Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Magistrale in Informatica

Tesi di Laurea

L'IMPORTANZA ED IL RUOLO DELL'HAZARD ANALYSIS IN AMBITO FERROVIARIO E RELATIVA APPLICAZIONE ALL'APPARATO IMR DI RFI

THE IMPORTANCE AND ROLE OF HAZARD ANALYSIS IN THE RAILWAY SECTOR AND ITS APPLICATION TO RFI'S IMR APPARATUS

GIULIA DALLAI

Relatore: *Prof. Andrea Bondavalli*
Correlatore: *Dott. Tommaso Zoppi*

Anno Accademico 2019-2020

Giulia Dallai: *L'importanza ed il ruolo dell'hazard analysis in ambito ferroviario e relativa applicazione all'apparato IMR di RFI,* Corso di Laurea Magistrale in Informatica, © Anno Accademico 2019-2020

INDICE

1 Introduzione 7
  1.1 Scopo della tesi 8
2 Introduzione alla Dependability e agli Standard relativi al settore ferroviario 9
  2.1 SIL - Safety Integrity Level 13
3 L'Hazard Analysis 15
  3.1 Tecniche di Hazard analysis 15
  3.2 L'analisi HAZOP 16
  3.3 Il processo per la valutazione del rischio 19
4 L'apparato IMR (Interfaccia Mobile Remota) 23
  4.1 Apparati centrali 23
  4.2 La manutenzione della linea ferroviaria 24
  4.3 L'apparato IMR 25
  4.4 Architettura IMR 25
    4.4.1 Tablet Operatore 26
    4.4.2 Server IMRG 26
    4.4.3 Server IMRW 27
    4.4.4 Server IMRS 27
  4.5 Procedura di Connessione 27
    4.5.1 Funzionalità del Terminale Operatore 29
    4.5.2 Il piano schematico 31
    4.5.3 Il quadro luminoso 32
  4.6 Schema funzionale 32
5 Hazard analysis dell'Apparato IMR 35
  5.1 Autenticazione Tablet e Scelta Stazione 36
    5.1.1 Rischi individuati 37
  5.2 Login IMR 40
    5.2.1 Rischi individuati 41
  5.3 Visualizzazione Terminale Operatore (TO) 43
    5.3.1 Rischi individuati 45
  5.4 Esecuzione comando AM 47
    5.4.1 Rischi individuati 48
  5.5 Selezione Piano Schematico (PS), Quadro Luminoso (QL), Log 55
    5.5.1 Rischi individuati 57

6 Mitigazioni 59
6.1 Utilizzo di una One Time Password 59
6.2 Utilizzo del protocollo PVS 61
6.3 Direttive comportamentali 63
7 Conclusioni 65

ELENCO DELLE FIGURE

Figura 1 Diagramma EN 50 126 [13] 11
Figura 2 Classificazione SIL [15] 13
Figura 3 Le parole guida utilizzate durante il processo di Hazard Analysis [4] 17
Figura 4 Fase di Esaminazione 18
Figura 5 Il processo per la valutazione dei rischi 20
Figura 6 Tabella per la classificazione delle frequenze [4] 20
Figura 7 Tabella per la classificazione della severità [4] 21
Figura 8 Matrice dei rischi [4] 21
Figura 9 Apparati centrali 24
Figura 10 Architettura IMR 26
Figura 11 Procedura di Connessione 28
Figura 12 Icone del Terminale Operatore 30
Figura 13 Piano schematico stazione di Oderzo 31
Figura 14 Quadro luminoso stazione di Oderzo 32
Figura 15 Schema funzionale Tablet Operatore e AM 33
Figura 16 Schema funzionale IMRW, IMRS, DM e IMRG 33
Figura 17 Sequence Diagram fase Autenticazione Tablet e Scelta Stazione 36
Figura 18 Sequence diagram fase Visualizzazione TO 44
Figura 19 Sezione Hazard Analysis Visualizzazione TO 46
Figura 20 Sezione Hazard Analysis Esecuzione comando AM 54
Figura 21 Sequence diagram Selezione PS, QL, Log 56
Figura 22 Sezione hazard analysis Selezione PS, QL, Log 58
Figura 23 Il ruolo dello Smartphone nell'apparato IMR 60
Figura 24 Sequence diagram Esecuzione comando 61
Figura 25 Protocollo PVS 63

"Contro un attacco esperto non c'è garanzia di difesa, ma contro una difesa esperta non si sa dove attaccare"
— Sun Tzu

1

INTRODUZIONE

L'Information Technology (IT) svolge un ruolo fondamentale nella vita di tutti i giorni, nel modo in cui riusciamo a relazionarci, a lavorare, a vivere la nostra quotidianeità. L'IT permea quasi tutti i nostri comportamenti quotidiani e può essere considerata lo strumento più efficace per la creazione di ricchezza economica da parte delle aziende.
Grazie all'IT infatti le aziende hanno potuto generare vantaggi e sfruttare nuove opportunità. Oggi questi vantaggi e benefici, comprensivi di applicazioni, funzionalità e infrastrutture, sono alla portata di tutti.
Visto l'importante ruolo assunto dall'IT, nasce l'esigenza di preservare i sistemi informatici; a questa necessità fa capo l'*hazard analysis*, o analisi dei rischi, un processo di valutazione delle criticità inerenti un sistema informatico.
Il **rischio** è la potenzialità che un'azione o un'attività porti a una perdita o ad un evento indesiderabile. Quello del rischio è un concetto connesso con le aspettative umane e la loro capacità di predizione/intervento in situazioni non note o incerte. L'uomo nel corso degli anni ha imparato a confrontarsi con il rischio con un atteggiamento di sfida, ricercando sempre più un equilibrio tra razionalizzazione degli eventi e utilizzo dell'intuito. Nel linguaggio comune, rischio è spesso usato come sinonimo di probabilità di una perdita o di un pericolo/minaccia. In generale, ogni indicatore di rischio è proporzionale all'effetto atteso e alla sua probabilità di accadimento. [14]
L'esigenza di iniziare a quantificare i rischi è nata in ambito bancario, infatti fin dal tardo medioevo i banchieri sono abituati a gestire il rischio di credito, ovvero il principale rischio a cui essi sono esposti. I banchieri lombardi che a partire dal 1100 operavano in Francia, Germania ed Inghilterra utilizzavano già efficaci tecniche di mitigazione del rischio di credito, quali ad esempio la richiesta di cessione in pegno di oggetti di valore.[8]
Non è possibile individuare un comportamento umano o un'attività natu-

rale che non venga sottoposta a rischi temporanei o costanti; solamente le scienze pure, come la matematica o la fisica, governate dalle ferree leggi del puro determinismo, non si confrontano con tale concetto.

1.1 SCOPO DELLA TESI

Gli obiettivi proposti nel lavoro di tesi sono quelli di riportare l'importanza dell'*Hazard analysis* in ambito ferroviario e di applicare tale procedura all'apparato Interfaccia Mobile Remota (IMR) di RFI. Tale apparato nasce con lo scopo di migliorare e velocizzare l'esecuzione delle operazioni di manutenzione lungo le linee ferroviarie. Tramite l'IMR deve diventare possibile per un operatore, tramite un tablet, effettuare una serie di operazioni, come impedire il passaggio di treni in una zona della linea ferroviaria, senza recarsi fisicamente in stazione per ottenere l'autorizzazione. Poichè il malfunzionamento di una qualunque delle fasi dell'operazione è critica per la vita dell'operatore e per il funzionamento della linea, tale procedura remota deve essere sicura, quindi eventuali malfunzionamenti devono essere visibili per l'operatore. Grazie alla procedura di hazard analysis è stato possibile evidenziare le principali criticità del sistema in questione e quindi ricercare una soluzione oppurtuna per ognuna di esse.

2

INTRODUZIONE ALLA DEPENDABILITY E AGLI STANDARD RELATIVI AL SETTORE FERROVIARIO

I sistemi informatici complessi, ovvero tutti quei sistemi composti da sottosistemi indipendenti in grado di interagire fra loro, vengono adoperati sempre più frequentemente per svolgere compiti altamente critici, che compromettono la sicurezza e l'incolumità delle persone. Si pensi per esempio ai sistemi di controllo di aerei, delle centrali nucleari o ai sistemi ferroviari. É di fondamentale importanza che tali sistemi adottino delle tecniche in grado di mantenere sempre corrette le funzioni per le quali sono destinati.
La **dependability** è una caratteristica dei sistemi e consiste nella loro capacità di mostrarsi "affidabili" nei confronti degli utilizzatori, tale caratteristica porta gli utilizzatori a potersi "fidare" del sistema stesso e a poterlo quindi utilizzare senza particolari preoccupazioni.[6] La dependability è un concetto che comprende all'interno del suo significato i seguenti attributi:

- Disponibilità (*Availability*): è la prontezza del sistema nell'erogare un servizio corretto; misura la fornitura di servizio corretto, rispetto all'alternanza tra servizio corretto e non corretto.
- Affidabilità (*Reliability*): è la capacità del sistema di erogare un servizio corretto in modo continuo, misura la fornitura continua di un servizio corretto.
- Confidenzialità (Confidentiality): è l'assenza di diffusione non autorizzata di informazioni; misura l'assenza di esposizione non autorizzata di informazione.
- Manutenibilità (*Mantainability*): la capacità del sistema di subire modifiche e riparazioni; misura il tempo necessario per ristabilire un servizio corretto.

- Sicurezza (*Safety*): è l'assenza di conseguenze catastrofiche sull'utente e sull'ambiente circostante.
- Sicurezza (*Security*): è vista come la contemporanea esistenza di availability, confidentiality e integrity. [6]

Ciascuno di questi attributi può essere più o meno importante in base all'applicazione: la disponibilità del servizio è sempre richiesta, anche se può variare sia l'importanza relativa che il livello quantitativo richiesto; la affidabilità, la sicurezza, la confidenzialità e gli altri attributi possono essere richiesti o meno.
Il grado con cui un sistema possiede questi attributi deve essere interpretato in senso probabilistico e non in senso assoluto, deterministico; a causa dell'inevitabile occorrenza dei guasti i sistemi non sono mai totalmente disponibili, affidabili, safe o secure. Per questo gli attributi di dependability possono essere definiti in senso probabilistico così da poterli trattare in modo quantitativo. [6] Lo sviluppo di sistemi dependable richiede l'utilizzo combinato di quattro tipologie di tecniche:

- **Prevenzione dei guasti**: per prevenire l'occorrenza o introduzione di guasti nel sistema;
- **Tolleranza ai guasti**: per erogare un servizio corretto anche in presenza di guasti;
- **Rimozione dei guasti**: per ridurre il numero o la gravità dei guasti;
- **Previsione dei guasti**: per stimare il numero di guasti presenti nel sistema, la loro incidenza futura o le loro probabili conseguenze.[2]

I sistemi informatici forniscono servizi sempre più sofisticati e per questo richiedono standard qualitativi sempre più elevati.
Nel **settore ferroviario** le principali normative che sono state varate in ambito europeo sono le seguenti:

- EN 50126: stabilisce delle linee guida per la realizzazione dell'attività RAMS (Reliability-Availability-Mantainability-Safety) lungo tutto il ciclo di vita di un prodotto ferroviaro. Questa normativa è da ritenersi applicabile ad agni tipo di prodotto destinato ad operare nel settore ferroviario, si tratti di un impianto fisso, di un treno oppure anche solo di un impianto che lo compone. Dato il suo carattere generale, la normativa non dà elementi specifici nè tantomeno esprime requisiti quantitativi. [13]

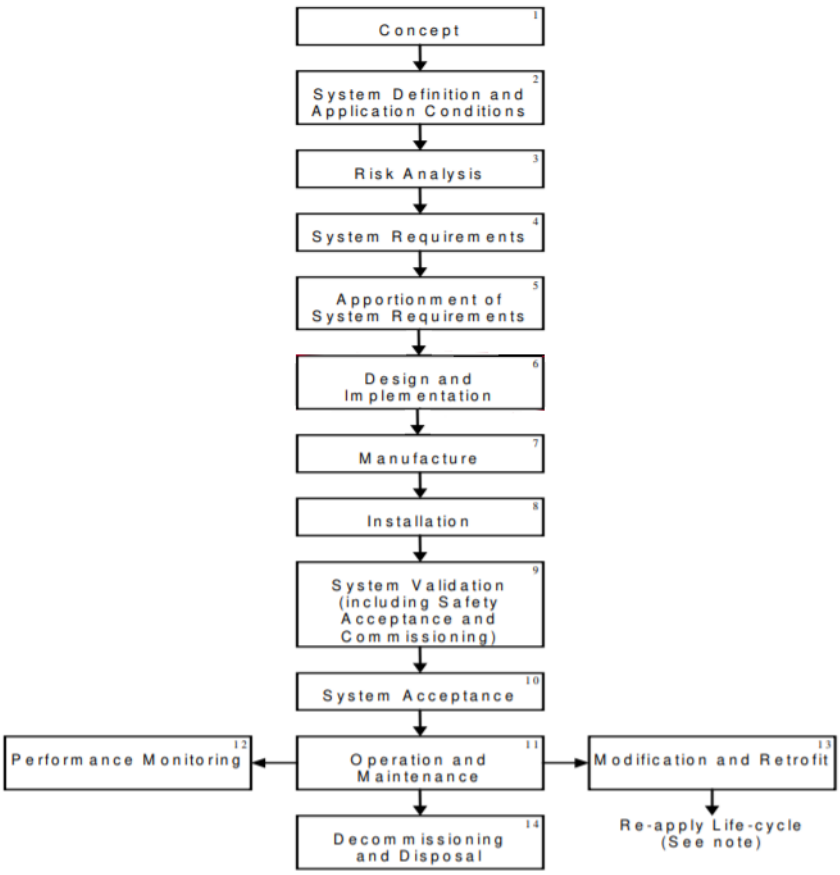


Figura 1: Diagramma EN 50 126 [13]

- EN 50128: relativa allo sviluppo di software per applicazioni di sicurezza. [11]
- EN 50129: inerente allo sviluppo di apparecchiature elettriche/elettroniche di sicurezza per il segnalamento ferroviario.
- EN 50121: riguarda le relazioni tra i sistemi ferroviari ed il mondo esterno, con particolare riguardo alla compatibilità elettromagnetica.
- EN 50155: inerente le condizioni del materiale elettico utilizzato nelle fasi di sviluppo, costruzione e testing.
- EN 50159: affronta invece la sicurezza delle comunicazioni in ambito ferroviario [12].

Nel diagramma sono riportate le fasi del ciclo di vita relative alla normativa EN50126. Le prime fasi hanno come obiettivo quello di definire le

funzioni del sistema, l'interazione con l'ambiente esterno e le interfacce. Inoltre devono essere pianificate le attività di safety e di verifica e validazione. Le normative EN50128 e EN50129 vengono utilizzate in particolare nella fase 6 (Design and implementation): in questa fase viene definita l'architettura dei sottosistemi e inoltre viene affrontato lo sviluppo hardware e software.[11]
Lo standard EN50126 descrive gli elementi chiave che devono essere definiti per gestire la safety di un sistema:

- politica generale sulla safety;
- piano di safety;
- registro degli azzardi;
- controlli interni al sistema;
- sistema per riportare i fallimenti;
- sistema per la gestione delle azioni correttive;
- processo di valutazione dei rischi per individuare gli azzardi.

Tale normativa, come tante altre in diversi ambiti, richiede che prima che il sistema inizi a operare, tutti i rischi siano stati misurati e valutati e che siano considerati tollerabili.[13]
Il rischio è quindi l'unità di misura del sistema di gestione della safety. Misurare un rischio non è semplice, non esiste infatti uno strumento diretto per effettuare tale operazione. E' possibile però utilizzare due approcci indiretti:

- la statistica, per misurare i rischi del passato;
- l'hazard analysis, per predirre i rischi del futuro.

Ovviamente la nostra attenzione si concentra sull'analisi dei rischi, con lo scopo di evidenziare le problematiche a cui un certo sistema può andare incontro.

2.1 SIL - SAFETY INTEGRITY LEVEL

Un'altra normativa che è opportuno riportare è la IEC 61508 (Sicurezza funzionale di sistemi Elettrici/Elettronici/Elettronici Programmabili), applicabile ai più svariati settori industriali, dal settore dell'industria di processo (ad esempio chimico e petrolchimico), ai macchinari, al settore dei trasporti. La norma IEC 61508 definisce quattro livelli di Safety Integrity Level (da SIL1 a SIL4), ciascuno dei quali definisce una misura quantitativa della necessaria riduzione del rischio e quindi il grado di affidabilità che il sistema di sicurezza deve raggiungere per poter garantire tale riduzione.
Nella norma sono definiti i metodi per la determinazione del PFD (Probability of Failure on Demand) o PFH (Probability of Failure per Hour) e del RRF (Risk Reduction Factor), utilizzati durante la classificazione SIL. [15]

SIL	PFD	PFD (power)	RRF
1	0.1–0.01	$10^{-1} – 10^{-2}$	10–100
2	0.01–0.001	$10^{-2} – 10^{-3}$	100–1000
3	0.001–0.0001	$10^{-3} – 10^{-4}$	1000–10,000
4	0.0001–0.00001	$10^{-4} – 10^{-5}$	10,000–100,000

SIL	PFH	PFH (power)	RRF
1	0.00001-0.000001	$10^{-5} – 10^{-6}$	100,000–1,000,000
2	0.000001-0.0000001	$10^{-6} – 10^{-7}$	1,000,000–10,000,000
3	0.0000001-0.00000001	$10^{-7} – 10^{-8}$	10,000,000–100,000,000
4	0.00000001-0.000000001	$10^{-8} – 10^{-9}$	100,000,000–1,000,000,000

Figura 2: Classificazione SIL [15]

3

L'HAZARD ANALYSIS

3.1 TECNICHE DI HAZARD ANALYSIS

La valutazione dei rischi rappresenta il momento fondamentale per la prevenzione delle criticità nelle aziende con lo scopo di individuare e risolvere i problemi che è possibile riscontrare. Esistono molti strumenti e tecniche disponibili per l'identificazione di potenziali pericoli e problemi di operabilità, di seguito sono riportate i più utilizzati: [2]

- **Checklists**: lista di voci che occorre controllare e spuntare per verificare che una determinata serie di operazioni sia stata eseguita correttamente. Si tratta di uno dei metodi più semplici e meno costosi per la valutazione dei rischi, molto utile per rilevare gli errori di progettazione più comuni [3];

- **Fault Modes and Effects Analysis (FMEA)**: analisi eseguita preventivamente e quindi basata su considerazioni teoriche e non sperimentali. Come primo passo viene effettuata la scomposizione del sistema in sottosistemi, per ognuno di essi devono essere elencati tutti i possibili guasti e successivamente le cause e le conseguenze. Negli anni '80 fu usata dalla Ford per ridurre i rischi visto che un modello di automobile, la Pinto, presentava un problema ripetitivo di rottura del serbatoio che causava incendi in caso di incidenti; [1]

- **Fault Tree Analysis (FTA)**: tecnica analitica in cui innanzitutto viene individuato uno stato indesiderato in cui può venire a trovarsi il sistema e in seguito viene effettuata un'analisi per determinare tutti i modi credibili in cui l'evento indesiderato può verificarsi. La FTA ha trovato sempre più occasioni di applicazione, nel mondo manifatturiero come anche più di recente in quello dei servizi, risultando oggi uno dei metodi più semplici ed efficaci nell'analisi dell'affidabilità e sicurezza dei sistemi. [10]

- **Studio "What-if"**: viene condotto utilizzando un approccio del tipo brainstorming; si inizia con l'analizzare pericoli già noti al team di lavoro per arrivare ad altri potenziali scenari incidentali; fra i suoi scopi primari è compresa la stima delle conseguenze del "peggior caso" verificabile. Ha il pregio di poter essere applicata, secondo le esigenze, più o meno dettagliatamente; [3]

- **HAZOP**: esercizio finalizzato all'individuazione di deviazioni dagli intenti di progetto che possono portare ad inconvenienti di sicurezza o di esercizio. Tale procedura, attraverso l'uso di parole guida appositamente create, è in grado di evidenziare le criticità che un sistema può incontrare nel suo ciclo di vita. [4]

Alcune tecniche, come le Checklists e lo Studio "What-If", possono essere utilizzate all'inizio del ciclo di vita del sistema o se non è richiesta un'analisi dettagliata; al contrario, se vogliamo avere informazioni più complete sui pericoli a cui è sottoposto il sistema è opportuno procedere con un'analisi **HAZOP** (**HAZ**ard and **OP**erability analysis).

3.2 L'ANALISI HAZOP

Tale tecnica ha avuto origine da studi di tipo assicurativo, specie su grandi impianti di processo, estendendo la sua applicazione ad ambiti e dimensioni diverse. L'HAZOP mira all'individuazione dei pericoli esistenti nella gestione di un determinato processo lavorativo. Tali pericoli sono identificati e indagati sulla base di deviazioni, siano esse accidentali o meno, di parametri chiave, caratteristici del processo in esame. [3]
L'espressione *hazard analysis* viene sinteticamente utilizzata per indicare un processo che in pratica comprende 4 fasi: [4]

- *Definizione*: in questa fase gli obiettivi e lo scopo dell'analisi devono essere definiti. Questa prima fase è fondamentale per chiarire quali siano i confini del sistema e le sue interfacce con altri sistemi, in modo tale che l'analisi non si discosti in aree irrilevanti rispetto all'obiettivo;

- *Preparazione*: questa fase ha lo scopo di ottenere le informazioni necessarie per effettuare l'analisi e di convertire tali informazioni in un formato adatto. In seguito deve essere riportata una descrizione del progetto contenente tutti i dettagli tecnici e amministrativi necessari. Devono essere fornite informazioni circa le condizioni ambientali in

cui il sistema opererà, qualifiche, abilità ed esperienza del personale operativo e di manutenzione e infine devono essere riportate le problematiche evidenziate in sistemi simili. Non di minore importanza è l'operazione di stima del tempo necessario per condurre l'analisi che deve essere eseguita in questo frangente; infine, devono essere scelte le parole guida più adeguate per condurre l'analisi del sistema, considerando che una parola guida troppo specifica può limitare le idee e la discussione, al contrario una troppo generica potrebbe non focalizzare lo studio in modo efficiente.

Negativo	NOT/NO	Mancata esecuzione della funzione considerata
Modifica quantitativa	MORE	Il valore del dato è al di fuori dell'intervallo consentito (maggiore)
Modifica quantitativa	LESS	Il valore del dato è al di fuori dell'intervallo consentito (minore)
Modifica quantitativa	PART OF	La funzione viene eseguita dal sistema solo in parte
Modifica quantitativa	AS WELL AS	Le impurità presentano simultaneamente l'esecuzione di un'altra operazione
Tempo	EARLY	La funzione viene eseguita in anticipo
Tempo	LATE	La funzione viene eseguita in ritardo
Sostituzione	OTHER THAN	La funzione viene eseguita completamente, ma fornisce un risultato diverso da quello atteso
Ordine o sequenza	Before	Qualcosa è successo troppo presto in una sequenza
Ordine o sequenza	After	Qualcosa è successo troppo tardi in una sequenza

Figura 3: Le parole guida utilizzate durante il processo di Hazard Analysis [4]

- *Esaminazione*: questa è la fase che rappresenta la vera e propria analisi del sistema. Come prima cosa viene diviso il sistema in parti, tale divisione deve essere effettuata in modo pertinente ai fini dell'analisi; in seguito deve essere spiegato il ruolo progettuale della parte in questione, gli elementi pertinenti e le eventuali caratteristiche associate agli elementi identificati. Per ogni parte del sistema devono essere individuate le parole guida appropriate, ovvero quelle che possono dar luce a eventuali criticità. Le parole guida vengono esaminate nel contesto dell'elemento o della caratteristica studiata per rilevare eventuali deviazioni credibili dall'intento progettuale. Qualora venga trovata una deviazione credibile, viene effettuata un'indagine per individuare tutte le cause e le conseguenze. Le deviazioni vengono classificate in base al potenziale impatto e alla loro frequenza di accadimento, come vedremo in seguito. Di

fondamentale importanza è identificare la presenza di meccanismi di protezione e rilevamento della deviazione che possono essere inclusi nella parte selezionata. Questo procedimento viene ripetuto per ogni parte del sistema, per ogni parola guida e per ogni sua interpretazione, al fine di riuscire a individuare tutti i rischi a cui il sistema può andare incontro.
Quando una parte è stata del tutto esaminata, dovrebbe essere contrassegnata come completata.

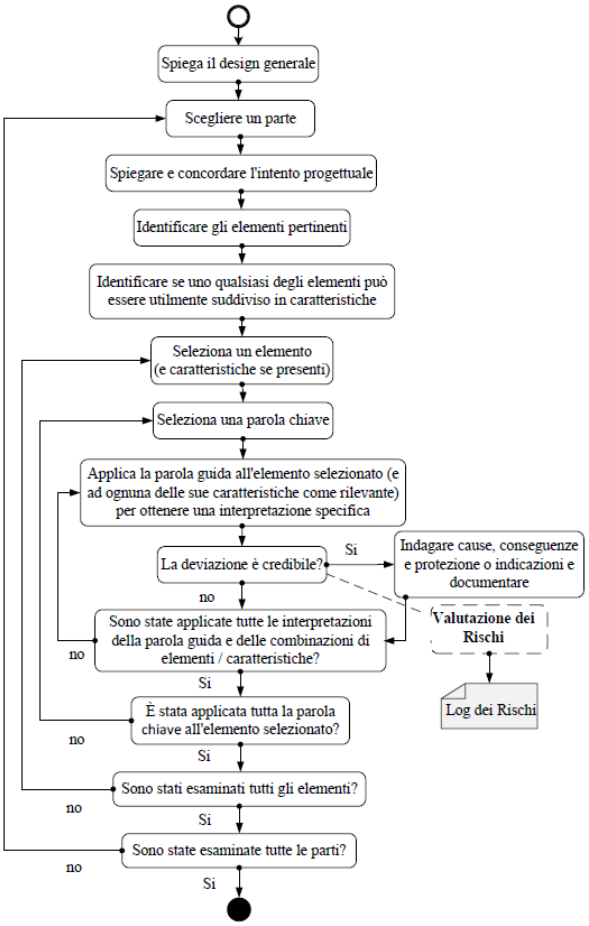


Figura 4: Fase di Esaminazione

- *Documentazione*: per completare l'analisi e ottenere tutti i suoi benefici è opportuno documentarla. Esistono due approcci per effettuare tale procedura: registrazione completa o solo per eccezione. La registrazione completa comporta la registrazione di tutti i risultati. Questo metodo può risultare ingombrante ma sicuramente completo di tutte le informazioni; al contrario, la registrazione delle

eccezioni implica la memorizzazione esclusivamente dei rischi identificati e dei problemi di operabilità. In tal caso la quantità di dati da memorizzare è inferiore e sicuramente la gestione di questi ultimi è più semplice.
Una buona documentazione dovrebbe includere dettagliatamente quanto segue:

- dettagli dei pericoli identificati e problemi di operabilità;
- raccomandazioni per eventuali ulteriori studi su aspetti specifici del progetto utilizzando tecniche diverse, se necessario;
- azioni necessarie per affrontare le problematiche individuate durante lo studio;
- un elenco di tutte le parti considerate nell'analisi, insieme alla motivazione associata all'eventuale esclusione di determinate parti del sistema;
- elenco di tutti i disegni, specifiche, schede tecniche, report, ecc...

Attraverso la registrazione per eccezioni le informazioni sui vari rischi sono descritte in maniera piuttosto concisa, senza riportare informazioni dettagliate.
Nella documentazione ogni azzardo, problema operativo o pericolo, insieme alle proprie eventuali cause, dovrebbe essere registrato come elemento separato e indipendente.
Infine, dovrebbe essere adottato un sistema di numerazione per fare in modo che ogni rischio, problema operativo, mitigazione e raccomandazione venga identificato in maniera univoca. Per garantire il recupero della documentazione, è opportuno che essa venga archiviata.

3.3 IL PROCESSO PER LA VALUTAZIONE DEL RISCHIO

Come precedentemente anticipato nella fase di esaminazione è opportuno effettuare una valutazione del rischio riscontrato. Infatti, secondo la normativa EN 50126, prima che il sistema inizi a operare, è richiesto che tutti i rischi vengano misurati, valutati e considerati tollerabili. [13]
Le attività di valutazione del rischio vengono condotte con lo scopo di quantificare il rischio associato ad ogni pericolo. Per ogni comportamento anomalo individuato viene analizzata la frequenza di occorrenza e la sua

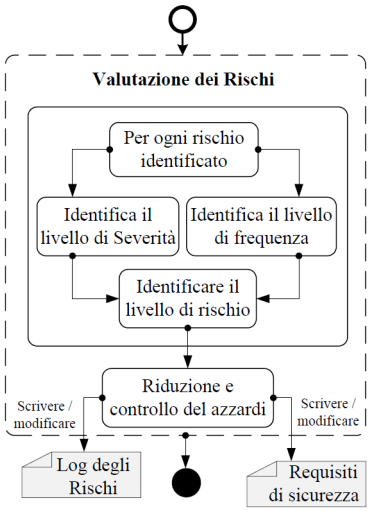


Figura 5: Il processo per la valutazione dei rischi

severità. Dal connubio di queste informazioni è possibile identificare il livello del rischio.

Categoria	Descrizione
Inverosimile	Estremamente improbabile che accada. Si può assumere che la situazione pericolosa possa non presentarsi
Improbabile	Improbabile che accada, ma possibile. Si può assumere che la situazione pericolosa possa presentarsi eccezionalmente
Remoto	Probabile che accada qualche volta nella vita del sistema. Ci si può ragionevolmente aspettare che la situazione pericolosa si presenti qualche volta
Occasionale	Probabile che accada parecchie volte. Ci si può aspettare che la situazione pericolosa si presenti parecchie volte
Probabile	Accadrà parecchie volte. Ci si può aspettare che la situazione pericolosa si presenti spesso
Frequente	Probabile che accada frequentemente. La situazione pericolosa si presenterà continuamente

Figura 6: Tabella per la classificazione delle frequenze [4]

Quest'ultimo può essere classificato come:

- trascurabile
- tollerabile
- indesiderabile
- intollerabile.

Categoria	Conseguenze	Malfunzionamenti del servizio
Catastrofico	Il quadro della situazione presentato agli operatori contiene informazioni incorrette e fornisce un supporto fuorviante per le decisioni	Il sistema riconosce erroneamente alcuni eventi e produce un quadro della situazione completamente diverso dalla realtà
Critico	Il quadro della situazione non è presentato agli operatori e nessuna azione decisionale può essere intrapresa	Il sistema subisce una perdita di dati rilevanti per cui non riesce a produrre un quadro della situazione
Marginale	Il sistema fornisce un supporto non completo ma sufficiente per la gestione della situazione	Il sistema non riconosce tutti gli eventi e produce un quadro della situazione incompleto ma consistente
Insignificante	Il sistema garantisce le sue principali funzionalità correttamente	Il sistema subisce una parziale perdita di dati rilevanti, ma riesce comunque a ricostruire correttamente un quadro della situazione completo e consistente

Figura 7: Tabella per la classificazione della severità [4]

Qualora il livello del rischio sia trascurabile o tollerabile non è necessario individuare un'opportuna mitigazione, in quanto il verificarsi del rischio non viene ritenuto pericoloso nei confronti del sistema, ugualmente se l'incombensa del pericolo è altamente improbabile. Negli altri casi l'analisi procede con la ricerca dell'opportuna soluzione che avrà come scopo o ridurre la severità del rischio oppure la sua frequenza di occorrenza.

FREQUENZA DI ACCADIMENTO	LIVELLO DI RISCHIO			
Frequente	Indesiderabile	Intollerabile	Intollerabile	Intollerabile
Probabile	Tollerabile	Indesiderabile	Intollerabile	Intollerabile
Occasionale	Tollerabile	Indesiderabile	Indesiderabile	Indesiderabile
Remoto	Trascurabile	Tollerabile	Indesiderabile	Indesiderabile
Improbabile	Trascurabile	Trascurabile	Tollerabile	Tollerabile
Inverosimile	Trascurabile	Trascurabile	Trascurabile	Trascurabile
	Insignificante	*Marginale*	*Critico*	*Catastrofico*
	LIVELLO DI SEVERITA'			

Figura 8: Matrice dei rischi [4]

4

L'APPARATO IMR (INTERFACCIA MOBILE REMOTA)

L'apparato IMR di RFI nasce con lo scopo di migliorare e velocizzare l'esecuzione delle operazioni di manutenzione lungo le varie linee ferroviarie; tramite questo apparato molte operazioni vengono remotizzate, dando la possibilità all'operatore, tramite il tablet, di eseguire una serie di comandi senza recarsi fisicamente in stazione.

4.1 APPARATI CENTRALI

Per assegnare a ciascun treno il percorso previsto nelle stazioni, nei bivi o nelle altre località di servizio, è necessario predisporre gli scambi nella posizione voluta, assicurarsi che il percorso del treno non abbia interferenze con il percorso di altri treni e che sia libero nel momento programmato. Queste condizioni si concretizzano attraverso impianti tecnologici di varie generazioni: gli Apparati Centrali. Scopo degli Apparati Centrali di una tratta, a prescindere dalla tecnologia utilizzata, è garantire la movimentazione in sicurezza dei treni, sia in stazione che durante il percorso.
L'**apparato centrale elettrico a itinerari** (ACEI) realizza l'itinerario in sicurezza attraverso un unico comando impartito mediante un pulsante o una tastiera dal DM (Dirigente Movimento). Alcuni di questi apparati sono comandabili a distanza e quindi rendono possibile la gestione di più stazioni o di una intera linea contemporaneamente.
L'**apparato centrale computerizzato** (ACC) rappresenta l'evoluzione tecnologica degli Apparati Centrali realizzati con tecnologia tradizionale elettromeccanica, come l'ACEI. Con l'introduzione degli apparati ACC infatti le apparecchiature elettromeccaniche vengono sostituite con analoghi dispositivi elettronici, realizzati con componenti sia hardware che software, in grado comunque di garantire i medesimi livelli di sicurezza. Attraverso l'ACC vengono introdotti adeguati strumenti di diagnostica automatizzata che permettono al personale della manutenzione di ef-

Figura 9: Apparati centrali

fettuare le operazioni correttive necessarie in caso di guasto in tempi notevolmente ridotti rispetto alla soluzione elettromeccanica utilizzata precedentemente. [5]

4.2 LA MANUTENZIONE DELLA LINEA FERROVIARIA

Prima di introdurre la descrizione dell'apparato IMR, è opportuno delineare come opera il sistema RFI di Manutenzione della Linea.
Ogni stazione ferroviaria può essere considerata divisa in zone, ciascuna rappresentante una specifica sezione: la loro visualizzazione in una singola immagine viene detta sinottico.
Ogni zona può essere considerata indipendente dalle altre zone confinanti, infatti, qualora si renda necessario un intervento di manutenzione, è possibile impedire il passaggio dei treni esclusivamente in quella data sezione. Tale operazione viene gestita tramite l'armadio chiavi di zona, ovvero un pannello contenente tutte le chiavi delle zone. Una chiave non inserita nel pannello indica la non agibilità della zona per qualunque operazione che non sia di manutenzione.
Ad esempio, supponiamo che sia necessario effettuare operazioni di manutenzione nella zona x, l'operatore si reca all'armadio chiavi di zona, prende la chiave x, la sfila dal pannello e la tiene con sè fino alla fine delle operazioni di manutenzione. Una volta concluse tali operazioni, l'operatore torna in stazione e ripone la chiave nell'armadio chiavi di zona.
Il problema ricorrente è che l'armadio spesso è lontano dal luogo in cui deve essere eseguita la manutenzione, quindi, all'operatore occorre spesso troppo tempo per prendere la chiave e riporla.
Di seguito è riportata la procedura completa per la rimozione di una

chiave dall'armadio:

1. chiedere l'autorizzazione al guardiano dell'armadio;
2. fare una mezza rotazione della chiave sull'armadio;
3. chiamare l'autorità centrale per chiedere l'autorizzazione;
4. staccare la chiave e iniziare le operazioni di manutenzione[9].

4.3 L'APPARATO IMR

L'apparato IMR nasce con lo scopo di evitare che l'operatore debba andare fisicamente all'armadio chiavi di zona a prelevare la chiave necessaria per effettuare le operazioni di manutenzione.
RFI vuole fare in modo che il sistema di terra ACEI/ACC comunichi con il nuovo dispositivo IMR. La funzione di questo apparato è quella di fornire connettività all'ACEI/ACC che è attualmente isolato. Il tablet comunicherà quindi con il dispositivo IMR e quest'ultimo inoltrerà i comandi agli apparati ACEI/ACC.
Dato che il malfunzionamento di una qualunque operazione è critico per la vita dell'operatore e per il corretto funzionamento della linea, tale procedura remota deve essere eseguita in completa sicurezza ed eventuali malfunzionamenti devono essere visibili per l'operatore. A tale scopo è opportuno procedere con una dettagliata analisi dei rischi.

4.4 ARCHITETTURA IMR

L' architettura Terra-Tablet dell'apparato IMR evidenzia due zone distinte:

- un'area non sicura, comprendente il Tablet e i server IMRG e IMRW, potenzialmente esposti a minacce dannose e che non sono costruiti per soddisfare qualsiasi vincolo di sicurezza;
- un'area sicura, comprendente il server locale IMRS e gli enti di stazione. Tutte le azioni che avvengono in tale zona funzionano in conformità con il SIL con cui sono state certificate, con una probabilità di guasti catastrofici ragionevolmente bassa.

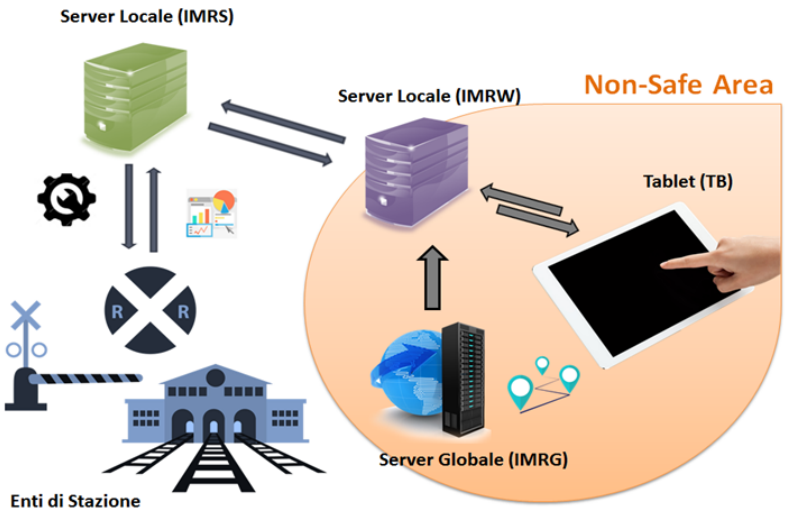


Figura 10: Architettura IMR

4.4.1 *Tablet Operatore*

Ogni addetto AM viene dotato di un tablet TB commerciale per consentire la remotizzazione delle operazioni che richiederebbero l'accesso fisico all'armadio chiavi di zona.
Come evidenziato dall'immagine, il tablet si trova nell'area non sicura e pertanto le azioni eseguite devono essere rigorosamente regolamentate per evitare problemi di safety. Il dispositivo mobile esegue una Web App tramite la quale il manutentore potrà comunicare con l'apparato di terra e potrà inviare comandi e visualizzare lo stato della linea e degli enti.

4.4.2 *Server IMRG*

Tale componente si trova nell'area non sicura, è un server generico senza nessun vincolo di safety o security. Le due uniche funzioni di IMRG sono:

- effettuare un reindirizzamento iniziale dell'AM all'IMRW corretto in base alla stazione che l'AM seleziona,
- fungere da repository condivisa delle chiavi pubbliche degli agenti di manutenzione.

4.4.3 *Server IMRW*

Tale componente, come i due appena descritti, si trova nella zona non sicura dell'architettura. Il ruolo del server è quello di esporre i servizi web che possono essere chiamati remotamente dagli utenti e di assemblare le pagine web sulla base dei dati forniti da IMRS.

4.4.4 *Server IMRS*

Questo server sicuro gestisce, controlla, valida e verifica le interazioni tra l'operatore e gli apparati computerizzati di stazione. Tale componente è progettato, sviluppato e certificato SIL4, si trova infatti nella zona sicura. Le principali funzioni sono di seguito elencate:

- gestire l'autenticazione,
- controllare i comandi inviati dall'AM e comunicare con gli attuatori
- memorizzare dati critici
- comunicare con l'IMRW, fornendogli i dati necessari all'assemblaggio delle pagine web necessarie.

4.5 PROCEDURA DI CONNESSIONE

Di seguito è riportata la procedura di connessione del tablet:

1. l'agente di manutenzione (AM), dopo aver acceso il Tablet ed aperto la Web App, specifica la stazione in cui sta operando;

2. il Tablet chiede al server globale IMRG l'indirizzo del server locale IMRW relativo alla stazione in cui l'AM deve eseguire le operazioni di manutenzione;

3. una volta che l'AM ottiene l'indirizzo del server di stazione, viene stabilita automaticamente una connessione punto-punto diretta con IMRW;

4. l'AM immette le informazioni per l'autenticazione sul server locale: qualcosa che sa (la password) e qualcosa che possiede (la chiave privata);

5. la coppia unsername-password viene crittografata utilizzando la chiave privata e inviata al server locale IMRW, che la reinoltra al server sicuro IMRS, assieme all'elenco delle chiavi pubbliche memorizzate su IMRG;

6. l'autenticazione viene interamente eseguita su IMRS;

7. se la fase di autenticazione è andata a buon fine, verrà inviata la schermata del Terminale Operatore sul Tablet.

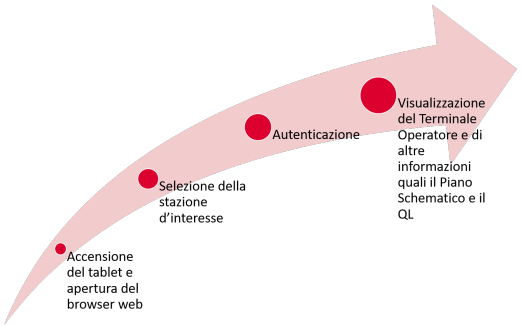


Figura 11: Procedura di Connessione

4.5.1 *Funzionalità del Terminale Operatore*

Il Terminale Operatore (TO) è lo strumento attraverso il quale un operatore è in grado di comunicare con l'apparato centrale ACC/ACEI, inoltrando comandi e ricevendo informazioni utili sullo stato del sistema. Dal TO devono essere attivabili principalmente le seguenti funzioni:

- Funzioni di Movimento (formazione itinerari, formazione istradamenti, etc);
- Funzioni di Ente (manovra deviatoio, esclusione ente, soccorsi, etc);
- Funzioni di Soccorso mirate per i Movimenti;
- Funzioni per la gestione delle Anormalità e degli Allarmi;
- Funzioni per la messaggistica e la modulistica.

A ciascuna categoria di funzioni è associato uno specifico menù, a cui corrisponde un sottomenù, più o meno articolato a seconda del tipo di funzione. Al fine di rendere più immediata possibile la scelta delle funzioni da eseguire, l'accesso ai menù è possibile attraverso icone che determinano l'apertura delle maschere corrispondenti.
Nello specifico, le icone presenti nella schermata Terminale Operatore rappresentano i seguenti enti:

- DV - Deviatoio
- SCF - Scarpa Fermacarri
- SE - Segnale Alto
- TCH - Posto a Terra
- CDB - Circuito di Binario di Stazione
- CDBL - Corcuito di Binario di Linea
- SB - Segnale Basso
- PL - Passaggio a Livello di Stazione
- PLL - Passaggio a Livello di Linea
- LINEA - Punto di Linea

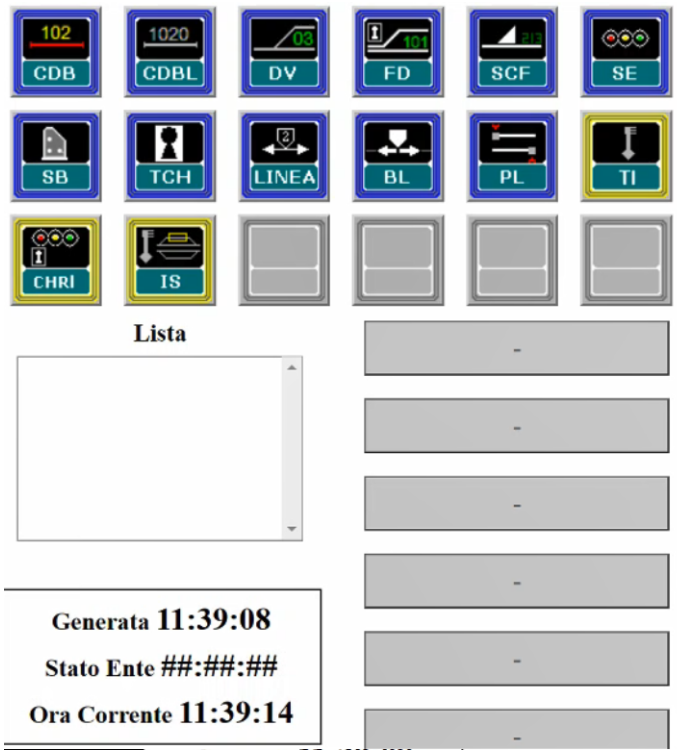


Figura 12: Icone del Terminale Operatore

- BL - Inversione di Blocco
- BLO - Blocco Semplice Binario
- AVV - Segnale di Avviso
- FD - Fermadeviatoio
- CHRl - Chiave Rallentamento Segnale Alto
- TI - Chiave Titolare interruzione
- FS - Fuori Servizio di Linea

Attraverso le icone corrispondenti ai vari enti sarà possibile eseguire una vastità di comandi invocabili dall'operatore tramite IMR.[9]
Quindi, le icone sono riportate in alto a sinistra e i relativi sottomenù vengono eventualmente generati dopo aver cliccato sul simbolo specifico. La modalità d'inoltro del comando può essere differenziata, infatti per alcuni comandi è richiesta la pressione dei tasti o - INVIO per confermare l'esecuzione, mentre altre volte, per i comandi critici, il comando deve essere autorizzato dal dirigente di movimento (DM) per diventare effettivo.

Nella sezione destra della schermata è possibile visualizzare una porzione del quadro luminoso relativa alla zona in cui l'agente di manutenzione sta effettuando le operazioni necessarie.
Nella schermata del Terminale Operatore viene riportata l'ora corrente insieme all'ora in cui è stato generato il quadro luminoso e lo stato dell'ente. Il quadro luminoso viene aggiornato periodicamente e l'ora dell'ultimo aggiornamento viene rappresentata in modo tale che l'operatore, confrontando l'ora corrente con l'ora in cui è stato generato il quadro luminoso, possa capire quanto le informazioni riportate siano attendibili.
Oltre al Terminale Operatore, tramite dei pulsanti riportati in alto a destra, è possibile accedere anche alla **schermata di Log** che offre informazioni sulle ultime operazioni eseguite, al **Piano schematico** e al **Quadro luminoso**, queste due schermate offrono ulteriori informazioni sullo stato del sistema.

4.5.2 *Il piano schematico*

Il **piano schematico** rappresenta senza il rispetto delle proporzioni la topografia di una stazione e riporta con un'apposita simbologia tutti gli enti di piazzale, sia relativi all'armamento che all'impianto di segnalamento, questi ultimi opportunamente numerati, nonché altri elementi essenziali a caratterizzare la stazione per le esigenze della circolazione (fabbricato viaggiatori, marciapiedi, sottopassi pedonali, attraversamenti stradali, eventuali gallerie ecc.)

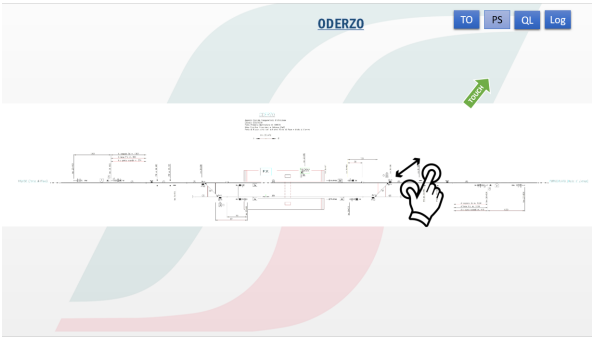


Figura 13: Piano schematico stazione di Oderzo

4.5.3 *Il quadro luminoso*

Il **quadro luminoso** prende il suo nome dalla possibilità che gli è precipua di cambiare aspetto in alcune parti per indicare all'operatore la situazione degli itinerari dei treni, degli instradamenti delle manovre, della disposizione dei segnali, della posizione dei deviatori, dell'occupazione dei binari e quant'altro sia necessario per garantire regolarità e sicurezza all'interno di una stazione ferroviaria. Questi controlli vengono offerti da lampadine poste dietro il quadro stesso che cambiano aspetto (acceso-spento) e attraverso filtri colorati rappresentano la situazione (SIL4) che si presenta nel piazzale della stazione. [7]

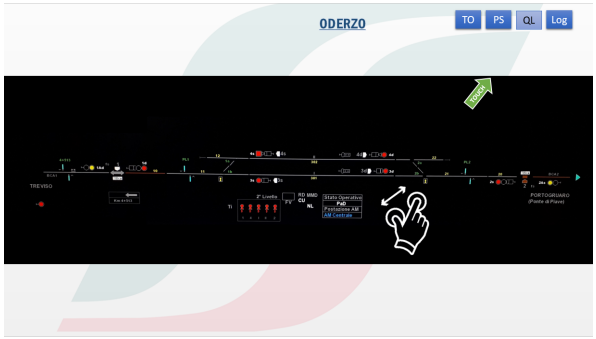


Figura 14: Quadro luminoso stazione di Oderzo

4.6 SCHEMA FUNZIONALE

Per riuscire a comprendere a pieno tutti i compiti e le operazioni che devono essere effettuate dai componenti presenti nell'apparato IMR è stato necessario utilizzare uno schema funzionale. Tale schema descrive graficamente tutti gli attori del sistema e i rispettivi ruoli: in verde sono riportati i componenti, in rosso i blocchi che descrivono le operazioni critiche e in blu i blocchi che descrivono le operazioni non critiche.

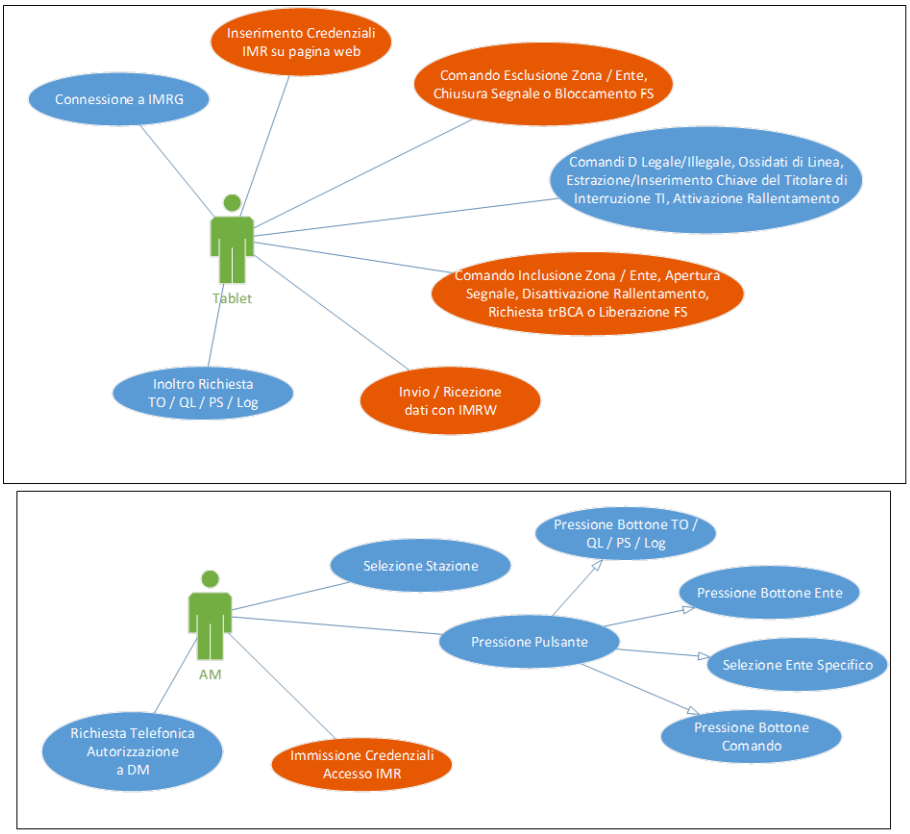


Figura 15: Schema funzionale Tablet Operatore e AM

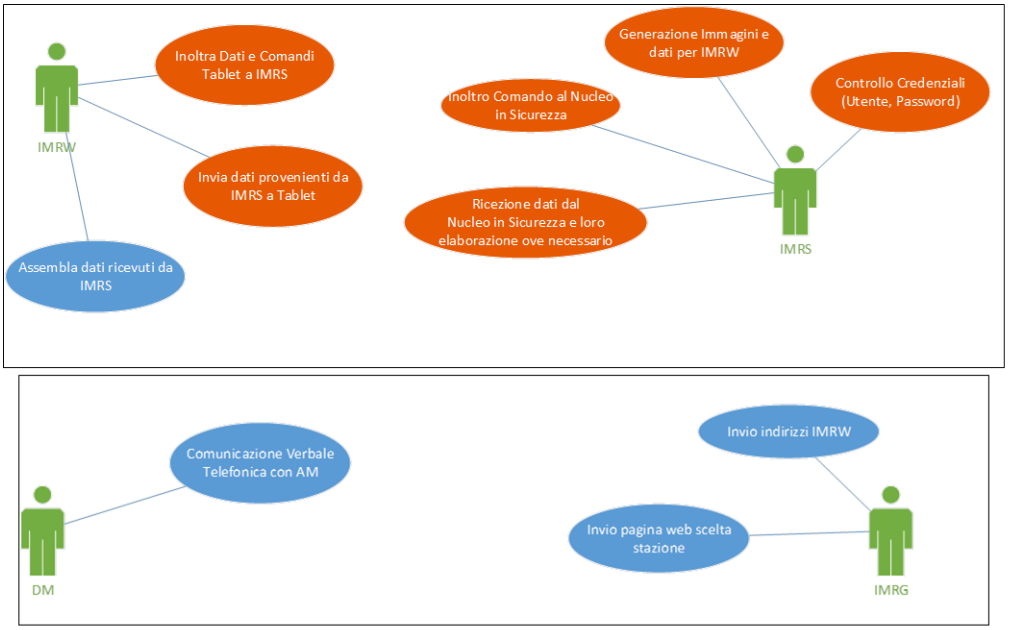


Figura 16: Schema funzionale IMRW, IMRS, DM e IMRG

5

HAZARD ANALYSIS DELL'APPARATO IMR

In questo capitolo viene riportata l'analisi dei rischi vera e propria. Sono state studiate le situazioni pericolose e i rischi associati e per ognuna di esse sono state descritte le relative cause e conseguenze. Come suggerito dalla tecnica HAZOP, il sistema viene suddiviso in più parti e per ognuna di esse viene innanzitutto definito l'intento progettuale.
In seguito vengono selezionati gli elementi delle parti e per ognuno di essi vengono applicate le parole guida elencate nei capitoli precedenti in ogni loro interpretazione.
Per ogni rischio evidenziato verranno riportate la frequenza di occorrenza e la severità dell'azzardo; dall'unione di queste due informazioni verrà ricavata la valutazione dell'azzardo in questione. Se il livello di rischio è trascurabile o tollerabile non sarà necessario individuare la mitigazione. Al contrario, se il livello del rischio è indesiderabile o intollerabile, verrà riportato un appropriato meccanismo di protezione o delle indicazioni atte a risolvere la problematica rilevata.
Una volta che verranno applicate le interpretazioni di tutte le parole guida a tutti gli elementi progettuali, la sezione sarà contrassegnata come completata e si passerà ad esaminare le parti successive.
Tutte le informazioni relative all'Hazard analysis sono riportate in un file excel con lo scopo di tener traccia di tutte le cause, conseguenze e mitigazioni rilevate. In tale file excel ogni azzardo viene contrassegnato in maniera univoca da un id in modo tale da riuscire a orientarsi nella tabella. Nel seguente capitolo, per semplicità, il sequence diagram del sistema è stato suddiviso in cinque sezioni e per ognuna di essere sono stati riportati i principali rischi individuati durante l'analisi.

5.1 AUTENTICAZIONE TABLET E SCELTA STAZIONE

La prima parte del sistema analizzata è quella relativa all'autenticazione sul Tablet e alla selezione della stazione d'interesse da parte dell'addetto alla manutenzione (AM).

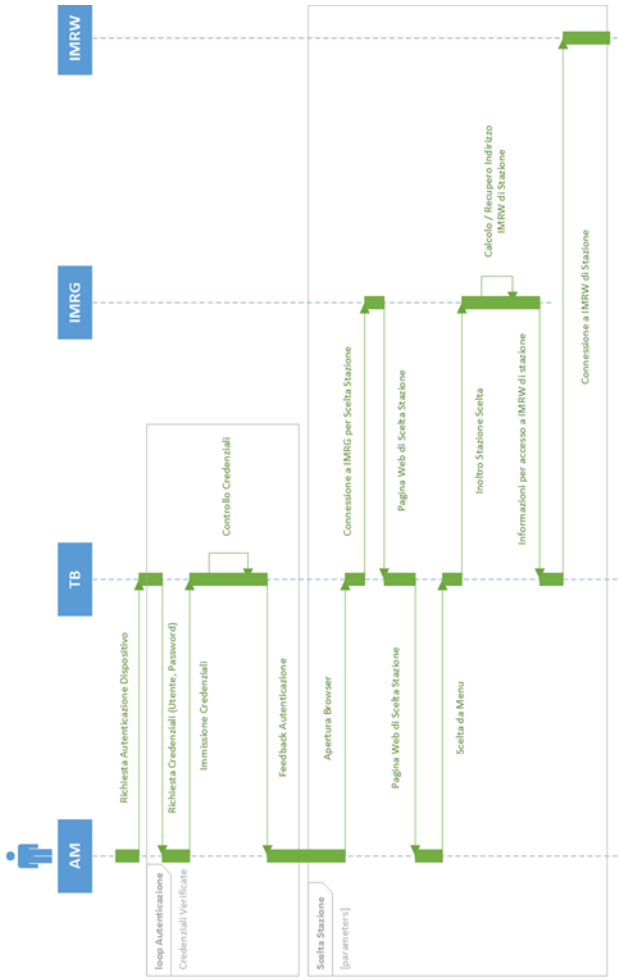


Figura 17: Sequence Diagram fase Autenticazione Tablet e Scelta Stazione

Durante questa fase i componenti attivi sono:

- Addetto alla manutenzione;
- Tablet;
- Server IMRG;
- Server IRMW.

Come viene evidenziato dal sequence diagram questa sezione può essere divisa in due sottosezioni:

- loop autenticazione;
- scelta stazione.

L'autenticazione al dispositivo è la prima operazione che l'AM deve effettuare, durante questa fase le credenziali vengono verificate direttamente dal Tablet. Il server IMRG sarà presente solo in questa fase e nella successiva, in quanto il suo unico ruolo è quello di reindirizzare la connessione verso il server IRM locale e di memorizzare le chiavi pubbliche dell'AM. La reindirizzazione all'IMRW avviene immediatamente dopo la scelta della stazione da parte dell'AM.

5.1.1 *Rischi individuati*

Durante l'analisi di questa fase sono stati individuati vari rischi mediante l'utilizzo delle parole guida. Tale analisi ha evidenziato quasi tutti rischi *tollerabili*, infatti molto spesso la severità dei suddetti rischi è stata classificata come *insignificante*, in quanto gli azzardi non comportano problemi per la safety, tra i quali:

- a causa di un attacco esterno o di un errore accidentale del sistema IMRG, il Tablet potrebbe non ricevere la pagina Web per scegliere la stazione e quindi l'AM potrebbe non riuscire a effettuare le operazioni di manutenzione;
- a causa di un attacco esterno o di un errore di rete, la pagina Web per scegliere la stazione potrebbe essere ricevuta dal Tablet con eccessivo ritardo e l'AM dovrebbe attendere prima di poter selezionare la stazione desiderata;
- a causa di un attacco esterno o di un errore accidentale di IMRG, potrebbe non venir inviato l'indirizzo relativo all'IMRW al Tablet da parte del server IMRG che quindi non sarebbe in grado di connettersi al server relativo alla stazione in oggetto e non sarebbe possibile avviare il lavoro;
- a causa di un attacco esterno o di un errore accidentale del sistema IMRG, potrebbe venir inviato con eccessivo ritardo l'indirizzo relativo all'IMRW al Tablet da parte del server IMRG; senza l'utilizzo di

un protocollo adeguato si può perdere traccia dei messaggi inviati e ricevuti in ritardo. Questo rallenta il lavoro dell'AM;

- a causa di un attacco esterno o di un errore accidentale del sistema IMRG, potrebbe venir inviato al Tablet un indirizzo relativo al server IMRW sbagliato, quindi il Tablet non riuscirebbe a connettersi al server relativo alla stazione in oggetto e non sarà possibile avviare il lavoro;

- a causa di un errore umano, o del touchscreen del Tablet, potrebbe venir selezionata la stazione sbagliata;

- a causa di un attacco esterno potrebbe venir recapitata dall'AM una lista di stazioni parziale e potrebbe non includere la stazione obiettivo; l'AM non sarebbe così in grado di autenticarsi al server locale ed eseguire le sue mansioni;

- a causa di un errore accidentale del server IMRG, di un attacco esterno o di un errore di rete generico, il Tablet potrebbe non riuscire a contattare il server IMRG. In tal caso la stazione non potrebbe essere selezionata.

Di seguito sono invece riportati i rischi *intollerabili* individuati in questa sezione:

- un attaccante potrebbe creare un messaggio per il Tablet oppure alterarne uno già esistente con lo scopo di indirizzare il Tablet verso un server IMRW diverso da quello relativo alla stazione in oggetto. Il Tablet quindi verrebbe reindirizzato su un server che potrebbe offrire un'interfaccia simile a quella attesa, ciò potrebbe indurre l'AM a immettere le sue credenziali. Il server dell'attaccante potrebbe funzionare da man-in-the middle tra l'AM ed il vero server;

- un attaccante potrebbe inviare al Tablet una pagina web per scegliere la stazione diversa da quella originale per influire negativamente sul sistema (creando un nuovo messaggio oppure alterando uno già esistente). In questo modo il Tablet quindi verrebbe reindirizzato su un server che potrebbe offrire un'interfaccia simile a quella attesa, ciò potrebbe indurre l'AM a immettere le sue credenziali. L'attaccante in tal caso verrebbe a conoscenza di informazioni riservate che potrebbe utilizzare al fine di danneggiare il sistema;

- un attaccante potrebbe far connettere il Tablet ad un server che replica il comportamento di IMRG es. Tramite social engineering. L'AM verrebbe reindirizzato su un server che potrebbe offrire un'interfaccia simile a quella attesa, ciò potrebbe indurre l'AM a condividere alcune informazioni personali come le credenziali per l'accesso. A questo punto, il server dell'attaccante potrebbe funzionare da man-in-the middle tra l'AM ed il vero server.

Nella seguente immagine è presente una sezione del file di log relativo alla fase in questione:

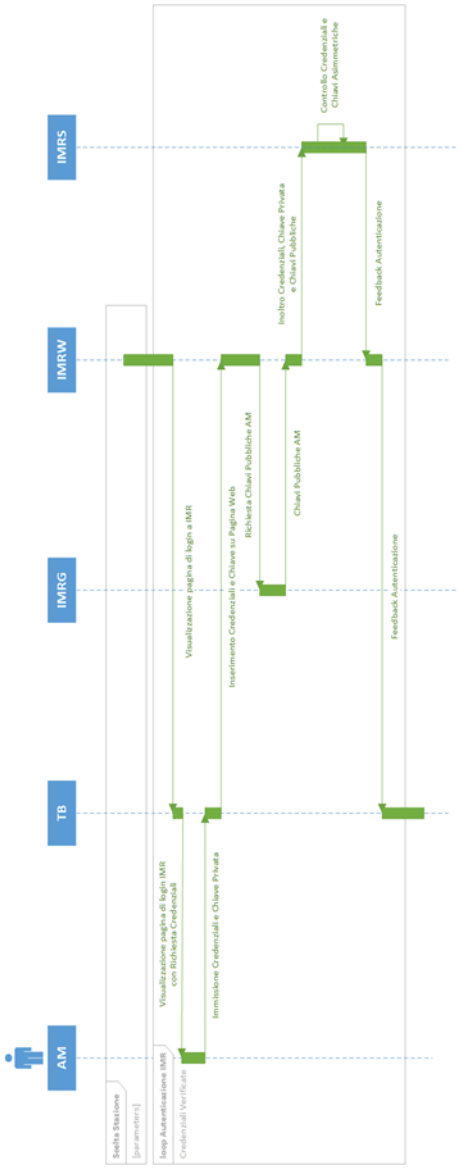
Comp.	Funzionalità	Hazop	Hazard potenziale	Cause	Conseguenze	Frequenza pre-mitigazione	Severità pre-mitigazione	Rischio pre-mitigazione
AM	Selezione Stazione	NOT/NO	Stazione non selezionata	Errore dell'AM	non si avvia la configurazione - non impatta la safety	Probabile	Insignificante	Tollerabile
		NOT/NO	Stazione non selezionata	Errore del tablet (e.g., schermo bloccato).	non si avvia la configurazione - non impatta la safety	Probabile	Insignificante	Tollerabile
		MORE	Seleziona due o più stazioni	Duplicazione e modifica dell'input al tablet.	Il server safe non permette che siano selezionate piu di una stazione. L'output all'AM visualizza il nome della stazione cui è connesso.	Occasionale	Insignificante	Tollerabile
		LESS	N/A	-	-	-	-	-
		PART OF	Viene recapitata all'AM una lista di stazioni da cui scegliere che è parziale e potrebbe non includere la stazione obiettivo.	L'attaccante vuole impedire che il manutentore riesca ad autenticarsi al sistema	L'AM non è in grado di autenticarsi al server locale IMR ed eseguire le sue mansioni.	Probabile	Insignificante	Tollerabile
		PART OF	Viene visualizzata dall'AM una lista di stazioni da cui scegliere che è parziale e potrebbe non includere la stazione obiettivo.	Fallimento della comunicazione, dell'elaborazione dei messaggi o della visualizzazione dati.	L'AM non è in grado di autenticarsi al server locale IMR ed eseguire le sue mansioni.	Probabile	Insignificante	Tollerabile
		EARLY	N/A	-	-	-	-	-
		LATE	N/A	-	-	-	-	-
		OTHER THAN	La stazione viene selezionata, ma non si visualizza l'output sul tablet	Errore del tablet (errore di visualizzazione)	L'AM non avvia il lavoro in assenza di notifica di connessione alla stazione. Non impatta la safety.	Occasionale	Insignificante	Tollerabile
		OTHER THAN	La stazione viene selezionata, ma si visualizza come output sul tablet una stazione differente	Errore del tablet (errore di visualizzazione)	Il L'AM non avvia il lavoro in assenza di notifica di connessione alla stazione corretta.	Remoto	Insignificante	Trascurabile
		OTHER THAN	La stazione viene selezionata, ma il reindirizzamento avviene su un server diverso dagli IMRW locali autorizzati	L'attaccante vuole reindirizzare l'AM su un altro server allo scopo di ottenere credenziali o altre informazioni	L'AM viene reindirizzato su un server che potrebbe offrire una interfaccia simile a quella attesa, e potrebbe indurre l'AM a condividere alcune informazioni personali come le credenziali per l'accesso.	Occasionale	Insignificante	Tollerabile
		OTHER THAN	La stazione viene selezionata, ma il reindirizzamento sull'IMRW locale in oggetto non si completa con successo	L'attaccante vuole impedire che il manutentore riesca ad autenticarsi al sistema	L'AM non è in grado di autenticarsi al server locale IMR ed eseguire le sue mansioni.	Probabile	Insignificante	Tollerabile
		OTHER THAN	La stazione viene selezionata, ma il reindirizzamento sull'IMRW locale in oggetto non si completa con successo	Fallimento della comunicazione	L'AM non è in grado di autenticarsi al server locale IMR ed eseguire le sue mansioni.	Probabile	Insignificante	Tollerabile

5.2 LOGIN IMR

In questa fase i componenti che intervengono sono:

- Addetto manutenzione;
- Tablet;
- Server IMRG;
- Server IRMW;
- Server IMRS.

L'operazione di autenticazione coinvolge quasi tutti i componenti dell'apparato IMR. Questa operazione avviene mediante ID/Password e un meccanismo di chiave asimmetrica (pubblica-privata). L'addetto manutenzione immette le proprie credenziali e la chiave privata, la chiave pubblica è invece memorizzata dal server centrale IMRG che ha il compito di inviarla all'IMRW. Il server IMRW inoltra tutte le informazioni relative all'autenticazione al server IMRS che si occuperà di verificare l'effettiva correttezza di quest'ultime e quindi di inviare la schermata del Terminale Operatore al Tablet se l'utente è autorizzato. IMRS è un server sicuro, progettato, sviluppato e certificato SIL4 ed è per questo che il controllo delle credenziali viene effettuato su quest'ultimo e non su IMRW.



5.2.1 *Rischi individuati*

Quasi tutti i rischi individuati in questa sezione non coinvolgono la safety del sistema. Se l'AM non riesce ad autenticarsi all'IMR locale e quindi non riesce a svolgere le sue mansioni per qualunque causa (errore umano, errore accidentale sul server, attacco esterno ecc..), si verifica un problema per la availability e la security del sistema ma non per la safety, quindi tali rischi vengono classificati come *tollerabili*.

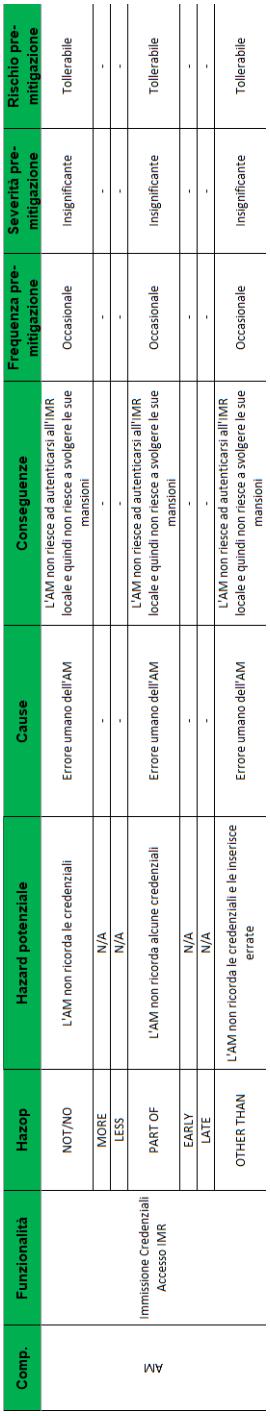
Di seguito sono riportati i principali azzardi individuati:

- a causa di un errore accidentale del server IMRG, di un attacco esterno o di un errore di rete generico, il Tablet potrebbe non riuscire a contattare il server IMRG. In tal caso le chiavi pubbliche non potranno essere recuperate;
- se a causa di un errore umano, l'AM inserisce credenziali errate oppure non le ricorda, non sarà possibile effettuare l'operazione di autenticazione e l'AM non potrà effettuare le sue mansioni;

Di seguito sono invece riportati alcuni dei rischi classificati come *intollerabili*, per i quali è opportuno individuare un'appropriata mitigazione:

- un attaccante potrebbe riuscire a rubare le credenziali nella non-safe area e appropriarsene con lo scopo di accedere al sistema;
- a causa di un errore accidentale del sistema IMRS, può non venir effettuato il controllo credenziali. I successivi comandi potrebbero essere a rischio in presenza di utenti malintenzionati;
- a causa di un errore accidentale del sistema IMRS, due utenti potrebbero essere confusi. Un utente potrebbe usare l'account di un utente diverso;
- a causa di un errore accidentale del sistema IMRS, due utenti fisicamente differenti potrebbero essere riconosciuti come lo stesso utente e confusi tra di loro.

Nella seguente immagine è presente una sezione del file di log della fase in questione:



Comp.	Funzionalità	Hazop	Hazard potenziale	Cause	Conseguenze	Frequenza pre-mitigazione	Severità pre-mitigazione	Rischio pre-mitigazione
AM	Immissione Credenziali Accesso IMR	NOT/NO	L'AM non ricorda le credenziali	Errore umano dell'AM	L'AM non riesce ad autenticarsi all'IMR locale e quindi non riesce a svolgere le sue mansioni	Occasionale	Insignificante	Tollerabile
		MORE	N/A	-	-	-	-	-
		LESS	N/A	-	-	-	-	-
		PART OF	L'AM non ricorda alcune credenziali	Errore umano dell'AM	L'AM non riesce ad autenticarsi all'IMR locale e quindi non riesce a svolgere le sue mansioni	Occasionale	Insignificante	Tollerabile
		EARLY	N/A	-	-	-	-	-
		LATE	N/A	-	-	-	-	-
		OTHER THAN	L'AM non ricorda le credenziali e le inserisce errate	Errore umano dell'AM	L'AM non riesce ad autenticarsi all'IMR locale e quindi non riesce a svolgere le sue mansioni	Occasionale	Insignificante	Tollerabile

5.3 VISUALIZZAZIONE TERMINALE OPERATORE (TO)

Durante le operazioni relative a questa fase, intervengono i seguenti componenti:

- Addetto manutenzione;
- Tablet;
- Server IRMW;
- Server IMRS.

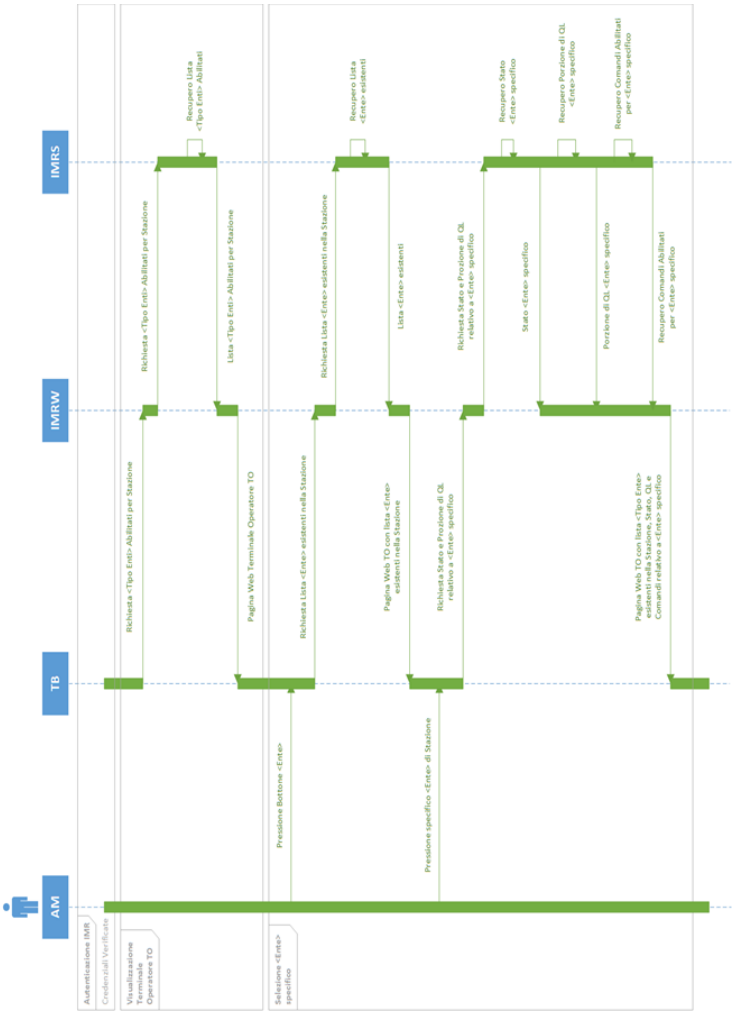


Figura 18: Sequence diagram fase Visualizzazione TO

Anche qui è possibile rilevare due sottosezioni:

- visualizzazione Terminale Operatore TO;
- selezione <Ente> specifico.

Infatti, dopo aver verificato la correttezza delle credenziali, viene inviata dall'IMRS al Tablet la pagina web del Terminale Operatore che riporta tutti gli Enti abilitati per quella determinata stazione.
L'AM in questa fase è in grado di selezionare i pulsanti degli <Enti> di stazione e l'IMRS inoltrerà la relativa pagina Web TO con lista <Tipo Ente> esistenti nella Stazione, Stato, QL, e i comandi relativi all'Ente specifico.

5.3.1 *Rischi individuati*

Le uniche operazioni che l'AM può effettuare in questa sezione sono quindi: "Pressione bottone <Ente>" e "Pressione specifico <Ente> di Stazione". L'IMRS si occuperà invece di recuperare la lista degli enti esistenti per quella stazione, lo stato degli enti, la porzione di QL specifica e i comandi abilitati. Poichè in questa fase l'AM non si occupa di inviare nè comandi critici nè informazioni sensibili, non vengono evidenziati particolari pericoli per la safety del sistema, tra i principali:

- a causa di un attacco esterno o di un errore di comunicazione, i messaggi inoltrati dall'IMRW all'IMRS, contenenti le richieste degli enti abilitati per stazione, potrebbero venir eliminati, creati, ritardati o ripetuti. Ciò comporterebbe alcuni malfunzionamenti, tuttavia non verrebbe impattata la safety del sistema;

- a causa di un attacco esterno o di un errore di comunicazione, i messaggi inoltrati dall'IMRS all'IMRW, contenenti la lista degli enti abilitati per stazione, potrebbero venir eliminati, creati, ritardati o ripetuti. Ciò comporterebbe alcuni malfunzionamenti, tuttavia non verrebbe impattata la safety del sistema;

- a causa di un errore del touchscreen del Tablet o di un errore umano, l'AM potrebbe non riuscire a visualizzare la lista degli elementi per l'ente richiesto;

- a causa di un errore del touchscreen del Tablet o di un errore umano l'AM potrebbe non riuscire a visualizzare lo stato dell'ente specifico;

- a causa di un attacco esterno o di un malfunzionamento del dispositivo, un messaggio contenente le richieste relative a queste sezione del sequence diagram potrebbe venir modificato con una richiesta critica per la safety (es. esecuzione di un comando critico). Il mes-

Comp	Funzionalità	Hazop	Hazard potenziale	Cause	Conseguenze	Frequenza pre-mitigazione	Severità pre-mitigazione	Rischio pre-mitigazione
AM	Pressione Bottone Ente	NOT/NO	Impossibilità di premere il bottone	Errore del touchscreen che non permette la pressione	Non si visualizza la lista degli elementi per l'ente richiesto	Occasionale	Insignificante	Tollerabile
		MORE	Un bottone viene premuto due volte	Errore del touchscreen o dell'operatore	Si visualizza la lista degli elementi per l'ente richiesto	Occasionale	Insignificante	Tollerabile
		LESS	Un bottone non è premuto adeguatamente	Errore del touchscreen o dell'operatore	Non si visualizza la lista degli elementi per l'ente richiesto	Occasionale	Insignificante	Tollerabile
		PART OF	N/A	-	-	-	-	-
		EARLY	N/A	-	-	-	-	-
		LATE	N/A	-	-	-	-	-
		OTHER THAN	Nel tentativo di premere il bottone, l'utente ne preme erroneamente un'altro.	Errore AM, bottoni troppo vicini	L'AM visualizza la lista di enti disponibili nella stazione, relativo però ad una tipologia di ente diversa da quella richiesta.	Probabile	Insignificante	Tollerabile
		OTHER THAN	Il bottone viene premuto, ma il sistema recepisce la pressione del bottone relativo ad un altro ente	Errore del tablet (es., del touchscreen)	L'AM visualizza la lista di enti disponibili nella stazione, relativo però ad una tipologia di ente diversa da quella richiesta.	Probabile	Insignificante	Tollerabile
AM	Selezione Ente Specifico	NOT/NO	Impossibilità di selezionare l'ente specifico	Errore del touchscreen che non permette la pressione	L'AM non riesce a visualizzare lo stato dell'ente specifico.	Occasionale	Insignificante	Tollerabile
		MORE	-	-	-	-	-	-
		LESS	-	-	-	-	-	-
		PART OF	-	-	-	-	-	-
		EARLY	-	-	-	-	-	-
		LATE	-	-	-	-	-	-
		OTHER THAN	Nel tentativo di selezionare uno specifico ente, l'utente ne sceglie erroneamente un'altro.	Errore AM, menù di scelta con opzioni troppo vicine	Il tablet visualizza lo stato di un ente diverso da quello che l'AM vuole visualizzare.	Occasionale	Insignificante	Tollerabile
		OTHER THAN	Il bottone viene premuto, ma il sistema recepisce la pressione del bottone relativo ad un altro ente specifico	Errore del touchscreen		Remoto	Insignificante	Trascurabile

Figura 19: Sezione Hazard Analysis Visualizzazione TO

saggio potrebbe essere riconosciuto come legittimo e la richiesta essere eseguita. Questo azzardo viene valutato come *intollerabile*;

- a causa di un attacco esterno o di un malfunzionamento del dispositivo, il messaggio contenente le informazioni inviate dal server IMRS inerenti lo stato del sistema(pagina web TO, lista <Ente> esistente per stazione e comandi relativi all'ente) potrebbe venir modificato da un messaggio contenente informazioni errate. Il messaggio potrebbe essere riconosciuto come legittimo e l'AM potrebbe essere ingannato da tali informazioni. Questo azzardo viene valutato come *intollerabile*.

5.4 ESECUZIONE COMANDO AM

Questa sezione si occupa di analizzare la fase in cui l'AM vuole eseguire un comando. I componenti che hanno un ruolo attivo sono:

- Addetto manutenzione (AM);
- Tablet Operatore;
- Server IMRW;
- Server IMRS;
- ACC;
- Dirigente movimento (DM);

Questa è l'unica fase in cui è presente anche il Dirigente movimento con il ruolo di autorizzare l'esecuzione dei comandi critici.
In questa fase il Tablet si occupa di inoltrare i comandi all'IMRW, che di conseguenza li comunicherà al Server locale IMRS; tale server sicuro, appartenente alla safe area, trasmette al nucleo in sicurezza le operazioni da eseguire.
Il nucleo in sicurezza, dopo aver attuato il comando, invia i dati sullo stato del sistema all'IMRS che eventualmente si occuperà di elaborarli. Le informazioni verranno in seguito inviate al Tablet, in modo tale che l'AM venga informato dello stato del sistema.

5.4.1 *Rischi individuati*

In questa fase viene descritta la procedura più delicata, infatti vengono trasportate informazioni sensibili che potrebbero essere utilizzate da un attaccante per danneggiare catastroficamente il sistema. Poichè in questa sezione le criticità individuate sono molteplici, esse sono state suddivise sulla base della loro causa. L'analisi ha portato a individuare varie situazioni indesiderabili, quali:

CRITICITÀ CAUSATA DA UN ERRORE UMANO

- a causa di un errore umano (es. pulsanti troppo vicini sul Tablet), l'AM, nel tentativo di premere il bottone per eseguire un comando, potrebbe cliccare erroneamente su un altro pulsante. In questo caso quindi l'AM inoltrerebbe al server IMRS un comando diverso da quello che avrebbe voluto eseguire;

CRITICITÀ CAUSATE DA UN ERRORE ACCIDENTALE DEL SISTEMA

- a causa di un errore accidentale del server IMRS, dati e immagini potrebbero venir generati in modo non corretto (informazioni aggiuntive, alterate o parziali). Potrebbero essere mostrate informazioni erronee anche su comandi critici all'AM;
- a causa di un errore accidentale del server IMRS, potrebbe venir creato un comando da inoltrare al nucleo in sicurezza. Il nuovo comando potrebbe venire riconosciuto come legittimo e venire eseguito, causando eventualmente gravi problemi;
- a causa di un errore accidentale del server IMRS, potrebbe venir duplicato un comando da inoltrare al nucleo in sicurezza. Il nuovo comando potrebbe venire riconosciuto come legittimo e venire eseguito, causando eventualmente gravi problemi;
- a causa di un errore accidentale del server IMRS, potrebbe venir ritardato eccessivamente un comando da inoltrare al nucleo in sicurezza. Il comando potrebbe essere eseguito con ritardo, nel caso pessimo alterando lo stato della linea;
- a causa di un errore accidentale del server IMRS, potrebbe venir alterato un comando da inoltrare al nucleo in sicurezza. Il nuovo comando potrebbe venire riconosciuto come legittimo e venire eseguito, causando eventualmente gravi problemi;

- a causa di un errore accidentale del server IMRS potrebbero non venir ricevuti i dati provenienti dal nucleo in sicurezza. I dati non verrebberp ricevuti dal IMRS e quindi l'AM non potrebbe visualizzare le informazioni;
- a causa di un errore accidentale del server IMRS potrebbero venir ricevuti dati alterati (informazioni aggiuntive, modificate o parziali) provenienti dal nucleo in sicurezza. I nuovi dati potrebbero venire riconosciuti come legittimi, quindi eventualmente verrebberp visualizzate dall'AM informazioni errate;
- a causa di un rallentamento sul server IMRS potrebbero venir ricevuti in ritardo i dati dal nucleo in sicurezza. La comunicazione con l'AM diventerebbe più lenta del previsto o eventualmente impossibile. Nel caso peggiore, azioni (inclusioni/esclusioni) effettuate sull'ente verrebbero notificate in ritardo all'AM, che nel frattempo potrebbe trovarsi in pericolo.
- a causa di un errore del touchscreen del Tablet, il dispositivo potrebbe recepire la pressione di un pulsante diverso da quello effettivamente premuto dall'AM. In questo caso quindi verrebbe inoltrato al server IMRS un comando diverso da quello che l'AM avrebbe voluto eseguire;

CRITICITÀ CAUSATE DA UN ATTACCO ESTERNO

- a causa di un attacco esterno, potrebbe essere alterato il messaggio contenente il comando "Esclusione Zona/Ente, Chiusura Segnale o Bloccamento FS" inserito dall'AM sul Tablet (es. potrebbe essere modificata la zona da escludere). Il manutentore potrebbe recarsi nella zona che aveva specificato (pensandola esclusa), con il rischio che i treni passino di lì. In questo caso l'attaccante dovrebbe anche modificare la notifica di conferma esecuzione del comando;
- a causa di un attacco esterno, potrebbe essere eliminato il messaggio contenente il comando "Esclusione Zona/Ente, Chiusura Segnale o Bloccamento FS" inserito dall'AM sul Tablet. Il manutentore potrebbe andare nella zona (pensandola esclusa), con il rischio che i treni passino di lì. In questo caso l'attaccante dovrebbe anche creare la notifica di conferma esecuzione del comando;
- un attaccante potrebbe modificare l'orologio del Tablet per far sembrare la porzione di QL recente quando in realtà non lo è. Il ma-

nutentore potrebbe essere a rischio, non avendo la possibilità di visualizzare la lista aggiornata dei comandi;

- a causa di un attacco esterno, di un errore nel canale, sul Tablet o sul dispositivo, potrebbe venir eliminato un messaggio tra Tablet e Server IMRW. Ciò causerebbe possibili perdite di dati sensibili e malfunzionamenti di procedure che richiedono l'esecuzione di determinate azioni in sequenza;

- un attaccante potrebbe voler duplicare un messaggio nella comunicazione Tablet-Server IMRW per influire negativamente sul sistema. Si ripresenterebbe l'informazione già visualizzata in un momento precedente, che potrebbe, nel caso peggiore, trarre in inganno l'AM sulla situazione di inclusione/esclusione di una qualche zona di stazione;

- un attaccante potrebbe voler creare un nuovo messaggio nella comunicazione Tablet-Server IMRW per influire negativamente sul sistema. Il nuovo messaggio potrebbe venire riconosciuto come legittimo, causando eventualmente gravi problemi al sistema sulla base del suo contenuto (incluso trarre in inganno l'AM rispetto a inclusione/esclusione di una qualche zona di stazione);

- a causa di un attacco esterno o di un errore di rete, un messaggio nel canale Tablet-IMRW potrebbe venir inviato con ritardo. Il messaggio potrebbe non arrivare in tempo all'AM o al Server. Senza l'utilizzo di un protocollo adeguato si può perdere traccia dei messaggi inviati e che poi sono stati ricevuti in ritardo;

- a causa di un attacco esterno, di un errore sul server o sul dispositivo, un messaggio nella comunicazione Tablet-Server IMRW potrebbe venire alterato. Il nuovo messaggio potrebbe venire riconosciuto come legittimo, causando eventualmente gravi problemi al sistema sulla base del suo contenuto (incluso trarre in inganno l'AM rispetto a inclusione/esclusione di una qualche zona di stazione);

- a causa di un attacco esterno, potrebbe essere replicato il messaggio contenente le informazioni circa il comando "Inclusione Zona/Ente, Apertura Segnale, Disattivazione Rallentamento, Richiesta trBCA o Liberazione FS" inserito dall'AM sul Tablet. Potrebbe arrivare un comando vecchio di inclusione in una zona esclusa e mettere a rischio la sicurezza dell'AM;

- a causa di un attacco esterno, potrebbe essere alterato il comando "Inclusione Zona/Ente, Apertura Segnale, Disattivazione Rallentamento, Richiesta trBCA o Liberazione FS" inserito dall'AM sul Tablet. Potrebbe quindi venire inclusa una zona diversa da quella indicata, l'AM si troverebbe quindi in pericolo;

- a causa di un attacco esterno, sul Tablet o sul server IMRW, dopo l'inclusione della zona richiesta dall'AM, quest'ultimo potrebbe non ricevere la notifica di avvenuta esecuzione del comando. L'AM potrebbe rimanere nella zona mettendo a rischio la propria sicurezza;

- a causa di un attacco esterno o di un errore sul server IMRW, potrebbe venire accidentalmente creato un messaggio contenente un comando e quindi inviato verso il server IMRS; si creerebbe una situazione di incertezza per l'AM. Il nuovo messaggio potrebbe venire riconosciuto come legittimo, causando eventualmente gravi problemi al sistema sulla base del suo contenuto;

- a causa di un attacco esterno o di un errore sul server IMRW, potrebbe venire alterato un messaggio e inviato verso il server IMRS; in tal caso il messaggio alterato potrebbe venire riconosciuto come legittimo, causando eventualmente gravi problemi al sistema sulla base del suo contenuto;

- a causa di un attacco esterno o malfunzionamento dei server, potrebbe venir duplicato un messaggio dal server IMRW al Tablet. Si creerebbe una situazione di incertezza per l'AM. Il nuovo messaggio potrebbe venire riconosciuto come legittimo, causando eventualmente gravi problemi al sistema sulla base del suo contenuto;

- a causa di un attacco esterno o malfunzionamento dei server, potrebbe venir ritardato eccessivamente un messaggio dal server IMRW al Tablet. Nel caso peggiore potrebbero essere fornite all'AM informazioni errate;

- a causa di un attacco esterno, di un errore accidentale del server IMRW, i dati ricevuti dal server IMRS potrebbero non venire assemblati. Tali informazioni non saranno visualizzabili. L'AM potrebbe non sapere se un comando è stato eseguito con successo dal nucleo in sicurezza o meno;

- a causa di un attacco esterno o di un errore accidentale del server IMRW i dati ricevuti dal server IMRS potrebbero venire assemblati in modo non corretto (informazioni aggiuntive, alterate o parziali). L'AM potrebbe non sapere se un comando sia stato eseguito con successo dal nucleo in sicurezza o meno;

Sono stati invece classificati come tollerabili i seguenti azzardi:

CRITICITÀ CAUSATE DA UN ERRORE UMANO

- a causa di un errore umano o per l'indisponibilità della rete telefonica (per malfunzionamento o attacco), l'AM potrebbe non riuscire a effettuare la telefonata al DM (o dimenticarsene); secondo la procedura, in mancanza di conferma del DM, il comando non verrebbe eseguito dal nucleo in sicurezza.

- a causa di un errore umano o per l'indisponibilità della rete telefonica (per malfunzionamento o attacco), l'AM potrebbe non riuscire a scambiare telefonicamente tutte le informazioni con il DM. L'AM sarebbe costretto a richiamare il DM;

- a causa di un errore umano, dopo che l'AM ha chiamato il DM per avvisarlo del comando che vuole portare a termine, il DM potrebbe non autorizzare tale comando. Secondo la procedura, in mancanza di conferma del DM, il comando non verrebbe eseguito dal nucleo in sicurezza;

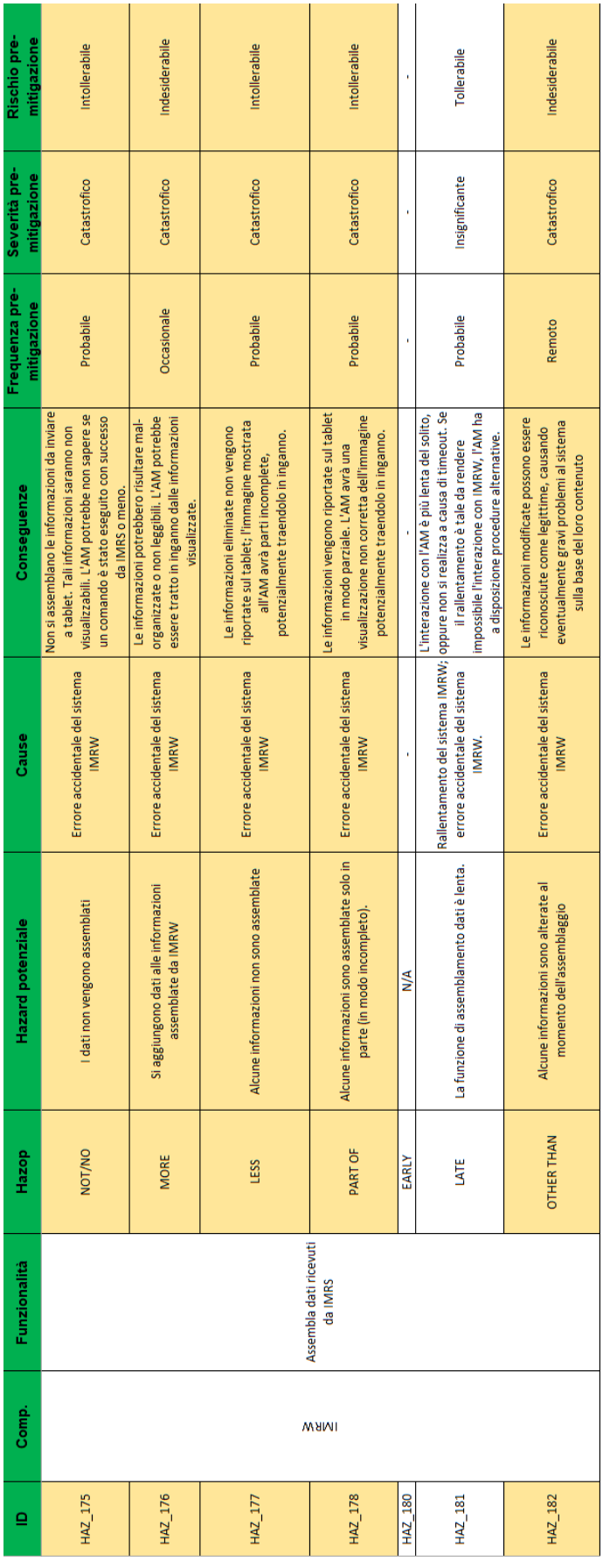
CRITICITÀ CAUSATE DA UN ERRORE ACCIDENTALE DEL SISTEMA O DI COMUNICAZIONE

- a causa di un errore del touchscreen del Tablet o del dispositivo, l'AM potrebbe non essere in grado di premere il pulsante per effettuare il comando;

- a causa di un errore generico del Tablet o della comunicazione, il comando "Esclusione Zona/Ente, Chiusura Segnale o Bloccamento FS" inserito dall'AM potrebbe non venir comunicato al server IMRW. In questo caso non verrebbe ricevuta la conferma di esecuzione del comando dall'AM;

- a causa di un errore generico del Tablet o della comunicazione, il comando "Esclusione Zona/Ente, Chiusura Segnale o Bloccamento FS" inserito dall'AM potrebbe venir comunicato come duplicato;

- a causa di un errore generico del Tablet o della comunicazione, il comando "Esclusione Zona/Ente, Chiusura Segnale o Bloccamento FS" inserito dall'AM, potrebbe venir comunicato con ritardo;
- a causa di un errore di comunicazione, un messaggio contenente un comando inviato dal Server IMRW al server IMRS, potrebbe essere eliminato e quindi il comando non eseguito;
- a causa di un errore di comunicazione o di un malfunzionamento del server IMRW un messaggio contenente un comando inviato dal Server IMRW al server IMRS potrebbe essere replicato e quindi il comando eseguito due volte;
- a causa di un errore di rete locale, un messaggio contenente un comando inviato dal Server IMRW al server IMRS potrebbe essere inviato con ritardo, il completamento dell'esecuzione del comando sarebbe ritardata di conseguenza;
- a causa di un errore accidentale del server IMRW, i dati ricevuti dal server IMRS potrebbero venire assemblati in ritardo. Si creerebbe una situazione di incertezza da parte dell'AM sul fatto che il comando sia stato eseguito o meno. Per procedura, in questo caso l'AM dovrebbe il DM;
- a causa di un errore accidentale del server IMRS, dati e immagini potrebbero non venir generati. Si creerebbe una situazione di incertezza da parte dell'AM sul fatto che il comando sia stato eseguito o meno. Per procedura, in questo caso l'AM dovrebbe consultare il DM;
- a causa di un errore accidentale del server IMRS dati e immagini potrebbero venir generati con ritardo. Si creerebbe una situazione di incertezza da parte dell'AM sul fatto che il comando sia stato eseguito o meno. Per procedura, in questo caso l'AM dovrebbe consultare il DM;
- a causa di un errore accidentale del server IMRS, un comando da inoltrare al nucleo in sicurezza potrebbe venir eliminato e quindi non venir eseguito dal sistema. L'AM non riceverebbe notifica dell'esecuzione del comando.



ID	Comp.	Funzionalità	Hazop	Hazard potenziale	Cause	Conseguenze	Frequenza pre-mitigazione	Severità pre-mitigazione	Rischio pre-mitigazione
HAZ_175	IMRW	Assembla dati ricevuti da IMRS	NOT/NO	I dati non vengono assemblati	Errore accidentale del sistema IMRW	Non si assembla le informazioni da inviare a tablet. Tali informazioni saranno non visualizzabili. L'AM potrebbe non sapere se un comando è stato eseguito con successo da IMRS o meno.	Probabile	Catastrofico	Intollerabile
HAZ_176			MORE	Si aggiungono dati alle informazioni assemblate da IMRW	Errore accidentale del sistema IMRW	Le informazioni potrebbero risultare mal-organizzate o non leggibili. L'AM potrebbe essere tratto in inganno dalle informazioni visualizzate.	Occasionale	Catastrofico	Indesiderabile
HAZ_177			LESS	Alcune informazioni non sono assemblate	Errore accidentale del sistema IMRW	Le informazioni eliminate non vengono riportate sul tablet; l'immagine mostrata all'AM avrà parti incomplete, potenzialmente traendolo in inganno.	Probabile	Catastrofico	Intollerabile
HAZ_178			PART OF	Alcune informazioni sono assemblate solo in parte (in modo incompleto).	Errore accidentale del sistema IMRW	Le informazioni vengono riportate sul tablet in modo parziale. L'AM avrà una visualizzazione non corretta dell'immagine potenzialmente traendolo in inganno.	Probabile	Catastrofico	Intollerabile
HAZ_180			EARLY	N/A	-	-	-	-	-
HAZ_181			LATE	La funzione di assemblamento dati è lenta.	Rallentamento del sistema IMRW; errore accidentale del sistema IMRW.	L'interazione con l'AM è più lenta del solito, oppure non si realizza a causa di timeout. Se il rallentamento è tale da rendere impossibile l'interazione con IMRW, l'AM ha a disposizione procedure alternative.	Probabile	Insignificante	Tollerabile
HAZ_182			OTHER THAN	Alcune informazioni sono alterate al momento dell'assemblaggio	Errore accidentale del sistema IMRW	Le informazioni modificate possono essere riconosciute come legittime, causando eventualmente gravi problemi al sistema sulla base del loro contenuto	Remoto	Catastrofico	Indesiderabile

Figura 20: Sezione Hazard Analysis Esecuzione comando AM

CRITICITÀ CAUSATE DA UN ATTACCO ESTERNO

- a causa di un attacco esterno, potrebbe essere eliminato il messaggio contenente le informazioni circa il comando "Inclusione Zona/Ente, Apertura Segnale, Disattivazione Rallentamento, Richiesta trBCA o Liberazione FS" inserito dall'AM sul Tablet. La zona non verrebbe inclusa. In questo caso non verrebbe ricevuta la conferma di esecuzione del comando dall'AM;
- a causa di un attacco esterno, malfunzionamento dei server o errore di rete i dati provenienti dal server IMRS, inoltrati dal server IMRW al Tablet, potrebbero venire eliminati. Si creerebbe una situazione di incertezza da parte dell'AM sul fatto che il comando sia eseguito o meno. Per procedura, in questo caso l'AM dovrebbe consultare il DM;

5.5 SELEZIONE PIANO SCHEMATICO (PS), QUADRO LUMINOSO (QL), LOG

Le operazioni descritte in questa sezione si occupano di fornire informazioni all'AM circa lo stato del sistema da vari punti di vista. Come riportato nel capitolo precedente, oltre al Terminale Operatore, è possibile accedere anche alla schermata di Log, al Piano schematico e al Quadro luminoso della stazione. Tutte queste schermate offrono elementi aggiuntivi che possono essere utilizzati dall'AM per effettuare il proprio lavoro in maniera più completa.
In questa sezione i componenti che operano sono:

- Addetto manutenzione (AM);
- Tablet Operatore;
- Server IMRW;
- Server IMRS.

Ogni volta che l'AM preme l'icona relativa al Quadro luminoso o alla schermata Log o al Piano schematico, la richiesta viene inoltrata al server IMRW e infine al server IMRS che si occupa di restituire le informazioni richieste.
Una porzione del quadro luminoso è presente anche nella schermata del Terminale Operatore, quindi ogni volta che viene disattivata o attivata una zona, viene inviata una richiesta all'IMRS per ottenere il quadro luminoso della zona in oggetto.

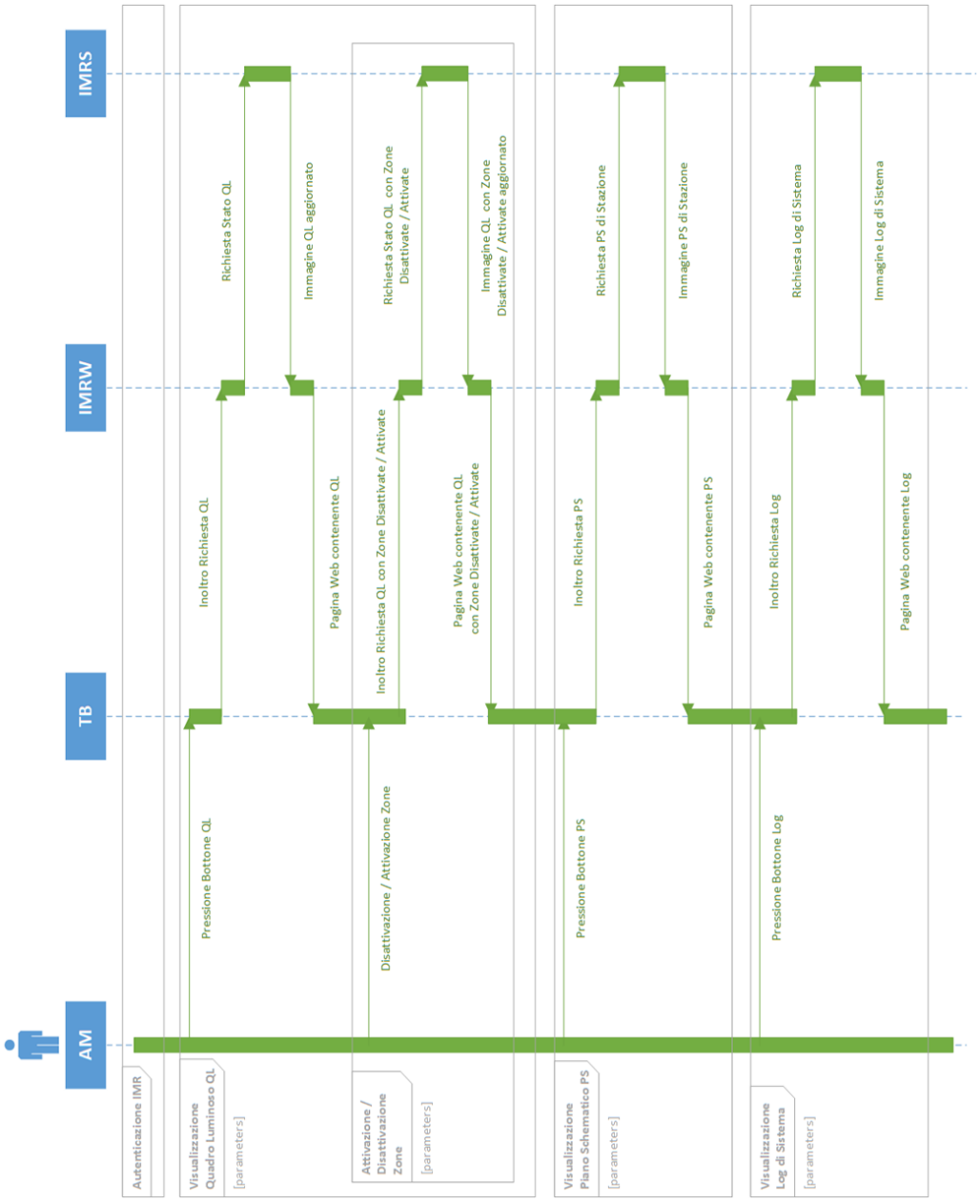


Figura 21: Sequence diagram Selezione PS, QL, Log

5.5.1 *Rischi individuati*

Questa sezione non presenta particolari problemi per quanto riguarda la safety del sistema. I principali rischi evidenziati sono:

- a causa di un attacco esterno oppure di un errore accidentale del sistema, una richiesta per visionare le suddette schermate potrebbe non venire inoltrata dal Tablet, in tal caso comunque non viene compromessa la sicurezza dell'AM;
- a causa di un attacco esterno oppure di un errore accidentale del sistema, potrebbe venire creata una richiesta per visionare le varie schermate. Nemmeno questo scenario impatta la sicurezza dell'AM;
- a causa di un attacco esterno oppure di un errore accidentale del sistema la richiesta per visionare le schermate potrebbe essere inoltrata con eccessivo ritardo; la richiesta verrebbe quindi eseguita con ritardo, come nei casi precedenti, questo scenario, non prevede l'esecuzione di comandi critici per la safety;
- a causa di un attacco esterno oppure di un errore accidentale del sistema, le schermate corrispondenti al PS, QL, e Log potrebbero venire alterate con lo scopo di fornire informazioni errate all'AM circa lo stato del sistema;
- a causa di un attacco esterno oppure di un errore accidentale del sistema potrebbe venire alterata una richiesta per visionare le varie schermate. La nuova richiesta potrebbe essere critica per la safety; tale rischio viene identificato come *intollerabile*.

Comp.	Funzionalità	Hazop	Hazard potenziale	Cause	Conseguenze	Frequenza pre-mitigazione	Severità pre-mitigazione	Rischio pre-mitigazione
Tablet	Inoltro Richiesta TO / QL / PS / Log	NOT/NO	Richiesta non inoltrata dal tablet	Attaccante intercetta e rimuove la richiesta	La richiesta, che prevede una funzione non critica per la safety, non raggiunge l'IMRS e non è eseguita	Probabile	Insignificante	Tollerabile
		NOT/NO	Richiesta non inoltrata dal tablet	Errore del tablet	La richiesta, che prevede una funzione non critica per la safety, non raggiunge l'IMRS e non è eseguita	Probabile	Insignificante	Tollerabile
		NOT/NO	Richiesta non inoltrata dal tablet	Errore del canale	La richiesta, che prevede una funzione non critica per la safety, non raggiunge l'IMRS e non è eseguita	Probabile	Insignificante	Tollerabile
		MORE	Richiesta inoltrata autonomamente, all'insaputa dell'AM	Attaccante genera e invia una richiesta	La richiesta è eseguita, ma non prevede l'esecuzione di comandi critici per la safety	Probabile	Insignificante	Tollerabile
		MORE	Richiesta inoltrata autonomamente, all'insaputa dell'AM	Errore del tablet	La richiesta è eseguita, ma non prevede l'esecuzione di comandi critici per la safety	Probabile	Insignificante	Tollerabile
		MORE	Richiesta inoltrata autonomamente, all'insaputa dell'AM	Errore del canale	La richiesta è eseguita, ma non prevede l'esecuzione di comandi critici per la safety	Probabile	Insignificante	Tollerabile
		LESS	N /A	-	-	-	-	-
		PART OF	N/A	-	-	-	-	-
		EARLY	N/A	-	-	-	-	-
		LATE	Richiesta trattenuta ed inviata in ritardo	Errore del tablet, del canale, oppure opera di un'attaccante	La richiesta è eseguita, ma non prevede l'esecuzione di comandi critici per la safety	Probabile	Insignificante	Tollerabile
		OTHER THAN	Richiesta modificata con un'altra richiesta critica per la safety ed inviata	Errore del tablet, del canale, oppure opera di un'attaccante	La richiesta è eseguita	Probabile	Catastrofico	Intollerabile
		OTHER THAN	Richiesta modificata con un'altra richiesta non critica per la safety ed inviata	Errore del tablet, del canale, oppure opera di un'attaccante	la richiesta è eseguita	Probabile	Insignificante	Tollerabile

Figura 22: Sezione hazard analysis Selezione PS, QL, Log

6

MITIGAZIONI

Nel capitolo precedente sono stati analizzati i principali azzardi individuati nell'apparato IMR e molti di questi sono stati classificati come *intollerabili*; per questi ultimi è opportuno realizzare una procedura di mitigazione. La mitigazione può avere come scopo quello di ridurre la severità dell'azzardo oppure renderlo meno frequente, in modo tale che possa venir considerato *tollerabile* per il sistema. In questo capitolo+ sono descritte le due mitigazioni applicate all'apparato successivamente all'hazard analysis:

- utilizzo di una One Time Password;
- utilizzo del protocollo PVS.

Tramite l'utilizzo di una OTP infatti è possibile rendere tollerabili tutte le criticità riscontrate nella fase di "Esecuzione comando AM" descritta nel capitolo precedente. Invece, attraverso l'utilizzo del protocollo PVS sono stati mitigati tutti i rimanenti azzardi.

6.1 UTILIZZO DI UNA ONE TIME PASSWORD

Dall'analisi è risultato che la maggior parte della situazioni indesiderabili si verificherebbe quando l'AM tenta di eseguire un comando critico. Infatti è possibile che, a causa di un attacco esterno oppure accidentalmente, il messaggio contenente il comando venga eliminato o alterato, così come la risposta di conferma di esecuzione del comando. Per ovviare a tale problematica è stato pensato di aggiungere all'architettura dell'apparato un ulteriore dispositivo: lo Smartphone.
Tale dispositivo viene impiegato dal sistema quando l'AM ha intenzione di eseguire un comando critico per la sicurezza, con lo scopo di utilizzare un canale alternativo per convalidare il comando.
In particolare, quando l'AM decide di effettuare un comando critico,

l'IMRS invia la richiesta di conferma del comando al Tablet; per attuare tale operazione, l'AM deve inserire sul Tablet una One Time Password pervenuta intanto sullo Smartphone tramite un canale alternativo. Quindi, una volta che l'IMRS riceve la richiesta di esecuzione di un comando critico, risponde:

- al Tablet, inviando una immagine contenente il comando ricevuto, incluse alcune informazioni associate;
- allo Smartphone, inviando una informazione contenente il comando ricevuto e una OTP.

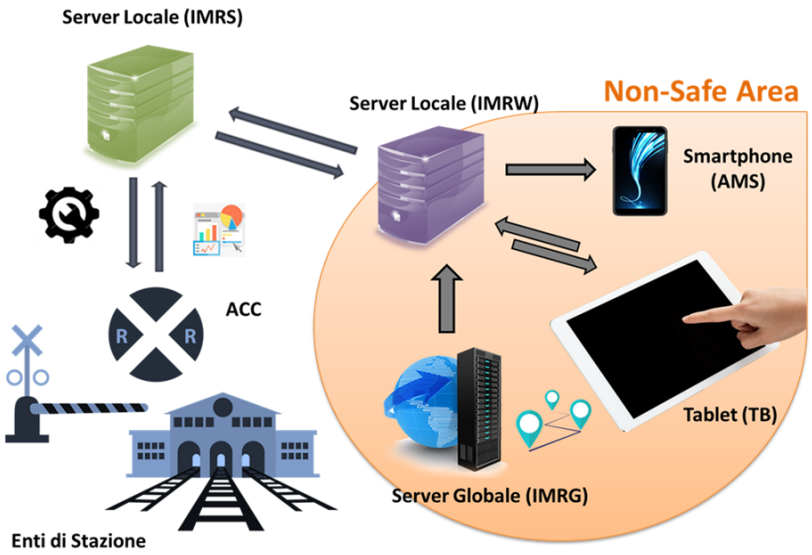


Figura 23: Il ruolo dello Smartphone nell'apparato IMR

In questo modo l'AM può verificare la consistenza delle informazioni giunte su Tablet e Smartphone e in seguito inserire la OTP sul Tablet per confermare il comando. A questo punto il server IMRS potrà inoltrare il comando al nucleo in sicurezza, se la password risulta verificata.
Se il nucleo esegue il comando, viene inviata dal server IMRS:

- al Tablet: una immagine che contiene la conferma del comando (o le informazioni richieste) e una nuova OTP;
- allo Smartphone: la stessa OTP e le informazioni accessorie per confermare i dati contenuti nell'immagine.

Attraverso questa procedura è possibile contrastare eventuali contraffazioni alle informazioni eseguite da un attaccante.

Invece, se il nucleo non esegue il comando, viene inviata una notifica solo verso il Tablet, senza OTP. Non avendo OTP da inserire, l'AM ne conclude che il comando non è stato eseguito.
Durante tutta la procedura appena descritta l'AM è direttamente responsabile di confrontare visivamente che le informazioni giunte sui dispositivi combacino, incluse le OTP. L'AM inoltre è anche responsabile di non assumere la corretta esecuzione del comando, qualora la procedura realizzata non rispetti lo schema descritto.
Nell'immagine seguente è possibile osservare il sequence diagram della fase *Esecuzione comando* con gli aggiornamenti riguardanti l'aggiunta dell'utilizzo della OTP.

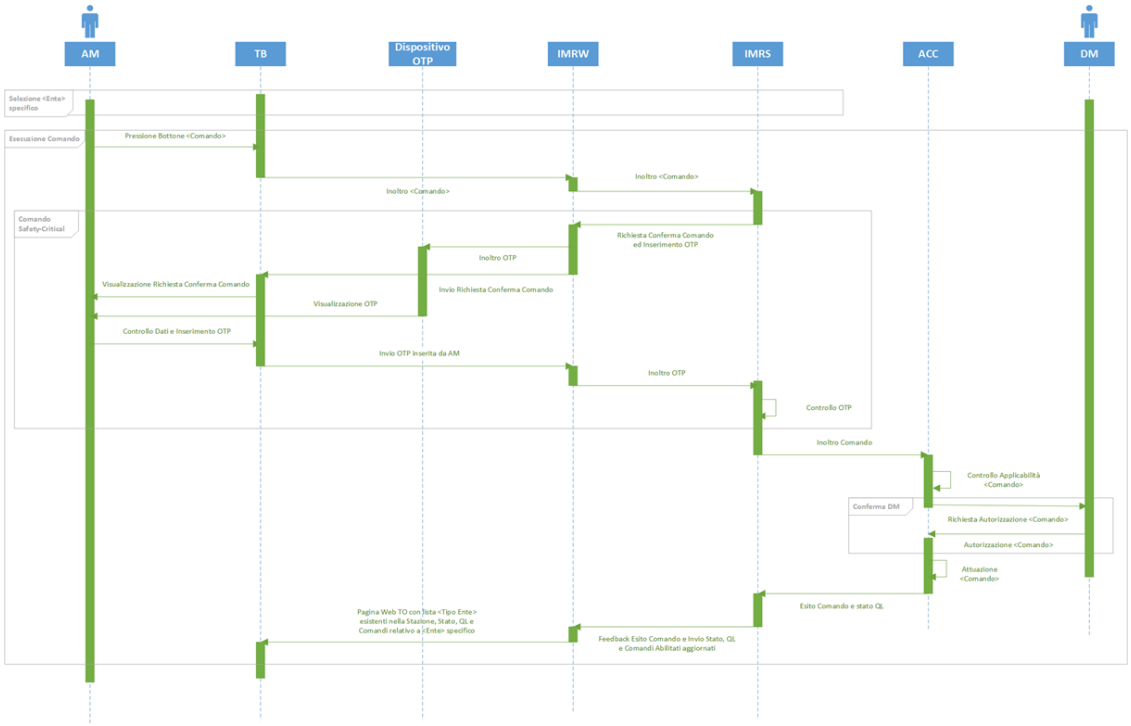


Figura 24: Sequence diagram Esecuzione comando

6.2 UTILIZZO DEL PROTOCOLLO PVS

Poiché i canali di comunicazione ordinari non sono affidabili, l'apparato IMR adotta un protocollo noto come Protocollo Vitale Standard (PVS), ideato da RFI per consentire interazioni sicure tra diversi dispositivi. Per imporre la safety di tutte le comunicazioni la procedura deve essere progettata secondo lo standard EN50159 [12] e dovrebbe essere codificata

come linguaggio di medio-basso livello in accordo allo standard EN50128 [11].
Il protocollo PVS fornisce un livello di safety insieme alla protezione contro l'accesso non autorizzato attraverso l'uso di codici di sicurezza e tecniche crittografiche. Le tecniche e gli algoritmi inclusi nel protocollo sono stati identificati tra quelli collaudati, validati e proven-in-use nel settore ferroviario.
Il protocollo può essere riassunto come un software aggiuntivo che fornisce le funzionalità OSI di sessione e presentazione tramite:

- codici di sicurezza (per garantire l'integrità del messaggio);
- numero di sequenza (per evitare la re-sequenziazione, ripetizione, inserimento e cancellazione di messaggi);
- execution cycle (per ottenere la freshness del messaggio);
- identificativi di nodo, sorgente e destinazione, univoci (per l'autenticità);
- crittografia.

Dall'unione di questi meccanismi è possibile garantire comunicazioni sicure.
La comunicazione bidirezionale tra IMRS e IMRW è condotta tramite messaggi scambiati attraverso il protocollo PVS, di conseguenza entrambi i server dovranno aprire un canale di comunicazione bidirezionale.
Invece l'interazione tra il server IMRW e il Tablet prevede una procedura più articolata:

- il server genera delle pagine HTML tramite opportuno linguaggio di scripting lato-server;
- questo flusso HTTP viene intercettato da uno script, il PVS Server, che prende il messaggio e lo usa come payload per una comunicazione PVS;
- il messaggio PVS così creato viene inviato al Tablet su una porta predefinita sulla quale ascolta il modulo PVS Client;
- il modulo PVS Client, dopo aver ricevuto i dati PVS, li decapsula e li reinoltra sulla porta HTTP (default: 80) del Tablet.

Quando l'AM vuole inviare dei comandi tramite TB al server IMRW, verrà eseguito il procedimento a ritroso, sfruttando lo stesso canale sicuro.

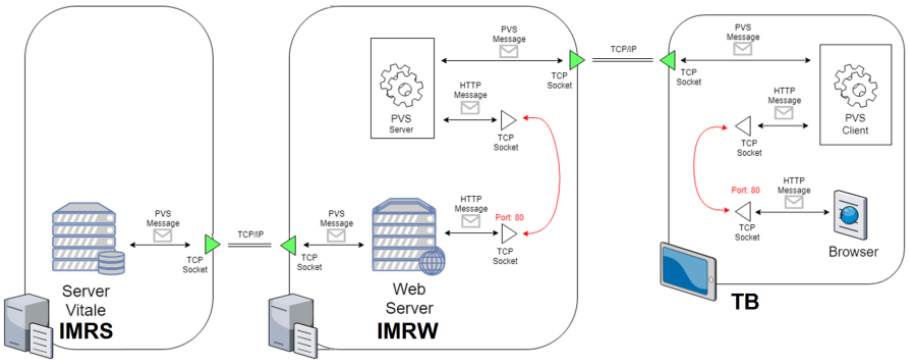


Figura 25: Protocollo PVS

6.3 DIRETTIVE COMPORTAMENTALI

Tramite l'utilizzo delle due mitigazioni appena descritte, tutti i rischi classificati come *intollerabili* nel capitolo precedente, possono venir rivalutati e considerati invece come *ammissibili* per l'apparato IMR. Infatti, attraverso l'uso del protocollo PVS e della procedura che prevede l'inserimento delle OTP, la safety del sistema non è più a rischio.
Di seguito sono state inserite alcune linee guida per l'utilizzo del sistema, per cercare di ottimizzare l'impiego di quest'ultimo:

- *avere a disposizione un tablet di riserva*: questo accorgimento è necessario quando il tablet utilizzato dall'operatore non riesce a eseguire correttamente le operazioni di base (touchscreen non reattivo, spegnimento improvviso del tablet, mancata gestione della batteria ecc..);
- *riaggiornamento pagina*: da effettuare quando ad esempio la lista delle stazioni non è completa;
- *utilizzare password potenti*: per fare in modo che il meccanismo di autenticazione tramite password sia solido e sia difficile per un attaccante introdursi nel sistema è necessario che la password adottata sia più complessa possibile. E' quindi consigliabile utilizzare sia lettere maiuscole che minuscole, segni e numeri;
- *numero tentativi autenticazione limitati*: è possibile che un attaccante per accedere al sistema abbia intenzione di provare tutte le password di un dizionario. Per evitare che tale attacco sia possibile, è necessario imporre che i tentativi di autenticazione siano limitati,

ad esempio un numero appropriato di tentativi di autenticazione potrebbe essere pari a 3;

- *modificare la password periodicamente*: per garantire la sicurezza del sistema è opportuno che le password degli addetti manutenzione vengano modificate periodicamente;
- *memorizzare la chiave privata in sicurezza*: per evitare che il file contente la chiave privata possa essere reperibile da individui non autorizzati ad accedere al sistema, è opportuno che venga salvato in una posizione di massima sicurezza;
- *effettuare l'autenticazione periodicamente*: per fare in modo che il Tablet non possa essere utilizzato da terzi per l'esecuzione di comandi, sarebbe bene che periodicamente venga effettuata l'operazione di login da parte dell'AM.

7

CONCLUSIONI

I sistemi informatici complessi vengono adoperati sempre più frequentemente per svolgere compiti altamente critici che coinvolgono la sicurezza e l'incolumità delle persone. E' pertanto di fondamentale importanza che vengano adottate delle tecniche in grado di mantenere sempre corrette le funzioni per le quali sono destinate.
In ambito informatico il concetto di difesa è sempre più rilevante, infatti riuscire a possedere una solida difesa permette di tutelare i dati da attacchi esterni e di preservare i sistemi dai danni inerenti l'integrità, la disponibilità e la confidenzialità delle informazioni in essi custodite. Attraverso l'adozione di soluzioni hardware e software è possibile raggiungere un elevato grado di protezione; tali soluzioni innalzano il livello di difesa, ma non possono garantire la totale protezione dei sistemi informatici, infatti le tecniche sviluppate dagli attaccanti per ottenere le informazioni desiderate, diventano sempre più mirate ed esperte. Quindi, è di fondamentale importanza rimanere sempre aggiornati sulle nuove tecniche di attacco e continuare a indagare sulle vulnerabilità dei software e dei protocolli di comunicazione, con lo scopo di riuscire a anticipare le mosse dell'attaccante.
Concludendo, nel lavoro appena descritto riguardante l'apparato IMR, è stato possibile osservare che *l'hazard analysis rappresenta una delle operazioni fondamentali per la prevenzione delle criticità* in un sistema informatico. Attraverso le parole guida delineate dalla procedura è stato possibile individuare tutti i potenziali pericoli e i problemi di operatività che possono portare a condizioni di funzionamento non conformi. Grazie a questa procedura sono state trovate tutte le mitigazioni necessarie ad affrontare le situazioni critiche a cui il sistema potrebbe andare incontro. Infatti, tramite l'utilizzo di un canale alternativo per confermare l'esecuzione del comando e l'adozione del protocollo PVS, un operatore è in grado di effettuare tutte le attività di manutenzione in totale sicurezza. Tale analisi, oltre a migliorare le condizioni di sicurezza del sistema, può

anche essere utilizzata in futuro per essere aggiornata e considerata un punto di partenza per effettuare ulteriori analisi ancor più dettagliate.

BIBLIOGRAFIA

[1] IEC - *IEC 60812, "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)"* (Cited on page 15.)

[2] Andrea Bondavalli - *Analisi quantitativa dei Sistemi Critici* (Cited on pages 10 and 15.)

[3] OSHA - *1910.119, "Process safety management of highly hazardous chemicals"* (Cited on pages 15 and 16.)

[4] IEC - *IEC 61882, "hazard and operability studies (HAZOP studies)"* (Cited on pages 3, 16, 17, 20, and 21.)

[5] `http://www.rfi.it/rfi/SICUREZZA-E-INNOVAZIONE/Tecnologie/Apparati-centrali` - *Apparati Centrali* (Cited on page 24.)

[6] A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr - *Basic Concepts and taxonomy of dependable and secure computing* (Cited on pages 9 and 10.)

[7] `https://it.wikipedia.org/wiki/Quadro_luminoso` - *Quadro luminoso* (Cited on page 32.)

[8] `www.econopoly.ilsole24ore.com/2016/10/04/storia-quasi-breve-del-risk-management-nelle-banche/` - *Storia quasi breve del risk management nelle banche* (Cited on page 7.)

[9] Andrea Ceccarelli, Mohamad Gharib, Andrea Bondavalli, Tommaso Zoppi - *Specifica Architettura IMR* (Cited on pages 25 and 30.)

[10] CENELEC - *EN 61025, "Fault tree analysis(FTA)"* (Cited on page 15.)

[11] CENELEC - *EN 50128, "Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems"* (Cited on pages 11, 12, and 62.)

[12] CENELEC - *EN 50159 Railway applications-Communication, signalling and processing systems-Safety-related communication in transmission Part 2 (2001)* (Cited on pages 11 and 61.)

[13] CENELEC - *EN 50126, "Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS* (Cited on pages 3, 10, 11, 12, and 19.)

[14] `http://www.ruleworks.co.uk/riskguide/` - *The Risk Management Guide - A to Z and FAQ Reference* (Cited on page 7.)

[15] IEC - *IEC 61508, "61508 functional safety of electrical/electronic/-programmable electronic safety-related systems"* (Cited on pages 3 and 13.)