UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA INDUSTRIALE

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA DELLA SICUREZZA CIVILE E INDUSTRIALE

Tesi di Laurea Magistrale in

Ingegneria della Sicurezza Civile e Industriale

Correlazione tra safety e security nel trasporto aereo

Relatore: Dott. Ivan Rizzolo

Laureando: MARCO ZANCONATO

ANNO ACCADEMICO 2018-2019

Riassunto

Questa tesi si pone l'obiettivo di indagare come safety e security, nell'ambito dell'aviazione civile, si influenzino l'un l'altra. Si cercherà quindi di esaltare i nessi causali e le criticità, messe in evidenza dall'applicazione contemporanea delle misure, relative ai due ambiti della sicurezza. Introducendo la questione da un punto di vista generale, verrà prima fatto un inquadramento nel settore della sicurezza del trasporto aereo, con i concetti base, che la definiscono, e i riferimenti normativi, che la regolamentano. Verranno presentati alcuni modelli e tecniche alla base delle valutazioni di sicurezza, con particolare attenzione ai temi dell'analisi retrospettiva e dell'integrazione tra i due settori. L'obiettivo della tesi sarà poi raggiunto tramite lo studio di eventi aeronautici, in cui l'interazione tra fattori di safety e di security ha generato situazioni diverse tra loro. L'analisi metodologica dei casi studio permetterà di esaltare le strette correlazioni tra i due ambiti della sicurezza.

Indice

INTRODUZIONE 1

CAPITOLO 1 - Introduzione alla safety 3

1.1 DEFINIZIONE 3

1.2 STORIA DELLA SAFETY 3

1.3 DEFINIZIONE DEL RISCHIO CORRELATO ALLA SAFETY 6

1.4 APPROCCIO ALLA SAFETY 7

1.5 VALUTAZIONE DEL RISCHIO SAFETY 9

CAPITOLO 2 - Introduzione alla security 13

2.1 DEFINIZIONE 13

2.2 STORIA DELLA SECURITY 13

2.3 DEFINIZIONE DEL RISCHIO CORRELATO ALLA SECURITY 16

2.4 APPROCCIO ALLA SECURITY 18

2.5 VALUTAZIONE DEL RISCHIO SECURITY 22

CAPITOLO 3 - Il quadro normativo 25

3.1 LA NORMATIVA INTERNAZIONALE 25

3.1.1 Gli annessi e la safety 27

3.1.2 L'annesso 17 28

3.1.3 L'annesso 13 28

3.2 LA NORMATIVA EUROPEA 29

3.2.1 Safety 30

3.2.2 Security 32

3.3 GLI ENTI ITALIANI 34

3.3.1 ENAC 34

3.3.2 ANSV 35

3.3.3 ENAV 36

CAPITOLO 4 - L'analisi retrospettiva 37

4.1 IL SAFETY REPORT 37

4.2 IL FATTORE UMANO 38

4.2.1 Il modello SHELL 39
4.3 IL MODELLO DI REASON 41
4.3.1 Il modello “Fallible Machine” 41
4.3.2 Il modello “Swiss Cheese” 43
4.3.2.1 Decision makers 45
4.3.2.2 Line management 45
4.3.2.3 Preconditions 46
4.3.2.4 Unsafe acts 46
4.3.2.5 Defences 47
4.4 L’INCHIESTA INCIDENTALE 47
CAPITOLO 5 - Le interazioni tra safety e security 51
5.1 CORRELAZIONI 51
5.1.1 Interferenze negative 51
5.1.2 Combinazione positiva 53
5.2 APPROCCIO DI GESTIONE INTEGRATA 54
5.2.1 Modello per l’analisi delle correlazioni 56
5.2.1.1 Esempi di possibili scenari applicabili al modello 59
5.2.1.2 Implicazioni pratiche 60
5.3 ANALISI POST INCIDENTALE DI EVENTI CON CORRELAZIONE TRA SAFETY E SECURITY 60
5.3.1 Profondità dell’interferenza 63
CAPITOLO 6 - Il volo Philippine Airlines 434 65
6.1 RESOCONTO DEI FATTI 65
6.2 ANALISI DEGLI EVENTI 67
6.2.1 Eventi negativi 67
6.2.1.1 Il controllo degli accessi 67
6.2.1.2 Riconoscimento dell’attentatore 68
6.2.1.3 Segnalazione dei comportamenti sospetti 69
6.2.1.4 Protezione dei cavi di comando 69
6.2.1.5 Accesso ai dati dell’aeromobile 70
6.2.2 Eventi positivi 70
6.2.2.1 Capacità dell’equipaggio 70
6.2.2.2 Altri fattori casuali 71

6.3 IDENTIFICAZIONE DELLE CAUSE 72
6.4 CONSIDERAZIONI 76
6.4.1 Analogia con il volo United Airlines 232 77
6.4.2 Analogia con il disastro di Tenerife 78
CAPITOLO 7 - Il volo Germanwings 9525 79
7.1 RESOCONTO DEI FATTI 79
7.1.1 L'inchiesta incidentale 80
7.2 ANALISI DEGLI EVENTI 82
7.2.1 Sistema di chiusura della porta della cabina di pilotaggio 83
7.2.2 L'idoneità al volo 84
7.2.2.1 Gestione delle informazioni mediche 84
7.2.2.2 Il volo precedente 86
7.2.2.3 Misure contro l'inidoneità al volo del pilota 87
7.3 IDENTIFICAZIONE DELLE CAUSE 88
7.4 CONSIDERAZIONI 91
CONCLUSIONI 93
RIFERIMENTI BIBLIOGRAFICI 95

Introduzione

L'aviazione civile è un settore in costante crescita, rappresentando una delle attività di traino dell'economia mondiale. Crisi economiche e disordini geopolitici non hanno rappresentato un ostacolo all'aumento del traffico aereo, che, dal 2000 ad oggi, è più che raddoppiato. Annualmente il numero di voli cresce e continuerà a crescere di un valore superiore al 4%, vale a dire che in vent'anni sarà oltre il doppio del numero attuale. Una sempre maggior richiesta di spostamento da parte di persone, che per scelta o per necessità, utilizzano il sistema di trasporto aereo. Di questo passo, si stima che nel 2040 ci saranno più di 20 miliardi di passeggeri che prenderanno un aereo.

Un così grande incremento dell'attività rende inevitabilmente più complicato garantire gli adeguati livelli di sicurezza. L'aumento infatti riguarda la portata, ovvero il numero di passeggeri, ma anche la diffusione capillare del settore, con la creazione di sempre nuove infrastrutture e nuovi soggetti che vi operano. Le difficoltà di controllare tutte queste attività, senza inficiare l'efficienza del servizio, possono facilmente ridurre i livelli di sicurezza. E il problema della sicurezza è di fondamentale importanza, perché le conseguenze derivanti da eventuali lacune possono avere risvolti catastrofici. Non per niente, nonostante il sistema di trasporto aereo sia risaputo essere il più sicuro, l'opinione pubblica è ancora fortemente sensibile a incidenti o inconvenienti, anche non gravi, accorsi in volo.

Negli studi di sicurezza nell'aviazione, si deve considerare ogni minimo dettaglio, con un'analisi dettagliata ed eseguita a tutto tondo. Parlando di sicurezza è bene approfondire, sin dall'inizio, a quale contesto si fa riferimento. In italiano esiste un solo termine, sicurezza, per esprimere due parole che in inglese sono tra loro differenti: *safety* e *security*. Questi concetti vanno ad indicare due campi di applicazione che, pur essendo tra loro correlati, si discostano per gli obiettivi e conseguentemente anche per le misure adottate. Il primo termine esprime la sicurezza intesa come il garantire l'incolumità delle persone, prevenendo l'accadimento di eventi accidentali, attraverso velivoli affidabili e personale preparato. La security invece comprende l'insieme di misure messe in atto per contrastare atti intenzionali, compiuti per arrecare danno, quali attentati terroristici.

Queste due facce della sicurezza, per quanto possano sembrare lontane, in un settore complesso quale quello aeronautico, sono strettamente interconnesse tra loro. È questo l'obiettivo della tesi, indagare le correlazioni tra safety e security nel settore del trasporto aereo e negli eventi aeronautici. In particolare saranno analizzati dei casi studio, con l'utilizzo di metodologie dell'analisi post incidentale, per evidenziare tali relazioni.

Capitolo 1

Introduzione alla safety

1.1 Definizione

Quando si parla di safety si fa riferimento a quel campo della sicurezza inerente ai rischi di esercizio del velivolo e perciò orientato alla tutela della salute e dell'incolumità delle persone. La definizione di safety è associabile al concetto giuridico di colpa, quindi tutti quegli episodi in cui sono stati commessi errori accidentali, siano essi diretti o indiretti (di gestione delle operazioni), e che hanno portato a condizioni non sicure. Lo svolgimento di qualsiasi attività, comporta inevitabilmente un rischio, che, pur essendo ineliminabile, può essere ridotto ad un livello ritenuto accettabile. L'obiettivo della safety è sostanzialmente la prevenzione degli eventi accidentali, che possano creare danno a persone o cose, e l'adozione di misure protettive, necessarie nel caso si verificasse un incidente. La safety, per quanto riguarda gli altri settori lavorativi più comuni, è solitamente nota come sicurezza sul lavoro. Nel settore dell'aviazione civile, assume un'accezione più ampia e viene estesa anche alla salvaguardia della salute dei passeggeri e delle attrezzature. Safety concretamente significa disporre di mezzi efficienti ed affidabili che garantiscano assenza di guasti, personale preparato ed addestrato in grado di svolgere adeguatamente le proprie mansioni e di saper gestire le diverse situazioni nelle quali è chiamato ad intervenire.

1.2 Storia della safety

Pur esistendo voli di linea già dai primi decenni del XX secolo, l'aviazione commerciale iniziò ad assumere importanza economica e sociale solo dopo la II Guerra Mondiale. Da allora si è assistito ad un continuo e sempre maggiore aumento del trasporto aereo, giungendo ad oggi con quasi 9 miliardi di passeggeri ogni anno in tutto il mondo. Ruolo chiave per la crescita esponenziale del settore è il livello di sicurezza, che deve essere garantito, date le elevate conseguenze di un eventuale incidente. Dagli albori dell'aviazione commerciale sono stati fatti enormi passi in avanti, sia dal punto di vista tecnologico che umano. Ad oggi, si è

giunti a quello che rappresenta, assieme al settore dell'industria nucleare, uno dei sistemi più avanzati di gestione della sicurezza, tale da rendere il trasporto aereo il metodo di spostamento più sicuro disponibile.

L'evoluzione tecnologica ha, da sempre, dato un forte contributo al progressivo aumento del livello della safety. In particolar modo, i primi decenni dell'aviazione hanno visto il miglioramento incrementale delle componenti meccaniche, che hanno reso i velivoli sempre più affidabili e ed efficienti. Fino alla fine agli anni '60, rimase diffusa la convinzione che gli incidenti fossero conseguenza di guasti o di fallimenti della macchina. Perciò, lo sviluppo e le indagini rimasero focalizzate sul miglioramento tecnico dei velivoli, fino a quando, nonostante il livello tecnologico raggiunto, il numero di incidenti subì un aumento.

A partire dagli anni '70, l'attenzione si spostò verso il fattore umano, riconoscendo la limitazione delle sue capacità, e si cercò di analizzare la sua interazione con le macchine. Gli studi si concentrarono dapprima sull'ergonomia, ovvero la realizzazione di attrezzature e di strumentazioni facilmente adattabili agli operatori, e non più viceversa. Successivamente si introdusse una sempre crescente automazione dei sistemi, riducendo così il carico di lavoro umano. Semplificazione dei compiti dei piloti, regole per la gestione della fatica, addestramento, sono solo alcuni degli aspetti su cui si lavorò. Il concetto di fattore umano, per alcuni decenni, fu inteso limitatamente al singolo individuo, dove è l'operatore a sbagliare e tutti gli sforzi venivano fatti per limitarne l'errore. Procedure operative, addestramento e strumentazioni adeguate consentirono una netta riduzione degli incidenti, ma col tempo ci si rese conto che ciò non era sufficiente.

Fu solo a partire dagli anni '90 che si iniziò a parlare, per la prima volta, di errori organizzativi. Il fattore umano prendeva quindi un'accezione più ampia, contestualizzato nell'insieme di tutte le condizioni organizzative, e di come quest'ultime andassero ad incidere sul comportamento dei singoli. Ci si accorse che non è sufficiente fornire un ambiente di lavoro sicuro, con strumenti tecnologici, regole e personale addestrato, ma è fondamentale accertarsi che le condizioni di sicurezza rimangano tali. Le procedure possono non essere rispettate, le regole violate e le attrezzature fornite degradarsi e non essere più idonee. Una miglior sorveglianza, a tutti i livelli del sistema, è stata accompagnata dall'introduzione della cultura della sicurezza. Grazie ad una maggior consapevolezza e partecipazione, si è andato a ridurre sempre più l'errore umano, non più colpevolizzando il responsabile, ma individuando le condizioni che lo hanno portato a sbagliare.

Il monitoraggio continuo della sicurezza, tramite la raccolta dei dati, inizialmente introdotto come misura di controllo, ha portato, agli inizi del XXI secolo, alla nascita dell'attuale approccio basato sui sistemi di gestione. Fino ad allora, la sicurezza era stata realizzata prevalentemente in modo reattivo, ovvero in risposta a incidenti e inconveniente occorsi. I sistemi di gestione hanno facilitato l'applicazione di un approccio di tipo proattivo, anticipando possibili inconvenienti, grazie all'analisi dei dati raccolti e al riesame del sistema. L'implementazione del sistema di gestione garantisce vantaggi, semplificando notevolmente l'organizzazione ed il controllo del sistema, al punto da essere oramai considerata la prassi per organizzare la sicurezza di una qualsiasi azienda strutturata, specie nel settore aeronautico.

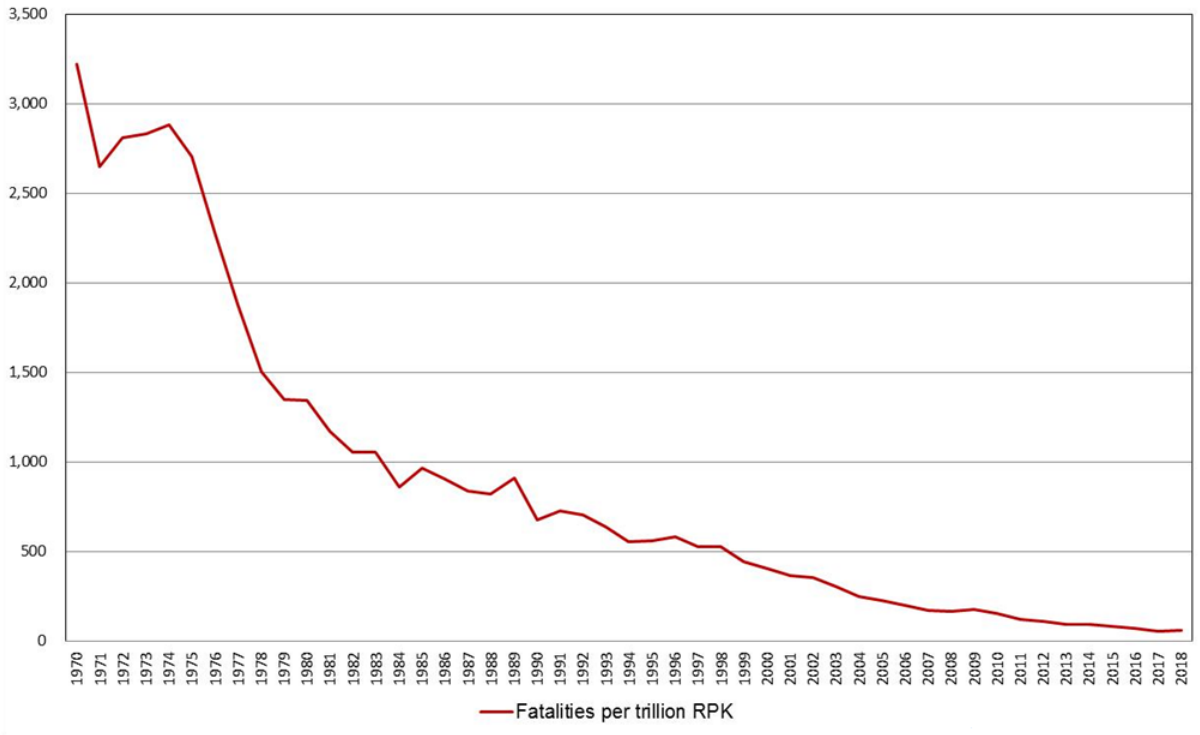

Figura 1.1. *Variazione del numero di morti per RPK (Revenue Passenger Kilometers, ovvero distanza percorsa da ciascun passeggero pagante) dal 1970 al 2018.*

Il continuo progresso ha portato a standard di sicurezza che oggi sono elevatissimi. Considerando l'incremento continuo del traffico aereo si può dire che la safety ha avuto un miglioramento esponenziale. Solitamente infatti, ad un aumento della produttività (in questo caso maggior numero di voli, distanze percorse e passeggeri trasportati) corrisponde una riduzione della sicurezza, ovvero maggior numero di incidenti. Secondo le statistiche ICAO, invece, anche considerando solo l'ultimo decennio, gli incidenti nel mondo si sono ridotti,

passando dai 139 verificatisi nel 2008, ai 98 del 2018. Questi dati, se confrontati con l'andamento del traffico aereo (in aumento di oltre il 4% ogni anno), mostrano andamenti opposti, segno che la sicurezza migliora in modo incrementale. Il grafico in figura 1.1 mostra esattamente questa tendenza: il numero di incidenti mortali, normalizzato per km percorsi, è in discesa, grazie sia alla minor frequenza con cui si verificano gli incidenti, che alla ridotte conseguenze quando questi accadono.

1.3 Definizione del rischio correlato alla safety

Nella safety aeronautica, il concetto di rischio è analoga a quella utilizzata in qualsiasi altro settore. Come viene riportato nel Manuale ICAO 9859, il rischio è una combinazione tra la probabilità che un incidente si verifichi (probabilità, P) e il danno che tale incidente può causare (severità, S).

$$R = P \times S. \tag{1.1}$$

Tale definizione può essere trasposta per realizzare una matrice di rischio, un metodo di valutazione semplice e intuitivo, al punto da essere comunemente usato in qualsiasi attività e che viene riportato anche da ICAO. Si vanno perciò a definire le righe e le colonne di tale matrice, corrispondenti rispettivamente a probabilità e severità.

Safety Risk		*Severity*				
Probability		*Catastrophic A*	*Hazardous B*	*Major C*	*Minor D*	*Negligible E*
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

Figura 1.2. *Matrice di rischio definita dal Safety Management Manual (DOC ICAO 9859)*

La probabilità è un valore che indica quanto è verosimile che una condizione pericolosa possa avere conseguenze, con danni a persone o cose. Alla probabilità può quindi essere assegnato

un valore secondo una scala numerica da 1 a 5, corrispondente alle condizioni di evento estremamente improbabile, improbabile, remoto, occasionale e frequente. Analogamente per la severità possiamo definire una scala composta da 5 categorie: trascurabile, minore, maggiore, pericoloso e catastrofico. Queste categorie definiscono quanto una determinata situazione può essere pericolosa. Le conseguenze di tali situazioni possono essere varie e spaziare da interruzione delle attività, ritardi dei voli, utilizzo delle procedure di emergenza, passando poi a danni materiali alle attrezzature o alle persone, fino alla distruzione del velivolo e alla morte di persone. Per ciascun pericolo, si può in questo modo quantificare il rischio correlato e valutarlo in relazione alla soglia di tollerabilità del rischio stesso. Per valori bassi il rischio sarà accettabile, richiedendo semplicemente il mantenimento della situazione attuale. Azioni di mitigazione saranno invece richieste per un rischio medio, anche se comunque rimane tollerabile. Contrariamente valori elevati di rischio, sono da considerarsi inaccettabili e si deve intervenire immediatamente, per ridurre il rischio, o interrompere le attività.

1.4 Approccio alla safety

Il sistema di gestione della sicurezza (*safety management system*) è alla base dell'organizzazione della safety nell'aviazione. Caratteristica chiave è il controllo costante sul sistema, tramite la raccolta di dati e parametri relativi alla sicurezza. Definendo dei parametri di valutazione, noti come *safety performance indicator*, si possono valutare le prestazioni complessive dell'azienda e monitorare l'andamento della sicurezza. Queste informazioni sono fondamentali per comprendere dove è necessario intervenire e mettere in atto azioni correttive. Con l'implementazione del sistema di gestione infatti, non ci si limita ad adempiere agli obblighi normativi, ma si mette in atto un processo di miglioramento continuo dell'azienda, garantendo così un livello di sicurezza sempre maggiore. È in questo modo che si sono raggiunti gli attuali livelli di sicurezza. Tutti gli standard per i sistemi di gestione sono sviluppati secondo una schema, definito *high level structure*. Questo definisce una struttura circolare delle operazioni, con continuo monitoraggio e miglioramento del sistema stesso, definito attraverso quattro fasi:

- *plan*, ovvero la pianificazione delle attività produttive, con individuazione dei processi, delle procedure e delle risorse da impiegare;

- *do*, che è la realizzazione di quanto programmato in precedenza, nel rispetto delle politiche dell'azienda;
- *check*, cioè il monitoraggio e la verifica del raggiungimento degli obiettivi e dei risultati programmati;
- *act*, inteso come l'individuazione di misure correttive per il miglioramento del sistema, tramite il riesame della direzione.

L'implementazione della safety può essere svolto con diversi tipi di approccio: reattivo o proattivo. Si può agire in risposta alle condizioni già presenti in azienda, ovvero analizzare le carenze che si sono verificate e correggerle in modo da evitare il ripetersi di tali situazioni. L'approccio proattivo invece anticipa quelli che saranno i possibili pericoli e attua delle misure preventive. L'applicazione del sistema di gestione permette l'integrazione dei due approcci, ottenendo un notevole vantaggio. L'analisi dei dati raccolti con il monitoraggio, infatti, definisce un quadro della situazione attuale, ma allo stesso tempo permette anche di individuare le tendenze di sicurezza, che, proiettate nel futuro immediato, consentono di prevedere possibili situazioni critiche. L'analisi proattiva risulta particolarmente utile in presenza di variazioni sostanziali del sistema, come l'introduzione di nuove procedure, attrezzature o personale. L'elaborazione e l'adattamento delle informazioni, raccolte in occasioni di modifiche analoghe attuate in precedenza, consentono di prevedere il comportamento del sistema ed adottare preventivamente misure contro i probabili rischi.

Il sistema di gestione della sicurezza è uno strumento molto utile anche per la gestione delle risorse, problema non da poco per un corretto funzionamento dell'azienda. È necessario, infatti, mantenere un giusto equilibrio tra produzione e sicurezza. Trascurare la sicurezza, per puntare tutto sulla produttività, avrà come conseguenza inevitabile il verificarsi di un incidente, con conseguenze anche gravi e probabili ripercussioni sull'azienda (danni economici, d'immagine, mancata produzione, ecc.). Viceversa, tentare di ridurre rischi già di per sé accettabili porta solo a spese eccessive, che possono mettere in difficoltà le capacità produttive della società e portarla a bancarotta. Nel grafico sicurezza-produttività (figura 1.3), si individua una fascia nella quale rimanere per poter avere un funzionamento ottimale dell'azienda. È necessario quindi indirizzare le risorse in un modo da ottimizzarne i benefici, ovvero mitigando quei rischi in cui, a fronte di una spesa minore, le misure adottate hanno maggior effetto. Al di fuori della zona di sicurezza (*safety space*), ricadiamo nelle situazioni

estreme di bancarotta, per eccessivi investimenti, e di catastrofe, conseguente a sicurezza inadeguata.

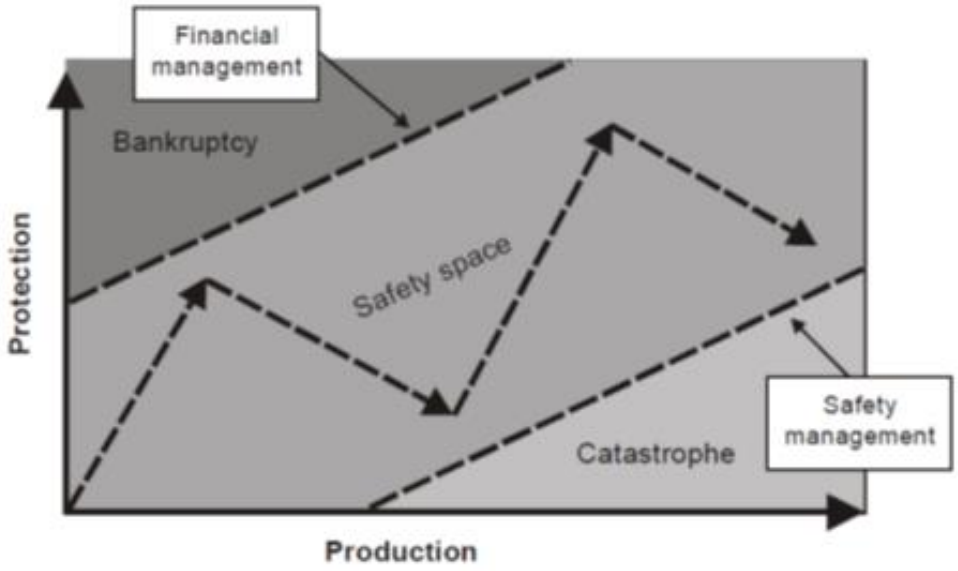

Figura 1.3 *Grafico produttività – sicurezza. La zona di safety space è individuata dall'equilibrio tra produzione e sicurezza*

1.5 Valutazione del rischio safety

In precedenza abbiamo visto la definizione qualitativa di rischio, per mezzo della matrice di rischio. Questo approccio, dal punto di vista pratico, risulta semplice e di immediata applicazione. Per questo è ampiamente utilizzato in ambienti lavorativi comuni, ma nel settore aeronautico, la semplice definizione qualitativa del rischio risulta limitativa e semplicistica. La ridotta precisione e superficialità delle informazioni, possono fornire un'immagine non esaustiva del rischio che si sta valutando, dati i numerosi fattori che entrano in gioco in un evento aeronautico. Per questo è necessario implementare il concetto della matrice di rischio, sviluppando modelli di tipo probabilistico, che fanno uso di variabili per la quantificazione numerica dei fattori. La formula per la definizione del rischio, pur rimanendo invariata nel concetto, risulta così modificata:

$$R = Se \times \varphi. \tag{1.2}$$

Dove: S_e: Severità; φ: Frequenza.

La severità è ricalcolata in relazione agli impatti che il fattore organizzativo ed il contesto ambientale possono avere sull'esito dell'evento. La severità risulta perciò così definita:

$$Se = Sa \times \frac{fo + fc}{2}. \tag{1.3}$$

S_e, il nostro valore finale, rappresenta la severità effettiva dell'evento ed è ottenuta dalla combinazione di tre fattori:

- S_a, la severità assoluta, è definita su una scala da 1 a 5 ed indica il livello intrinseco di pericolosità dell'evento, indipendentemente dal contesto in cui si verifica.
- f_o è il fattore di impatto organizzativo, compreso tra 1 e 1,5, che va a considerare le ripercussioni che un definito evento ha sull'operatività della organizzazione, sia in termini di produttività che di danno economico.
- f_c, infine, è il fattore di impatto contestuale; esso è correlato al contesto ambientale e fisico in cui l'evento si verifica. Questo fattore, come il precedente, è variabile tra 1 e 1,5, e dipende da diversi fattori, come caratteristiche ambientali e meteorologiche, o condizioni fisiche e psicologiche degli operatori.

Anche la definizione della probabilità cambia. Non più classificata solo qualitativamente, si quantifica numericamente la frequenza con cui l'evento in analisi si manifesta. La frequenza è calcolata come:

$$\varphi = \frac{Na}{Nt}. \tag{1.4}$$

I parametri indicano rispettivamente:

- N_a è il numero di volte in cui l'evento si verifica in un determinato arco di tempo (solitamente un anno).
- N_t è un valore assoluto che fornisce un riferimento sul totale delle operazioni svolte e, a seconda delle attività, tiene in considerazione un diverso parametro. Esso quindi indica: il numero totale di ore di volo se si tratta di una compagnia aerea, il numero totale di interventi per le operazioni di manutenzione e il numero totale di movimenti di terra nel caso di un aeroporto.

Attraverso questa formulazione possiamo eseguire delle valutazioni complete e precise, sulla base delle quali ottimizzare gli interventi di miglioramento del sistema.

Capitolo 2

Introduzione alla security

2.1 Definizione

Con il termine security si intende la prevenzione di atti intenzionali di interferenza illecita (*unlawfull interference*), i quali hanno come obiettivo creare danno alle persone o alle cose. Dal punto di vista giuridico tali azioni rientrano nella definizione di dolo, essendo compiuti con il proposito di offendere. Sono compresi quindi gli atti di terrorismo, quali attentati e dirottamenti, gli atti vandalici, gli attacchi informatici e lo spionaggio. A differenza della safety, le cui cause sono da ricercare esclusivamente all'interno dell'azienda, le minacce di security sono prevalentemente di tipo esterno. Da sempre l'aviazione civile è stata bersaglio di attacchi da parte di terroristi, perché colpire un settore come quello aereo garantisce eclatanza a livello globale e forte impatto sull'opinione pubblica. Episodi di questo genere, molto frequenti nei primi decenni del settore aereo, sono notevolmente ridotti specialmente dopo gli episodi dell'11 settembre 2001, con un intensificamento dei controlli degli accessi negli aeroporti e un miglioramento della strumentazione impiegata. L'efficacia della security aeroportuale è ormai tale che episodi di terrorismo, a bordo di aerei, sono praticamente inesistenti, riversandosi piuttosto su altri settori meno controllati (vedasi l'utilizzo di automezzi o autoveicoli per compiere attentati). I problemi inerenti alla security sono comunque non da sottovalutare, soprattutto per la continua evoluzione e la diversità dei mezzi impiegati. Al giorno d'oggi, si affrontano sempre nuove sfide, come il costante aumento degli attacchi informatici, o la facilità con cui è possibile reperire droni, il cui utilizzo può rappresentare una sorgente di pericolo.

2.2 Storia della security

L'aviazione civile, da quando iniziò ad avere un ruolo chiave nella società ed economia mondiale, divenne uno degli obiettivi principali di attentatori e terroristi. Per i gruppi di attivisti, colpire voli di linea garantiva visibilità e impatto sulla gente. Nei primi decenni

furono presenti molte difficoltà nel contrastare questi fenomeni, che divennero sempre più frequenti. Inoltre il costante aumento del traffico aereo, rese complicato e lento l'intervento per contenere i tentativi di attentati. Negli anni '70 e '80, gli episodi di dirottamento e presa in ostaggio a bordo dei voli di linea furono i più frequenti, il più delle volte con lo scopo di negoziare la liberazione di prigionieri, o ottenere richieste politiche o l'estorsione di pagamenti. I controlli agli accessi negli aeroporti, incrementati in risposta a tali azioni, riuscirono a ridurre l'introduzione di articoli proibiti, ma allo stesso tempo spinsero gli attentatori a trovare soluzioni alternative, per aggirare le barriere adottate. Ne è esempio l'impego di armi di dimensioni sempre più ridotte o il camuffamento delle stesse in oggetti di uso comune. Gli episodi di bombe a bordo degli aerei seguirono esattamente questa tendenza. Inizialmente gli esplosivi erano nascosti semplicemente in zaini e valigie, che venivano imbarcati o abbandonati a bordo. Questo fenomeno, che prese piede a partire dalla metà degli anni '80, portò alla realizzazione di bombe sempre più studiate, arrivando alla miniaturizzazione degli ordigni, negli anni '90. Si vedrà successivamente, in un caso studio, di una bomba realizzata con un orologio da polso come timer e l'esplosivo nascosto in un contenitore di liquido per lenti a contatto.

L'11 settembre 2001 rappresentò la vera svolta nell'approccio alla security. Per la prima volta degli aerei, dopo essere stati dirottati, furono usati, con successo, come armi per colpire degli obiettivi più grandi. Da allora gli Stati Uniti e i Paesi europei, adottarono delle strategie di cooperazione contrastando efficacemente il fenomeno del terrorismo nell'aviazione civile. Gli attacchi terroristici si sono quindi maggiormente concentrati in quelle aree dove i controlli sono minori e dove è maggiore la presenza di gruppi terroristici. In alcune zone gli attentati non sono diminuiti ma anzi si sono intensificati: Nord Africa, Medio Oriente, l'area sub-Sahariana (Somalia) ed alcuni Stati asiatici sono le zone dove, negli ultimi anni, si sono registrati un maggior numero di attentati. Gli attacchi sono prevalentemente bombe a bordo, introdotte talvolta anche da personale interno, ma persino attacchi missilistici sia contro aerei in volo sia contro gli aeroporti.

Nei Paesi con minor attentati, la questione security non va comunque sottovalutata. Infatti sono sempre più frequenti nuovi fenomeni, diversi degli attacchi classici, ma che comunque possono rappresentare una minaccia concreta. Tra questi si può citare l'utilizzo di droni, la cui diffusione è sempre maggiore e la loro applicazione è molto diversificata. Ad esempio, li si può utilizzare per attività di intelligence, ovvero raccolta di immagini e informazioni, con le

quali poter programmare un attacco. Oppure gli stessi potrebbero anche essere usati come armi per causare danni all'aeromobile. Si sono già verificati, negli ultimi anni, episodi di impatti in volo con aeromobile in decollo o in fase d'approccio. Questi scontri, pur essendo non intenzionali e privi di conseguenze rilevanti per il velivolo, sono un segnale della pericolosità di tali attrezzature. Alcuni attentati hanno visto l'uso di droni caricati con esplosivo, contro particolari obiettivi, e non è escluso che tale tecnica possa essere riproposta, per colpire proprio il settore dell'aviazione civile.

L'uso di laser, per disturbare i piloti durante le fasi di approccio, è un altro fenomeno in crescente aumento. Le operazione di atterraggio sono solitamente eseguite tramite volo strumentale, per cui l'accecamento momentaneo del pilota è comunque compensato dai supporti elettronici. Alcuni laser però sono risultati particolarmente potenti, arrivando addirittura a causare danni alla retina di alcuni pilota. Sono facilmente immaginabili le complicazioni che ciò può comportare allo svolgimento delle operazioni in volo, pur con il supporto dei sistemi informatici.

Infine, ma non meno rilevate è il cyber terrorismo, dato che la sempre maggior informatizzazione dei sistemi offre notevoli opportunità di attacco. Generalmente gli attacchi informatici, si limitano ad un danno virtuale, come può essere il furto di informazioni e dati sensibili o l'accesso alle funzionalità di un sistema informatico. Nel 2015, ad esempio, la compagnia aerea nazionale polacca fu oggetto di un attacco hacker, che mise fuori uso il sistema che emetteva i piani di volo, causando così la cancellazione e il ritardo di decine di voli. Episodi del genere sono inevitabilmente seguiti da una perdita di immagine per l'azienda, e quindi, indirettamente, ad un danno economico anche rilevante. Ma gli strumenti informatici potrebbero essere utilizzati anche per causare danni reali, ad esempio prendendo il controllo di un sistema di comando connesso ad una rete. Proprio per quanto riguarda il settore aereo, nel 2014 fu rivelata l'effettiva possibilità di violare il sistema di controllo dell'aeroplano, dai sedili dei passeggeri, attraverso la connessione Wi-Fi di bordo. Infatti, se la comunicazione tra la rete dei passeggeri e quella del cockpit non è sufficientemente protetta, è possibile sfruttare le lacune per accedere ai sistemi di comando. Un attacco di questo genere renderebbe, di fatto, inutili le misure antintrusione della cabina di pilotaggio finora adottate per contrastare i dirottamenti, con conseguenze catastrofiche.

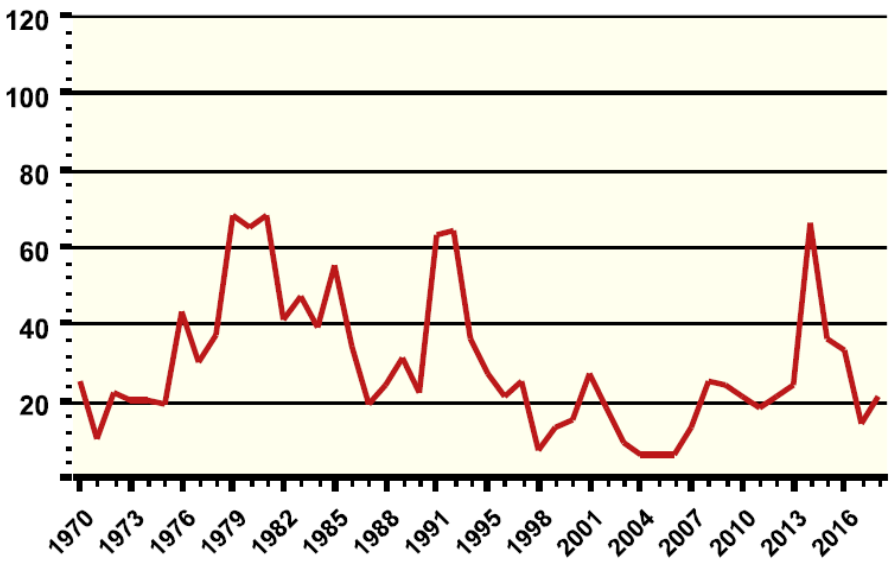

Figura 2.1. *Numero di azioni terroristiche compiute contro l'aviazione civile mondiale per anno, dal 1970 al 2018 (fonte Global Terrorism Database).*

A conferma di quanto affermato in precedenza, il grafico in figura 2.1 mostra l'andamento discontinuo del numero di attentati compiuti contro l'aviazione civile, a livello globale. Al contrario della safety, dove abbiamo una tendenza in costante diminuzione, in security c'è una continua contrapposizione tra l'adozione di misure e il verificarsi di nuove fenomeni di terrorismo. Abbiamo quindi periodi di riduzione degli eventi, come gli anni immediatamente successivi al 2001, dove le misure messe in atto riescono a contenere efficacemente gli attentati. In altri periodi invece, l'attività dei terroristi prende il sopravvento, come il picco del 2014, dovuto all'intensificamento dell'attività dell'ISIS, concentrata soprattutto in Libia, Somalia e Pakistan.

2.3 Definizione del rischio correlato alla security

La definizione di rischio security, ricalca quello visto per la safety, ma si discosta per la tipologia di pericolo che viene analizzato. Il concetto di base rimane invariato, ovvero che la combinazione tra la frequenza e il danno definisce il valore del rischio, relativo ad un determinato pericolo. Questo pericolo, però, non è più una caratteristica intrinseca dell'ambiente lavorativo, ma si identifica con una minaccia esterna. Esso può essere individuato come qualsiasi attività che può causare danni o generare esposizione ad azioni malevoli. Nella security, quindi, non si valuta più la probabilità di accadimento di un

determinato evento accidentale, ma piuttosto la possibilità che una minaccia possa avere successo, sfruttando le vulnerabilità del sistema.

Si introducono perciò due concetti chiave: la vulnerabilità e la minaccia. Il primo termine, pur non esistendone una definizione esatta, è associato al livello con cui una struttura è protetta. Più precisamente la vulnerabilità può essere definita come l'insieme di difetti e debolezze di un'infrastruttura, o di un sistema, che la rendono esposta a pericoli e minacce, che possono danneggiarla o interromperne la capacità operativa. In altre parole, si può indicare la vulnerabilità come il grado con cui il sistema avrà probabilità di subire danni e conseguenze, a causa dell'esposizione a interferenze e forzature esterne.

Per quanto riguarda il secondo concetto, la minaccia, essa è determinata dalla probabilità che venga condotto un attacco contro uno specifico obiettivo, in un definito lasso di tempo. Va quindi individuata una specificità, ovvero un obiettivo preciso a cui l'attacco è indirizzato, come può essere ad esempio un volo con a bordo delle persone, verso cui gli attentatori vogliono creare il danno. La minaccia, per essere considerata tale deve possedere una determinata credibilità, ovvero una combinazione tra l'intenzione e la capacità. L'intenzione presuppone l'esistenza di un gruppo attivista o anche di singoli elementi, guidati da una motivazione, sia essa di carattere religioso, sociale o economico, che li spinga a compiere determinate azioni malevoli. Allo stesso tempo, tali soggetti devono avere la capacità effettiva di compiere tali azioni, ovvero devono disporre, anche solo potenzialmente, dei mezzi e delle risorse necessarie a mettere in atto un piano d'attacco.

Ritornando alla definizione del rischio security, il danno è banalmente determinato dalla gravità delle conseguenze di un attacco. La frequenza invece può essere definita come la combinazione tra la probabilità di subire un attacco e la probabilità che le difese messe in atto falliscano, consentendo il successo dell'attacco. Quindi, il rischio security può essere formulato come segue:

$$R = (T \times V) \times S. \tag{2.1}$$

Dove: T: minaccia (T*hreat*);

V: vulnerabilità (*Vulnerability*);

S: danno (*Severity*).

Per quanto riguarda la definizione del danno, va aggiunta una considerazione. Il rischio security, nella sua accezione più classica, prevede misure protettive da atti il cui scopo è creare danno a persone e cose. In questo senso, quindi, la severità è direttamente dipendente dalle conseguenze immediate dell'attacco. Ciò significa che, per la sua determinazione, si terrà conto della gravità delle ferite riportate dalle persone, dei danni subiti dalle attrezzature e dalle infrastrutture. Ma gli effetti di un attacco potrebbero essere anche di tipo non materiale, ovvero indebolire o rendere inefficace una struttura o un sistema. Particolare importanza, in questo senso, viene assunta dal concetto di infrastruttura critica. Questa è definita come una risorsa, il cui funzionamento ricopre un ruolo fondamentale all'interno della società o di un'organizzazione. L'interruzione del servizio di un'infrastruttura strategica, sia tale indisponibilità totale, temporanea o anche solo parziale, si ripercuote sull'intero sistema, intaccandone il corretto funzionamento e la sicurezza. Tali infrastrutture sono solitamente associate a servizi quali energia, trasporti, telecomunicazioni e sistemi informatici, ma anche sanità e servizi di emergenza. La mancanza di uno di questi servizi può avere effetto negativi sulle altre strutture, creando disordini e vulnerabilità, divenendo maggiormente esposte a possibili attacchi.

2.4 Approccio alla security

In opposizione con la safety, dove il rischio è più logico e facilmente prevedibile, la security richiede grande e costante capacità di adattamento. La minacce possono diversificarsi enormemente tra loro per obiettivi, metodi e mezzi, così come una stessa minaccia può evolversi nel tempo, adottando tecniche sempre diverse. Le misure di security, di conseguenza, non si dovrebbero basare solo sulle esperienze passate, ma richiedono una certa dinamicità, nel prevedere e anticipare le mosse di chi potrebbe attaccare. Storicamente elaborare tali azioni si è sempre rivelato essere un'impresa non da poco e spesso non efficace. Solitamente, si sono adottate misure in protezione da una tipologia di attacco, dopo averlo subìto, ma l'attentatore sarà così portato a studiare una strategia alternativa, che aggiri tale contromisura. Una misura, per quanto innovativa ed efficace nel breve periodo, a lungo termine potrebbe essere facilmente eludibile. Questo perché le tecniche di attacco diventano costantemente più affinate, richiedendo misure di difesa altrettanto efficaci, che riescano a contrastarle. Così come vengono sviluppate nuove attrezzature per la difesa, l'evoluzione

tecnica favorisce anche gli attentatori, che sfruttano le nuove tecnologie, adattandole ai loro fini.

Attualmente la maggior parte degli sforzi di security si focalizzano sul controllo degli accessi, in modo da assicurare un ambiente sicuro entro il quale operare. Oltre alle classiche attrezzature per lo screening, ovvero metal detector e machine ai raggi X per i bagagli, si sono aggiunti strumenti in grado di rilevare la presenza di esplosivi. Questi strumenti, specializzati per esplosivi solidi (ETD, *Explosive Trace Detection System*) e liquidi (LEDs, *Liquid Explosive Detection System*), possono rilevare anche tracce residue delle sostanze, riducendo, assieme alla limitazione nel trasporto di liquidi, il rischio di bombe a bordo degli aeromobili. Tutte queste misure potrebbero comunque non bastare, per questo è necessario implementare un sistema di controlli a più livelli. L'analisi comportamentale è un'altra procedura che va a sommarsi all'insieme dei controlli. Tentare un'azione illecita, in un ambiente altamente controllato e sorvegliato, crea sicuramente ansia e stress, sensazioni difficili da mascherare a lungo e che spesso il corpo trasmette inconsciamente. Personale addestrato a captare questi segnali, tramite l'osservazione dei comportamenti dei passeggeri, permette di individuare preventivamente criminali o terroristi. Infine, vanno citate le liste "No Fly", degli elenchi in cui la varie Nazioni inseriscono le generalità dei sospettati di coinvolgimento con il terrorismo. Agli individui, che sono indicati su questa lista, non è consentito viaggiare su aerei commerciali, oppure, se è consentito, devono essere sottoposti ad ulteriori controlli. Questa misura, risulta particolarmente efficiente, se impiegata in combinazione alle nuove tecnologie, come il riconoscimento facciale biometrico, consentendo di individuare terroristi anche quando camuffati sotto falsa identità.

Nella discussione complessiva della security, va tenuto conto del fatto che la diffusione capillare del trasporto aereo ha ripercussioni sulla sicurezza del sistema complessivo. In tutte quelle aeree dove, per mancanza di risorse, i controlli sono inferiori, i terroristi possono ancora facilmente agire e colpire. Alcuni Paesi, a causa di uno sviluppo tecnico e tecnologico non ancora maturo, presentano infrastrutture più vulnerabili e per questo sono diventati i principali obiettivi di attentatori. Se a tale fattore si aggiunge un'elevata attività di gruppi terroristici, il rischio security risulta notevole. Come visto in precedenza questa situazione è particolarmente rilevante in alcuni Paesi africani e del Medio Oriente. Qui i livelli di sicurezza ridotti, non solo presentano diverse vulnerabilità dalle minacce esterne, ma vi è una notevole esposizione anche a quelle interne. Ad esempio, è più probabile che terroristi o loro

collaboratori riescano ad infiltrarsi come operatori presso gli aeroporti o nelle compagnie aeree, a causa di un insufficiente controllo interno. Non a caso, proprio nelle Nazioni sopracitate, anche recentemente, si sono verificati alcuni episodi di personale che ha introdotto bombe a bordo degli aerei. Mentre in Europa il Reg. 103/2019 obbliga ad attuare il controllo dei precedenti penali (*background check*) annualmente, negli altri Paesi è solitamente previsto ogni 5 anni, il che rende più complessi l'individuazione e il monitoraggio di minacce interne. La presenza di situazioni locali con sicurezza inferiore ha, però, ripercussioni considerevoli sull'intero sistema di trasporto aereo, rappresentando un pericolo anche per quei Paesi in cui i controlli sono efficaci. Come misura per evitare conseguenze indirette, sono stati proibiti i voli provenienti da tutti quei Paesi con elevata presenza di gruppi terroristici oppure in cui gli aeroporti non siano in grado di garantire adeguati livelli di sicurezza.

Anche le procedure necessitano di un continuo monitoraggio e miglioramento. In mancanza di adeguata supervisione, è facile che gli operatori non rispettino tutte le operazioni richieste, ampliando le vulnerabilità del sistema. Soprattutto perché le regole di security che vengono fornite sono rigide e vanno applicate, anche se in alcuni casi possono sembrare prive di senso. Infatti, proprio per il concetto alla base della security, ovvero della non divulgazione delle informazioni sensibili, spesso gli operatori non sono a conoscenza delle ragioni alla base dell'applicazione di una determinata misura. Risulta prevedibile che in presenza di procedure scomode, come potrebbe essere per l'equipaggio di bordo il dover passare più volte i controlli durante il turno lavorativo, gli operatori siano portati ad aggirare alcune regole o a non eseguire tutti i passaggi della procedura. Ulteriore punto fondamentale è la non prevedibilità delle procedure. Se quest'ultime sono costanti e non evolvono nel tempo, per chi è intenzionato ad aggirarle, sarà più facile studiarle e sfruttarne i punti critici. Un esempio di questa applicazione sono i controlli a campione dei passeggeri, che vengono eseguiti in modo casuale, al punto che nemmeno gli operatori stessi sono a conoscenza dell'ordine con cui effettuarli. Così, né minacce interne né minacce esterne potranno disporre di una vulnerabilità certa, su cui organizzare un'azione.

Analogamente alla safety, anche nella security la gestione delle risorse copre un ruolo chiave. L'elevato investimento in misure di difesa può essere un spesa inutile, così come trascurare le security aumenta notevolmente le probabilità di essere soggetti ad attacchi e che questi abbiano successo. Spesso, l'obiettivo di un attentato terroristico, diventa tale proprio per la

presenza di numerose vulnerabilità, piuttosto che per l'importanza o per il ruolo assunto dell'infrastruttura colpita. È di fondamentale importanza saper investire in modo mirato le risorse disponibili e per fare ciò è necessario mettere in atto un piano di intelligence, mirato ad individuare le possibili minacce. Risulta inutile difendersi da determinate tipologie di attacchi, quando è altamente improbabile che vengano messi in atto, sia per intenzione (nessun gruppo attivista interessato all'obiettivo) che per capacità (i gruppi con tale obiettivo non dispongono dei mezzi necessari per superare la misure già messe in atto). Se invece una minaccia è credibile, rafforzare le difese assume priorità maggiore. Notoriamente gli attacchi terroristici sono preceduti da una intensa attività di propaganda, che al giorno d'oggi viene messa in atto in rete. Riuscire a rilevare i segnali che preannunciano questi eventi è vitale, per evitare di trovarsi impreparati. In accordo con l'Annesso 17 ICAO, ciascuna Nazione deve tenere sotto costante controllo il livello e la natura della minaccia per l'aviazione, modificando il proprio Programma Nazionale di sicurezza, con adeguate misure e procedure contro gli atti di interferenza illecita. Sulla base delle informazioni raccolte dalla attività di intelligence, verranno indicate misure specifiche, che ciascun gestore o operatore dovrà adottare, per garantire la sicurezza delle proprie operazioni.

Un altro punto chiave per la security, sulla linea dei sistemi di gestione per la safety, sono i piani di qualità. Messi in atto da ogni Nazioni, ai sensi dell'Annesso 17 ICAO, i Programmi per il controllo della Qualità della sicurezza sono essenziali, per il monitoraggio e la verifica della corretta attuazione delle misure di security. Ciascun soggetto organizza le attività di controllo interne, su una struttura che ricalca un sistema di gestione della qualità. Il controllo di qualità si basa su un insieme di attività, che prevedono lo svolgimento di audit, l'effettuazione di ispezioni e test, con successiva gestione del follow-up quando necessario. Particolar importanza è ricoperta dai test di attenzione, in cui un auditor, in qualità di passeggero, tenta di introdurre dei simulacri di articoli proibiti all'interno dell'area sterile. Lo scopo è verificare la correttezza e l'efficacia nell'esecuzione delle operazioni di controllo, ma anche la conformità delle procedure attivate all'individuazione del simulacro. Questo tipo di verifiche, che devono essere previste dal controllo di qualità interno, vengono eseguite anche dalle autorità competenti, in Italia nello specifico da ENAC.

2.5 Valutazione del rischio security

Le metodologie che possono essere impiegate per la valutazione del rischio security sono analoghe a quelle solitamente utilizzate per la analisi di safety. Nell'approccio pratico alla security si è soliti utilizzare una matrice di rischio, chiamata *security risk matrix*. Essendoci lo stesso concetto di base, la struttura è analoga a quella vista per la safety, con un danno sulle colonne e una probabilità sulle righe. Riguardo quest'ultima variabile, la sua determinazione risulta particolarmente complessa, per questo può essere individuata in modo semplificato, identificandola con la vulnerabilità del sistema. Infatti, tenere in considerazione la probabilità di successo della minaccia potrebbe non avere senso, a causa dei molteplici fattori che concorrono a condizionare gli eventi. Considerare la vulnerabilità come parametro per la probabilità, invece risulta un'alternativa più efficace, consentendo di ottenere un'analisi più oggettiva. Ciò è possibile, associando alla vulnerabilità quantità misurabili del livello di protezione offerto dalle barriere previste. Per quanto riguarda la protezione materiale dei locali e degli ambienti di una struttura, esistono tre livelli di protezione attuabili:

- Controllo, costituito dalle attività di visita e ispezione dell'ambiente, svolte fisicamente da parte del personale;
- Sorveglianza, ovvero il controllo visivo a distanza, anche attraverso telecamere;
- Scudi e protezioni, posti come barriere fisiche e funzionali contro le intrusioni.

Quindi, in relazione alla presenza o meno delle suddette misure, si possono stabilire cinque classi di vulnerabilità.

- Esposto: quando non è presente alcuna barriera e l'ambiente è raramente controllato.
- Ragionevolmente esposto: equivalente ad ambienti non protetti, ma sorvegliati e controllati.
- Protetto: sono presenti tutti e tre i livelli di protezione, con un servizio minimo garantito.
- Molto protetto: l'ambiente è completamente controllato, sorvegliato e protetto.
- Estremamente protetto: quando le misure impiegate sono sofisticate ed hanno un elevato livello di continuità. Il livello di vulnerabilità per questa categoria è minimo.

Come per la safety, il danno, causato dall'attacco, può essere classificato in cinque livelli:

- Trascurabile: nessuna persona ferita e nessuna o minima conseguenza sul servizio.
- Minore: danni minimi a persone, che non richiedono il ricovero, ma ritardi sul servizio per la manutenzione necessaria.
- Maggiore: persone ferite, con ospedalizzazione, ma tempi di recupero totale brevi.
- Pericoloso: ferite gravi, con ospedalizzazioni lunghe e possibili disabilità permanenti; danni estremamente gravi agli ambienti e alle strutture.
- Catastrofico: perdite di vite umane e distruzione dell'infrastruttura.

La combinazione, dei valori della vulnerabilità con quelli della severità, ci fornirà un valore identificativo del valore di rischio. Esso potrà essere: accettabile (livello 4), richiedere un successivo monitoraggio (livello 3), necessitare di un'analisi con misure supplementari (livello 2) o essere non accettabile (livello 1). Tali valori, pur essendo qualitativi, risultano comunque molto efficaci e permettono una valutazione precisa del rischio.

	Severity Level				
Vulnerability Level	**S1 Negligeable**	**S2 Minor**	**S3 Major**	**S4 Hazardous**	**S5 Catastrophic**
L5 Exposed $Vul > V_4$	3	2	1	1	1
L4 Reasonably exposed $V_3 < Vul \leq V_4$	3	2	2	1	1
L3 Protected $V_2 < Vul \leq V_3$	4	3	2	2	1
L2 Greatly protected $V_1 < Vul \leq V_2$	4	3	3	2	1
L1 Extremely protected $Vul \leq V_1$	4	4	4	3	2

Figura 2.2. *Matrice di rischio security*

Capitolo 3

Il quadro normativo

La sicurezza nel mondo dell'aviazione civile copre un ruolo di importanza fondamentale, in particolar modo per le notevoli conseguenze che un incidente può avere. Garantire voli sicuri ha anche vantaggi indiretti, come una miglior immagine del sistema di trasporto stesso, un dettaglio non da poco, visto l'alta sensibilità dell'opinione pubblica in merito. La normativa aeronautica si è sviluppata man mano che il settore cresceva, diventando sempre più stringente, al fine di garantire un funzionamento efficace del sistema. Ad oggi la normativa può essere divisa in diversi livelli:

- gli accordi internazionali, che regolamentano gli spostamenti tra i vari Stati nel mondo;
- la normativa europea, più stringente e che garantisce standard più elevati tra i vari Paesi comunitari;
- la legislazione nazionale, identificabile come il recepimento e l'attuazione delle disposizioni di livello superiore;
- infine i regolamenti aeroportuali, cioè l'insieme di procedure e regole stabilite dal gestore, per assicurare la sicurezza di tutte le operazioni all'interno della struttura.

3.1 La normativa internazionale

A livello mondiale la figura di riferimento è ICAO, un'agenzia che elabora principi e tecniche, che gli Stati aderenti devono applicare, al fine di garantire la sicurezza e l'efficienza del trasporto aereo internazionale. L'organizzazione fu costituita nel 1944 a seguito della Convenzione di Chicago e ha sede a Montreal. Gli accordi presi in occasione della Convenzione rispecchiano i principi di uguaglianza e di uniformità tra tutti gli Stati. Ad oggi, vi aderiscono 193 Nazioni, che collaborano al fine di promuovere e assicurare un adeguato livello di sicurezza all'intero sistema di trasporto.

Pur non sostituendosi alle leggi locali degli Stati, tutti i voli internazionali devono rispettare quanto stabilito dalla disciplina emessa da ICAO. L'attività normativa viene pubblicata attraverso gli "Annessi", ovvero 19 documenti che rappresentano di fatto lo standard da applicare per ottenere un livello idoneo di sicurezza, in tutte le fasi di volo. Sono poi gli Stati aderenti a sviluppare una loro regolamentazione, tale da garantire il rispetto delle disposizioni stabilite da ICAO.

Di seguito si riporta l'elenco e i relativi argomenti degli annessi.

Annesso 1: Licenze del personale
Annesso 2: Regole dell'aria
Annesso 3: Meteorologia
Annesso 4: Carte di navigazione
Annesso 5: Unità di misura da usarsi nelle comunicazioni terra/bordo/terra
Annesso 6: Operazioni degli aeromobili
Annesso 7: Marche di nazionalità e di immatricolazione degli aeromobili
Annesso 8: Aeronavigabilità degli aeromobili
Annesso 9: Facilitazioni
Annesso 10: Telecomunicazioni aeronautiche
Annesso 11: Servizi del traffico aereo
Annesso 12: Ricerca e soccorso
Annesso 13: Inchieste sugli incidenti aeronautici
Annesso 14: Aerodromi
Annesso 15: Servizio di informazioni aeronautiche
Annesso 16: Protezione ambientale
Annesso 17: Misure di sicurezza contro gli atti di interferenza illecita
Annesso 18: Misure di sicurezza per il trasporto aereo di merci pericolose
Annesso 19: Gestione della sicurezza (Safety Management).

All'interno di ciascun annesso sono presenti delle regole (*standard*) di applicazione obbligatoria, perché riconosciute necessarie per la sicurezza e il regolare svolgimento del trasporto aereo internazionale. Ad esse, si aggiungono le raccomandazioni (*recommended pratice*), ovvero procedure o istruzioni il cui adempimento è auspicato, al fine di uniformare il sistema di trasporto tra i diversi Stati ad un livello più elevato. ICAO ha elaborato anche altri documenti, denominati DOCS, il cui intento è quello di fornire una guida nell'applicazione

pratica degli annessi. Infatti, mentre quest'ultimi sono volutamente generici, i DOCS, che si possono considerare dei "decreti attuativi", forniscono riferimenti tecnici e indicazioni precise.

3.1.1 Gli annessi e la safety

Gli annessi costituiscono un insieme di regole generali per il trasporto e la navigazione aerea, e rappresentano la principale fonte tecnica in tutto il mondo. Tutti i documenti sono studiati per favorire lo sviluppo e il progresso dell'aviazione civile, ma alcuni ricoprono un ruolo di maggior importanza, per quanto concerne nello specifico la sicurezza.

L'Annesso 2 è il documento che stabilisce le regole del volo generali, ma anche specifiche per quanto riguarda il volo a vista e strumentale. Sono trattate la realizzazione dei piani di volo, le misure contro le collisioni e le procedure per l'intercettazione.

Gli Annessi 6 e 8 sono fondamentali per garantire la sicurezza dei velivoli. Il primo stabilisce norme per la strumentazione di bordo e raccomandazioni per l'impiego degli aerei. Il secondo definisce i requisiti operativi minimi che gli aeromobili devono possedere, per poter essere ammessi alla navigazione internazionale. Il certificato di navigabilità, relativo a tali specifiche, si applica tanto alla costruzione dei velivoli (struttura meccanica, design ed equipaggiamenti), quanto alla loro manutenzione.

L'Annesso 14 definisce le caratteristiche fisiche degli aeroporti, comprese le infrastrutture e gli equipaggiamenti di cui devono essere dotati. Sono contenute le specifiche delle piste di atterraggio e degli altri elementi del lato volo (piste di rullaggio, piazzali), ovvero geometrie, dimensioni e caratteristiche della pavimentazione. Sono presentate anche le restrizioni per la presenza di ostacoli, le indicazioni per l'utilizzo della segnaletica e dell'illuminazione. Vari servizi devono essere previsti in un aeroporto, in accordo con tale Annesso, tra cui l'istituzione di squadre di emergenza e antincendio, misure contro il rischio di impatto con la fauna (*bird strike*) o le strutture per la rimozione del ghiaccio dai velivoli (*de-icing*). Contestualmente all'Annesso 14, ICAO pubblicò il DOC 9774, "*Manual on certification of aerodromes*", con il quale venivano fornite le linee guida agli Stati aderenti, per l'istituzione di un sistema di regolamentazione relativo alla progettazione ed alla gestione degli aeroporti.

Infine abbiamo l'Annesso 19 e il relativo DOC 9859, "*Safety Management Manual*". Insieme rappresentano i documenti chiave per l'organizzazione della safety in aviazione. In essi sono

descritte le modalità per l'implementazione di un sistema di gestione della sicurezza e gli elementi che lo devono costituire.

3.1.2 L'annesso 17

L'annesso 17 è l'unico che tratta specificamente di security. Con questo documento vengono fornite disposizioni generiche per la protezione da atti di interferenza illecita, affinché ciascuno Stato provveda ad istituire l'autorità competente e a stabilire un programma per la salvaguardia della security nell'aviazione civile. Tali disposizioni fanno riferimento sia a minacce interne che esterne all'organizzazione aziendale. Le prime si contrastano tramite i controlli di qualità, le certificazione del personale e i background check. Le prevenzione da minacce esterne concentra l'attenzione su diverse misure:

- controllo degli accessi, sia dei passeggeri che dei loro bagagli o di altre merci;
- protezione del velivolo e dell'equipaggio di volo (ad esempio nessun oggetto deve rimanere a bordo dopo lo sbarco dei passeggeri e la cabina di pilotaggio deve essere protetta da accessi non autorizzati);
- procedure per categorie speciali di passeggeri, come detenuti e agenti delle forze dell'ordine di scorta;
- protezione da minacce informatiche.

Negli altri Annessi sono presenti ulteriori misure di security, più specifiche per gli argomenti trattati da ciascuno. Queste regole e raccomandazioni, riportate come riferimento anche in allegato all'Annesso 17, si devono integrare con le corrispondenti misure di safety, come ulteriore conferma di quanto le due parti siano in relazione tra loro.

Analogamente per gli altri Annessi, anche per la security è presente un manuale, il DOC 8973 "*Aviation Security Manual*", il cui accesso è però riservato, ovvero limitato esclusivamente alle figure di competenza.

3.1.3 L'annesso 13

L'Annesso 13 stabilisce le procedure per lo svolgimento delle inchieste di incidenti nel settore dell'aviazione civile. L'obiettivo di tale documento è il raggiungimento dell'uniformità nella

modalità di esecuzione di un'inchiesta e nella classificazione degli eventi incidentali, oltre a definire regole per stabilire a chi compete l'esecuzione dell'investigazione. Quest'ultime stabiliscono che sarà lo Stato in cui si è verificato l'evento ad avere la responsabilità di condurre le indagini e ad adempiere ai relativi obblighi:

- notifica alle parti interessate, come la Nazione dell'operatore, quella dov'è registrato il velivolo, quella dov'è stato prodotto e ovviamente l'ICAO;
- protezione delle prove, in particolar modo FDR e CVR, e custodia dell'aeromobile;
- collaborazione con gli altri Stati partecipanti;
- invio del rapporto, preliminare e finale, alle parti interessate.

Al fine di semplificare e migliorare l'esecuzione di tali attività, gli Stati aderenti demandano i compiti ad appositi enti investigativi. In Italia, l'autorità competente è l'ANSV (Agenzia Nazionale per la Sicurezza del Volo). Non essendo sottoposta alla vigilanza del Ministero delle infrastrutture e dei trasporti, l'ANSV è un'autorità pubblica con posizione di terzietà, condizione necessaria per garantire l'imparzialità nel suo operato.

3.2 La normativa europea

La normativa UE ha implementato, per così dire, il lavoro già portato avanti da ICAO. Il livello di sicurezza, nei Paesi dell'Europa, è sempre stato considerato tra i più elevati a livello mondiale. La creazione di una normativa aeronautica specifica ha reso il sistema di trasporto europeo standardizzato a livelli superiori, in via ufficiale. Il precursore di tale normativa fu JAA (*Joint Aviation Authorities*), un'associazione che sviluppava decisioni, ma che gli Stati membri attuavano su base volontaria. La svolta avvenne con il regolamento CE 1592/2002 e la fondazione di EASA, l'agenzia europea per la sicurezza aerea (*European Air Safety Agency*), la quale elabora Regolamenti e Certificazioni, che essendo poi emessi da Parlamento Europeo, sono di applicazione obbligatoria. EASA è di fatto un organismo indipendente, con poteri e personalità giuridica, il cui compito primario è garantire la sicurezza del trasporto aereo e la protezione ambientale. Il modello introdotto del Regolamento 1592/2002 ricalca molto quello già utilizzato negli USA, il cui ente competente è FAA (*Federal Aviation Administration*). L'istituzione di un'agenzia specifica per il settore, come EASA, getta le basi

per la realizzazione di un più elevato livello di sicurezza, al punto che anche Paesi extra europei (Qatar, Emirati Arabi e Cina) si avvalgono dei suoi standard e delle sue certificazioni. Il ruolo dell'agenzia comprende:

- fornire supporto tecnico al Parlamento Europeo, per l'armonizzazione di regolamentazioni e certificazioni;
- sviluppare un mercato unico dell'aviazione dell'UE;
- elaborazione di norme tecniche;
- certificazione di aeromobili e di componenti;
- approvare le organizzazioni per la progettazione, la fabbricazione e la manutenzione di prodotti aeronautici;
- effettuare controlli di sicurezza e fornire sostegno ai Paesi dell'UE;
- promozione delle norme di sicurezza.

3.2.1 Safety

Per quanto riguarda la safety, la normativa di riferimento è il Regolamento UE 1139/2018, la cui introduzione ha abrogato il precedente Regolamento CE 1592/2002, con il quale fu istituito l'EASA. Il Regolamento 1139/2018 individua delle norme comuni per quanto riguarda il trasporto aereo, con l'obiettivo di stabilire e mantenere un livello elevato ed uniforme di sicurezza. Il suo campo di applicazione è quindi molto ampio. Sono definiti i poteri e gli obblighi dell'Agenzia, ma disciplina anche tutte le fasi del sistema aeronautico, che comprende la progettazione, la produzione, la manutenzione e l'esercizio degli aeromobili e delle loro parti. Analogamente, per quanto riguarda la progettazione, la manutenzione e la gestione degli aeroporti le regole generali sono trattate nel Regolamento 1139/2018. Sicuramente importante è la novità introdotta da questo documento, ovvero per la prima si approfondisce la tematica degli aeromobili a pilotaggio remoto. Sono definiti requisiti per l'immatricolazione dei droni e la formazione dei loro operatori, in relazione alla tipologia di attività svolte e non alla massa dello stesso. Particolare attenzione viene rivolta al rischio di collisione ed alla questione del trattamento dei dati personali, che dovrà rispettare il Regolamento UE 679/2019.

Il 1139/2018 rappresenta il Regolamento basico, che disciplina il sistema nella sua interezza, ma, al di sotto di esso, sono definite delle norme più specifiche per ciascun settore. In particolare si possono individuare due macro aree di competenza: quella associata agli operatori aerei, quindi più incentrata sulle operazioni in volo, e quella per i gestori aeroportuali, relativa alle operazioni di terra.

Per quanto riguarda il primo settore, la normativa è rappresentata dal Regolamento UE 965/2012 e dalle relative AMC (*Acceptable Means of Compliance*) emesse da EASA, che rappresentano le norme applicative. Quest'ultime, pur non essendo obbligatorie, nella pratica lo diventano, essendo fondamentali per riuscire ad applicare il Regolamento. La certificazione di operatore aereo viene stabilita tramite l'accertamento dei punti norma, ovvero disposizioni dettagliate che disciplinano tutte le operazioni di volo. Tali operazioni comprendono l'esercizio di un aeromobile per il trasporto di passeggeri, di merci e di posta, così come le attività di ispezione a terra. Elementi che caratterizzano tale Regolamento sono l'effettiva implementazione del safety management system e l'adozione di una cultura della sicurezza, che coinvolga tutte le figure aziendali, a partire dall'*Accountable Manager*, che rappresenta il vertice della struttura organizzativa. L'elemento di traino per lo sviluppo della sicurezza è il *Safety Manager*, che opera in collaborazione con il *Compliance Monitoring Manager*, il quale valuta costantemente la conformità del sistema.

Per quanto riguarda la certificazione di aeroporti, valgono le regole viste sopra per gli operatori, ma il riferimento normativo è il Regolamento UE 139/2014. Esso rappresenta, di fatto, un miglioramento del DOC ICAO 9774, con il quale erano già state introdotte le procedure di certificazioni, alcune indicazioni per l'organizzazione del gestore aeroportuale e l'attività ispettiva. Tale documento portò all'istituzione di un ente giuridico, per la regolamentazione e il controllo della sicurezza aerea. In Italia tale ente è ENAC, tra i cui compiti sono compresi:

- attività ispettiva, sanzionatoria e di certificazione, autorizzazione, coordinamento e controllo;
- regolamentazione tecnica del settore aeronautico;
- emanazione del Piano Nazionale di Sicurezza;
- valutazione e approvazione dei piani di rischio aeroportuali.

Il Regolamento 139/2014 sostituì, migliorandolo, quanto operato in precedenza secondo le disposizioni ICAO. Oltre a scendere molto più in dettaglio, quindi lasciando poco spazio ad interpretazioni, il nuovo regolamento introdusse diverse novità. Di rilievo è che la responsabilità del funzionamento sicuro dell'aeroporto ricade sul gestore aeroportuale, il quale è chiamato a garantire dei servizi adeguati al livello di traffico. Similmente a quanto visto per gli operatori aerei, la certificazione di aeroporto è dimostrata dalla conformità ai punti norma, verificati tramite checklist, e l'organizzazione della safety è basata sulle tre figure cardine: *Accountable Manager*, *Safety Manager* e *Compliance Monitoring Manager*.

3.2.2 Security

Il Regolamento CE 300/2008 è la norma principale per la security nel settore del trasporto aereo. Con esso sono stabilite le norme fondamentali comuni per la tutela di persone e beni, dagli atti di interferenza illecita. Tale regolamento riprende i concetti stabiliti dall'Annesso 17 ICAO, fornendo dei criteri per una sua interpretazione comune. Il Regolamento è applicato sia agli aeroporti che agli operatori aerei. Le disposizioni fornite sono comunque generali e l'attuazione viene rimandata agli Stati membri. In particolare quest'ultimi devono redigere un programma nazionale per la sicurezza dell'aviazione civile, che garantisca l'adempienza alla norma, ed uno per il controllo della qualità, in modo tale da monitorare il rispetto delle disposizioni.

In supporto al Regolamento 300/2008, la Commissione Europea ha emanato il Regolamento di esecuzione UE 1998/2015, fornendo delle disposizioni particolareggiate per l'attuazione delle norme comuni. Sono quindi stabilite delle regole specifiche per l'organizzazione della security negli aeroporti e del vettore aereo, come:

- requisiti per le aree sterili in aeroporto, per i controlli degli accessi e per il rilascio del tesserino aeroportuale;
- procedure per lo screening delle persone (passeggeri e personale) e degli oggetti (bagagli a mano e da stiva, merci e posta);
- regole per la sorveglianza e il pattugliamento;
- regole per le ispezioni di sicurezza dell'aeromobile;

- principi per la selezione e la formazione del personale;
- procedure per la protezione di merce messa in sicurezza e per il trasporto di merce ad alto rischio.

Tutte queste misure, devono inoltre integrarsi con quelle previste dai Regolamenti UE 139/2014 e 965/2012. Infatti anche quest'ultimi, in modo analogo a quanto visto per gli annessi ICAO, prevedono, al loro interno, alcune disposizioni di security per le operazioni negli aeroporti e in volo.

I requisiti e i principi individuati dalla normativa europea sono ricalcati anche dal DOC 30 ECAC. L'ECAC (*European Civil Aviation Conference*) è un organismo intergovernativo, il cui scopo è la promozione di un sistema di trasporto aereo sicuro, efficiente e sostenibile a livello europeo, attraverso l'armonizzazione delle politiche dell'aviazione civile degli Stati membri. A differenza di EASA, che è un organismo dell'Unione Europea, ECAC è frutto di un accordo internazionale (in questo senso simile a ICAO) e per questo comprende un maggior numero di Nazioni. Il DOC 30 costituisce un forte riferimento, al punto da essere stato anche recepito dall'Unione Europea e reso effettivo, pur non avendo, originariamente, natura obbligatoria. Esso contiene raccomandazioni e requisiti specifici sulle misure di security, sia per quanto riguarda passeggeri e aeromobili, che il personale. Questo documento, che attualmente è alla sua dodicesima revisione, ha introdotto alcuni concetti che ad oggi giocano un ruolo chiave sulla sicurezza dell'aviazione civile. Il più rilevante è sicuramente quello del "*One stop security*", che presuppone una uniformità dagli standard di sicurezza per tutti gli Stati. In base a questo principio ogni Paese può riconoscere ed accettare i controlli di sicurezza effettuati sui voli provenienti da altri Paesi membri, senza dover ripetere i controlli per i passeggeri che transitano sullo scalo. In questo modo, si mantiene un elevata efficienza del servizio, senza trascurare la sicurezza.

In Italia l'autorità designata per il coordinamento e il monitoraggio dell'attuazione delle norme comuni di sicurezza aerea è l'ENAC. Tra i suoi compiti ricade anche la redazione, l'attuazione e l'aggiornamento del Programma Nazionale per la Sicurezza e del Programma Nazionale per il controllo di Qualità della sicurezza dell'aviazione civile, così come previsto dal Regolamento 300/2008. Questi documenti descrivono disposizioni e procedure specifiche, per prevenire atti interferenza illecita o tentativi di introduzione di articoli proibiti nelle aree

potenzialmente a rischio. Al fine di controllare l'applicazione delle norme comuni dell'Unione Europea, ENAC effettua ispezioni, con e senza preavviso.

Sulla base del Programma Nazionale, saranno poi gli operatori aeroportuali e i vettori aerei a redigere un proprio programma per la sicurezza, con cui descrivere i metodi e le procedure da mettere in atto. Questi programmi vengono sottoposti all'approvazione dell'ENAC, che ne autorizza l'esecuzione e provvede alla certificazione del personale.

3.3 Gli enti italiani

Lo normativa italiana, per quanto concerne l'aviazione civile, è sostanzialmente costituita dal recepimento delle direttive europee e dall'attuazione degli impegni derivanti dagli accordi internazionali (Convenzione di Chicago). L'adempimento di tali obblighi ha portato all'istituzione di diverse autorità, che svolgono ruoli primari per la sicurezza aerea.

3.3.1 ENAC

Come abbiamo già visto nei paragrafi precedenti, in Italia ENAC, l'Ente Nazionale per l'Aviazione Civile, è l'autorità competente per la sicurezza del volo, sia essa intesa come safety che come security. Gli obiettivi che guidano ENAC mettono al centro dell'attenzione il passeggero e i suoi bisogni. Per questo la sue azioni sono indirizzate a garantire la sicurezza, la qualità dei servizi, la tutela dei diritti e l'equa competitività. L'ente, istituito con il D.Lgs. 250/1997, copre un ruolo chiave per l'attuazione delle normative internazionali ed europee, essendo l'autorità unica con compiti di:

- regolazione tecnica;
- certificazione;
- vigilanza;
- controllo.

Anche ENAC quindi disciplina la sicurezza del volo, emettendo una propria normativa. Questa normativa è in primo luogo composta da regolamenti e circolari. Nei primi sono contenuti requisiti tecnici e operativi, che riflettono quelli contenuti sia negli Annessi ICAO

che nelle Direttive dell'Unione Europea. Le circolari sono invece dei documenti integrativi, per migliorare la comprensione delle regole e favorirne l'applicazione. Le circolari si riferiscono ad argomenti specifici, fornendo un complesso di requisiti, derivanti dalla trattazione armonizzata delle norme applicabili. Per questo motivo, le circolari rappresentano un riferimento importante, per tutti i soggetti che operano nel settore aeronautico. Le circolari sono organizzate in nove serie, a seconda dell'ambito trattato. Si riportano alcune delle serie più rilevanti:

- Navigabilità (NAV), riguardanti la costruzione, la manutenzione e l'impiego dei velivoli.
- Operazioni Volo (OPV), inerenti a svolgimento delle operazioni di volo, procedure per le licenze, abilitazioni e attestazioni.
- Aeroporti (APT), relative alla sicurezza e l'operatività aeroportuale.
- Security (SEC), l'unica specifica per tale settore.

Tra gli altri compiti si ricordano la redazione del Programma Nazionale per la Sicurezza dell'aviazione civile, già discusso in precedenza, e l'attuazione delle raccomandazioni emesse dall'ANSV. In accordo con i requisiti dell'Annesso 13 di ICAO e del Regolamento CE 376/2014, ENAC provvede alla raccolta delle segnalazioni obbligatorie delle occorrenze e ne elabora una banca dati, per facilitare l'analisi delle informazioni.

3.3.2 ANSV

L'Agenzia Nazionale per la Sicurezza del Volo è l'autorità investigativa dello Stato italiano. Istituita nel 1999, con il recepimento della Direttiva CE 56/94, fu posta in posizione di terzietà rispetto al sistema dell'aviazione civile. Essa è infatti sottoposta alla vigilanza esclusivamente della Presidenza del Consiglio dei Ministri, a differenza di tutte le altre istituzioni aeronautiche, che sono dipendenti del Ministero delle infrastrutture e dei trasporti. Il ruolo primario dell'agenzia è lo svolgimento delle indagini di sicurezza, relative ad incidenti ed occorrenze avvenute nell'aviazione civile. Inoltre, qualora fosse necessario, collabora con gli enti investigativi di altre Nazioni, impegnate nelle indagini. Le inchieste incidentali vengono effettuate in adempienza agli obblighi previsti dall'Annesso 13 ICAO e ribaditi anche dal Regolamento UE 996/2010. Come affiancamento all'attività investigativa,

l'agenzia si impegna a compiere studi e indagini, per garantire miglioramenti nella sicurezza del volo.

Si aggiunge infine, alle altre funzioni dell'ANSV, la gestione di un sistema di segnalazione volontaria (*voluntary report*), ai sensi del Regolamento CE 376/2014. Tale sistema, diverso da quello di ENAC, raccoglie segnalazioni relative qualsiasi evento, verificatosi nel settore dell'aviazione civile, che è ritenuto pericoloso, anche solo potenzialmente.

3.3.3 ENAV

L'Ente Nazionale per l'Assistenza al Volo, è la società italiana che fornisce il servizio di controllo del traffico aereo (ATC), ai voli che operano nello spazio aereo di competenza nazionale. L'ente, che dal 2001 è diventato società per azioni, è sottoposta a controllo pubblico, nello specifico è subordinato al Ministero dell'economia e delle finanze ed è soggetto alla sorveglianza dell'ENAC. La società opera in esclusiva, svolgendo le attività che un tempo erano di competenza dell'Aeronautica Militare. ENAV controlla il traffico aereo, fornendo assistenza alla navigazione e informazioni aeronautiche, quali NOTAM e informazioni meteorologiche. Ne consegue che il corretto funzionamento di tali servizi è di fondamentale importanza per la sicurezza delle operazioni in volo.

Capitolo 4

L’analisi retrospettiva

4.1 Il safety report

Ai fini della sicurezza, un approccio sicuramente efficace per svolgere una valutazione dei rischi e migliorare l’implementazione del sistema di gestione, è quello dell’analisi retrospettiva. Essa indaga gli incidenti che si verificano durante le operazioni e, indagando sui motivi che portano all’evento, sviluppa delle correzioni tali da impedire il ripetersi dell’episodio. L’investigazione delle cause non si deve fermare a quelle dirette, ovvero strettamente correlate agli operatori sul campo, ma deve indagare anche quelle condizioni latenti, che sono presenti all’interno dell’organizzazione aziendale. L’indagine, per poter essere un efficace strumento di sicurezza, deve essere svolta per tutti quegli eventi che hanno portato ad una riduzione della sicurezza, con o senza conseguenze. Scorrendo la normativa ICAO, in particolare l’Annesso 13, possiamo andare ad individuare tre diversi gradi di incidenti:

- *incident*, ovvero un inconveniente (comunemente noto come *near miss*), durante lo svolgimento delle operazioni di un aereo, che ha messo o che potrebbe aver messo a repentaglio la sicurezza delle operazioni stesse;

- *serious incident*, un inconveniente le cui circostanze indicano che c’era un’elevata probabilità di incidente;

- *accident*, è l’incidente vero e proprio, quello dove si hanno come conseguenze danni (gravi o mortali) a persone, siano esse a bordo o meno, danni o cedimenti strutturali dell’aeromobile, oppure lo stesso sia disperso o inaccessibile.

Solitamente all’interno di un’organizzazione gli incidenti sono una minima parte, la cosiddetta “punta dell’iceberg”. Per ogni *accident* infatti, si possono individuare rispettivamente 300 *incident* non gravi e 30 *serious incident*. Si possono individuare un gran numero di situazioni pericolose, che avrebbero potuto avere conseguenze, anche gravi, ma che

sono state bloccate da altre barriere di sicurezza. Solitamente si è portati a colpevolizzare gli operatori, rei delle azioni che hanno portato all'incidente finale. Ma questo non è sicuramente l'approccio corretto, proprio in virtù del fatto che gli eventi con conseguenze sono rari e sono il risultato di un insieme di situazioni critiche, che devono verificarsi contemporaneamente. Concentrarsi, piuttosto, sui near miss è una procedura decisamente più efficace. All'interno dell'organizzazione aziendale, si possono presentare un gran numero di condizioni latenti, che, singolarmente, non hanno effetti negativi immediati e per questo motivo sono difficili da individuare. Il più delle volte, rimangono nascoste fino al verificarsi di un incidente.

L'analisi dei near miss è un ottimo strumento per l'individuazione e la correzione degli errori latenti. Premessa, per riuscire a svolgere in modo accurato e completo tale analisi, è che l'ambiente lavorativo debba basarsi sui principi di equità e giustizia (*just culture*). Ciascuna persona deve poter segnalare qualsiasi occorrenza o errore, senza timore di ripercussioni. Questo approccio deve coinvolgere il personale, facendolo diventare consapevole del proprio ruolo nei confronti della sicurezza. Diffondendo la giusta atmosfera di fiducia all'interno dell'azienda, si incoraggia le persone ad un comportamento responsabile, ma prevedendo comunque un sistema sanzionatorio, per tutti quegli atti di palese negligenza. Questo tipo di cultura viene ancor più incentivata dall'obbligo di segnalazione delle occorrenze, ai sensi del Regolamento EU 376/2014. Tale regolamento, infatti, prescrive alle organizzazioni il report obbligatorio di tuti gli eventi, che hanno rappresentato un rischio per la sicurezza. La raccolta dati e lo scambio delle informazioni permettono, così, il miglioramento complessivo di tutto il sistema di trasporto.

4.2 Il fattore umano

L'essere umano è portato per sua natura a sbagliare. Pur potendo migliorare le proprie prestazioni, l'errore è un effetto inevitabile, derivante dalle limitate capacità umane, e che deve essere tenuto in considerazione nelle analisi di sicurezza. Addestramento ed esperienza son ottimi strumenti per ridurre al minimo gli errori, ma non potranno mai eliminarli del tutto. Per questo si deve attuare una politica della sicurezza, che accetti l'errore e che adotti misure che ne annullino, o quanto meno ne limitino, gli effetti. Si devono introdurre barriere supplementari, costituendo un sistema "a strati", in modo tale che il fallimento di una delle misure previste non provochi automaticamente un incidente. Procedure, checklist e sistemi

automatizzati sono tutte barriere atte a prevenire gli effetti dell'errore umano. Ma per poter applicare in modo ottimale tali misure, è necessario analizzare il comportamento umano in relazione con esse. Esistono diversi modelli, sviluppati per lo studio del fattore umano, che possono impiegati a tale scopo.

4.2.1 Il modello SHELL

Uno dei modelli più utilizzati, per lo studio del fattore umano, è quello indicato da ICAO, ovvero il modello SHELL. Il nome deriva dalle componenti che il modello prende in analisi, in particolar modo si focalizza sulle loro interazioni. La rappresentazione a blocchi (figura 4.1) definisce la struttura del modello, ovvero dove l'elemento centrale si interfaccia contemporaneamente con gli altri quattro. La connessione tra i blocchi rappresenta uno scambio di energia e informazioni e, nel caso venisse a mancare, può portare al verificarsi di un incidente. La rappresentazione frastagliata dei contorni non è casuale, ma sta ad indicare proprio la delicatezza delle interfacce, che si devono incastrare per evitare che il sistema si scomponga. Gli elementi che costituiscono il modello sono: liveware (L), hardware (H), software (S) e environment (E).

Figura 4.1. *Schema grafico del modello SHELL*

Il blocco liveware rappresenta la componente umana del sistema. È l'elemento centrale e copre un ruolo fondamentale per il funzionamento dell'organizzazione. Il fattore umano è

caratterizzato da due aspetti contrapposti. È la parte più dinamica e adattabile, che è in grado di trovare soluzioni fuori dagli schemi, a situazioni non previste. Allo stesso tempo, però, è anche quella più vulnerabile e critica del sistema, in quanto è soggetto ad errore e la sua capacità di adattamento porta a mascherare le lacune presenti nel sistema. Queste carenze, anziché essere corrette, permangono creando potenziali condizioni di pericoli.

Con il termine liveware si fa riferimento ai diversi elementi che influenzano la natura umana:

- dimensione fisica, principalmente legate agli aspetti sensoriali;
- fattori fisiologici, ovvero fatica, salute e stress;
- fattori psicologici, tra cui sono compresi l'attenzione e i processi cognitivi, l'esperienza e le attitudini comportamentali;
- contesto sociale.

Per il funzionamento di un'organizzazione fatta di persone, la componente umana deve interfacciarsi con sé stessa. La connessione liveware-liveware si identifica perciò con l'insieme di fattori che compongo i rapporti tra le persone: l'interazione tra personalità, la comunicazione, il lavoro di squadra e la leadership.

Hardware comprende tutto ciò che è relativo alle macchine ed alla strumentazione. L'interfaccia uomo-macchina tiene in considerazione dell'ergonomia delle attrezzature, di come le informazioni vengano visualizzate e di come la strumentazione sia logica e intuitiva da utilizzare.

Con software invece si fa riferimento a tutti i sistemi non fisici: procedure, regolamenti, checklist, manuali, simbologia, programmi informatici, ecc. Come per la precedente, anche l'interfaccia liveware-software analizza la semplicità di comprensione e applicazione di tali elementi.

Infine environment, ovvero l'ambiente, inteso prevalentemente come i fattori fisici, ovvero temperatura, luce, rumore, vibrazioni e qualità dell'aria. Ma va anche a tener conto del contesto in senso più ampio, come condizioni organizzative, politiche ed economiche.

4.3 Il modello di Reason

Lo studio del fattore umano di Reason (1990) è ben noto nel settore dell'aviazione. Il modello proposto permette di identificare i fattori causali di una qualsiasi occorrenza. Lo schema, chiamato "*Swiss Cheese*", proprio per la sua struttura, mette in evidenza come ogni incidente sia il risultato di una combinazione di più fattori, derivanti dai fallimenti delle barriere poste come misure di sicurezza. Simbolicamente le vulnerabilità del sistema sono rappresentate dai buchi nelle fette di formaggio, che indicano le barriere. Quando i buchi si allineano e nessuna barriera riesce a fornire protezione dal pericolo, la successione degli eventi porta inevitabilmente all'incidente.

4.3.1 Il modello "Fallible Machine"

Lo studio compiuto da Reason parte dall'analisi del comportamento e dell'errore umano. L'uomo è visto come una macchina imperfetta, soggetta ad errori e per questo "fallibile". Per comprendere meglio come avvengano questi fallimenti, è necessario prima conoscere i processi con cui l'essere umano acquisisce le abilità, necessarie all'esecuzione delle mansioni lavorative. I processi di apprendimento avvengono attraverso livelli di astrazione sempre più complessi, fino al raggiungimento del valore massimo, corrispondente alle funzioni di un processo o sistema. Sulla base di questo principio, si possono identificare tre livelli di abilità (*Skill, Rule* e *Knowledge base*), a seconda del grado di conoscenza richiesta, definendo il modello SRK.

- *Skill-based behaviour*, conosciuto anche come senso motorio, una volta acquisito, richiede poco o nessun controllo cognitivo, diventando istintivo ed automatizzato.

- *Rule-based behaviour*, ovvero l'uso di regole e procedure per scegliere l'azione, in risposta ad una situazione conosciuta. Per l'applicazione di tali regole non è richiesta la conoscenza dei principi di funzionamento del sistema, ma le stesse possono essere apprese con l'esperienza o fornite tramite addestramento.

- *Knowledge-based behaviour*, è il livello più avanzato, dove è necessario sapere ed applicare i principi del sistema, per risolvere situazioni nuove e inaspettate. Il carico cognitivo richiesto è molto maggiore, dovendo analizzare la situazione e, in relazione

ad essa e agli obiettivi da raggiungere, pianificare la strategia e le operazioni da mettere in atto.

Sulla base di questa teoria è possibile individuare come il fattore umano condizioni il corretto funzionamento del sistema. La fallibilità è una caratteristica intrinseca della natura umana, ma è variabile e difficilmente esprimibile come formulazione numerica. Gli errori accadono a diversi livelli dell'organizzazione e possono avere correlazioni tra loro, anche quando il momento e il luogo in cui sono stati commessi è diverso. Si può fare una distinzione tra errori attivi ed errori latenti. I primi sono quelli commessi nel compiere una determinata attività, che richiede un'azione manuale. Questo tipo di errore viene commesso dall'operatore sul campo, che svolge le mansioni pratiche, come piloti e manutentori, ed è connesso prevalentemente ad azioni di tipo *skill-based*. Gli errori latenti sono invece quelli che avvengono nei processi decisionali e che spesso rimangono nascosti nel sistema, fino al verificarsi di un evento scatenante. Questi errori avvengono durante le fasi di pianificazione, anche se poi l'azione finale viene compiuta da un operatore, e rientrano nelle categorie dei comportamenti *rule-based* e *knowledge-based*.

Ma gli errori si possono ulteriormente classificare in tipologie più semplici.

- *Slips*, commessi solitamente nelle attività di routine, sono la conseguenza di inattenzione, distrazione o sovraccarico.

- *Lapses*, ovvero errori da lapsus di memoria, per cui un'azione viene dimenticata e non eseguita.

- *Mistakes*, sono relativi ad errori *rule-based* e *knowledge-based*. I primi comprendono errori per errata interpretazione delle regole o della situazione, e conseguente applicazione di procedure errate. I secondi, più complessi, sono dovuti a carenza di informazioni, mancanza di conoscenza o reazioni non razionali per situazioni di stress.

- *Violations*, con cui si fa riferimento a tutta quella serie di azioni compiute, nonostante siano espressamente vietate. Le violazioni possono essere volontarie o involontarie, e se ne possono indicare vari tipi, a seconda delle cause. Le violazioni più frequenti corrispondono a scorciatoie usate per semplificare o accelerare il lavoro, o messe in atto per guadagno personale, come la presenza di incentivi economici per la

produzione. Altre violazioni sono conseguenza di discrepanza tra regole e procedure o si verificano in situazioni eccezionali.

4.3.2 Il modello "Swiss Cheese"

Queste considerazioni viste per l'errore umano, possono essere applicate al contesto organizzativo di un'azienda, per indagare i fattori causali di un evento incidentale. In particolare si possono studiare ambienti complessi, per individuare le interazioni e le dipendenze multiple ai vari livelli dell'organizzazione. Il concetto base del modello di Reason è la suddivisione del sistema in strati, per gradi di profondità nel processo organizzativo, fino a scendere alle operazioni in prima linea. Per illustrare tale concetto, viene utilizzata la metafora delle fette di formaggio svizzero e da questo deriva il nome "*Swiss Cheese Model*". Ogni azienda o insieme è struttura con diversi strati, che corrispondono ai vari livelli della gestione. Le fette rappresentano le barriere adottate all'interno dell'organizzazione, relative a ciascun livello. I buchi invece indicano le debolezze e i fallimenti delle difese, ovvero errori, guasti e vulnerabilità del sistema. Il verificarsi di queste mancanze (i buchi nel formaggio), non comporta automaticamente il verificarsi di un'occorrenza, in quanto, solitamente, la successione degli eventi incontra la barriera successiva, interrompendosi. Quando però gli errori, latenti e attivi, si concatenano allineandosi, il pericolo riesce a superare tutte le barriere, portando ad un incidente.

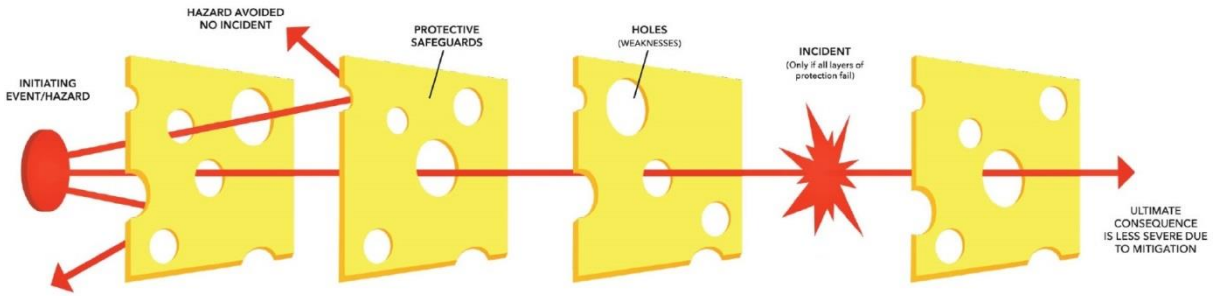

Figura 4.2. *Rappresentazione grafica del comportamento degli incidenti in un modello organizzativo multistrato (Swiss Cheese)*

Spesso, nell'analisi di un incidente, risulta difficile individuare le cause remote, che possono averlo originato. Solitamente, nel determinare i fattori scatenanti e nell'applicare le relative misure correttive, ci si focalizza sugli errori attivi, trascurando le carenze del sistema organizzativo. Questo approccio apparentemente logico, a lungo termine si rivela inefficace.

Infatti la costante presenza di errori nel management, inevitabilmente porta al ripetersi delle stesse situazioni di pericolo. Gli errori attivi, infatti, possono essere ridotti con l'addestramento e la formazione, ma sono ineliminabili e il loro verificarsi può facilmente dare luogo ad un occorrenza. Migliorando le difese presenti nella fase organizzativa, si interromperà la sequenza degli eventi alla sua origine. Questo concetto è ancor più chiaro se si osserva il modello "Swiss Cheese", in figura 4.3. Le varie fette, rappresentano le barriere poste ai diversi livelli del sistema. Gli errori sono quindi suddivisi in categorie a seconda che siano latenti o attivi. Nel dettaglio sono rappresentate cinque fette, ciascuna corrispondente ad un livello aziendale:

- Decision makers;
- Line management;
- Preconditions;
- Unsafe acts;
- Defences.

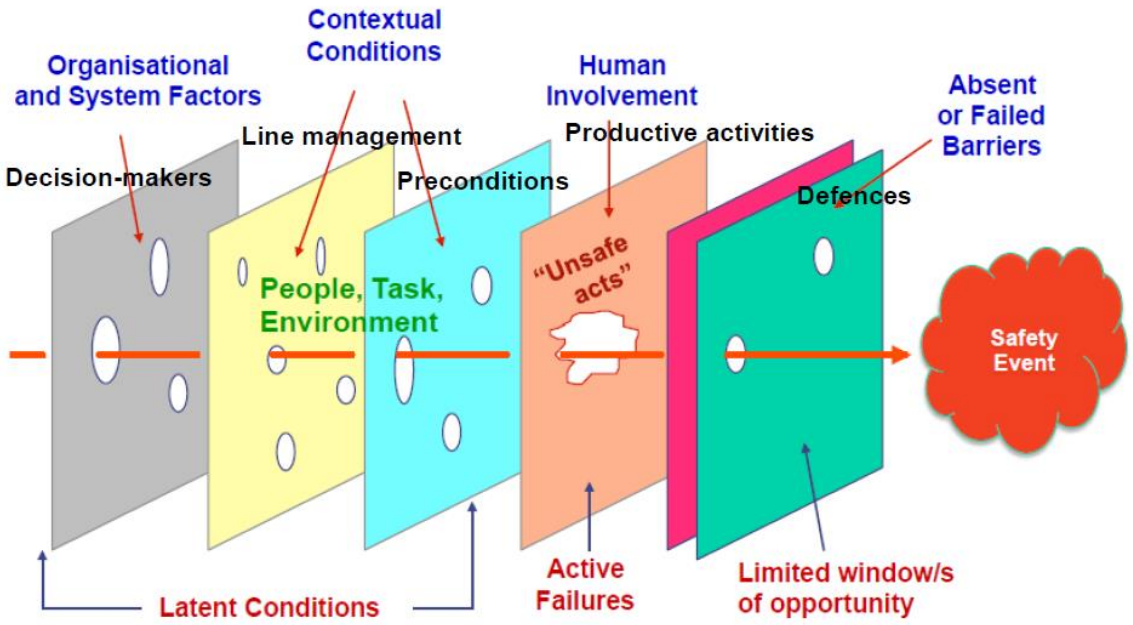

Figura 4.3. *Modello Swiss Cheese individuato dalla teoria di Reason*

4.3.2.1 Decision makers

In prima linea sono presenti i fattori organizzativi, correlati con l'alta dirigenza ed i portatori di interessi. Sono considerate in questo livello la politica aziendale e gli obiettivi, che definiscono la direzione e il modo con cui l'azienda opera. Si parla, quindi, di quelle che possono essere definite le condizioni latenti più estreme, in quanto hanno maggior impatto e possono condizionare tutte le successive. L'assenza di propensione alla sicurezza già ai vertici del sistema, automaticamente influenzerà in modo negativo anche tutti gli altri livelli sottostanti. Ad esempio, politiche che incentivano la produttività a discapito della sicurezza, porteranno inevitabilmente ad un aumento, sia in frequenza che in gravità, degli incidenti. Ne consegue che i vertici manageriali devono essere i primi a incoraggiare una cultura della sicurezza all'interno dell'azienda e promuoverla con decisioni in linea con essa. Dando l'esempio, è possibile coinvolgere tutti gli elementi dell'azienda e far sì che si impegnino a migliorarla. A livello dei decision makers, una tipica mancanza, che può manifestarsi, è l'errata convinzione nelle prestazioni aziendali e nel raggiungimento dei risultati. Spesso tali certezze sono derivate da feedback incompleti o da una cattiva raccolta delle informazioni, che distolgono l'attenzione dalle reali criticità del sistema.

In un sistema diffuso come quello del settore aereo, è necessario ampliare il campo di riferimento. Perciò, vanno considerati in questo livello anche fattori esterni a quelli delle singole aziende, come l'aspetto normativo, in particolar modo quello internazionale. Una legislazione specifica per il settore (si veda il caso europeo) fa la differenza, in termini di risultati, per tutto il settore aereo nel suo insieme. Banalmente le azioni di un'azienda non virtuosa possono avere ripercussioni anche sulla sicurezza di altre aziende, che invece lo sono. L'unico modo per ridurre tale rischio è una normativa che assicuri uno standard uniforme, tra i diversi soggetti attivi nel settore, e che interdica l'attività a chi non è in grado, per volontà o per mezzi, di garantire tale livello.

4.3.2.2 Line management

Il secondo livello è rappresentato dalla linea manageriale, che collega i vertici agli operatori sul campo. Infatti i compiti e le responsabilità vengono solitamente delegati dall'alta dirigenza ad amministratori minori, che, pur rispettando le politiche aziendali, prendono decisioni che incidono direttamente sui lavoratori. A livello dirigenziale, gli errori sono spesso dovuti a mancanza di competenza o conoscenza, che porta a decisioni sbagliate, influenzando le condizioni lavorative. Ciò può portare a procedure non definite o definite non

correttamente, attrezzature ed equipaggiamento non adeguato, mansioni e compiti affidati a personale non preparato. Nella delega delle responsabilità è quindi fondamentale individuare delle figure capaci e formate per svolgere tale ruolo.

Altre carenze di questo livello, possono essere annoverate come conseguenze del livello superiore, ad esempio risorse fornite non adeguate o mancato trasferimento di valori e cultura aziendale. Quest'ultimo caso, in mancanza dell'adeguata attività di sorveglianza, potrebbe portare a decisioni anche contrastanti con la politica aziendale o addirittura guidate da interessi personali dei dirigenti.

4.3.2.3 Preconditions

Le precondizioni rappresentano l'ultimo stadio degli errori latenti. Esse comprendono tutte quelle caratteristiche dell'ambiente lavorativo che favoriscono comportamenti non sicuri degli operatori. Può essere esempio la presenza di pericoli, come macchine e attrezzature non sicure, o l'assegnazione di mansioni pericolose, che richiedono uno specifico addestramento. Ma le precondizioni si possono verificare anche nell'ambiente comportamentale, come situazioni in cui gli operatori sono disincentivati dal segnalare errori e violazioni, per timore di ripercussioni, sia con i colleghi che con i superiori. Nei confronti di quest'ultimi va inteso sia come timore di incorrere in sanzioni personali, ma anche come ripercussioni sul gruppo, e quindi la volontà di proteggere i colleghi. A cascata, questo livello è fortemente influenzato dalle decisioni manageriali, che devono essere tali da rendere e mantenere sicure le condizioni relative allo svolgimento delle singole operazioni.

4.3.2.4 Unsafe acts

I comportamenti non sicuri rappresentano l'ultimo fattore decisivo per il verificarsi delle occorrenze. Rappresentano gli errori attivi, ovvero quelli compiuti dagli operatori sul campo, durante lo svolgimento delle operazioni. Questi comportamenti comprendono tutte le categorie di errori e valutazioni errate, la violazione, intenzionale o meno, delle procedure, e l'uso scorretto dell'attrezzatura. Il verificarsi di questi errori è determinato da precondizioni interne all'azienda, ma può anche essere soggetto ad influenze esterne. Si pensi ad esempio a problemi legati alla sfera personale del singolo operatore, che possono essere fonte di distrazione e condizionare in modo rilevante lo svolgimento delle mansioni. Gli errori attivi possono essere ridotti con l'addestramento, la formazione e le procedure, ma, proprio per l'elevata incidenza del fattore umano, non saranno mai completamente eliminabili.

4.3.2.5 Defences

L'accadimento di un occorrenza raramente coincide con il verificarsi di un danno. Il più delle volte, la presenza di ulteriori barriere consente di interrompere la catena incidentale, riducendo l'evento ad un inconveniente. Tali difese possono essere appositamente previste per specifiche situazioni, ma possono anche essere dovute a fattori fortuiti o fortunati. Ad esempio l'esperienza e l'abilità di un operatore possono rimediare una situazione pericolosa, mentre, in circostanze analoghe, una persona inesperta potrebbe reagire diversamente e perdere il controllo della situazione. O le condizioni ambientali, a seconda che siano buone o avverse, possono incidere sulle conseguenze di un'occorrenza. Difese specifiche comprendono invece misure di emergenza, come piani di evacuazione, impianti antincendio, sistemi automatici di intervento.

Anche quest'ultime barriere possono però risultare inefficaci o assenti. In tal caso la sequenza incidentale, che aveva superato tutti i precedenti livelli, non verrà interrotta e le conseguenze non saranno contenute, o lo saranno solo parzialmente.

4.4 L'inchiesta incidentale

In un settore come quello aereo, in cui il livello di sicurezza è molto elevato, il verificarsi di incidenti è spesso correlato al presentarsi di situazioni impreviste e diverse da quelle di eventi precedenti. Difficilmente lo stesso incidente si ripeterà più volte. Infatti al verificarsi di un evento, che mette in luce le carenze del sistema, segue immediatamente l'attuazione di misure correttive per tali mancanze. Come visto precedentemente, tale obiettivo è facilmente raggiunto grazie ai programmi di segnalazione e di analisi delle occorrenze. Questo concetto viene ulteriormente sviluppato con l'inchiesta incidentale. Ai sensi dell'Annesso 13 ICAO infatti, è fatto obbligo agli Stati aderenti di svolgere delle indagini, che vadano ad accertare le cause di un evento, e redigerne un rapporto. Tale relazione deve essere costituita da una struttura ben definita, che comprende: informazioni sui fatti, analisi, conclusioni e raccomandazioni di sicurezza. Quest'ultime, risultanti dall'analisi dell'occorrenza, risultano un punto chiave. Le raccomandazioni, infatti, sono indirizzate alle autorità e ai soggetti che operano nel settore dell'aviazione civile, e hanno lo scopo di apportare un miglioramento alla sicurezza di tutto il sistema e non solo ai soggetti coinvolti. La loro attuazione non è

obbligatoria, ma un eventuale rifiuto, da parte dello Stato che ha ricevuto la raccomandazione, deve essere motivato.

Per quanto riguarda lo sviluppo dell'inchiesta, si può identificare una procedura da seguire per lo svolgimento di un'analisi dell'incidente. Una volta attivata la commissione di investigazione, con definizione di ruoli e responsabilità, questa procede seguendo le fasi successivamente elencate.

- Raccolta dei dati e delle informazioni; ricostruzione logico-temporale dell'incidente.
- Scelta dei modelli e dei metodi con cui svolgere le analisi.
- Analisi dei dati e definizione delle cause.
- Valutazione dell'efficacia delle barriere e sviluppo delle raccomandazioni, per correggere le criticità evidenziate.
- Reporting e archiviazione dei dati.

Ogni fase risulta importante, ai fini dell'efficacia dell'indagine stessa e per favorire il miglioramento del sistema. In particolare, l'ultimo punto contribuisce all'elaborazione di banche dati, con le quali, non solo è possibile avere un quadro sull'andamento dell'intero settore e delle sue criticità, ma permette anche di sviluppare valutazioni di sicurezza sempre più accurate, grazie alla presenza di un crescente numero di informazioni storiche. Ovviamente a conclusione dell'inchiesta e dell'emanazione delle raccomandazioni, le modifiche proposte devono essere attuate, monitorate e successivamente riesaminate, per garantire l'effettiva efficacia.

Ai fini dell'indagine, senza comunque togliere valore alle altre fasi, la scelta del modello impiegato rappresenta sicuramente un passaggio delicato. I modelli disponibili con cui poter svolgere l'analisi di un incidente sono diversi e vari. Ciascun modello si focalizza su alcuni aspetti, piuttosto che su altri. Si può scegliere di approfondire il fattore umano, valutare l'efficacia delle barriere previste o indagare gli errori latenti. Per questo è bene selezionare accuratamente il modello, che più si adatta al sistema che si sta andando a studiare. Solitamente nello svolgimento di un'analisi retrospettiva, in un settore strutturato come quello aeronautico, è buona prassi utilizzare più modelli combinati, per avere la certezza della qualità e della completezza dell'indagine. Analizzare singolarmente le diverse metodologie

richiederebbe una trattazione eccessivamente ampia e non verranno perciò esposti, ma solamente accennati. In particolare, ai fini di questa tesi, risulta interessante individuare quei modelli utilizzabili per effettuare lo studio delle cause, sia per la safety che per la security. Come vedremo nel capitolo successivo, è possibile indagare contemporaneamente le cause di entrambi gli ambiti e valutare come si correlino, nello sviluppo di un evento incidentale.

Capitolo 5

Le interazioni tra safety e security

5.1 Correlazioni

Safety e security, per quanto possano sembrare occuparsi di settori lontani, sono in stretta correlazione tra loro, condizionandosi reciprocamente. Con correlazione si fa riferimento alla possibilità che uno dei due ambiti modifichi le condizioni dell'altro. L'influenza, che ciascuno può avere sull'altro, in determinate condizioni può anche avere effetti di miglioramento sul sistema, ma è più frequente che l'impatto abbia conseguenze negative, inficiando il livello di sicurezza di uno, dell'altro o di entrambi i settori.

5.1.1 Interferenze negative

Il caso in cui safety e security si influenzino negativamente, risulta essere una questione critica, sia per la maggior frequenza con cui si verificano situazioni che per le conseguenze, anche gravi, che ne vengono generate. Infatti, proprio a causa della netta differenza della tipologia di pericoli, da cui safety e security si tutelano, i principi di approccio ai due sistemi risultano spesso contradditori. Entrambi però prevedono l'applicazione di procedure e misure rigorose, la cui violazione o assenza causa una riduzione della sicurezza. Ciò provoca notevoli difficoltà di gestione generale, non essendo rari i casi in cui le misure adottate siano tra loro contrastanti e abbiano effetti opposti l'una sull'altra. Si possono addirittura verificare situazioni di paradosso, in cui un accorgimento di security può creare pericolo per la safety, e viceversa. Ci si ritrova quindi, il più delle volte, obbligati ad adottare soluzioni di compromesso, nel tentativo di soddisfare entrambe le richieste, senza però raggiungere la piena conformità per nessuno dei due casi. Gli esempi di queste situazioni sono diversi.

- La necessità di rinforzare la chiusura delle porte del cockpit, indispensabile per ragioni di security e diventata misura obbligatoria dopo l'11 settembre 2001, ha implicazioni non trascurabili sulla safety.

- L'evacuazione in occasione di un allarme antincendio (reale ma anche simulato), che può portare ad una riduzione delle barriere di security, lasciando libertà di azione ad un malintenzionato.

- Il cambio di rotta, per evitare di volare sopra una zona di conflitto, può causare la congestione del traffico aereo in alcuni punti, con possibile rischio di perdita di separazione tra velivoli in volo.

- La recinzione, prevista per impedire l'accesso all'area lato volo dall'esterno, che può rappresentare un ostacolo importante, soprattutto per aeroporti con piste di dimensioni ridotte.

- La sempre crescete necessità di interconnettere i diversi sistemi, le infrastrutture e le strumentazioni, per migliorarne la gestione ed implementare la sicurezza, può indirettamente creare delle falle, che possono essere sfruttate da hacker per accedere al sistema informatico.

Risulta evidente come situazioni di questo genere, comportino una riduzione della sicurezza complessiva, intesa come insieme di entrambe le componenti. L'aspetto positivo è che nel settore aereo gli standard sono elevati, al punto che tali debolezze sono compensate da altre misure. Infatti, sia safety che security sono strutturate "a strati", con un modello analogo a quello visto per lo "Swiss Cheese" di Reason. Per uno stesso pericolo vengono predisposte più barriere e, con l'eventuale fallimento di una di esse, risulta comunque garantita la protezione, grazie alla presenza delle rimanenti. Il verificarsi di un incidente richiede il fallimento contemporaneo di tutte le barriere, le quali, essendo in numero elevato, rendono tale evento di probabilità remota. La perdita di una delle difese, rappresenta comunque un abbassamento non trascurabile della sicurezza, anche se marginato dalla presenza di altri livelli, e non può essere sottovalutato.

Quando il fallimento di una difesa potrebbe essere conseguenza dell'interferenza tra safety e security, è necessario svolgere delle valutazioni supplementari, per cercare di trovare una soluzione che non penalizzi nessuno dei due settori. In situazioni di questo tipo, la risposta solitamente più immediata è attuare misure alternative a quelle attuali. Volendo indicare un esempio, si consideri una barriera fisica di security, come una recinzione o una porta bloccata, la cui presenza costituisce pericolo per la safety, creando intralcio alle vie d'esodo. La barriera fisica potrebbe essere sostituita da una funzionale, come un sistema di vigilanza o di

videosorveglianza; ma tale misura potrebbe risultare non sufficiente, nel caso in cui la risorsa da difendere sia critica per il sistema e richieda di essere molto protetta. Il problema di interferenza non risulterebbe così risolto, ma semplicemente modificato dalla sua configurazione iniziale. Permane una condizione latente potenzialmente pericolosa, che, se non trattata, nel lungo periodo potrebbe portare ad incidente.

Il caso peggiore di correlazione, che possa verificarsi, è quando un evento, relativo ad uno dei due ambiti, ha ripercussioni dirette sulla sicurezza dell'altro. Non vi è una vera interferenza a livello di barriere, ma semplicemente le conseguenze dell'evento si spostano, ricadendo sull'altro ambito. Un esempio banale di questa situazione, sono gli attentati terroristici, in cui i danni causati possono rappresentare un pericolo e le persone, eventualmente ferite, necessitano di essere soccorse. Le frequenze con cui si verificano eventi combinati sono basse, sicuramente inferiori a quelle con cui si verificano i singoli episodi distinti di safety o di security. Questa tipologia di correlazioni, che avvengono a livello di conseguenze, presenta però diverse difficoltà di trattazione e di gestione. La criticità è rappresentata dall'elevata imprevedibilità delle conseguenze, che rende estremamente complesso adottare delle misure combinate. Per questo motivo, il miglior approccio di gestione a tali correlazioni rimane l'ottimizzazione delle misure dei singoli settori. Avere elevati standard, sia di safety che di security, riduce la probabilità di accadimento di incidenti in generale e, di conseguenza, anche quella che l'evento abbia conseguenze correlate. In un certo senso, implementare di pari passo entrambi i settori può essere comunque definita gestione integrata. Questo è ancor più vero, se le risorse sono gestite in modo unico e distribuite, per ottenere il massimo miglioramento a livello generale.

5.1.2 Combinazione positiva

Come visto, le interferenze tra safety e security, generano prevalentemente effetti negativi. Pur essendo meno frequente, esiste anche la possibilità che i due ambiti puntino nella stessa direzione, ovvero che le misure adottate vadano a combinarsi, con un miglioramento per entrambi gli ambiti. Una tale situazione si verifica quando un determinato pericolo, inerente all'ambito della safety, può diventare un obiettivo da colpire per un terrorista. Si deve quindi ridurre l'esposizione delle persone al pericolo e, allo stesso tempo, proteggere l'elemento, fonte di pericolo, da attacchi esterni.

Volendo fare un esempio, in un'infrastruttura critica come un aeroporto, è di fondamentale importanza garantire la continuità del servizio elettrico. L'energia e l'illuminazione rappresentano dei fattori critici, la cui mancanza può creare pericoli, sia per la safety che per la security. Risulta vitale garantire l'energia anche in situazioni di emergenza, motivo per cui vengono solitamente predisposte delle sale batterie, a cui si vanno ad aggiungere dei generatori e i rispetti serbatoi di combustibile. Queste strutture rappresentano senza dubbio un pericolo per tutti gli operatori non addestrati, che vanno quindi protetti. Allo stesso tempo però, possono essere oggetto di atti intenzionali, come l'incendio o la manomissione, in quanto parte di un piano d'attacco. La mancanza di energia elettrica causerebbe diverse vulnerabilità e amplificherebbe le esistenti; la presenza di un incendio o esplosione potrebbe distrarre l'attenzione dall'obiettivo principale dei terroristi. Ne consegue che l'accesso a tali strutture va impedito sia al personale profano che ad eventuali intrusi. Una barriera fisica, come una porta bloccata, il cui accesso è consentito esclusivamente ad operatori addestrati ed autorizzati, è certamente una misura efficace, integrando sia safety che security. Va aggiunto che, al fallimento di questa barriera, si avrebbe una riduzione della sicurezza di entrambi gli ambiti. Per questo è ovviamente necessario implementare altre misure supplementari, che, fossero anche relative ad un singolo settore, migliorerebbero comunque la sicurezza complessiva.

5.2 Approccio di gestione integrata

Al fine di evitare situazioni di interferenza o di conflitto, sarebbe opportuno trattare le due attività come parte di un unico insieme, e non come discipline separate, cosa che invece viene comunemente fatta. Nel Safety Management Manual (DOC 9859 ICAO) si parla di implementazione di un sistema di gestione integrato. L'idea è di unire i diversi settori (qualità, sicurezza, ambiente, ecc.) sotto un unico servizio, che gestisca contemporaneamente tutte le questioni amministrative (certificazioni, autorizzazioni) ed economiche. Questa integrazione tra più settori è facilitata dall'analogia delle strutture dei diversi sistemi di gestione, come può essere tra sicurezza e qualità. La somiglianza delle procedure e dei metodi, evita così la ripetizione dei compiti e permette l'ottimizzazione le risorse. Si potrebbe pensare di applicare tale approccio anche nel caso di safety e security. Tale metodo dovrebbe effettuare una considerazione più ampia di rischi e benefici, e programmare le azioni in modo tale da

implementare di pari passo entrambi i sistemi. Per quanto applicabile a livello teorico, un tale approccio presenta numerose difficoltà di realizzazione.

La sfida principale nella concretizzazione di un sistema così integrato tra safety e security, è sicuramente rappresentata dalla normativa, che regolamenta in modo separato i due settori. Come visto in precedenza, ad ogni livello, sono presenti legislazioni indipendenti che stabiliscono requisiti, in modo specifico per ciascuno dei due ambiti. Le procedure e le misure, che derivano dall'attuazione della normativa, non tengono perciò conto delle possibili interferenze. In particolare, nel caso specifico della security le disposizioni sono rigide e di applicazione rigorosa. Nella safety, invece, esiste anche una minima flessibilità, con la possibilità di realizzare misure in deroga, temporanea o parziale, se necessario. Ciò nonostante in determinate situazioni, le difficoltà nell'adottare soluzioni che garantiscano la sicurezza, in entrambi gli ambiti, non è così scontato. Stabilire un'unica normativa, che raccolga, sotto a delle disposizioni comuni, sia safety che security, risulta a prescindere essere un compito assai arduo, proprio per la natura contradittoria dei due settori stessi.

Inevitabilmente, quindi, la ricerca di un approccio integrato ricade sull'operatore che è chiamato ad applicare le diverse norme. Nel processo di valutazione dei rischi, i fattori di safety e security dovrebbero essere considerati sullo stesso piano e interagenti in modo biunivoco tra di loro. Infatti gli stessi fattori possono portare a conseguenze diverse, per le possibili interferenze tra le variabili. In aggiunta, l'interazione tra più fattori causali comporta una modificazione delle probabilità che l'evento finale si verifichi. Si dovrebbero quindi individuare dei modelli per studiare le possibili correlazioni, in particolar modo per poter stimare le probabilità e quindi il rischio correlato. Esistono diversi modelli utilizzabili per lo studio di eventi sia di safety che di security. Strumenti come l'albero dei guasti e degli eventi, il Bow-Tie o l'ARMS, ad esempio, si adattano perfettamente all'applicazione in entrambi gli ambiti. Tali metodi, però, per le loro caratteristiche non si addicono perfettamente alla valutazione delle correlazioni tra safety e security. La mancanza principale, se così possiamo definirla, è la difficoltà nell'esprimere i rapporti di dipendenza tra i diversi fattori. Infatti, si individuano le cause e le conseguenze di un evento, ma per i fattori sullo stesso livello non è possibile rappresentarne le correlazioni, qualora esistessero.

5.2.1 Modello per l'analisi delle correlazioni

L'idea è quindi quella di realizzare un modello in grado di rappresentare i rapporti di dipendenza, tra i diversi fattori, e che permetta un'analisi, qualitativa e quantitativa, di possibili eventi incidentali e delle sue cause. Ciò è possibile, sfruttando lo studio degli alberi dei guasti, precedentemente compiuto, ed elaborando un diagramma logico per analizzare le sequenze combinate. L'analisi singola degli eventi di safety e security deve comunque essere svolta, prima di poter effettuare la valutazione integrata. Infatti il modello, che verrà brevemente presentato nei prossimi paragrafi, non rappresenta un'alternativa alla classica valutazione dei rischi, ma è uno strumento di analisi supplementare, che la completa.

L'albero dei guasti è un modello che, partendo dall'evento finale, denominato *top event*, definisce le cause che possono dare origine all'occorrenza, operando in modo induttivo e cioè ripercorrendo al contrario la sequenza incidentale. Per ciascuna causa si individuano delle sotto-cause, che la generano, e la cui combinazione è definita tramite operatori logici. Ripetendo il passaggio ad ogni livello, si scende lungo la catena incidentale, giungendo a definire le cause elementari, ovvero i fattori iniziatori che non hanno ulteriori precursori. Partendo quindi dall'analisi di eventi distinti di safety e di security, i rispettivi alberi dei guasti possono essere assemblati in una valutazione unificata.

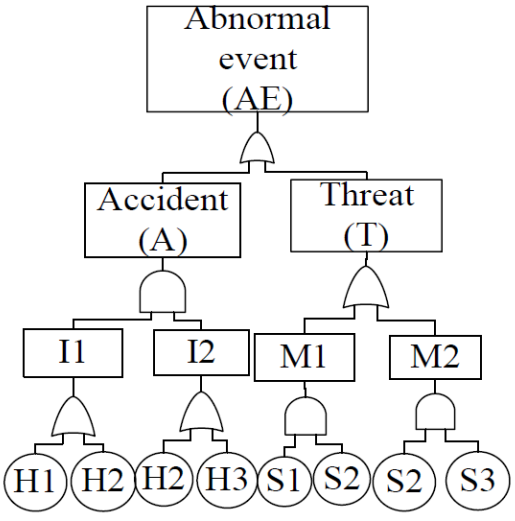

Figura 5.1. *Albero degli eventi per un evento anomalo*

Il top event di questa unione sarà indistintamente conseguenza dei fattori dei due ambiti e per questo lo definiamo, in modo generico, evento anomalo (*abnormal* event). Esso può derivare

da condizioni di safety, di security o una combinazione di entrambe. Non a caso l'interazione è indicata da un operatore "OR", che include sicuramente un elemento ma non esclude la possibilità che si verifichino entrambi.

Considerando un'unica generica occorrenza, è così possibile trattare alla pari, come parte di un unico insieme, gli eventi accidentali e gli atti intenzionali. Ma l'albero dei guasti presenta una struttura statica dei rapporti causali tra i diversi fattori. Convertendo l'albero dei guasti in un grafico bayesiano, possiamo invece valutare le connessioni in modo dinamico. La rete bayesiana è un particolare modello, che permette di descrivere le relazioni probabilistiche tra i diversi fattori. La struttura è un grafo aciclico diretto, con un'orientazione gerarchica di causalità. Ciascun collegamento rappresenta una particolare condizione di dipendenza statistica e quindi tutti gli elementi, che presentano in qualche modo una legame grafico, sono connessi tra loro. Viceversa, le variabili non collegate tra loro risultano essere indipendenti. Si definisce perciò uno schema logico, che focalizza l'attenzione sull'interazione consequenziale dei diversi elementi.

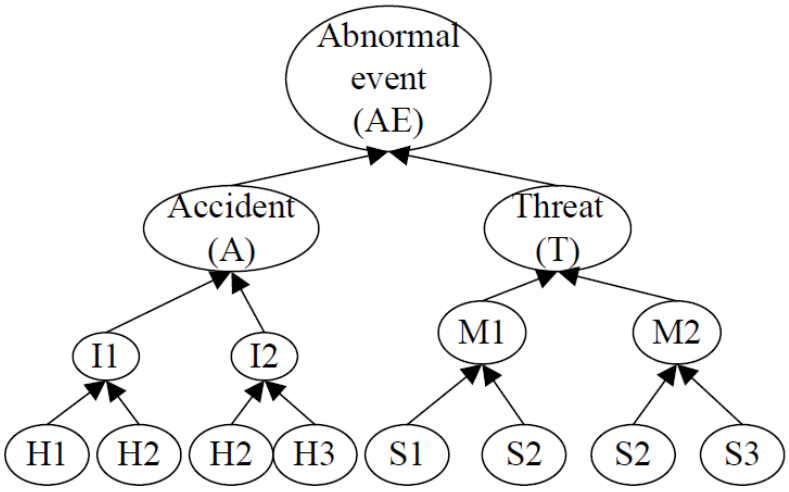

Figura 5.2. *Rete bayesiana per un evento anomalo*

L'utilizzo di un grafico di questo tipo, garantisce una maggior intuitività nell'individuazione delle relazioni tra i vari elementi. Ad esempio, se uno stesso elemento può contribuire al verificarsi di più eventi, quest'ultimi non posso essere considerati totalmente indipendenti tra loro. La probabilità dell'evento finale infatti sarebbe diversa dalla combinazione della probabilità dei singoli elementi. La flessibilità della rete bayesiana, consente di evidenziare come una causa comune possa contribuire a più eventi, rappresentandola con un unico nodo

che si dirama. Questa caratteristica, mette in risalto, in modo grafico, le relazioni logiche che legano i vari fattori.

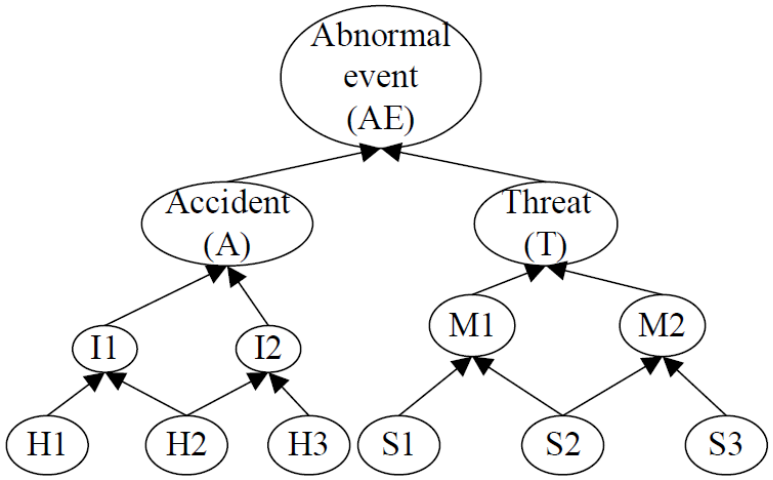

Figura 5.3. *Rete bayesiana con legami di dipendenza da fattori comuni*

Infine, creando connessioni tra le diverse variabili, possiamo individuare le correlazioni esistenti tra i diversi fattori di safety e di security. Si ottiene in questo modo un modello effettivamente integrato.

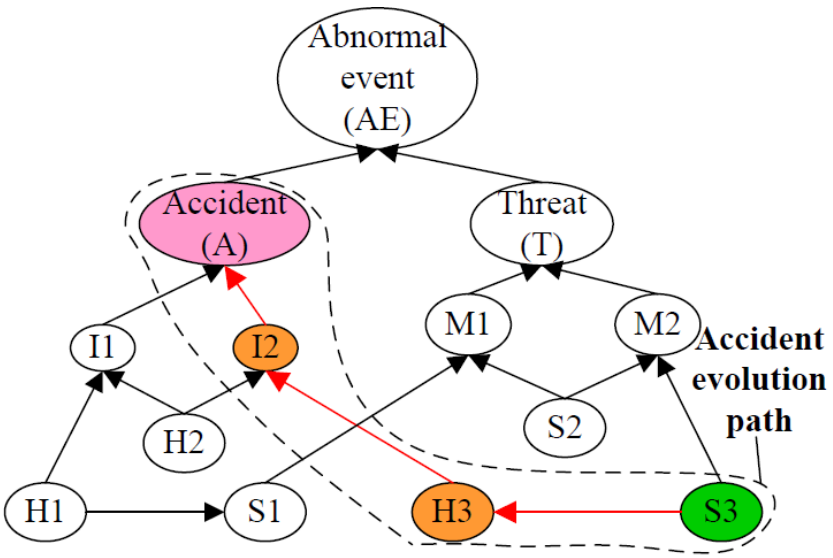

Figura 5.4. *Modello integrato per l'analisi delle correlazioni*

La rete bayesiana permette una valutazione qualitativa immediata, delle possibili combinazioni tra i fattori causali di un evento incidentale. Dall'esempio in figura 5.4, è

evidente come un fattore, individuato dall'ambito della security, possa risultare scatenante per una sequenza incidentale di safety. Analogamente può avvenire il contrario, ovvero che una condizione di safety degradi la protezione di security, aumentando le vulnerabilità del sistema.

5.2.1.1 Esempi di possibili scenari applicabili al modello

Per comprendere meglio il funzionamento del modello possiamo fare degli esempi. Una vulnerabilità di security, come una carenza dei controlli e delle barriere fisiche può consentire ad intrusi di accedere ad aeree critiche. L'intrusione può sfociare in una serie problematiche: si pensi ad un'invasione di pista, o anche semplicemente delle piste di rullaggio e del piazzale. Inevitabilmente si creano delle condizioni di safety, che impattano sulla sicurezza delle operazioni. Le ripercussioni potrebbero essere immediate, come l'aborto di un decollo o di un atterraggio, ma anche indirette, derivanti dalla chiusura temporanea della pista, come dirottamenti su altri aeroporti, congestione del traffico aereo, ecc.

Se il personale utilizza impropriamente un'uscita d'emergenza, questa, che di fatto rappresenta una misura fondamentale di safety, può trasformarsi in una vulnerabilità di security. Se l'uscita viene utilizzata, o addirittura lasciata aperta, quando non necessario, una possibile minaccia potrebbe sfruttarla per accedere nella struttura eludendo i controlli.

Un ulteriore esempio potrebbe essere quello rappresentato da una minaccia interna. Inefficaci controlli di security interni, sul personale (background check) o sui fornitori, possono far sì che questi creino intenzionalmente condizioni insicure. Ad esempio, la minaccia potrebbe essere rappresentata da un manutentore, che volontariamente monta sull'aeromobile un componente corrotto o non lo installa correttamente. Tale azione, se combinata con altre carenze di safety, come una supervisione non adeguata, può portare all'evento in cui un velivolo viene autorizzato a volare, nonostante non sia sicuro, con la possibilità che il componente guasto causi un incidente. Se per compiere tale azione, il manutentore sfrutta una criticità di safety, potremmo ricadere in una situazione in cui i due ambiti interferiscano ripetutamente tra loro. Un esempio di questo tipo di criticità potrebbe essere l'utilizzo di indicatori di quantità di carburante uguali per diversi modelli di aereo, con serbatoi di differente capacità. Una tale situazione, già verificatasi accidentalmente in passato con conseguenze catastrofiche (vedasi l'incidente del volo Tuninter 1153), consentirebbe uno scambio intenzionale delle componenti, con il risultato di falsare le rilevazioni del carburante presente nei serbatoi. Come nel volo Tuninter 1153, l'indicazione errata potrebbe incidere

negativamente sulle operazioni di rifornimento e portare al rischio di esaurire il carburante in volo.

5.2.1.2 Implicazioni pratiche

Per quanto riguarda l'applicazione pratica del modello, esso rappresenta un ottimo strumento per l'analisi qualitativa, essendo intuitivo e dinamico. Ma la definizione quantitativa della probabilità è una questione complessa. Tale calcolo riflette la valutazione precedentemente eseguita con gli alberi dei guasti. Già qui sono presenti delle discordanze, ovvero delle diversità tra i due ambiti. Mentre per i fattori di safety vi è una certa facilità nel reperire dati statistici o comunque nel determinare le variabili, come tassi di guasto o frequenze di errore, per le cause di security le probabilità di fallimento delle barriere, essendo soggette ad un gran numero di variabili, devono essere stimate. Ciò comporta una maggior soggettività nella procedura di quantificazione del valore, per quanto si possano definire metodi analitici di valutazione delle vulnerabilità. Inoltre, le interazioni tra safety e security sono varie e cambiano a seconda delle condizioni. In determinate situazioni, i fattori possono influenzarsi peggiorando in modo uniforme le conseguenze; in altri casi, uno stesso elemento può avere effetti opposti su safety e security. La probabilità finale dell'evento anomalo potrebbe non rappresentare correttamente il valore effettivo ed essere quindi sottostimata. Per questo motivo, il modello si appresta relativamente bene all'impiego in situazioni in cui safety e security sono in dipendenza diretta, ovvero quando il fallimento di una misura comporta una riduzione di sicurezza in entrambi i sensi. Di più complessa trattazione è invece la gestione di condizioni che non influenzano linearmente, allo stesso modo, i due ambiti.

5.3 Analisi post incidentale di eventi con correlazione tra safety e security

Come accade per le altre fasi della sicurezza, anche le inchieste incidentali vedono una trattazione separata tra safety e security. Per quel che riguarda la safety, l'Annesso 13 e il Regolamento CE 376/2014 hanno portato all'istituzione di un sistema di segnalazione, secondo il quale ogni inconveniente, rientrante in determinate categorie, deve essere reso noto. Tali normative hanno fatto sì che ogni aspetto venga indagato dettagliatamente e che le informazioni raccolte siano condivise, per il miglioramento dell'intero settore aereo. Al contrario in security, proprio per sua definizione e caratteristiche, le questioni vengono gestite

diversamente. Normalmente infatti, le varie problematiche vengono gestite internamente all'azienda stessa e da un numero ristretto di persone competenti, per proteggere le informazioni sensibili. Il manifestarsi di vulnerabilità di security, non comporta in automatico la sua segnalazione, anzi talvolta risulta conveniente all'azienda mantenere la riservatezza, per non correre il rischio di eventuali conseguenze, come una perdita d'immagine. Ovviamente tutto ciò va contestualizzato, perché quanto appena detto può verificarsi per tematiche meno gravi, come la cyber sicurezza. È sottointeso però che episodi di terrorismo, o che comunque possano rappresentare un pericolo per la pubblica sicurezza, vedano certamente l'intervento degli organi di polizia e delle autorità competenti.

Essendo l'analisi retrospettiva parte integrante del processo di miglioramento della sicurezza, è bene individuare dei metodi che consentano di eseguire correttamente l'indagine, qualora si verificassero degli eventi incidentali. Abbiamo visto, in precedenza, com'è possibile analizzare le relazioni, che si creano all'interno di un sistema, al fine di implementare una migliore e più completa valutazione dei rischi. I principi che devono guidare lo studio degli eventi derivanti dall'interferenza tra safety e security, uniscono gli obiettivi dell'analisi post incidentale e quelli dell'analisi delle correlazioni. Gli scopi sono quindi la ricerca delle cause, assieme alle correlazioni che tali fattori hanno avuto, e l'individuazione delle misure correttive. Possiamo così provare ad analizzare quali sono i metodi che meglio si adattano allo studio di eventi derivanti dall'interferenza tra safety e security.

I modelli per l'analisi retrospettiva sono vari e ciascuno focalizza su un particolare aspetto dell'indagine. Tra i metodi più impiegati, in praticamente ogni settore, si possono sicuramente annoverare l'albero dei guasti e l'albero degli eventi. Il primo analizza attraverso un processo induttivo, ovvero in senso opposto alla sequenza temporale di accadimento, le cause che hanno determinato un particolare evento e le loro connessioni logiche. L'albero degli eventi invece si focalizza sulle conseguenze, che tale evento può determinare. In particolare si analizzano l'efficacia di ciascuna barriera, messa in atto a proteggere il sistema, e si individuano i diversi scenari, derivanti dall'efficacia o meno delle difese. L'albero degli eventi è un procedimento deduttivo, in quanto si sviluppa seguendo l'ordine temporale, e ciascuna barriera genera una diramazione del grafico, in corrispondenza del suo fallimento o del suo successo.

Questi modelli, sviluppati per le analisi prospettiche di sicurezza, possono essere impiegati anche nelle indagini retrospettive, individuando la sequenza dell'evento incidentale. L'albero

dei guasti e l'albero degli eventi possono essere combinati, applicandoli insieme e analizzando la catena incidentale delle cause primarie fino alla sua conclusione. Come visto anche per l'analisi prospettica, vi è però una difficoltà nell'individuare le connessioni che si sono instaurate, tra i vari livelli e tra i diversi elementi. Perciò, nello svolgimento dell'inchiesta, è bene completare lo sviluppo di tali metodi, integrandoli con uno studio delle correlazioni. Il modello proposto, basato sulla rete bayesiana, si adatta perfettamente ad evidenziare la linea logico-sequenziale degli avvenimenti, anche nell'analisi post incidentale.

Come supporto, nella fase di individuazione delle cause, è preferibile tenere a mente anche il modello di sistema proposto nella teoria degli errori di Reason. Al fine di facilitare l'applicazione pratica del modello, è possibile definirne uno schema semplificato.

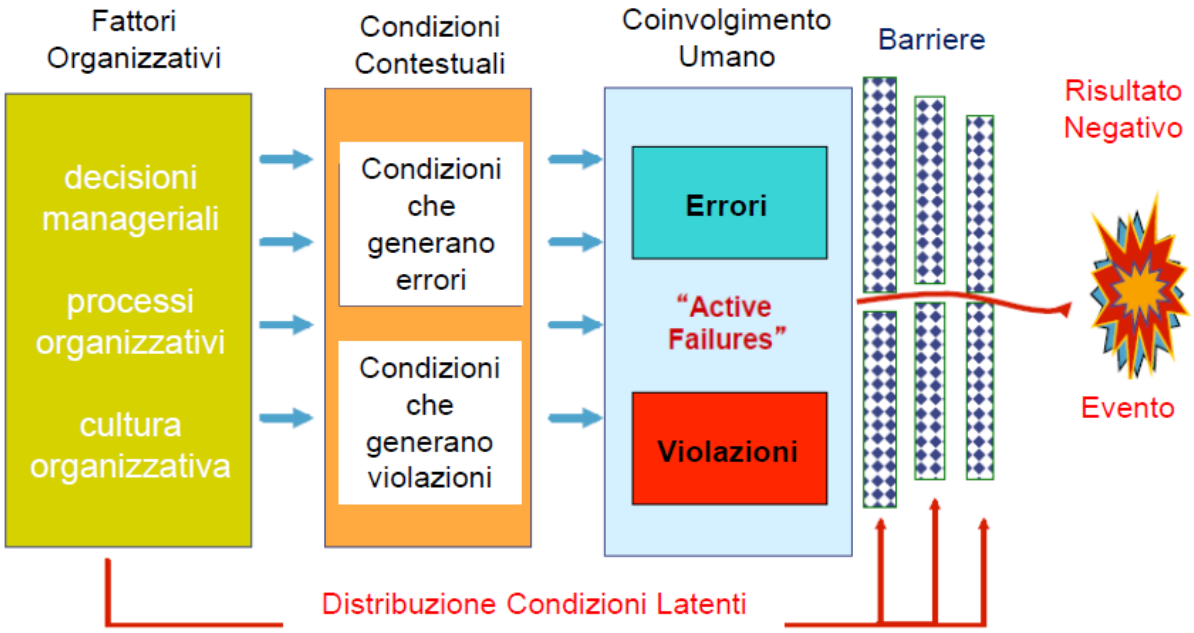

Figura 5.5. *Schema semplificato del modello di Reason, per l'analisi di inconvenienti*

In questa struttura si individuano quattro livelli di barriere, il cui fallimento contribuisce all'accadimento dell'incidente. I quattro livelli sono rappresentativi di:

- fattori organizzativi, siano essi relativi alla politica ed alla cultura organizzativa, o errori a livello dirigenziale;
- condizioni contestuali, ovvero particolari situazioni che portano ad errori o violazioni (ambiente lavorativo non salubre, strumenti inadeguati, presenza di pericoli, ecc.)

- coinvolgimento umano, che fa riferimento agli errori attivi, compiuti dal personale;
- barriere, che possono interrompere la sequenza incidentale o ridurne gli effetti.

Pur non essendo necessario ai fini della ricerca delle correlazioni, il modello di Reason si appresta bene all'individuazione di errori latenti e attivi, siano essi indistintamente di safety o di security. Definire la categoria a cui un errore appartiene, facilita l'individuazione della sua origine, contestualizzandolo nel sistema. Ciò risulta di grande aiuto per definire le misure correttive e le raccomandazioni, che sono necessarie ad evitare che l'incidente si verifichi nuovamente in un altro contesto.

5.3.1 Profondità dell'interferenza

Nell'analisi di un evento è interessante analizzare con che modalità si verificano le correlazioni tra safety e security. Precedentemente si sono viste già diverse casistiche e nei prossimi capitoli questo aspetto verrà ulteriormente sviluppato. Anticipando quanto si vedrà nell'analisi dei casi studio, si può già fare una distinzione tra due situazioni. Le interferenze infatti possono verificarsi a diversi gradi della catena incidentale, ovvero a livello di conseguenze o a livello di cause. La prima categoria fa riferimento a tutte quelle situazioni in cui un evento, verificatosi contestualmente ad un singolo ambito, ha delle conseguenze tali che i loro effetti modificano lo stato di sicurezza dell'altro ambito. Nel secondo caso invece gli elementi dei diversi settori interferiscono tra loro, generando precondizioni con riduzione delle sicurezza, intensa in senso generico del sistema, e possibilità di incidente.

La differenza sostanziale tra i due casi è nella loro gestione. Nella correlazione a livello di conseguenze, il modo più semplice ed immediato di intervenire è con l'implementazione delle difese dei singoli ambiti. Misure correttive riducono il ripresentarsi di determinate condizioni e quindi anche la probabilità di interferenza dovuta a tali eventi. La correlazione a livello di cause invece prevede che barriere con funzioni diverse vadano in conflitto, divenendo inefficaci. In questo caso è necessaria una valutazione integrata della situazione, per individuare delle misure alternative che riducano il rischio di interferenza.

Ovviamente tra le due categorie non vi è una distinzione netta, ma è piuttosto una differenza nell'approccio pratico. Vi possono anche essere dei casi limite, in cui le conseguenze di un evento interferiscano con altri fattori, esasperandone le criticità. Ma la varietà del livello a cui

i due settori possono interagire mette ancor più in risalto la necessità di attuare appositi studi e valutazioni. Per questo motivo, sia nella gestione che nell'indagine degli eventi con correlazione, è sempre bene attuare dei metodi integrati.

Capitolo 6

Il volo Philippine Airlines 434

L'episodio in questione è un attacco terroristico, avvenuto a bordo di un aereo di linea, tramite l'uso di un ordigno assemblato a bordo dell'aereo stesso. Il terrorista responsabile dell'esplosione fu poi scoperto essere Ramzi Yousef, già noto per l'attentato al World Trade Center del 1993. L'attacco, compiuto su questo volo, risultava di fatto essere una prova, con l'intento poi di riutilizzare la stessa tecnica su altri aerei, ma con esplosivi di maggiori dimensioni.

6.1 Resoconto dei fatti

Il volo 434, della Philippine Airlines, partiva da Manila, nelle Filippine, ed era diretto a Tokyo, in Giappone. Il viaggio non era però diretto, ma prevedeva uno scalo a Cebu, sempre nelle Filippine. L'11 dicembre 1994, alle 5:35, il Boeing 747-283B, decollava come previsto da Manila. A bordo dell'aereo erano presenti solo 43 passeggeri e tra questi c'era anche il terrorista Ramzi Yousef. L'attentatore era riuscito a prendere il volo utilizzando un falso passaporto italiano, sotto il nome di "Armaldo Forlani". Inoltre era riuscito a superare i controlli del metal detector, nascondendo il necessario per realizzare il detonatore (batterie, cavi e innesco) all'interno del tacco della scarpa. Una volta in volo, durante la prima tratta, Yousef entrò in bagno, dove, inosservato, assemblò la bomba utilizzando come timer per il detonatore un orologio da polso digitale, appositamente modificato. L'esplosivo utilizzato era la nitroglicerina liquida, tenuta nascosta in un contenitore di soluzione per lenti a contatto. Completata la bomba, Yousef impostò il timer a 4 ore, in modo tale che esplodesse durante la seconda tratta, ovvero lungo il volo da Cebu a Tokyo. Nascosta nuovamente l'esplosivo nel kit da toeletta, il terrorista uscì dal bagno e tornò al proprio posto. Successivamente, approfittando dei molti posti liberi, Yousef chiese ad un'assistente di volo il permesso di cambiare posto, con la scusante di una vista migliore. In realtà, il posto in cui sedette, non era casuale, ma era scelto in base a delle precise caratteristiche, necessarie ai fini dell'attacco. Infatti quel posto, il 26K, sotto cui l'attentatore posizionò la bomba, nei 747 era normalmente

situato direttamente sopra il serbatoio centrale. In questo modo, anche se l'ordigno era di dimensioni ridotte, la sua esplosione avrebbe innescato i combustili, portando alla distruzione del velivolo. Fortunatamente, in quella versione del 747, che era stata originariamente costruita per Scandinavian Airlines System, il 26K risultava essere posto al di sopra della stiva, due file più avanti rispetto al serbatoio centrale. Nascosta la bomba sotto il sedile, nella tasca del giubbotto salvagente, Yousef tornò al suo posto.

Una volta giunto a Cebu l'attentatore scese dall'aereo, assieme ad altre 25 persone. Dopo aver imbarcato 256 nuovi passeggeri, il 747 decollò alle 8:38. La partenza sarebbe dovuta avvenire alle 8:00, ma fu ritardata a causa della congestione aeroportuale. Alle 11:43, a 4 ore dall'attivazione del timer, il dispositivo si innescò. L'esplosione uccise immediatamente il passeggero seduto al posto 26K e ne ferì altri 10, seduti nei posti vicini. L'aereo, a seguito dell'urto, si inclinò improvvisamente verso destra, ma fu riportato in assetto dal pilota automatico. L'esplosione causò un buco, di circa mezzo metro di diametro, nel pavimento del comparto passeggeri e propagò nella stiva, ma fortunatamente non si verificarono ulteriori danni, né alla fusoliera esterna (un eventuale cedimento avrebbe portato alla depressurizzazione dell'aeromobile) né al carrello d'atterraggio. Furono invece danneggiati alcuni cavi di comando, con conseguente perdita di controllo dell'alettone destro, del timone e degli elevatori di coda. Il capitano Reyes, dopo aver lanciato il mayday, chiedeva il permesso di atterrare all'aeroporto di Naha, sull'isola di Okinawa. L'atterraggio di emergenza risultò più complicato del previsto. L'aereo, a causa dei danni subiti, non rispondeva ai comandi, né con l'autopilota inserito né in manuale. Dopo diversi tentativi, in cui provarono a forzare i comandi, l'equipaggio giunse alla soluzione di sfruttare la propulsione differenziale. Modificando i livelli di potenza dei motori in modo asimmetrico, fu possibile correggere lentamente la direzione del velivolo, per allinearla con la pista d'atterraggio. Progressivamente fu ridotta la spinta dei motori, scendendo di quota, e il combustibile in eccesso fu scaricato, consentendo di ridurre il più possibile la velocità ed esercitare un minor peso sul carrello in fase d'atterraggio. Alle ore 12:45, un'ora dopo l'esplosione il 747 atterrò all'aeroporto di Naha, senza ulteriori complicazioni.

Ad eccezione dell'unico passeggero morto in volo, tutte le altre persone (272 passeggeri e 20 membri dell'equipaggio) sopravvissero ed i feriti furono tempestivamente soccorsi. L'aver portato a terra il velivolo in sicurezza fu di fondamentale importanza anche per la raccolta di maggiori informazioni e la ricostruzione dettagliata della vicenda. Secondo i piani di Yousef,

l'aereo sarebbe dovuto esplodere in volo, mentre si trovava sopra il pacifico. I resti del velivolo, in quel caso, sarebbero precipitati e affondati, rendendo estremamente difficile la ricostruzione della vicenda. Invece, l'aver completato l'atterraggio in sicurezza, permise all'autorità di analizzare le prove a bordo dell'aereo. Dai frammenti dell'esplosione fu così possibile ricostruire le componenti utilizzate per assemblare l'ordigno, come le batterie, che risultarono essere un particolare modello venduto solo nelle Filippine. Essendo nota la presenza di alcuni terroristi a Manila, le investigazioni si concentrarono in questa città. Proprio a Manila, infatti, Yousef ed un suo complice lavoravano al progetto Bojinka, la versione successiva dell'attentato, in cui prevedevano di colpire contemporaneamente 11 voli diretti dall'Asia agli Stati Uniti. Ma un incendio nell'appartamento, avvenuto nel gennaio del 1995, fece scoprire i due terroristi. Yousef si diede alla fuga, venendo catturato in Pakistan, dopo un mese di ricerche, ed estradato negli USA.

6.2 Analisi degli eventi

Analizzando gli eventi accaduti, possiamo identificare una serie di condizioni, definibili come eventi positivi, che, se non si fossero verificate, le conseguenze sarebbero potute essere di gran lunga peggiori. Allo stesso tempo, altre barriere hanno invece fallito, poiché un loro eventuale intervento avrebbe contenuto ulteriormente i danni, o li avrebbe addirittura annullati, sventando l'attentato. Questi eventi, positivi e negativi, sono annoverabili in modo distinto all'ambito della safety o della security, eppure nell'insieme degli avvenimenti vanno tutti ad incidere, anche in diversa misura, sulle conseguenze finali.

6.2.1 Eventi negativi

Consideriamo inizialmente i fallimenti, ovvero quelle barriere che non hanno avuto efficacia o che erano assenti.

6.2.1.1 Il controllo degli accessi

La prima misura che avrebbe potuto - e dovuto - sventare l'attentato rientra tra gli elementi di security ed è il controllo dei passeggeri all'ingresso del lato volo in aeroporto. I controlli al metal detector non sono stati sufficienti a rilevare gli strumenti utilizzati per assemblare il detonatore. Infatti cavi e batterie erano stati nascosti, in modo ingegnoso, all'interno del tacco

della scarpa, che si trovava al di sotto del campo d'azione del metal detector. L'orologio da polso, usato poi come timer, nonostante fosse modificato superò tranquillamente i controlli, essendo comunque un oggetto di uso comune. Pure la nitroglicerina passò inosservata, poiché era stata nascosta in un contenitore di liquido per lenti a contatto. Al giorno d'oggi, strumenti quali i LEDs (*Liquid Explosive Detection System*) rileverebbero facilmente la presenza della nitroglicerina. In assenza di tali attrezzature, come in quella occasione, ricade tutto sulla sensibilità del operatore. L'addetto di sicurezza avrebbe dovuto, in primo luogo, essere in grado cogliere, dall'analisi comportamentale, i sintomi tipici di un soggetto che tenta di introdurre articoli proibiti oltre il varco. Solitamente attentatori inesperti lasciano trapelare nervosismo o agitazione, ma Yousef era abile e in ogni situazione è sempre riuscito a mostrarsi calmo, in modo tale da non destare sospetti. Inoltre fosse anche riuscito ad intuire la possibile presenza di articoli proibiti, l'operatore avrebbe dovuto avere l'addestramento e l'esperienza necessaria a riconoscere l'esplosivo.

6.2.1.2 Riconoscimento dell'attentatore

Una miglior attività di intelligence avrebbe potuto permettere di identificare Ramzi Yousef, ancor prima che si imbarcasse sull'aereo. Il terrorista era già ben noto alle autorità americane: il 26 febbraio 1993 realizzò l'attentato al World Trade Center, nel cui parcheggio sotterraneo, insieme ad altri 2 complici, fece esplodere un furgone, contenente quello che è considerato il più grande ordigno artigianale mai costruito. La bomba, una combinazione di 590 kg di nitrato di urea e 3 bombole di idrogeno compresso, uccise 6 persone e ne ferì 1042, molte delle quali rimasero intossicate dai fumi, che raggiunsero il 93° piano di entrambi le torri. Dopo l'attacco, partì una caccia all'uomo per catturare Yousef, al punto che divenne una delle 10 persone più ricercate dall'FBI. Nonostante ciò, un passaporto falso, per quanto fedelmente riprodotto, è stato sufficiente per superare i controlli. Si sarebbe potuto operare una maggior cooperazione e diffusione delle informazioni tra le Nazioni. Molto probabilmente, se Yousef avesse tentato di prendere un aereo negli USA, con le stesse modalità operate nelle Filippine, sarebbe stato immediatamente riconosciuto e catturato. Nelle Filippine invece agì inosservato. Inoltre gli strumenti a disposizione nel 1994 non possono essere paragonati a quelli attuali. Oggi si parla di riconoscimento biometrico, sistema computerizzato in grado identificare un soggetto tramite segni caratteristici, quali i tratti somatici, le impronte digitali o l'iride. Allora poteva risultare difficile anche solo condividere, con tutti gli operatori, la foto segnaletica di un ricercato. Come ulteriore fattore è necessario considerare la diversità tra le priorità delle

due Nazioni. L'obiettivo principale dei terroristi era risaputo essere gli USA e altre Nazioni occidentali. Non rientrava negli intenti del terrorista colpire altri Stati, come le Filippine, per cui veniva considerato un minaccia poco credibile.

6.2.1.3 Segnalazione dei comportamenti sospetti

Il volo da Manila a Cebu durò circa 1 ora e 15 minuti. Durante questo periodo, Yousef si spostò più volte a bordo dell'aereo: prima si recò al bagno, dove assemblò l'ordigno; nascondendo nuovamente la bomba all'interno del kit da toletta, ritornò al suo posto. In un secondo momento, si spostò al posto 26K per posizionare l'esplosivo, per ritornare infine al suo posto assegnato. Questi spostamenti furono notati da un'assistente di volo, la quale però li riporterà solo in un secondo momento, quando interrogata. Di fatto, il ripetuto cambio di posto, su un volo di così breve durata, difficilmente passa inosservato. Lo scalo a Cebu corrispondeva anche con il fine turno dell'hostess, la quale scese dall'aereo senza riportare l'informazione, né al personale di competenza né all'equipaggio che saliva a bordo per il turno successivo. Se l'informazione fosse passata, si sarebbe potuto avviare una ricerca a bordo del velivolo, che avrebbe probabilmente consentito di rinvenire l'ordigno. È pensabile che un controllo di routine interno al velivolo sia stato comunque svolto, ma in assenza di particolari sospetti individuare un ordigno di piccole dimensioni, in un posto specifico quale la tasca del giubbotto salvagente, posta sotto il sedile, è molto difficile. In situazioni normali, un controllo così accurato, avrebbe richiesto un tempo eccessivamente lungo, sicuramente non convenevole per la durata dello scalo.

6.2.1.4 Protezione dei cavi di comando

Arriviamo adesso a quello che rappresenta l'evento negativo per la safety. I cavi di comando non hanno resistito all'urto generato dall'esplosione. Ciò nonostante, non si può dire che il loro dimensionamento non fosse corretto: sicuramente un impatto di tale dimensione, in quel punto, non era ragionevolmente prevedibile. L'esplosione, per quanto di dimensioni contenute, si propagò verticalmente, in relazione alla forma e al posizionamento della bomba. L'energia fu assorbita principalmente dal passeggero seduto al posto 26K e, nella rimanente parte, dalla pavimentazione, che cedette. I cavi erano posti nel soffitto della stiva e furono investiti in modo diretto dall'urto. Cavi maggiormente protetti, comunque, non è detto sarebbero stati in grado di sopportare l'esplosione e mantenere le funzionalità richieste. Un posizionamento diverso dei cavi avrebbe probabilmente introdotto rischi diversi e non sarebbe stato

conveniente. La ridondanza, piuttosto, avrebbe garantito il corretto funzionamento del velivolo. Cavi di controllo ripetuti, con percorsi diversi, possono assicurare la funzionalità anche nel caso in cui un evento imprevedibile, come quello in questione, renda inutilizzabile uno dei due.

6.2.1.5 Accesso ai dati dell'aeromobile

Una piccola considerazione va fatta anche per la parte di protezione delle informazioni. Yousef sapeva che il posto 26K, nella configurazione usuale del Boeing 747, era situato immediatamente sopra il serbatoio principale. La fortuna ha poi voluto che l'aereo impiegato avesse una disposizione diversa dei posti a sedere, scongiurando un evento catastrofico. Se la bomba avesse avuto dimensioni maggiori, le probabilità di incidente fatale sarebbero state maggiori, nonostante il posizionamento non preciso. Anche perché non è di così difficile intuizione la posizione approssimativa del serbatoio, in relazione a quella dei sedili. Invece la quantità ridotta di nitroglicerina ha reso necessario che il contenitore, per causare i danni voluti, dovesse essere posto con precisione e tale posizione era ben nota al terrorista. Si sarebbe quindi potuto operare una miglior protezione di tali dati. Indubbiamente Youssef disponeva di abilità e mezzi non trascurabili per reperire le informazioni, ma limitare la diffusione di tali conoscenze, anche se apparentemente non sensibili, soltanto a chi di competenza, avrebbe se non altro reso più complicato l'operazione.

6.2.2 Eventi positivi

In opposizione, un'altra serie di fattori ha impedito che l'esito dell'evento fosse ancor più drammatico di quanto avvenuto.

6.2.2.1 Capacità dell'equipaggio

L'addestramento e l'esperienza del capitano furono fondamentali per riuscire a governare il velivolo, considerando i danni che lo stesso aveva subito. Quando l'autopilota smise di rispondere ai comandi, decise di assumere il controllo, consapevole del rischio che l'aereo potesse sbandare nuovamente a destra e perderne il controllo. Con freddezza mantenne il controllo della situazione e, fornendo le giuste istruzioni, guidò gli altri membri dell'equipaggio, riuscendo atterrare in sicurezza. Una situazione analoga, in cui il velivolo non rispondeva più ai comandi, accadde 5 anni prima, nel volo 232 della United Airlines. In quel caso l'esito però fu ben più grave, in quanto 111 dei 285 passeggeri morirono a seguito

dell'atterraggio violento. La miglior conclusione del Philippine Airlines 434 va sicuramente ricondotta alle abilità del pilota.

In modo analogo va evidenziata la preparazione degli assistenti di volo, che riuscirono a tranquillizzare i passeggeri, facendoli rimanere seduti ai loro posti, nonostante il panico a bordo - come si può ben immaginare - fosse diffuso. Bloccando sul nascere la formazione di disordini, l'equipaggio riuscì a prestare soccorso ai feriti in modo tempestivo ed efficace. Alcuni assistenti inoltre simularono di prendersi cura del ragazzo seduto al posto 26K, nonostante fosse deceduto subito dopo l'esplosione. Fingendo che avesse solo bisogno di una coperta e della maschera d'ossigeno, evitarono di creare ulteriore panico tra gli altri passeggeri.

Per il loro comportamento, l'allora Presidente filippino, Fidel Ramos, conferì a tutti i membri dell'equipaggio un riconoscimento, premiando la loro "gestione professionale di una situazione potenzialmente disastrosa".

6.2.2.2 Altri fattori casuali

Oltre queste barriere, controllabili, una serie di fattori ha modificato positivamente le sorti dell'evento. Tuttavia tali condizioni sono annoverabili come puramente casuali, alcune oltretutto non si sarebbero dovute nemmeno verificare. Ne è esempio il ritardo accumulato dal volo, per motivi di traffico all'aeroporto di partenza. Secondo i piani di Yousef, al momento dell'esplosione, l'aereo si sarebbe dovuto trovare al di sopra del Pacifico, nel punto del tragitto più lontano dalla terra ferma. I 38 minuti di ritardo, invece, hanno fatto sì che l'aeroporto di Naha fosse sufficientemente vicino, per poter compiere un atterraggio d'emergenza in breve tempo. Se il volo fosse stato puntuale, non è da escludere che l'elevata distanza dalla costa avrebbe costretto l'equipaggio ad effettuare un ammaraggio, con le conseguenti complicazioni dei soccorsi.

Altro fattore, già descritto in precedenza, è la posizione della bomba, relativa al serbatoio che avrebbe dovuto danneggiare. L'ordigno si sarebbe dovuto trovare esattamente sopra i serbatoi, ma fortuna volle che il velivolo presentasse una configurazione diversa dal modello principale. In questo modo, l'unico danno grave causato al velivolo fu la rottura dei cavi di comando. Ma va considerato anche il modo in cui fu posizionato l'ordigno, che, combinato con la conformazione dello stesso, ha fatto sì che l'esplosione si sviluppasse nella direzione verticale, anziché orizzontale. Quest'ultima sarebbe potuta rivelarsi comunque una condizione

pericolosa, poiché il 26K era un posto esterno, ovvero vicino alla fusoliera. A così breve distanza, un'esplosione propagante orizzontalmente avrebbe impattato direttamente sul rivestimento esterno ed è probabile che tale protezione sarebbe stata perforata, causando una depressurizzazione dell'aeromobile. In tal caso, si sarebbero resi necessari i respiratori per tutti i passeggeri e le operazioni di soccorso ai feriti si sarebbero rivelate decisamente più complicate.

6.3 Identificazione delle cause

L'evento iniziatore e le sue cause, possono essere ritenute appartenenti interamente all'ambito della security, sebbene le conseguenze siano ricadute sulla safety. Possiamo quindi svolgere delle indagini separate. Per quanto riguarda la ricerca delle cause, si può sviluppare un albero dei guasti, che analizza gli elementi di security e i relativi fallimenti. Essendo l'albero prettamente mirato all'indagine dell'incidente, sono stati inclusi solo gli elementi che hanno concorso, in senso stretto, alla definizione del top event. Possono essere identificate, un insieme di possibili cause, derivanti dalla combinazione di diverse cause elementari, tutte di security.

- L'inadeguatezza della strumentazione e delle procedure con cui venivano svolti i controlli degli accessi, che non sono stati in grado di rilevare la presenza degli articoli proibiti.

- La mancata identificazione del terrorista, dovuto sia a fattori latenti che attivi. Nel primo caso sono comprese l'insufficiente cooperazione internazionale (assenza delle liste No-Fly) e la sottovalutazione della minaccia terrorismo, sia livello di sistema Paese che aeroportuale. Nel secondo caso, un basso livello di allerta e un carente addestramento degli operatori hanno generato precondizioni, tali che l'analisi comportamentale fosse inefficace o non eseguita.

- Troviamo un addestramento insufficiente e procedure non ben strutturate, anche per gli operatori della compagnia aerea. In aggiunta era, molto probabilmente, presente anche un ambiente con una cattiva comunicazione o una cultura poco orientata alle questioni di security. Tutto ciò non ha consentito di avviare la ricerca, nonostante i segnali, lasciati dai continui e sospetti spostamenti del terrorista, fossero relativamente

evidenti. Anche il particolare design interno del velivolo ha contribuito a rendere difficile un possibile ritrovamento dell'ordigno durante le verifiche a bordo, sempre che quest'ultime siano state svolte.

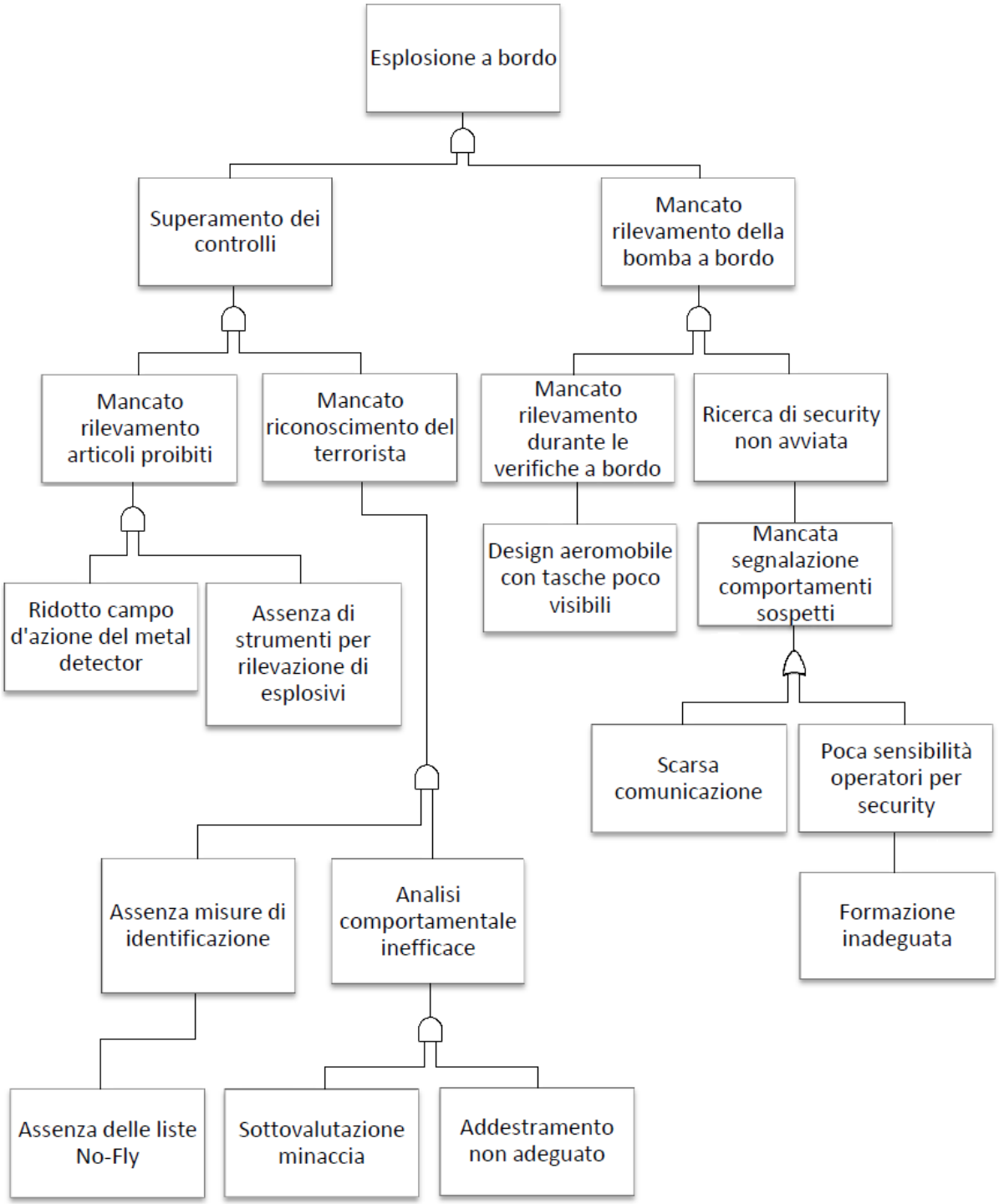

Figura 6.1. *Albero dei guasti per gli eventi di security*

Passando ora ad indagare le conseguenze che l'evento ha comportato, possiamo notare che tutte le ripercussioni sono sfociate in problematiche di safety. L'intento dell'attentatore era causare la distruzione del velivolo, con l'esplosione dei serbatoi, ma, per un insieme di cause fortuite, riuscì solo a danneggiarlo. L'unica barriera effettiva è rappresentata dall'abilità dell equipaggio di volo. Gli altri fattori, se modificati, avrebbero portato a differenti condizioni, che potevano compromettere la safety in modo diverso. È interessante quindi osservare come il fallimento e il successo delle barriere incidano sui possibili scenari, diversi da quello effettivamente verificatosi.

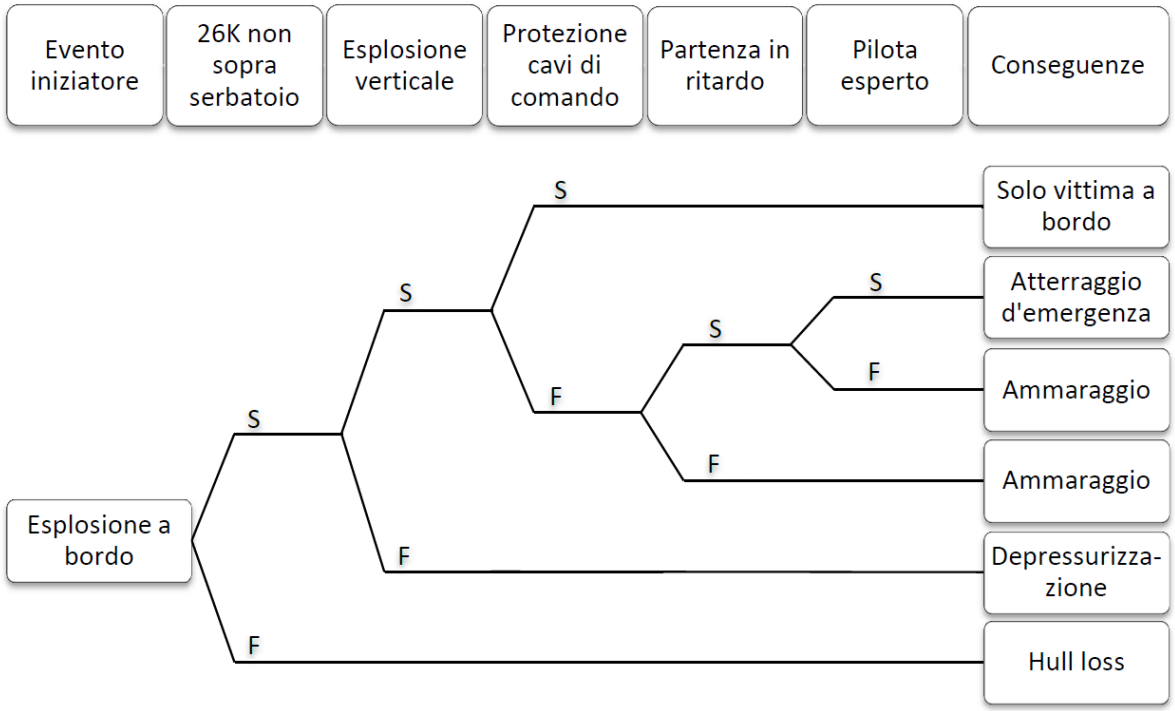

Figura 6.2. *Albero degli eventi per le conseguenze di safety*

- Se la bomba fosse stata posizionata sopra il serbatoio, come era nelle intenzioni del terrorista, l'esplosione avrebbe causato la distruzione totale dell'aereo (*hull loss*). I resti sarebbero precipitati sull'Oceano Pacifico, affondando per la maggior parte, e il loro recupero sarebbe stato molto complicato.

- Se l'esplosione si fosse propagata orizzontalmente, anziché verticalmente, avrebbe provocato maggiori danni alle persone, sedute nei posti vicini, e probabilmente anche morti in più. Inoltre il rivestiemento della fusoliera avrebbe ceduto, con la conseguente depressurizzazione del velivolo. In compenso i cavi di comando non sarebbero stati

danneggiati, consentendo un atterraggio più semplice e sicuro, dal punto di vista delle operazioni del pilota.

- Analogamente si sarebbe potutto atterrare senza complicazioni, se i cavi di comando fossero stati maggiormente protetti (ad esempio tramite rindondanza) e l'esplosione non ne avesse danneggiato il funzionamento.

- Infine nell'eventualità in cui il volo fosse stato puntuale, e quindi ben lontano dalla costa al momento dell'esplosione, oppure l'equipaggio fosse stato poco esperto, è probabile che non si sarebbe riuscito a compiere con successo l'atterraggio d'emergenza. L'esito finale quindi sarebbe stato incerto, con diversi possibili esiti: ammaraggio, l'evento più probabile, ma anche impatto al suolo, o eventualmente un atterraggio violento in pista.

Ricostruiti i percorsi logici dell'evento, si può infine classificare le cause per il loro livello di radicamento nel sistema.

Figura 6.3. *Modello di Reason per l'evento*

Possiamo costruire un modello di Reason (figura 6.3) che raccoglie ad ogni livello le principali cause dell'incidente. Dallo schema possono essere tratte le azioni correttive in corrispondenza degli errori latenti. Contestualizzando l'incidente, che si ricorda essere avvenuto nel 1994, notiamo che le misure segnalate sono già state implementate nel corso degli anni, alcune già in quelli immediatamente successivi.

6.4 Considerazioni

In generale, in eventi di security come attacchi terroristici, il cui obiettivo è proprio quello di causare danno alle persone, le ripercussioni sulla safety sono inevitabili. Nel caso in analisi, questa correlazione risulta ancora più evidente. Gli effetti dell'esplosione, per quanto minori rispetto alle intenzioni del terrorista, hanno richiesto una gestione d'emergenza della situazione, da parte del personale di bordo. L'impatto dell'evento fu puramente di safety, in quanto fu messa a rischio la salute dei passeggeri e l'integrità del velivolo. L'obiettivo dei piloti fu di gestire le difficoltà di manovra, per atterrare in modo sicuro.

L'evento ha comportato una situazione estrema ed imprevedibile, alla quale non era predisposta una procedura specifica. La decisione ricadde quindi sulla sensibilità del pilota, nel dover valutare come agire in modo da ridurre al minimo i rischi. Ad esempio tra le varie alternative prese in considerazione dall'equipaggio del Philippine Airlines 434, è probabile che vi fosse anche l'ammaraggio, ma che sia stato scartato in quanto troppo pericoloso, viste le maggiori difficoltà per le successive operazioni di soccorso.

Il caso studio mette in evidenza come safety e security interagiscano in modo diretto. Non si trattò di un'interferenza a livello delle cause elementari dell'evento, ma un episodio di security che ha causato un danno al sistema safety. Per queste situazioni, la gestione delle misure, relative ai due ambiti, è più convenevole che avvenga separatamente. Infatti si sarebbe dovuto implementare maggiormente le barriere di security, che hanno fallito, proprio per evitare alla radice il possibile accadimento dell'attentato. La gestione, immediatamente successiva all'evento, è invece ricaduta sulla safety. Si possono quindi identificare due macro-eventi, il primo di security e il secondo di safety. La conclusione di uno ha portato alla modificazione delle condizioni operative dell'altro.

La gestione di questa tipologia di correlazioni, è assumibile come l'insieme delle gestioni separate. Esiste una semplice consequenzialità, a livello di conseguenze tra eventi. Possiamo riassumere questa correlazione come una cattiva gestione di security che sfocia in un problema di safety. I due ambiti possono essere gestiti separatamente, applicando le rispettive misure. Nel caso della safety, la situazione risultante è un evento straordinario, tanto che non era prevista una procedura da seguire, specifica per questa circostanza. L'eccezionalità è sicuramente dovuta all'interferenza della security e gli effetti di tale relazione sono altamente inaspettati, motivo per cui viene difficile una gestione integrata. Basti pensare all'imprevedibilità del posizionamento di una bomba a bordo dell'aereo. Ai sensi dell'Annesso 17 ICAO, ogni velivolo, con massa a decollo eccedente i 45500 kg o in grado di trasportare più di 60 passeggeri, deve prevedere una zona a basso rischio bomba, proprio per minimizzarne gli effetti sull'aeromobile e i suoi occupanti, nel caso ne venisse rilevata una a bordo. Ma non è possibile prevedere gli effetti di un ordigno nascosto a bordo, non potendo anticiparne le caratteristiche e la posizione. Ne consegue che attuare una gestione integrata in casi simili risulta essere un'operazione eccessivamente complessa.

6.4.1 Analogia con il volo United Airlines 232

A conferma dell'ipotesi che, pur essendoci una correlazione, siamo di fronte a due eventi separati, si può riportare il caso del volo United Airlines 232. Gli eventi iniziatori furono di origine diversa, ma le conseguenze furono proprio le stesse. In questo caso, ci fu un cedimento esplosivo della ventola del motore di coda. I detriti della ventola furono proiettati in diverse direzioni ed alcuni colpirono il sistema idraulico di controllo, che passava sotto il motore, danneggiandolo. Il cedimento, dovuto a rottura a fatica, fu il risultato di manutenzione e controlli inadeguati. Il sistema di controllo fu danneggiato, compromettendo la possibilità di comandare il timone e gli equilibratori. Non si trattò quindi di un atto intenzionale, ma di carenze di safety. L'impatto però fu lo stesso: la riduzione della sicurezza del velivolo, dovuta alla perdita dei controlli. Anche in questo caso, l'unica soluzione, per poter direzionare l'aeromobile, fu sfruttare la propulsione differenziale. Si può dire quindi, per similitudine, che sia in questo caso che in quello della Philippine Airlines, si possono distinguere due eventi separati. Il primo evento, che in un caso è di security nell'altro di safety, ha avuto delle conseguenze tali da innescare, in entrambe le situazioni, delle ripercussioni

sulla safety. Quindi le misure correttive prevedono il miglioramento della sicurezza dei due ambiti in modo distinto, senza dover ricorrere ad una valutazione integrata approfondita.

6.4.2 Analogia con il disastro di Tenerife

Un'altra comparazione può essere fatta con il tragicamente noto disastro di Tenerife, avvenuto nel 1977 e in cui morirono 583 persone. L'evento, che rappresenta il più grave incidente aereo mai accaduto, si trattò della collisione tra due aerei passeggeri, avvenuta sulla pista di atterraggio. Nel verificarsi dell'evento, si manifestarono un insieme di precondizioni di safety:

- infrastruttura aeroportuale limitata, essendo uno scalo regionale;
- personale del controllo del traffico aereo non sufficientemente preparato;
- eccessiva confidenza del capitano e passività degli altri membri dell'equipaggio;
- scarsa visibilità.

Ma il vero fattore scatenante fu un evento di security. Infatti la mattina dell'incidente, ci fu un attentato all'aeroporto di Las Palmas, che fu chiuso preventivamente per timore di una seconda esplosione. I voli furono dirottati proprio sullo scalo di Tenerife, il cui traffico aereo subì una congestione. Ci fu un aumento imprevisto del numero di voli, al di sopra delle capacità dell'aeroporto, esasperando tutte le criticità di safety già esistenti. Di fatto si trattò di un incidente di safety, senza alcuna interferenza diretta di security. Sarebbe stata sufficiente una migliore gestione delle barriere di safety per evitare l'evento, anche perché la congestione dell'aeroporto sarebbe potuta essere causata da altri fattori.

Capitolo 7

Il volo Germanwings 9525

L'incidente che coinvolse il volo Germanwings 9525 è tragicamente noto, in quanto tale disastro fu causato da un'azione deliberata del pilota, il quale fece impattare l'aereo al suolo, nelle Alpi Francesi. Nessuna delle persone a bordo sopravvisse all'incidente.

7.1 Resoconto dei fatti

Il volo 9525, di Germanwings, operava tra Spagna e Germania, collegando Barcellona a Düsseldorf. Il 24 marzo 2015, l'Airbus A320-211 operava quella tratta, come programmato. Il decollo avvenne da Barcellona alle 9:00, con a bordo 144 passeggeri e 8 membri dell'equipaggio (2 piloti e 6 assistenti di volo). Lo stesso equipaggio quella mattina aveva completato senza nessun inconveniente la stessa tratta, ma in direzione opposta, ovvero partendo da Düsseldorf alle 6:01 e atterrando a Barcellona alle 7:57. A Barcellona venne fatto uno stop e, concluse le operazioni di sbarco e imbarco, si ripartì in direzione di Düsseldorf. Fu il copilota ad eseguire le operazioni di decollo e, dopo circa 3 minuti dal decollo, venne inserito l'autopilota, per completare la salita fino a 38000 piedi. Fino a quel momento non vi fu nessun segnale che facesse presagire quello che sarebbe successo dopo. Come confermato dalle registrazioni del CVR, tutte le operazioni procedettero normalmente, fino a quando il capitano lasciò la cabina di pilotaggio. Infatti, dopo aver raggiunto l'altitudine di crociera ed aver impostato la rotta del volo, il capitano si recò alla toilette, chiedendo al copilota di continuare a rilevare le comunicazioni radio. Circa 30 secondi dopo che la porta della cabina era stata chiusa, l'altitudine selezionata venne cambiata, da 38000 piedi a 100 piedi. L'autopilota cambiò modalità, riducendo la potenza dei motori e iniziando lentamente la discesa. La velocità di discesa iniziale era di 1700 piedi/min. A quel punto venne modificata anche la regolazione della velocità, passando da essere gestita automaticamente dal sistema a controllata dal pilota. Il valore della velocità selezionata fu cambiato diverse volte, per poi essere impostato a 302 nodi, corrispondente ad una discesa di quasi 3500 piedi/min. Dopo quasi 3 minuti dall'inizio della discesa, il centro di controllo di Marsiglia, con il quale l'aereo

era precedentemente in contatto radio, chiese a che altitudine fossero autorizzati a volare. Il copilota non rispose al controllo radio, che tentò di entrare in contatto altre 2 volte. Il valore selezionato di velocità aumentò nuovamente, fino a 323 nodi. Dopo 4 minuti che il capitano aveva lasciato la cabina di pilotaggio, suonò per la prima volta il segnale di richiesta d'accesso. Ulteriori tentativi di contatto, da parte del centro di controllo, non ottennero nessuna risposta da parte del copilota, il quale aumentò un'ultima volta la velocità, al valore di 350 nodi. Nei minuti successivi, seguirono ripetute richieste di accesso alla cabina di pilotaggio, prima tramite il citofono, poi bussando in modo progressivamente più insistente. Oltre al centro di controllo di Marsiglia, il controllore della Difesa Aerea Francese e l'equipaggio di un altro aereo tentarono di entrare in contatto con il copilota, ma senza ricevere risposta. Negli ultimi secondi di volo, prima della schianto, si attivarono gli allarmi di collisione con il terreno, ma furono ignorati. Alle 9:41:06 l'aereo impattò violentemente al suolo, causando la morte di tutte le persone a bordo.

7.1.1 L'inchiesta incidentale

Le indagini, come previsto dall'annesso 13 ICAO, furono svolte dal BEA (*Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile*), essendo l'incidente avvenuto in territorio francese. Collaborarono gli enti nazionali per la sicurezza aerea di Germania (la compagnia e l'aereo erano tedeschi), Spagna (per fornire i dati relativi allo scalo a Barcellona) ed altre autorità, sia nazionali che internazionali. Non essendoci sopravvissuti e quindi nessuno che potesse testimoniare su come si svolsero i fatti, il FDR (Flight Data Recorder) e il CVR (Cockpit Voice Recorder) giocarono un ruolo fondamentale per la ricostruzione dell'accaduto. I dati di volo e le registrazioni, delle comunicazioni e dei rumori in cabina, hanno permesso di ripercorrere le azioni compiute dal copilota. Nel rapporto d'inchiesta pubblicato da BEA, sono segnalati in modo puntuale i momenti cruciali, definiti tramite l'analisi dei dati di FDR e CVR. Si riporta di seguito, la ricostruzione delle ultime fasi del volo.

1. Ore 9:27:20. L'aereo raggiunge quota 38000 piedi, corrispondente all'altitudine di crociera.

2. Ore 9:30:00. L'ultima comunicazione tra l'equipaggio di volo e il centro di controllo di Marsiglia, il quale chiede di impostare la rotta verso il waypoint di IRMAR.

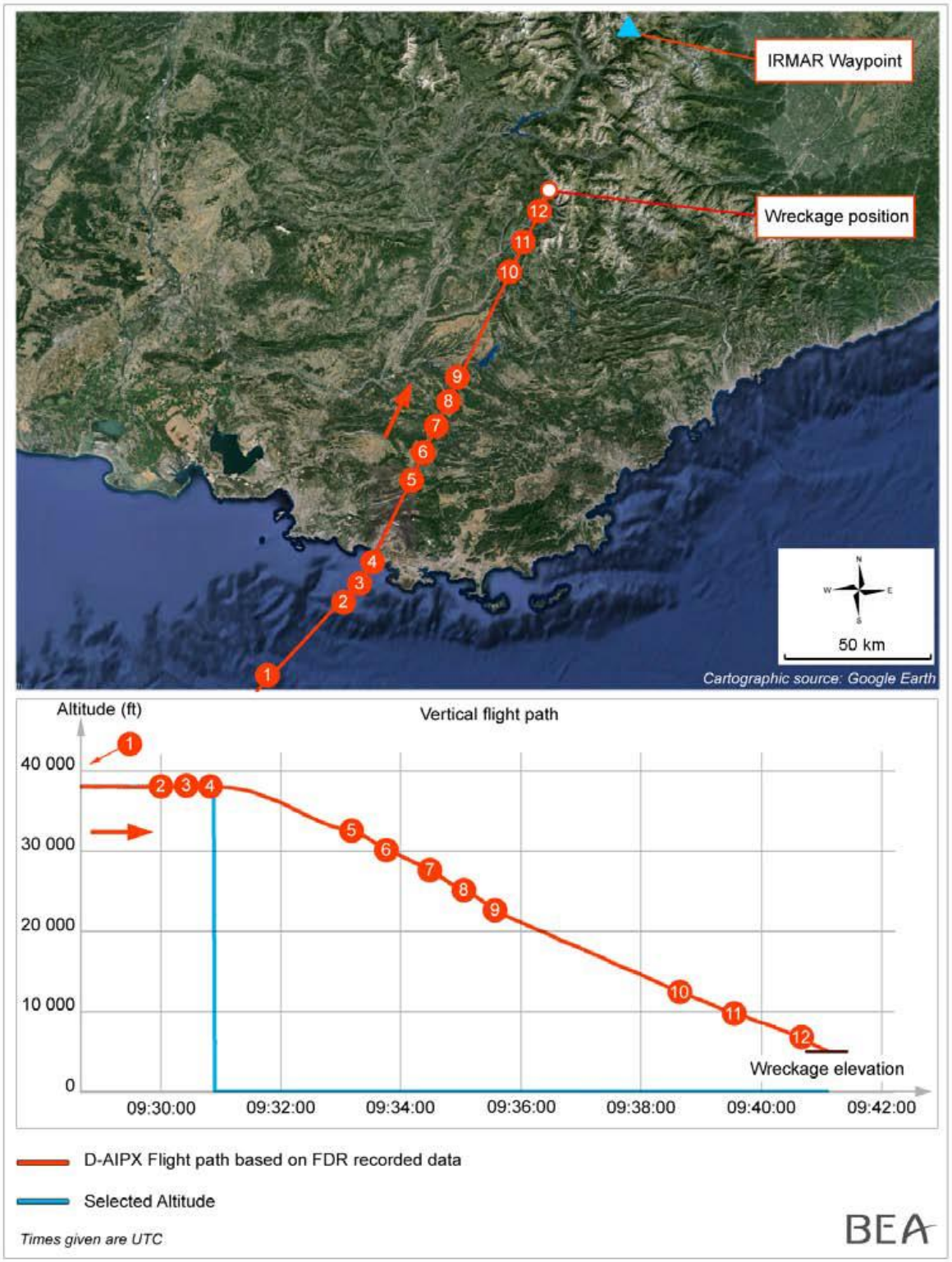

Figura 7.1. *Rappresentazione spaziale e temporale delle fasi salienti degli ultimi minuti del volo Germanwings 9525 (Fonte BEA)*

3. Ore 9:30:24. Il capitano lascia la cabina di pilotaggio.
4. Ore 9:30:53. Il copilota imposta l'autopilota, per scendere a quota 100 piedi.
5. Ore 9:33:12. Il copilota imposta l'autopilota, per aumentare la velocità a 308 nodi.
6. Ore 9:33:47. L'aereo si trova a quota 30000 piedi. Il controllore chiede a che altitudine sono autorizzati a volare, ma il copilota non risponde.
7. Ore 9:34:31. Suona il segnale di richiesta d'accesso alla cabina.
8. Ore 9:35:03. Il copilota aumenta la velocità a 350 nodi.
9. Ore 9:35:32. Si sente per la prima volta il rumore di una persona che bussa alla porta del cockpit. I rumori proseguiranno sempre più insistenti, per 3 minuti e mezzo.
10. Ore 9:38:38. Il controllore della difesa aerea francese cerca, per 3 volte, di entrare in contatto con il copilota, ma senza ottenere risposta.
11. Ore 9:39:30. Il primo di 5 colpi violenti alla porta della cabina.
12. Ore 9:40:41. Gli allarmi di prossimità con il terreno iniziano a suonare. Dopo 25 secondi l'aereo impatta con il suolo.

Sulle base delle informazioni ottenute dalle registrazioni, si è poi proceduto con indagini più approfondite, ricercando le condizioni latenti che hanno fatto sì che l'incidente si verificasse.

7.2 Analisi degli eventi

Le conseguenze dell'accaduto sono state catastrofiche, con la distruzione del velivolo e la morte di tutti i passeggeri. Nessuna barriera, di tutte quelle previste, è riuscita ad interrompere la sequenza che ha portato all'incidente, né a limitarne i danni. Perciò, a differenza del precedente, il caso studio in questione non presenta nessun evento positivo. Di seguito si analizza l'insieme degli eventi negativi.

7.2.1 Sistema di chiusura della porta della cabina di pilotaggio

La cabina di pilotaggio era separata dal lato passeggeri da una porta, dotata di un sistema di chiusura elettrico e meccanico. I pannelli separatori avevano una composizione a sandwich, tale da garantire la resistenza alle armi da fuoco, esplosivi e altri sistemi di intrusione, come previsto dall'annesso 6 ICAO. Tale misura era conseguenza degli attacchi terroristici dell'11 settembre 2001 ed era mirata ad impedire l'accesso di persone estranee. Il sistema di chiusura, a triplo scatto, veniva normalmente controllato elettronicamente dalle postazioni di entrambi piloti, tramite degli appositi dispositivi di comando. Sempre dal lato interno della cabina era presente anche un blocco di tipo meccanico, come misura aggiuntiva al sistema elettronico. Quando un membro dell'equipaggio (un assistente di volo o un pilota che si era momentaneamente assentato) necessitava di entrare, doveva comunicarlo ai piloti tramite una tastiera numerica, posta esternamente, dal lato passeggeri. Digitando il codice per la richiesta, un segnale acustico comunicava la richiesta ai piloti, i quali potevano, dalla loro postazione, sbloccare o tenere bloccata la porta. Per ragioni di safety, era possibile digitare un codice di emergenza, che sbloccava la porta se entro 15 secondi non era compiuta nessuna azione di risposta da parte dei piloti. Questa misura era necessaria per situazioni di incapacità del pilota rimasto in cabina, ad esempio in caso di malore. Il sistema, proprio perché pensato per proteggere i piloti da intrusioni esterne, non prevedeva misure nella situazione opposta, ovvero in cui la minaccia fosse stata interna all'abitacolo. Chiunque si trovasse all'interno poteva intenzionalmente tenere bloccata la porta ed impedire l'accesso in cabina.

Durante il corso delle investigazioni, risultò che un'altra compagnia aerea aveva implementato un sistema che permetteva di isolare la zona della toilette dal compartimento passeggeri. Il sistema consisteva nel bloccare, tramite l'uso di un pannello, il passaggio tra le due zone. L'operazione, che doveva essere eseguita da un assistente di volo, permetteva di ottenere una zona di controllo sicura, priva di estranei, con maggior sicurezza per l'equipaggio di volo nel momento in cui lasciava la cabina.

Tale soluzione, però, non avrebbe potuto comunque impedire l'incidente, in quanto la porta del cockpit sarebbe stato comunque possibile bloccarla dall'interno. Affinché fosse efficace, nella situazione in oggetto, si sarebbe dovuto prevedere un ulteriore sistema che impedisse il bloccaggio simultaneo delle due porte. Per ottenere ciò, si poteva far sì che il bloccaggio di una porta, automaticamente comportasse lo sbloccaggio dell'altra. In questo modo, nel caso in

cui uno dei piloti lasci la cabina, si è protetti da interferenze illecite, ma allo stesso tempo si rende impossibile, ad una minaccia interna, di chiudercisi dentro.

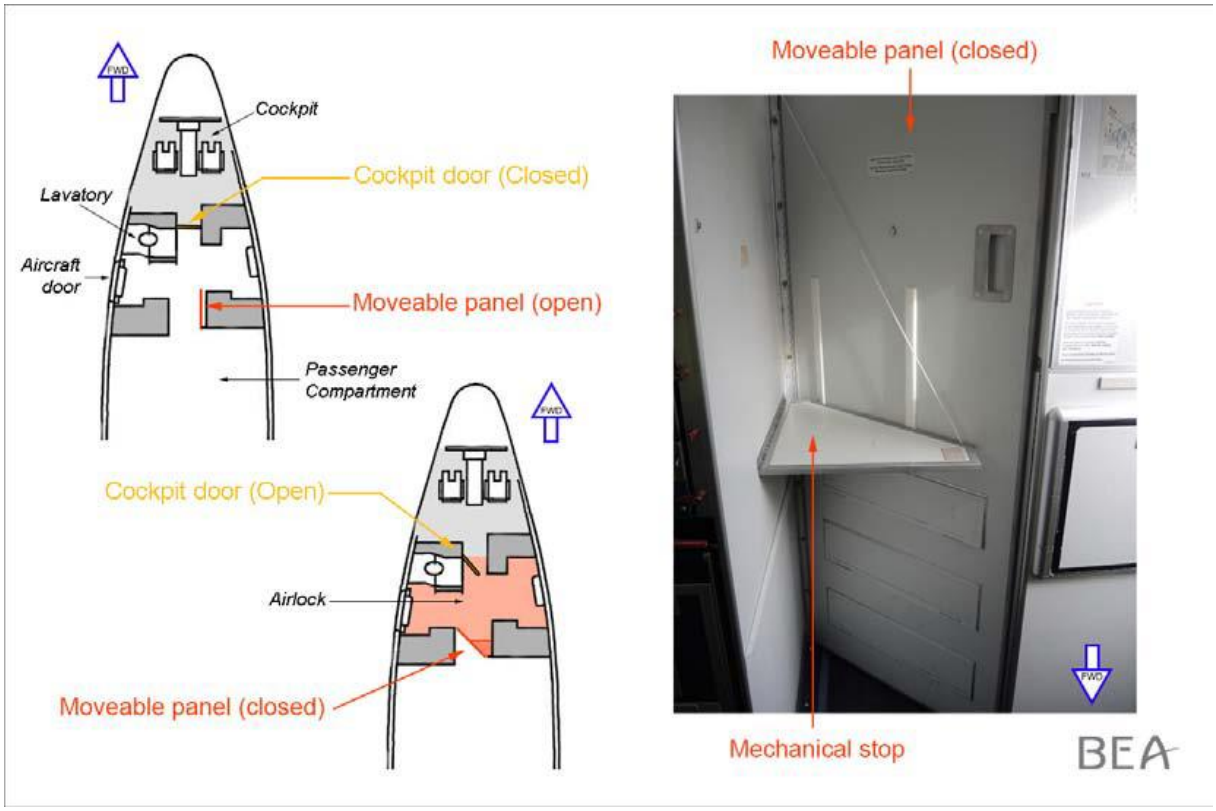

Figura 7.2. *Schema e foto del sistema di bloccaggio meccanico (Fonte BEA)*

7.2.2 L'idoneità al volo

Nell'annesso 1 ICAO sono stabiliti i requisiti, fisici e mentali, che un pilota deve possedere per esercitare i diritti di licenza. Tali requisiti sono assicurati tramite la valutazione medica di Classe 1, verificando l'assenza di malattie o disabilità, che possano improvvisamente impedire al pilota di condurre l'aereo in sicurezza. La valutazione comprende anche l'individuazione di disordini mentali o altri disturbi psicologici.

7.2.2.1 Gestione delle informazioni mediche

Il copilota, responsabile dell'atto, aveva precedentemente sofferto di episodi di depressione nel 2008, durante il suo periodo di addestramento per diventare pilota. Pur non avendo sintomi psicotici, la depressione lo portava ad aver pensieri suicida, perciò sospese il percorso formativo per sottoporsi ad un trattamento specifico. Dieci mesi dopo, la depressione fu

dichiarata superata ed ottenne nuovamente il certificato medico di classe 1. Il certificato venne rilasciato ma con restrizioni, ovvero che un'eventuale ricaduta lo avrebbe invalidato. Ripreso il programma di addestramento, nel 2010 superò l'esame scritto ed ottenne l'abilitazione per l'A320. Nel giugno 2014 iniziò la carriera come copilota presso Germanwings, ma già in dicembre dello stesso anno comparvero i primi sintomi di una ricaduta, con problemi di vista e disturbi del sonno. A partire da metà febbraio 2015 e fino ad una settimana prima dell'incidente, il copilota si fece visitare da 5 diversi dottori privati. I vari medici riscontrarono sintomi di ansia e psicosi, rilasciando certificati di malattia e rinviando il giudizio ad uno psichiatra o psicoterapeuta per un trattamento. Nessuno dei certificati venne mai recapitato a Germawings. Secondo la legislazione tedesca, i documenti medici erano soggetti a protezione e riservatezza delle informazioni. In particolare, il codice penale prevedeva sanzioni fino all'arresto, nel caso in cui un professionista rivelasse segreti personali e privati dei propri pazienti. Eccezioni, per quanto riguarda la riservatezza medica, esistevano, ma solo con il consenso della persona, oppure qualora ciò si rendesse indispensabile al fine di tutelare la sicurezza di altri o del paziente stesso. Pur essendo presente questa possibilità, non esisteva nessun obbligo di segnalazione per il professionista. Quindi se ad un pilota venivano diagnosticate malattie incompatibili con il suo incarico, il medico curante non era tenuto ad informare né le autorità né l'azienda presso la quale operava il pilota. Non esistendo alcun obbligo, il medico non era sicuramente incentivato a comunicare la situazione, oltretutto rischiando di violare la riservatezza medica. Si creò quindi una situazione di conflitto tra la protezione delle informazioni e la sicurezza aeronautica.

Nello stesso periodo, tra febbraio e marzo, il copilota consultò anche uno psichiatra il quale gli prescrisse degli antidepressivi e dei sonniferi. L'assunzione di tali farmaci in concomitanza con l'esercizio dei compiti di pilota, come riportato anche dall'annesso 1 ICAO, può comportare situazioni di grave pericolo. I soggetti con depressione, che assumono farmaci, non dovrebbero essere autorizzati a volare, a meno che una valutazione medica non accerti che, nel caso specifico, i medicinali assunti non interferiscano sullo svolgimento in sicurezza dei propri incarichi. La valutazione supplementare non venne mai eseguita, essendo l'azienda all'oscuro della situazione. Dalle visite annuali, effettuate per il rinnovo del certificato di Classe 1, risultò non esserci alcuna presenza di disordini mentali, di personalità o comportamentali. Secondo il parere di molti esperti di medicina aeronautica, effettuare analisi specifiche per identificare malattie mentali, durante i controlli di routine, è

inappropriato o non produttivo. Però in casi di episodi pregressi, come quello in questione, sarebbe stato utile prevedere delle verifiche più approfondite o una maggior frequenza delle visite periodiche, pur non essendoci nessun obbligo a riguardo.

7.2.2.2 Il volo precedente

Valutare la probabilità che un pilota diventi non idoneo al volo è un'operazione difficile, specie nel caso di psicosi improvvise, che sono rare e perciò difficilmente prevedibili. Oltretutto, si fa affidamento sulla presenza di un secondo pilota, che può continuare a svolgere i compiti, in caso di incapacità del collega. Il copilota, nei giorni e nelle ore precedenti, non mostrò mai i sintomi della depressione di cui soffriva, tanto che nessuno dei piloti con cui volò notò comportamenti strani. Nemmeno i familiari ne erano al corrente. L'unica informazione, che avrebbe permesso di intervenire in modo preventivo, erano i dati del volo precedente. Infatti il copilota, che si era già trovato in un'occasione da solo in cabina, durante la fase di approccio a Barcellona, aveva modificato l'altitudine selezionata. Analogamente a come fece successivamente, impostò ripetutamente il livello di volo a 100 piedi, tornando però ogni volta al valore per cui era autorizzato a volare.

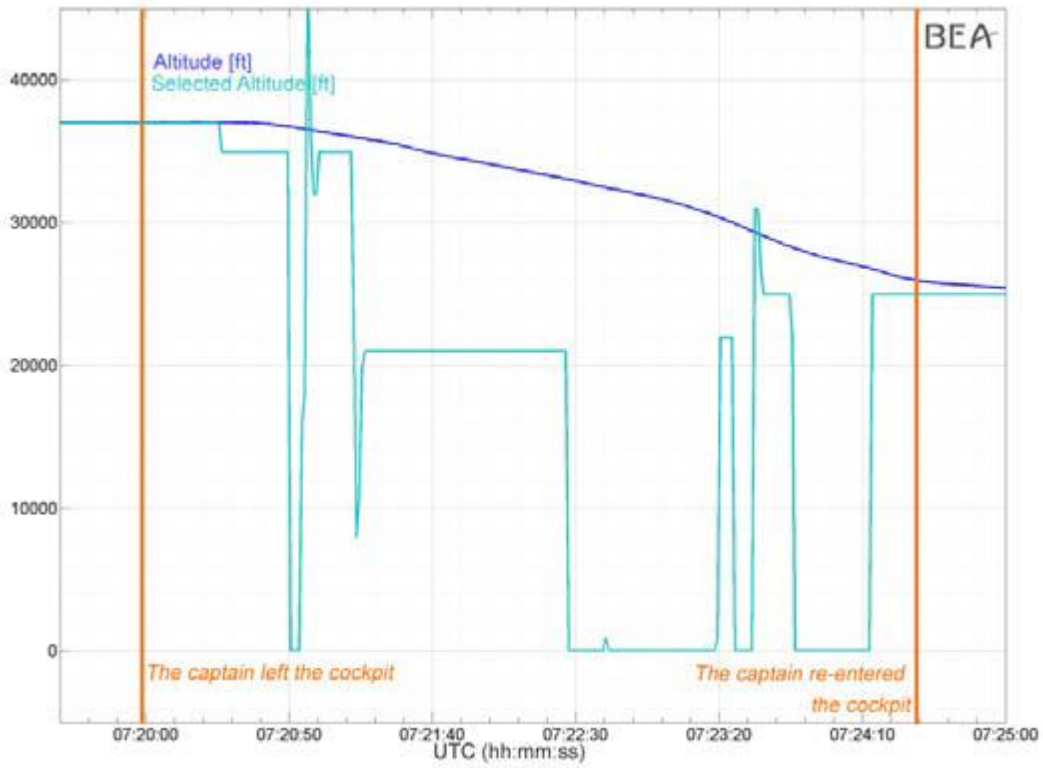

Figura 7.3. *Andamento nel tempo dall'altitudine selezionata (in azzurro) e dell'altitudine del velivolo (in blu) indicate in piedi (Fonte BEA)*

Questo comportamento può essere interpretato come una prima intenzione di suicido, non portata a termine. Essendo già nella fase di approccio all'aeroporto, nessuno notò queste variazioni, poiché l'autopilota esegue questi cambi di altitudine in modo graduale, facendo così apparire l'andamento della discesa pressoché invariato. L'aereo era dotato di un sistema di trasmissione dati, compatibile con il Mode S EHS, che trasmetteva sia le informazioni sulla posizione ma anche i parametri di volo, tra cui l'altitudine selezionata. Tale sistema permette ai controllori di sapere in anticipo i movimenti dell'aereo e gestire al meglio ogni deviazione. Sfortunatamente i radar civili francesi, pur ricevendoli, non visualizzavano ancora tali informazioni sui monitor dei controllori di volo. Fossero stati visti quei dati, si sarebbe potuto intervenire fermando in via preventiva il copilota, non appena giunto a Barcellona.

7.2.2.3 Misure contro l'inidoneità al volo del pilota

Per quanto riguarda il calcolo del rischio accettabile, per incapacità del pilota, vanno analizzati due aspetti. Il primo punto riguarda la consuetudine di considerare la presenza di due piloti, a bordo dell'aereo, un'adeguata misura di safety. Infatti, in caso di sopravvenuta incapacità, durante il volo, si riteneva sufficiente il fatto che un secondo membro dell'equipaggio avrebbe comunque assicurato la continuità delle operazioni. Tutte le valutazioni di sicurezza, perciò faceva affidamento su questa considerazione.

Come secondo aspetto, si aggiunge il fatto che l'inabilità, fosse essa fisica o mentale, era trattata nello stesso modo. Ciò dava per scontato che un pilota inadatto al volo, dichiarasse autonomamente le proprie non idoneità. Il copilota era ben consapevole delle sue condizioni, ma non ha mai segnalato all'azienda la sua situazione. È probabile che tale comportamento sia il risultato della preoccupazione di perdere l'incarico, situazione che il copilota non sarebbe stato in grado di accettare. Ogni giovane pilota era coperto da un'assicurazione, nel caso fosse stato dichiarato non idoneo al volo, entro i primi anni dall'inizio della carriera. L'assicurazione però copriva esclusivamente le spese sostenute durante l'addestramento e non prevedeva risarcimenti per il mancato guadagno, derivante dalla perdita dell'incarico. A questo, va aggiunto il dover rinunciare alle proprie passioni e ambizioni, e il ruolo sociale che l'incarico da pilota rappresentava. Ci sono diversi validi motivi, quindi, che possono aver spinto il copilota a mantenere segreta la sua depressione.

Per situazioni di questo tipo, erano presenti numerosi programmi di supporto psicologico, messi a disposizione da Germawings. Questi programmi, che prevedevano una partecipazione

anonima, per facilitarne la partecipazione, venivano svolti con successo ed erano ben strutturati. Il copilota, però, non vi prese mai parte e questo può essere dovuto ad una poca pubblicizzazione degli stessi. Avere degli strumenti di supporto efficaci ma non incentivarli, ha lo stesso risultato di non averli. Un maggior impegno nel rendere nota l'esistenza di questi programmi, avrebbe potuto incoraggiare il copilota a farsi aiutare nelle sue difficoltà.

7.3 Identificazione delle cause

A differenza del volo Philippine Airlines 434, in questo caso studio safety e security si influenzano reciprocamente a vari livelli del sistema. Per evidenziare tali connessioni è bene utilizzare lo schema logico, basato sul grafico bayesiano (figura 7.4). Come si può notare dal diagramma, un insieme di fattori di safety hanno portato a delle precondizioni, tali da consentire al copilota di compiere un atto intenzionale. In questo senso, l'azione in sé risulta un evento di security, che però è avvenuto in un contesto di safety. Infatti, le diverse cause radice sono relative alla salute dei piloti ed alla gestione delle problematiche, derivanti da un'eventuale inabilità al volo. Le misure messe in atto non sono risultate sufficienti, ad impedire che il copilota, non idoneo al volo, si ritrovasse in servizio. La depressione, unita all'uso di farmaci antidepressivi, ha portato il copilota a compiere un atto intenzionale. È probabile che sia stato soggetto a psicosi, con istinti suicida o anche alienazione dalla realtà. Questa condizione ha interferito contemporaneamente con una misura di security e una di safety. Quest'ultime risultano essere in particolare contrasto. Infatti la protezione della cabina di pilotaggio dalle intrusioni, può potenzialmente rendere inefficace la misura di sicurezza che si basa sulla presenza di due piloti. Se la si combina con un atto intenzionale, si ha l'impossibilità di intervenire per fermarlo, nonostante il secondo pilota sia presente a bordo. In questo caso si può notare un intenso grado di correlazione tra i due ambiti, a diversi livelli della sequenza incidentale.

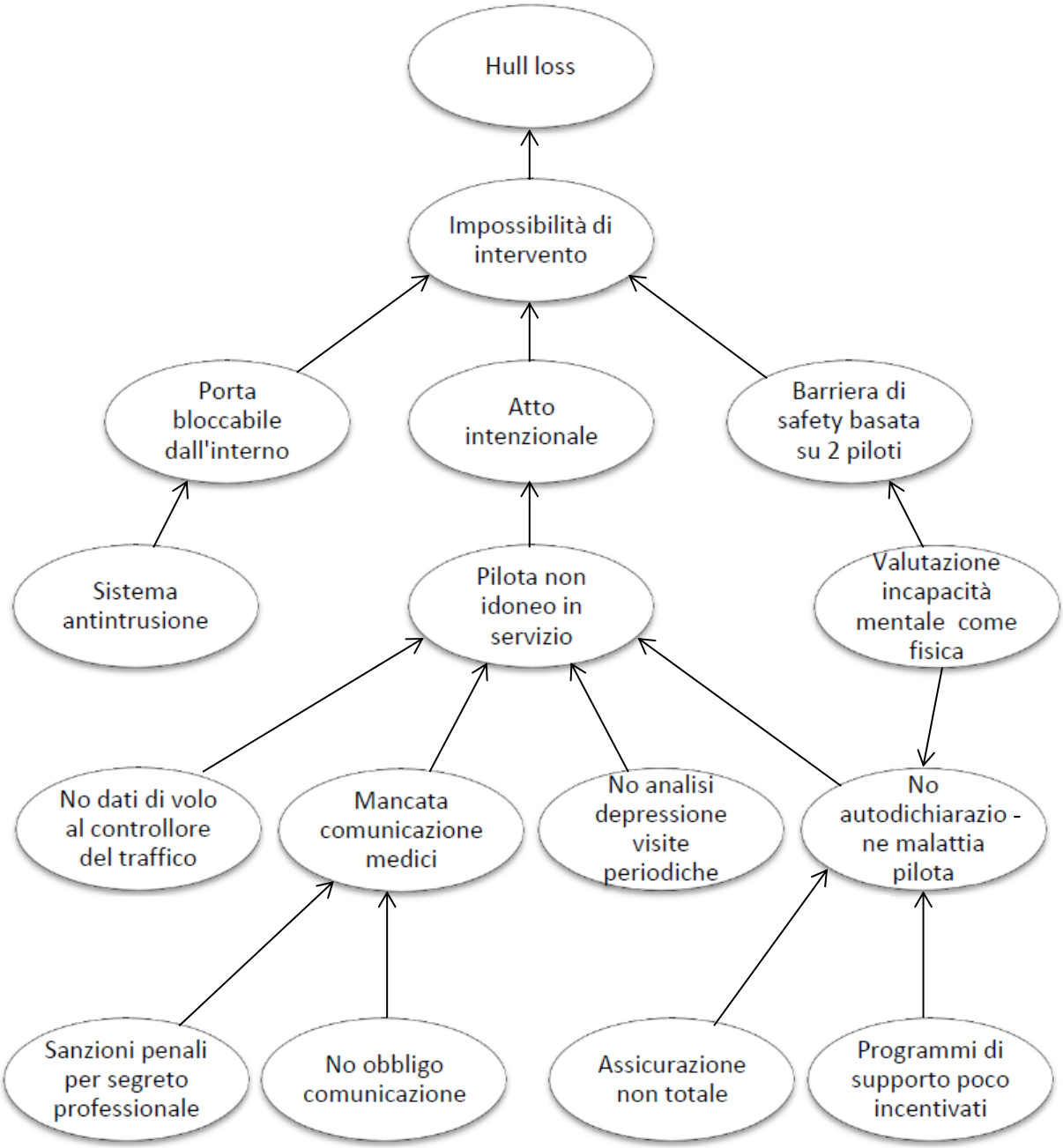

Figura 7.4. *Schema logico integrato (rete Bayesiana) dell'evento*

Provando ora a classificare gli errori verificatisi, notiamo che l'incidente presenta diversi fattori latenti sia a livello di sistema di trasporto aereo che nell'organizzazione aziendale. Un insieme di condizioni, derivanti dalla legislazione nazionale e dalla gestione aziendale, hanno fatto sì che un problema, decisivo per l'idoneità al volo, venisse sottovalutato e non rilevato. I

fattori latenti sono comunque tutti annoverabili alla safety, che hanno portato a delle precondizioni in cui si è verificata l'interferenza con la security.

Figura 7.5. *Modello di Reason per le cause dell'evento*

Le raccomandazioni, emesse da BEA, ricalcano gli errori latenti individuati.

- Necessità di equilibrio tra riservatezza medica e sicurezza pubblica, e quindi di regole chiare per le segnalazioni.
- Definire condizioni di follow-up, per seguire i piloti con episodi pregressi di problemi psicologici e psichici.
- Inclusione di misure per ridurre il rischio socio-economico, derivante dalla perdita di licenza per ragioni mediche.

- Miglior promozione dei programmi di supporto per piloti.

7.4 Considerazioni

A differenza di quanto visto per l'attentato a bordo della Philippine Airlines, in questo caso studio i fallimenti riguardano barriere di safety. Tali difese, però sono risultate in conflitto con altre misure di security. In particolare, i fattori di contrasto sono stati la confidenza sulla presenza di più piloti, come misura contro l'incapacità di uno dei due, e il sistema di chiusura della cabina, per tutelare l'equipaggio da intrusioni non autorizzate. Questa è sicuramente l'interferenza tra safety e security più rilevante, che non essendo stata considerata, ha portato all'incidente. In questo caso un'adeguata analisi integrata, avrebbe potuto prevenire tale occorrenza. Si sarebbe potuto attuare delle misure alternative, come un diverso sistema di chiusura delle porte. A livello teorico si potrebbe anche analizzare l'impiego di sistemi di pilotaggio da remoto, misura già sperimentata in alcuni voli cargo, e che potrebbe essere una misura di sicurezza per entrambi gli ambiti. Per la safety, garantisce il controllo sul velivolo anche in caso di incapacità del pilota, senza richiedere la presenza di altro personale a bordo, poiché è sufficiente predisporre una squadra a terra, pronta ad intervenire in caso di necessità. Per la security, invece, anche in caso di dirottamento potrebbe essere possibile mantenere il controllo sulle operazioni dell'aeromobile, se si inibissero i comandi a bordo. Ovviamente ciò si ripercuoterebbe in modo notevole sulla gestione della cyber security, che coprirebbe un ruolo cruciale, per garantire il corretto funzionamento del sistema. Per questo motivo, un sistema di questo genere vede ancora difficile applicazione nell'aviazione civile.

È per situazioni come questa, vista nel volo Germanwings 9525, che andrebbe implementato un sistema di gestione integrato. Queste interferenze non possono essere rilevate, fintanto che i sistemi vengono trattati in modo separato o fino a quando un inconveniente non manifesta la pericolosità di tale condizione. Come in questo caso infatti, non era prevedibile che un membro dell'equipaggio si chiudesse all'interno della cabina, fino a quando questa misura di security non si è scontrata con un problema di safety, ovvero l'incapacità mentale del pilota. Possiamo dire, in contrapposizione all'altro caso, che le correlazioni di questo tipo, avvengono a livello di cause. I diversi fattori si influenzano l'uno l'altro, creando condizioni pericolose, che concorrono alla generazione di un unico evento finale anomalo. Questo tipo di

interazioni possono essere studiate, con lo scopo di valutare il rischio ad esse correlato. Il modo più adeguato di ridurre questo rischio è proprio tramite la gestione integrata.

L'inchiesta incidentale, condotta da BEA, si concluse con una serie di raccomandazioni mirate a prevenire il ripetersi di situazioni in cui un pilota non idoneo, sia in servizio. Non venne fornita una soluzione alternativa alla questione del sistema di chiusura, anche per la presenza di episodi precedenti in cui un membro dell'equipaggio riusciva a commettere comunque il suicidio, nonostante fossero presenti entrambi i piloti in cabina. Si è preferito perciò concentrarsi sullo sviluppare un miglior approccio per individuare i casi di depressione e stabilire dei metodi condivisi per il loro trattamento.

Conclusioni

Con questo documento abbiamo visto il ruolo della sicurezza in settore complesso come quello del trasporto aereo. Pur essendo già considerato il sistema di trasporto più sicuro, è richiesto uno sforzo notevole per mantenere gli standard elevati ed impedire un degrado della sicurezza, dovuto ad esempio all'aumento del traffico aereo. Un aspetto che può causare la riduzione della sicurezza del sistema, è proprio la correlazione tra safety e security. Questa problematica è stata evidenziata, tramite i casi studio, che hanno esaltato la gravità delle possibili conseguenze dovute all'interferenza.

Le interazioni, tra eventi accidentali ed atti intenzionali, possono essere considerate un fattore dipendente dall'elevata presenza di misure di sicurezza, previste nel sistema. Da una parte questo aspetto viene esaltato, poiché, essendo presenti numerose barriere di diversi ambiti, le probabilità che esse interferiscano tra loro sono maggiori. Dall'altro lato gli effetti diretti di questo fenomeno sono contenuti, proprio grazie ai molteplici strati di difese, che intervengono compensando l'eventuale fallimento di un livello. Questa seconda condizione rappresenta un'arma a doppio taglio però, perché, se le correlazioni non sono accuratamente studiate, possono permanere nel sistema come condizioni latenti e rimanere celate fino a quando non si manifestano con un incidente.

La gestione delle correlazioni risulta perciò essere un processo complesso, che richiede un'analisi supplementare delle valutazioni separate. Proprio per loro natura, safety e security presentano caratteristiche ben diverse e, anche per questo motivo, sono regolamentate da differenti normative. A questo, si aggiunge il fatto che le interferenze possono essere affette da un'elevata imprevedibilità. Ma agli attuali livelli di sicurezza, raggiunti nel sistema di trasporto aereo, non è possibile sottovalutare nessun aspetto. Ne consegue la necessità di sviluppare dei metodi, che consentano di studiare in modo approfondito la problematica, al fine di eliminare anche questa incertezza. In questa senso c'è ancora molto lavoro da fare, e la problematica non potrà definirsi risolta fino a quando non si adotterà la gestione integrata di safety e security come prassi comune, impiegandola sistematicamente ad ogni livello del sistema trasporto aereo. Un obiettivo ambizioso, difficilmente raggiungibile se non guidato in prima linea dalle autorità competenti.

Riferimenti bibliografici

P. C. Cacciabue, I. Oddone, I. Rizzolo (2017). Risk methods for the assessment of security of large structures: the case of an international airport.

Guozheng Song, Faisal Khan, Ming Yang (2018). Probabilistic assessment of integrated safety and security related abnormal events: a case of chemical plants.

Cacciabue, Oddone, Rizzolo (2019). Sicurezza del Trasporto Aereo (Springer Ed.).

David Gillen, William G. Morrison (2015). Aviation security: Costing, pricing, finance and performance.

Galileo Tamasi, Micaela Demichela (2011). Risk assessment techniques for civil aviation security.

Maggiore, Gajetti, Bonifacino (2017). Dal Fattore Umano alla Safety in Aviazione (Esculapio Ed.).

L. Guerra, T. Murino, E. Romano (2008). Airport risk assessment: a probabilistic approach.

Materiale didattico e appunti delle lezioni del corso *Sicurezza nel trasporto e nelle infrastrutture strategiche*.

Siti web

https://www.enac.gov.it/

https://www.icao.int/

https://www.bea.aero/

https://it.wikipedia.org/

https://www.aviation-report.com/

https://www.bazl.admin.ch/

https://europa.eu/

https://ourworldindata.org/

https://www.start.umd.edu/gtd/

https://www.ict.org.il/

https://www.mlit.go.jp/