ISARail

LA GESTIONE DEL RISCHIO IN AMBITO FERROVIARIO

Ingegner
Antonio Masucci

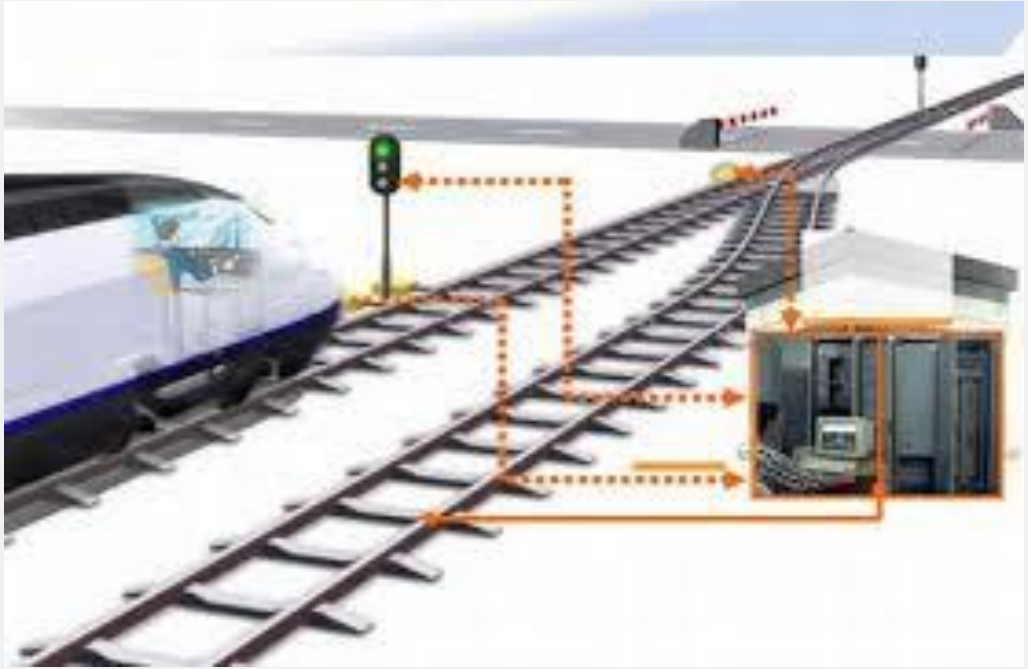
ISARail – Technical Director

La conseguenza di una informazione corrotta

La conseguenza di una informazione corrotta

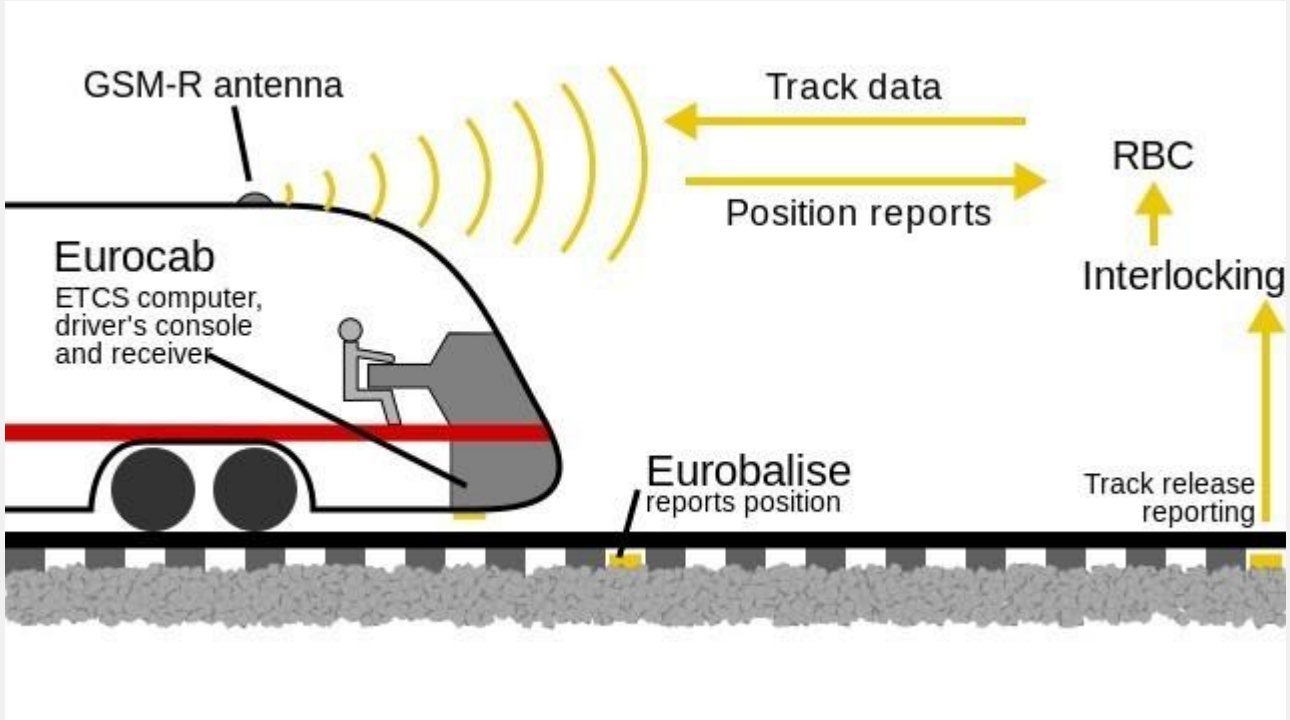
I SISTEMI DI SICUREZZA – Segnalamento Ferroviario

Comunicazione con sistema di trasmissione chiuso



I SISTEMI DI SICUREZZA – Segnalamento Ferroviario

Comunicazione con sistema di trasmissione aperto



NORME DI RIFERIMENTO – ANTE DIRETTIVA SICUREZZA

Norme Cenelec:

- EN 50126 Applicazioni ferroviarie, tranviarie, filotranviarie, metropolitane
  La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS) 2000-03

- Sistemi di telecomunicazione, segnalamento ed elaborazione - Software per sistemi ferroviari di comando e di protezione 2002-04

- EN 50129 Applicazioni ferroviarie, tranviarie, filotranviarie, metropolitane
  Sistemi elettronici di sicurezza per il segnalamento 2000-04

LA SICUREZZA DELLE FERROVIE

I livelli di sicurezza del sistema ferroviario dell'Unione sono generalmente elevati. La sicurezza ferroviaria deve essere mantenuta e continuamente migliorata tenendo conto del **progresso tecnico e scientifico** e dello sviluppo del diritto dell'Unione e internazionale, e **dell'impatto del fattore umano**

Il parlamento Europeo ha istituito un **quadro normativo comune per la sicurezza delle ferrovie** armonizzando il contenuto delle norme di sicurezza, la certificazione di sicurezza delle imprese ferroviarie, le funzioni e il ruolo delle autorità nazionali preposte alla sicurezza:

DIRETTIVA (UE) 2016/798 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO dell'11 maggio 2016 sulla sicurezza delle ferrovie

LA DIRETTIVA SICUREZZA E IL CONTROLLO DEL RISCHIO

I principali attori nel sistema ferroviario dell'Unione, i gestori dell'infrastruttura e le imprese ferroviarie, devono assumere piena responsabilità per la sicurezza della propria parte del sistema.
Ogniqualvolta appropriato, essi dovrebbero cooperare nell'attuare le misure di controllo del rischio.

A tal fine ciascuna attore deve applicare i metodi descritti nei metodi comuni di sicurezza (common safety methods - CSM):

- metodo armonizzato in materia di monitoraggio,
- metodo armonizzato in materia di valutazione della conformità
- metodo armonizzato in materia di ***controllo e valutazione del rischio***

Metodo armonizzato in materia di controllo e valutazione del rischio

REGOLAMENTO DI ESECUZIONE (UE) **N. 402/2013**
DELLA COMMISSIONE del 30 aprile 2013
relativo al metodo
comune di sicurezza per la determinazione e valutazione dei rischi
e
che abroga il regolamento (CE) n. 352/2009

«metodi comuni di sicurezza» (CSM): i metodi che descrivono la valutazione dei livelli di sicurezza, la realizzazione degli obiettivi di sicurezza e la conformità con gli altri requisiti in materia di sicurezza

REGOLAMENTO DI ESECUZIONE (UE) N. 402/2013 - Gestione del Rischio

L'allegato I dettaglia il modo in cui debba essere sviluppato il procedimento di gestione dei rischi.

Il procedimento di gestione comprende:

•Il procedimento di valutazione dei rischi finalizzato ad individuare gli eventi pericolosi, i rischi, le corrispondenti misure di sicurezza e i requisiti di sicurezza risultanti che il sistema da valutare deve soddisfare;

•La dimostrazione della conformità del sistema ai requisiti di sicurezza individuati;

•Gestione di tutti gli eventi pericolosi individuati e misure di sicurezza corrispondenti.

REGOLAMENTO DI ESECUZIONE (UE) N. 402/2013 - Procedimento di valutazione dei rischi

Nell'ambito del procedimento di valutazione dei rischi si procede seguendo gli step sotto elencati:

•definizione del sistema;
•definizione della metodologia dell'analisi del rischio;
•definizione dei criteri di accettazione del rischio;
•definizione delle proprietà degli eventi pericolosi che consiste nella identificazione e definizione di tutti gli elementi caratterizzanti gli eventi pericolosi;
•analisi del sistema;
•determinazione dei rischi;
•individuazione delle azioni mitigative;
•ripetizione della determinazione dei rischi (a seconda del criterio di accettazione dei rischi adottato);
definizione dei requisiti di sicurezza del sistema

REGOLAMENTO DI ESECUZIONE (UE) N. 402/2013 - STIMA DEL RISCHIO

Il regolamento 402 [4] prescrive che per ogni evento pericoloso venga stimato il rischio attraverso:

- la stima della frequenza di accadimento dell'evento pericoloso;
- analisi e classificazione delle conseguenze;
- combinazione dei due fattori sopra elencati e classificazione del rischio.

Il 402 prescrive che dopo la stima del rischio debba seguire la determinazione del rischio atta a determinare il livello di accettabilità del rischio.

A tal fine l'analisi dei rischi per ogni evento pericoloso considera due fasi:

- valutazione iniziale del rischio;
- valutazione finale del rischio.

Il primo rappresenta il livello di rischio al tempo in cui la situazione pericolosa viene identificata,
il secondo rappresenta il livello di rischio dopo che azioni mitigative sono state messe in atto.

ISARail group
TRUST IN SKILL • INDEPENDENCE • IMPARTIALITY • INTEGRITY

REGOLAMENTO DI ESECUZIONE (UE) N. 402/2013 - Criteri di accettazione dei rischi

L'accettabilità dei rischi del sistema da valutare viene determinata sulla base di uno o più dei seguenti criteri di accettazione del rischio:

a) applicazione di codici di buona pratica
b) confronto con sistemi analoghi;
c) stima accurata dei rischi.

I rischi associati agli eventi pericolosi disciplinati dal **sistema di riferimento** si considerano accettabili

Se uno o più eventi pericolosi individuati sono controllati da **codici di buona pratica**, i rischi ad essi associati devono considerarsi accettabili.

Ciò implica che:

a) non è necessario analizzare ulteriormente tali rischi;
b) l'applicazione dei codici di buona pratica come il sistema di riferiemto deve essere annotata nel registro degli eventi pericolosi come requisito di sicurezza per gli eventi pericolosi di cui trattasi.

Gestione del Rischio: Dall'analisi delle modifiche di sistema allo sviluppo di sistemi

EN 50126-1 Applicazioni ferroviarie – La specificazione e la dimostrazione di affidabilità, disponibilità, manutenibilità e sicurezza (RAMS) – parte 1: Processo generale RAMS - **2017**

EN 50128 Applicazioni ferroviarie — Sistemi di comunicazione, segnalamento e trattamento - Software per sistemi di controllo e protezione ferroviari – **2011**

EN 50129 Applicazioni ferroviarie — Sistemi di comunicazione, segnalamento e trattamento — Sistemi elettronici riguardanti la sicurezza per il segnalamento – **2018**

EN 50126-2 Applicazioni ferroviarie – La specificazione e la dimostrazione di affidabilità, disponibilità, manutenibilità e sicurezza (RAMS) – parte 1: Approccio di sistema per la sicurezza - **2017**

Gestione del Rischio e CENELEC.

EN 50126-1 - § 6.3 Risk Assessment

If the risk analysis identified cases with risk "broadly acceptable", there is no need to specify further requirements for those cases.

If the risk analysis concluded that a risk is not "broadly acceptable", the risk analysis activity shall be continued by choosing and applying a 'risk acceptance principle' (RAP), before applying risk evaluation. The three risk acceptance principles are:

a) use of Code of Practice (CoP);

b) comparison with a similar system as a reference;

c) Explicit risk estimation (ERE) (qualitative or quantitative).

Once the RAP has been chosen and applied, the process continues with the risk evaluation (determing the achievement of the criteria associated to the selected RAP) and the specification of safety requirements.

The tolerable safety risk of a railway system is dependent upon the risk acceptance criteria (RAC) set by the legal framework, or by the railway duty holder in accordance with the rules given by legal framework.

NOTE 3 Details for safety, including specification of basic integrity and safety integrity, is provided in EN 50126-2.

Gestione del Rischio e CENELEC.

EN 50126-2 - § 8 Risk Assessment

8 Risk assessment

8.1 Introduction

The core part of the Risk assessment (i.e. analysis and evaluation) is performed at phase 3 of the life-cycle and continued as appropriate through the system life-cycle. This clause describes:

- Sub-clause 8.2: Risk analysis with identification of the hazards and their consequences;
- Sub-clause 8.3: Selection of risk acceptance principles, related acceptance criteria and risk evaluation. Risk acceptance principles are;
  - o Use of Code of Practice;
  - o Use of a reference system;
  - o Use of Explicit Risk Estimation.
- Sub-clause 8.4: Application of explicit risk estimation

The risk assessment process can be described as several tasks such as Risk Analysis, Hazard Identification, Consequence Analysis, Risk Evaluation, Selection of Risk Acceptance Principles.

8.2 Risk Analysis

8.2.1 General

Initially, the analysis is performed qualitatively, identifying all contributing factors and their combination without quantification.

The risk analysis process is an iterative process. It shall start with the definition of the system under consideration. Then the hazards, the risks, the associated safety measures, and the resulting safety requirements for the system under consideration shall be identified.

Consequence analysis, see 8.2.3, involves gathering and documenting data that describe the effects of a hazard. The recommended approach is to use accident data, wherever available, and/or to consult experts on the environment related to the system or process under consideration (i.e. "domain experts").

8.2.2 The risk model

Where needed to support hazard identification, hazard classification and the selected risk acceptance principles a risk model should be defined. Causes, hazards and accidents stand in a many-to-many relationship, such as:

Reg. 402/2013 – Organismo di Valutazione del Rischio.

Articolo 6

Valutazione indipendente

1. Un organismo di valutazione effettua una valutazione indipendente dell'adeguatezza dell'applicazione del procedimento di gestione dei rischi di cui all'allegato I e dei relativi risultati. L'organismo di valutazione in questione deve soddisfare i criteri di cui all'allegato II. Se l'organismo di valutazione non è già designato dalla legislazione unionale o nazionale vigente, il proponente designa il più rapidamente possibile nel corso del procedimento di valutazione il proprio organismo di valutazione.

2. Per svolgere la valutazione indipendente, l'organismo di valutazione:

a) si assicura di disporre di una conoscenza approfondita della modifica rilevante sulla base della documentazione fornita dal proponente;

b) effettua una valutazione dei procedimenti applicati per gestire la sicurezza e la qualità nelle fasi di progettazione e attuazione della modifica rilevante, se tali procedimenti non sono già certificati da un organismo di valutazione della conformità pertinente;

c) effettuare una valutazione dell'applicazione di tali procedimenti di qualità e di sicurezza in fase di progettazione e attuazione delle modifiche rilevanti.

Dopo aver completato la sua valutazione in conformità alle lettere a), b) e c), l'organismo di valutazione elabora il rapporto di valutazione della sicurezza di cui all'articolo 15 e all'allegato III.

Reg. 402/2013 – Organismo di Valutazione del Rischio.

Articolo 7

Accreditamento/riconoscimento dell'organismo di valutazione

L'organismo di valutazione di cui all'articolo 6 è:

a) accreditato dall'organismo nazionale di accreditamento di cui all'articolo 13, paragrafo 1, in base ai criteri definiti nell'allegato II; oppure

b) riconosciuto dall'organismo di riconoscimento di cui all'articolo 13, paragrafo 1, in base ai criteri definiti nell'allegato II; oppure

c) l'autorità nazionale preposta alla sicurezza ai sensi del disposto dell'articolo 9, paragrafo 2.

Organismo di Valutazione del Rischio - ISARail.

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual Recognition Agreements

ilac-MRA

Allegato 1 al Certificato di accreditamento n° 065E Rev. 08
Enclosure 1 to the accreditation Certificate n° 065E Rev. 08

rilasciato a / *issued to:* **ISARail S.p.A.**

Ispezione di Tipo A nei seguenti settori:

- Regolamento di Esecuzione (UE) n. 402/2013 Metodo Comune di sicurezza per la determinazione e valutazione dei rischi (Sede di Via Gorizia 1, 80033 Cicciano - NA) (vedere l'Allegato 2 al Certificato)

Inspection of Type A in the following sectors:

- *Commission Implementing Regulation (EU) n. 402/2013 Common safety method for risk evaluation and assessment (Headquarters in Via Gorizia 1, 80033 Cicciano - NA) (see the Enclosure 2 to the Certificate)*

Organismo di Valutazione del Rischio - ISARail.

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual Recognition Agreements

ilac-MRA

Allegato 2 al Certificato di accreditamento n° 065E Rev. 08
Enclosure 2 to the accreditation Certificate n° 065E Rev. 08

rilasciato a / *issued to:* **ISARail S.p.A.**

Aggiornato in data: 08-11-2019

Regolamento di Esecuzione (UE) n. 402/2013 Metodo Comune di sicurezza per la determinazione e valutazione dei rischi
Organismo di valutazione del procedimento di gestione dei rischi ("AsBo"), nei seguenti ambiti:

1. Sottosistemi strutturali
   - Materiale rotabile
   - Infrastrutture
   - Controllo-comando e segnalamento a terra
   - Controllo-comando e segnalamento a bordo
   - Energia
2. Sottosistemi funzionali e settori
   - Esercizio e gestione del traffico
   - Manutenzione

e alla loro integrazione in sicurezza nel sistema ferroviario.

Riferimenti a norme e specifiche:
Decisioni della Commissione Europea "Specifiche Tecniche di Interoperabilità (STI)" applicabili al sistema ferroviario transeuropeo ad alta velocità e convenzionale;
Decreti e Linee Guida dell'Agenzia Nazionale per la Sicurezza delle Ferrovie italiana (ANSF);
EN 50126 (IEC 62278) – RAMS;
EN 50128 (IEC 62279) – Software;
EN 50129 (IEC 62425) – Sistemi di sicurezza.

Gestione del Rischio in Ambito Ferroviario – Code of Practice

Allegato I al REGOLAMENTO DI ESECUZIONE (UE) **N. 402/2013** DELLA COMMISSIONE del 30 aprile 2013 relativo al metodo comune di sicurezza per la determinazione e valutazione dei rischi e che abroga il regolamento (CE) n. 352/2009

Valutazione indipendente dell'adeguatezza dell'applicazione del procedimento di gestione dei rischi impiegato e dei relativi da parte di un organismo di valutazione del rischio .

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

2.1. Misura e visualizzazione della velocità (tachimetro) - controllo della velocità massima dei movimenti di manovra

La funzionalità “Controllo della velocità massima dei movimenti di manovra” viene descritta al § 11.3 dell’allegato al succitato decreto ANSF 1/2015.

Req_Fun_VM_04. Il sistema deve limitare la velocità massima della locomotiva a 30 km/h.

Req_Fun_VM_05. Il sistema deve prevedere un dispositivo per fornire un allarme sonoro.

Req_Fun_VM_06. Il sistema deve rilevare quando la velocità della locomotiva eccede la velocità massima di un valore compreso tra 2 e 5 km/h (in particolare che la velocità della locomotiva sia compresa tra 32 e 35 km/h).

Req_Fun_VM_07. Quando il sistema rileva che la velocità della locomotiva eccede la velocità massima di un valore compreso tra 2 e 5 km/h (in particolare che la velocità della locomotiva sia compresa tra 32 e 35 km/h) allora deve:

- attivare il dispositivo per fornire un allarme sonoro.
- attivare un timer di 5 secondi;
- porsi in attesa che la velocità della locomotiva scenda al di sotto della velocità massima di 30 km/h.

Req_Fun_VM_08. Quando il sistema rileva:

- O cheè scaduto il timer di 5 secondi;
- O che la velocità della locomotiva eccede la velocità massima di oltre 5 km/h (in particolare supera i 35 km/h)

Deve:

- provvedere al taglio della trazione;
- provocare la frenatura di emergenza fino all’arresto della locomotiva.

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

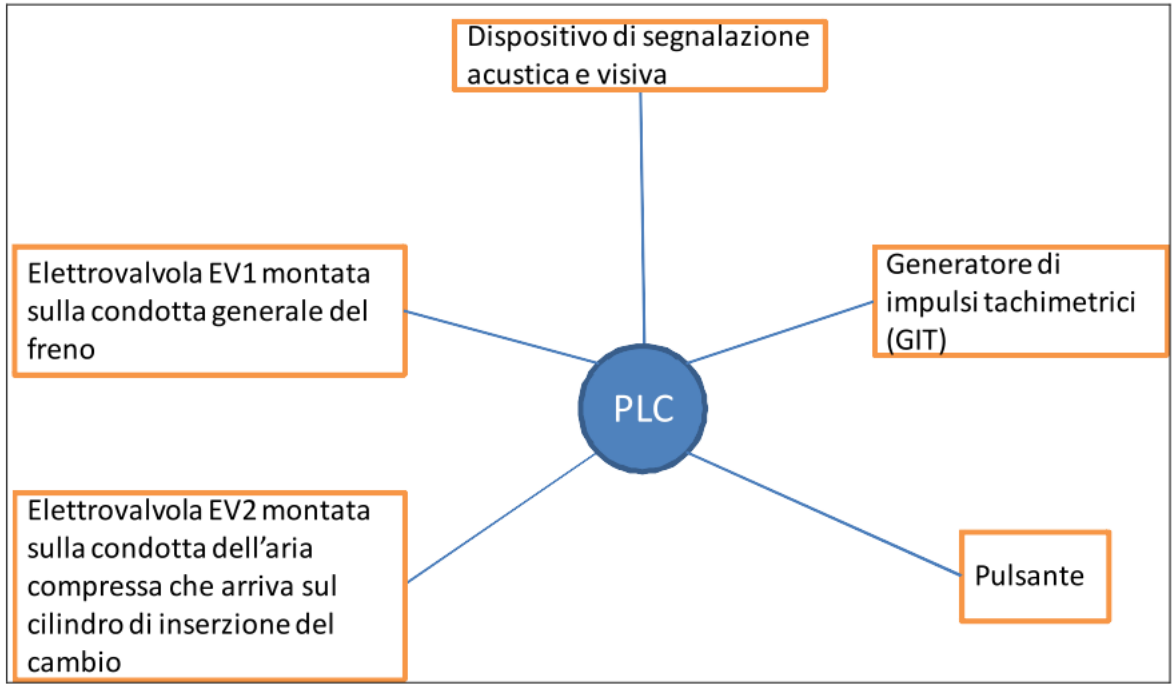


Figura 1: Schema di principio dell'architettura HW del dispositivo di sicurezza

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 4: Definizione del Sistema

Aspetti inerenti la definizione del sistema	Sistema di sicurezza dei movimenti di manovra
a) gli obiettivi del sistema (finalità prevista);	Il sistema deve implementare le funzione di sicurezza: • Supero velocità massima; • Controllo Atto Partenza; • Controllo Vigilante, • Registrazione eventi; descritte al § 11 dell'allegato al decreto ANSF 1/2015.
b) le funzioni e gli elementi del sistema, se del caso (compresi, tra gli altri, elementi umani, tecnici ed operativi);	Il sistema deve implementare le funzione di sicurezza descritte al § 11 dell'allegato al decreto ANSF 1/2015. Per la descrizione del sistema si rimanda al capi tolo.
c) la delimitazione del sistema, anche in riferimento ai sistemi che interagiscono con esso;	Il sistema deve essere istallato sulle locomotive da manovra il cui impiego é limitato nell'ambito delle località di servizio del Sistema Ferroviario Italiano. Il sistema comprende i componenti illustrati in Figura 1. Di seguito si riporta l'elenco dei componenti e la rispettiva ubicazione sulla locomotiva: • PLC (nel quadro elettrico); • Elettrovalvola EV1 (sulla condotta generale del freno); • Elettrovalvola EV2 (sulla condotta dell'aria compressa collegata al cilindro di inserzione del cambio); • Generatore di impulsi tachimetrici (sull'asse lato corpo boccola); • Dispositivo di segnalazione acustica/visiva (in cabina di guida in prossimità del banco di guida); • Pulsante per l'azione di riconoscimento da parte del personale di manovra (sul banco di guida).

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

d) punti d'interazione materiali (sistemi che interagiscono) e funzionali (input ed output funzionali);	Per svolgere le funzioni previste, il sistema si interfaccia con i seguenti componenti della locomotiva: • Impianto del freno (condotta generale); • pacco batterie (per la tensione di alimentazione); • rodiggio (asse lato corpo boccola); • cambio (cilindro di inserzione); • banco di guida; • sistema di avviamento del motore.
e) le condizioni ambientali del sistema (ad esempio, flusso termico ed energetico, urti, vibrazioni, interferenze elettromagnetiche, utilizzo operativo);	Il sistema deve essere istallato sulle locomotive da manovra il cui impiego é limitato nell'ambito delle località di servizio del Sistema Ferroviario Italiano.
f) le misure di sicurezza esistenti e, previe le necessarie iterazioni, la definizione dei requisiti di sicurezza individuati nel corso del procedimento di valutazione dei rischi;	Il sistema per assolvere la sua funzione prevede una unità centrale costituita da un PLC (programmable logic controller) ampiamente usato in ambito industriale e ferroviario. Il PLC viene programmato attraverso i diagrammi Ladder il quale è un linguaggio di programmazione di tipo grafico. I linguaggi di tipo grafico sono raccomandati dalla norma EN 50128 [5] (vedi § 8.4.4.1) per la produzione del codice sorgente degli algoritmi applicativi. LI Ladder figura tra i linguaggi grafici raccomandati dalla succitata norma EN 50128[5] (vedi Tabella A.16).

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

	Il sistema, per assolvere la sua funzione, deve monitorare la velocità della locomotiva. Per il rilievo della velocità viene impiegato un GIT (generatore di impulsi tachimetrici) montato all'estremità del fusello di uno degli assi della locomotiva. In ambito ferroviario il GIT, montato sul fusello dell'asse, è ampiamente utilizzato per il rilievo della velocità del rotabile. Il sistema per assolvere la sua funzione utilizza delle elettrovalvole monitorate ed attivate dal PLC. L'implementazione della funzione avviene con il ricorso alla logica negata ovvero le elettrovalvole sono normalmente aperte e quando alimentate si chiudono. La logica negata viene ampiamente utilizzata per la sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza. I componenti del sistema sono alimentati in tensione continua di 24 V e tali da non generare induzione elettromagnetica. Per i requisiti di sicurezza derivanti dall'analisi del rischio si rimanda al § 5.4.
g) le ipotesi che determinano i limiti della valutazione dei rischi.	Un sistema analogo a quello cui il presente documento si riferisce è già stato implementato e istallato sulle locomotive da manovra a partire dal 2010. Tuttavia per tale analogo sistema non risulta documentazione relativa al monitoraggio dell'esercizio che potrebbe fornire dati per la stima accurata dei rischi di tipo quantitativo o dimostrare nella pratica che il sistema garantisce un livello di sicurezza accettabile. In considerazione di ciò e dell'ambito di applicazione del sistema, la stima del rischio viene implementata sotto il profilo qualitativo.

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

L'analisi viene svolta attraverso l'utilizzo della tecnica FMEA: a partire dalla architettura di base descritta al §4 vengono individuati i modi di guasti dei componenti e valutate le ripercussioni di detti guasti sul funzionamento del dispositivo di sicurezza complessivo.
La FMEA viene eseguita compilando una tabella contenete le colonne i cui campi sono descritti in Tabella 5.

Tabella 5: Descrizione delle colonne della tabella FMEA

Nome del campo	Descrizione
FMEA ID	Stringa alfa numerica, assegnata per scopi di tracciabilità, avente il formato A_##, dove A coincide con l'identificativo del componente/funzione e ## è un numero a due cifre che conta i modi di guasti per lo specifico componente/funzione.
ID del Componente/Funzione	Sigla che individua il componente/funzione analizzato/a
Modo di guasto	Descrizione del modo di guasto del componente analizzato
Causa di guasto	Descrizione della causa che può generare il modo di guasto
Effetto locale	L'impatto del modo di guasto sul funzionamento, funzione o lo stato del componente/funzione analizzato. Gli effetti locali sono registrati quando diversi dai modi di guasto.
Effetto finale	Effetto sul funzionamento del sistema del modo di guasto individuato per il componente/funzione sotto analisi.
Severità	Classificazione della severità degli effetti finali. La classificazione è quella utilizzata anche per gli eventi pericolosi e definita in Tabella 2.

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 6: Lista dei modi di guasto

FMEA ID	ID del Componente	Modo di guasto	Causa di guasto	Effetto locale	Effetto finale	Severità
GIT_01	GIT	Il Git fornisce al PLC un segnale corrispondente alla velocità nulla quando il locomotore da fermo incomincia a muoversi. Il PLC considera il locomotore fermo.	GIT rotto		Il treno si muove senza essere controllato dal personale di manovra e non viene arrestato dal dispositivo di sicurezza.	Catastrofico
GIT_02	GIT	Il GIT fornisce al PLC un segnale corrispondente ad un valore di velocità inferiore al valore di velocità alla quale il locomotore si sta effettivamente muovendo. Il PLC attribuisce al veicolo una velocità inferiore a quella alla quale il locomotore si sta effettivamente muovendo.	GIT rotto		Il treno si muove ad una velocità superiore al limite consentito e il dispositivo di sicurezza non interviene. La locomotiva può sviare.	Catastrofico
GIT_03	GIT	Il GIT viene staccato, il git è funzionante, il git fornisce il segnale corrispondente alla velocità nulla quando il locomotore da fermo	GIT manomesso		Il treno si muove senza essere controllato dal dispositivo di sicurezza. La locomotiva può muoversi senza essere controllata dal personale	Catastrofico

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 6: Lista dei modi di guasto

FMEA ID	ID del Componente	Modo di guasto	Causa di guasto	Effetto locale	Effetto finale	Severità
GIT_01	GIT	Il Git fornisce al PLC un segnale corrispondente alla velocità nulla quando il locomotore da fermo incomincia a muoversi. Il PLC considera il locomotore fermo.	GIT rotto		Il treno si muove senza essere controllato dal personale di manovra e non viene arrestato dal dispositivo di sicurezza.	Catastrofico
GIT_02	GIT	Il GIT fornisce al PLC un segnale corrispondente ad un valore di velocità inferiore al valore di velocità alla quale il locomotore si sta effettivamente muovendo. Il PLC attribuisce al veicolo una velocità inferiore a quella alla quale il locomotore si sta effettivamente muovendo.	GIT rotto		Il treno si muove ad una velocità superiore al limite consentito e il dispositivo di sicurezza non interviene. La locomotiva può sviare.	Catastrofico
GIT_03	GIT	Il GIT viene staccato, il git è funzionante, il git fornisce il segnale corrispondente alla velocità nulla quando il locomotore da fermo	GIT manomesso		Il treno si muove senza essere controllato dal dispositivo di sicurezza. La locomotiva può muoversi senza essere controllata dal personale	Catastrofico

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

FMEA ID	ID del Componente	Modo di guasto	Causa di guasto	Effetto locale	Effetto finale	Severità
		è in moto sotto la supervisione del personale di condotta.				
Pulsante_02	Pulsante	Il PLC riceve dal pulsante di riconoscimento il segnale corrispondente all'azione di riconoscimento del personale di manovra pur non essendo egli vigile. Il PLC considera che la locomotiva sta passando da ferma a in moto o che è nello stato di moto sotto la supervisione del personale di manovra.	Il pulsante viene pigiato dal corpo del personale di manovra che non è vigile.		Il treno si muove senza essere controllato dal personale di manovra e non viene arrestato dal dispositivo di sicurezza.	Catastrofico
EV2_01	EV2	La Elettrovalvola EV2 non si chiude quando riceve il corrispondente segnale dal PLC. (il PLC toglie tensione)	Elettrovalvola EV2 guasta		Il treno non viene arrestato in tempo in uno dei seguenti casi: • incomincia a muoversi senza essere controllato dal personale di condotta; • si sta muovendo senza che il personale di condotta sia vigile • si sta muovendo ad una velocità	Catastrofico

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 7: Eventi pericolosi e classificazione del rischio

Codice dell'Hazrd	Descrizione dell'Hazard	Causa dell'Hazard	ID del Componente/Funzione	Effetto dell'Hazard	Frequenza	Severità	Livello di rischio
HZ_01	Il Git fornisce al PLC un segnale corrispondente alla velocità nulla quando il locomotore da fermo incomincia a muoversi. Il PLC considera il locomotore fermo.	GIT guasto	GIT	Il treno si muove senza essere controllato dal personale di manovra e non viene arrestato dal dispositivo di sicurezza. La locomotiva può sviare, impattare contro un altro veicolo, investire delle persone.	Remota	Catastrofica	Intollerabile
HZ_02	Il GIT fornisce al PLC un segnale corrispondente ad un valore di velocità inferiore al valore di velocità alla quale il locomotore si sta effettivamente muovendo. Il PLC attribuisce al veicolo una velocità inferiore a quella alla quale il locomotore si sta effettivamente muovendo.	GIT guasto	GIT	Il treno si muove ad una velocità superiore al limite consentito e il dispositivo di sicurezza non interviene. La locomotiva può sviare.	Remota	Catastrofica	Intollerabile
HZ_03	Il GIT viene staccato,	GIT	GIT	Il treno si muove ad una	Probabile	Catastrafica	Intollerabile

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 9: Valutazione del rischio associato agli eventi pericolosi

PROBABILITA'	**LIVELLI DI RISCHIO**			
Frequente				
Probabile				**HZ_15, HZ_03**
Occasionale				
Remoto				**HZ_01, HZ_02, HZ_04, HZ_05, HZ_08, HZ_09, HZ_10,HZ_11**
Improbabile				**HZ_06, HZ_07, HZ_12, HZ_13, HZ_14**
Inverosimile				
	Insignificante	Marginale	Critico	Catastrofico
	GRAVITA'			

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 11: Eventi pericolosi

Codice dell'Hazrd	Descrizione dell'Hazard	Causa dell'Hazard	ID del Componente/Funzione	Effetto dell'Hazard	Frequenza	Severità	Livello di rischio	Mitigazioni	Frequenza finale	Severità finale	Livello di rischio finale
HZ_01	Il Git fornisce al PLC un segnale corrispondente alla velocità nulla quando il locomotore da fermo incomincia a muoversi. Il PLC considera il locomotore fermo.	GIT guasto	GIT	Il treno si muove senza essere controllato dal personale di manovra e non viene arrestato dal dispositivo di sicurezza. La locomotiva può sviare, impattare contro un altro veicolo, investire delle persone.	Remota	Catastrofica	Intollerabile	Impiego di due GIT montati su due assi differenti. Il PLC riceve i segnali provenienti dai due GIT e li confronta per vedere se sono uguali. Se il PLC rileva che i due segnali sono diversi considera i GIT guasti e provoca il taglio trazione e la frenatura della locomotiva e visualizza su interfaccia grafica il messaggio di testo "Arresto per differenza	Inverosimile	Catastrofico	Tollerabile

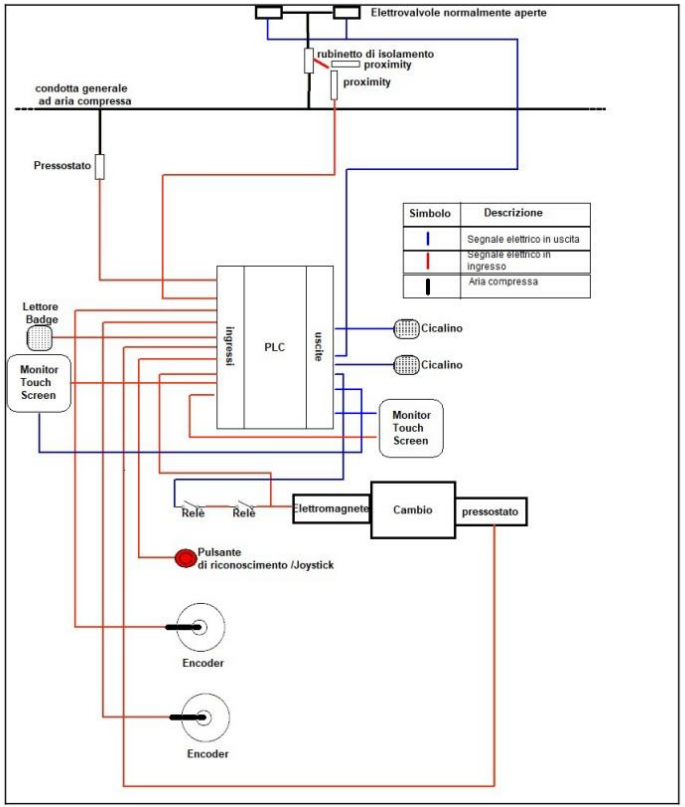
Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Tabella 12: Valutazione del rischio associato agli eventi pericolosi mitigati

PROBABILITA'	**LIVELLI DI RISCHIO**			
Frequente				
Probabile				
Occasionale				
Remoto				
Improbabile				
Inverosimile				**HA_01, HA_02, HA_03, HA_04, HA_05, HA_06, HA_07, HA_08; HA_09, HA_10, HA_12, HA_13, HA_14**
	Insignificante	Marginale	Critico	Catastrofico
	GRAVITA'			

Gestione del Rischio in Ambito Ferroviario – ESEMPIO

Figura 3: Schema componenti HW



THANK YOU

FOR YOUR ATTENTION

ISARail group

TRUST IN SKILL • INDEPENDENCE • IMPARTIALITY • INTEGRITY

Via Gorizia n.1 | IT-80033 | Cicciano (NA) | Italy

www.isarail.com | marketing@isarail.com | antonio.masucci@isarail.com