto dell'attacco, più avanti verranno proposte tutte le misure di prevenzione e protezione capaci di massimizzare l'indice BaSS. In particolare verranno ripresentate in maniera sintetica quelle discusse in letteratura, quelle attualmente esistenti. Ma possiamo ora ad analizzare nel dettaglio le componenti della funzione di Probabilità e di Impatto.

Esse si suddividono in due categorie. La prima categoria dipende soltanto da un fattore ovvero il reato ed è costituita da impatto e andamento delle serie storiche. La seconda categoria invece dipendente da due componenti (filiale e reato) è caratterizzata da fattori di vulnerabilità di area, fattori di vulnerabilità filiale e percezione della vulnerabilità di una filiale.

1. L'impatto $I(r_i)$
2. L'andamento delle serie storiche di r_i
3. vulnerabilità dell'area in cui si colloca f_j al reato r_i

4. vulnerabilità di f_j al reato r_i
5. percezione della vulnerabilità di f_j al reato r_i

4.3.1 L'impatto

Come già detto in precedenza, prima di parlare di impatto, è necessario comprendere pienamente la differenza tra rischio e incertezza, poiché l'impatto che un reato ha sugli ASSET di una dipendenza bancaria non è determinabile in maniera precisa. "L'impatto dell'incidente (ovvero l'entità del danno associato all'evento avverso), infatti, può cambiare in relazione a circostanze esterne che, vista la loro natura aleatoria, non sono prevedibili in modo certo e univoco".

Determinare l'impatto non è cosa semplice. Come già affermato, esso cambia a seconda di circostanze esterne non controllabili e di cambiamenti dell'ambiente in cui un dato reato trova esecuzione. Data dunque la natura aleatoria e non prevedibile dell'impatto si è cercato di stimarne il valore in base all'ampiezza che l'impatto dell'incidente ha sulle **due dimensioni caratterizzanti la sicurezza della dipendenza bancaria**, ovvero l'oggetto della sicurezza (asset) e la tipologia di sicurezza (safety & security). L'impatto di uno specifico reato dipende quindi dall'impatto che lo stesso ha sulle due dimensioni della sicurezza:

$$I = F(I_{sec,c}, I_{saf,c}, I_{saf,d}, I_{sec,cc}, I_{sec,cs}, I_{sec,atm}, I_{sec,bs}, I_{sec,im}, I_{sec,co})$$

Per ogni tipologia di reato precedentemente identificato è possibile determinare la magnitudo dell'impatto grazie alla seguente matrice

Tabella ordinamento in base a impatto

	Cliente		Dip.	Cassa		Cassette	Beni	ATM	Immag.	Comp.	TOT
	Saf	Sec	Saf	Sec	Sec	Strutt.	Sec	Sec	Sec	Comm.	
Rapina al Cliente	X	X	X						X		4
Rapina Cassa	X		X	X					X		4
Rapina C. Sicurezza	X		X		X				X		4
Rapina Beni Strutt	X		X			X			X		4
Rapina all'ATM	X	X						X			3
Frode con falsa identità	X	X		X							3
Rapina fuori filiale	X	X									2
Rapina al portavalori (trasporto)			X						X		2
Rapina portavalori			X					X			2

(op. di caricamento)										
Attacco ATM logico							X	X		2
Attacco ATM fisico							X	X		2
Furto di identità	X	X								2
Furto con destrezza	X	X								2
Dannegg. Per danno Imm.						X		X		2
Dannegg. Per interr. Serv.						X		X		2
Dannegg. Per Furto.						X		X		2
Furto F.O.L. Cassa				X						1
Furto F.O.L. C. Sicurezza					X					1
Furto F.O.L. B. Strutt						X				1
Util. False Cred. ATM		X								1
Frode con False Cred.				X						1
Frode con Falsi Titoli				X						1

Tabella 32. Matrice Minaccia-Asset per il calcolo dell'impatto

Come è possibile notare i reati che hanno un valore di impatto maggiore sono le rapine. Questo è evidente se si pensa che la rapina è il reato che va ad impattare non soltanto sulla security e quindi sul patrimonio, ma soprattutto sulla safety e quindi sulla salute psichica e fisica delle persone che lavorano in banca e di quelle che si trovano lì per richiedere servizi.

L'impatto sulla safety non è trascurabile poiché si tratta della salute delle persone. Garantire l'incolumità psico-fisica del cliente, nonché del dipendente della filiale è la ragione principale per cui si fa sicurezza. Durante una rapina in banca è importante salvaguardare il patrimonio delle persone, ma ancora più importante risulta essere la protezione di chi si trova sul luogo al momento dell'evento, per limitare eventuali danni alla persona o, persino sfiorare la tragedia.

4.3.2 Andamento delle serie storiche

L'indagine statistica è stata effettuata su un campione di 720 eventi criminosi perpetrati sul territorio italiano nell'orizzonte temporale che va dal 2005 al 2011 per rapine e attacchi atm, mentre orizzonte temporale 2009-2011 per danneggiamenti e furti.

Lo studio comparativo tra i diversi eventi è stato effettuato prendendo in esame il periodo comune a tutti e quattro gli eventi.

Innanzitutto i crimini che sono stati esaminati sono i seguenti:

1. Attacchi ATM
2. Rapina

- 3. Furti
- 4. Danneggiamenti



Figura 62. TIPOLOGIA DEGLI EVENTI CRIMINOSI orizzonte temporale 2009-2011

Se si passa ad analizzare i crimini andati a buon segno per il rapinatore/criminale emerge un dato interessante: i crimini con esito positivo per il criminale sono stati superiori rispetto a quelli sventati.



Figura 63. Esito delle rapine

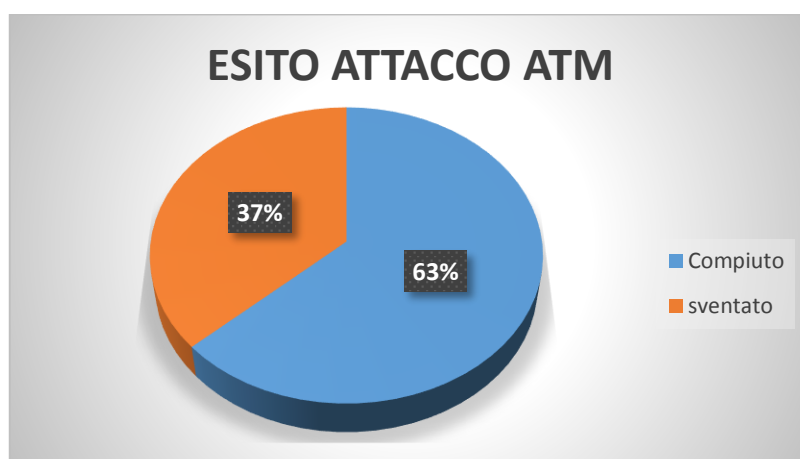


Figura 64. Esito degli attacchi all'atm

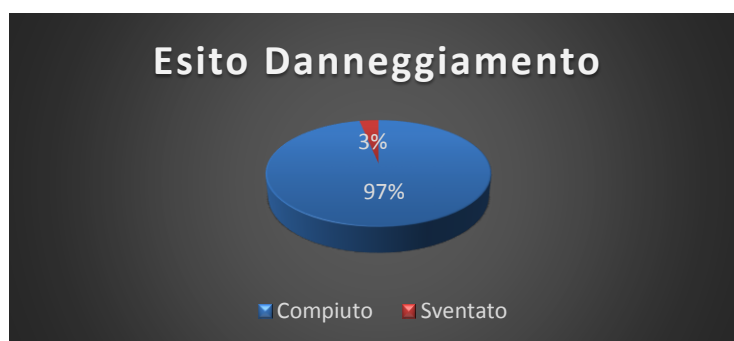


Figura 65. Esito degli eventi di danneggiamento

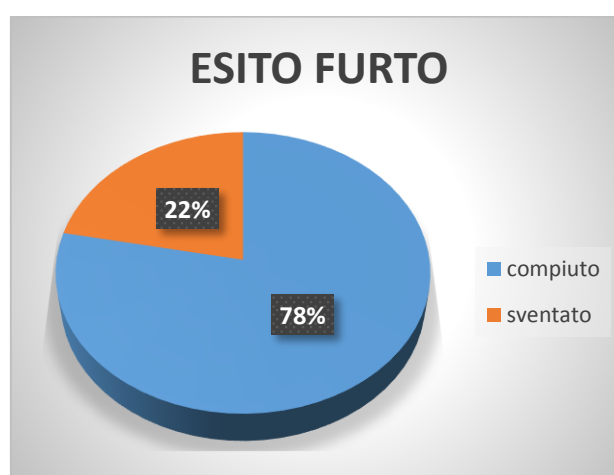


Figura 66. Esito degli eventi di furto

Questo dato fa dedurre che le misure di sicurezza adottate finora si siano rivelate poco efficaci. Per quanto riguarda le rapine, sarebbe auspicabile l'introduzione sistemi di sicurezza che siano capaci di bloccare i criminali nel proprio intento prima di essere riusciti a superare l'ingresso. Ciò che si intende fare è arrestare l'azione sul nascere e tutelare quindi non soltanto il patrimonio sul quale il rapinatore ha puntato il suo interesse, ma soprattutto coloro che lavorano in banca e le persone che vi si trovano al momento del reato. Utilizzare, infatti, misure che "captino" la presenza di armi non sempre ha avuto esito positivo soprattutto per la capacità e la bravura dei criminali di bypassare il sistema di sicurezza. Ecco perché questo limite ha fatto sì che ci si concentrasse verso misure che potessero identificare i criminali già all'esterno, non soltanto l'arma che egli ha con sé, ad esempio attraverso sistemi di riconoscimento dei volti, o dei gesti e delle posture da essi adottati.

Per ciò che concerne gli attacchi all'ATM, invece, sebbene da una prima e breve analisi potrebbe emergere una minore importanza degli eventi di attacco agli ATM (visto che non solo sono in numero inferiore rispetto agli eventi di danneggiamento e rapina ma hanno anche un tasso di successo "crimine compiuto" inferiore rispetto a tutti gli altri), è necessario tenere in considerazione il danno economico derivante dai suddetti attacchi. Prendendo in considerazione questo ultimo dato, si evince infatti che da un punto di vista economico i danni derivanti da attacchi agli ATM sono considerevoli.

Nei seguenti grafici vengono presentati i danni economici derivanti dalle diverse tipologie di reato.

RAPINA COMPIUTA IMPORTO DERUBATO	N. EVENTI	%
Danno d'immagine	162	68,35%
<=1000	8	3,38%
>1000-<=5000	12	5,06%
>5000-<=10000	15	6,33%
>10000-<=20000	23	9,70%
>20000-<=50000	8	3,38%
>50000-<=100000	3	1,27%
>100000-<=200000	4	1,69%
>200000	2	0,84%

Tabella 33. Importo derubato/Danno economico derivante da rapine.

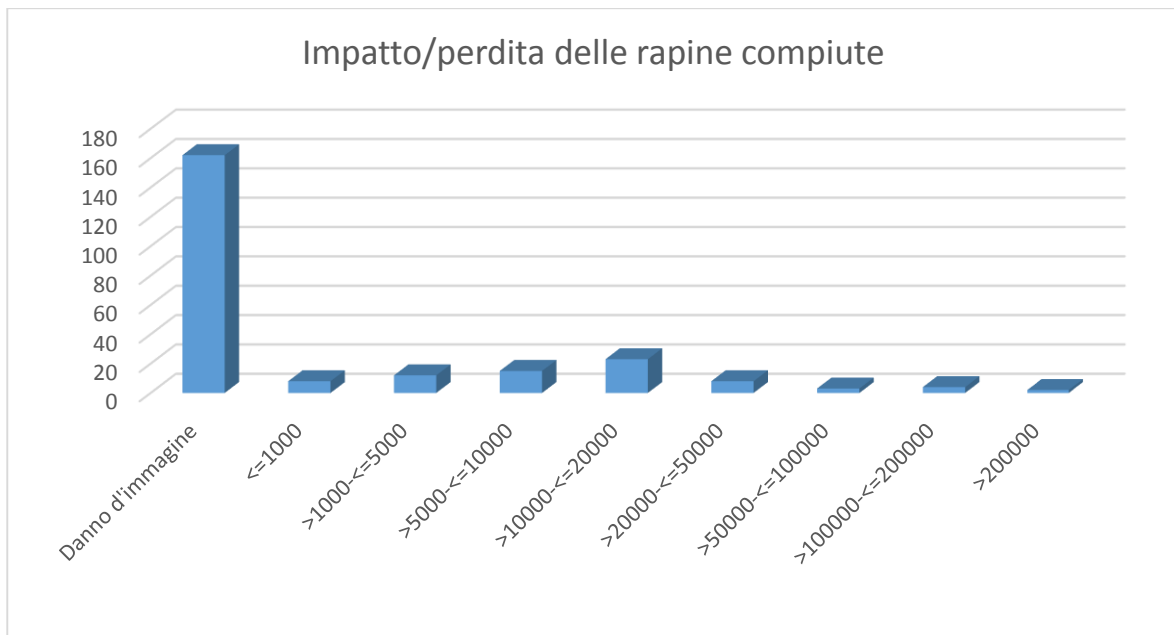


Figura 67. Impatto/perdita delle rapine compiute

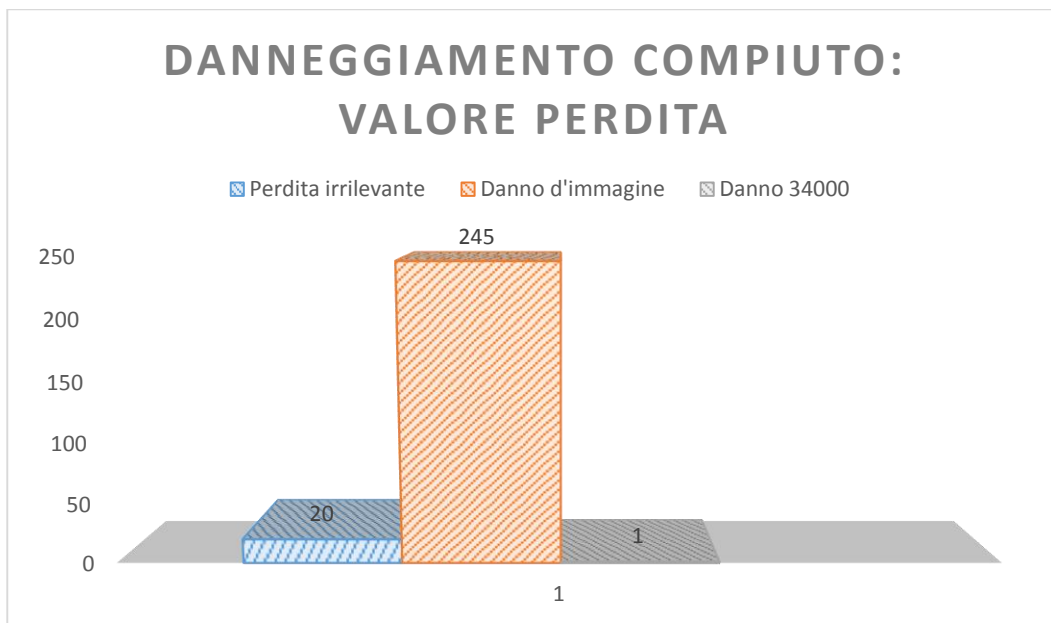


Figura 68. Danno subito/Perdita economica derivante da azione di danneggiamento

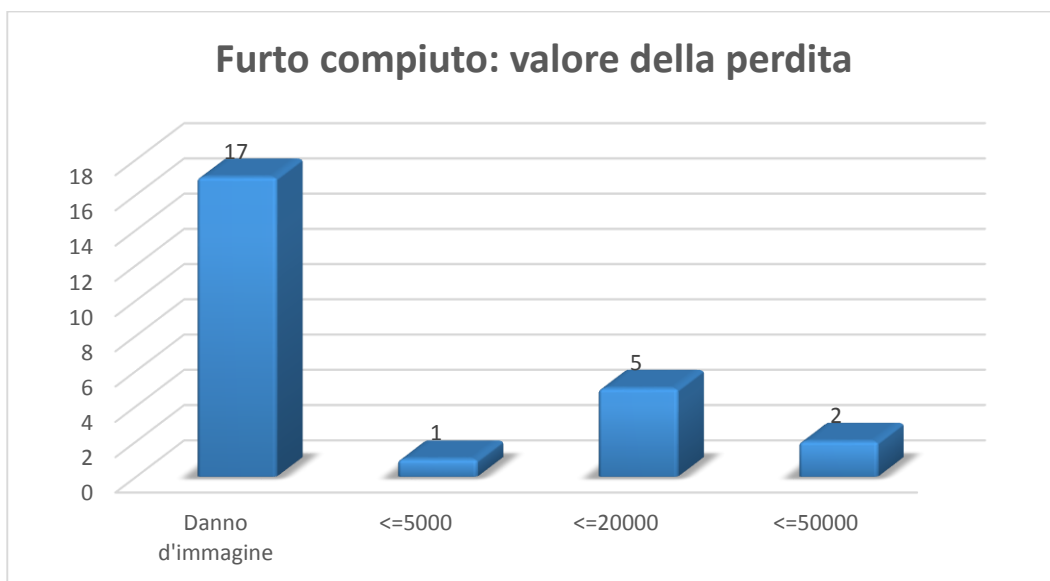


Figura 69. Danno subito/Perdita economica derivante da azioni di furto

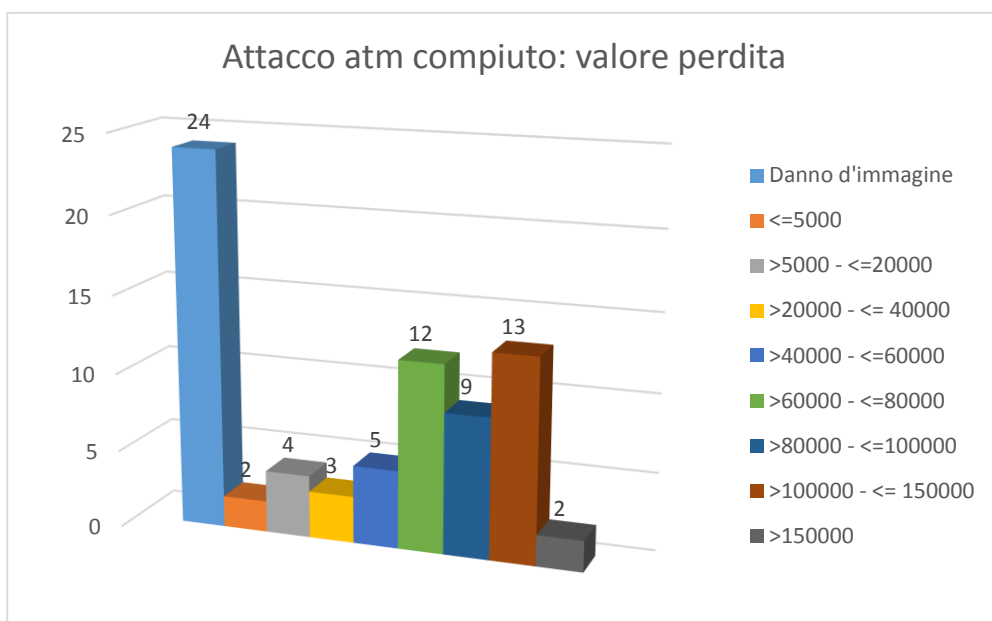


Figura 70. Danno subito/Perdita economica derivante da attacchi agli atm

Si può notare, infatti, che gli attacchi all'atm sono quelli che hanno generato alla banca perdite economiche ingenti. Questo dato è un riflesso del fatto che le banche hanno ridotto la circolazione del denaro contante all'interno della filiale come azione atta a limitare il numero di attacchi alla stessa, spostandolo all'interno delle Automated Teller Machine (ATM). Questo comportamento ha indirizzato l'interesse dei criminali verso gli erogatori di denaro contante, consapevoli che in essi avrebbero trovato quantità di denaro elevate.

Come possiamo vedere dal grafico qui sopra riportato sul valore della perdita all'ATM, gli attacchi ai bancomat hanno determinato bottini di gran lunga superiori alle altre tipologie di attacco. Il numero più elevato di eventi si registra nella fascia da 100.000 a 150.000 euro, con un bottino medio di 83.178 euro. La percentuale di attacchi all'ATM che si sono risolti esclusivamente in un danno di immagine è sensibilmente inferiore rispetto alle altre categorie di reato.

Per quanto riguarda le azioni di danneggiamento, gli eventi che hanno determinato una perdita economica diretta sono in numero irrisorio rispetto a quelli che hanno cagionato un danno di immagine (il 92% dei casi) o comunque perdite irrilevanti.

Questione simile per quanto riguarda le perdite economiche derivanti da azioni di furto. Nel 68% dei casi tali perdite si traducono in danni di immagine. I danni economici diretti si attestano principalmente sotto la soglia dei 20.000 euro e, nel campione in esame, mai sopra la soglia dei 50.000 euro.

Con riferimento agli attacchi all'ATM, inoltre, si osserva una elevata concentrazione di eventi criminosi in prossimità del fine settimana. In particolare, di sabato si concentrano oltre il 50 % degli attacchi all'ATM. Ciò è presumibilmente dovuto al fatto che per il fine settimana gli ATM vengono caricati in genere con un quantitativo di contante superiore (per far fronte alle due giornate di chiusura della dipendenza bancaria). Questo dato interessante ha consentito di tirare fuori una misura che garantisce il caricamento della macchina ogni qualvolta venga superata la soglia limite. Si tratta dunque di gestire il carico degli ATM in funzione del tasso di svuotamento degli stessi o sulla base, comunque, di modelli predittivi finalizzati a minimizzare i depositi inutilizzati di denaro.

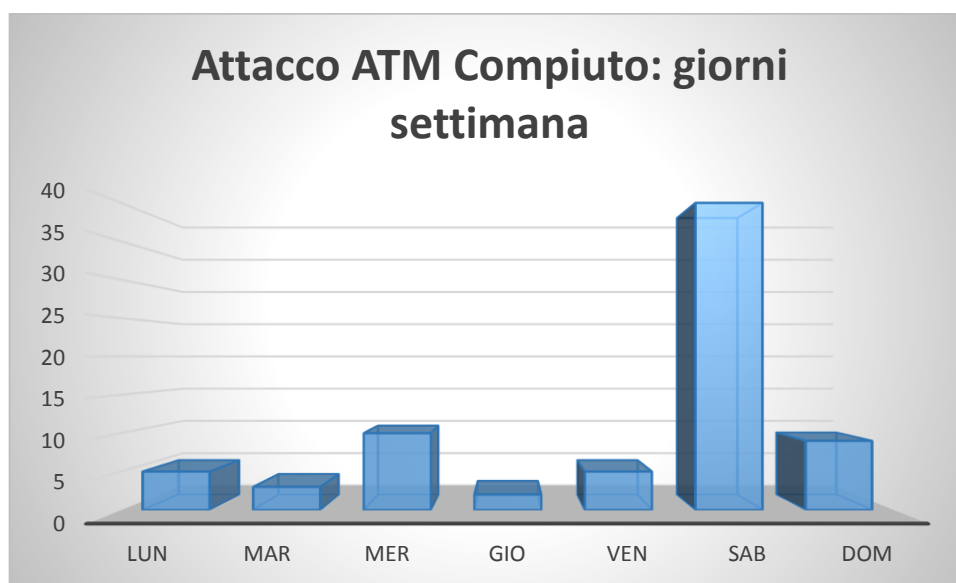


Figura 71. ATTACCO ATM COMPIUTO: Giorni della settimana

Qui di seguito viene presentata una classifica degli eventi criminosi a partire dall'analisi delle serie storiche. In particolare la classifica è stilata tenendo in considerazione 4 criteri e assegnando a ciascun crimine un valore da 0 a 4 per ogni criterio. L'assegnazione del peso è avvenuta attribuendo valore max, ovvero 4 all'evento che per il criterio in esame ha presentato un alto valore nella serie storica, valore 1 a quello che ha ottenuto un valore o una percentuale bassa. I criteri utilizzati sono stati i seguenti:

- numero di eventi nel tempo
- esito evento (percentuale crimine andato a segno sul totale)
- perdita economica (valore importo sottratto)
- evoluzione temporale

ad es. il crimine con numero di occorrenze più alto ha avuto valore 4, è stato assegnato peso 4 anche a quello con maggiore importo sottratto (perdita economica più alta) rispetto agli altri 3 eventi criminosi

Reato	Numero	Esito	Perdite econ	Evoluz temp	Tot
Attacco logico ATM	2	1	4	4	11
Attacco fisico ATM	2	1	4	4	11
Util. False Cred. ATM	2	1	4	4	11
Rapina fuori filiale	3	3	3	0	9
Rapina al Cliente	3	3	3	0	9
Rapina cassa	3	3	3	0	9
Rapina C. Sicurezza	3	3	3	0	9
Rapina Beni Strutt	3	3	3	0	9
Rapina all'ATM	3	3	3	0	9
Frode con Falsa Identità	1	2	2	4	9
Rapina Portavalori (trasp)	3	3	3	0	9
Rapina Portavalori (car.)	3	3	3	0	9
Furto Identità	1	2	2	4	9
Furto con destrezza	1	2	2	4	9
Dannegg per danno Imm	4	4	1	0	9

Dannegg. Per interr. Serv.	4	4	1	0	9
Dannegg. Per Furto.	4	4	1	0	9
Furto F.O.L cassa	1	2	2	4	9
Furto F.O.L C.Sicurezza	1	2	2	4	9
Furto F.O.L. B. Strutt	1	2	2	4	9
Frode con False Cred.	1	2	2	4	9
Frode con Falsi Titoli	1	2	2	4	9

Tabella 34. Ranking Reati-Serie storiche

Per poter poi individuare i reati sui quali concentrare l'attenzione in termini di misure di sicurezza con l'obiettivo di ridurre il rischio è stata stilata una classifica che mettesse insieme l'ordine ottenuto dalla tabella impatto e l'ordinamento derivante dalla serie storica.

Gli eventi con un punteggio alto saranno quelli su cui dovrà essere rivolta la maggiore attenzione in termini di tecnologie di protezione da adottare.

Reato			Totale
Rapina al Cliente	9	4	13
Rapina cassa	9	4	13
Rapina C. Sicurezza	9	4	13
Rapina Beni Strutt	9	4	13
Attacco logico ATM	11	2	13
Attacco fisico ATM	11	2	13
Rapina all'ATM	9	3	12
Util. False Cred. ATM	11	1	12
Frode con Falsa Identità	9	3	12
Rapina fuori filiale	9	2	11
Rapina Portavalori (trasp)	9	2	11
Rapina Portavalori (car.)	9	2	11
Furto Identità	9	2	11
Furto con destrezza	9	2	11
Dannegg. Per danno imm	9	2	11
Dannegg. Per interr. Serv.	9	2	11
Dannegg. Per Furto.	9	2	11
Furto F.O.L cassa	9	1	10

Furto F.O.L C.Sicurezza	9	1	10
Furto F.O.L. B. Strutt	9	1	10
Frode con False Cred.	9	1	10
Frode con Falsi Titoli	9	1	10

Tabella 35. Tabella dei punteggi per ciascun reato

Come si può notare dalla tabella dei punteggi, i reati da tenere sotto controllo sono le rapine e gli attacchi all'atm. Queste due tipologie di eventi richiedono misure di prevenzione e protezione più evolute rispetto a quelle esistenti. L'obiettivo è quello di proporre tecnologie che riducano drasticamente il numero di reati e di conseguenza il rischio di subire un attacco.

4.3.4 Vulnerabilità dell'area in cui si colloca la filiale, rispetto a ciascun reato

La vulnerabilità dell'area in cui è ubicata l'agenzia purtroppo agisce di riflesso sulla dipendenza stessa che non può limitare gli effetti che derivano dall'essere esposta ai pericoli del posto. Dal focus group è scaturito che i fattori di debolezza dell'area e quindi i fattori che incidono sull'attaccabilità della dipendenza sono i seguenti:

1. Ubicazione dell'immobile	<ul style="list-style-type: none"> ◆ Zona isolata ◆ Zona periferica ◆ Zona semi-periferica ◆ Zona centrale
2. Raggiungibilità dell'immobile	<ul style="list-style-type: none"> ◆ Veicolare veloce, in prossimità di grandi arterie ◆ Veicolare veloce ◆ Veicolare lenta ◆ Solo pedonale
3. Distanza degli insediamenti delle Forze dell'ordine	<ul style="list-style-type: none"> ◆ Oltre i 5 km dall'agenzia (vie di collegamento particolarmente trafficate) ◆ Oltre i 5 km dall'agenzia ◆ A meno di 5 km dall'agenzia ◆ A meno di 3 km dall'agenzia ◆ A meno di 1 km dall'agenzia

4. Ubicazione dell'agenzia	<ul style="list-style-type: none"> ◆ Esterna (accesso diretto da strada) ◆ Esterna (accesso diretto da strada) in zone ad alta frequentazione ◆ Interna con presidi aperti (c/o centri commerciali, ospedali, ASL, etc.) ◆ Interna con presidi chiusi (c/o enti, caserme, ministeri, etc.)
5. Locali confinanti con l'agenzia	<ul style="list-style-type: none"> ◆ Esistono locali confinanti per cui non si hanno garanzie di presidio ◆ Esistono locali confinanti, ma sono adeguatamente presidiati ◆ Nessuno
6. Spazi aperti confinanti con l'agenzia	<ul style="list-style-type: none"> ◆ Esistono spazi aperti con scarsa visibilità generale ◆ Esistono spazi aperti con adeguata visibilità diurna ◆ Esistono spazi aperti con adeguata visibilità diurna / notturna ◆ Nessuno

Tabella 36. Fattori vulnerabilità area

Analizzando in maniera un po' più dettagliata questi fattori emerge ad esempio che l'ubicazione dell'immobile rappresenta una vulnerabilità di area perché collocare l'agenzia in un luogo isolato potrebbe aumentare il rischio di attacco da parte dei malviventi. Il fatto di non essere visto, incentiva il malfattore nel suo intento criminoso consapevole di agire indisturbato. Se a questo si aggiunge una raggiungibilità dell'immobile veicolare veloce e una distanza dagli insediamenti delle forze dell'ordine elevata, la possibilità di attacchi tende ad aumentare e di conseguenza i rischi a cui è esposta la filiale si moltiplicano.

Questi fattori sono indicati come vulnerabilità di area perché non si riferiscono alle caratteristiche della filiale stessa, ma a quelle del luogo circostante in cui essa si trova ad operare. C'è da dire che questi aspetti non possono essere controllati da sistemi e tecnologie utilizzati per proteggere la filiale da attacchi che la riguardano all'interno o sistemi per proteggere gli atm. La riduzione della vulnerabilità dell'area quindi esula dagli obiettivi di questo lavoro.

I fattori di vulnerabilità della filiale sono i fattori di debolezza tipici di una filiale in rapporto ad uno specifico reato. La filiale è sottoposta spesso a rischi come rapine, furti, danneggiamenti. Questi pericoli sono rafforzati dal fatto che ogni dipendenza bancaria deve scontrarsi con i

fattori di debolezza che la caratterizzano. Tuttavia le vulnerabilità possono essere rimosse o quantomeno limitate mediante l'introduzione di sistemi di sicurezza più evoluti, capaci di superare i limiti dei sistemi tradizionali. Per poter individuare le misure in grado di ridurre il livello di vulnerabilità e contrastare dunque la criminalità nei confronti delle agenzie bancarie è necessario chiarire prima di tutto quali sono i fattori individuati come punti di debolezza di una filiale.

In particolare sono stati identificati i seguenti fattori:

- 1. Accessi all'agenzia:** l'ingresso principale costituisce una fonte di rischio furto e rapina. Le rapine avvengono spesso perché il rapinatore accede indisturbato passando dalla bussola senza problemi, assumendo le "sembranze" del cliente abituale. Misure capaci di limitare i problemi dei sistemi presenti all'accesso sono l'introduzione di tecnologie di smart face e gesture recognition capaci di riconoscere il criminale e bloccargli l'accesso. Altre forme di accesso che costituiscono pericolo sono rappresentate da finestre, cunicoli o accessi mediante un locale confinante.
- 2. Numerosità delle casse interne:** all'aumentare del numero di casse aumenta la vulnerabilità dell'agenzia. Il fatto di dover gestire un numero elevato di casse e controllare di conseguenza diversi monitor associati alle telecamere di videosorveglianza può rappresentare un vantaggio per il rapinatore poiché può approfittare della disattenzione temporanea dell'operatore alla postazione video e della distrazione fisiologica che si manifesta con il trascorrere del tempo per agire su una di essa.
- 3. Assenza sistemi di protezione contanti per le casse interne e per i caveau:** La mancanza di sistemi che segnalino un furto o una rapina o, ancora meglio, che impediscano l'apertura delle casse e l'accesso nei caveau rappresenta una vulnerabilità.
- 4. Numerosità degli sportelli ATM:** è facile pensare che all'aumentare del numero di sportelli Atm aumenta il grado di vulnerabilità. Quest'ultimo continuerà a crescere se la filiale presenta sportelli atm sparsi in luoghi isolati. La loro collocazione in luoghi isolati, infatti, aumenta il rischio degli atm di essere soggetti ad attacchi perché incrementa la percezione della vulnerabilità di quella filiale nella mente del criminale.
- 5. Assenza di sistemi di protezione per gli ATM o per le operazioni di caricamento degli stessi:** l'assenza di sistemi di protezione per gli atm è un aspetto che non va trascurato in quanto il furto del denaro presente all'interno della macchina genera le perdite economiche più ingenti, così come le rapine durante le operazioni di caricamento. Attualmente le rapine e i furti agli atm sono cresciuti proprio perché si è diffusa la percezione nel criminale della limitazione dell'uso del contante all'interno della dipendenza e della sua presenza all'interno delle macchine.
- 6. Assenza sistema di protezione cassette di sicurezza:** proteggere le cassette di sicurezza da eventuali furti è estremamente importante poiché si tratta di un servizio di custodia che consente ai titolari di conservarvi valori, documenti o oggetti preziosi con un'elevata

privacy e con un elevato grado di sicurezza. Trattandosi quindi di custodia di oggetti di elevato valore è estremamente importante garantirne la sicurezza mediante sistemi che siano capaci di impedirne l'apertura nelle situazioni di pericolo. Proprio per tale ragione l'accesso al servizio viene di norma effettuato in stanze blindate, a volte presenti nel caveau delle banche, all'interno delle quali il cliente viene lasciato solo per effettuare in piena privacy le operazioni di immissione o di estrazione di oggetti/valori dalla cassetta di sicurezza. L'assenza, quindi di sistemi che proteggono le cassette di sicurezza rappresenta una vulnerabilità elevata perché avrebbe un forte impatto sulla security del cliente.

- 7. Assenza Sistema di protezione Perimetrale:** Le difese perimetrali sono rappresentate da tutte quelle misure che dovrebbero impedire, o perlomeno scoraggiare, l'accesso dei rapinatori nella dipendenza bancaria. La protezione perimetrale dell'agenzia risulta essere il principale modo per scoraggiare i criminali.
- 8. Assenza servizio di piantonamento:** il servizio di piantonamento svolge un'ottima funzione di deterrenza nei confronti dei criminali soprattutto se fornito in determinati orari e luoghi strategici. L'assenza di piantonamento può essere fatale soprattutto per quelle filiali maggiormente esposte al rischio, ad esempio per quelle collocate in zone isolate e lontane dagli insediamenti delle forze dell'ordine.
- 9. Assenza di servizio di videocollegamento/videosorveglianza:** la videosorveglianza oltre ad essere un deterrente rappresenta uno strumento di trasmissione delle immagini in diretta ad una centrale operativa remota o per la ricostruzione dell'evento e l'eventuale riconoscimento del criminale.
- 10. Assenza impianto di allarme.** L'impianto di allarme è importante perché consente di segnalare una rapina in corso, mentre in orario di chiusura della dipendenza consente di proteggere i mezzi forti e le aree interne della banca da un potenziale furto. L'assenza di impianto di allarme favorisce l'azione del criminale che può intrufolarsi all'interno anche di notte e portare a compimento il reato senza il timore di essere scoperto.
- 11. Assenza sistema di rilevazione permanenza nei locali:** l'assenza di sistemi di rilevazione di permanenza dei locali facilita l'azione del criminale che può agire indisturbato senza subire la pressione del tempo.
- 12. Prestazioni/obsolescenza degli impianti di sicurezza.** Il controllo periodico dei sistemi di sicurezza è importante per garantirne l'efficacia e il funzionamento degli stessi e quindi ridurre il rischio di attacchi.
- 13. Comportamenti non adeguati da parte del personale:** i comportamenti non adeguati da parte del personale nel momento in cui si verifica una rapina potrebbero complicare la situazione, già rischiosa, in cui ci si trova e generare confusione e panico tra clienti e dipendenti stessi. È necessario, perciò, integrare le misure di difesa con comportamenti adeguati da adottare quotidianamente nel corso dell'attività lavorativa. Emerge dunque

che occorre formare ed informare non soltanto il personale addetto alla vigilanza, ma anche i dipendenti della banche sulle dinamiche comportamentali e sul temperamento da tenere nel caso in cui ci si trovi di fronte ad una rapina.

Dalla percezione della vulnerabilità si evince che non è semplice delineare un quadro del rapinatore occasionale poiché le sue mosse sono difficilmente prevedibili, per tale ragione ci si concentra sul rapinatore professionista e sul suo comportamento tipo. È infatti possibile tirare fuori delle azioni, dei movimenti, delle posture, dei gesti che il professionista mette in atto prima di concretizzare il suo intento doloso nei confronti di una filiale obiettivo.

Come riportato nel paragrafo relativo alla percezione della vulnerabilità, generalmente il malvivente con esperienza effettua sopralluoghi frequenti prima di attuare la sua azione criminosa, studia bene i dispositivi adottati dalla specifica agenzia e che potrebbero indurre scarsa appetibilità ed accessibilità al bottino, analizza le vulnerabilità dell'area e quelle presenti in filiale cercando di colpire a partire da esse. Se da un lato questo potrebbe essere un punto di forza del malvivente, che studiando ogni dettaglio riesce a programmare i movimenti, dall'altro può trasformarsi in un punto di debolezza perché questi stessi movimenti potranno essere osservati e studiati da chi fa sicurezza per realizzare un sistema che sia in grado di riconoscerli e di lanciare l'allarme.

Reato	Fattore
Furto	Accessi all'agenzia, Numerosità delle casse interne, Assenza di sistemi protezione contanti per le casse interne e per i caveau, Numerosità degli sportelli ATM, Assenza di sistemi protezione per gli ATM, Assenza Sistema di protezione Cassette Sicurezza, Assenza Sistema di protezione Perimetrale, Assenza Servizio di piantonamento, Assenza Impianto di videosorveglianza, Assenza Impianto Allarme, Assenza Sistema di rilevazione permanenza nei locali dell'agenzia, Prestazioni/Obsolescenza degli impianti di sicurezza, Comportamenti non adeguati da parte del personale
Rapina	Accessi all'agenzia, Numerosità delle casse interne, Assenza di sistemi protezione contanti per le casse interne e per i caveau, Numerosità degli sportelli ATM, Assenza di sistemi protezione per gli ATM o per le operazioni di caricamento degli stessi, Assenza Sistema di protezione Cassette Sicurezza, Assenza Sistema di protezione Perimetrale, Assenza Servizio di piantonamento, Assenza Impianto di videosorveglianza, Assenza Impianto Allarme, Assenza Sistema di rilevazione permanenza nei locali dell'agenzia, Prestazioni/Obsolescenza degli impianti di sicurezza, Comportamenti non adeguati da parte del personale

Frode	Assenza Servizio di piantonamento, numerosità delle casse interne, Assenza impianto di videosorveglianza, Prestazioni/Obsolescenza degli impianti di sicurezza, Comportamenti non adeguati da parte del personale
Danneggiamento	Impianto di videosorveglianza, Obsolescenza degli impianti di sicurezza installati

Tabella 37. Vulnerabilità specifiche della filiale

4.4 Fase 3: Individuazione delle azioni correttive intese a ridurre il rischio di incidenti

In questa fase del lavoro di ricerca ci si occuperà di individuare quelle azioni che consentano di minimizzare il rischio legato all'esecuzione dei reati ai danni delle dipendenze bancarie. Ciò significa individuare l'insieme delle azioni (AZ) che consentano di minimizzare la funzione obiettivo del nostro modello di rischio:

$$\min_{r_i \in RD, f_j \in RD} \sum Risk(r_i, f_j) = \min_{r_i \in RD, f_j \in RD} \sum P(r_i, f_j) \times I(r_i, f_j)$$

Quindi andremo ad individuare quelle azioni in grado di:

- prevenire il rischio di reato → che hanno effetto diretto sul minimizzare la funzione $P(r_i, f_j)$
- reagire al reato (proteggere la filiale in caso di esecuzione del reato) → che hanno effetto diretto sul minimizzare la funzione $I(r_i, f_j)$

Al fine di individuare correttamente le misure più adatte alla prevenzione o alla protezione delle banche da potenziali attacchi criminali è stato ritenuto opportuno approfondire il tema andando ad analizzare la letteratura scientifica ampiamente discussa nel paragrafo 3.2. Partendo dallo studio della letteratura è emerso che i luoghi che sono soggetti ad atti criminosi sono noti come infrastrutture critiche. Le infrastrutture critiche sono quelle strutture quali porti, aeroporti, siti istituzionali e banche, che si trovano continuamente a rischio di atti vandalici, sabotaggi fisici ed informatici, attentati e minacce al patrimonio fisico come furti, rapine, incendi dolosi ed occupazioni (Anderson & Malm, 2006).

Lo stato dell'arte ha permesso di analizzare numerose misure. Le misure di sicurezza passate in rassegna, sono state sia di natura tecnologica che organizzativa.

Un elenco delle misure individuate a seguito dell'analisi dello stato dell'arte è di seguito presentato.

Misura di sicurezza		Descrizione
1 Tecnologie biometriche		
	Sistema biometrico basato su <i>Impronte digitali</i>	Una impronta digitale è un'impronta lasciata dai dermatoglifi dell'ultima falange delle dita delle mani. Il riconoscimento biometrico è effettuato confrontando caratteristiche come la tipologia globale dell'impronta, la posizione e la tipologia di alcuni punti distintivi, l'orientamento e frequenza delle creste, la posizione ed il tipo delle minuzie (terminazioni, biforcazioni delle creste) (Maltoni, Maio, Jain, & Prabhakar, 2009).
	Sistema biometrico basato su <i>Riconoscimento del volto</i>	Si tratta di un processo di acquisizione del tratto biometrico a scarsa invasività. I sistemi biometrici basati sul volto possono utilizzare caratteristiche globali o misurazioni locali.
	Sistema biometrico basato su <i>Iride</i>	L'iride è considerato il tratto biometrico più accurato. Un limite alla diffusione di questa tecnologia consiste nel fatto che il processo di acquisizione delle immagini iridee viene considerato invasivo e pericoloso per la vista da parte di numerosi utenti. I sistemi biometrici basati sull'iride sono inoltre relativamente costosi. La maggior parte di questi sistemi biometrici è basata sul calcolo di una stringa binaria che ne incorpora le caratteristiche distintive, chiamata Iriscodex (Daugman, 2004).
	Sistema biometrico basato sulla <i>Geometria della mano</i>	I sistemi biometrici basati sulla geometria della mano, forniscono sicuramente un'accuratezza inferiore a quella dei sistemi basati sull'analisi dell'iride o delle impronte digitali o iride. Tuttavia questa tecnica è particolarmente apprezzata in quanto è ritenuta come poco invasiva dagli utenti. Il metodo è basato sull'acquisizione di una fotografia della mano mentre essa è posizionata su un supporto (eventualmente con l'ausilio di pioli per aiutare il corretto posizionamento). (Sidlauskas & Tamer, 2008).
	Sistema biometrico basato sulla <i>Retina</i>	I sistemi basati sulla retina sfruttano l'unicità dei pattern delle vene presenti sulla zona posteriore del bulbo oculare per effettuare il riconoscimento biometrico. La distribuzione dei vasi sanguinei sulla retina è infatti principalmente casuale ed univoca per ogni individuo. Tra i principali vantaggi, è da annoverare che questo tratto biometrico è difficilmente falsificabile, in quanto la parte esaminata si trova all'interno dell'occhio. Per lo stesso motivo, però, la scansione della retina viene vista come intrusiva e potenzialmente dannosa (Jain, Ross, & Prabhakar, 2004)
2	Tecnologie di sniffer artificiali	"nasi elettronici" o "sniffer chimici" che rilevano sostanze illecite, polvere da sparo o materiale esplosivo
3	Radar e telecamere termiche e visive	rilevazione immediata e localizzazione di un intruso. Le telecamere con ristretto campo visivo sono utilizzate per l'identificazione e il tracciamento di un oggetto

4	Body scanner	Permette una ispezione corporale, finalizzata alla ricerca di armi e/o esplosivi, senza alcun contatto fisico con gli addetti alla sicurezza.
5	Televisione a Circuito chiuso (TVCC) o Closed Circuit Television (CCTV)	Telecamere che trasmettono il segnale verso specifici o limitati set di monitor e/o videoregistratori. Gli impianti TVCC sono utilizzati prevalentemente come sicurezza passiva, ossia sistemi che registrano 24 ore su 24 e al verificarsi di eventi vandalici, attentati o qualsiasi evento di questo tipo, le immagini registrate vengono analizzate per ricostruire il fatto (Matchett, 2003). Bisogna tuttavia sottolineare che nei sistemi di videosorveglianza tradizionale con elevati numeri di monitor da sorvegliare, soltanto il 3% delle immagini vengono effettivamente viste in tempo reale dagli operatori di sorveglianza e che inoltre tali operatori necessitano di una pausa fisiologica di circa 5 minuti ogni ora (Wallace & Diffley, 1988). Questi fattori limitano fortemente l'efficacia di questi sistemi di sorveglianza.
6	Sistemi di videosorveglianza affiancati a sistemi intelligenti di supporto alle decisioni	Superano i limiti degli impianti TVCC. Consentono, infatti, di rilevare in maniera semiautomatica situazioni di rischio, comportamenti anomali o individuazione di persone sospette
7	modello di ottimizzazione attacker defender	Il concetto chiave di un modello di questo tipo risiede nella minimizzazione dei costi per il "defender" in riferimento a potenziali attacchi.
8	piattaforma di simulazione denominata CIMS	CIMS fornisce un ambiente visuale e interattivo per osservare effetti a cascata e conseguenza di perturbazioni delle infrastrutture. La piattaforma consente di identificare la "sotto-rete" critica (ovvero insieme di asset coinvolti nella relazione causa-effetto), i punti di debolezza della rete e le possibili contromisure.
9	modello di valutazione delle vulnerabilità delle infrastrutture, denominato I-VAM (Infrastructure Vulnerability Assessment Model).	Le componenti di protezione del sistema vengono definite secondo le dimensioni di <i>deterrenza</i> , <i>rilevazione</i> , <i>ritardo</i> e <i>contromisure</i>
10	Modello di simulazione basato sulla presenza di due agenti "intelligenti (attaccante e difensore)	Il difensore è modellato come una serie di sensori (sistemi di protezione attiva) e barriere (sistemi di protezione passiva) accoppiati secondo la logica di limitare e reagire agli attacchi. Viene presentato uno scenario di simulazione relativo alla protezione fisica di un aeroporto. Nel modello, il sensore ha una certa probabilità di rilevare una delle seguenti situazioni: – Nessun pericolo rilevato.

		<ul style="list-style-type: none"> – Possesso di armi – Comportamento Sospetto – Persona di interesse (ad es. Ricercato). <p>Una volta che un sensore (automatico o persona) ha rilevato una situazione di rischio (in maniera corretta o errata) e quindi l'informazione passa nel "defense action block", è possibile intraprendere una delle seguenti azioni:</p> <ul style="list-style-type: none"> – Nessuna azione – Ripetere la rilevazione (ad es. una persona passa nuovamente attraverso il metal detector dopo aver rimosso alcuni oggetti personali). – Effettuare un controllo ulteriore (ad es. manuale) – Bloccare il sospetto
11	Sistemi di sorveglianza basati sull'analisi dei movimenti umani.	
13	Framework di rilevazione di "incidenti" all'ATM	<p>Si propone un framework per la rilevazione tramite video di eventi criminosi ai danni degli ATM.</p> <p>L'autore propone un'architettura di sistema suddivisa in tre parti. La prima parte comprende una telecamera che cattura le immagini video. La seconda parte è il modulo di rilevamento di oggetti multipli che rilevano l'esistenza di più di una persona nei pressi dell'ATM. Se si rileva più di una persona, allora verrà visualizzato un prompt per l'utente. Se il cliente acconsente alla presenza delle altre persone, le informazioni vengono passate al modulo di riconoscimento delle attività che hanno il compito di analizzare il comportamento umano. Se l'interazione avviene normalmente allora la transazione vera e propria potrà avere luogo altrimenti viene prodotto un allarme nei confronti degli addetti alla sicurezza</p>
14	sistema di videosorveglianza intelligente capace di rilevare comportamenti e traiettorie anomale	<p>Sistema di videosorveglianza intelligente capace di rilevare comportamenti e traiettorie anomale. Al fine di analizzare le traiettorie per il comportamento di interesse, l'atrio della banca è stato suddiviso in diverse aree, in particolare zona periferica, zona bancone, zona tavolo; la restante superficie è stata definita come area aperta. Se una persona è in piedi all'interno di una zona designata, la persona è contrassegnata come operativo. Le persone nella zona aperta possono essere in fila, in piedi o in movimento. Per determinare se una persona è in coda viene definito un raggio di azione. Una persona è contrassegnata come "in coda", se un'altra persona all'interno di questo raggio di azione è a sua volta in coda o si trova allo sportello.</p> <p>Per ATM: Comportamento sospetto all'interno o nei pressi</p>

		dell'Atm (ad es. utente che entra senza effettuare operazioni; vagare nella filiale senza utilizzare l'ATM o contattare un membro del personale per un periodo di tempo prolungato; Interagire con l'ATM per un periodo di tempo insolito oppure presenza di più persone contemporaneamente nei pressi di un ATM. Movimenti repentini nei pressi di un ATM. In caso di comportamento anomalo viene segnalato un warning ad una centrale operativa.
15	modello basato sul paradigma dello "usability inspection method" degli ATM	Questo metodo, chiamato Security Usability Symmetry (SUS) sfrutta gli approcci teorici relativi alle macchine automatiche ed introduce il concetto di Multifunction Teller Machine (MTM). Viene dimostrato, tramite un caso di studio come utilizzare questo modello durante la progettazione di sistemi interattivi utilizzabili e sicuri.
16	Sistema Atm con finger print e One time Password. architettura tecnologica innovativa basata sulla raccolta di impronte digitali del cliente e del suo numero di cellulare al momento dell'apertura del conto	Quando il cliente immette la propria carta all'interno dell'ATM deve posizionare il dito sul modulo finger print, per poi ottenere automaticamente un codice a 4 cifre generato ogni volta attraverso un modem GSM collegato al microcontrollore ed inviato come messaggio al cellulare del cliente. Il codice deve essere inserito dal cliente premendo i tasti sul touch screen, e solo dopo egli sarà in grado di svolgere ulteriori azioni.
17	Fattori di deterrenza e sorveglianza naturale	Introduzione di una serie di apprestamenti di sicurezza all'interno delle filiali quali installazione di telecamere, presenza di guardie giurate, protezione degli addetti allo sportello e l'uso di vetrate trasparenti che consentono la visibilità dall'esterno garantendo la cosiddetta sorveglianza naturale

Tabella 38. Tecnologie analizzate in letteratura

Nello stato dell'arte inizialmente è stata fatta una review delle **tecnologie biometriche**: sistemi biometrici basati sulle impronte digitali, sistemi biometrici basati sulla geometria della mano, sistemi biometrici basati sul riconoscimento del volto, sistemi biometrici iridei e sistemi biometrici basati sulla retina.

I sistemi biometrici basati sulle impronte digitali risultano essere molto precisi in quanto le impronte digitali presentano caratteristiche di immutabilità ed individualità.

I sistemi biometrici basati sulla retina sfruttano l'unicità dei pattern delle vene presenti sulla zona posteriore del bulbo oculare e quindi risultano essere difficilmente falsificabili (Jain, Ross, & Prabhakar, 2004). Tuttavia poiché la parte esaminata si trova all'interno dell'occhio si tratta di

un sistema altamente invasivo. Si tratta di una tecnologia sicuramente molto precisa, ma in contrasto con le esigenze di bassa invasività auspicata dagli istituti bancari.

Un limite alla diffusione del sistema biometrico basato sull'iride riguarda anch'esso il fatto di essere troppo intrusivo e risultare molto pericoloso durante il processo di acquisizione delle immagini iridee. I sistemi biometrici basati sulla geometria della mano forniscono sicuramente un'accuratezza inferiore a quella dei sistemi basati sull'analisi dell'iride, della retina o delle impronte digitali, ma sono apprezzati in quanto ritenuti poco invasivi. Sidlauskas e Tamer (2008) ne descrivono il metodo affermando che è basato sull'acquisizione di una fotografia della mani mentre essa è posizionata su un supporto.

Tra le tecnologie biometriche, si possono tuttavia considerare i sistemi di **smart face recognition**, in quanto scarsamente invasivi. Si tratta di un sistema di riconoscimento del volto a scarsa invasività. Ad esso è associato anche un sistema anticamuffamento che consente di impedire l'accesso a soggetti non chiaramente identificabili. In particolare è una tecnologia di riconoscimento dei volti con vista su un Database delle forze dell'ordine e dei clienti "buoni". Se è un volto riconosciuto, la banca decide se:

1. Farlo entrare
2. Bloccarlo
3. Ingresso con riserva (presenza sospetta segnalata alla vigilanza, utente seguito da drone etc.).

I sistemi biometrici basati su iride e retina sebbene siano molto precisi risultano essere altamente invasivi per gli utenti e dunque in contrasto con gli obiettivi del lavoro di creare una filiale aperta e accogliente.

Si è passati poi ad analizzare le **tecnologie di sniffer artificiali**. Queste tecnologie sono state discusse ampiamente in Bonfanti (2014).

Si è discusso di ***Radar e telecamere termiche e visive***, mentre altri autori hanno analizzato le tecnologie di ***body scanner***. Queste ultime emettono onde millimetriche, ossia emissioni elettromagnetiche a bassa frequenza e hanno come obiettivo quello di rilevare oggetti addosso ad una persona (vengono rilevati tutti i materiali, metallici e non metallici: liquidi, gel, plastica, ceramica ecc., nonché tutti i tipi di oggetti: armi, esplosivi sia standard che assemblati, sostanze stupefacenti, denaro, carta ecc.). Questa misura è utilizzata negli aeroporti.

Le banche considerano la tecnologia di body scanner altamente invasiva nonché dannosa per la salute del cliente. I clienti che aprono un conto presso una specifica filiale si recano sicuramente con maggior frequenza presso la stessa e questo potrebbe avere effetti negativi sul benessere fisico degli stessi: i ripetuti passaggi dal body scanner, per poter accedere all'interno della dipendenza, a lungo andare, potrebbero rivelarsi nocivi perché il corpo si troverebbe a dover assorbire ripetutamente le radiazioni. Inoltre oltre ad essere pericoloso perché si tratta di emissione di radiazioni ionizzanti va a ledere anche la privacy personale. Per queste ragioni si esclude l'utilizzo di questa tecnologia

Alcuni autori si sono soffermati sulle **Televisione a Circuito chiuso (TVCC) o Closed Circuit Television (CCTV)**, ovvero telecamere che trasmettono il segnale verso specifici o limitati set di monitor e/o videoregistratori.

Gli impianti TVCC, come già discusso nel primo capitolo, sono utilizzati prevalentemente come sicurezza passiva. Le immagini registrate verranno analizzate solamente nel caso in cui si verifichi un attacco (rapina, danneggiamento, furto, attacco atm) ai danni della dipendenza. I video corrispondenti a ciascuna telecamera, per aumentare l'efficacia della protezione, devono essere costantemente sorvegliati da un operatore. Tuttavia l'essere umano è sottoposto a perdita di concentrazione dovuta al trascorrere del tempo. La diminuzione fisiologica dell'attenzione fa sì che molte immagini sfuggano alla sua attenzione, dunque non sempre la videosorveglianza sortisce esito positivo per la sicurezza. Per tale ragione altri autori hanno discusso di **sistemi di videosorveglianza affiancati a sistemi intelligenti di supporto alle decisioni** i quali consentono di rilevare in maniera semiautomatica le situazioni di rischio e di agire di conseguenza.

Come evinto dall'analisi dello stato dell'arte, altri autori si sono soffermati sui modelli di simulazione di eventi criminosi, c'è chi ha definito modelli di ottimizzazione orientati a rendere le infrastrutture critiche più resistenti agli attacchi, altri ancora hanno definito modelli di valutazione delle vulnerabilità delle infrastrutture critiche. Mentre c'è chi ha proposto un **framework di rilevazione di "incidenti" all'ATM**.

Il sistema di rilevazione degli incidenti all'ATM è interessante in quanto, come già descritto nel primo capitolo, è un'architettura suddivisa in tre parti. La prima parte comprende una telecamera che cattura le immagini video. La seconda parte è il modulo di rilevamento di oggetti multipli che rilevano l'esistenza di più di una persona nei pressi dell'ATM. Se si rileva più di una persona, allora verrà visualizzato un prompt per l'utente. Se il cliente acconsente alla presenza delle altre persone, le informazioni vengono passate al modulo di riconoscimento delle attività che hanno il compito di analizzare il comportamento umano. Se l'interazione avviene normalmente allora la transazione vera e propria potrà avere luogo altrimenti viene prodotto un allarme nei confronti degli addetti alla sicurezza.

In Bhaltilak, Kaur, & Khosla (2014) viene presentata una review sui **sistemi di protezione di sorveglianza basati sull'analisi dei movimenti**. I sistemi di protezione basati sull'analisi dei movimenti umani fanno parte delle misure proposte anche da questo lavoro. In particolare, si parla di **sistema di gesture recognition** in grado di riconoscere comportamenti sospetti e traiettorie anomale. Si tratta di un sistema di apprendimento su rete neurale capace di riconoscere un set limitato di posture (salto, bancone, mani alzate, prese di ostaggi, persone a terra etc.).

La gesture recognition è una tecnologia adottata anche per gli atm. In questo specifico caso è in grado di riconoscere comportamenti insoliti nei pressi delle postazioni atm. Comportamenti sospetti possono essere ad esempio la sosta nelle vicinanze della macchina senza l'esecuzione

di operazioni, oppure la presenza di più persone contemporaneamente, o ancora movimenti repentini nelle vicinanze dell'atm etc.

Sempre in riferimento alla sicurezza degli ATM abbiamo potuto vedere dall'analisi della letteratura scientifica che (Jaiswal & Bartere, 2014) propongono un approccio basato sulla raccolta delle impronte digitali dei clienti e del suo numero di cellulare al momento dell'apertura del conto. Quando il cliente immette la propria carta all'interno dell'ATM deve posizionare il dito sul modulo finger print, per poi ottenere automaticamente un codice a 4 cifre generato ogni volta attraverso un modem GSM collegato al microcontrollore ed inviato come messaggio al cellulare del cliente. Il codice deve essere inserito dal cliente premendo i tasti sul touch screen, e solo dopo egli sarà in grado di svolgere ulteriori azioni.

Questo sistema noto come **tecnologia finger print con one time password** viene proposto come misura capace di limitare gli incidenti conseguenti lo smarrimento, il furto o la clonazione della carta. Affinchè il criminale in possesso della carta possa appropriarsi del denaro presente sul conto associato alla stessa, dovrà prelevare l'importo desiderato. Tutto questo è reso possibile soltanto nel caso in cui sussistano due condizioni:

1. Si disponga del cellulare dell'intestatario della carta (sul quale come già affermato verrà inviato il codice da inserire per poter effettuare l'operazione)
2. Si disponga anche della sua impronta digitale (e questo è impossibile poiché l'impronta è univoca per ogni persona).

Questi passaggi evidenziano fortemente la validità e l'efficacia della misura.

In riferimento alla sicurezza degli atm, dall'analisi della serie storica si è osservata un'elevata concentrazione di eventi criminosi in prossimità del fine settimana. In particolare, di sabato si concentrano oltre il 50 % degli attacchi all'ATM. Ciò è presumibilmente dovuto al fatto che per il fine settimana gli ATM vengono caricati in genere con un quantitativo di contante superiore (per far fronte alle due giornate di chiusura della dipendenza bancaria). Questa considerazione ha portato a proporre una misura organizzativa volta a minimizzare il numero di attacchi all'atm durante il fine settimana: **Caricamento intelligente ATM**. In questo modo l'atm non verrà caricato il venerdì con un elevato importo per poter far fronte ai due giorni non lavorativi, ma verrà incaricata una persona che si occuperà di ricaricare la macchina ogni qualvolta viene superata la soglia limite. Si tratta dunque di gestire il carico degli ATM in funzione del tasso di svuotamento degli stessi o sulla base, comunque, di modelli predittivi finalizzati a minimizzare i depositi inutilizzati di denaro.

Le ultime due misure che vengono analizzate sono la tecnologia di **Anti tampering ATM** e la **Volumetric change detection**. Si tratta di misure utilizzabili sia per ATM interni (atm che si trovano all'interno della filiale stessa, o comunque nelle sue vicinanze), sia per quelli esterni, vale a dire per quegli atm ubicati in zone lontane dal luogo in cui è posizionata la filiale di appartenenza.

La prima tecnologia è costituita da sensori di contatto su pannello e intero bancomat. Si tratta di trasmettitori /ricevitori infrarossi che scattano quando viene introdotto un corpo estraneo (ad esempio l'introduzione di una forcina nella bocchetta erogatrice). Alla rilevazione il sistema reagisce in due modi:

1. Contatta la vigilanza
2. Si mette in out of service

La tecnologia di volumetric change detection, invece, è in grado di rilevare modifiche (macro) di un ambiente dell'agenzia o locale ATM, ad esempio presenza di valigetta esplosiva, bomboletta di gas, etc., o anche modifiche (micro) della geometria di un ATM, per rilevare ad esempio l'applicazione di skimmer, false tastiere, microtelecamere, etc

MISURA	DESCRIZIONE
Smart face recognition (eventualmente con sistemi di anticamuffamento)	<p>La smart face recognition fa parte della categoria dei sistemi biometrici.</p> <p><u>SFR sia all'ingresso delle filiali (e ATM chiusi) che su ATM aperti: è una tecnologia di riconoscimento dei volti con vista su un DB delle forze dell'ordine e dei clienti "buoni". Se è un volto riconosciuto, la banca decide se:</u></p> <ol style="list-style-type: none"> 1. Farlo entrare 2. Bloccarlo 3. Ingresso con riserva (presenza sospetta segnalata alla vigilanza, utente tracciato da videocamere con segnalazioni audio, utente seguito da drone etc. <p><u>In letteratura:</u> secondo Reynolds e Bank (2006) la tecnologia di riconoscimento facciale risulta essere molto utile per risolvere problemi di identificazione ed autenticazione, tuttavia il suo utilizzo in questo senso è limitato al riconoscimento di soggetti precedentemente registrati ed in genere viene utilizzata per il controllo agli accessi del personale autorizzato. Ciò nonostante i nuovi sviluppi tecnologici consentono di utilizzare queste tecnologie per attività volte al controllo ed alla riduzione delle frodi agli sportelli bancari.</p> <p>I sistemi biometrici basati su iride, geometria mano o retina sebbene siano molto precisi risultano essere molto invasivi per gli utenti e dunque in contrasto con gli obiettivi del progetto di creare una filiale aperta e accogliente</p>

Tecnologie di sniffer artificiali	<p>“nasi elettronici” o “sniffer chimici” che rilevano sostanze illecite, polvere da sparo o materiale esplosivo</p> <p><u>In letteratura:</u> (Bonfanti, 2014)</p>
Gesture recognition all'interno della filiale (individuare comportamenti sospetti o traiettorie anomale)	<p>Sistema di apprendimento su rete neurale</p> <p>Per la filiale: Riconoscimento di un set limitato di posture (salto bancone, mani alzate, prese di ostaggi, persone a terr, etc.)</p> <p>In letteratura: (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010). Sistema di videosorveglianza intelligente capace di rilevare comportamenti e traiettorie anomale. Al fine di analizzare le traiettorie per il comportamento di interesse, l'atrio della banca è stato suddiviso in diverse aree, in particolare zona periferica, zona bancone, zona tavolo; la restante superficie è stata definita come area aperta. Se una persona è in piedi all'interno di una zona designata, la persona è contrassegnata come operativo. Le persone nella zona aperta possono essere in fila, in piedi o in movimento. Per determinare se una persona è in coda viene definito un raggio di azione. Una persona è contrassegnata come "in coda", se un'altra persona all'interno di questo raggio di azione è a sua volta in coda o si trova allo sportello (o utilizza l'ATM).</p>
Gesture recognition per ATM	<p>Per atm: Riconoscimento di un set limitato di posture (piede di porco in mano, etc.)</p> <p>In letteratura: (Blauensteiner, Kampel, Musik, & Vogtenhuber, 2010) Comportamento sospetto all'interno o nei pressi dell'Atm (ad es. utente che entra senza effettuare operazioni; vagare nella filiale senza utilizzare l'ATM o contattare un membro del personale per un periodo di tempo prolungato; Interagire con l'ATM per un periodo di tempo insolito oppure presenza di più persone contemporaneamente nei pressi di un ATM. Movimenti repentini nei pressi di un ATM). In caso di comportamento anomalo viene segnalato un warning ad una centrale operativa.</p>
Atm con fingerprint e One time Password	<p>Quando il cliente immette la propria carta all'interno dell'ATM deve posizionare il dito sul modulo fingerprint, per poi ottenere automaticamente un codice a 4 cifre generato ogni volta attraverso un modem GSM collegato al microcontrollore ed inviato come messaggio al cellulare del cliente. Il codice deve essere inserito dal cliente premendo i tasti sul touchscreen, e solo dopo egli sarà in grado di svolgere ulteriori azioni.</p>

	Letteratura: (Jaiswal & Bartere, 2014)
Caricamento variabile ATM	Caricamento degli ATM temporizzato o effettuato in base al tasso di riempimento dell'ATM
Riconoscimento volumetrico	Il sistema è in grado di rilevare la modifica dell'ambiente (ad esempio presenza di valigetta esplosiva, bomboletta di gas, etc.) o della geometria dell'ATM (per rilevare presenza di skimmer, false tastiere, microtelecamere, ecc.)
Riconoscimento manomissione	Sensori di contatto su pannello e intero bancomat. Trasmettitore/ricevitore infrarossi che scatta quando viene introdotto un corpo estraneo (ad esempio forcina nella bocchetta erogatrice). Alla rilevazione il sistema può reagire in due modi: <ol style="list-style-type: none"> 1. Contatta vigilanza 2. Si posiziona su out-of-service

Tabella 39. Descrizione tecnologie di protezione

4.5 Fase 4: Definizione del modello di rischio di Filiale

Le contromisure sono state clusterizzate in 5 livelli di sicurezza. A ciascuna contromisura è stato associate un grado di rilevanza rispetto alla coppia “minaccia – asset”. Ad ogni controllo di sicurezza è stato poi associato un grado di rilevanza in funzione di ogni coppia minaccia-asset. Tale valore corrisponde all'efficacia che lo specifico controllo ha sia rispetto alla coppia minaccia-asset sia rispetto alla combinazione con altri controlli efficaci sulla medesima coppia minaccia-asset. A ciascuna graduazione dei controlli di sicurezza è stato possibile associare un costo medio mensile che ha permesso di effettuare un'analisi dei costi-benefici puntuale delle contromisure da introdurre nelle attività di trattamento del rischio.

Le banche, generalmente rendono il processo di trattamento del rischio più efficiente organizzando le contromisure disponibili in una serie di Configurazioni Minime di Sicurezza da mettere in campo rapidamente in funzione dell'indice di rischio misurato per l'agenzia. Tali Configurazioni Minime dovranno consentire di ottenere un rischio residuo accettabile da migliorare, solo se necessario, con ulteriori interventi correttivi puntuali.

Successivamente sono stati stimati gli impatti conseguenti ad un evento criminoso e infine è stato possibile definire un modello in grado di valutare il rischio complessivo. Per la determinazione del rischio complessivo sono state stimate le vulnerabilità, le minacce e l'indice di rischio.

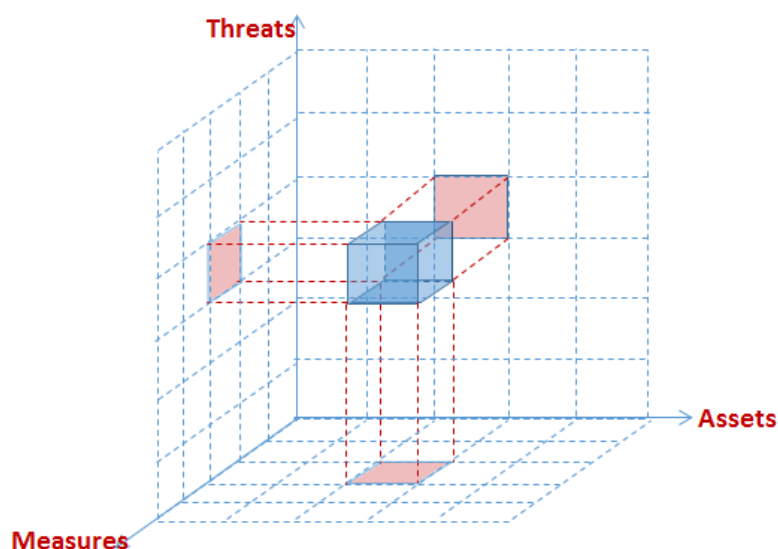


Figura 72. La tripla Minaccia, Asset, Contromisura

Per ciascuna minaccia presa in esame, le tabelle seguenti riportano inoltre le relazioni individuate con gli asset e i controlli di sicurezza e le valorizzazioni stimate delle rispettive rilevanze.

Il significato attribuito ai 5 livelli di *Rilevanza* è il seguente:

1. *Marginale*
2. *Poco Influyente*
3. *Influente*
4. *Rilevante*
5. *Determinante*

L'attribuzione di questi livelli di rilevanza è stata effettuata in maniera qualitativa all'interno del focus group, confrontandoci con gli esperti di sicurezza e tenendo conto delle analisi delle serie storiche dei reati nei confronti delle dipendenze bancarie. Un esempio di attribuzione dei livelli di rilevanza nei confronti del rischio rapina è riportato nella seguente tabella.

Rapina		
Asset	Controllo	Rilevanza
Persone	Ubicazione dell'immobile	3
	Raggiungibilità dell'immobile	3
	Distanza degli insediamenti delle FF.OO.	3
	Ubicazione dell'agenzia	3
	Locali confinanti con l'agenzia	3

Rapina		
Asset	Controllo	Rilevanza
	Sistema di accesso	5
	Spazi aperti confinanti con l'agenzia	1
	Cunicoli/intercapedini confinanti con l'agenzia	2
	Misure di protezione contanti per le Casse Interne	4
	Misure di protezione perimetrale specifiche per i mezzi forti (e.g. Locale Tecnico di Sicurezza)	4
	Servizio di piantonamento	5
	Rilevatori antintrusione perimetrale dell'impianto di allarme	4
	Servizio di ispezione/verifica	5
	Impianto di allarme	4
	Altri accessi all'agenzia	4
	Prestazioni degli impianti di sicurezza installati	2
	Obsolescenza degli impianti di sicurezza installati	2
	Impianto di videosorveglianza	5
	Attuazione delle norme comportamentali	4
	Strumenti di sensibilizzazione relativi alle norme comportamentali da rispettare	3
	Fruizione delle attività formative sulle misure di sicurezza previste	3
	Strumenti per la raccolta delle segnalazioni finalizzate al miglioramento continuo delle norme comportamentali in vigore	3
Cassa Contanti	Ubicazione dell'immobile	3
	Raggiungibilità dell'immobile	3
	Distanza degli insediamenti delle FF.OO.	3
	Ubicazione dell'agenzia	4
	Locali confinanti con l'agenzia	4
	Cunicoli/intercapedini confinanti con l'agenzia	4
	Spazi aperti confinanti con l'agenzia	1

Rapina		
Asset	Controllo	Rilevanza
	Altri accessi all'agenzia	4
	Numerosità delle Casse Interne	3
	Misure di protezione contanti per le Casse Interne	5
	Numerosità dei mezzi forti per il ricovero dei valori	4
	Misure di protezione perimetrale specifiche per i mezzi forti (e.g. Locale Tecnico di Sicurezza)	5
	Misure di protezione aggiuntive per i mezzi forti	4
	Servizio di piantonamento	5
	Servizio di ispezione/verifica	4
	Sistema di accesso	5
	Impianto di videosorveglianza	5
	Impianto di allarme	4
	Rilevatori antintrusione perimetrale dell'impianto di allarme	4
	Sistema di rilevazione permanenza nei locali dell'agenzia	4
	Prestazioni degli impianti di sicurezza installati	4
	Obsolescenza degli impianti di sicurezza installati	3
	Attuazione delle norme comportamentali	4
	Strumenti di sensibilizzazione relativi alle norme comportamentali da rispettare	3
	Fruizione delle attività formative sulle misure di sicurezza previste	3

Tabella 40. Esempio Tabelle di rilevanza

Alcuni controlli di sicurezza si caratterizzano per un effetto deterrente particolarmente efficace nei confronti delle *condizioni contestuali degli eventi criminosi*. In particolare, alcuni controlli di sicurezza come:

- **Ubicazione dell’Agenzia,**
- **Servizio di piantonamento,**
- **Impianto di videosorveglianza,**

si caratterizzano per la capacità di indurre, per agenzie interne (a centri commerciali, ministeri, etc.) e per alcune specifiche graduazioni, un livello di sicurezza aggiuntivo su altri controlli di sicurezza. Associando un *Costo Medio Mensile* (ordine di costo) a ciascuna graduazione dei controlli di sicurezza sarà possibile effettuare un'analisi costi-benefici puntuale delle contromisure da introdurre nelle attività di trattamento del rischio. La figura seguente riporta inoltre una mappatura di esempio tra *Configurazioni Minime di Sicurezza* e *Controlli di Sicurezza*.

CONFIGURAZIONI MINIME DI SICUREZZA	MISURE MINIME PREVISTE	COD CONTROLLO	NOME CONTROLLO	GRADUAZIONE
Configurazione BASE	Sliding door	C20	Sistema di accesso	1
	Roller Cash	C10	Misure di protezione contanti per le Casse Interne	4
	VDS	C21	Impianto di videosorveglianza	>=3
Configurazione A	Bussole (MD non attivo)	C20	Sistema di accesso	2
	Roller Cash	C10	Misure di protezione contanti per le Casse Interne	4
	VDS	C21	Impianto di videosorveglianza	>=3
Configurazione B	Bussole (MD non attivo)	C20	Sistema di accesso	4
	Roller Cash	C10	Misure di protezione contanti per le Casse Interne	4
	VDS	C21	Impianto di videosorveglianza	>=3
Configurazione C	Bussole (MD non attivo)	C20	Sistema di accesso	2
	Roller Cash	C10	Misure di protezione contanti per le Casse Interne	4
	Vigilanza	C18	Servizio di piantonamento	>=2

Configurazione D	Bussole (MD non attivo)	C20	Sistema di accesso	4
	Roller Cash	C10	Misure di protezione contanti per le Casse Interne	4
	VDS	C21	Impianto di videosorveglianza	3
	Vigilanza	C18	Servizio di piantonamento	>=2

Tabella 41. Mappatura di esempio tra Configurazioni Minime di Sicurezza e Controlli di Sicurezza.

CAPITOLO 5: Una proposta risolutiva per la reingegnerizzazione della gestione della sicurezza nelle dipendenze bancarie

5.1 Elementi per la reingegnerizzazione della gestione della sicurezza nelle filiali bancarie.

Sulla base dei risultati emersi dall'analisi della situazione attuale, si evince che non è possibile prevedere con sufficiente accuratezza il comportamento a rischio di evoluzione negativa del potenziale malvivente. L'analisi della letteratura infatti non ci consente di stabilire il modus operandi tipico di chi compie un'azione ai danni di una dipendenza bancaria. Avere conoscenza del comportamento complessivo del malvivente avrebbe consentito di introdurre una serie di barriere, anche fisiche, atte a limitare l'azione del criminale, al fine di ostacolarne i movimenti. In ogni caso, considerando che i movimenti sono molto dinamici, anche qualora si introducessero delle barriere di carattere fisico, sarebbero comunque by-passabili, perché il malvivente potrebbe cambiare strategia di attacco, prendendo atto di quelle barriere. Pertanto, secondo un punto di vista infrastrutturale, non è possibile stabilire un layout "sicuro" per la filiale che sia, da un lato fruibile dal cliente (ovvero coniughi gli aspetti di sicurezza della dipendenza bancaria con l'accessibilità, la rapidità, ed il senso di sicurezza e tranquillità richiesto dal cliente che si reca fisicamente presso la filiale) mentre dall'altro non si evincono elementi sufficienti per proporre nuove soluzioni infrastrutturali atte a preservare la safety e la security della Dipendenza Bancaria. Tali soluzioni infrastrutturali potrebbero infatti essere, oltre che invasive, di dubbia efficacia. Come meglio specificato in precedenza, è infatti necessario andare incontro alle esigenze commerciali delle banche, le cui funzioni di marketing spingono per rendere gli sportelli bancari sempre più simili alle altre attività commerciali. In tal senso, le dipendenze bancarie si stanno man mano alleggerendo da soluzioni infrastrutturali passive (quali ad esempio inferriate e vetri antiproiettili) in quanto in contrasto con le esigenze di immagini aziendale e con le percezioni dei dipendenti e dei clienti (che si sentono letteralmente "chiusi in gabbia").

Dallo studio della letteratura scientifica, emerge che è molto più efficace concentrarsi non sul comportamento complessivo (ovvero il modus operandi) ma sulle singole azioni intraprese dall'individuo. Sono stati pertanto individuati degli strumenti di carattere tecnologico ed organizzativo che consentono da un lato di prevenire l'azione delinquenziale (attraverso meccanismi di dissuasione psicologica) e dall'altro di reagire prontamente nel momento in cui il malvivente entra in azione.

Quindi, sebbene il processo di reingegnerizzazione andrebbe portato avanti sulle dimensioni infrastrutturali, tecnologiche ed organizzative, si può affermare che nel caso in esame risulta

efficace intervenire sugli aspetti tecnologici ed organizzativi, mentre risulta essere poco efficiente e costoso intervenire su quelli infrastrutturali.

Pertanto, il modello reingegnerizzato di filiale si compone sia di indicazioni a carattere organizzativo che tecnologico, aspetti che dovranno fondersi nella piattaforma di controllo. Il Modello Reingegnerizzato della filiale prevede dunque:

- a) **Usa di una Piattaforma di controllo.** La piattaforma di controllo è un'architettura modulare, flessibile ed estensibile. Queste caratteristiche si sono rese necessarie affinché le attività di manutenzione e sviluppo di server e software si possano eseguire in maniera semplice.

L'architettura software è di tipo multi tier ed è fruibile tramite rete internet. Inoltre affinché ciascun operatore possa intervenire con le proprie competenze, qualora lo si renda necessario, è stata predisposta una piattaforma. Questa piattaforma consente agli operatori di condividere le conoscenze di ciascuno e renderle sovrapponibili

Tali caratteristiche verranno meglio definite nei prossimi paragrafi.

- b) **Accorgimenti Organizzativi**

- a. Dissuasori psicologici (ad esempio l'utilizzo di vetri trasparenti): La presenza di vetrate trasparenti risulta essere un buon dissuasore: La visibilità, come affermato nel capitolo 3, rende il potenziale autore di reato maggiormente a rischio rispetto al contesto circostante in cui decide di agire, nonché rispetto alla presenza di "guardiani capaci". Si afferma sempre più l'idea che la trasparenza delle vetrate delle filiali sia una componente fondamentale della diminuzione del rischio rapina, in accordo anche con le Forze dell'ordine. Il focus dell'analisi è che il potenziale autore di reato, nel suo processo decisionale (ammesso che egli sia un autore professionista), prenderà fortemente in considerazione il fatto di essere visto dall'esterno dei locali delle banche. Ecco che si inizia a parlare di sorveglianza naturale (o informale o di vicinato) come strumento di deterrenza.
- b. Caricamento bancomat: Un altro accorgimento organizzativo riguarda il caricamento dell'Atm. È stata osservata un'elevata concentrazione di eventi criminosi in prossimità del fine settimana. I criminali infatti sanno che le dipendenze bancarie, per far fronte alle giornate di chiusura nel fine settimana, caricano gli atm con un quantitativo di contante superiore rispetto ai giorni feriali. Questa considerazione ha portato a proporre una misura organizzativa volta a minimizzare il numero di attacchi all'atm durante il fine settimana: **Caricamento intelligente ATM**. In questo modo l'atm non verrà caricato il venerdì con un elevato importo per poter far fronte ai due giorni non lavorativi, ma verrà incaricata una persona che si occuperà di ricaricare la macchina ogni qualvolta venga superata la soglia limite. Si tratta,

dunque, di gestire il carico degli ATM in funzione del tasso di svuotamento degli stessi o sulla base, comunque, di modelli predittivi finalizzati a minimizzare i depositi inutilizzati di denaro.

- c. Formazione del personale: risulta essere una misura organizzativa estremamente importante. Non è facile conoscere in anticipo le azioni del rapinatore, soprattutto in caso di imprevisti. Ma ancor meno facile è prevedere le reazioni di coloro che subiscono la minaccia diretta dei banditi. Non è realizzabile un'azione preventiva davvero efficace sul cliente. Irrrinunciabile è, quindi, la sensibilizzazione del personale in ordine alle condotte da tenere affinché la rapina si concluda in tempi brevi e, soprattutto, senza gravi conseguenze. È importante perciò sottolineare il ruolo attivo del dipendente a tutela della sicurezza propria e altrui. Tale ruolo va inteso esclusivamente in termini di consapevolezza e adozione di comportamenti cautelativi; è da escludersi ogni resistenza attiva nei confronti dei rapinatori, poiché la principale preoccupazione degli istituti di credito è e resta la salvaguardia dell'integrità fisica del personale e dei clienti. La formazione anticrimine è importante perché i contenuti vertono sui comportamenti da adottare non solo nel momento in cui la rapina è in corso, ma anche prima e dopo il verificarsi di un evento criminoso.
- c) Nuova gestione del controllo della sicurezza (modello di controllo centralizzato). Come già precedentemente discusso la centralizzazione delle attività consentirebbe di liberare gli addetti alle attività di controllo da compiti operativi che potrebbero risultare alienanti. Inoltre consentirebbe di ridurre il numero di organico e questo si tradurrebbe in una diminuzione dei costi della sicurezza.
- d) Adozione di misure tecnologiche a carattere preventivo e reattivo

5.2 Le dipendenze bancarie secondo una prospettiva di Cyber Physical Space

Le filiali bancarie sono spazi fisici che, tradizionalmente, rappresentano il punto di incontro tra le banche e i loro clienti. Negli ultimi anni, l'industria bancaria si trova ad affrontare un panorama competitivo in rapido cambiamento che sta mettendo pressione alla rilevanza e alla futura redditività delle banche tradizionali. Le filiali stanno gradualmente modificando il loro aspetto: da luoghi in cui i clienti solitamente si recano per effettuare transazioni economiche, come depositi, pagamenti e prelievi, a spazi aperti in cui i clienti possono sperimentare accoglienza.

Le filiali bancarie stanno diventando punti vendita commerciali dove consulenti professionali offrono prodotti finanziari diversificati e complessi. In questi posti i consulenti bancari possono gestire relazioni con i clienti per vendere portafogli articolati di prodotti effettuando strategie di marketing cross-selling e up-selling.

Allo stesso tempo, le transazioni economiche si spostano dallo sportello bancario alle piattaforme controllate a distanza, normalmente collocate vicino la filiale (bancomat) o accessibili via web (Internet / mobile banking). Per facilitare questa trasformazione, anche il layout e la struttura della filiale stanno cambiando. In particolare, le misure di sicurezza tradizionali definite "hard measures" (finestre blindate, guardie armate, metal detectors, telecamere di sicurezza visibili, ecc.) verranno rimossi dalla vista dei clienti.

Sebbene queste misure siano importanti per garantire la protezione delle strutture e delle persone, esse provocano nei clienti un senso di ansietà e generano una cattiva sensazione di pericolo imminente che porta le persone ad evitare di entrare nella filiale o starvi all'interno il più breve tempo possibile. Sfortunatamente, l'obiettivo di ridurre il senso di ansietà si scontra con il bisogno di garantire la protezione delle persone e delle proprietà presenti all'interno della filiale.

Sfruttando le potenzialità dell'Internet of Things, ci proponiamo di rimodellare le filiali bancarie come un CPSS in grado di realizzare un ambiente più confortevole e più sicuro per i clienti e i dipendenti, e in grado di proteggere anche le attività fisiche della filiale.

Qui di seguito, proponiamo un framework per modellare i processi di safety e security in una filiale bancaria. Da un punto di vista della protezione fisica, le filiali bancarie subiscono costantemente minacce di attacchi criminali. Un attacco criminale può essere considerato come una sequenza di azioni che si verificano in uno spazio di interazione, con lo scopo di ottenere un beneficio ingiusto e/o provocare un danno alle persone o alle organizzazioni. Rielaborando il modello descrittivo proposto da Volpentesta (2015) per la descrizione dei processi di interazione all'interno di uno smart environment, di seguito definiamo e discutiamo gli elementi che riguardano la safety e la security delle filiali bancarie:

- **Persone**: *Esseri umani che sono entrati in un vero e proprio ambiente fisico. A seconda del ruolo possiamo identificare i seguenti tre tipi di attori in questa categoria:*
 - *Cliente: è una persona che utilizza uno o più dei servizi forniti dalla banca.*
 - *Dipendente: è una persona che lavora per un'istituzione bancaria sotto un contratto di lavoro.*
 - *Attaccante: è una persona che svolge un'azione penalmente rilevante (reato) per ottenere un beneficio improprio e per danneggiare qualcuno o qualcosa*
- **Minaccia**: *Un evento negativo potenziale contro una filiale bancaria. Identifichiamo i seguenti tipi di minacce:*
 - *rapina: rubare da una banca mentre i dipendenti e i clienti bancari sono sottoposti a violenza o minacce di violenza, insinuando la paura nella vittima.*
 - *Furto: l'appropriazione indebita della proprietà altrui.*
 - *Frode: è l'uso di mezzi potenzialmente illegali per ottenere denaro, beni o altre proprietà possedute o detenute da un'istituzione bancaria.*
 - *Danno: un danno intenzionale o non intenzionale alla proprietà di qualcuno.*

- Asset bancari: l'insieme di beni materiali e immateriali a rischio di attacchi criminali. Abbiamo identificato i seguenti asset di una filiale bancaria: clienti, dipendenti, contanti, ATM, competitività commerciale, immagine, beni fisici, cassaforte.
- Armi: qualsiasi dispositivo utilizzato con l'intento di procurare danni o minacciare persone, strutture o sistemi
- Sistemi di safety e security: l'insieme di tecnologie, strumenti e procedure organizzative in grado di prevenire o reagire a una minaccia contro una filiale bancaria. Possono essere classificati in:
 - Sistemi tradizionali: misure statiche volte a prevenire/ostacolare i danni agli asset bancari scoraggiando i potenziali criminali a compiere l'attacco. Due tipologie appartengono a questa categoria: le misure tradizionali dette "hard" (misure strutturali quali finestre blindate, guardie armate, porte blindate, porte di chiusura temporanea) e misure "soft" (misure psicologiche come vetri trasparenti; controlli di sicurezza) (Conrath, 1999).
 - sistemi basati su IoT: oggetti intelligenti che sfruttano le funzionalità dell'IoT per fornire servizi di security e safety. Questi sistemi richiedono l'attivazione (automatica o guidata dall'uomo) di una contromisura a seguito di un evento rischioso (Baker 2012). Il riconoscimento dell'evento si basa su sensori che consentono alle persone di interagire con la banca o di attivare procedure di protezione (Bhalthilak et al., 2014). Tali sistemi sono basati su interazioni uomo-macchina o macchina-macchina
- Piattaforme ICT: l'hardware di base, le reti e il software utilizzati per fornire servizi IT in una filiale bancaria e per gestire i sistemi di sicurezza basati su IoT.
 Le persone, gli asset bancari, le piattaforme ICT e i sistemi di sicurezza basati sull' IoT, nonché le interazioni tra questi elementi, costituiscono le componenti fondamentali per la creazione di un CPS all'interno di una dipendenza bancaria. In generale, un'interazione è definita come l'evento nel corso del quale due o più entità comunicano o reagiscono reciprocamente, implicando una modifica dello stato di un'entità. In generale, lo stato di un'entità può essere modellato attraverso i seguenti elementi:
 - Identità: si riferisce a un sottoinsieme di elementi che non variano nel tempo e caratterizzano un gruppo di entità (ad es. Clienti, denaro, bancomat) o più specificamente un'unica entità in un ambiente intelligente (ad esempio chi è la persona, il PIN della carta ATM).
 - posizione: questa voce si riferisce alla posizione di ciascuna entità all'interno della dipendenza bancaria. Questo stato dell'oggetto può essere determinato utilizzando la posizione assoluta o una posizione relativa a un punto fisso nello smart environment.

- Distanza: posizione relativa tra due entità all'interno di una dipendenza bancaria.
- movimento: cambiamenti della posizione dell'entità (o parte di esso) rispetto al tempo. Il loro stato può essere rappresentato da una sequenza di valori parametrici che descrivono l'entità che si muove attraverso la filiale bancaria (ad esempio sequenza di posizioni, direzione, velocità, accelerazione).

All'interno di una dipendenza bancaria, le interazioni tra le persone e gli asset possono essere rilevate, interpretate e mediate attraverso sistemi di sicurezza basati sull'Internet of things. Ogni azione influenza lo stato delle entità all'interno dello smart environment. In alcuni casi, un sottoinsieme di azioni eseguite dagli esseri umani in una filiale bancaria può essere riconosciuto come minaccioso e può innescare una serie di azioni di sicurezza (ad esempio una contromisura) che coinvolge persone (aggressori, clienti, dipendenti), beni fisici, sicurezza e sistemi di sicurezza. Definiamo "*security patterns*" la sequenza di azioni che coinvolgono entità di contesto all'interno di una filiale in seguito alla rilevazione di una minaccia.

5.3 Verso un Intelligent Protection Systems per la gestione della sicurezza di filiale

All'interno di questo lavoro viene proposto una soluzione di IPS basata su una profonda riprogettazione del sistema di monitoraggio. I risultati delle interviste hanno enfatizzato il fatto che rendere "intelligente" un sistema richiede l'acquisto e l'installazione di sensori ed attuatori che spesso si rivelano molto costosi e comunque invasivi (Laput et al., 2015). D'altro canto, l'importanza di rendere più intelligente qualsiasi sistema di protezione è condivisa in letteratura (Augusto, 2007). L'approccio comune per l'aggiornamento di un ambiente in un ambiente intelligente è quello di installare Smart Objects che contengano funzionalità di rilevamento (ad esempio: interruttori di luce) e/o di associare tag e sensori "universali" ad oggetti che non sono "intelligenti" (Amadi-Echendu et al. al., 2017). Il limite risiede nel fatto che la funzionalità di rilevamento è generalmente limitata all'oggetto stesso (ad esempio: un interruttore intelligente sa se è acceso o spento) o quando serve la sua funzione di base (ad esempio, un rilevatore di presenza).

Un sistema di Supervisione e Controllo della sicurezza delle dipendenze bancarie deve consentire di monitorare i dati delle agenzie, di semplificare la manutenzione ordinaria e straordinaria, di gestire l'archiviazione dei dati con il collegamento a pacchetti software e gestionali. Il sistema proposto, può essere visto come una evoluzione naturale dei cosiddetti sistemi PSIM (Physical Security Information Management).

Tale approccio si basa sul concetto che anche i sistemi di sicurezza producono «dati». I dati, opportunamente contestualizzati e correlati, diventano informazioni che presentate in modo strutturato e organizzato aiutano i processi decisionali e aumentano la possibilità di automazione delle reazioni per aiutare operatori ed amministratori nello svolgimento delle

loro funzioni di routine e nei momenti di criticità. La piattaforma si fa carico delle complessità procedurali e operative, automatizza le procedure di routine e interviene nella gestione di eventi critici analizzando la situazione e presentando agli addetti alla sicurezza la visione completa di tutte le componenti pertinenti alla situazione in corso.

I PSIM inoltre, per loro natura, raggiungeranno una utenza operativa più vasta e variegata degli attuali sistemi PSIM. Infatti, molti dipartimenti di un gruppo bancario potranno essere interessati alle informazioni raccolte dallo PSIM e in esso disponibili. Questo impone la necessità di predisporre interfacce utente sempre più ergonomiche e semplici, personalizzabili per tipologia di utente o per singoli specifici utenti.

L'analisi effettuata applica alla sicurezza fisica concetti di information management e business intelligence traendo il massimo vantaggio dalla convergenza dei sistemi sicurezza verso l'utilizzo esclusivo di tecnologie ICT. La convergenza ICT, oltre a costituire fonte di ottimizzazioni in sé, permette l'analisi in tempo reale di una grande quantità di informazioni. Questo consente di implementare un approccio "olistico" alla sicurezza dove l'intero sistema è interpretato come un organismo nel quale le funzionalità disponibili sono maggiori e migliori della somma delle funzionalità dei singoli sottosistemi.

Esistono da anni sul mercato sistemi di supervisione che integrano diverse applicazioni nell'ambito dei sistemi di sicurezza fisica attiva. Storicamente questi sistemi sono stati sviluppati sulla base di tre diverse logiche, dipendenti dal tipo di azienda produttrice:

- Sistemi composti da hardware e software proprietari, nati per fidelizzare il cliente finale sulle proprie soluzioni, poco adatti alla integrazione di componenti prodotti da terze parti. Questa configurazione è caratterizzata da un forte lock-in nei confronti di un fornitore, *scarsamente flessibile e disponibile all'integrazione di hw di terze parti;*
- Sistemi basati su un software di supervisione predisposto alla integrazione di hardware e sottosistemi di terze parti, ma che richiedono attività di configurazione e startup spesso lunghe e costose. La soluzione si caratterizza per *complessità di installazione/configurazione che comporta maggiori costi di attivazione dell'impianto e necessità dell'intervento del fornitore ad ogni richiesta di variazione delle configurazioni.*
- Sistemi di supervisione progettati da aziende produttrici di uno dei tipici sottosistemi di sicurezza (controllo accessi, anti intrusione, videosorveglianza, etc) che integrano nel proprio software i sottosistemi "non core" prodotti da aziende terze. In questo caso, *la gestione del sottosistema della azienda produttrice è spesso di buon livello, ma risulta carente la gestione degli altri sottosistemi di sicurezza.*

Lo studio proposto appartiene ad un segmento di mercato relativamente nuovo, al quale viene attribuita una forte potenzialità di crescita, grazie alle interazioni tra la videosorveglianza, il controllo accessi, l'antintrusione, il rilevamento incendi, la

manomissione e le nuove tecnologie dominanti nel mercato della sicurezza fisica. L'integrazione tra sotto-sistemi eterogenei consente di raccogliere e correlare gli eventi provenienti dai diversi dispositivi esistenti, di sicurezza e non, per aumentare in modo proattivo le capacità del personale a identificare e risolvere le situazioni.

La convergenza "sicurezza – tecnologia – organizzazione" mette enfasi sull'importanza del fatto che tutti coloro che sono coinvolti, nelle diverse funzioni, siano in grado di lavorare tutti insieme in modo collaborativo, per ridurre il livello di rischio. È proprio questo il paradigma alla base del disegno della piattaforma integrata: l'uomo è al centro e la sua intelligenza consente di prevenire e gestire in maniera ottimale le minacce, mantenendo la coerenza con le regole e i processi dell'organizzazione e con il supporto delle tecnologie che ne estendono le capacità d'azione. La piattaforma non si basa più sull'accesso separato a diverse fonti informative fornite da diversi sistemi con un basso livello di integrazione, ma gestisce informazioni provenienti da fonti eterogenee e integrate in un unico modello operativo, inserito all'interno delle procedure e delle regole aziendali, realizzando un obiettivo di sicurezza estesa e integrata a copertura di un perimetro completo e definito. La sala di controllo evolve quindi verso il concetto di centro di comando e controllo, che opera le funzioni di monitoraggio della sorveglianza, di controllo e gestione degli allarmi, di dispacciamento delle attività e di coordinamento centralizzato di tutte le risorse sul campo. L'approccio è da "System Integrator" tramite un framework applicativo e tecnologico da utilizzare come acceleratore progettuale non solo nella fase di realizzazione ed installazione dell'impianto ma atto a gestirne le evoluzioni durante l'intera vita dello stesso. La piattaforma di controllo "indipendente" e non dello specifico produttore della tecnologia adottata non vincola all'utilizzo di quel particolare sensore ed il sistema potrà evolvere andando ad integrare soluzioni a seconda delle esigenze che si possono venire a creare.

L'analisi finora effettuata rispetta quei vincoli definiti dall'indagine dell'IMS Research IMS/IHS e Frost & Sullivan negli USA nel 2010, che sancisce definitivamente la digitalizzazione della sicurezza fisica e l'apertura architettuale dei sistemi come valore aggiunto essenziale, che si è tradotta in sintesi in 7 requisiti che permettono di distinguere un PSIM da una comune piattaforma software di supervisione:

- **Connettività e integrazione:** ricezione di dati da un numero qualsiasi di apparati o sistemi di sicurezza; capacità di integrazione sia nell'ambito della sicurezza fisica che rispetto ad altri sistemi di gestione dell'azienda (sia nei siti periferici che nell'interazione tra essi e il sistema centrale)
- **Gestione Real Time e configurazione controllata:** possibilità di configurare e modificare dal centro di controllo procedure e parametri a bordo dei vari sistemi e

dispositivi in ogni livello della infrastruttura (antintrusione, controllo accessi, videosorveglianza, ecc.)

- **Correlazioni e Verifiche:** connessione automatica centro-periferia e correlazioni multiple tra diversi apparati per la sicurezza; verifiche real-time e gestione flessibile delle interazioni correlate.
- **Visualizzazione:** in caso di evento il PSIM deve essere in grado di visualizzare graficamente informazioni sulla situazione in modo da dare a chi deve gestire l'evento un'idea anche complessiva della natura dell'evento, del contesto locale e dell'ampiezza della minaccia.
- **Processi di gestione eventi basati su procedure guidate:** avvio immediato dell'operatore su un percorso guidato passo-passo, basato su procedure mirate al contenimento o al contrasto della minaccia, monitorizzando progressivamente l'esito delle attività svolte sul posto.
- **Affidabilità e Resistenza:** caratteristiche di robustezza e ripristino della piattaforma di sistema per ogni modulo ed a tutti i livelli, per assicurare la continuità del servizio e il ritorno alla normalità della gestione sia in caso di guasto parziale che di disastro totale.
- **Reportistica e Riesame post-evento:** tracciabilità e verbalizzazione documentata della gestione dell'evento anche ai fini della ricostruzione criminologica dell'accaduto e della sua gestione.

5.3.1 L'utilizzo di Synthetic Sensors per la trasformazione della filiale in "ambiente intelligente"

Questa ricerca propone un modello di un Intelligent Protection System (IPS) progettato per ottimizzare la sicurezza e migliorare le prestazioni del processo di gestione della sicurezza delle dipendenze bancarie. Il modello si basa sulla reingegnerizzazione del processo di gestione della sicurezza delle dipendenze bancarie in corso e la caratterizzazione del Cyber Physical System (CPS) sottostante. La leva per il reengineering è dunque l'utilizzo delle tecnologie IoT, la cui adozione può supportare la trasformazione delle filiali in ambienti intelligenti.

L'importanza di rendere più intelligente qualsiasi sistema di protezione è ampiamente condivisa in letteratura (Augusto, 2007). Tuttavia, sia la letteratura che le interviste effettuate nel corso del focus group enfatizzano il fatto che rendere "intelligente" un sistema richiede l'acquisto e l'installazione di sensori ed attuatori si può rivelare molto costoso e comunque invasivo (Laput et al., 2015).

Diversi sono gli approcci da utilizzare per dotare di intelligenza l'ambiente che ci circonda. Sulla base del numero di sfaccettature distinte rilevate (ad es. stati, eventi) e del numero di sensori necessari per ottenere questo risultato, si possono identificare le seguenti categorie di sensori (Laput, 2017):

- **Special-Purpose Sensors:** La forma più intuitiva e prevalente del sensing è quella di utilizzare un singolo sensore per monitorare un singolo aspetto di un ambiente. Questa tipologia di sensori è caratterizzata da una particolare robustezza per problemi di rilevamento ben definiti, come ad esempio sensori di occupazione di un ambiente e sistemi di apertura automatica delle porte. Ad esempio, un sensore di occupazione può rilevare solo l'occupazione e un sensore di apertura della porta può rilevare solo quando una porta è aperta. Non esiste una nozione di generalità; ogni aspetto viene monitorato da un sensore specifico e indipendente.
- **Distributed Sensing Systems:** Un'altra soluzione può riguardare anche la possibilità di inserire molti sensori in un ambiente, che possono essere collegati in rete, formando un sistema di rilevazione distribuito. Questo approccio può essere utilizzato per rendere più ampia l'area di rilevazione (ad esempio, rilevamento di occupazione attraverso un intero magazzino) o aumentare la qualità della rilevazione attraverso letture complementari. I sensori distribuiti possono essere omogenei (ad esempio una serie di sensori di occupazione ad infrarossi identici) o eterogenei (cioè un mix di tipi di sensori). Un sistema di security è un esempio classico di sistema distribuito eterogeneo, in cui sensori di porte, sensori di finestre, sensori di rumore, sensori di occupazione e persino telecamere lavorano insieme per una singola classificazione di evento: c'è un intruso? Questo è un esempio di sistema distribuito di tipo molti-a-uno, e quindi occupa la parte inferiore destra della tassonomia. Di converso, un sistema di rilevazione delle interazioni tra gli oggetti di un'ambiente attuato da numerosi sensori, è classificabile come un sistema di sensoristica distribuito di tipo molti a molti (Tapia et al, 2004). Quindi, i sistemi distribuiti occupano l'intero lato destro della Figura. Un sistema di rilevamento distribuito, come ci si potrebbe aspettare, dipende in larga misura dalla qualità della distribuzione del sensore. Raggiungere la saturazione del sensore necessaria implica spesso una distribuzione considerevole, forse dozzine di sensori anche per un piccolo contesto. Questo può essere costoso; con sensori che costano spesso \$ 30 o più, anche le piccole installazioni possono diventare onerose. Inoltre, con la crescita del numero di sensori, c'è il pericolo di diventare invasivi contesti sensibili, come potrebbe essere una dipendenza bancaria.
- **Infrastructure-Mediated Sensing:** al fine di ridurre i costi di installazione e l'invasività dei sistemi distribuiti, diverse ricerche hanno esaminato la possibilità di implementare reti di sensori basati su un infrastruttura di rete già disponibile. Un tipico esempio è rappresentato dalle tecnologie "power line" per far comunicare tra di loro i sensori. Ad esempio, in Felicetti et al., (2015), viene presentato un sistema per l'efficienza energetica in ambienti domestici basato su sensori infrastructure-mediated.

Sebbene sia molto più generale degli altri approcci già discussi, questo approccio è ancora vincolato dalla classe di infrastrutture con cui è accoppiata. Ad esempio, in un ambiente domestico, un sensore con attacco idraulico può rilevare l'uso del lavandino, della doccia, ma non l'utilizzo del forno a microonde.

Molti dei suddetti sistemi utilizzano il sensing diretto, cioè un sensore che fisicamente si accoppia ad un oggetto o un'infrastruttura di interesse. Questo approccio è popolare in quanto generalmente produce un'eccellente qualità del segnale. Tuttavia, l'alimentazione di tali sensori può risultare problematica, poiché la maggior parte degli oggetti non dispone di prese di corrente (prendiamo ad esempio un sensore di apertura di una finestra). Perciò, tali sistemi si possono basare su batterie che devono essere periodicamente ricaricate/sostituite, oppure richiedono la connessione alla rete elettrica (anche se questo limita le posizioni dei sensori possibili o richiede che i cavi vengano installati nell'ambiente). Fortunatamente, è anche possibile "sensare" lo stato e gli eventi indirettamente, senza dover fisicamente accoppiarsi agli oggetti. Per esempio, in Kim et al. (2009) viene esplorato il rilevamento dell'utilizzo dell'apparecchio con un sensore installato nelle vicinanze. Prendiamo in esempio un frigorifero: quando l'apparecchio è in diverse modalità di funzionamento (ad es., il compressore frigorifero in funzione, le luci interne accese / spengono) emette disturbi elettromagnetici differenti che possono essere acquisiti e riconosciuti. In Ward et al. (2006), vengono utilizzati sensori acustici per riconoscere l'utilizzo di utensili in un impianto.

Nel complesso, il sensing indiretto consente una maggiore flessibilità nel posizionamento, spesso consentendo ai sensori di essere meglio integrati nell'ambiente o addirittura nascosti e quindi meno invadenti. Tuttavia, questo si ripercuote sulla qualità di rilevazione del segnale: più ci si allontana da un oggetto o da un'area di interesse, tanto più diminuisce la sensibilità dello strumento.

- **General purpose settings:** Sempre più spesso, le "schede" dei dispositivi di rilevazione sono popolate da un'ampia varietà di sensori che garantiscono un uso flessibile. L'approccio ideale di rilevamento occupa la parte superiore sinistra della tassonomia, in cui un sensore può consentire molte sfaccettature sensibili, e più specificatamente, al di là di ogni singolo oggetto strumentato. L'incarnazione definitiva di questo approccio sarebbe un singolo sensore onnisciente in grado di digitalizzare un intero ambiente.

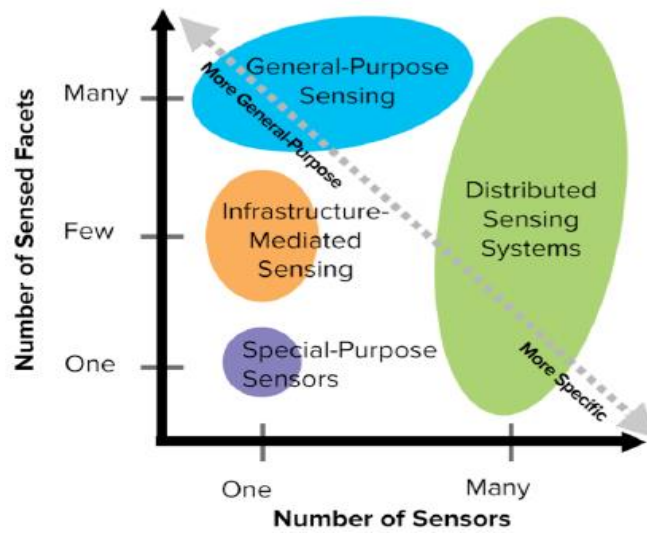


Figura 73. Approcci all'environmental sensing

Una analisi di sensori (commercialmente disponibili o introdotti dalla letteratura scientifica) che offrono diversi gradi di general –purpose sensing è illustrata di seguito.

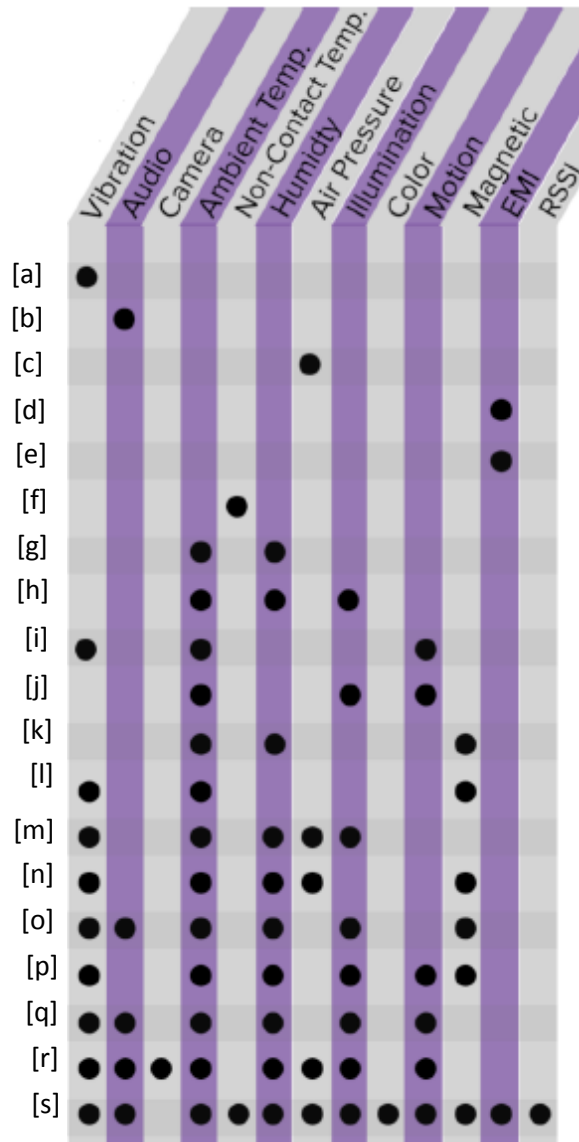


Figura 74. Funzionalità di general purpose sensor disponibili commercialmente o in letteratura

- a. Knocki: Turn Any Surface into a Remote Control. <http://knocki.com/>
- b. Fogarty, J., Au, C., Hudson, S.E.. 2006. Sensing from the basement: a feasibility study of unobtrusive and low-cost home activity recognition. In Proceedings of the 19th annual ACM symposium on User interface software and technology (UIST '06). ACM, New York, NY, USA, 91-100.
- c. Froehlich, J.E., Larson, E., Campbell, T., Haggerty, C., Fogarty, J., Patel, S.N.. 2009. HydroSense:
- d. Gupta, S., Reynolds, M.S., Patel, S.N. 2010. ElectriSense: single-point sensing using EMI for electrical event detection and classification in the home. In Proceedings of the 12th ACM international conference on Ubiquitous computing (UbiComp '10). ACM, New York, NY, USA, 139-148.
- e. Rowe, A., Gupta, V., Rajkumar, R. 2009. Low-power clock synchronization using electromagnetic energy radiating from AC power lines. In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09). ACM, New York, NY, USA, 211-224.
- f. Beltran, A., Erickson, V.L. Cerpa, A.E. 2013. ThermoSense: Occupancy Thermal Based Sensing for HVAC Control. In Proceedings of the 5th ACM Workshop on Embedded Systems For EnergyEfficient Buildings (BuildSys'13). ACM, New York,
- g. EchoFlex: Clean Tech Lighting & Temperature Controls. Last accessed: January 20, 2017. <http://www.echoflexsolutions.com/>

- h. Cao Wireless Sensor Tags: Monitor and Find Everything from the Internet. Last accessed: January 20, 2017. <http://www.caogadgets.com/>
- i. Sen.se Mother. The Universal Monitoring Solution. Last accessed: January 20, 2017. <https://sen.se/mother/>
- j. Fails, J., Olsen D., 2003. A design tool for camera-based interaction. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03). ACM, New York, NY, USA, 449- 456. DOI=http://dx.doi.org/10.1145/642611.642690
- k. Sears WallyHome: Smart Home Sensing and Moisture Detection. Last accessed: January 20, 2017. <https://www.wallyhome.com/>
- l. Samsung Electronics. SmartThings: Smart Home, Intelligent Living. Last accessed: January 20, 2017. <https://www.smarthings.com>
- m. Texas Instruments. SimpleLink SensorTag. Last accessed: January 20, 2017. http://www.ti.com/ww/en/wireless_connectivity/sensortag2015/gettingStarted.html
- n. Dialog Semiconductor. IoT Sensor Development Kit. Last accessed: January 20, 2017. <http://www.dialog-semiconductor.com/iotsensor>
- o. Relayr Wunderbar. Last accessed: January 20, 2017. <https://relayr.io/wunderbar/>
- p. Libelium. WaspMote Event Module. Last accessed: January 20, 2017. <http://www.libelium.com/products/waspmote/>
- q. Notion. Wireless Home Monitoring System. Last accessed: January 20, 2017. <http://getnotion.com/>
- r. Matrix One. The World's First IoT App Ecosystem. Last accessed: January 20, 2017. <http://matrix.one/>
- s. Laput, G., Zhang, Y., Harrison, C. (2017, May). Synthetic Sensors: Towards General-Purpose Sensing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 3986-3999). ACM.

Tabella 42. Funzionalità di general purpose sensor

Lo studio esplorativo effettuato da Laput et al., (2017) ha rivelato che, mentre i dati dei sensori a basso livello possono essere ad alta fedeltà, spesso non rispondono alla vera intenzione degli utenti. Pertanto, una chiave potrebbe essere quello di supportare la "virtualizzazione" di dati a basso livello, introducendo un modello di astrazione rilevante attraverso un paradigma denominato "synthetic sensor".

In questo quadro, i dati dei sensori esposti agli utenti finali sono "virtualizzati" in costrutti di livello superiore, quelli che meglio possono tradursi nei modelli mentali degli utenti.

Da un punto di vista architettonico, è possibile rilevare eventi che si manifestano in un ambiente attraverso i dati del sensore a basso livello. Ad esempio, quando un rubinetto è in funzione, un tag sensore vicino può raccogliere vibrazioni indotte dai tubi dietro al muro e dalle caratteristiche acustiche dell'acqua corrente.

Questi sistemi supportano due modalità di machine learning: addestramento manuale (ad esempio, tramite un'interfaccia utente appositamente creata) o l'apprendimento automatico (ad esempio, tramite metodi di clustering non supervisionati).

L'output del livello di apprendimento automatico è un sensore "sintetico" che estrae dati a basso livello (ad es., vibrazioni, luce, audio, colore, sensori EMI) in rappresentazioni centrate sull'utente (ad es. segnalazione della presenza di un intruso). Una volta inviati i dati, viene eseguita la segmentazione automatica degli eventi sul lato server. Per ridurre gli effetti del

rumore ambientale, il server utilizza un modello di sfondo adattativo per ogni canale del sensore.

L'approccio comune per l'aggiornamento di un ambiente in un ambiente intelligente è quello di installare Smart Objects che contengano funzionalità di rilevamento (ad esempio: interruttori di luce) e/o di associare tag e sensori "universali" oggetti che non sono "intelligenti". Il limite risiede nel fatto che la funzionalità di rilevamento è generalmente limitata all'oggetto stesso (ad esempio: un interruttore intelligente sa se è acceso o spento) o quando serve la sua funzione di base (ad esempio, un rilevatore di presenza). Altri ostacoli all'introduzione del CPS includono un'interoperabilità su larga scala e l'impossibilità di fornire interpretazioni complesse o l'identificazione di fatti "indiretti" (o impliciti).

In genere, l'interoperabilità è generalmente difficile da ottenere su larga scala; solo pochi oggetti sono interoperabili, formando quindi "silos di dati" indipendenti che ostacolano un'esperienza olistica (Laput et al., 2017, p.3986). Inoltre gli output dei sensori tradizionali possono fornire risposta a domande semplici (ad es. "la porta è aperta?") ma non a domande reali e complesse ("è in corso un evento criminale nella filiale?"). Domande complesse non possono essere risolte dai sensori tradizionali (Tripolitsiotis et al, 2017).

Inoltre, gli approcci tradizionali portano ad un notevole aumento dei costi ed è un motivo principale per cui gli intervistati non hanno ancora suggerito di aggiornare le BB secondo un paradigma IoT. In questo lavoro proponiamo un approccio innovativo alla Cyber Physical Security basato sull'utilizzo dei cosiddetti "indirect sensors" opportunamente nascosti nell'ambiente (Lloret et al., 2015). Seguendo questo approccio, un sensore fisico può consentire la rilevazione di molte tipologie di dati che generalmente richiedono l'utilizzo di diversi oggetti. Il rilevamento indiretto si basa su un singolo sensore onnisciente in grado di digitalizzare interi edifici. Per realizzare tale approccio, sono disponibili due tecnologie diverse: Computer vision, basata su smart cameras dotate di sensori multipli e sensori sintetici, che rappresentano l'integrazione della capacità di rilevamento presenti in molti dispositivi (Grill et al., 2015; Dimitrova, 2016, Laput et al., 2017). Nel caso dei sensori sintetici le capacità di rilevamento in entrambi i casi possono riguardare vibrazioni, audio, temperatura dell'ambiente, temperatura di contatto, umidità, pressione atmosferica, illuminazione, colore, movimento, magnetiche, interferenze elettromagnetiche, RSSI - Indicatore di resistenza del segnale ricevuto. In ogni caso, i sensori utilizzano algoritmi di machine learning per elaborare i dati raccolti, in modo da poter essere riconfigurati per identificare vari tipi di attività ed essere in grado di rilevare eventi primari (ad esempio: un openbox è aperto, un umano con una pistola sta attraversando la porta di ingresso della BB, ecc.). Grazie all'utilizzo di algoritmi di machine learning, i sistemi possono inferire eventi secondari (ad esempio: la cassaforte è aperta a causa delle attività di riempimento previste e solo il personale autorizzato è presente, l'uomo con la pistola è una guardia armata

autorizzata ad entrare nella BB. In entrambi i casi si tratta di "falsi positivi": il sistema riconosce che la situazione non è pericolosa e non è necessaria alcuna azione aggiuntiva.

Per migliorare ulteriormente l'efficacia dei sistemi di computer vision, la piattaforma IPS può essere dotata di un sistema di riconoscimento di comportamenti umani e di emozione, la cui applicazione nella videosorveglianza è stata ampiamente studiata (Morris e Trivedi, 2008) (Poppe, 2010). L'obiettivo è quello di prevenire comportamenti dannosi di persone sulla scena aiutando a prevenire gli attacchi riconoscendo automaticamente i comportamenti comportamentali a "evoluzione negativa" a rischio, i comportamenti con un rischio concreto per anticipare un crimine. In questo senso, Blauensteiner et al. (2010) propone una piattaforma che, integrando la scienza dell'informatica con gli elementi della sociologia, è in grado di registrare il comportamento delle persone che commettono furti per analizzarli statisticamente e utilizzare dati per prevenire futuri attacchi.

5.4 Implicazioni organizzative derivanti dalla reingegnerizzazione del processo

Per ciò che concerne gli aspetti organizzativi, sono emerse diverse aree di intervento, qui di seguito riportate:

- Formazione dei Dipendenti relativamente alla reazione al verificarsi di un evento criminoso ai danni della filiale. La formazione dei dipendenti è una misura organizzativa non trascurabile. Essa permette di armonizzare ed equilibrare le procedure, le norme, le reazioni e i comportamenti per gestire un'emergenza; tentare di rimuovere quegli atteggiamenti e comportamenti che possono aumentare il rischio per la propria ed altrui salute; modificare, per quel che è possibile, la propria percezione del rischio.
- Gestione efficace dell'ATM (ad es. caricamento bancomat fine settimana). La gestione efficace dell'ATM serve a ridurre il numero di attacchi ai bancomat durante il fine settimana, quando la macchina risulta essere caricata con un quantitativo superiore di contante rispetto ai giorni lavorati.
- Meccanismi organizzativi per il controllo di filiale. Attualmente il controllo della dipendenza bancaria è demandato alla singola filiale. La centralizzazione delle attività di controllo di più dipendenze bancarie, consentirebbe di liberare gli addetti alle attività di controllo da compiti operativi che in alcuni casi possono essere anche alienanti, o comunque comportare stanchezza e distrazione, come ad esempio il controllo costante di uno o più monitor. Nell'ottica della crescita dell'organizzazione e dell'empowerment del personale di controllo, l'operazionalizzazione di questi meccanismi organizzativi per il controllo di filiale si può istanziare attraverso una piattaforma di controllo intelligente che sia in grado di minimizzare i "falsi positivi" e che supporti l'addetto nell'identificazione di situazione di rischio ad evoluzione negativa. Tale piattaforma consente inoltre di minimizzare il numero di persone

addette al controllo: attraverso un sistema di supporto all'identificazione di situazioni critiche, un solo addetto sarà in grado di controllare contemporaneamente più dipendenze bancarie, evitando non solo azioni alienanti, ma comportando un evidente risparmio in termini di costi della sicurezza.

Alla luce di quest'ultima considerazione, è possibile evidenziare il forte legame tra l'aspetto organizzativo e quello tecnologico. Secondo quest'ultima dimensione, sono state infatti proposte una serie di misure che dovranno essere considerate nella piattaforma di controllo oggetto di questo capitolo.

Di seguito, sono riportate le principali modifiche relative ai processi di gestione di sicurezza illustrati nel capitolo 3.

- **P1.** I flussi continui di dati generati dall'IPS potrebbero essere utilizzati per supportare molti processi di business intelligence. Con l'uso dell'IPS, tutte le misure di protezione sono costantemente monitorate in modo che il CSO possa conoscere in tempo reale e senza l'intervento del direttore della filiale. Inoltre, in caso di attacco criminale, l'IPS può:
 - creare automaticamente una precisa relazione scritta sul crimine che viene data all'ufficio di polizia
 - aggiornare il repository delle dipendenze bancarie e inviare relazioni periodiche a soggetti interessati come il consiglio di amministrazione, il CFO e l'Associazione Nazionale Bancaria. L'aggiornamento è ora basato su dati segnalati obiettivi e non mediati evitando così gli errori dovuti all'intervento umano.

Utilizzando algoritmi di machine learning, i dati raccolti possono essere utilizzati dal CSO per calcolare un profilo di rischio in tempo reale per ogni BB, al fine di progettare un insieme personalizzato di misure di protezione. Inoltre, dall'analisi degli attacchi passati, il modello può prestare maggiore attenzione ai rischi endogeni. L'analisi potrebbe beneficiare ulteriormente di un'integrazione con repository di attacchi criminali presso l'Associazione Nazionale Bancaria. Operativamente, l'IPS identifica l'insieme delle minacce e delle vulnerabilità e calcola il loro peso che viene utilizzato per formulare la funzione di valutazione dei rischi. Il CSO convalida la funzione di valutazione dei rischi proposta dall'IPS. Per ogni BB il sistema calcola il suo profilo di rischio in tempo reale. Le caratteristiche di ogni BB, incluse le misure di protezione già adottate, sono definite nel momento in cui l'IPS viene implementato. Le modifiche delle caratteristiche della BB e l'introduzione di nuove misure di protezione vengono aggiornate come output del processo P3. Per ogni BB, il sistema suggerisce un insieme di misure di protezione ad hoc da adottare. Il CSO valuta i suggerimenti IPS e sceglie le misure di protezione da adottare. Il CSO valuta le nuove misure di protezione eventualmente individuate ed aggiorna la base di conoscenza dello IPS.

- **P2:** Nessuna modifica.
- **P3:** Nessuna modifica del flusso logico delle attività. In ogni caso, le attività sono supportate dall'IPS e, quando viene introdotta una nuova misura di protezione all'interno di una dipendenza, le sue caratteristiche devono essere aggiornate nell'IPS.
- **P4:** L'IPS consente la gestione della sicurezza remota di una filiale, in quanto è in grado di gestire i dati provenienti dai sensori appartenenti al CPS. Se vengono rilevate anomalie l'IPS (o un dipendente attraverso l'IPS) informa automaticamente il CSO e il direttore di filiale; inoltre, l'IPS consente alla manutenzione predittiva di prevedere e prevenire la localizzazione e l'ora delle anomalie più diffuse. Quando l'IPS rileva un nuovo evento, fa un matching tra il nuovo evento e quelli già esistenti nella base di conoscenza, al fine di:
 - Riconoscere il tipo di evento.
 - Proporre in tempo reale una contromisure adeguata.

Se l'evento è considerato pericoloso (un attacco criminale o una situazione che potrebbe eventualmente diventare un attacco criminale), la guardia di sicurezza nella sala di controllo riceve un messaggio di avviso dall'IPS e suggerimenti sulla possibile reazione. Nel frattempo, l'intelligenza di sistema è in grado di attuare reazioni automatiche se presenti nella sua base di conoscenza. La guardia di sicurezza valuta l'evento e prende una decisione appropriata (ad esempio richiede l'intervento delle autorità di contrasto del crimine). Tutti i dettagli dell'evento vengono caricati automaticamente nel repository IPS e contribuiscono ad ampliare la base di conoscenze.

- **P5:** Tutti gli eventi riconosciuti e gestiti tramite l'IPS sono memorizzati automaticamente con tutti i possibili dettagli (ad es.: durata, minaccia, arma, numero di criminali, valore delle perdite, asset di colpa ...). L'IPS produce rapporti periodici alle parti interessate il CFO, l'Associazione Nazionale Bancaria e altri).

I 5 sottoprocessi descritti sopra nella situazione di destinazione sono graficamente rappresentati mediante un diagramma BPMN (vedi Figura seguente):

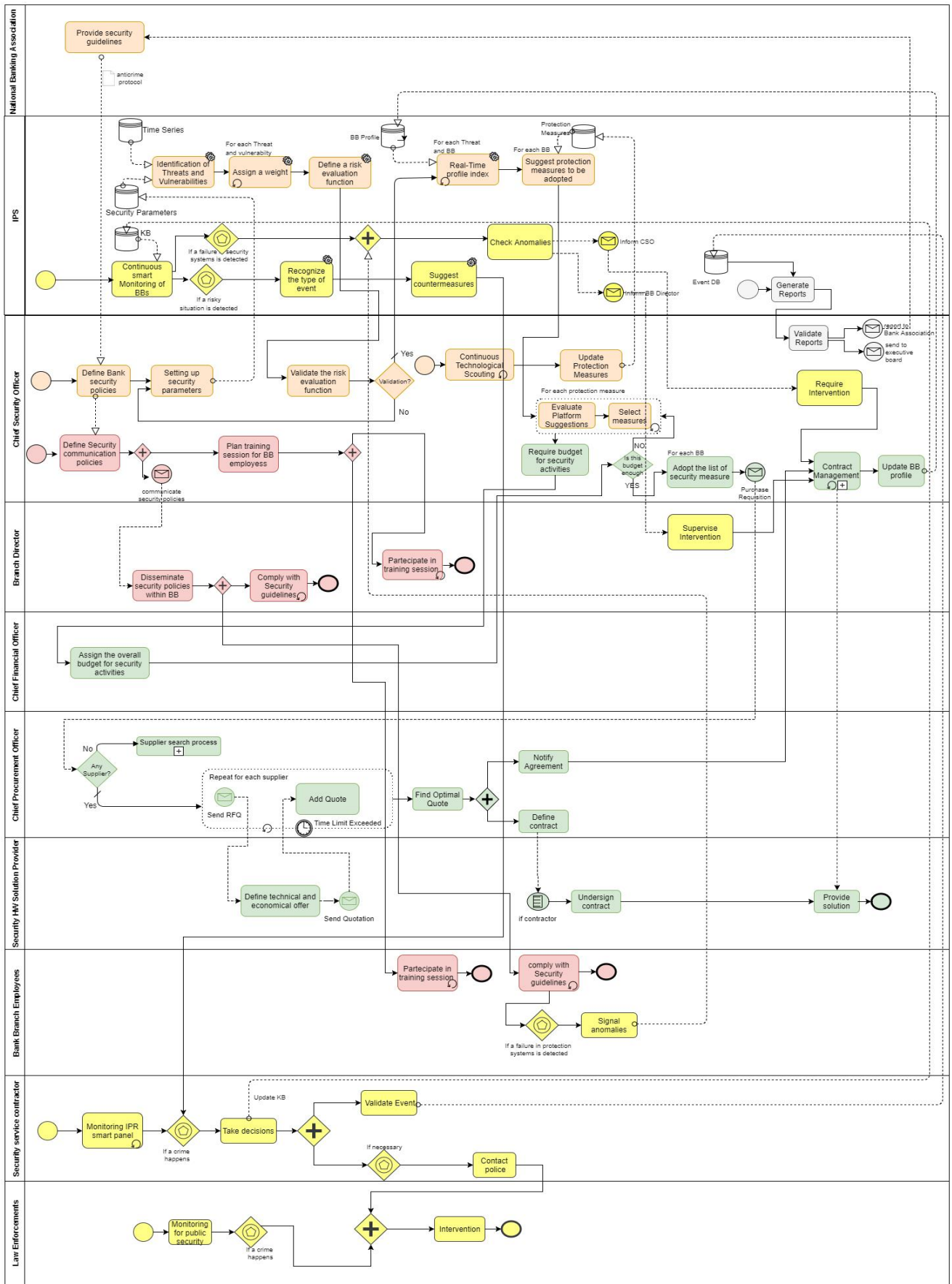


Figura 75. I processi di gestione della sicurezza. Situazione TO BE

5.5 Focus group: alcune considerazioni sulle proposte to-be

In questa fase l'obiettivo era quello di raccogliere un parere tecnico e qualificato da parte degli opinion leader del settore della sicurezza pubblica e privata, sull'efficacia, criticità e vantaggi, eventuali correttivi e suggerimenti di miglioramento proposti. Il sistema è articolato in sottosistemi tecnologici e misure organizzative ed è diretto a contrastare tali eventi criminosi e a ridurre al minimo il rischio di accadimento, l'impatto, gli effetti e le conseguenze negative. La discussione si apre dopo aver illustrato ai partecipanti in modo approfondito le soluzioni proposte

Si parte con la spiegazione delle ipotesi di lavoro alla base della costruzione del "modello" di sicurezza, formulate sulla base della letteratura scientifica e della casistica dei reati e dei dati empirici sulla tipologia delle rapine, e addividendo alla tesi che è necessario e conveniente agire sui fattori di prevenzione che possano di fatto impedire e limitare e dunque ridurre al minimo il rischio dell'accadimento di tali eventi criminosi, con l'obiettivo anche di ridurre l'impatto e le conseguenze negative che possono derivare a seguito del verificarsi dell'evento.

Entrando poi nel dettaglio vengono illustrati con dovizia di particolari tutti gli aspetti tecnici, tecnologici e organizzativi, di ognuna delle otto misure e sistemi di sicurezza collegati ad un'unica piattaforma informatica. Da questa è possibile monitorare e rilevare in *real time* tutti i segnali di warning, di intrusione e violazione a danno delle dipendenze bancarie, grazie all'uso di sensori posti in ogni periferica in cui agiscono tali sistemi, con la possibilità eventualmente di agire direttamente, prevenendo, riducendone la portata e l'impatto dell'evento criminoso, oltre che il rischio di accadimento, e in alcuni casi, inibendo le azioni del soggetto o criminale che tenta di effettuare la rapina. I partecipanti sono stati dunque invitati e stimolati ad esprimere la loro idee sul modello di sicurezza proposto, le loro opinioni orientamenti e pareri sulle specifiche tematiche legate ai singoli sistemi e misure organizzative.

In ultimo, l'obiettivo del focus non era portare il gruppo verso l'assunzione di decisioni, né ricercarne il consenso su un argomento. Il focus group aveva l'obiettivo di tirare fuori al massimo da ciascun partecipante le *expertise* e le opinioni su un argomento specifico, attraverso un confronto costruttivo.

La discussione si apre sul tema delle rapine che avvengono all'interno delle filiali bancarie, sulle dinamiche e gli aspetti che caratterizzano o possono caratterizzare queste tipologie di eventi criminosi, sulle conseguenze e gli effetti, soffermandosi sui sistemi e misure di sicurezza diretti a prevenirle e contrastarle. In particolare l'attenzione si focalizza subito su uno dei primi sistemi illustrato ai partecipanti, legato agli strumenti e tecnologie di videosorveglianza, più specificatamente di biometria facciale in grado di riconoscere e memorizzare i visi delle persone e dunque degli eventuali criminali che si apprestano a compiere la rapina.

- Punti di forza, criticità, suggerimenti e soluzioni

I partecipanti sono stati sollecitati ad esporre le proprie esperienze, al fine di riuscire a tracciare un quadro delle problematiche “percepiti”. Innanzitutto, riconoscono ed evidenziano la grande portata innovativa e le grandi potenzialità di applicazione di tali tecnologie rilevando nel contempo alcune criticità e soluzioni di miglioramento come era nell’obiettivo del focus.

Le criticità evidenziate durante la discussione riguardano in particolare le semplici azioni messe in atto dal criminale, di camuffamento e copertura del viso, di solito molto frequenti nelle rapine (i partecipanti ne evidenziano per loro esperienza un’elevata casistica) dirette ad aggirare ed eludere i sistemi di videosorveglianza che di fatto renderebbero inefficace tali sistemi.

“...queste dinamiche accadono spesso e non solo nel contesto bancario, il soggetto in questione sa innanzitutto dove sono poste le telecamere facendo attenzione a nascondersi il viso, abbassandosi la visiera del cappello, o mettendo sciarpa e occhiali scuri così da essere irriconoscibile alle telecamere, nei furti è un cosa che capita quotidianamente”

Tale affermazione, in parte inizialmente avallata da uno degli intervistati, è stata poi di fatto articolata anche da altri partecipanti. L’attenzione si è poi rivolta alle possibili soluzioni da adottare per ovviare a tale inconveniente.

Sicuramente il problema si potrebbe superare introducendo il divieto tassativo di entrare con il viso coperto e di introdurre e usare oggetti che in qualche modo possano essere impiegati per nascondere, tale controllo ovviamente deve essere preventivo e deve avvenire prima che il soggetto acceda nei locali della filiale. Difatti questo è uno dei presupposti di funzionamento del sistema che preventivamente inquadrando e riconoscendo il viso blocca all’entrata il criminale. Si fa giustamente notare che:

“...il sistema dovrebbe funzionare quando si entra nella bussola, nella porta girevole della banca e in essa io non dovrei entrare con il viso coperto così già il sistema inquadra e memorizza il mio viso, anche perché potrei nascondermi il viso una volta entrato nella filiale, è dunque prima dell’entrata o al momento dell’entrata nella bussola che devo fare in modo che il criminale non entri con il viso coperto, altrimenti il sistema non avrebbe ragione di essere applicato preventivamente”

Ancora viene sottolineato un altro aspetto importante che si collega al discorso del rispetto delle regole e dei divieti che possono essere posti a garanzia di tutti gli utenti e per evitare l’accadimento di tale episodi delinquenti:

“...la banca non è un ente pubblico, non è un edificio pubblico, dove la gente si reca per avere erogato dei servizi pubblici, è un edificio privato, è un luogo privato quindi si può decidere di imporre delle regole, per cui nel nostro caso possiamo applicare il divieto di entrare con il viso coperto...diverso è il caso in cui per eludere tali sistemi il criminale potrebbe ricorrere a sistemi di camuffamento più complessi, trasformando e truccando il viso per evitarne il riconoscimento o ricorrendo addirittura in un travestimento, qui il problema si porrebbe ma si tratterebbe comunque di casi isolati...”

Nel corso della discussione sono stati evidenziati altri elementi di criticità di questi sistemi che riguardano alcuni aspetti tecnici e di rispetto della privacy legati all'acquisizione delle immagini dei volti delle persone. Si fa notare che siccome tali tecnologie sono basate sul rilevamento biometrico del viso delle persone, per cui si stabilisce l'identità di un soggetto a partire anche da un insieme di persone registrate, il problema è la costruzione e la continua implementazione di una valida, efficace ed affidabile banca dati che digitalizzi i visi. A ciò si aggiungerebbe un problema di rispetto o violazione della privacy che deve essere comunque tenuto in considerazione nella costruzione di questa tipologia di base dati. Su tali aspetti molti sono stati gli interventi rivelatisi molto utili per affrontare efficacemente le problematiche e per tentare di offrire soluzioni adeguate.

"...se è vero che la telecamera inquadra il viso, non esiste ancora però una banca dati per fare una comparazione di quel viso. Inoltre nove volte su dieci le telecamere delle banche non hanno una qualità sufficiente quindi molto spesso la telecamera diventa più un deterrente che non uno strumento efficace. Quindi sarebbe necessario raggiungere un'ottima qualità dell'immagine utilizzando telecamere di alta definizione, ma la cosa più necessaria è avere una banca dati delle immagini del viso"

Sulle difficoltà legate alla costruzione di un data base e alla necessità del rispetto delle regole di privacy oltre che sull'efficacia del sistema di intercettare il criminale viene ancora osservato:

"...per quanto riguarda il potenziamento della sicurezza in banca attraverso il sistema dei sensori sniffer che rilevano la polvere da sparo e quelli che rilevano i movimenti sospetti e il viso, si apre uno scenario molto ampio specialmente nel riconoscimento dei visi perché è noto l'arrivo della criminalità dall'Est Europa. Permangono comunque delle criticità dovute al fatto di non poter disporre una banca dati dei visi aggiornata messa a disposizione dalle autorità competenti come ad esempio le questure; senza considerare i casi, spesso molto frequenti, di criminali stranieri che non essendo stati correttamente individuati e identificati commettono il reato e poi si allontanano dall'Italia rimanendo impuniti. Persiste secondo me ancora un problema di privacy anche per i clienti della banca, nella realizzazione e costruzione della banca dati delle immagini dei volti degli stessi che occorrerebbe contattare di volta in volta per acquisire le identità ciò richiederebbe tempi molto lunghi..."

Queste difficoltà secondo l'opinione di alcuni in molti casi non sono insuperabili. La problematica del data base del cliente..

"potrebbe essere superata attraverso il personale della banca che periodicamente convoca i clienti per aggiornare i questionari...o per far firmare loro i contratti bancari...certo se la convocazione deve essere fatta ad hoc ha un costo ma se rientra nelle normali funzioni della banca allora ciò non costituirebbe un ostacolo"

Mentre sul fronte data base viene ribadito che sicuramente il problema della sua costruzione come tutti i sistemi di dati potrebbe presentare delle difficoltà iniziali ma quello di cui si

parla è un sistema incrementale in grado di “apprendere” (si parla di reti neurali) che acquisisce, elabora e restituisce le informazioni in maniera intelligente. Su questo punto è stato osservato che:

“...l’evoluzione del sistema è quello di mettere in comune e condividere tutte le basi dati delle immagini dei visi di tutte le banche e non di una sola banca, ciò potrebbe essere realizzato a livello nazionale in accordo con l’associazione di categoria ABI. Si tratta quindi di realizzare un data base incrementale adottando la metodologia delle reti neurali in grado di apprendere. Si può avere ad esempio anche il caso che il viso di un cliente non viene riconosciuto è questo è già un warning, dunque verrebbero considerate tutte le casistiche. Il criminale dell’Est, ancora per ritornare sull’esempio, se la prima volta non viene riconosciuto perché non si ha la schedatura del suo viso ma viene intercettato a delinquere, la seconda volta che prova a fare la rapina essendo già schedato il sistema è in grado di bloccarlo...”

Anche alle complicazioni legate al rispetto della legge sulla privacy si possono trovare delle valide soluzioni tecniche. Si è evidenziato in proposito che:

“...il problema della privacy viene risolto perché ad ogni volto o utente si associa a livello informatico un codice alfanumerico una stringa numerica per cui non si deve far ricorso al riconoscimento tramite foto (...) il volto non deve comparire...il riconoscimento viene fatto per il tramite di questo codice a cui si associa il viso di una persona e dunque l’utente”

La collaborazione tra banche e forze dell’ordine e sicurezza urbana

Un altro aspetto abbastanza dibattuto che in realtà sembrava esulare dall’argomento centrale del focus era collegato al discorso iniziale della sicurezza urbana e della collaborazione che si può instaurare tra banche e forze dell’ordine. È stato giustamente evidenziato che un’integrazione tra sistemi di videosorveglianza e di sicurezza privati e pubblici potrebbe contribuire e rendere maggiormente sicura l’intera area con un beneficio per tutti gli utenti ma soprattutto per la banca stessa che godrebbe di una maggiore protezione e “percezione” di invulnerabilità, fattore quest’ultimo molto importante nel modello di sicurezza proposto. Si fa notare inoltre che tutto ciò è subordinato ad un corretto ed efficace funzionamento dei sistemi di videosorveglianza pubblici che invece come spesso accade non sono sempre funzionanti ed efficienti.

“...il rapinatore deve poter essere ripreso dalle telecamere esterne urbane, quando queste funzionano correttamente, in modo da rendere agevole l’intervento delle forze dell’ordine e arrivare in tempi brevi alla cattura del rapinatore...”

La discussione continua su un tema che va al di là degli aspetti meramente tecnici ma che ha sicuramente delle implicazioni importanti anche se indirette sui sistemi di protezione e sicurezza: si parla di scarsa efficienza del sistema giudiziario e di un sistema sanzionatorio poco incisivo e severo nei confronti dei molti soggetti che compiono questa tipologia di reati che in mancanza di certezza della pena trovano conveniente reiterare.

“...uno dei problemi che potrebbe incidere anche se indirettamente sulla diffusione dei reati di rapina è che il delinquente abituale non ha la certezza della pena e quindi fa la rapina anche con la pistola giocattolo in questo modo non ha nemmeno l’aggravante dovuto all’intenzione di offendere...per cui il secondo giorno è fuori dal carcere (...). Ci sono purtroppo oltre ai delinquenti occasionali anche i delinquenti professionali e abituali che reiterano il reato in virtù anche di questa poca severità delle pene”

Si fa notare che se da un lato sono molto importanti questa sinergia e collaborazione tra sistemi e soggetti della sicurezza pubblica e privata, dall’altro diventa fondamentale mettere in campo delle efficaci azioni preventive di contrasto (anche attraverso un inasprimento delle pene se necessario) che riducano al minimo il rischio dell’accadimento di tali eventi criminosi ne riducano l’impatto e il danno

“...l’obiettivo di tali sistemi è anche quello di prevenire, fare in modo che l’evento criminoso non avvenga e qualora avvenga fare in modo di ridurre il danno, di accelerare l’evento, mettere subito in fuga il criminale e fare il modo che il delinquente vada via il prima possibile...”

I danni all’immagine e le rapine fuori dalla banca ma vicine alla banca

Approfondendo ancora il tema della sicurezza dentro e fuori la banca e della collaborazione tra vigilanza pubblica e privata è stato rilevato che sono molto frequenti i casi di rapina e di scippo che avvengono fuori ma a distanza ravvicinata dalla filiale a danno di quell’utente che ha appena effettuato un’operazione di prelievamento. Ci si chiede quindi come debbano essere considerati questi casi. Questi casi di solito molto frequenti, in effetti, non rientrano nella sfera di competenza della banca perché avvengono fuori dei propri locali, per cui la banca non avrebbe la responsabilità di prevenirli e spetterebbe quindi alle forze dell’ordine. Ma dalle osservazioni seguenti emergono altri importanti aspetti che dimostrano che non è sempre così.

“...si tratta di una tipologia di reati sui quali la banca non può intervenire direttamente in fase di progettazione di misure di prevenzione e protezione (...) Il caso della persona che viene rapinata dopo che esce dal perimetro della banca diventa purtroppo una questione di sicurezza dell’area, la banca non può avere il controllo di tutta l’area, quella spetta alle forze dell’ordine...”

Da qui si rafforza la tesi della collaborazione tra forze dell’ordine e forze di sicurezza private e si apre un’altra questione importante legata alla percezione della vulnerabilità della banca e al danno d’immagine che una banca può subire in caso di rapina al di là dello scippo perpetuato ai danni magari di un soggetto più indifeso come una persona anziana.

...qui si parla soprattutto dell’entità del danno che posso fare ad una banca rapinandola anche in termini di immagine rendendo manifesta la vulnerabilità della banca stessa, un caso questo che non può paragonarsi a quello dello scippo ai danni di una persona anziana che può essere rapinata da qualche delinquente anche sotto casa... la rapina in banca è un evento più complesso fatta da professionisti...stiamo qui parlando di criminalità organizzata e non microcriminalità

Rispetto a questa problematica è stato giustamente argomentato che la banca non può rimanere indifferente e rimandare la responsabilità alle forze dell'ordine. Difatti se la rapina avviene nei pressi o come spesso accade vicino alla banca ai danni di un cliente che ha appena prelevato dei contanti, anche se la banca non ha competenza e non è suo compito intervenire per impedire che ciò avvenga, si ha comunque un danno di immagine se si diffonde la notizia che in quella zona e nei pressi di quella banca c'è stata una rapina, ciò avrebbe produrrebbe lo stesso effetto di una rapina fatta direttamente in banca.

Le azioni criminose e le frodi che si perpetuano ai danni delle dipendenze bancarie sono diverse così come le dinamiche che le caratterizzano. Nel corso del tempo si sono evolute divenendo sempre più sofisticate in risposta ai cambiamenti e alle evoluzioni tecnologiche e informatiche dei sistemi di transazione finanziaria e di pagamento e dei sistemi di protezione e sicurezza attualmente in uso nelle banche. Oggi si parla dei fenomeni molto diffusi di *cyber-crime* e di rapine informatiche compiute ai danni dei clienti e delle banche da parte di pirati e hacker delle rete che si infiltrano nei computer che controllano i bancomat e le carte di credito, prelevando denaro, e nei sistemi che regolano il trasferimento di fondi tra conti correnti. Tutti i partecipanti dunque sono concordi nell'affermare che le rapine "classiche" fatte presso le dipendenze bancarie sono in calo come dimostrano anche le ultime statistiche.

Più delle rapine ormai le banche si preoccupano di contrastare le azioni criminali più sofisticate, le frodi informatiche e gli altri sistemi evoluti impiegati nei furti telematici divenuti sicuramente più redditizi meno rischiosi delle rapine stesse trattandosi inoltre di fenomeni più estesi che possono riguardare e coinvolgere più istituti bancari...e quindi credo che ormai le banche si stiano attrezzando per proteggersi da questi tipi di reati più che dalle rapine.

Le rapine come è stato osservato dai più nella maggior parte dei casi sono compiute da soggetti sprovveduti che si improvvisano rapinatori, e non da veri criminali professionisti

"...noi lavoriamo con tutti i grossi istituti bancari d'Italia e posso affermare che la maggior parte delle sequenze video che noi abbiamo avuto modo di osservare insieme alle forze dell'ordine quando sono avvenuti i diversi eventi mostrano dei rapinatori assolutamente riconoscibili in banca (...). Come si diceva prima le rapine avvengono nella stragrande maggioranza dei casi in meno di tre minuti e si può osservare in queste sequenze video banalmente un ragazzo che entra con il volto pulito entrare in banca e nell'arco di qualche secondo scavalca il banco dell'addetto allo sportello e prende quello che riesce al volo e scappa. Questa è la rapina tipo nella stragrande maggioranza dei casi. Poi ci sono le rapine con gli ostaggi, più da film le cui dinamiche sono un po' diverse...

"...penso che questi fenomeni stanno spegnendosi... perché la rapina in banca la fa la criminalità di basso cabotaggio e livello, il disperato il drogato, è gente debole dal punto di vista criminale facilmente individuabile, adesso l'organizzazione criminale percorre altre strade utilizza altri sistemi per una rapina...fino a poco tempo fa le facevano ai furgoni portavalori fuori dal luogo protetto...secondo me le rapine alle banche fatte all'interno delle banche, le tentate rapine, stanno diventando molto rare come

dimostrato anche dalle statistiche...costituiscono l'elemento debole della catena della criminalità...la gang e la 'ndrina rapine in banca non ne fa più.

Una soluzione su tutte: riduzione della circolazione del denaro contante

Dagli interventi dei partecipanti emerge che per contrastare efficacemente le azioni criminali a danno delle banche (divenute come appena rilevato più evolute e complesse) occorre avere un approccio globale alla problematica della sicurezza, adottando sistemi di sicurezza più complessi, composti da più misure non solo di tipo informatico, ma rafforzando anche i sistemi tradizionali e intervenire laddove possibile anche attraverso provvedimenti indiretti, quali ad esempio la riduzione del contante.

"...prima abbiamo parlato di percezione di sicurezza e sicurezza effettiva. Ho visto i dati degli utenti di quanto si sentano sicuri in banca e secondo me, la sicurezza effettiva va in senso opposto. I sistemi di sicurezza sono al primo posto per dare garanzia di tranquillità poi c'è la presenza delle forze dell'ordine a seguire la vigilanza e poi per ultimo la limitazione nell'uso del contante. Secondo me è esattamente il contrario. Nel senso che, premesso che se si vuole rapinare una banca se c'è una guardia giurata anziché andare con il taglierino si può andare in quattro con un fucile, se c'è invece solo il metal detector si può andare con un semplice taglierino, insomma i metodi ci sono sempre. Bisognerebbe invece evitare di essere appetitosi per i rapinatori, quindi secondo me l'elemento principale per prevenire le rapine diventa la limitazione nell'uso del contante. Poi sicuramente la vigilanza è importante per contrastare il fenomeno, le forze dell'ordine sono importanti, i sistemi di sicurezza quando funzionano sono importanti perché danno anche la sensazione e la percezione di sicurezza. Secondo me bisogna fare in modo che la banca non abbia denaro perché chi fa una rapina in banca a meno che non sia uno sprovveduto, sa sicuramente anche quanti soldi ci sono, quindi se sa che in banca ci sono pochi soldi, considerato il rischio magari desiste dall'impresa".

"...posso affermare che la tendenza è quella che la nostra azienda si sta attrezzando e tutte le banche si stanno attrezzando nell'impegno di sistemi che limitino e regolino di gran lunga l'uso del contante...e questo appunto è un grande deterrente per quegli episodi di criminalità. È il caso del ragazzo che entra in filiale apparentemente senza nulla e può prendere anche una biro e scavalcare il bancone dello sportello, però se dall'altra parte non c'è contante sul banchetto del cassiere non può rubare nulla è questo che avviene nelle nostre filiali..."

Con riferimento a queste ultime affermazioni ritornando alla problematica dei danni e le ripercussioni che può subire una banca in caso di rapina che spesso superano di gran lunga il danno economico e patrimoniale stesso della somma di denaro trafugata dall'agente criminale, si fa osservare che:

"...il problema però che la banca non può ridurre l'uso del contante a zero, il danno per la banca non è il furto delle 50 o 100 euro... il danno per la banca è che l'operatore di cassa subisce uno shock chiama ai danni la banca e questo ha un costo per la banca"

"...infatti ciò non deve succedere...difatti se si sparge la voce e la notizia che quella filiale è stata sottoposta a ripetuti attacchi anche se questi hanno prodotto zero per il criminale, si torna al discorso dell'impatto che può avere la rapina dal punto di vista dell'immagine, perché il messaggio che passa è

che quella filiale non è sicura e vulnerabile ed è un danno all'immagine...ecco perché il discorso importante è agire sulla prevenzione ed evitare al massimo il rischio che tali eventi accadano..."

Quindi diventa sempre più importante puntare sulla prevenzione. È su questo che deve puntare il pacchetto dei sistemi di sicurezza da proporre; pacchetto che potrebbe essere anche utilizzato come attività di marketing al fine di rafforzare l'immagine della banca comunicando e pubblicizzando che l'adozione di tali tecnologie è in grado di garantire la piena sicurezza agli utenti che si recano in banca ed essere un grande deterrente in grado di prevenire e respingere efficacemente tutte le azioni criminali.

Le rapine agli atm e l'efficacia dei sistemi di sicurezza

Quanto affermato dai partecipanti in merito alla necessità di controllare e limitare l'uso del contante quale forte deterrente per scongiurare il verificarsi di queste azioni criminali trova pieno riscontro nei dati di trend del fenomeno che vede una riduzione delle rapine in banca a fronte di un contestuale e considerevole aumento, negli ultimi anni, degli attacchi e rapine agli ATM dove il criminale sa di poter trovare con maggiore probabilità denaro contante e dove è più facile e soprattutto meno rischioso agire il più delle volte indisturbati. Ancora, sulla convenienza del criminale di concentrarsi più sugli ATM che non sulle rapine in banca è stato giustamente osservato che:

"...le rapine agli ATM sono sempre molto meno rischiose delle rapine in banca... si va di sera in una via o zona poco illuminata dove magari non passa nessuno e si ha tutto il tempo di fare quello che vuole...a mezzogiorno o in pieno giorno in banca si ci pensa prima di fare una rapina. Gli atm dunque sono molto più vulnerabili...posso ad esempio agire tranquillamente con il casco della moto in testa senza essere riconosciuto, in banca invece con il casco in testa non posso sicuramente entrare"

"...considero ottimali le soluzioni per quanto riguarda gli ATM sia la parte dell'OTP (One Time Password, è un sistema che funziona come la chiavetta usata per la sicurezza delle operazioni di home-banking che genera un codice che cambia di volta in volta per prelevare contante dai bancomat) che il sistema che monitora la volumetria degli ATM, sono due proposte che chi si occupa di queste cose apprezza molto, che tra l'altro non ci ha mai proposto nessuno, le trovo molto interessanti specialmente l'OTP.

"L'OTP della carta bancomat, allo stesso modo della Key dell'Home Banking, la vedo molto efficace perché previene un altro fatto: il furto della carta che quindi senza questo One Time Password non può essere utilizzata dal malvivente perché come succede spesso assieme alla carta si conserva il codice di sicurezza rendendo così facilissimo l'uso fraudolento della carta..."

"...magari si fa un'unica chiavetta sia per la carta bancomat che per l'home banking risparmiando ed evitando duplicazioni abbattendo così i costi per la banca e rendendo più facile la vita all'utente che si trova ad avere un unico strumento senza avere tanti key o password, per cui avere un unico chiave key di sicurezza per tutti i sistemi di pagamento mettendo insieme la tecnologia di una ATM e le altre tecnologie si potrebbe aprire un'altra filone di ricerca positiva da lato della sicurezza dei portali home banking per contrastare il fenomeno del fishing...anche se è una questione di cyber security che comunque completerebbe il quadro della sicurezza..."

“Il sistema dei sensori che rileva le forcine inserite nelle fessura di prelievo dei soldi e degli infrarossi sono soluzioni che già esistono sono montate sugli ATM anche se non collegate al sistema di videosorveglianza e delle forze dell’ordine come prevede il vostro sistema di sicurezza. ¹⁴”

...la parte di video sorveglianza in questo caso è importante perché, il movimento della forcina o altro oggetto inserito nella fessura, che viene rilevato dal sensore in caso di manomissione ed allerta la sorveglianza è un fatto ancora più importante, questo perché per esperienza personale, la videosorveglianza non può avere un occhio attento sempre su tutto, su tante telecamere per vedere che succede, quindi il sensore che crea un alert è un’ottima soluzione...

Rispetto a quest’ultima osservazione viene fornito un approfondimento e una spiegazione del funzionamento del sistema adottato per chiarirne meglio le tecnologie e la soluzioni innovative adottate riguardanti la piattaforma informatica di comando che sovrintende l’intero apparato. Tutti i sensori del sistema non sono sensori stand-alone che creano solamente un alert o un suono, ma sono tutti collegati ad una piattaforma per cui la persona addetta alla vigilanza e alla sicurezza controlla e riceve una serie di allarmi, dei warning, la telecamera mostra quello che sta succedendo in quel punto e si può decidere l’azione di mettere fuori uso il bancomat o allertare la vigilanza. Ci sono quindi una serie di livelli di controllo e diverse modalità di azioni per inibire le azioni di rapina, e il tutto fa parte di un unico sistema integrato, ed è qui la portata innovativa del sistema.

¹⁴ La dinamica del furto con la “forcina” è una tecnica semplicissima per rubare dai bancomat. Grazie ad una forcina inserita nella fessura predisposta alla fuoriuscita dei soldi, i ladri riescono a bloccare l’uscita del denaro. La vittima a questo punto, ignara della cosa, entra in banca per protestare e loro intervengono, tolgono la forcina e si portano via i soldi prelevati, si fa per dire, dalla vittima.

5.6 Intelligent Protection System: Architettura funzionale e Scenari di Utilizzo

La piattaforma tecnologica web based introdotta prevede un'architettura di tipo client-server in cui ad un nodo centrale (la control room), a seguito dell'applicazione del modello di rischio all'istante t_0 , sono connesse le n filiali. All'interno della control room agiscono m operatori, (un operatore sarà in grado di gestire più filiali) e un manager incaricato di gestire la Knowledge Base e aggiornare il modello di rischio.

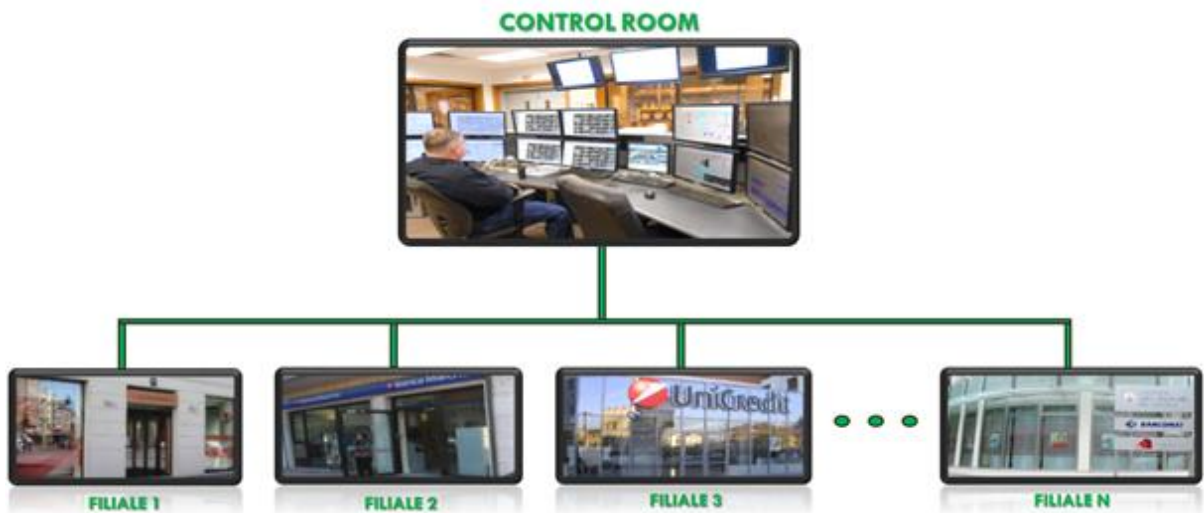


Figura 76. Struttura logica della piattaforma

L'architettura logica della piattaforma è stata frutto di attente analisi per quanto riguarda la modularità, flessibilità ed estensibilità della stessa affinché, le eventuali, future attività di sviluppo e manutenzione del server e del software fossero le più agevoli e stabili possibili.

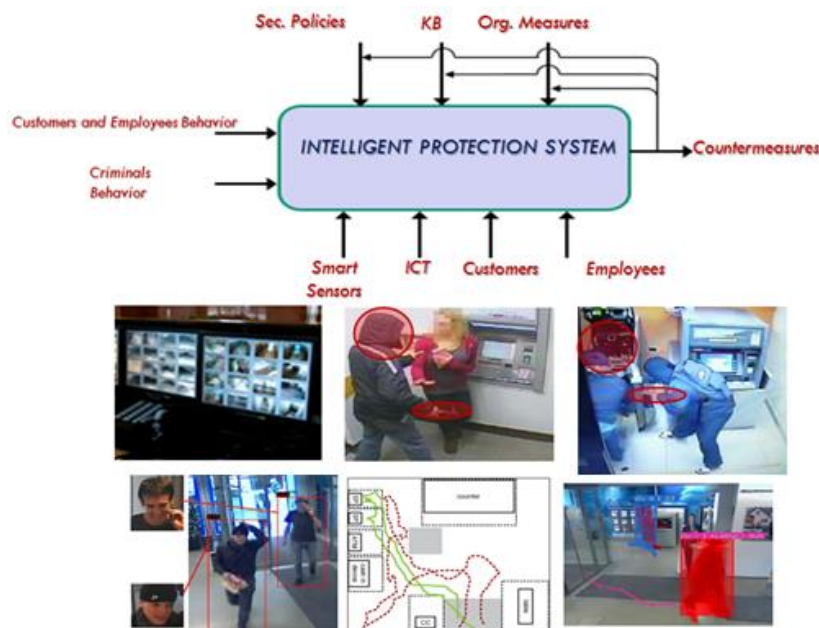


Figura 77. Schema logico e possibili scenari

Dal punto di vista dell'architettura software il modello riflette la struttura delle applicazioni multi tier fruibili attraverso la rete internet, e che utilizza i meccanismi di comunicazione interprocesso tipici delle soluzioni di tipo enterprise.

E' inoltre emersa la necessità di predisporre una piattaforma, ovvero un ambiente di lavoro, che consentisse agli operatori la più ampia possibilità di intervento relativamente alle conoscenze condivise nel gruppo di lavoro, al fine di massimizzare l'impegno di ciascun elemento e rendere sovrapponibili le conoscenze di ciascuno.

La figura seguente mostra le varie componenti interessate e come avviene il flusso di informazioni dalle agenzie alla centrale operativa di controllo.

Il modello applicativo prevede una serie di componenti e di flussi informativi fra le stesse schematizzabili come segue:

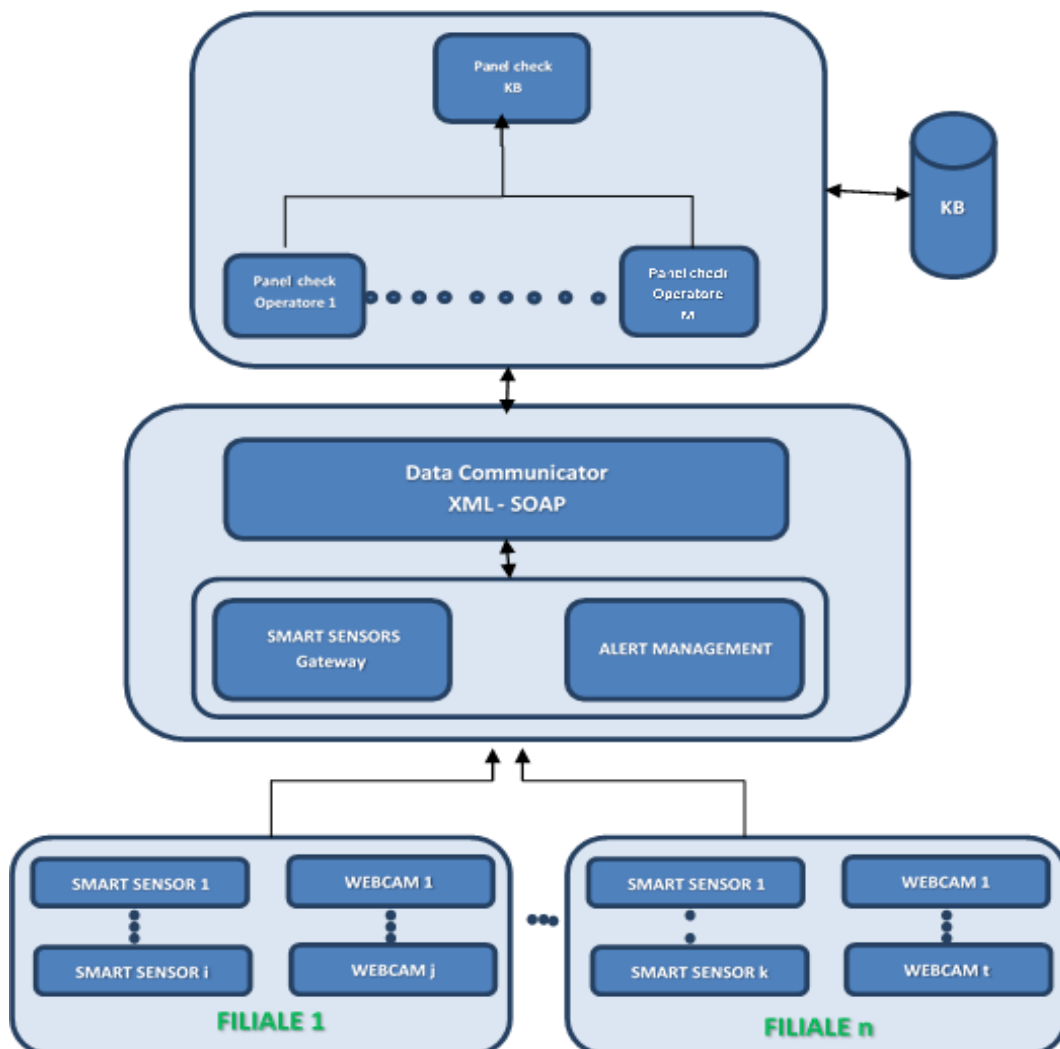


Figura 78. Architettura della piattaforma

Vediamo in dettaglio le varie componenti coinvolte nel processo:

- **Agenzie:** sono le agenzie sparse sul territorio dove sono installate le webcam, i sensori ed altri eventuali componenti che trasmettano gli eventuali allarmi generati.
- **Gesture Recognition:** è il sistema che si occupa di riconoscere, attraverso i segnali video delle telecamere, eventuali movimenti che possano indurre a ritenere che ci sia una infrazione.
- **Gestione Allarmi:** rappresentano tutti gli avvisi di allarmi generati dai sensori (sfondamento, intrusione, etc) che vengono inviati come lista testuale alla centrale
- **Data Communicator:** è il protocollo di comunicazione trasmissione tra i sistemi di riconoscimento (che filtrano gli allarmi assegnando loro un livello di gravità) e la piattaforma che andrà a visualizzarli sul pannello di controllo. Tale comunicazione si basa su web service XML/RPC.
- **Pannello Operatore Tecnico:** è l'interfaccia che l'operatore tecnico utilizza per monitorare gli allarmi che arrivano e li classifica in funzione di alcuni parametri.
- **Pannello Operatore Manager:** è l'interfaccia riservata al Manager attraverso la quale visualizza i dati sotto forma di statistiche ed imposta eventuali modifiche al sistema di misura di sicurezza.
- **DB:** è il Data Base sul saranno memorizzati tutti gli eventi e le decisioni prese. Naturalmente contiene tutta la base di conoscenza del sistema sulle misure di sicurezza e il modello di rischio.

I passaggi eseguiti dall'operatore tecnico per ottenere la gestione completa dell'evento secondo i criteri canonici del PSIM sono:

- a. informazione immediata
- b. verifica efficiente
- c. telegestione dell'evento e dei suoi sviluppi situazionali con un procedimento guidato passo-passo
- d. coinvolgimento operativo di altre funzioni per interventi e per escalation
- e. conclusione, verbalizzazione e storicizzazione

In particolare per ogni singola voce avremo:

- a. informazione immediata: coda allarmi dei nuovi eventi e di quelli in fase di gestione;
- b. verifica efficiente: pulsanti contestualizzati per attivare i controlli in tempo reale della situazione
- c. cruscotto video:
 - a) visualizzazione live di una o più telecamere associate all'evento (cosa sta accadendo);
 - b) visualizzazione di video pre-evento (cosa è successo prima della segnalazione);

- c) commutazione a una videoronda mirata con le telecamere appropriate per quell'evento (se e come l'evento sta evolvendo in una situazione)
- d. oggetti dinamici, posti su mappe, planimetrie, sinottici e qualsiasi altro sfondo grafico, permettono di localizzare il punto dell'evento nell'ambito di un comprensorio, di un edificio, di un piano, oppure di un macchinario, apparato, quadro elettrico; gli oggetti dinamici sono configurati per evidenziare uno stato mediante colorazione e animazione; allo stesso tempo consentono di eseguire attivazioni, reset, pop-up informativi di stato (azionamenti intuitivi, mirati) ovviamente nei limiti del profilo autorizzativo
- e. cruscotto pop-up di verifica di stati/attivazione di comandi per singolo punto/sensore della Centrale di Gestione Eventi se questa lo consente; realizza la telegestione dell'elemento chiave del sito
- f. la gestione di eventi e situazioni, guida l'operatore lungo un percorso procedurale passo-passo, presentando automaticamente le informazioni correlate: persone, servizi, e risorse necessarie a verifiche e interventi; il verbale non si chiude se l'operatore non ha rispettato la procedura e una segnalazione ne informa un livello responsabile, anche in una diversa Control Room
- g. archiviazione del log che traccia tutto il processo di gestione fino alla verbalizzazione in una base dati
- h. possibilità di interagire con altri sistemi informatici interni ed esterni come quelli del ticketing e della vigilanza

Il Deployment Diagram mostra l'architettura dal punto di vista fisico e logistico di un sistema. Tale diagramma può descrivere i computer e i vari dispositivi presenti, mostrare le varie connessioni che intercorrono tra di essi e, ancora, il software che è installato su ogni macchina.

Applichiamo ora i precedenti componenti alla nostra piattaforma. Nella figura seguente (Schema Attori) vengono visualizzati i principali attori che sono coinvolti nell'utilizzo della piattaforma (tale struttura riprende quella iniziale dei componenti coinvolti).

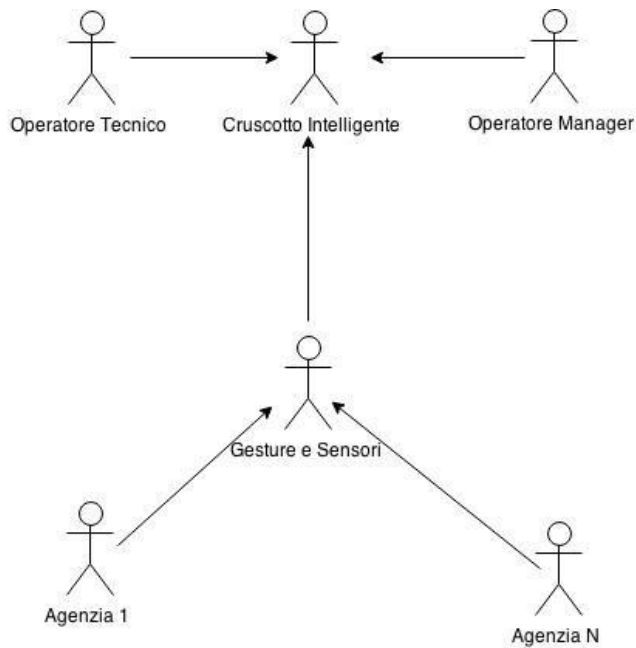


Figura 79. Schema Attori - Use Case Diagram

Passiamo adesso alla rappresentazione dei casi d’uso. In particolare avremo:

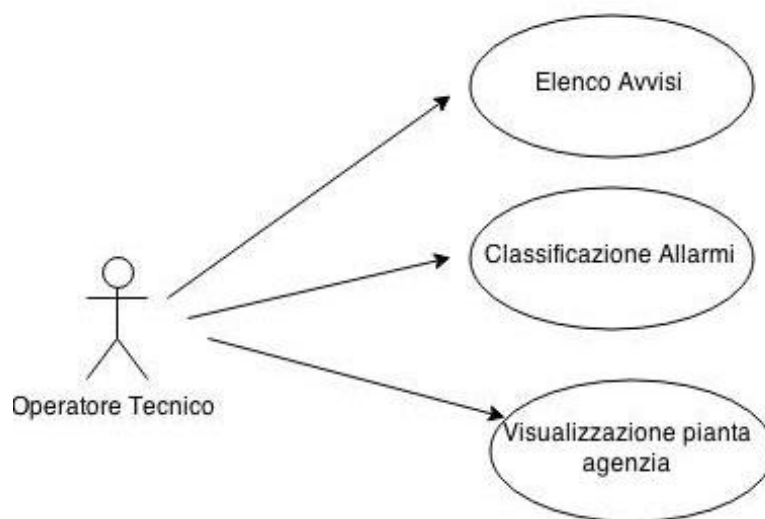


Figura 80. Operatore Tecnico - Use Case Diagram

La figura precedente riguarda lo “Use Case” dell’operatore tecnico che dovrà compiere una serie di operazioni che rappresentano una delle caratteristiche principali della piattaforma.

Un ulteriore Use Case riguarda l’Operatore Manager, colui che definisce nella piattaforma le regole da utilizzare in funzione dell’analisi effettuate.

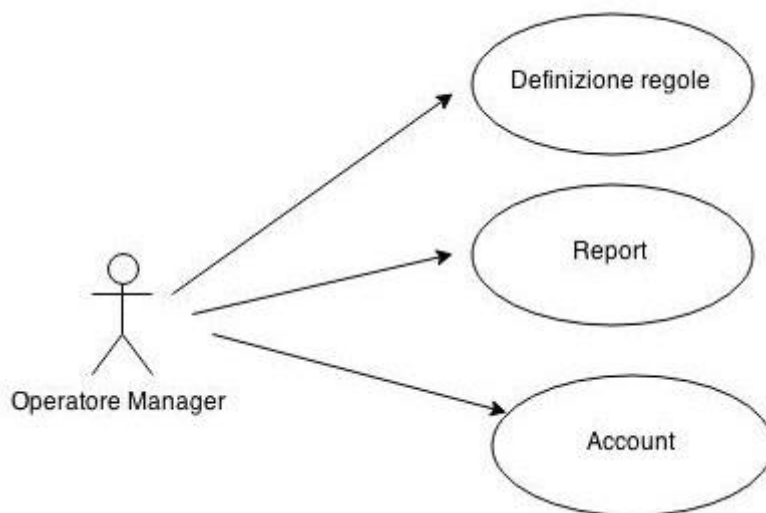


Figura 81. Operatore Manager - Use Case Diagram

Un ulteriore Use Case riguarda invece una componente della piattaforma che si identifica con dei sistemi automatici di gestione e classificazione dei segnali che arrivano dalle agenzie.

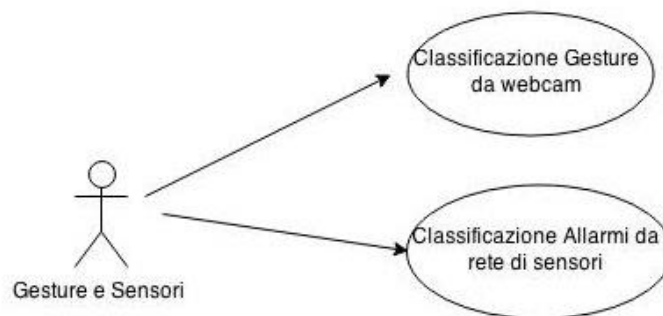


Figura 82. Sensori - Use Case Diagram

In questa figura sono rappresentate le funzionalità che devono compiere i due sistemi di analisi dei dati provenienti dalle agenzie. Questi dati vengono classificati e passati alla piattaforma assegnando loro un livello di allarme opportuno.

Vediamo adesso lo schema delle principali funzioni della piattaforma.

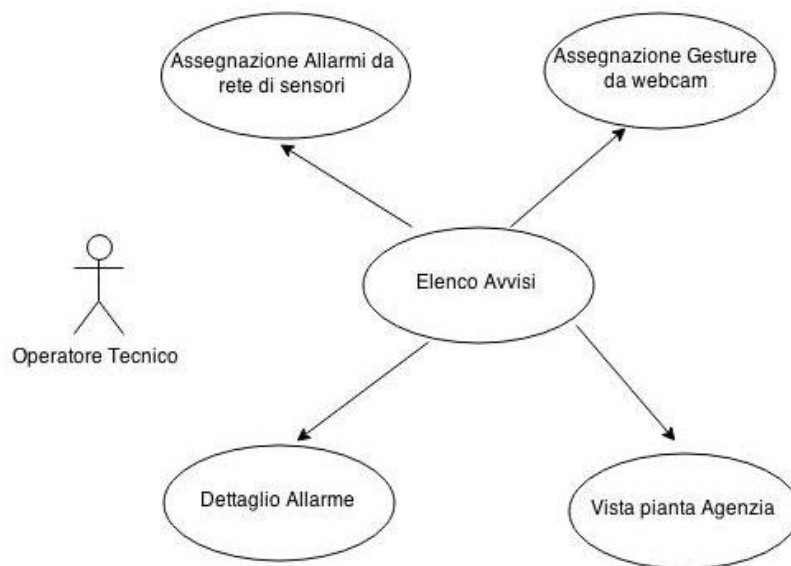


Figura 83. Gestione avvisi per Operatore Tecnico - Use Case Diagram

Lo schema di deployment della piattaforma è qui di seguito presentato. Lo scopo è quello di descrivere il sistema in termini di risorse hardware e di relazioni fra di esse.

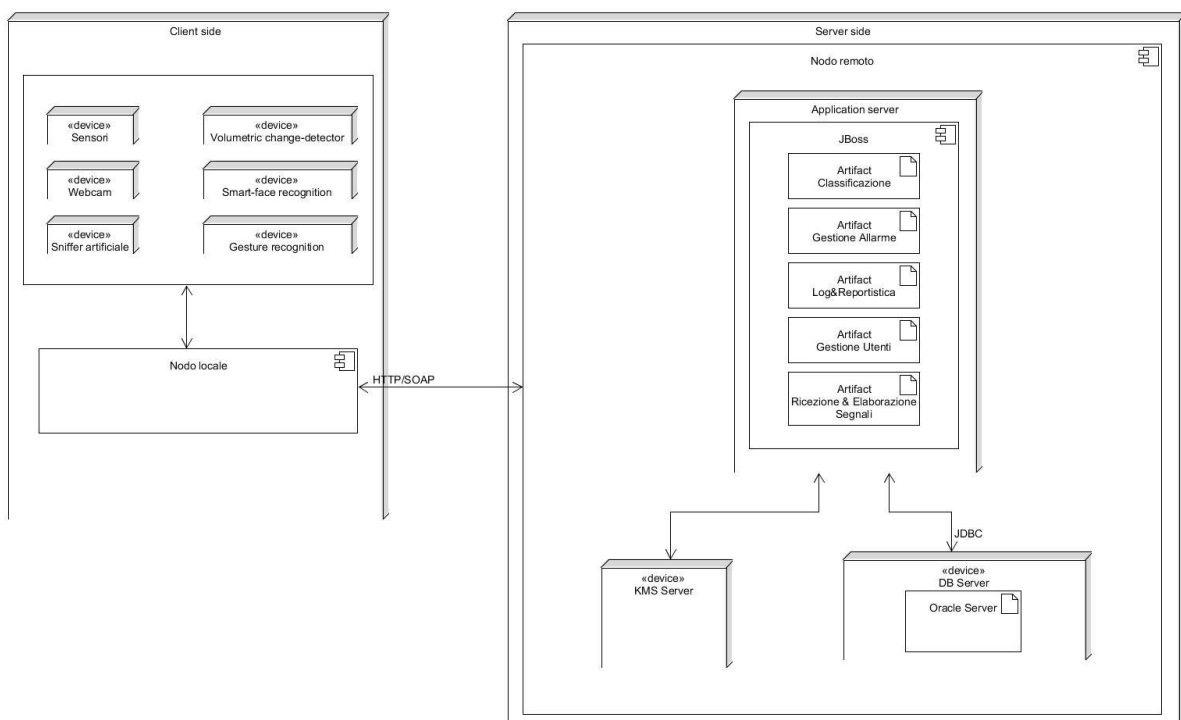


Figura 84. Schema di Deployment della piattaforma

L'uso della piattaforma tecnologica consente di rilevare i segnali provenienti dai sensori/webcam delle filiali, analizzarli e, in maniera automatizzata o semi automatizzata, proporre ed eseguite delle contromisure. Lo schema attori che interagiscono sulla piattaforma è il seguente:

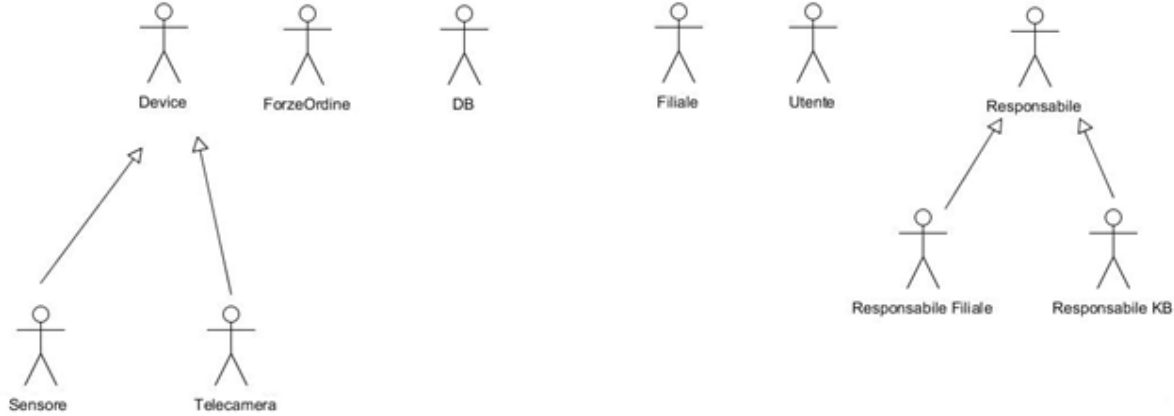


Figura 85. Schema Attori

Il class diagram della piattaforma può essere così rappresentato:

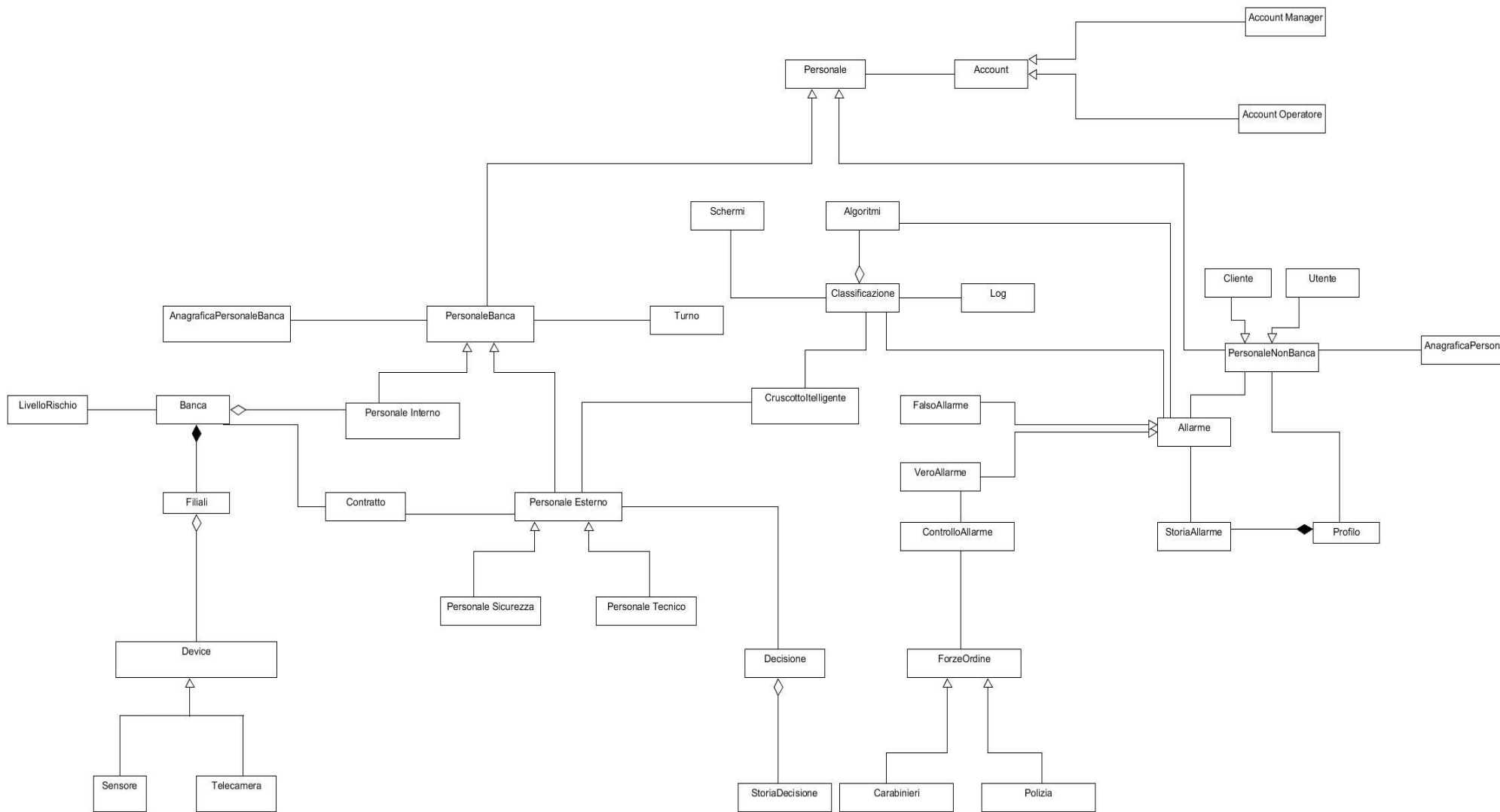


Figura 86. Class Diagram

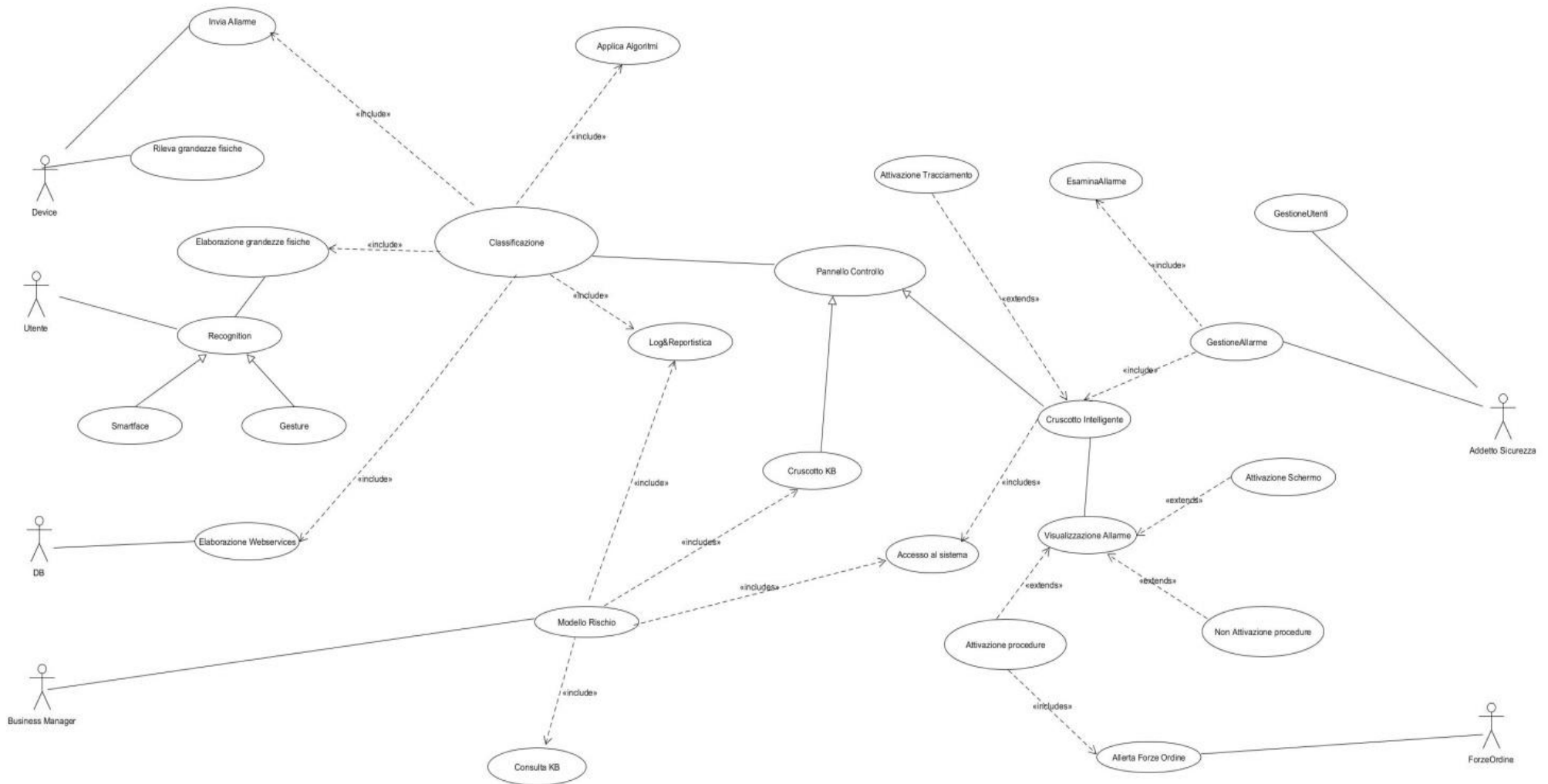


Figura 87. Use Case Diagram Complessivo

Un sistema PSIM, nelle sue componenti logiche basilari, è costituito da:

1. PSIM Server System;
2. Client Application: Consolle Operatore;
3. Remote Configuration Application: configura i sistemi remoti;
4. PSIM Configuration Administration: configura il sistema PSIM.

PSIM Server System

Lo PSIM Server System è a sua volta costituito da diverse componenti hardware e software dedite alla connessione e gestione dei sistemi remoti, alla ricezione, memorizzazione e gestione degli eventi, alla loro distribuzione e visualizzazione sulle diverse consolle operatore competenti territorialmente e distribuite geograficamente, alla connessione e comunicazione dei sistemi e servizi interni e molto altro.

Di seguito si descrivono gli applicativi e le funzioni software minimali necessarie alla componente Server di un sistema PSIM evoluto indicato nella precedente figura.

D.B. - Base Dati. Applicazione che consente la creazione, manipolazione e l'interrogazione efficiente dei dati (database management system – DBMS). La particolare applicazione utilizzata (Microsoft SQL Server, Oracle, MySQL, ecc.) dovrà essere ridondata e assicurare la sincronizzazione immediata con uno o più Database server in rete.

Core. Insieme di applicativi e funzionalità installati su uno stesso server o installabili su differenti server tra loro connessi in rete, purché:

- gestiscano le segnalazioni, informazioni e dati provenienti dai sistemi remoti, effettuandone una opportuna conversione nel formato interno idoneo;
- storicizzino i dati provenienti dai sistemi remoti o generati internamente al sistema;
- interrogino o aggiorni il database, assecondando gli algoritmi di funzionamento del sistema;
- eseguano i comandi generati dal sistema o comandati dagli operatori del sistema, convertendoli nell'idoneo formato del particolare sistema remoto che li deve eseguire;
- permettano l'opportuno aggiornamento delle segnalazioni ai vari Client Applications;
- permettano l'esecuzione delle richieste di tutti i prospetti di riepilogo (allarmi, anomalie, lista impianti inseriti, lista impianti disinseriti, ecc.), effettuate dalle consolle associate o generate internamente dal sistema;
- effettuino il Monitoraggio e la gestione dei processi interni al sistema;
- eseguano tutte le funzionalità grafiche e video.

Primary. Server e applicazioni che assicurano la comunicazione in primaria (Tcp/Ip) con i sistemi remoti. Ognuna di tali applicazioni implementa un numero massimo predefinito di connessioni. Il numero di Primary server necessari per la comunicazione e il numero di

applicativi Primary necessari varia in funzione del numero di siti remoti e delle politiche di Business Continuity e Disaster Recovery da applicare.

Backup. Server e applicazioni che assicurano la comunicazione secondaria o di backup con i sistemi remoti. Ognuna di tali applicazioni implementa un numero massimo predefinito di canali di connessione. Il numero di Backup server necessari per la comunicazione e il numero di applicativi di Backup necessari varia in funzione del numero di siti remoti e delle politiche di Business Continuity e Disaster Recovery da applicare.

La comunicazione che viene instaurata tra il sistema PSIM Server e i sistemi dislocati nelle varie agenzie periferiche si basa sul paradigma Client-Server in modalità real time, con elevati livelli di performance delle applicazioni.

Questa architettura è particolarmente indicata per tali sistemi, permettendo allo PSIM di individuare e visualizzare all'operatore tutti i sistemi remoti non raggiungibili o che evidenziano problematiche di comunicazione di rete. Infatti, per i sistemi PSIM, risulta fondamentale ricevere nel minor tempo possibile gli eventi generati dal campo, e quindi acquista importanza strategica la riduzione minimale della latenza dell'informazione per ogni sistema.

Client Application

È il sistema utilizzato dagli operatori della Control Room. Particolare attenzione deve essere dedicata alla progettazione e realizzazione della sua componente grafica (GUI - Graphical User Interface), al fine di soddisfare requisiti di progettazione stringenti (norme ISO). Sistemi Client funzionalmente analoghi possono differire significativamente tra loro a livello grafico, agevolando o meno l'attività dell'operatore di C.R.

Un sistema Client Application può essere suddiviso in molteplici applicativi funzionali; di seguito si evidenziano i più significativi.



Figura 88. Caratteristiche funzionali della console operatore

- *Event Manager*: componente software che ha il compito di ottenere gli eventi dal server e di visualizzarli opportunamente. In particolare deve:

- ❖ ottenere esclusivamente gli eventi di competenza;
- ❖ ottenere gli eventi in forma incrementale, onde ridurre al minimo il traffico dati di rete;
- ❖ aggiornare lo stato di tutti i componenti dei siti gestiti;
- ❖ visualizzare, ove necessario, gli eventi e il loro stato.

- *Command Manager*: componente software che ha il compito di inviare il comando generato dall'operatore al server, monitorarne lo stato di avanzamento, evidenziandone la corretta, o meno, esecuzione.

- *Report Manager*: componente software che ha il compito di gestire la richiesta di visualizzazione dei prospetti e dati.

- *Multimedia Manager*: componente software che permette l'iterazione dinamica delle componenti planimetriche e video dei siti gestiti.

- *Remote Site Viewer*: componente software che esegue la ricerca del sito configurato in base dati. Occorre permettere la ricerca inserendo un numero minimo di caratteri identificativi consecutivi del sito. La ricerca deve permettere la visualizzazione di tutti i siti, per nome o codice, che contengono i caratteri inseriti.

Remote Configurator

È il sistema utilizzato dai gestori tecnici della Control Room. Tale applicativo deve permettere la configurazione nel sistema PSIM, in particolare di tutte le componenti afferenti i diversi sottosistemi di sicurezza locali. I dati, tramite esso configurati, sono utilizzati e gestiti dagli operatori, permettendo la corretta identificazione e gestione delle dinamiche di sicurezza dei singoli siti remoti monitorati.

Una corretta progettazione della parte grafica facilita l'attività tecnica di inserimento e configurazione del sistema.

PSIM Configurator

È il sistema utilizzato per la configurazione interna dello PSIM. Tale applicativo deve permettere la configurazione delle componenti interne al sistema PSIM, ivi compresi tutti i server e le workstation necessarie al funzionamento. Esso, inoltre, deve contenere un Dictionary interno, caratterizzante tutte le componenti del sistema, capace di definirle univocamente, oltre a prevedere dei tool interni amministrativi per l'analisi e il monitoraggio del sistema.

Descrizione generale dello PSIM

Di seguito una descrizione generale delle funzionalità e delle modalità operative di un sistema Bank PSIM. Lo schema precedente consiglia, per un miglior utilizzo del sistema da parte degli operatori di Control Room, l'utilizzo di 4 differenti monitor. Il sistema, naturalmente, funziona correttamente con un diverso numero di monitor disponibili.

Di seguito una descrizione funzionale ipotizzando l'utilizzo dei 4 monitor.

Main Window

- ❖ Gestione dei livelli di accesso secondo differenti livelli gerarchici.
- ❖ Profilatura utenti, associazione gruppi siti monitorati.
- ❖ Finestra di Ricezione e Gestione eventi.
- ❖ Cruscotto di monitoraggio siti e agenzie.
- ❖ Monitoraggio e gestione comandi.
- ❖ Sistema di reportistica, documentazione analitica della attività del sistema.
- ❖ Finestra di ricerca dinamica sito.

Events Window

- ❖ Finestra dedicata di Ricezione e Gestione eventi
- ❖ Applicazione filtri dinamici agli eventi.
- ❖ Gestione secondo priorità e livelli di gravità (escalation degli allarmi).
- ❖ Correlazione tra eventi e immagini associate (live e registrate).
- ❖ Gestione integrata delle procedure di Sicurezza.
- ❖ Gestione dinamica comandi ai siti.

Maps Window

- ❖ Rappresentazione grafica delle informazioni attraverso l'impiego di icone dinamiche, pulsanti, animazioni.
- ❖ Mappe grafiche pluri-livello con navigazione interno siti.
- ❖ Mappe grafiche e interfaccia operatore customized.
- ❖ Gestione dinamica visualizzazione eventi su mappa dell'area, realizzazione comandi ed eventi.
- ❖ Monitoraggio, gestione e comando sito tramite mappa grafica.

Video Window

- ❖ Flussi video visualizzati su singolo monitor in modalità "matrice virtuale".
- ❖ Visualizzazione automatica flussi video associati a eventi prioritari.
- ❖ Piano delle video ispezioni programmate e correlate con i fattori di rischio.
- ❖ Visualizzazione, ricerca ed estrazione di immagini registrate.

Funzioni Bank PSIM evolute

I primi sistemi PSIM bancari, sistemi di centralizzazione allarmi, furono realizzati con l'obiettivo prevalente di monitorare le segnalazioni (allarmi, manomissioni e guasti)

provenienti dalle centrali di allarme installate nelle agenzie. Per molti anni non vi è stata integrazione tra i sistemi di centralizzazione e i sistemi video. Inizialmente a causa della modalità di registrazione analogica del video, successivamente a causa dei primitivi sistemi di compressione delle immagini poco efficienti.

A partire dalla seconda metà dello scorso decennio, grazie al miglioramento della compressione video, in particolare attraverso i codec MPEG4, e all'ampliamento della banda di trasmissione dati, si è iniziata l'integrazione del video nei sistemi Bank PSIM.

Ad oggi, un sistema Bank PSIM collaudato permette almeno le seguenti funzioni video.

- ❖ Correlazione tra eventi e video, con visione, a richiesta dell'operatore, del video live delle telecamere correlate all'evento.
- ❖ Proiezione in automatico, senza intervento dell'operatore, del video live delle telecamere correlate a un evento prioritario.
- ❖ Proiezione, a richiesta dell'operatore, del video registrato delle telecamere correlate a un evento di allarme.
- ❖ Richiesta dall'operatore autorizzato del download, di un qualsiasi intervallo temporale, purché nei limiti di legge, delle immagini registrate da una o più telecamere.
- ❖ Richiesta di video ispezioni periodiche, ad esempio in caveau, locali cassette, ecc.

Un'ulteriore evoluzione dei sistemi PSIM bancari, iniziata da pochi anni e in stretta correlazione con i sistemi di sicurezza locali, prevede l'integrazione di sottosistemi di sicurezza fisica

Gestione e Monitoraggio siti a rischio elevato

Non tutti i siti remoti hanno la stessa rilevanza: esistono siti, agenzie bancarie, che hanno una maggiore rilevanza dal punto di vista della sicurezza, sia per la quantità di denaro gestita, sia per la funzione caveau e/o cassette di sicurezza, sia perché dislocate in aree geografiche a maggior rischio sicurezza. Risulta quindi opportuno differenziare la modalità di gestione di tali agenzie classificate a "Maggior Rischio Sicurezza" rispetto alla totalità delle agenzie monitorate, almeno in determinati intervalli temporali, che, usualmente, coincidono con l'orario di apertura dell'agenzia.

Il sistema Bank PSIM implementa la funzionalità per la quale è possibile configurare, per tali agenzie a "Maggior Rischio Sicurezza" e per definiti intervalli temporali, la loro gestione automatica a un particolare operatore o a gruppi di operatori (definiti operatori alta sicurezza).

In funzione delle esigenze del cliente, sarà possibile, nell'intervallo temporale indicato:

1. rimuovere il monitoraggio di tali agenzie dalla gestione della Control Room, associandola esclusivamente all'operatore o operatori incaricati;

- aggiungere il monitoraggio all'operatore o operatori incaricati, permettendo ai restanti operatori della Control Room la visione degli eventi e segnalazioni di tali agenzie.

Quale sia la modalità di configurazione prescelta, il sistema Bank PSIM deve prevedere un algoritmo di assegnazione tale che, in assenza di login da parte dell'operatore assegnatario, distribuisca in automatico le filiali non monitorate ai restanti operatori alta sicurezza o, in assenza totale di essi, agli operatori standard di control room.

Gli operatori alta sicurezza, usualmente, monitorano un numero ristretto di agenzie a "Maggior Rischio Sicurezza", e per esse operano:

- gestendo tutti gli eventi (segnalazioni e allarmi) dei soli siti "Maggior Rischio Sicurezza" correlati con il particolare operatore alta sicurezza;
- visualizzando su monitor gli allarmi prioritari;
- eseguendo la telegestione e il telecontrollo aree, zone, sensori e attuatori;
- visualizzando per ciascuna agenzia almeno una telecamera del salone;
- proiettando nel sito remoto la Guardia Virtuale;
- monitorando lo stato degli accessi al sito e degli eventi tecnologici;
- gestendo remotamente le serrature elettroniche associate ai mezzi forti;
- monitorando e gestendo le correlazioni generate nel sito e nel server PSIM.

La Figura sottostante evidenzia l'attività del sistema PSIM nella gestione dedicata a un "operatore di alta sicurezza" e relativamente alle agenzie a "Maggior Rischio Sicurezza".



Figura 89. Attività di un PSIM

Diagnosi dei Sistemi e tracciatura eventi

Tutti i sistemi PSIM, in particolare quelli di un sistema critico come un sistema bancario, devono evidenziare immediatamente qualsiasi anomalia o fallimento dei servizi applicativi, processi o risorse hardware ad essi collegati.

Il principio fondamentale deve essere che tutti i componenti connessi al sistema devono essere monitorati. È quindi necessario evidenziare a tutti gli operatori collegati al sistema con l'applicativo Client Application la problematica riscontrata.

Tale problematica deve essere evidenziata a video tramite:

- evento di allarme, indicante la tipologia di servizio, applicativo, processo o sistema in difficoltà
- etichetta colorata in area dedicata dell'interfaccia, visibile all'operatore e di colorazione tale da indicare:
 - tutti i componenti correttamente funzionanti (solitamente di colore verde);
 - – presenza di almeno un componente non funzionante ma sistema ancora correttamente funzionante (solitamente di colore giallo);
 - presenza di almeno un componente non funzionante con sistema non funzionante (solitamente di colore rosso).

Nei sistemi Bank PSIM, l'etichetta colorata può essere unica e indicativa dello stato del sistema. In tal caso, l'operatore deve poter velocemente ottenere i dettagli di tutti i componenti del sistema, al fine di identificare immediatamente il componente non funzionante.

Altro aspetto fondamentale di un PSIM Server System è rappresentato dalla sua capacità di memorizzare, tracciare e correlare tutte le informazioni provenienti da tutti i siti monitorati.

Il PSIM Server System implementa un sistema completo di event logging delle informazioni e un software in grado di estrapolare ed elaborare tali informazioni in ordine ed esaudire le richieste provenienti sia dall'operatore di Control Room, relative al monitoraggio di un sito o agenzia, sia del tecnico di sala, relative al monitoraggio del sistema.

L'operatore di Control Room, al fine di attivare le migliori azioni di contrasto a eventi insorti nel sito monitorato, ha la necessità di comprendere perfettamente la condizione di sicurezza del sito.

A tal fine deve essere coadiuvato da un sistema software di reportistica in grado di fornirgli a video e su richiesta, le informazioni storicizzate (event logging), permettendogli di effettuare filtri basati su:

- data/ora di inizio e fine;
- tipologia dell'elemento;
- tipologia dell'evento;
- famiglia/gruppo a cui è associata la segnalazione/evento.

Il tecnico di sala ha il compito di monitorare il comportamento del sistema in ogni sua componente, per cui ha la necessità di visualizzare, oltre ai report disponibili per l'operatore, anche report delle segnalazioni interne allo PSIM Server System, sia segnalazioni generate tra servizi, applicativi e server sia segnalazioni generate internamente al sistema per la gestione dei siti remoti; report di segnalazioni ed eventi trasversali a più siti locali. Ad esempio ricorrenza di un dato evento, in un dato intervallo temporale, in uno specifico insieme di siti; report dei comandi inviati a uno o più siti remoti. Con possibilità di individuare per uno specifico comando, in un dato intervallo temporale, i siti dove esso è stato inviato e gli utenti che hanno eseguito il comando.

Business Continuity e Disaster o Service Recovery

Un sistema o un'infrastruttura si dicono critici se un loro fallimento (cioè l'impossibilità di fornire il servizio, o i servizi, per il quale sono stati realizzati) può avere conseguenze critiche su persone, ambiente, beni (in tal caso si parla di sistema *safety critical*) o sulle finanze (sistema *business critical*). Sono ad esempio infrastrutture critiche le telecomunicazioni, i trasporti, il sistema elettrico, gli acquedotti, la finanza, la distribuzione del gas, ma anche il sistema di pilotaggio di un treno o di un aereo, il controllo elettronico di stabilità di un'automobile, il sistema di telecomunicazioni di un satellite.

Un sistema Bank PSIM è un sistema critico, sia per la safety (si pensi ai rischi delle persone in caso di rapina in banca) sia, naturalmente, per le finanze.

Fondamentale per un funzionamento corretto ed efficace di tali sistemi è la capacità di analizzarne le caratteristiche sia prestazionali che di sicurezza, disponibilità o affidabilità che ci attestino l'adeguatezza di tali sistemi dal momento che ad essi sono demandate mansioni sempre più delicate e critiche.

Si rende quindi necessario lo studio di tecniche che siano volte alla misurazione del grado di affidabilità (*dependability*) di un sistema, ad esempio quante volte esso fallisce durante una sua esecuzione, quanto sono gravi i suoi fallimenti e quanto tempo è necessario per ripristinare un corretto funzionamento dello stesso.

Il concetto di affidabilità (*dependability*) non è di facile formalizzazione. In effetti, essa è un attributo di qualità, composto a sua volta dai seguenti attributi (*dependability attributes*).

- **Availability (disponibilità):** definita dalla Recommendation E.800 della International Telecommunications Union (ITU-T) come la capacità di un sistema di essere in uno stato per eseguire una funzione richiesta in uno specifico istante di tempo o entro un certo istante di tempo in uno specifico intervallo, assunto che eventuali risorse esterne necessarie all'esecuzione della funzione siano disponibili.
- **Reliability (affidabilità):** definita dall'ITU-T Recommendation E.800 come la capacità di un sistema di eseguire una data funzione per un certo intervallo di tempo.

- **Safety (sicurezza di utenti o ambiente):** definita come l'assenza di conseguenze catastrofiche su utenti o sull'ambiente in caso di fallimento del sistema.
- **Integrity (integrità):** rappresenta l'assenza di alterazioni improprie del sistema.
- **Maintainability (manutenibilità):** indica la possibilità di effettuare manutenzione sul sistema in seguito all'occorrenza di fallimenti attraverso l'applicazione di una strategia di riparazione (ad esempio, la riparazione o la sostituzione di un componente rotto).
- **Security:** è composta a sua volta da tre attributi:
 - **Availability:** disponibilità del servizio offerto dal sistema esclusivamente per utenti non autorizzati;
 - **Confidentiality:** prevenzione dalla diffusione non autorizzata di informazioni;
 - **Integrity:** prevenzione da alterazioni improprie dello stato del sistema.

Le cause che possono portare un sistema a fornire un servizio non corretto, quindi fallire (service failure), sono molteplici e possono manifestarsi in qualsiasi fase del suo ciclo di vita. Esempi di fallimento sono guasti hardware, errori in fase di progettazione hardware o software, interventi errati di manutenzione.

Una service failure è quindi un evento in corrispondenza del quale si verifica una transizione da servizio corretto a servizio non corretto mentre l'evento in corrispondenza del quale si verifica la transizione inversa viene detto service recovery.

Un sistema Bank PSIM, essendo *business critical* e *safety critical* deve assicurare una elevata reattività nel ripristinare il corretto servizio del sistema, assicurando una propria continuità operativa (*Business Continuity* e *Service Recovery*). Tali concetti possono essere soddisfatti implementando delle ridondanze locali su tutti i componenti critici del sistema.

Diversamente, volendo soddisfare anche problematiche di *Disaster Recovery*, occorre prevedere un insieme di misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione dei servizi, a fronte di gravi emergenze, dovute a calamità naturali, climatiche o di natura umana (errori umani o atti di terrorismo), che ne intacchino la regolare attività. Occorre pertanto prevedere dispositivi tecnologici e logistico/organizzativi alternativi, attivi e funzionanti ma posti in stand by, presenti in differente location geografica.

5.6.1 Interfacce piattaforma

Per alcuni degli scenari di allarme a seguito di potenziale attacco, sono stati definiti i relativi activity diagram, use case diagram e sequence diagram che illustrano il comportamento degli attori e l'uso della piattaforma in tali casi nonché i mock-up delle interfacce web

Di seguito saranno illustrate una serie di possibili interfacce, da considerare come prototipi, da utilizzare in fase sviluppo della piattaforma in conformità a quanto visto precedentemente sulla sequenza del trattamento degli eventi.

La possibilità di gestire, tramite un'unica interfaccia, tutti i sistemi coinvolti nella sicurezza dell'area permette di massimizzare l'efficacia dei sistemi e l'efficienza delle operazioni.

La disponibilità di un'architettura flessibile ed aperta comprensiva di una politica di gestione degli accessi ad autorizzazioni differenziate, la possibilità del raggruppamento dei sensori per zone e la gestione degli stessi differenziabile su calendari personalizzabili unitamente ad un'architettura client/server comprensiva di unità server di fail-over rendono la piattaforma la soluzione ideale per il controllo di zone sensibili ed ad alto rischio.

La piattaforma deve prevedere l'accesso al programma per mezzo di un'autenticazione basata su username a password.

Il modulo di autenticazione permette una flessibile politica di accesso differenziando tra utenti amministratori ed operatori, con possibilità di personalizzazione dei permessi sulla base del gruppo, del ruolo o del singolo utente.

Azionando quasi esclusivamente il mouse, un operatore della sicurezza, senza competenze informatiche, seguirà il percorso procedurale previsto per ogni tipo di evento utilizzando tutte le informazioni contestuali che la piattaforma concentra e organizza sul posto di lavoro. A colpo d'occhio, l'operatore può avere tutte le informazioni necessarie per eseguire ciò che la procedura di trattamento dell'evento ha previsto nella fattispecie sia in fase di verifica dell'attendibilità dell'evento che nel corso dell'intervento. Se, come spesso accade, non si tratta di un evento di allarme, il risultato sarà stato ottenuto senza impegnare risorse inutilmente o a sproposito.

Questo può avvenire poiché la piattaforma, attraverso la base di conoscenza, sarà in grado di imparare attraverso le varie scelte effettuate nel tempo dall'operatore, e quindi assegnare un livello di allarme maggiore o minore ai vari avvisi che arrivano.

Vediamo di seguito il dettaglio di come potrebbero essere le interfacce rispetto allo stato degli eventi e ai possibili scenari che si possono incontrare.

Di seguito sono presentate una serie di possibili soluzioni per la visualizzazione dei dati e dei comandi da utilizzare per la catalogazione degli allarmi.

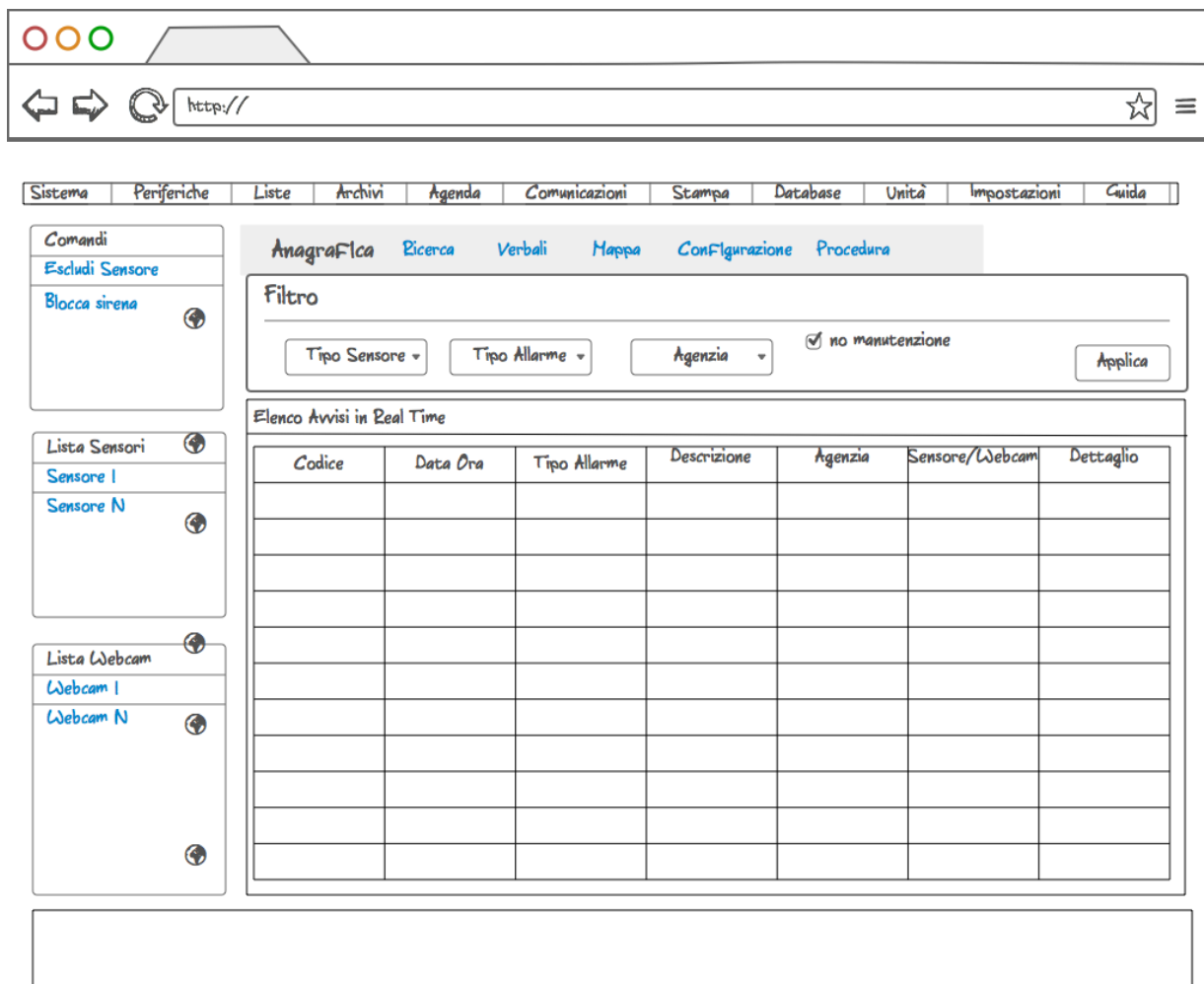


Figura 90. Mock-up piattaforma operatore

Nella figura precedente è rappresentata la schermata principale della piattaforma. La pagina visualizza l'elenco degli allarmi con il relativo stato e dei pulsanti che consentono di eseguire una serie di comandi per il controllo e la gestione dell'intervento.

Questa è stata suddivisa in diverse sezioni che andiamo ad esplicitare.

- Menù principale: è composto da una serie di voci che riguardano le funzionalità che possono essere richiamate in modo diretto.
- Menù di sinistra: elenco dei comandi, dei sensori e delle webcam organizzati per tipologia.
- La parte centrale della pagina invece viene utilizzata per visualizzare l'elenco degli allarmi che arrivano sul cruscotto. L'allarme viene visualizzato all'operatore con una serie di attributi associati quali: codice, data e ora, tipo allarme, descrizione, agenzia dove si è verificato, tipologia di sensore, eventuale dettaglio.

Una seconda pagina che rappresenta la visualizzazione delle webcam che trasmettono flussi video dalle varie agenzie è di seguito visualizzata.

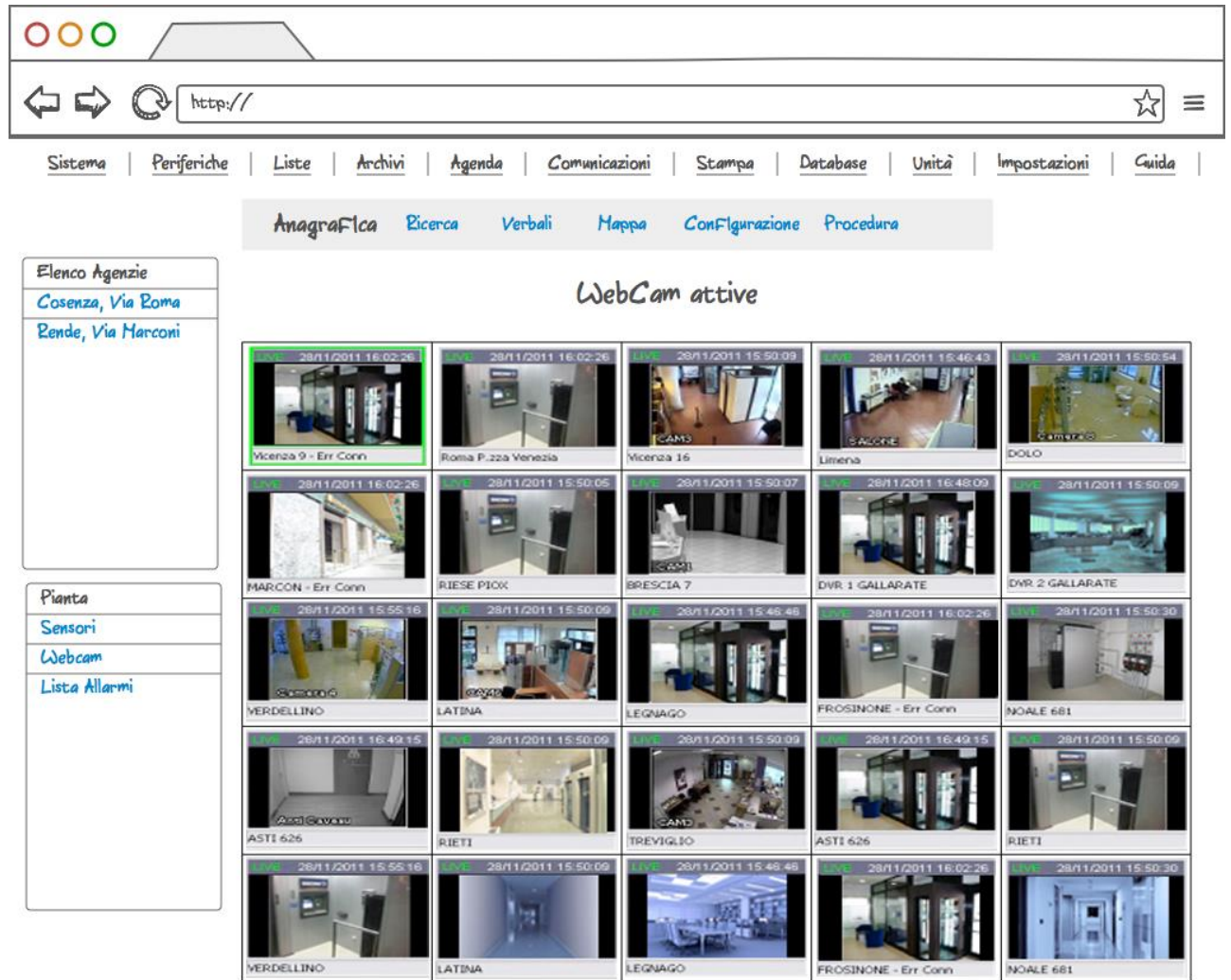


Figura 91. Mock-up videosorveglianza

In questa pagina l'operatore visualizza le webcam delle varie agenzie e cliccando su una singola cella potrà vedere il dettaglio della scelta effettuata.

Un esempio di dettaglio a cui potrà accedere è la visualizzazione della pianta di una singola agenzia che possiamo vedere di seguito.

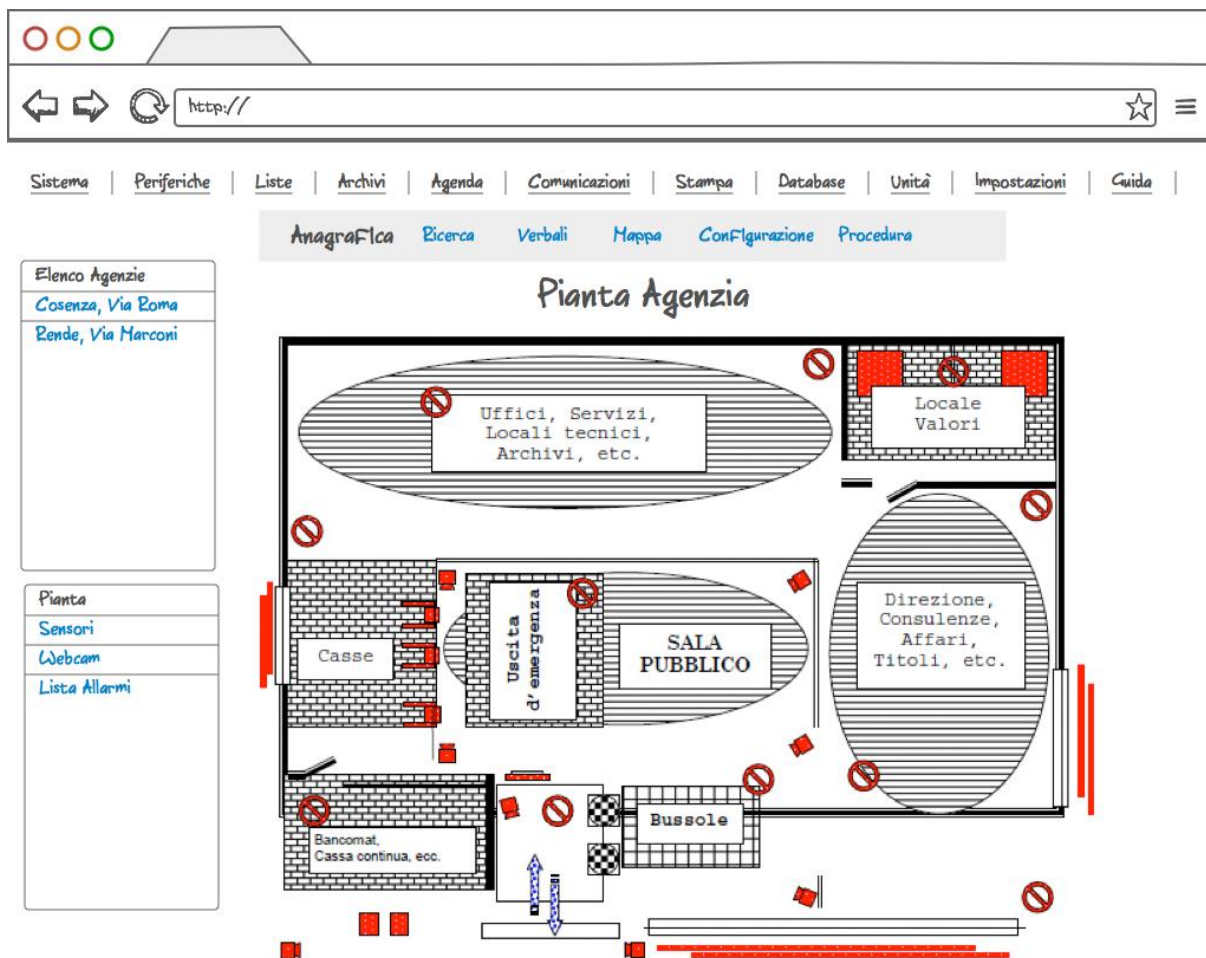


Figura 92. Mock-up visualizzazione interattiva pianta

Anche in questo caso l'operatore può cliccare su un sensore presente sulla piantina e visualizzare il dettaglio di ciò che ha scelto.



Figura 93. Esempio di scenario reale



Figura 94. Esempio di Control Room



Figura 95. Esempio pannello operatore

Il presente diagramma mostra, in maniera del tutto generale, le attività da seguire in caso di allarme presso una delle filiali afferenti alla piattaforma.

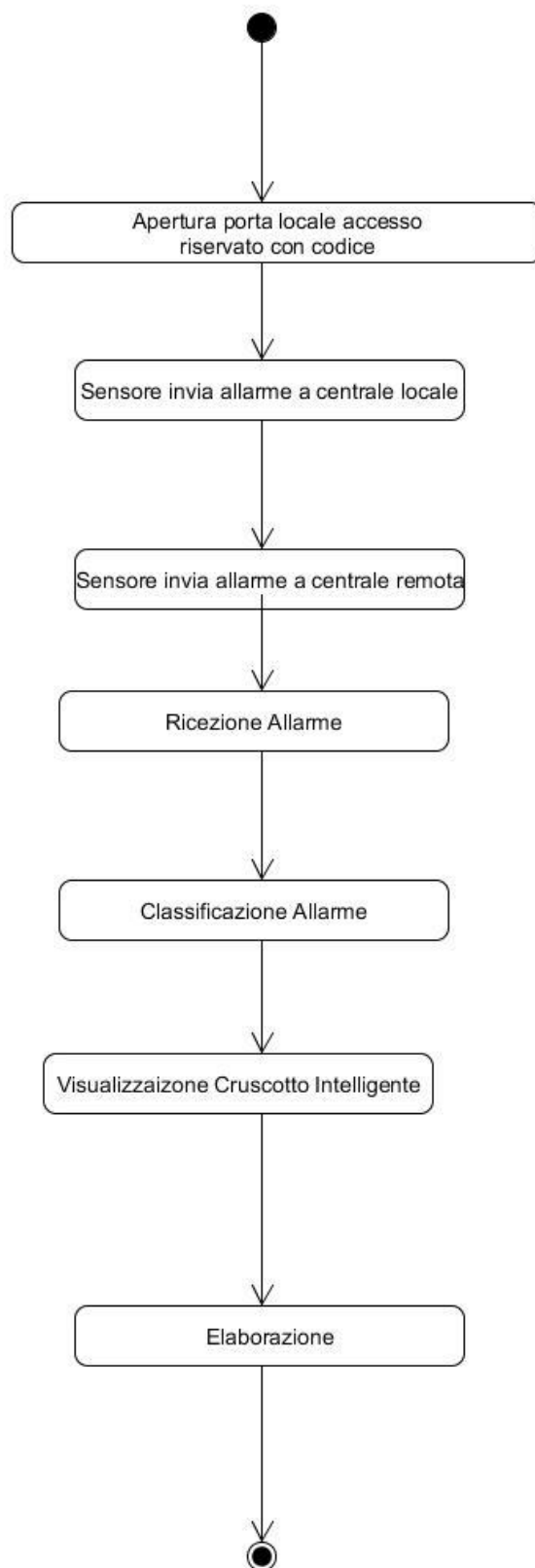


Figura 96. Flusso logico segnalazione allarme

Nel caso si verifichi un allarme, il sistema IPS prevede la classificazione di tale allarme. La classificazione avviene mediante l'esecuzione degli algoritmi di classificazione e la decisione, ultima, dell'operatore circa l'eventualità di contattare le forze dell'ordine in caso di un vero allarme.

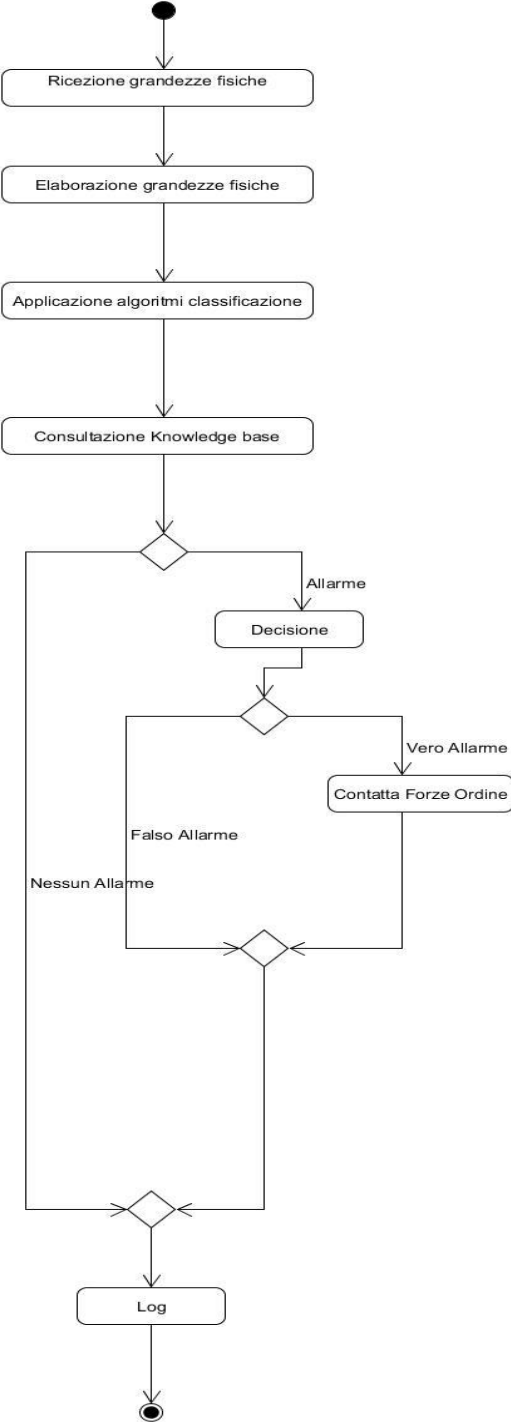


Figura 97. Flusso logico - Classificazione della segnalazione

A ciascuna filiale nonché ad ogni singolo allarme il sistema associa un *alert*. Tale *alert* viene associato dal sistema a seguito di una opportuna associazione ad opera del *Decision Manager*. Esso, consultando la KB, in base agli eventi pregressi effettua la classificazione.

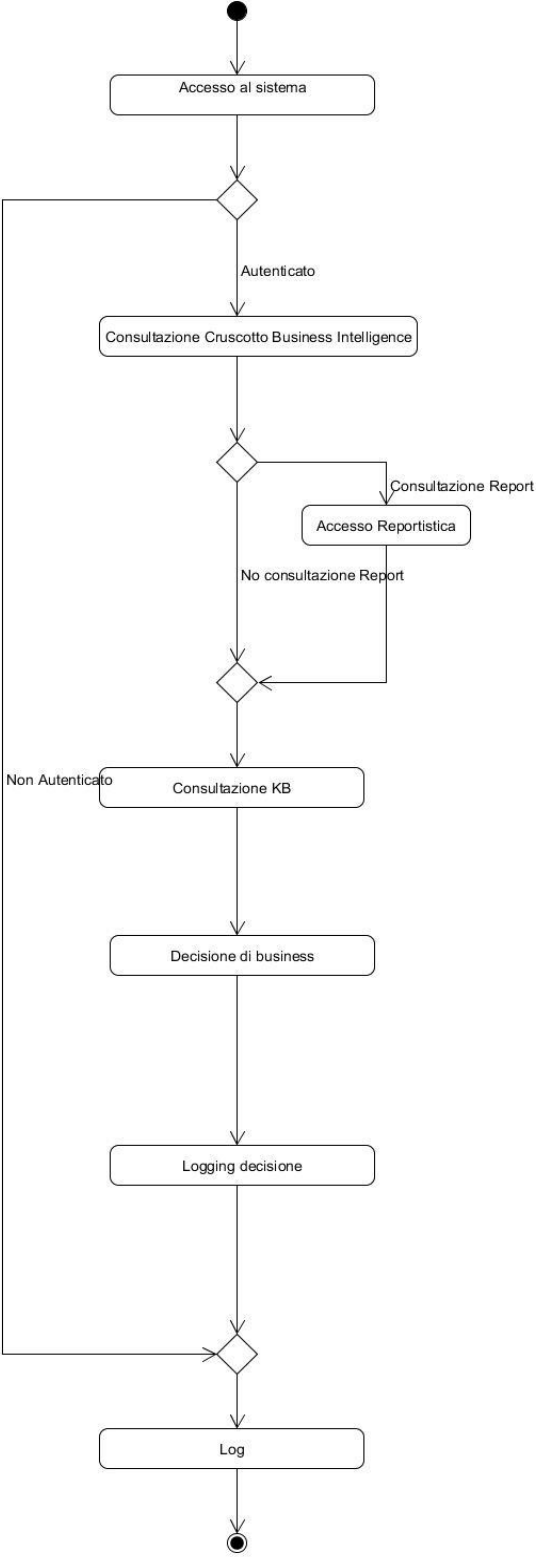
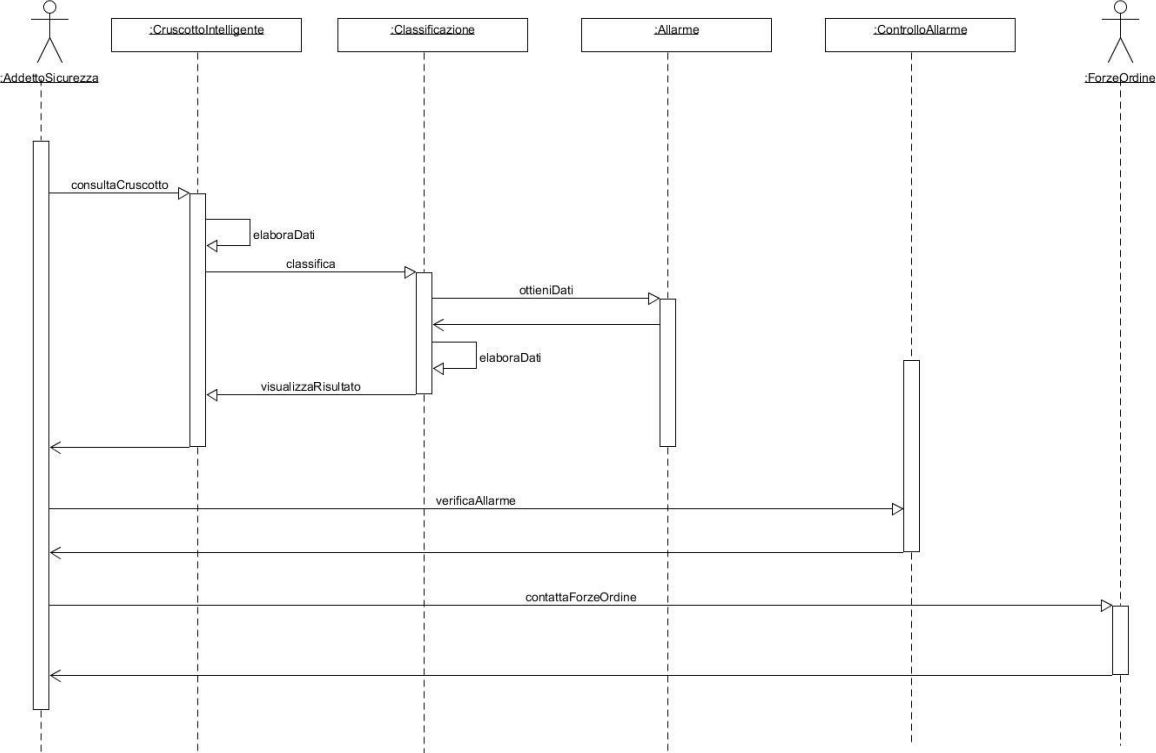


Figura 98. Flusso logico decision manager

Qualora si verifichi un allarme che comporti la necessità di contattare le Forze dell'Ordine, il sistema prevede il seguente scenario.



L'invio di un segnale di allarme, da parte di una delle filiali appartenenti alla piattaforma IPS, comporta la seguente sequenza di azioni ed i relativi attori/classi interessati.

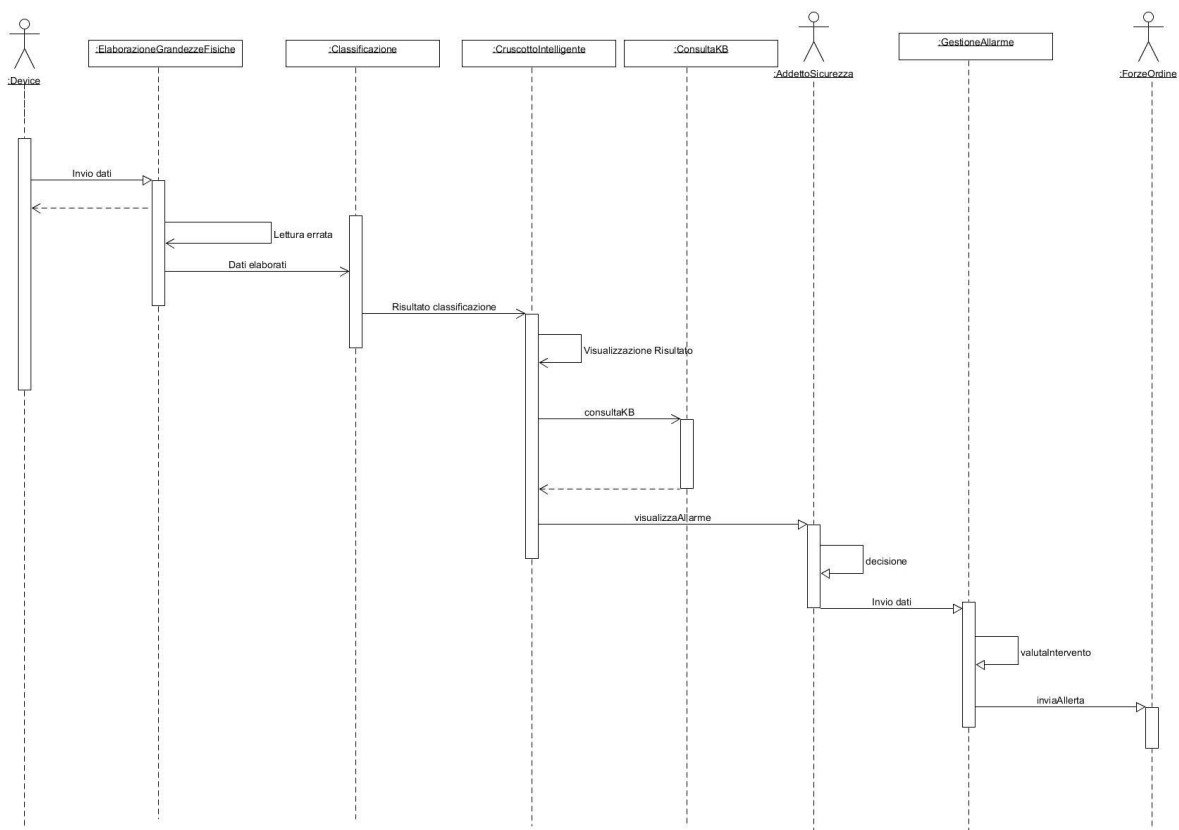


Figura 99. Sequence Diagram

5.7 Performance Analysis: un confronto tra la situazione attuale e la soluzione proposta

L'adozione di un IPS è giustificata da un punto di vista aziendale in quanto migliora le prestazioni del processo in termini di efficienza e di efficacia contro gli attacchi criminali.

Riduzione dei costi. Il livello di automazione che l'adozione di IPS può dare a un gruppo bancario dipende da variabili multiple e da esigenze specifiche. L'adozione di un IPS consente al gruppo bancario di ridisegnare il monitoraggio delle dipendenze bancarie. Ciò comporta l'automazione delle attività svolte dalla sala controllo riducendo il numero di guardie di sicurezza, riducendo il numero di guardie armate per la dipendenza bancaria e eliminando i sensori perimetrali / volumetrici. Un IPS più complesso può sostituire le misure di prevenzione tecnologica (eliminando i rilevatori metallici, chimici ed esplosivi e / o sostituendo il sistema di identificazione) se sono attivi specifici sensori e / o moduli di riconoscimento dei volti. Chiaramente, i costi per introdurre e mantenere un IPS sono relativamente bassi se confrontati con i costi di un sistema di protezione tradizionale. Successivamente proponiamo una stima convalidata dei principali costi diretti e dei risparmi sui costi dall'adozione dell'IP. La stima dei costi iniziali è basata su valutazioni personali degli

autori che sono state ulteriormente esaminate da due consulenti esperti di IoT prima di essere inviati agli intervistati per la convalida finale.

Il costo iniziale per la creazione di una piattaforma IPS con un minimo di funzioni può variare da 5 a 10 milioni di € (costo fisso), più il costo di ogni dipendenza bancaria della rete (da 5.000 a 20.000 €). Il costo di manutenzione annuale può essere compreso tra 1 e 2 milioni di euro (per la piattaforma centrale) e da 1.000 a 5.000 € per ogni dipendenza bancaria.

Un IPS riduce a 1 il numero di guardie di sicurezza nella sala di controllo per ogni dipendenza bancaria (attualmente è 2). Questo costo non è inferiore a 30.000 € all'anno. Ci sono valori simili per le guardie armate (un massimo di 1 per ogni dipendenza bancaria, attualmente ci sono almeno 2). Dopo l'adozione di IPS, il gruppo bancario potrebbe internalizzare il servizio di sicurezza ora tipicamente esternalizzato con ulteriori risparmi per non meno di € 50.000 all'anno. Ulteriori risparmi derivano dall'eliminazione del sistema di allarme perimetrale / volumetrico.

Tali valori vanno considerati a livello aziendale. I principali gruppi bancari in Italia controllano reti di mille DIPENDENZA BANCARIA. Alla fine del 2016, la rete dei primi due gruppi bancari rappresentava 4.000 (Unicredit) e 3.900 (Intesa Sanpaolo) dipendenze bancarie; gruppi più piccoli a livello nazionale controllano reti che vanno da 500 a 2000 dipendenze bancarie. Decine di milioni di euro di risparmio dei costi possono essere ragionevolmente attesi a livello aziendale dalla creazione di IPS su scala globale.

L'IPS introduce una significativa riduzione del carico di lavoro e un ripensamento delle attività degli attori coinvolti. In primo luogo, il ruolo della CSO viene rimosso da tutti i compiti operativi legati alla valutazione del rischio della dipendenza bancaria e alla gestione REM. Queste attività sono automatizzate e eseguite dall'IPS. Il CSO è limitato alle attività manageriali e mantiene un ruolo di convalida per le decisioni proposte dall'IPS. In secondo luogo, il direttore della dipendenza bancaria smette di avere un ruolo operativo nei processi di sicurezza. Ancora una volta, le informazioni relative alle misure di protezione vengono raccolte e monitorate dall'IPS. Il personale della dipendenza bancaria deve rispettare solo le procedure di sicurezza definite dal CSO al fine di preservare la propria sicurezza e quella di altre persone della dipendenza bancaria. In terzo luogo, adottando l'IPS, i dipendenti delle dipendenze bancarie non sono tenuti a svolgere attività di monitoraggio e segnalazione relative a anomalie o attacchi criminali. Inoltre, non ci sono impatti significativi per il CPO e per il CFO né per i fornitori di soluzioni di sicurezza. Infine, un IPS consente un monitoraggio intelligente di molte dipendenze bancarie da una sala di controllo univoco centralizzata. Pertanto, il numero complessivo di guardie di sicurezza per l'intera rete di dipendenze bancarie è sensibilmente ridotto, nonché il numero di guardie armate, la cui presenza al di fuori della dipendenza bancaria diventa anche facoltativa.

Riduzione dei tempi. Il tempo complessivo del processo target dipende dalla stima del dipende del lead time, process time and waiting times associati ai processi secondari. Nella

seguinte tabella sono indicati per la situazione attuale e la situazione target dei processi P1, P4 e P5, che saranno sostanzialmente modificati dalla reingegnerizzazione, tenendo in considerazione solo gli attori contrattualmente legati al gruppo bancario (attività svolte dai membri delle forze dell'ordine e dalla Banking Association sono escluse dal calcolo). Per la situazione attuale, il tempo è calcolato in base ai valori medi di tempo di processo dati dagli intervistati, mentre, per la situazione target, le stime iniziali sono date sulla base delle valutazioni personali degli autori. I valori target sono stati ulteriormente riesaminati da due consulenti esperti di IoT prima di essere inviati agli intervistati per la convalida finale.

Sub-Processes	P1		P4		P5	
	AS IS	TO BE	AS IS	TO BE	AS IS	TO BE
Time (days)						
Lead Time	80	8	6	4	21	7
Process Time	14	4	2	1	16	5
Waiting Time	66	4	4	3	5	2

Tabella 43. Confronto Situazione AS IS (valori medi) e TO BE (stima)

È importante sottolineare che mentre il processo P1 viene eseguito una volta all'anno, alcune attività vengono ripetute molte volte ogni anno. Alcune attività appartenenti a P4 e P5 vengono svolte in qualsiasi momento in cui si verifica un evento criminale, mentre altre attività appartenenti a P4 vengono ripetute ogni volta che viene rilevata un'anomalia. Ciò significa che il risparmio di tempo su una base annuale può essere impressionante.

Informazioni corrette e aggiornate: i dati vengono raccolti direttamente dai sensori senza intervento umano e in tempo reale. Le informazioni memorizzate all'interno dell'IPS sono complete, corrette e non ridondanti. I grandi flussi di dati generati e elaborati dal CPS sono fondamentali per migliorare la produttività, ridurre i costi marginali, migliorare la qualità delle informazioni, agevolare e automatizzare i processi decisionali. La qualità del processo è senza dubbio migliorata in quanto tutti i sottoprocessi che necessitano di informazioni per prendere decisioni possono essere ricavate da quella parte dell'IPS che aggiorna la base di conoscenza e il repository dei dati.

Maggiore sicurezza. Le misure di protezione sono sempre attive poiché l'IPS consente il monitoraggio continuo del loro stato di funzionamento e richiede un intervento tempestivo in caso di danni. I dati continui raccolti su attacchi criminali (come tipologia, modalità, posizione dell'attacco e disponibilità di nuove misure di protezione) da tutte le dipendenze del gruppo bancario consentono al REM di essere più efficace. L'IPS dispone di capacità predittive sulla posizione, il tempo e le modalità di attacchi criminali futuri e fornisce indicazioni sulla prevenzione e la reazione al delitto anche senza modificare una misura di protezione. Il modulo di apprendimento macchina consente al sistema di ridurre in modo.

Di seguito alcuni scenari di intervento della piattaforma

scenario 1: riconoscimento volti sospetti e contromisure successive – modulo di smart face recognition e tracciamento

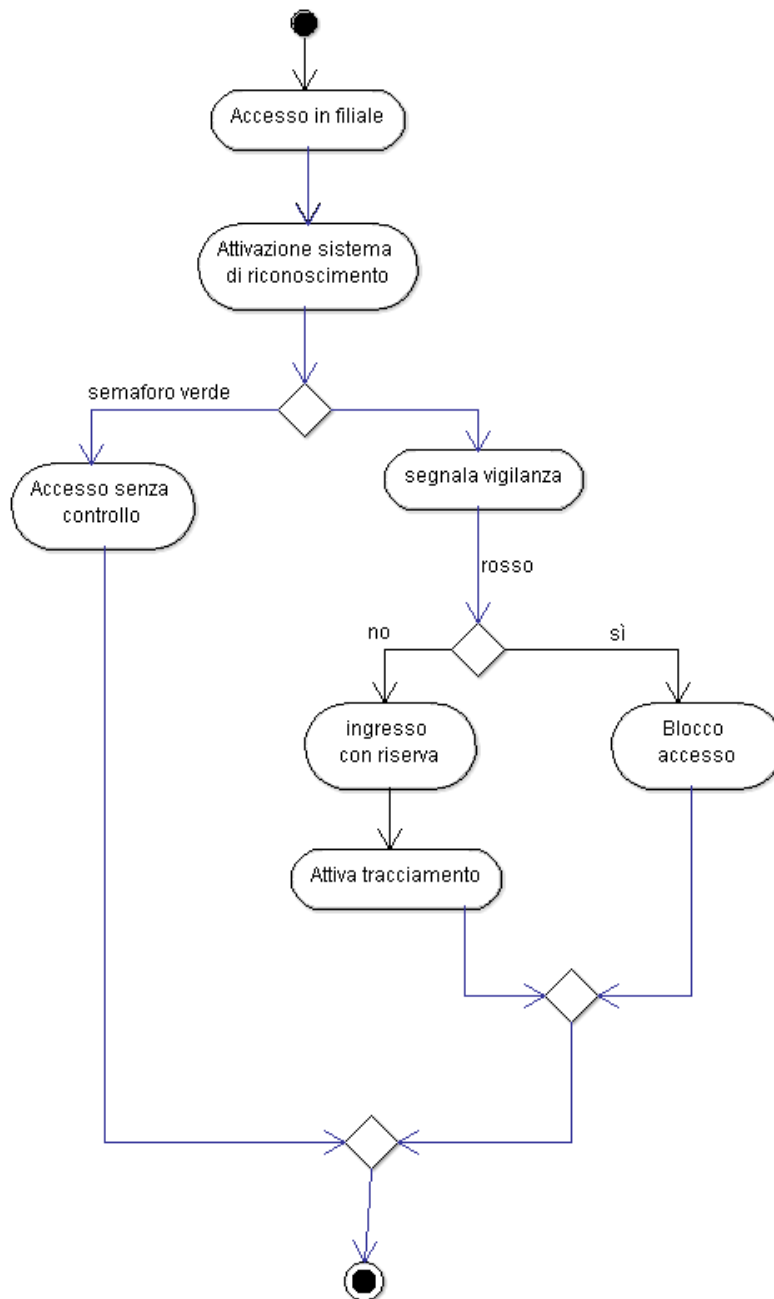


Figura 100. Scenario Smart Face Recognition

ATTIVITÀ 1. Accesso in filiale. Si presenta una persona all'ingresso della filiale. La presenza viene monitorata dalla telecamera che attiva così il sistema di riconoscimento.

INPUT: identificazione sagoma in movimento

OUTPUT: rilevazione persona

ATTORI: persona (cliente, dipendente o malvivente), Piattaforma IPS (modulo smart face recognition)

ATTIVITÀ 2. Attivazione sistema di riconoscimento. Il sistema entra nel DB per ricercare la persona che sta per accedere in filiale. Se la persona è conosciuta come non pericolosa (cliente della banca, dipendente) allora si attiva il "semaforo verde" (assenza di pericolo specifico), nel caso in cui invece la persona viene riconosciuta come potenzialmente pericolosa si ricorre ad ulteriori accertamenti.

INPUT: rilevazione persona

OUTPUT: segnale di sicurezza

ATTORI: piattaforma IPS (modulo smart face recognition)

ATTIVITÀ 3. 3a. Accesso senza controllo o 3b. Segnala alla vigilanza. L'attività 3 dipende dal segnale in output dell'attività 2. Se il segnale restituito ha dato semaforo verde viene consentito l'accesso (attività **3a**) e si chiude il processo. Nel caso in cui, invece, il segnale non risulta verde, il sistema segnala la persona alla vigilanza (attività **3b**).

INPUT: segnale di sicurezza dell'attività 2

OUTPUT **3a**: apertura porta

OUTPUT **3b**: notifica alla vigilanza

ATTORI: Persona, piattaforma IPS

ATTIVITÀ 4. 4a. Ingresso con riserva o 4b. Blocco accesso. L'attività 4 dipende dall'attività **3b**, in particolare in seguito alla segnalazione inviata alla vigilanza, quest'ultima restituisce l'anagrafica del soggetto in esame. Se viene restituito "semaforo rosso" si blocca l'accesso (attività **4b**) e il processo termina. Se il semaforo non è rosso (semaforo giallo) viene consentito l'ingresso con riserva (attività **4a**).

INPUT: Dati persona in esame

OUTPUT 4b: anagrafica di persona pericolosa

OUTPUT 4a: anagrafica persona non schedata tra i pericolosi, ma potenzialmente pericolosa.

ATTORI: Piattaforma IPS

ATTIVITÀ 5. Attivazione tracciamento. Dopo aver consentito l'accesso con riserva si avvia il tracciamento tramite telecamera della persona e termina il processo.

INPUT: persona potenzialmente pericolosa

OUTPUT: esito tracciamento

ATTORI: piattaforma IPS

scenario 2: riconoscimento di attacco ad un ATM tramite oggetto contundente tipo sbarra o arma da fuoco (da WP4) – modulo di gesture recognition

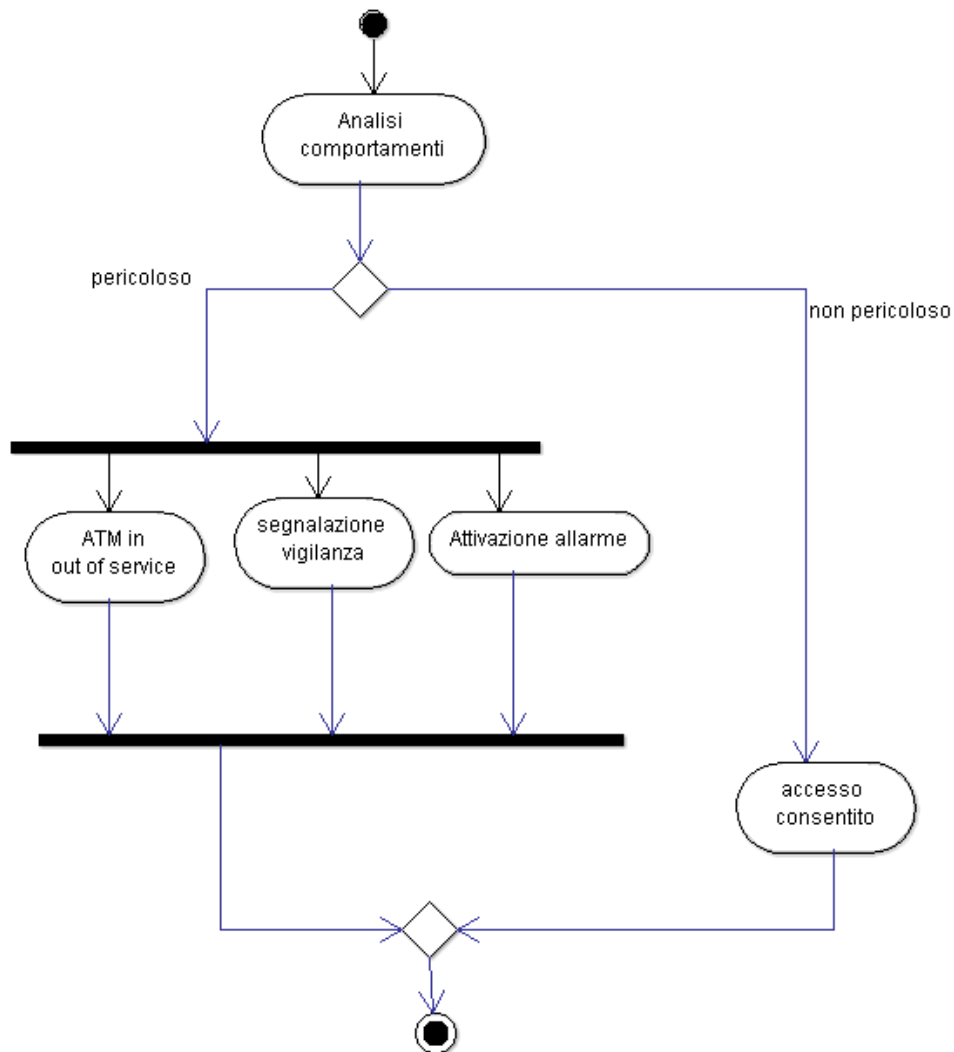


Figura 101. Scenario Gesture Recognition

ATTIVITÀ 1. Analisi comportamenti. Si analizza il comportamento del soggetto presente in ATM. Se dall’analisi da parte del sistema di gesture recognition evidenzia che il comportamento identificato è pericoloso allora si passa alle attività 2,3,4 le quali vengono

svolte parallelamente. Nel caso in cui invece l'esito dell'analisi rileva un comportamento non pericoloso si passa all'attività 5.

INPUT: azione

OUTPUT 1: segnale di pericolo

OUTPUT 2: segnale positivo

ATTORI: Piattaforma IPS (modulo gesture recognition)

ATTIVITÀ 2, 3, 4. ATM in out of service (attività 2). Se l'esito dell'attività 1 ha riscontrato un comportamento pericoloso il sistema mette l'ATM fuori servizio. Parte l'allarme (attività 4) e viene inviato il segnale alla vigilanza (attività 3) e si chiude il processo.

INPUT: segnale di pericolo (output 1)

OUTPUT: contromisure

ATTORI: piattaforma IPS

ATTIVITÀ 5: Accesso consentito. Se l'esito dell'analisi di gesture recognition ha individuato un comportamento non pericoloso viene consentito l'accesso e si chiude il processo.

INPUT: segnale positivo

OUTPUT: atm in servizio

ATTORI: piattaforma IPS

Considerazioni Conclusive

Il fenomeno emergente dell'IoT sta introducendo una notevole discontinuità tecnologica che sta rimodellando significativamente il modo in cui viviamo e lavoriamo. Tuttavia, troppo di sovente il fenomeno viene considerato soltanto come il banale risultato dello sviluppo della tecnologia, mentre non viene preso in opportuna considerazione la componente di discontinuità rappresentata dalle potenzialità di sviluppo che sono state messe a disposizione degli utilizzatori di tecnologia e, in particolar modo, alle possibilità offerte dalle tecnologie nell'ambito della revisione dei processi aziendali. La tecnologia non può essere relegata al ruolo di mero strumento di supporto e di "accelerazione" di processi spesso vecchi e inefficienti. Se quindi vi è stata una forte discontinuità negli "strumenti" disponibili, questa non sempre si è tradotta in una discontinuità nello svolgimento dei processi cui venivano applicati, cioè nella finalizzazione di tali strumenti ad una revisione e riorganizzazione dei processi su basi di maggiore efficienza ed efficacia.

In questo nuovo contesto di "tecnologia diffusa" vi sono alcuni aspetti che vanno considerati: innanzitutto la tecnologia che diviene, in un certo senso, sempre più "inclusa" negli oggetti, ricoprendo un ruolo sempre più abilitante funzioni a elevato valore aggiunto non direttamente derivanti dalla tecnologia in sé, ma dalle caratteristiche degli oggetti connessi; dalla "tecnologia diffusa", cioè presente "ovunque", e dalla possibilità di far comunicare "qualsiasi oggetto con qualsiasi altro" nasce la possibilità di sviluppare "sistemi" assolutamente nuovi, con caratteristiche oggi ancora non completamente note: saranno quindi disponibili oggetti "intelligenti" che costituiranno sistemi "intelligenti", superando anche la "disomogeneità" di genere e funzionale degli oggetti stessi.

Attualmente interagiamo continuamente con oggetti intelligenti, al fine di ottenere servizi che rendono la vita di tutti i giorni più semplice e più sicura, riducendo lo sforzo cognitivo necessario ad interagire con l'ambiente circostante. Gli "smart objects", ovvero oggetti fisici supportati da tecnologie elettroniche che li rendono connessi e "intelligenti", sono capaci di rilevare, registrare ed interpretare le azioni che si stanno svolgendo nell'ambiente circostante, ed inoltre sono in grado di comunicare tra loro e con le persone. Questi oggetti costituiscono degli elementi cardine per i cosiddetti "smart environment", ovvero ambienti capaci di acquisire ed applicare conoscenza al fine di migliorare l'esperienza e garantire la sicurezza delle persone. Smart objects e Smart Environments rappresentano componenti fondamentali del cosiddetto Internet of Things ed utilizzano uno standard di comunicazione per fornire servizi context-aware basati su interazioni esplicite (su input dell'utente) o implicite (quando gli smart object riconoscono le azioni dell'utente). Per le aziende diventa di fondamentale importanza capire il potenziale dell'IoT al fine di gestire i loro processi di business e la loro strategia tecnologica (Del Giudice, 2016 a, p. 2). L'adozione di queste nuove tecnologie va al di là della semplice automazione di processo (Forrester, 2015). I dati generati dai processi di IoT hanno il potenziale sia per migliorare la produttività aziendale,

per la riduzione dei costi marginali e la semplificazione ed automatizzazione dei processi decisionali. Infatti i grandi flussi di dati generati dagli Smart Objects non solo vengono trasmessi e trattati, ma anche gestiti e trasformati (Eftekhari e Akhavan, 2013).

Nel primo capitolo sono state delineate le problematiche relative alla gestione della sicurezza fisica delle dipendenze bancarie. In particolare, è stato evidenziato come l'evoluzione della natura delle filiali bancarie secondo una prospettiva di "apertura al cliente", unitamente alle problematiche relative all'incidenza dei reati (che rappresentano tutt'ora un fenomeno in costante crescita sia negli USA che in Europa), rappresenta una sfida per la gestione della safety e della security delle filiali. Il crescente interesse dei criminali verso gli sportelli fisici e l'esistenza di sistemi di sicurezza obsoleti ha comportato la necessità di introdurre sistemi di gestione della sicurezza innovativi in grado di garantire un livello di sicurezza che sia equiparabile al livello raggiunto per la sicurezza informatica, ambito nel quale si sono concentrati finora i maggiori investimenti e sforzi di ricerca.

Il secondo capitolo è stato dedicato all'analisi della letteratura scientifica con lo scopo di identificare strumenti metodologici ed opportunità tecnologiche volte al miglioramento nei processi di gestione della sicurezza nelle dipendenze bancarie. In particolare sono stati analizzati gli approcci al miglioramento dei processi aziendali, concentrando l'indagine su due principali famiglie di metodologie, ovvero Business Process Reengineering e Business Process Improvement. È stato inoltre studiato il ruolo della tecnologia nel miglioramento dei processi aziendali, analizzando le due prospettive che vedono la tecnologia quale fattore abilitante il cambiamento dei processi aziendali oppure come strumento di supporto per il cambiamento stesso. È stato evidenziato come le innovazioni in ambito ICT ed Internet possono essere considerate di rilevante impatto nel ripensamento dei processi aziendali, sottolineando nello specifico il ruolo della nuova ondata tecnologica dell'IoT quale "acceleratore" di processi spesso vecchi e inefficienti. L'IoT rappresenta un'importante leva per la reingegnerizzazione degli Istituti Bancari. Tale paradigma, se correttamente introdotto e gestito, ha il potenziale per migliorare le prestazioni del processo, in termini di efficacia per ridurre il rischio di attacchi criminali e aumentare l'efficienza operativa.

A partire dall'analisi effettuata nel capitolo precedente, nel terzo capitolo è stata introdotta una metodologia di reingegnerizzazione che comprende quattro fasi fondamentali:

- FASE 1: Rilevazione della situazione attuale.
- FASE 2: Analisi della situazione attuale.
- FASE 3: Modellazione della situazione obiettivo.
- FASE 4: Analisi comparativa.

Nel terzo capitolo, al fine di rilevare la situazione attuale, è stato fondamentale effettuare una review esaustiva della letteratura per ricostruire la conoscenza eterogenea nel dominio di sicurezza delle dipendenze bancarie. Questo ambito di studi è purtroppo caratterizzato da una natura riservata delle informazioni, in quanto la maggior parte dei documenti si riferisce

a report di sicurezza prodotti da istituti bancari e consulenti di sicurezza. Per superare queste limitazioni sull'accesso dei dati, oltre ad una review della letteratura scientifica (quale fonte di dati secondari) è stata effettuata una survey qualitativa per la raccolta dei dati primari, secondo la metodologia del Focus Group. In particolare è stato preso a riferimento un gruppo ristretto di esperti di sicurezza bancaria con lo scopo di raccogliere informazioni per la rilevazione della tecnologia utilizzata e le principali modalità organizzative relative ai processi di gestione della sicurezza nei principali istituti bancari italiani.

È stata dunque effettuata la modellazione degli attuali processi relativi alla gestione della sicurezza delle dipendenze bancarie utilizzando le tecniche BPMN (Business Process Management Notation). Questa fase è stata finalizzata ad evidenziare debolezze nella configurazione AS-IS e fornire linee guida per la ridefinizione di un Intelligent Protection System in grado di migliorare le prestazioni aziendali, sfruttando le nuove opportunità derivanti dall'IoT. In particolare, sono stati sottolineati diverse limitazioni sia nelle misure di protezione che nei processi organizzativi. In particolare le misure fisiche di protezione più diffuse non presentano alcun livello di intelligenza, sono costose e di dubbia efficacia, ma soprattutto, non integrate. Per ciò che invece concerne gli aspetti di natura organizzativa, si evidenziano sostanziali debolezze nei processi di gestione operativa delle procedure di sicurezza, sul sistema di reporting ed analisi degli eventi criminosi e sul processo di definizione ed implementazione del modello di rischio. A tal riguardo, si evidenzia che i modelli attualmente adottati consentono di definire un indice di rischio per la filiale ma non un profilo di rischio. L'indice di rischio si riassume semplicemente in un valore numerico, non in grado di evidenziare le esigenze di sicurezza di ciascuna filiale. Inoltre tali modelli di valutazione del rischio hanno elevati lead times e prestano scarsa attenzione ai fattori esogeni, quali l'evoluzione del numero di attacchi nel tempo e tipologia degli attacchi a livello nazionale e locale; la disponibilità di nuovi sistemi di protezione; i cambiamenti nei modi in cui i criminali conducono attacchi criminali; ed il peggioramento della situazione del contesto socioeconomico che può portare ad un aumento generale dei reati predatori.

Sono state dunque identificate tre principali aree di miglioramento per ciò che riguarda la gestione della sicurezza delle dipendenze bancarie:

- *Definizione di un modello innovativo per la valutazione del rischio di filiale.*
- *Definizione di un modello reingegnerizzato dei processi di sicurezza delle dipendenze bancarie.*
- *Definizione di una soluzione tecnologica per la gestione della sicurezza fisica (Intelligent Protection System) basato sul paradigma Internet of Things.*

A tal proposito, il capitolo 4 è stato interamente dedicato alla definizione del modello di valutazione del rischio di filiale. L'analisi della letteratura nell'ambito del risk management ha consentito la definizione di una metodologia finalizzata ad ottenere un modello per la definizione del profilo di rischio di filiale. La metodologia adottata consta nei seguenti 4 passi

1. Identificazione del rischio
2. Valutazione del rischio
3. Individuazione delle azioni correttive atte a ridurre il rischio
4. Definizione del Modello di rischio di filiale

Per ciò che concerne l'identificazione del rischio, si evidenzia che l'obiettivo della sicurezza è quella di preservare gli assets dalle minacce. Sono stati dunque definiti gli assets *oggetto della sicurezza*, ovvero ciò che deve essere tutelato dalle minacce (i reati). A partire dalle 4 tipologie di minacce individuate e alla luce dei diversi reati trattati per ciascuna minaccia è possibile giungere ad una struttura tassonomica degli stessi. Questa struttura tassonomica consentirà di esprimere in maniera semplificata tutti gli eventi criminosi da cui una dipendenza bancaria dovrà proteggersi. Per quanto riguarda la VALUTAZIONE DEL RISCHIO, abbiamo introdotto una funzione di rischio che tiene conto di due componenti:

- La probabilità che un reato si verifichi in uno specifico intervallo di tempo.
- L'impatto, ovvero la magnitudo del danno provocato dall'evento criminoso

$$\min_{r_i \in RD, f_j \in RD} Risk(r_i, f_j) = \min_{r_i \in RD, f_j \in RD} \sum P(r_i, f_j) \times I(r_i, f_j)$$

Dove:

$P(r_i, f_j)$ probabilità che il reato i venga compiuto sulla filiale j sarà funzione della vulnerabilità dell'area in cui si colloca la filiale f_j , dalla frequenza del reato, mentre l'impatto dipende dalla vulnerabilità specifiche della filiale rispetto al reato r_i ,

Abbiamo dunque analizzato un campione di 840 crimini nei confronti di dipendenze bancarie avvenuti in Italia. L'analisi delle serie storiche e degli asset su cui i crimini incidono hanno consentito di definire la matrice di impatto, utile a calcolare la funzione $I(r_i, f_j)$

La terza fase ha riguarda la definizione delle azioni in grado di:

- prevenire il rischio di reato : azioni che hanno effetto diretto sul minimizzare la funzione $P(r_i, f_j)$
- reaire al reato (proteggere la filiale in caso di esecuzione del reato): azioni che hanno effetto diretto sul minimizzare la funzione $I(r_i, f_j)$

La quarta fase infine è stata dedicata alla definizione del modello di rischio che tiene conto della tripla T (asset, minaccia, contromisura). In particolare, per ogni contromisura, è stato associato un grado di rilevanza rispetto all'asset che preservano da una specifica minaccia. Questo valore dipende dall'efficacia di uno specifico controllo di sicurezza contro la coppia minaccia-asset e dalla combinazione con altri controlli di sicurezza sulla stessa coppia minaccia-asset (rapporto di rafforzamento reciproco).

L'analisi effettuata consente di concludere che non è possibile stabilire un layout "sicuro" per la filiale che sia fruibile dal cliente, ovvero coniughi gli aspetti di sicurezza della dipendenza bancaria con l'accessibilità, ed il senso di tranquillità richiesto dal cliente che si reca fisicamente presso la filiale. Quindi, sebbene il processo di reingegnerizzazione andrebbe portato avanti sulle dimensioni infrastrutturali, tecnologiche ed organizzative, si

può affermare che nel caso specifico risulta efficace intervenire sugli aspetti tecnologici ed organizzativi.

Il quinto ed ultimo capitolo è stato dedicato alla modellazione della situazione obiettivo (TO-BE) attraverso introduzione di soluzioni di natura organizzativa e tecnologica per il miglioramento dei processi di gestione della safety e security delle filiali. Considerando l'approccio di reingegnerizzazione adottato, ed in particolar modo i risultati della FASE 2 della metodologia (Analisi della situazione attuale), abbiamo proposto l'adozione di una nuova "visione" della dipendenza bancaria secondo una prospettiva di natura "cyber-fisica". Il livello tecnologico di una filiale può essere modellato come un Cyber Physical System in cui le misure di protezione (tradizionali ed intelligenti) sono in grado di interagire tra di loro e con gli esseri umani attraverso un'infrastruttura di rete. Recenti sviluppi nell'ambito degli smart object, vanno nella direzione dei cosiddetti *indirect sensors*. Seguendo questo approccio, un sensore fisico può consentire la rilevazione di molte tipologie di dati che generalmente richiedono l'utilizzo di diversi oggetti. Il rilevamento indiretto si basa su un singolo sensore onnisciente in grado di digitalizzare interi edifici. Tale soluzione porta a superare la complessità ed i costi derivanti dalle soluzioni in ambito IoT attualmente disponibili, motivi per i quali ancora non è stato proposto in maniera concreta un approccio alla ridefinizione delle dipendenze bancarie secondo il paradigma IoT. Ciò consente di introdurre sistemi di protezioni intelligenti (Intelligent Protection System) in grado di ottimizzare la sicurezza e migliorare le prestazioni del processo di gestione della sicurezza delle dipendenze bancarie. Ciò determina la riconfigurazione dei processi di gestione della sicurezza (opportunamente modellato tramite tecniche BPMN) secondo il nuovo paradigma. Considerando la mancanza di esempi di best practices in quest'ambito, è stata infine effettuata una valutazione qualitativa su quelle che dovrebbero essere le potenzialità derivanti dall'adozione dello IoT nei processi di gestione della sicurezza. Abbiamo proposto dunque una discussione su ciò che l'IPS può fornire in termini di efficienza (risparmio di tempo, riduzione dei costi) e efficacia (sicurezza migliorata). Tale soluzione è stata validata da un campione di esperti opportunamente interrogati tramite la metodologia del Focus Group.

Questo lavoro di ricerca suggerisce che l'adozione di tecnologie IoT all'interno delle imprese richiede un approccio efficace alla gestione della tecnologia al fine sfruttare tutti i vantaggi possibili per migliorare le prestazioni del processo (Del Giudice, 2016b). In questo lavoro di tesi vengono illustrate le modalità di applicazione di una metodologia di Business Process Reengineering volte a migliorare i processi di interazione tra esseri umani ed altri componenti di un Cyber Physical System, volti a migliorare le performance dei processi aziendali (Yu et al., 2011). Nello specifico, la metodologia è stata applicata al dominio del processo di gestione della sicurezza delle banche, con l'intento di contribuire alla trasformazione delle dipendenze bancarie in "ambienti intelligenti". Lo studio è stato in particolar modo verticalizzato sulla situazione italiana. Il contesto italiano è particolarmente

sensibile alle problematiche relative alla gestione della safety (salvaguardia dell'incolumità psicofisica delle persone) e della security (preservazione degli assets fisici e logici di una organizzazione) delle dipendenze bancarie, dove è altissima l'incidenza dei reati nei confronti degli istituti bancari (60% dei reati registrati in tutta Europa).

I risultati ottenuti confermano gli studi di Ozil (2015) secondo cui i flussi di Big Data generati ed elaborati dai Cyber Physical Systems sono fondamentali per migliorare la produttività, ridurre i costi marginali, migliorare la qualità delle informazioni, facilitare ed automatizzare il processo decisionale. Come ampiamente sottolineato nel corso della trattazione, la migliore configurazione dei processi organizzativi non può essere ottenuta facendo affidamento esclusivamente sulla tecnologia, ma richiede l' "orchestrazione" di funzionalità software (Intelligenza Artificiale, Machine Learning, Business Process Management Systems), di aspetti organizzativi e decisionali, delle risorse umane (Impiegati delle dipendenze bancarie, clienti, addetti alla sicurezza), oggetti fisici (misure di protezione tradizionali e oggetti intelligenti (synthetic sensors e sistemi video evoluti) (Candra et al., 2016; Doan et al., 2011). L'introduzione di un sistema di protezione intelligente (Intelligent Protection System - IPS) automatizza la maggior parte delle attività operative di sicurezza, offrendo agli operatori delle dipendenze bancarie l'opportunità di concentrarsi verso le attività operative volte alla fidelizzazione della clientela, vitale per gli istituti bancari (Brunier et al., 2016). L'approccio integrato descritto in questa trattazione potrebbe essere utilizzato anche in altre tipologie di contesto. Un interessante ambito di applicazione può essere rappresentato dalle cosiddette "infrastrutture critiche", ovvero tutte quelle infrastrutture, quali porti, aeroporti, luoghi governativi, banche, caratterizzati da un elevato rischio di attacchi terroristici ed altre tipologie di minacce quale incendi, occupazioni, vandalismo (Anderson and Malm, 2006). Per tali infrastrutture, solo un approccio integrato ai sistemi di sicurezza può essere efficace nell'assicurare safety e security, proponendo "sistemi di protezione fisica che integrino persone, procedure e attrezzature per la protezione di beni e strutture da furti, sabotaggi o altri attacchi umani di natura dolosa" (Garcia, 2007, p.1). "La progettazione di un sistema di protezione fisica efficace richiede un approccio metodico in cui il progettista pesa gli obiettivi del sistema rispetto alle risorse disponibili e quindi valuta il progetto proposto per determinare quanto la soluzione sia in grado di soddisfare gli obiettivi " (Garcia, 2007, p.1) . L'IPS che proponiamo in questo documento riflette la direzione indicata da Garcia (2007).

In senso più generale, è incoraggiante confrontare i risultati ottenuti con quelli di altre ricerche relative all'IoT e ai processi aziendali. Ad esempio, Ferretti e Schiavone (2016) hanno evidenziato come l'IoT aiuta enormemente la riprogettazione e il miglioramento di tutti i principali processi aziendali dei porti marittimi. I requisiti sono un'attenta pianificazione e coinvolgimento di tutte le parti interessate del porto marittimo e di professionisti esterni. De Senzi Zancul et al. (2016) propongono invece un sistema di customizzazione di prodotto basata su una piattaforma IoT, applicato nell'ambito

dell'industria manifatturiera. Tuttavia, mentre quest'ultimo era finalizzato ad ottenere un incremento in termini di ricavi, le lessons learned applicabili all'ambito della sicurezza delle dipendenze bancarie può seguire l'approccio indicato da Del Giudice, Campanella e Dezi (2016), i quali hanno riferito che l'impiego di soluzioni IoT può ripercuotersi un maggiore ritorno sull'investimento (ROI). L'intersezione tra le teorie sui sistemi di sicurezza fisica e sui sistemi IoT rappresentano la chiave per far progredire la ricerca nei confronti di un nuovo ambito di studio che potrebbe essere denominato Internet of Banks (IoB).

Limitazioni e sviluppi futuri

La metodologia proposta in questo articolo è stata derivata dalla letteratura scientifica attualmente disponibile.

Anche se le banche vengono considerate infrastrutture critiche, si registrano una serie di limitazioni in termini di caratteristiche, processi e attori specifici di questo ambito di riferimento che non consentono di approcciarsi allo studio della sicurezza delle dipendenze bancarie nella stessa maniera in cui viene affrontato per altre infrastrutture critiche. Sfortunatamente, le informazioni e i documenti relativi alle sicurezza delle dipendenze bancarie sono difficilmente reperibili. Si tratta infatti di documenti contenenti informazioni e dati sensibili, coperti da riserbo e ai quali può accedere solo un numero ristretto di società di consulenza in ambito security. Queste limitazioni sono state superate attraverso un approccio qualitativo alla ricerca, facendo ricorso alla metodologia del Focus Group. Le informazioni e i dati forniti dai rispondenti variano in termini di esperienze personali, preferenze e motivazione. In particolare, le informazioni su tempo, costi e flussi di attività insieme alle caratteristiche delle diverse misure di protezione sono state oggetto di una lunga e complessa attività di convalida che ha richiesto un elaborato processo di coordinamento. L'applicazione del modello target richiederebbe la convalida in modo analogo. Tuttavia questa semplificazione è stata inevitabile e ci ha permesso non solo di rilevare la situazione attuale nell'ambito della sicurezza bancaria, ma anche di valutare la proposta risolutiva presentata in questo lavoro.

Sviluppi futuri potrebbero riguardare una fase di realizzazione e testing della piattaforma IPS proposta, al fine di valutare in maniera quantitativa e puntuale, i vantaggi derivanti dalla nuova soluzione. Anche se i dirigenti intervistati hanno manifestavano la loro volontà di collaborare e di innovare il loro approccio alla sicurezza, abbiamo percepito una certa resistenza al cambiamento, principalmente basata su aspetti culturali e una certa paura che potrebbe derivare dall'introduzione di una soluzione di sicurezza "non testata". Pertanto, suggeriamo che un efficace processo di change management è indispensabile per l'applicazione dell'IPS ad un contesto reale e che i Chief Security Officer devono predisporre politiche di comunicazione convincenti, piani e sessioni di formazione dettagliate per tutti gli

attori coinvolti. Una soluzione alternativa, ed in un certo senso meno costosa e radicale, potrebbe riguardare la valutazione della soluzione proposta attraverso opportuni strumenti di simulazione di processo. La simulazione di processo è la tecnica che consente di rappresentare processi, persone e tecnologie in un modello dinamico di computer. Poiché il software di simulazione tiene traccia delle statistiche sugli elementi del modello, le prestazioni di un processo possono essere valutate analizzando i dati di output del modello (Tumay, 1995) La simulazione dei processi aziendali aiuta a comprendere, analizzare e progettare processi. Con l'utilizzo della simulazione i processi (ri)progettati possono essere valutati e confrontati. La simulazione fornisce stime quantitative dell'impatto che un processo modificato potrebbe avere sulle prestazioni del processo stesso e una scelta quantitativamente supportata per una migliore progettazione (Jansen-Vullers e Netjes, 2006). Un modello di simulazione riflette la realtà e viene utilizzato per simulare tale realtà in un computer. Allo stesso modo in cui un architetto utilizza disegni di costruzione per comprendere un edificio, un analista di sistemi può utilizzare modelli di simulazione per valutare un processo aziendale. Quando la simulazione è appropriata? Alcune ragioni sono:

- L'acquisizione di conoscenze di una situazione esistente o di una proposta futura. Dalla creazione di grafici e simulando un processo aziendale, diventa evidente quali parti sono critiche. Queste parti possono quindi essere esaminate più da vicino.
- Un vero esperimento è troppo costoso. La simulazione è un modo economico per analizzare diverse alternative. Soprattutto quando si avvia un nuovo processo aziendale, la simulazione permette di risparmiare tempo e denaro.
- Un vero esperimento è troppo pericoloso. Alcuni esperimenti non possono essere realizzati in realtà.

Per tali ragioni, gli stadi futuri di questo studio prevederanno innanzitutto l'identificazione e lo studio di simulation languages e simulation packages opportuni per il nostro lavoro e l'applicazione di questi strumenti per la valutazione della soluzione TO-BE, prima della sua effettiva implementazione.

Riferimenti Bibliografici

Aarts, E., & De Ruyter, B. (2009). New research perspectives on Ambient Intelligence. *Journal of Ambient Intelligence and Smart Environments*, 1(1), 5-14.

ABI. (2013). Protocollo di intesa per la prevenzione della criminalità in banca. Tratto da [www.abi.it](http://www.abi.it/DOC_Mercati/Rischi/Sicurezza-filiali-Frodi/ProtocolloAnticrimine_ABI_Prefetture%202013.pdf):
http://www.abi.it/DOC_Mercati/Rischi/Sicurezza-filiali-Frodi/ProtocolloAnticrimine_ABI_Prefetture%202013.pdf

Accenture, 2016. ATM Benchmarking Study 2016 and Industry Report

Aguilar-Saven, R.S. (2004), 'BUSINESS PROCESS MODELLING: REVIEW AND FRAMEWORK', *INTERNATIONAL JOURNAL OF PRODUCTION ECONOMICS*, Vol. 90, pp. 129-149.

- Alamá, L., Conesa, D., Forte, A., & Tortosa-Ausina, E. (2015). The geography of Spanish bank branches. *Journal of Applied Statistics*, 42(4), 722-744.
- Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information & Management*, 44(6), 547-567.
- Al-Somali, S., Gholami, R., & Clegg, B. (2009). An investigation into the acceptance of online banking in Saudi Arabia. *Technovation*, 29, 130–141.
- Anderson, J., & Malm, A. (2006). Public-Private Partnerships and the Challenge of Critical Infrastructure Protection. In M. Dunn, & V. Mauer, *International Critical Information Infrastructure Protection Handbook (Vol II)* (p. 139-167). ETH Zurich: Center for Security Studies.
- Anglano, C. (2010). Le tecniche informatiche per la sottrazione di dati riservati. GLI USI ILLECITI DELLE FORME DI PAGAMENTO ELETTRONICO.
- Anselmi, E. (2011a). Attacchi ai Bancomat - Le protezioni antiskimmer e “antitaccheggio”- Integrazione protezione esplosioni e scasso. *Banche e Sicurezza 2011*.
- Anselmi, E. (2011b). Rapine Furti e Clonazioni: le tecnologie per difendersi. *Banche e Sicurezza 2011*.
- Artley, W., & Stroh, S. (2001). *The Performance-Based Management Handbook: Volume 2 - Establishing an Integrated Performance Measurement System*.
- Astarita, G. (2005). Le Linee Guida per la protezione delle unità produttive e logistiche chimiche. XXI Convegno 3ASI.
- Attaran, M. (2004), “Exploring the relationship between information technology and business process reengineering”, *Information & Management*, Vol. 41 No. 5, pp. 585-596.
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- Augusto, J. C. (2007). Ambient intelligence: the confluence of ubiquitous/pervasive computing and artificial intelligence. In *Intelligent Computing Everywhere* (pp. 213-234). Springer London.
- Augusto, J. C., Nakashima, H., & Aghajan, H. (2010). Ambient intelligence and smart environments: A state of the art. *Handbook of ambient intelligence and smart environments*, 3-31.
- Bagnall, J., Bounie, D., Huynh, K. P., Kosse, A., Schmidt, T., Schuh, S. D., & Stix, H. (2014). Consumer cash usage: A cross-country comparison with payment diary survey data. White paper of European Central Bank.
- Baker, P. R. (2012). *Physical Protection Systems*. In P. R. Baker, & D. Benny, *The Complete Guide to Physical Security*. CRC Press
- Ballou, B. (2005). *Enterprise Risk Management—Integrated Framework*.
- Banca d'Italia. (2013). Nuove disposizioni di vigilanza prudenziale per le banche.
- Basilea III. (2010). *The Liquidity Coverage Ratio and liquidity risk monitoring tools*. Bank for International Settlements.
- Berg, H. P. (2010). Risk management: procedures, methods and experiences. *Risk Manage*,1, 79-95.

- Bertocchi, G., Emanuele, C. V., Paoluzzi, A., & Zollo, R. (2008). Videosorveglianza e rappresentazione tridimensionale: una possibile convergenza? *Memoria per Security e Safety*.
- Bhaltlak, K. V., Kaur, H., & Khosla, C. (2014). Human Motion Analysis with the Help of Video Surveillance: A Review. *International Journal of Computer Science & Information Technologies*, 5(5).
- Biazzo, S. (2002), 'PROCESS MAPPING TECHNIQUES AND ORGANISATIONAL ANALYSIS', *Business Process Management Journal*, Vol. 8, No. 1, pp. 42-52.
- Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.
- Blauensteiner, P., Kampel, M., Musik, C., & Vogtenhuber, S. (2010). A socio-technical approach for event detection in security critical infrastructure. *IEEE Computer Society Conference on In Computer Vision and Pattern Recognition Workshops (CVPRW,,* (p. 23-30).
- Bonfanti, M. E. (2014). From Sniffer Dogs to Emerging Sniffer Devices for Airport Security: An Opportunity to Rethink Privacy Implications? *Science and Engineering Ethics*, 20(3), 791-807.
- Borzycki, M. (2006). Bank robbery in Australia: trends & issues in crime and criminal justice. *Australian Institute of Criminology ISSN 0817-8542*.
- Braz, C., Seffah, A., & M'Raihi, D. (2007). Designing a trade-off between usability and security: a metrics based-model. *Human-Computer Interaction—INTERACT 2007* (p. 114-126). Berlin: Springer Heidelberg.
- Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces*, 36(6), 530-544.
- Brunier, F., Pätsch, C., Stradtman, F., (2016) Transforming the banking branch Three essential roles for the branch in the everyday bank By Frederic. *Accenture White Paper*
- Bunn, A., & Guthrie, R. (2009). Occupational Health and Safety in the banking industry. *Legal Issues in Business*, 11, 80.
- Burns, A., McDermid, J., & Dobson, J. (1992). On the meaning of safety and security. *The Computer Journal* 35.1 (1992), 35(1), 3-15.
- Candra, Z. M., Truong, H. L., & Dustdar, S. (2016, June). On Monitoring Cyber-Physical-Social Systems. In *Services (SERVICES), 2016 IEEE World Congress on* (pp. 56-63). IEEE.
- Caparvi, R. (2006). *L'impresa bancaria. Economia e tecniche di gestione*.
- Cepas (a cura di) (2006). *Raggiungere i risultati con la gestione per processi. Migliorare i processi per essere competitivi*, FrancoAngeli S.r.l., Milano.
- CeTiF (2014). *L'evoluzione dello Sportello bancario Modelli distributivi, innovazione tecnologica e supporto multicanale*
- Chapin, N. (1971), *Flowcharts*, Auerbach Publishers, Princeton
- Chiu, S. H., Lu, C. P., & Wen, C. Y. (2006). A Motion Detection-Based Framework for Improving Image Quality of CCTV Security Systems. *Journal of forensic sciences*, 51(5), 1115-1119.

- CIFAS. (2004). http://www.cifas.org.uk/identity_fraud. Tratto da CIFAS - The UK's Fraud Prevention Service.
- CIMIP. (2009). <http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm>. Tratto da Center for Identity Management and Information Protection.
- Clarke, R. V., Field, S., & McGrath, G. (1991). Target hardening of banks in Australia and displacement of robberies. *Security Journal*, 2(2), 84-90.
- Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In *IST-Africa Conference Proceedings, 2011* (pp. 1-9). IEEE.
- COM. (2008). Direttiva del Consiglio relativa all'individuazione e alla designazione delle IC europee e alla valutazione della necessità di migliorarne la protezione. Bruxelles.
- Conrath, E. J. (1999). *Structural design for physical security: State of the practice*. ASCE Publications.
- Cook, D. J., & Das, S.K. (2005). *Smart environments: technologies, protocols, and applications*, John Wiley and Sons
- Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2009). Ambient intelligence: Technologies, applications, and opportunities. *Pervasive and Mobile Computing*, 5(4), 277-298.
- Costantini M., Cassaro F., 2001, "Reingegnerizzazione dei Processi", rapporto finale. Ministero dell'Università e della Ricerca Scientifica e Tecnologica (COFIN).
- Cox, T., & Griffiths, A. (1995). *Work-related stress: Nature and assessment*.
- Cravera, A. (2011, Settembre). L'abilità di decidere oggi. *L'impresa*(8).
- Crescentini, A., Sada, A., & Giossi, L. (2007). *Elogio della sicurezza. Aspetti multidisciplinari tra scienza e pratica*.
- Cucchiella, F., & Gastaldi, M. (2006). Risk management in supply chain: a real option approach. *Journal of Manufacturing Technology Management*, 17(6), 700-720.
- Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4), 2233-2243.
- D'Agata, G. (2012). *Skimming: la clonazione di carte di credito e bancomat*. Tratto da Giro di vite: <http://www.girodivite.it/Skimming-la-clonazione-di-carte-di.html>
- Daugman, J. (2004). How iris recognition works. *IEEE Transactions on circuits and systems for video technology*, 14(1), 21-30.
- Davenport, T. H. (1995). Business process reengineering: where it's been, where it's going. *Business process change: Reengineering concepts, methods and technologies*, 1-13.
- Davenport, T. H., & Stoddard, D. B. (1994). Reengineering: business change of mythic proportions?. *MIS quarterly*, 121-127.
- Davenport, T. H., & Short, J. E. (1990). The new industrial engineering: information technology and business process redesign, *Sloan Management Review*, 31 (4)

- Davidson, W. H. (1993). Beyond re-engineering: the three phases of business transformation. *IBM systems Journal*, 32(1), 485-499.].
- De Gregorio, E. (2011). Dynamics of a robbery: criminological aspects, security issues and prevention—an exploratory study. *Police Practice and Research: An International Journal*, 12(3), 253-264.
- Dee, H. M., & Velastin, S. A. (2008). How close are we to solving the problem of automated visual surveillance? *Machine Vision and Applications*, 19(5-6), 329-343.
- Del Conte, F. (2008). La sicurezza in banca: safety o security?
- Del Giudice, M. (2016 a), "Discovering the Internet of Things (IoT) within the business process management: A literature review on technological revitalization", *Business Process Management Journal*, Vol. 22 No. 2, pp. 263-270.
- Del Giudice, M. (2016 b), "Discovering the Internet of Things (IoT): technology and business process management, inside and outside the innovative firms", *Business Process Management Journal*, Vol. 22 No. 2.
- Del Giudice, M., Campanella, F. and Dezi, L. (2016). "The bank of things: An empirical investigation on the profitability of the financial services of the future". *Business Process Management Journal*, Vol. 22, No. 2, 324-340.
- Del Re, E. C. (2009). Il 'furto di identità'. *GNOSIS - Rivista Italiana d'Intelligence*, n. 4 , ottobre-dicembre.
- Deming, W. E. (1950). *Elementary principles of the statistical control of quality: a series of lectures*. Nippon Kagaku Gijutsu Remmei
- Department of Justice Canada. (2010). http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32471.html. Tratto da Department of Justice Canada.
- Diebold Nixdorf (2016). *The Global Classroom: Branch Transformation*. White Paper
- Dimitrova, M. (2016). Towards Design of High-Level Synthetic Sensors for Socially-Competent Computing Systems. In *Revolutionizing Education through Web-Based Instruction* (pp. 20-34). IGI Global.
- Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, 16(2), 147-166.
- Dipartimento del Tesoro. (2011). http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/prevenzione_frodi_credito_consumo.html. Tratto da Dipartimento del Tesoro.
- Doan, A., Ramakrishnan, R., and Halevy, A. Y. (2011), "Crowdsourcing systems on the world-wide web", *Communications of the ACM*, Vol. 54 No. 4, pp. 86-96.
- Dohr, A., Modre-Opsrian, R., Drobits, M., Hayn, D., & Schreier, G. (2010, April). The internet of things for ambient assisted living. In *Information technology: new generations (ITNG)*, 2010 seventh international conference on (pp. 804-809). Ieee.

- Dolan, P., & Peasgood, T. (2007). Estimating the economic and social costs of the fear of crime. *British Journal of Criminology*, 47(1), 121-132.
- Dudenhoeffer, D. D., Permann, M. R., & Manic, M. (2006). A framework for infrastructure interdependency modeling and analysis. *Proceedings of the 38th conference on Winter simulation*, (p. 478-485).
- Dudenhoeffer, D. D., Permann, M. R., & Manic, M. (2006). A framework for infrastructure interdependency modeling and analysis. *Proceedings of the 38th conference on Winter simulation*, (p. 478-485).
- Dugato, M. (2014). Analyzing Bank Robbery in Italy. In *Organized Crime, Corruption and Crime Prevention* (p. 115-125). Springer International Publishing.
- Dumas, M. (2011). On the convergence of data and process engineering. In *Advances in Databases and Information Systems*(pp. 19-26). Springer Berlin/Heidelberg.
- EAST (2017). EUROPEAN ATM CRIME REPORT 2016. European ATM Security Team
- EBF (2016). Physical security report 2015 – EUROPEAN BANKING FEDERATION
- Eftekhari, N., and Akhavan, P. (2013), “Developing a comprehensive methodology for BPR projects by employing IT tools”, *Business Process Management Journal*, Vol. 19 No.1, pp. 4-29.
- EY (2015), “Cybersecurity and the Internet of Things. Insights on governance, risk and compliance”, available at [http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-ofthings/\\$FILE/EY-cybersecurity-and-the-internet-of-things.pdf](http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-ofthings/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf) (accessed 17 August 2017).
- Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, 27(3), 571-583.
- Fan, X., Huang, H., Qi, S., Luo, X., Zeng, J., Xie, Q., & Xie, C. (2015). Sensing home: a cost-effective design for smart home via heterogeneous wireless networks. *Sensors*, 15(12), 30270-30292.
- FBI (2016). BANK CRIME STATISTICS – 2015. U.S. DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION WASHINGTON.
- FDIC (2017), The U.S. Federal Deposit Insurance Corporation. Table CB01: Number of Institutions, Branches and Total Offices FDIC-Insured Commercial Banks (Available at <https://www5.fdic.gov/hsob/HSOBRpt.asp> - Accessed on May 2017)
- Felicetti, C., De, R., Raso, C., Felicetti, A. M., & Ammirato, S. (2015). Collaborative smart environments for energy-efficiency and quality of life. *International Journal of Engineering and Technology*, 7(2), 543-552.
- Finklea, K. M. (2010). Identity Theft: Trends and Issues. CRS Report for Congress.
- Flavián, C., Guinaliu, M., & Torres, E. (2006). How bricks-and-mortar attributes affect online banking adoption. *International Journal of Bank Marketing*, 24(6), 406-423.
- Forrester (2015), “The Internet Of Things Has The Potential To Connect And Transform Businesses But Early Adopters Have Focused Mostly On Efficiency Plays”, available at

<https://assets.cdn.sap.com/sapcom/docs/2015/08/54f65c37-3b7c-0010-82c7-eda71af511fa.pdf>
(accessed 13 June 2017).

Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., & Heinonen, S. (2005). Perspectives of ambient intelligence in the home environment. *Telematics and informatics*, 22(3), 221-238.

G4S Report (2016). Integrated Report and Accounts 2016, available at http://www.g4s.com/-/media/G4S/Global/Files/Annual-Reports/AR-2016-Extracts/G4S_2016IR_Final_PDF.ashx

Gamassi, M., Piuri, V., Sana, D., Scotti, F., & Scotti, O. (2006). Scalable distributed biometric systems – Advanced techniques for security and safety. *Instrumentation & Measurement Magazine, IEEE*, 21-28.

Gamassi, M., Piuri, V., Sana, D., Scotti, F., & Scotti, O. (2006). Scalable distributed biometric systems – Advanced techniques for security and safety. *Instrumentation & Measurement Magazine, IEEE*, 21-28.

Gárate, A., Herrasti, N., & López, A. (2005, October). GENIO: an ambient intelligence application in home automation and entertainment environment. In *Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies* (pp. 241-245). ACM.

García, C. G., Meana-Llorián, D., G-Bustelo, B. C. P., & Lovelle, J. M. C. (2017). A review about Smart Objects, Sensors, and Actuators. *International Journal of Interactive Multimedia and Artificial Intelligence*, 4(Special Issue on Advances and Applications in the Internet of Things and Cloud Computing).

Garcia, M. L. (2007). *Design and evaluation of physical protection systems*. Butterworth-Heinemann.

Geetha, S., Madhusudanan, J., Krishnamoorthy, M., & Venkatesan, V. P. (2016, August). Design of Emotions context based Smart ATM Environment. In *Proceedings of the International Conference on Informatics and Analytics* (p. 63). ACM.

Gentili, A. (2011). *Strategiedi contrasto del falso nummario e delle frodi informatiche*. Banche e Sicurezza 2011.

Goldman Sachs (2014), “The Internet of Things: Making sense of the next mega-trend” available at <http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf> (accessed 14 November 2016)

Gortz, M., Ackermann, R., Schmitt, J., & Steinmetz, R. (2004, October). Context-aware communication services a framework for building enhanced ip telephony services. In *Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on* (pp. 535-540). IEEE.

Goya, K., Zhang, X., Kitayama, K., & Nagayama, I. (2009). A method for automatic detection of crimes for public security by using motion analysis. *IIH-MSP'09. Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (p. 736-741). IEEE.

Grabisch, M., Kojadinovic, I., & Meyer, P. (2008). A review of methods for capacity identification in Choquet integral based multi-attribute utility theory: Applications of the Kappalab R package. *European journal of operational research*, 186(2), 766-785.

- Grill, T., Polacek, O., & Tscheligi, M. (2015). Conwiz: The contextual wizard of oz. *Journal of Ambient Intelligence and Smart Environments*, 7(6), 719-744.
- Grohmann, A., & Vacca, A. (1994). *Il Retail Banking in Italia*.
- Guazzoni, C., & Ronsivalle, G. B. (2008). An Artificial Neural Network for Bank Robbery Risk Management: The OS. SI. F Web On-Line Tool of the ABI Anti-crime Department. *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08* (p. 1-10). Berlin: Springer Heidelberg.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7), 1645-1660.
- Guerette, R. T., & Clarke, R. V. (2003). Product life cycles and crime: Automated teller machines and robbery. *Security Journal*, 16(1), 7-18.
- Guha, S., & Kettinger, W. J. (1993). Business process reengineering. *Information Systems Management*, 10(3), 13–22.
- Hammer, M. (1990). Reengineering work: don't automate, obliterate. *Harvard business review*, 68(4), 104-112.
- Hammer, M. and Champy, J. (2009), *Reengineering the Corporation: Manifesto for Business Revolution*, Harper Business Essentials.
- Hammer, M., & Champy, J. (1993). *Reengineering the corporation*.
- Han, J., Pauwels, E. J., de Zeeuw, P. M., & de With, P. H. (2012). Employing a RGB-D sensor for real-time tracking of humans across multiple re-entries in a smart environment. *IEEE Transactions on Consumer Electronics*, 58(2).
- Hand, M. (1991), "Designing quality into business processes", *Management Accounting*, January
- Hardaker, J. B., Huirne, R. B., Anderson, J. R., & Lien, G. (2004). *Coping with risk in agriculture* (No. Ed. 2). CABI publishing.
- Harrington H.J., 1991, *Business Process Improvement: The Breakthrough Strategy for Total Quality, Productivity, and Competitiveness* - Kindle Edition
- Havey, M. (2005), *Essential Business Process Modelling*, O'Reilly, U.S.A.
- Höbe, L. (2015). The Changing Landscape of the Financial Services. *International Journal of Trade, Economics and Finance*, 6(2), 145.
- Hodges, M. (2000). Elements of an Effective Safety and Health Program. *Tratto da United States Department of Labor*: http://www.osha.gov/SLTC/pptpresentations/safety_health_program/index.html
- Hofacker, I. and Vetschera, R. (2001), 'Algorithmical Approaches to Business Process Design', *Computers & Operations Research*, Vol. 28, pp. 1253-1275.

- Hoppe M.J., Wells E.A., Morrison D.M., Gilmore M.R., Wilsdon A. (1995) 'Using focus groups to discuss sensitive topics with children', *Evaluation Review* 19 (1): 102-14.
- Hribernik, K. A., Ghrairi, Z., Hans, C., & Thoben, K. D. (2011, June). Co-creating the Internet of Things—First experiences in the participatory design of Intelligent Products with Arduino. In *Concurrent Enterprising (ICE), 2011 17th International Conference on* (pp. 1-9). IEEE.
- Iaconis, M. (2011). Quadro di riferimento sulla Sicurezza anticrimine nelle banche italiane. Bancasicura 2011.
- Iaconis, M., Limentanti, J., & Rossi, G. (2011). Soluzioni innovative di sicurezza per le banche.
- INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & 1668 Nanosystems, in: Co-operation with the Working Group RFID of 1669 the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, 1670 Version 1.1, 27 May 2008.
- Ishikawa, K. (1985). *What is total quality control? The Japanese way*. Prentice Hall
- Jain, A. K. (2007). Technology: Biometric recognition. *Nature*, 449, 38-40.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), 4-20.
- Jaiswal, A. M., & Bartere, M. (2014). Enhancing ATM Security using fingerprint and GSM Technology. *International Journal of Computer Science and Mobile Computing*, 3(4), 28-32.
- Jennex, Murray E., "Assessing Knowledge Loss Risk" (2009). AMCIS 2009 Proceedings. Paper 446.
- Juvara, F. (2012). Gli attacchi ai trasportatori di valori. Tratto da Securindex: http://www.securindex.com/notizie/banche/gli_attacchi_ai_trasportatori_di_valori-5242
- Kabay, M. (2014). Understanding studies and surveys of computer crime. In Bosworth, S.; Kabay, M.; Whyne, E. (Eds.) *Computer Security Handbook*. Hoboken, New Jersey: John Wiley & Sons, Inc. 10.1–10.12.
- Kim, Y., Schmid, T., Charbiwala, Z. M., & Srivastava, M. B. (2009, September). ViridiScope: design and implementation of a fine grained power monitoring system for homes. In *Proceedings of the 11th international conference on Ubiquitous computing* (pp. 245-254). ACM.
- KMPG Advisory (2013). Sportelli bancari e nuovi modelli distributivi: Contesto di riferimento e scenari evolutivi
- Knight, F. H. (1921). *Risk, uncertainty and profit*. New York: Hart, Schaffner and Marx.
- Kreuger R.A. (1988) *Focus groups: a practical guide for applied research*. London: Sage.
- Koubarakis, M. and Plexousakis, D. (2002), 'A Formal Framework for Business Process Modelling and Design', *Information Systems*, Vol. 27, pp. 299-319.
- Kreuger R.A. (1988) *Focus groups: a practical guide for applied research*. London: Sage.

- Laput, G., Lasecki, W. S., Wiese, J., Xiao, R., Bigham, J. P., & Harrison, C. (2015, April). Sensors: Adaptive, rapidly deployable, human-intelligent sensor feeds. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 1935-1944). ACM.
- Langley, G. J., Nolan, K. M., & Nolan, T. W. (1994). The foundation of improvement. *Quality Progress*, 27(6), 81-86
- Langley, G. J., Moen, R. D., Nolan, K. M., Nolan, T. W., Norman, C. L., & Provost, L. P. (2009). *The improvement guide: a practical approach to enhancing organizational performance*. John Wiley & Sons.
- Lee, E. A. (2008, May). Cyber physical systems: Design challenges. In Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on (pp. 363-369). IEEE.
- Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18-23.
- Lindley, D. V. (2006). *Understanding uncertainty*. John Wiley & Sons.
- Lindsay, A., Downs, D. and Lunn, K. (2003), 'BUSINESS PROCESSES - ATTEMPTS TO FIND A DEFINITION', *Information and Software Technology*, Vol. 45, pp. 1015-1019.
- Lippi, F. (2007). Phishing e Pharming. Istituti di Credito: responsabilità civile e risvolti penali . Tratto da Federico Lippi: <http://www.federicolippi.it/content/view/41/30/>
- Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional*, 3(1), 27-32.
- Liu, Z., Yang, D. S., Wen, D., Zhang, W. M., & Mao, W. (2011). Cyber-physical-social systems for command and control. *IEEE Intelligent Systems*, 26(4), 92-96.
- Lloret, J., Canovas, A., Sendra, S., & Parra, L. (2015). A smart communication architecture for ambient assisted living. *IEEE Communications Magazine*, 53(1), 26-33.
- Lorini, R. (2005). *La Security Governance in banca: i benefici di un approccio integrato*. Atti del Convegno BANCASICURA. Padova.
- Lorini, R. (2005). *La Security Governance in banca: i benefici di un approccio integrato*. Atti del Convegno BANCASICURA. Padova.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated.
- Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. *Journal of Business Logistics*, 29(1), 133-155
- Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34(1), 1-13.
- Maruccia, A. (2009). Un trojan all'attacco dei bancomat russi. Tratto da PuntoInformatico: <http://punto-informatico.it/2579683/PI/News/un-trojan-all-attacco-dei-bancomat-russi.aspx>

- Mastrobuoni, G. (2014). *Optimizing Behavior During Bank Robberies: Theory and Evidence on the Two Minute Rule*.
- Matchett, A. R. (2003). *CCTV for security professionals*. Butterworth-Heinemann.
- Matricardi, C. (2007). Cassazione: clonazione del Bancomat? A volte la responsabilità può essere dell'Istituto di credito. Tratto da Studio Cataldi : http://www.studiocataldi.it/news_giuridiche_asp/news_giuridica_4733.asp
- Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. In *From active data management to event-based systems and more* (pp. 242-259). Springer Berlin Heidelberg.
- Matthews, R., Pease, C., & Pease, K. (2001). Repeated bank robbery: themes and variations. *Crime Prevention Studies*, 12, 153-164.
- Mauboussin, M. J. (2007). *More Than You Know: Finding Financial Wisdom in Unconventional Places*. Columbia University Press.
- Messina, M. (2002). *NUOVI CONCETTI SULLA PROTEZIONE ANTIRAPINA*. Bancasicura.
- Meyer, G. G., Främling, K., & Holmström, J. (2009). Intelligent products: A survey. *Computers in industry*, 60(3), 137-148.
- Mills, A. (2001). A systematic approach to risk management for construction. *Structural survey*, 19(5), 245-252.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516.
- Misra, K. B. (2008). *Handbook of Performability Engineering*.
- Morgan D.L. (1988) *Focus groups as qualitative research*. London: Sage.
- Neroth, P. (2011). Beyond body scanners. *Engineering & Technology*, 6(8), 50 – 52.
- Ning, H., Liu, H., Ma, J., Yang, L. T., & Huang, R. (2016). Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology. *Future Generation Computer Systems*, 56, 504-522.
- Noble, F. (1991), “Seven ways to develop office systems: a managerial comparison of office system development methodologies”, *The Computer Journal*, Vol. 34 No. 2, pp. 113-121.
- Norton. (2006). Frode on-line: pharming. Tratto da Norton: <http://it.norton.com/cybercrime-pharming/promo>
- Onado, M. (2000). *Mercati e intermediari finanziari*.
- O'Rourke, T. D. (2007). Critical infrastructure, interdependencies, and resilience. *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING*, 37(1).
- O'Rourke, T. D. (2007). Critical infrastructure, interdependencies, and resilience. *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING*, 37(1).

- Ossif. (2009). Carica di gas fa esplodere Atm. Tratto da <http://www.ossif.it/Engine/RAServePG.php/P/301810010300/M/251810010303>
- Ossif. (2010a). Accorgimenti per limitare le alterazioni e le falsificazioni di assegni bancari e circolari. Tratto da http://www.carabinieri.it/internet/imagestore/cittadino/consigli/tematici/pdf/Falsificazioni_Assegni.PDF.
- Ossif. (2010b). Rapporto sui furti ai danni delle dipendenze bancarie. Tratto da <http://www.ossif.it/Engine/RAServePG.php/P/323510010300/M/251810010303>
- Ozil, P. (2015), "BPM of Things: the Next Generation of the Internet of Things" available at <http://data-informed.com/bpm-of-things-the-next-generation-of-the-internet-of-things/> (accessed 19 April 2017).
- Paget, F. (2009). Frodi finanziarie e Internet Banking: minacce e contromisure.
- Paradi, J. C., & Zhu, H. (2013). A survey on bank branch efficiency and performance research with data envelopment analysis. *Omega*, 41(1), 61-79.
- Patel, K., & Brown, I. (2016). Towards a Theory of Multi-Channel Banking Adoption amongst Consumers. *The Electronic Journal Information Systems Evaluation Volume*, 19(3).
- Penz, E., Sinkovics, R. R. (2013). Triangulating consumers' perceptions of payment systems by using social representations theory: A multi-method approach. *Journal of Consumer Behaviour*, 12(4), 293-306.
- Pierantozzi, D. (1998). La gestione dei processi nell'ottica del valore: miglioramento graduale e reengineering: criteri, metodi, esperienze. Egea
- Poslad, S. (2009). Ubiquitous computing smart devices, smart environments and smart interaction. S. Poslad, *Ubiquitous Computing Smart Devices, Smart Environments and Smart Interaction* (pp. pp. 115-133). Wiley.
- Powell, S.G., Schwaninger, M. and Trimble, C. (2001), 'Measurement and Control of Business Processes', *System Dynamics Review*, Vol. 17, No. 1, pp. 63-91.
- PwC (2016), *Cambiare per sopravvivere: l'evoluzione del ruolo della Filiale in Italia*
- Race K.E., Hotch D.F., Parker T. (1994) 'Rehabilitation program evaluation: use of focus groups to empower clients', *Evaluation Review* 18 (6): 730-40
- Ramparany, F., & Boissier, O. (2002, July). Smart devices embedding multi-agent technologies for a pro-active world. In *Proc. of the Ubiquitous Computing Workshop*.
- Ramsay, M., & Newton, R. (1991). The effect of better street lighting on crime and fear: A review.
- Reynolds, G. S., & Bank, W. F. (2006). Facial Recognition: A Biometric For The Fight Against Check Fraud. *Journal of Economic Crime Management*, 4(2).
- Rinaldi, S. M. (2004). Modeling and simulating critical infrastructures and their interdependencies. *System sciences, Proceedings of the 37th annual Hawaii international conference on. IEEE*.

- Roberts, L. (1994), Process reengineering: The key to achieving breakthrough success. Asq Press.
- Ronsivalle, G. (2011). Neural and Bayesian Networks to Fight Crime: the NBNC Meta-Model of Risk Analysis. In D. C. Hui, Artificial Neural Networks - Application . InTech, ISBN: 978-953-307-188-6.
- Ronsivalle, G. B. (2007). The ABI On Line Simulation" Bank Robberies". An Innovative Instrument for the Robbery Risk Management in the Italian Banking System. Proceedings of EDEN.
- Ryan, N., Cinotti, T. S., & Raffa, G. (2005). Smart environments and their applications to cultural heritage. Smart Environments and their Applications to Cultural Heritage, 7.
- Sadri, F. (2011). Ambient intelligence: A survey. ACM Computing Surveys (CSUR), 43(4), 36.
- Sanislav, T., & Miclea, L. (2012). Cyber-physical systems-concept, challenges and research areas. Journal of Control Engineering and Applied Informatics, 14(2), 28-33
- Scheer, A.W. (1994), Business Process Reengineering, Reference Models for Industrial Enterprises, Springer,
- SERIT. (2014). SEcurity Research in Italy. Tratto da www.piattaformaserit.it.
- Short, J. E., & Venkatraman, N. (1992). Beyond business process redesign: redefining Baxter's business network. Sloan management review, 34(1), 7.
- Sidlauskas, D., & Tamer, S. (2008). Hand geometry recognition. In Handbook of Biometrics (p. 91–107). Berlin: Springer.
- Sigismondi, A. (2008). Ladri d'identità, "Identity Crimes". Tratto da Consulente Legale Privacy: <http://www.consulentelegaleprivacy.it/approfondimentidett.php?id=181>
- Sinibaldi, A. (2009). La gestione dei processi in azienda. Introduzione al Business Process Management: Introduzione al Business Process Management. FrancoAngeli.
- Smirnov, A., Levashova, T., Shilov, N., & Sandkuhl, K. (2014, October). Ontology for cyber-physical-social systems self-organisation. In Open Innovations Association (FRUCT16), 2014 16th Conference of (pp. 101-107). IEEE.
- Smith and Fingar, 2003, Business Process Management - The Third Wave, Meghan-Kiffer Press, Tampa)
- Stasi, R. (2007). Survey sul furto di identità elettronica tramite Internet. Banche e Sicurezza 2007.
- Strnadl, C. F. (2006). Aligning business and it: The process-driven architecture model. Information Systems Management, 23(4), 67–77.
- Sujith, B. (2014). Crime Detection and Avoidance in ATM: A New Framework. International Journal of Computer Science & Information Technologies, 5(5).
- Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on (Vol. 5, pp. V5-376). IEEE.
- Tapia, E. M., Intille, S. S., & Larson, K. (2004, March). Activity recognition in the home using simple and ubiquitous sensors. In *Pervasive* (Vol. 4, pp. 158-175).

- Towle, H. K. (2004). Identity theft: myths, methods, and new law. Rutgers Computer and Technology Law Journal, Vol. 30 Nbr. 2.
- Trkman, P. (2010). The critical success factors of business process management. International journal of information management, 30(2), 125-134.
- Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). Supply Chain Management: An International Journal, 16(6), 474-483
- Tummala, V. R., & Burchett, J. F. (1999). Applying a risk management process (RMP) to manage cost risk for an EHV transmission line project. International Journal of Project Management, 17(4), 223-235.
- TUSL. (2008). decreto legislativo n. 81 del 9 aprile 2008. Testo unico in materia di salute e sicurezza nei luoghi di lavoro.
- Vaccaro, M. (2005). Safety and Security.
- Valiris, G. and Glykas, M. (1999), "Critical review of existing BPR methodologies: the need for a holistic approach", Business process management journal, Vol. 5 No. 1, pp. 65-86.
- Valiris, G. and Glykas, M. (2004), 'Business Analysis Metrics for Business Process Redesign', Business Process Management Journal, Vol. 10, No. 4, pp. 445-480.
- Van der Aalst, 2004, "Business Process Management – a personal view", Business Process Management Journal, Vol. 10, N. 2, pp. 135-139;
- Van Der Aalst, W. M. (2013). Business process management: a comprehensive survey. ISRN Software Engineering, 2013.
- van der Aalst, W.M.P., ter Hofstede, A.H.M. and Weske, M. (2003), 'Business Process Management: A Survey', Lecture Notes in Computer Science, Vol. 2678, pp. 1-12.
- Vergidis K., Turner, C.J. and Tiwari, A. (2008), 'Business Process Perspectives: Theoretical Developments vs. Real-World Practice', International Journal of Production Economics, vol. 114, pp. 91-104.
- Volkner, P. and Werners, B. (2000), 'A DECISION SUPPORT SYSTEM FOR BUSINESS PROCESS PLANNING', European Journal of Operational Research, Vol. 125, pp. 633-647.
- Volpentesta, A. P. (2015). A framework for human interaction with ubiquitous services in a smart environment. Computers in Human Behavior, 50, 177-185.
- Volpentesta, A. P., Ammirato, S., & Palmieri, R. (2011). Investigating effects of security incident awareness on information risk perception. International Journal of Technology Management, 54(2/3), 304-320.
- Wallace, E., & Diffley, C. (1988). CCTV control room ergonomics . Police Scientific Development Branch (PSDB), Technical Report 14/98.
- Walsh, I., Forth, P., Thogmartin, S., Bickford, J., Desmangles, L., & Berz, K. (2010). Building a High-Powered Branch Network in Retail Banking. The Boston Consulting Group.

- Wang, F. Y. (2010). The emergence of intelligent enterprises: From CPS to CPSS. *IEEE Intelligent Systems*, 25(4), 85-88.
- Want, R. (2006). An introduction to RFID technology. *IEEE pervasive computing*, 5(1), 25-33.
- Ward, S., & Chapman, C. (2003). Transforming project risk management into project uncertainty management. *International Journal of Project Management*, 21(2), 97-105.
- Ward, J. A., Lukowicz, P., Troster, G., & Starner, T. E. (2006). Activity recognition of assembly tasks using body-worn microphones and accelerometers. *IEEE transactions on pattern analysis and machine intelligence*, 28(10), 1553-1567.
- Weisel, D. L. (2007). Bank Robbery. US Department of Justice, Office of Community Oriented Policing Services.
- Weiss, W. E. (2008). Dynamic security: An agent-based model for airport defense. *Proceedings of the 2008 Winter Simulation Conference*, (p. 1320-1325).
- Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computer and Security*, 24(6), 448-459.
- Williamson, O. (1975). *Markets and Hierarchies: analysis and antitrust implications*.
- Wu, F. J., Kao, Y. F., & Tseng, Y. C. (2011). From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile Computing*, 7(4), 397-413.
- Zakarian, A. and Kusiak, A. (2001), 'Process Analysis and Reengineering', *Computers & Industrial Engineering*, Vol. 41, pp. 135-150.
- Zeng, J., Yang, L. T., Lin, M., Ning, H., & Ma, J. (2016). A survey: Cyber-physical-social systems and their system-level design methodology. *Future Generation Computer Systems*
- Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2015). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*.
- Zyczkowski, M., Szustakowski, M., Czurapinski, W., Dulski, R., Kastek, M., & Trzaskawka, P. (2011). Integrated mobile radar-camera system in airport perimeter security. In *SPIE Security+ Defence*. International Society for Optics and Photonics.