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

Tesi di Laurea

TITOLO ITALIANO

TITOLO INGLESE

NOME CANDIDATO

Relatore: *Relatore*
Correlatore: *Correlatore*

Anno Accademico 2018-2019

INDICE

ELENCO DELLE FIGURE

"Inserire citazione"
— Inserire autore citazione

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 è entrata nella nostra vita in modo estremamente intenso, permeando quasi tutti i comportamenti quotidiani e ottenendo un'importanza rilevante anche a livello aziendale, oggi infatti può essere considerata lo strumento più efficace per la creazione di ricchezza economica.
Grazie all'IT le aziende hanno potuto generare vantaggi e sfruttare nuove opportunità. Oggi questi vantaggi e benefici, comprensivi di buone pratiche, applicazioni, funzionalità e infrastrutture, sono alla portata di tutti.
Visto l'importante ruolo assunto dall'IT, nasce l'esigenza di preservare tali sistemi dai danni inerenti l'integrità, la disponibilità e la confidenzialità delle informazioni in essi custodite.
A questa necessità fa capo l'*hazard analysis*, o analisi dei rischi, un processo di valutazione delle criticità inerenti un sistema informatico.
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]
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.
Non è possibile individuare un comportamento umano o un'attività na-

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

1.1 GESTIONE DEI RISCHI NEI SISTEMI INFORMATICI

I sistemi informatici complessi vengono adoperati sempre più frequentemente per svolgere compiti altamente critici, che coinvolgono la sicurezza e l'incolumità delle persone. Si pensi per esempio ai sistemi di controllo di aerei, delle centrali nucleari, dei sistemi ferroviari o anche solo ai sistemi di transazioni monetarie. 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.[10] 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.

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 safety, 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. [2] 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.[11]

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.
- EN50128: relativa allo sviluppo di software per applicazioni di sistema.
- EN50129: inerente allo sviluppo di apparecchiature elettriche/elettroniche di sicurezza per il segnalamento ferroviario.

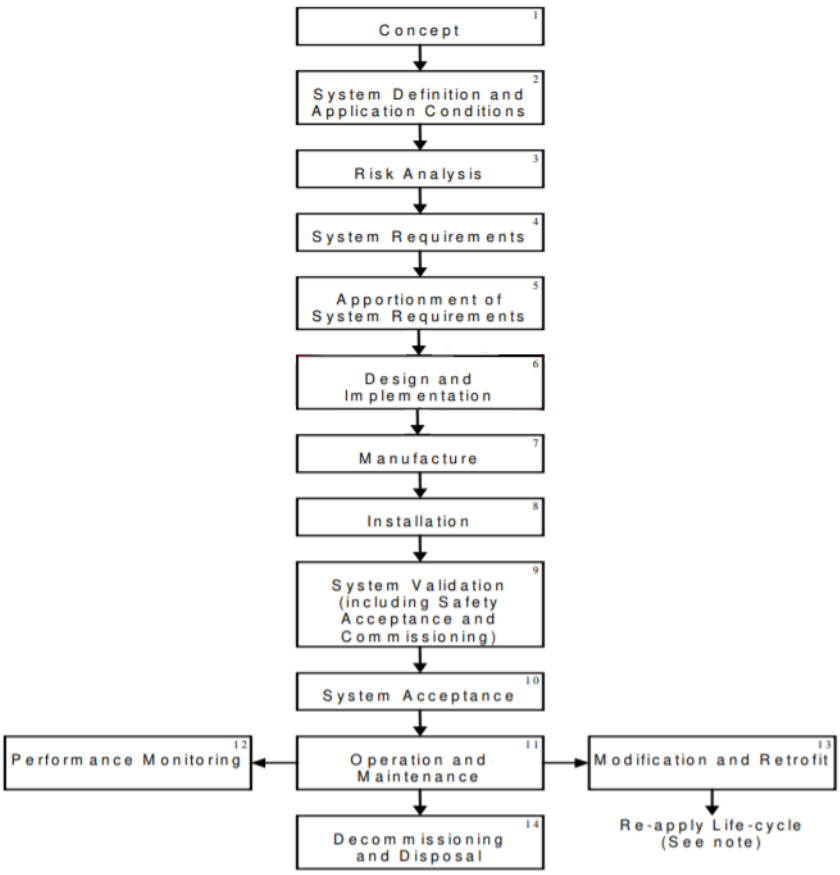


Figura 1: Diagramma EN 50 126

- EN50121: riguarda le relazioni tra i sistemi ferroviari ed il mondo esterno, con particolare riguardo alla compatibilità elettromagnetica.
- EN50155: inerente le condizioni del materiale elettico utilizzato nelle fasi di sviluppo, costruzione e testing.

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.
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.
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'analisi dei rischi, 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. [11]

2

L'ANALISI DEI RISCHI

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:

- **Checklists**: lista di voci che occorre controllare e spuntare per verificare che una determinata serie di operazioni sia stata eseguita correttamente;
- **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; [1]
- **Fault Tree Analysis**: 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. [2]
- **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;
- **HAZOP**: esercizio che si svolge attraverso la formulazione di alcune specifiche domande strutturate; è finalizzato all'individuazione di deviazioni dagli intenti di progetto che possono portare ad inconvenienti di sicurezza o di esercizio. [3]

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, tale tecnica verrà descritta e approfondita successivamente.
Nella seguenti tesi verrà esposta l'hazard analysis dell'apparato IMR di RFI per la manutenzione delle varie linee ferroviarie.
L'obiettivo del lavoro è quello di individuare tutti i potenziali pericoli, sia quelli essenzialmente rilevanti per l'area immediata del sistema, sia quelli con una sfera di influenza più ampia.
Per effettuare tale lavoro è stata utilizzata la strategia **HAZOP** (**HAZ**ard and **OP**erability analysis); 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 *analisi dei rischi* viene sinteticamente utilizzata per indicare un processo che in pratica comprende 4 fasi:

- *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;

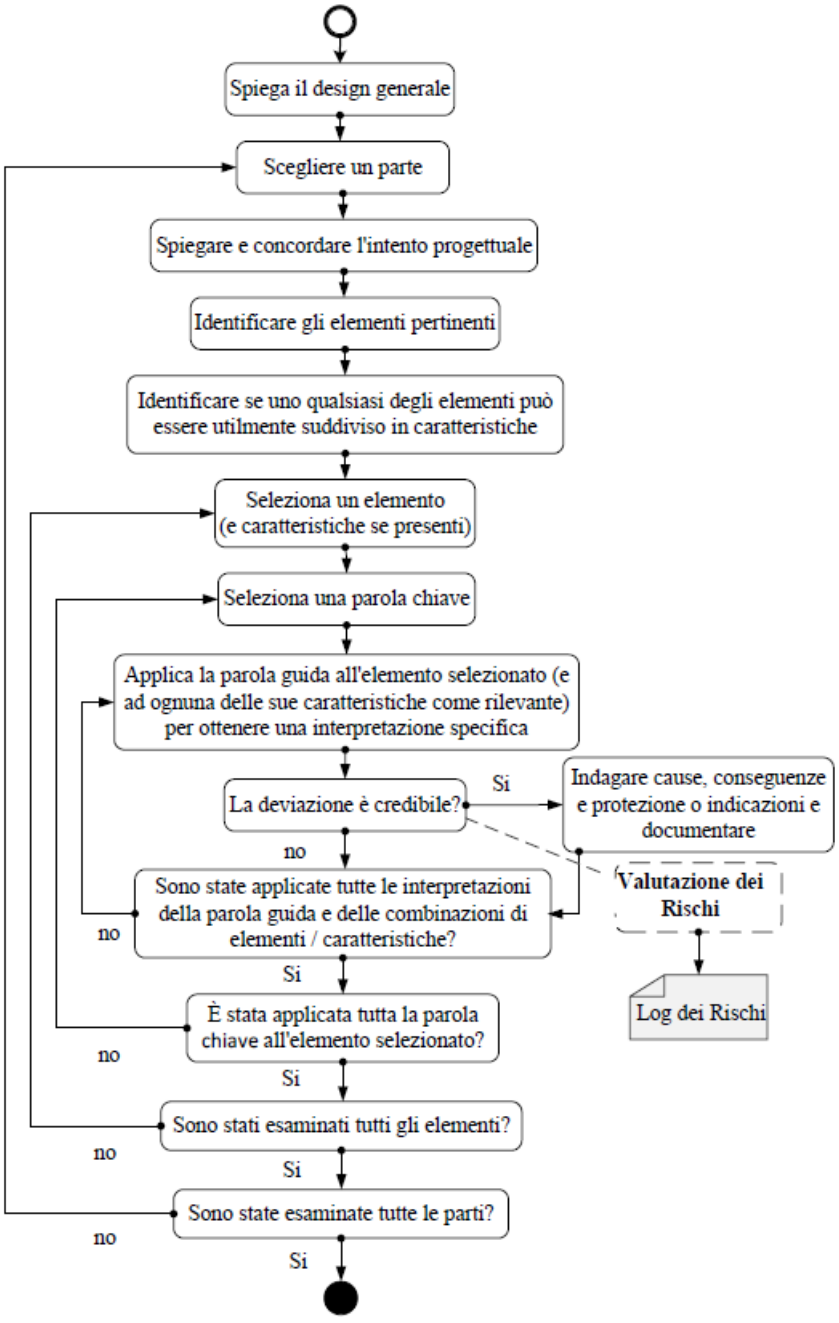
- *Preparazione*: questa fase ha lo scopo di ottenere le informazioni necessarie per effettuare l'analisi e di convertire tali informazioni in un formato adatto. In seguito deve essere riportata una descrizione del progetto contenente tutti i dettagli tecnici e amministrativi necessari. Devono essere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

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

- *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. Di seguito viene riportato il diagramma di flusso della procedura appena descritta:



- *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.

2.0.1 *Il processo per la valutazione del rischio*

Come precedentemente anticipato nella fase di esaminazione è opportuno effettuare una valutazione del rischio riscontrato.
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

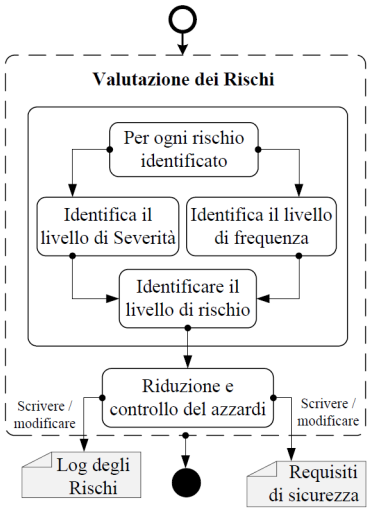


Figura 2: Il processo per la valutazione dei rischi

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 3: Tabella per la classificazione delle frequenze

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 4: Tabella per la classificazione della severità

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 5: Risk Matrix

3

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; prima di introdurre la descrizione di tale apparato, 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].

3.1 APPARATI CENTRALI

Un ruolo fondamentale per eseguire le operazioni di manutenzione della linea è costituito dagli apparati centrali. Infatti, 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 effettuare le operazioni correttive necessarie in caso di guasto in tempi notevolmente ridotti rispetto alla soluzione elettromeccanica utilizzata precedentemente. [5]

3.2 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

Figura 6: Apparati centrali

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.

3.3 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.

3.3.1 *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

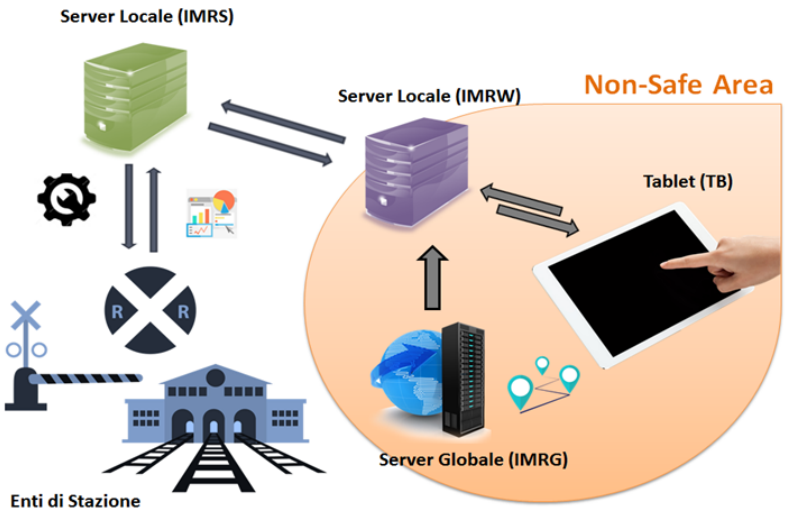


Figura 7: Architettura IMR

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.

3.3.2 *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.

3.3.3 *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.

3.3.4 *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.

3.4 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.

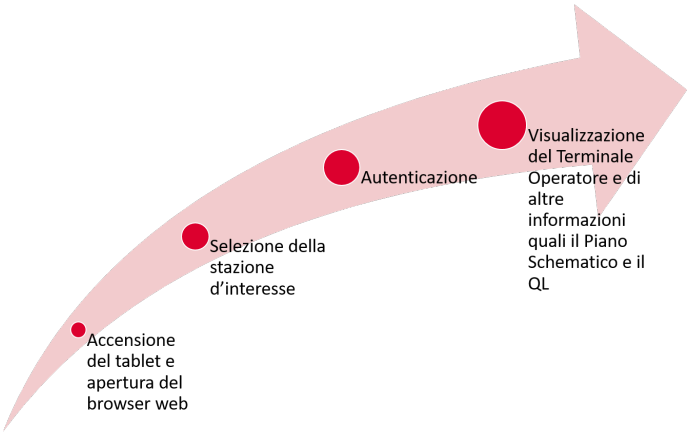


Figura 8: Procedura di Connessione

3.4.1 *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
- 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,

Figura 9: Icone del Terminale 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.

3.4.2 *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.) [6]

3.4.3 *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,

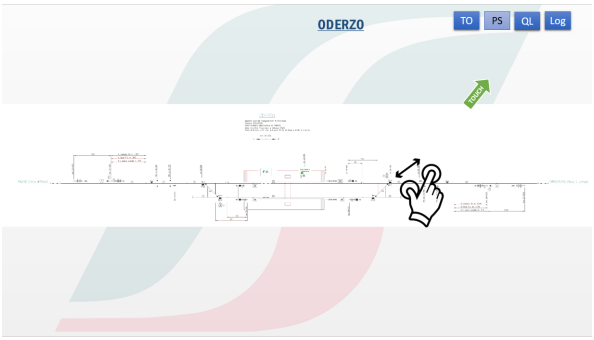


Figura 10: Piano schematico stazione di Oderzo

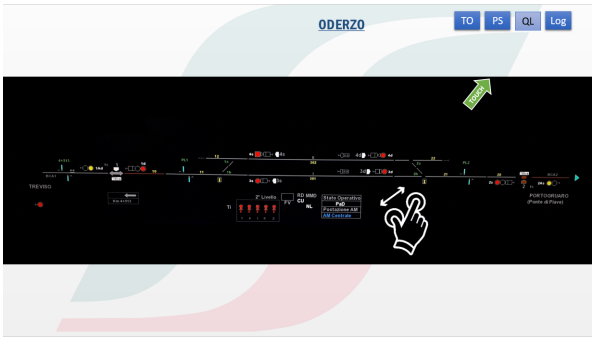


Figura 11: Quadro luminoso stazione di Oderzo

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]

4

HAZARD ANALYSIS DELL'APPARATO IMR

In questo capitolo viene riportata l'analisi dei rischi vera e propria. Sono state studiate tutte le situazioni pericolose e i rischi associati e sono state individuate mitigazioni per permettere di ridurre la probabilità di occorrenza degli hazards a un livello accettabile, aumentando la safety del sistema. 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. Se tale procedura evidenzia delle criticità, verranno indagate le rispettive cause e conseguenze.
Per ogni rischio evidenziato verranno riportati 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.

4.1 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 operazioni critiche e in blu i blocchi che descrivono operazioni non critiche.

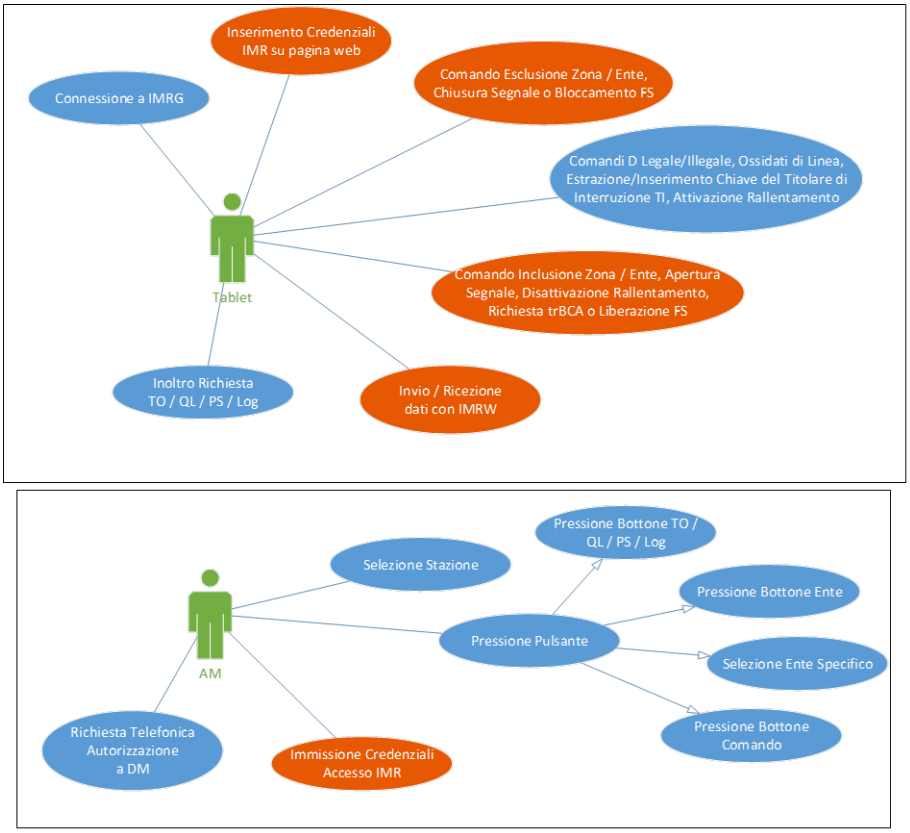


Figura 12: Schema funzionale Tablet Operatore e AM

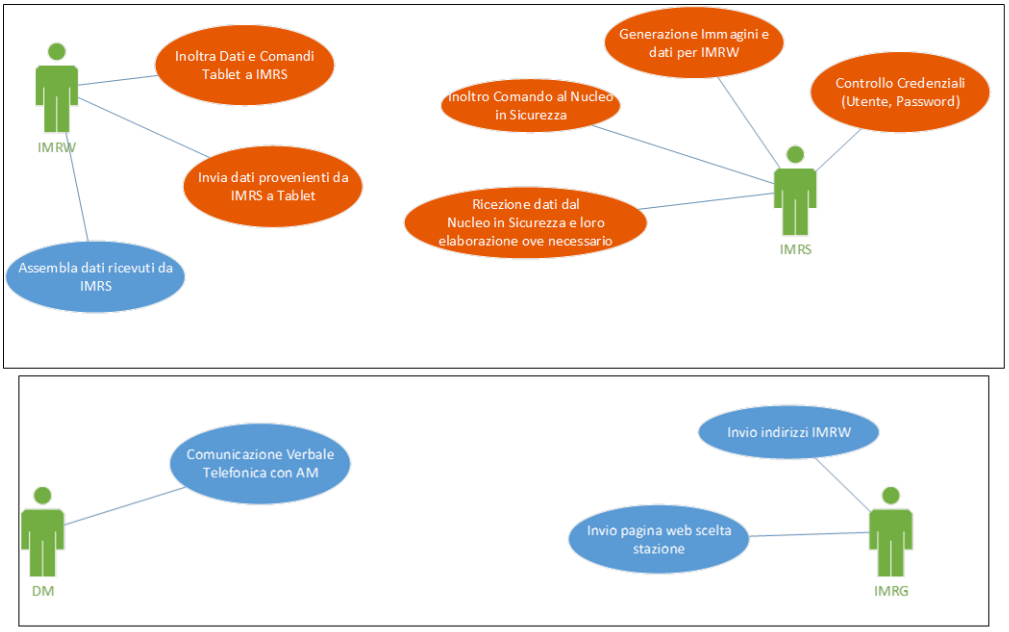


Figura 13: Schema funzionale IMRW, IMRS, DM e IMRG

4.2 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 manutenzione (AM).
Durante questa fase i componenti attivi sono:

- Addetto 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'addetto manutenzione deve effettuare, durante questa fase le credenziali vengono verificate direttamente dal Tablet. Il server IRMG sarà presente solo in

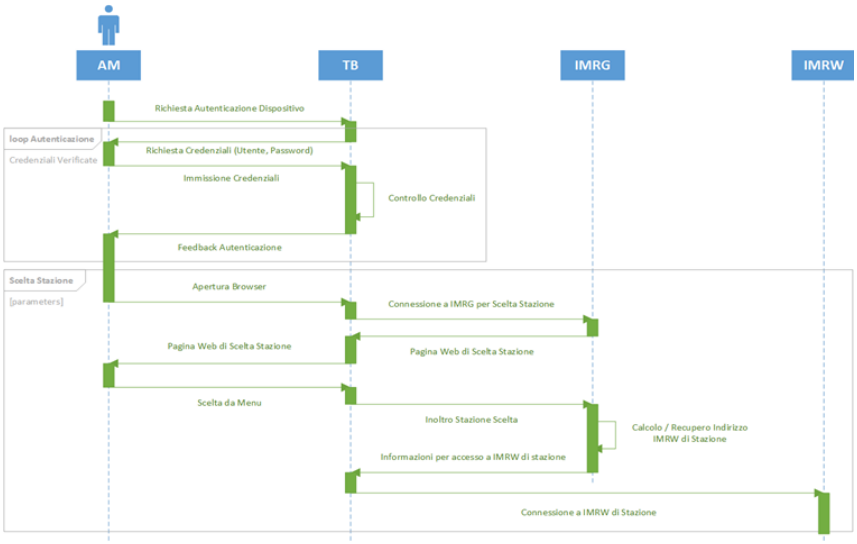


Figura 14: Sequence Diagram prima fase

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'addetto manutenzione.

4.2.1 *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 di suddetti rischi è stata classificata come *insignificante*, in quanto gli azzardi non comportano problemi per la safety. Tra i rischi *intollerabili* individuati in questa sezione del sequence diagram riportiamo il caso in cui l'AM venga reindirizzato su un server che potrebbe offrire un'interfaccia simile a quella attesa offerta da IMRG, 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.

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'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

Figura 15: Sezione hazard analysis prima fase

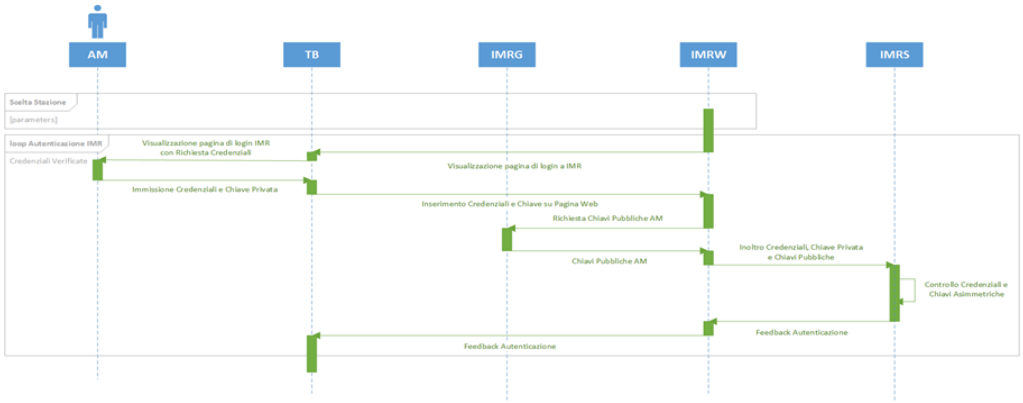


Figura 16: Sequence diagram seconda fase

4.3 LOGIN IMR

Nella fase di autenticazione da parte dell'AM all'apparato IMR intervengono:

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

L'operazione di autenticazione coinvolge praticamente 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.

4.3.1 *Rischi seconda parte*

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 classificato come *tollerabili*.

4.4 VISUALIZZAZIONE TERMINALE OPERATORE (TO)

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

- Addetto manutenzione;

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

Figura 17: Sezione hazard analysis seconda fase

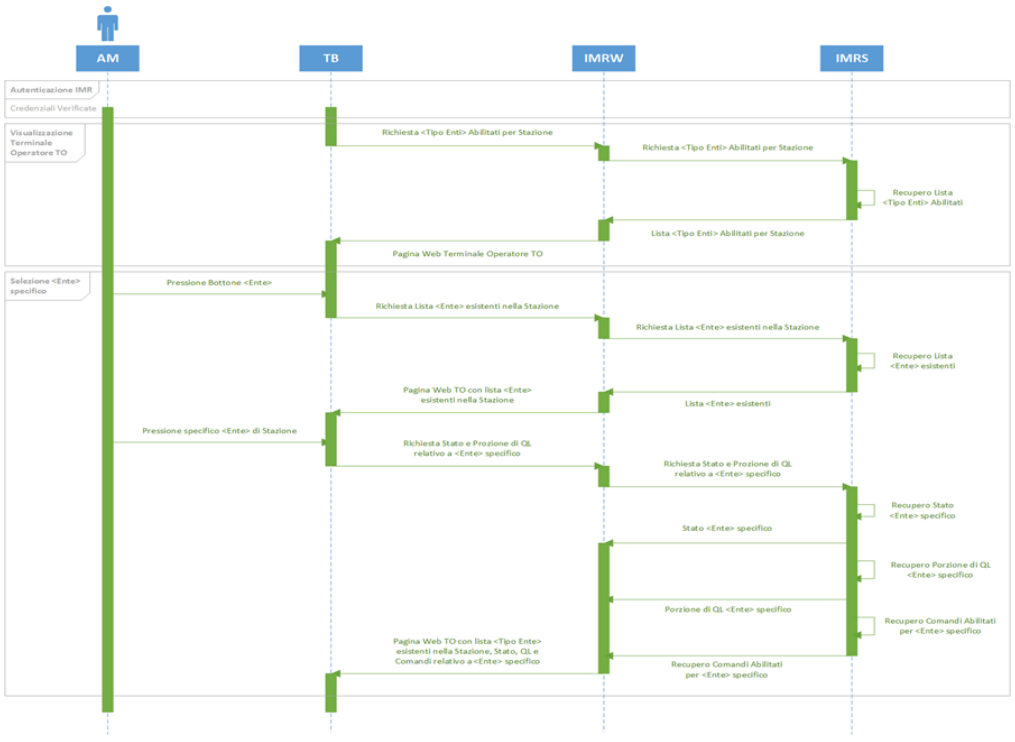


Figura 18: Sequence diagram terza fase

- Tablet;
- Server IRMW;
- Server IMRS.

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'addetto manutenzione può quindi iniziare a inviare i comandi opportuni per le operazioni di manutenzione. L'AM in questa fase è in grado di premere i bottoni 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.

4.4.1 *Rischi terza parte*

4.5 ESECUZIONE COMANDO AM

NON VA BENE IL SEQUENCE DIAGRAM

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

BIBLIOGRAFIA

[1] Wikipedia - *FMEA* (Cited on page 13.)

[2] Andrea Bondavalli - *Analisi quantitativa dei Sistemi Critici* (Cited on pages 9 and 13.)

[3] Wikipedia - *HAZOP* (Cited on pages 13 and 14.)

[4] www.analisideirischinformatici.it - *ANALISI DEI RISCHI INFORMATICI E POLICY SULLA SICUREZZA AZIENDALE*

[5] http://www.rfi.it - *Apparati Centrali* (Cited on page 22.)

[6] http://www-3.unipv.it- *Circolazione ed Impianti di Sicurezza e Segnalamento* (Cited on page 28.)

[7] Wikipedia - *Quadro luminoso* (Cited on page 29.)

[8] IlSole24Ore - *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 22 and 27.)

[10] Wikipedia - *Dependability* (Cited on page 8.)

[11] Lorenzo Falai - *Certification of Critical Systems* (Cited on pages 9 and 11.)