

TECNICHE DI ANALISI E VALUTAZIONE DEI RISCHI

NEI SISTEMI DI TRASPORTO A GUIDA VINCOLATA

ING. DOMENICO PUGLIESE

OBIETTIVO DEL CORSO

- Analizzare il nuovo approccio normativo per la gestione della sicurezza nei trasporti a guida vincolata
- Introdurre il concetto di Autorizzazione di Sicurezza
- Introdurre il concetto di Sistema di Gestione della Sicurezza
- Introdurre le tecniche di Gestione dei rischi
- Principi generali della EN 50126
- Analisi e valutazione dei rischi secondo il Regolamento UE 402/2013
- Principi del Regolamento 1078/2012 sul monitoraggio continuo
- Criteri di accettabilità dei rischi

NORMATIVA DI RIFERIMENTO NAZIONALE

- decreto-legge 10 settembre 2021, n. 121, convertito con modificazioni in legge 9 novembre 2021, n. 156
- decreto legislativo 14 maggio 2019, n. 50 di recepimento della Direttiva 798/2016 «Direttiva Sicurezza»
- decreto ANSFISA del 28 dicembre 2023 - Disciplina dei requisiti per il rilascio dell'autorizzazione di sicurezza relativa ai sistemi di trasporto pubblico a guida vincolata, ai sensi dell'articolo 6, comma 1, lettera b), del decreto-legge 10 settembre 2021, n. 121, convertito con modificazioni in legge 9 novembre 2021, n. 156;

NORMATIVA EUROPEA DI RIFERIMENTO E STANDARD TECNICI

- EN 50126 - Applicazioni ferroviarie, tranviarie, filotranviare, metropolitane – La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS)
- REGOLAMENTO 762/2018 - metodo comune di sicurezza relativo ai requisiti del sistema di gestione della sicurezza a norma della direttiva (UE) 2016/798;
- REGOLAMENTO (UE) N. 402/2013 relativo al metodo comune di sicurezza per la determinazione e valutazione dei rischi.
- REGOLAMENTO (UE) N. 1078/2012 relativo a un metodo di sicurezza comune per il monitoraggio che devono applicare le imprese ferroviarie, i gestori dell'infrastruttura che hanno ottenuto un certificato di sicurezza o un'autorizzazione di sicurezza e i soggetti responsabili della manutenzione

IL NUOVO APPROCCIO PER LA GESTIONE DELLA SICUREZZA NEI SISTEMI DI TRASPORTO AD IMPIANTI FISSI

- Con decreto-legge 10 settembre 2021, n. 121, convertito con modificazioni in legge 9 novembre 2021, n. 156:
  - sono state trasferite ad ANSFISA le funzioni esercitate dagli USTIF del MIT.
  - è stato previsto anche per gli **Esercenti** dei sistemi di trasporto a impianti fissi il rilascio dell'**autorizzazione di sicurezza**.
  - ha affidato ad ANSFISA il compito di disciplinare i requisiti per il rilascio dell'autorizzazione di sicurezza relativa al sistema di trasporto costituito dall'infrastruttura e dal materiale rotabile, con i contenuti di cui agli articoli 9 e 11 del decreto legislativo 14 maggio 2019, n. 50, per quanto applicabili, nonché, d'intesa con il MIT, le modalità per la realizzazione e l'apertura all'esercizio di nuovi sistemi di trasporto a impianti fissi.

DECRETO ANSFISA DEL 28 DICEMBRE 2023

Agenzia Nazionale per la Sicurezza delle Ferrovie
e delle Infrastrutture Stradali e Autostradali

«Disciplina dei requisiti per il rilascio dell'autorizzazione di sicurezza relativa ai sistemi di trasporto pubblico a guida vincolata, ai sensi dell'articolo 6, comma 1, lettera b), del decreto-legge 10 settembre 2021, n. 121, convertito con modificazioni in legge 9 novembre 2021, n. 156»

VISTO il Decreto Legge 28 settembre 2018, n. 109 "Disposizioni urgenti per la città di Genova, la sicurezza della rete nazionale delle infrastrutture e dei trasporti, gli eventi sismici del 2016 e 2017, il lavoro e le altre emergenze", convertito con modificazioni dalla Legge 16

REGISTRO UFFICIALE.Int.0081906.28-12-2023

SISTEMI DI TRASPORTO A GUIDA VINCOLATA – TGV

Sono definiti nel Decreto del 28 dicembre 2023

sistema di trasporto pubblico guidato da almeno una rotaia o vincolato ad una linea di alimentazione elettrica, destinato all'esercizio di trasporti locali, servizi passeggeri urbani ed extraurbani, con veicoli semoventi e operanti sia segregati che non dal traffico stradale e pedonale.

Tali sistemi comprendono:

- le metropolitane e le metropolitane leggere, con e senza conducente, come definite dalla UNI 8379, e i sistemi assimilabili;
- le tranvie e le tranvie veloci (metro-tranvie), come definite dalla UNI 8379, e i sistemi assimilabili;
- i sistemi filoviari

AUTORIZZAZIONE DI SICUREZZA

Art. 11 del d.lgs. n. 50/2019

Attestato rilasciato dall'ANSFISA che dimostra che un **esercente** ha adottato tutte **le misure necessarie per assicurare la sicurezza di esercizio**.

Ciò include:

- **Valutazione e gestione dei rischi:** identificazione e analisi dei potenziali pericoli e definizione di misure preventive e di controllo.
- **Definizione di processi e procedure:** standardizzazione delle attività per garantire la sicurezza in ogni fase (circolazione dei veicoli, manutenzione, gestione delle emergenze, ecc.).
- **Verifica della competenza del personale:** assicurare che il personale coinvolto nelle attività abbia le competenze e la formazione necessarie.
- **Controllo e monitoraggio continuo:** monitoraggio costante delle attività e verifica dell'efficacia delle misure di sicurezza adottate.
- **Miglioramento continuo:** implementazione di un processo di miglioramento continuo per adeguare il sistema all'evoluzione delle normative e delle migliori pratiche.

SISTEMA DI GESTIONE DELLA SICUREZZA (SGS)

- **Art. 11 del d.lgs. n. 50/2019**
- **Reg. 762/2018**
- **ISO 9001**

- **<u>le misure necessarie per assicurare la sicurezza di esercizio</u>** sono descritte in un documento denominato **SGS**
- Quindi l'**Autorizzazione di Sicurezza** certifica che l'esercente ha ***implementato e attuato*** un proprio **SGS** ed è in grado di operare in modo sicuro nell'area di esercizio prevista, corrispondente alla singola infrastruttura, o di gestire e far funzionare l'infrastruttura in modo sicuro, tenendo conto delle caratteristiche delle tratte, dei rotabili e del servizio di trasporto.

Reg. 1078/2012

ELEMENTI ESSENZIALI DI UN SGS

Art. 8 del d.lgs. n. 50/2019
Reg. 762/2018
ISO 9001

- Un SGS è un insieme di elementi **interconnessi** che un'organizzazione mette in atto per gestire i rischi e garantire la sicurezza delle proprie attività.
- Gli elementi essenziali di un SGS così come definiti dal d.lgs.50/2019 sono:

1. **Politica di sicurezza:** Dichiarazione formale dell'impegno dell'organizzazione verso la sicurezza, definendo obiettivi, principi e responsabilità.
2. **Valutazione dei rischi:** Identificazione e analisi dei pericoli e dei rischi associati alle attività dell'organizzazione, al fine di determinarne la probabilità e l'impatto potenziale.
3. **Pianificazione:** Definizione di misure preventive e protettive per controllare i rischi identificati, stabilendo priorità, risorse e responsabilità.
4. **Implementazione:** Attuazione delle misure di sicurezza pianificate, attraverso procedure, istruzioni di lavoro, formazione e comunicazione.
5. **Monitoraggio e controllo:** Verifica periodica dell'efficacia delle misure di sicurezza, attraverso ispezioni, audit, analisi degli incidenti e degli eventi mancati.

ELEMENTI ESSENZIALI DI UN SGS

6. **Miglioramento continuo:** Revisione periodica del SGS per identificare aree di miglioramento e implementare azioni correttive e preventive.
7. **Responsabilità e coinvolgimento:** Definizione chiara delle responsabilità a tutti i livelli dell'organizzazione e coinvolgimento attivo del personale nella gestione della sicurezza
8. **Comunicazione e consultazione:** Stabilire canali di comunicazione efficaci per informare e consultare il personale sulle questioni di sicurezza.
9. **Formazione e addestramento:** Garantire che il personale sia adeguatamente formato e addestrato sulle procedure di sicurezza e sull'utilizzo delle attrezzature.
10. **Documentazione:** Mantenere una documentazione completa e aggiornata del SGS, comprese politiche, procedure, valutazione dei rischi, piani di emergenza e registri di controllo.

COME UN ESERCENTE MONITORA IL PROPRIO SGS

REGOLAMENTO (UE) N. 1078/2012 DELLA COMMISSIONE

del 16 novembre 2012

relativo a un metodo di sicurezza comune per il monitoraggio che devono applicare le imprese ferroviarie, i gestori dell'infrastruttura che hanno ottenuto un certificato di sicurezza o un'autorizzazione di sicurezza e i soggetti responsabili della manutenzione

PROCESSO DI MONITORAGGIO CONTINUO

REGOLAMENTO (UE) N. 1078/2012 DELLA COMMISSIONE

del 16 novembre 2012

relativo a un metodo di sicurezza comune per il monitoraggio che devono applicare le imprese ferroviarie, i gestori dell'infrastruttura che hanno ottenuto un certificato di sicurezza o un'autorizzazione di sicurezza e i soggetti responsabili della manutenzione

Il processo di monitoraggio prevede le seguenti attività:

- la definizione di una strategia, di priorità e piani di monitoraggio;
- la raccolta e l'analisi delle informazioni;
- l'elaborazione di un piano d'azione per casi di non conformità inaccettabili rispetto ai requisiti stabiliti nel sistema di gestione;
- l'attuazione del piano di azione, quando quest'ultimo sia stato elaborato;
- la valutazione dell'efficacia delle misure del piano d'azione, quando quest'ultimo sia stato elaborato.

NUOVO APPROCCIO

- Con il nuovo complesso normativo si sta compiendo un cambio di approccio nella **gestione della sicurezza nei sistemi di trasporto a impianti fissi** così come avvenuto negli anni sia nel settore ferroviario, ma prima ancora, nel settore aereo.

APPROCCIO REATTIVO/PRESCRITTIVO/DETERMINISTICO



APPROCCIO PRESTAZIONALE/RISK BASED/PROBABILISTICO







APPROCCIO REATTIVO/PRESCRITTIVO/DETERMINISTICO

- L'**approccio reattivo/prescrittivo/deterministico**, si basa principalmente sulla conformità a norme e regolamenti preesistenti e sull'attuare misure per evitare il **ripetersi** di un evento indesiderato già accaduto.
- **Il miglioramento del sistema avviene in maniera discreta ed è legato al presentarsi di eventi indesiderati.**
- Quindi l'elemento chiave di questo approccio è la **prevedibilità** che un evento indesiderato possa ri-verificarsi e l'esistenza della possibilità di **prevenirne** gli eventuali danni.

CARATTERISTICHE PRINCIPALI DELL'APPROCCIO REATTIVO

- **Norme e standard:** Vengono definite regole e standard dettagliati che specificano come devono essere progettati, costruiti, mantenuti e utilizzati tutti gli elementi di un sistema di trasporto (veicoli, infrastrutture, ecc..)
- **Conformità:** L'obiettivo principale è garantire che tutte le attività e i processi siano conformi a queste norme e standard.
- **Ispezioni e controlli:** Vengono effettuati controlli e ispezioni regolari per verificare la conformità alle regole.
- **Sanzioni:** In caso di non conformità, vengono applicate sanzioni.

LIMITI DELL'APPROCCIO REATTIVO

- **Mancanza di flessibilità:** L'approccio prescrittivo può essere rigido e non adattabile a situazioni nuove o impreviste che in genere si basa sull'attuare misure per evitare il **ripetersi** di un evento indesiderato già accaduto.
- **Focus sulla conformità:** L'attenzione è focalizzata sulla conformità alle regole, piuttosto che sulla valutazione e gestione dei rischi specifici.
- **Difficoltà nell'affrontare rischi emergenti:** Le norme e gli standard possono non essere in grado di coprire tutti i possibili scenari di rischio, soprattutto quelli legati a nuove tecnologie o cambiamenti nel contesto operativo.

APPROCCIO PRESTAZIONALE O RISK BASED

- L'**approccio prestazionale** o **risk-based** rappresenta una filosofia di gestione che si concentra sulla **valutazione e mitigazione dei rischi**.
- Anziché aderire rigidamente a regole e procedure predefinite (approccio prescrittivo), questo approccio si adatta alle specificità di ogni situazione, analizzando i potenziali pericoli e adottando misure mirate per ridurne l'impatto.
- Si mettono in atto tecniche tese ad individuare tutti i possibili **pericoli** e tutte le possibili **cause latenti** (near miss) che possono portare al verificarsi di un evento indesiderato.
  - Brainstorming, What-IF, Analisi Storiche, Checklist, Analisi di scenari,

PRINCIPI CHIAVE DELL'APPROCCIO PRESTAZIONALE

- **Identificazione di tutti i possibili pericoli**: Individuare tutte le possibili fonti di danno, che si tratti di guasti tecnici, errori umani, eventi naturali o altri fattori.
- **Valutazione dei rischi legati ad ogni pericolo**: Analizzare la probabilità che un determinato pericolo si verifichi e la gravità delle conseguenze che potrebbe causare.
- **Classificazione dei rischi**: in base alla loro gravità e probabilità, concentrando le risorse e gli sforzi sulle aree più critiche.
- **Implementazione di misure preventive/protettive**: per ridurre o eliminare i rischi identificati.
  - Queste misure possono variare ampiamente, dalla manutenzione preventiva alla formazione del personale, dall'implementazione di sistemi di sicurezza avanzati alla definizione di procedure operative dettagliate.
- **Monitoraggio e revisione**: Verificare periodicamente l'efficacia delle misure di controllo e aggiornare la valutazione dei rischi in base all'evoluzione delle condizioni operative e delle nuove informazioni disponibili.

VANTAGGI DELL'APPROCCIO PRESTAZIONALE

- **Maggiore flessibilità:** Consente di adattare le misure di sicurezza alle specificità di ogni situazione, anziché applicare regole rigide e uniformi.
- **Migliore allocazione delle risorse:** Permette di concentrare le risorse e gli sforzi sulle aree più critiche, ottimizzando l'efficacia degli interventi di sicurezza.
- **Maggiore proattività:** Incoraggia l'identificazione e la gestione dei rischi prima che si verifichino incidenti, anziché limitarsi a reagire dopo che si sono verificati.
- **Miglioramento continuo:** Promuove un processo di apprendimento e miglioramento continuo, in cui le lezioni apprese dagli incidenti e dagli eventi mancati vengono utilizzate per aggiornare e migliorare il sistema di gestione della sicurezza.

In conclusione, l'approccio prestazionale o risk-based rappresenta un'evoluzione fondamentale nella gestione della sicurezza nei trasporti. Concentrandosi sulla valutazione e mitigazione dei rischi, questo approccio consente di migliorare continuamente gli standard di sicurezza e di prevenire incidenti, garantendo al contempo una maggiore flessibilità e adattabilità.

IN SINTESI

approccio reattivo:

- Si concentra sull'analisi dell'incidente dopo che si è verificato.
- Mira a identificare le cause immediate e adottare misure correttive specifiche per evitare che l'incidente si ripeta nello stesso punto.
- Si concentra principalmente sulle cause dirette dell'incidente specifico.

approccio prestazionale (risk-based)

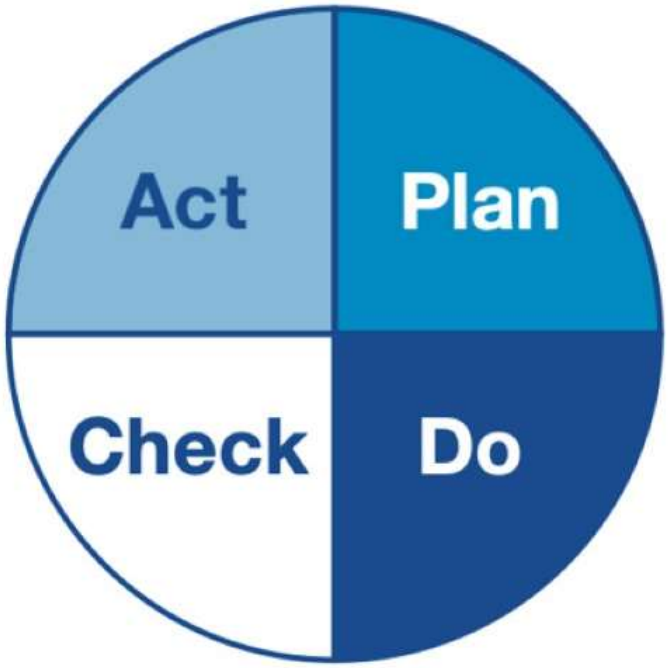
- Si concentra sulla valutazione e gestione dei rischi prima che si verifichino incidenti.
- Mira a identificare tutti i potenziali pericoli (non solo quelli che hanno causato l'incidente specifico) e valutare la probabilità e le conseguenze di ciascuno.
- Consente di adottare misure preventive e protettive generalizzate per ridurre il rischio in qualsiasi punto della rete e in qualsiasi condizione.
- Promuove un approccio proattivo e di miglioramento continuo, in cui i dati sugli incidenti passati vengono utilizzati per aggiornare la valutazione dei rischi e migliorare le misure di sicurezza

APPROCCIO PRESTAZIONALE BASATO SUL CICLO DI DEMING

- L'approccio prestazionale offre una visione più ampia e proattiva della sicurezza, consentendo di prevenire incidenti, migliorare l'allocazione delle risorse e promuovere un processo di **miglioramento continuo.**
- L'approccio prestazionale è un approccio metodologico che si fonda sulla famiglia degli standard **ISO 9000** già adottati nella gestione della qualità basato sul **CICLO DI DEMING o PDCA (Plan-Do-Check-Act).**
- La ratio è:
  - "qualità" requisito irrinunciabile come la "sicurezza"
  - metodo che impone il miglioramento continuo

CICLO DI DEMING (PDCA)

- Metodologia di gestione che mira al miglioramento continuo attraverso un processo ciclico e iterativo.
- Questo approccio è ampiamente utilizzato in diversi settori, tra cui l'industria, i servizi e la sanità, per ottimizzare processi, prodotti e servizi.



CICLO DI DEMING (PDCA)



Plan (Pianificare):

- si definiscono gli obiettivi;
- si identificano i processi necessari per raggiungerli
- si pianificano le attività da svolgere.
- si raccolgono dati e informazioni per comprendere la situazione attuale
- si stabiliscono gli indicatori di performance per misurare i progressi.

Do (Fare):

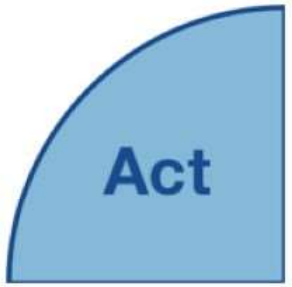
- si implementano le attività pianificate;
- si eseguono i processi definiti
- si raccolgono i dati relativi alle performance;
- si documentano le attività svolte e le eventuali difficoltà incontrate.



CICLO DI DEMING (PDCA)

Check (Verificare):

- si analizzano i dati raccolti per verificare se gli obiettivi sono stati raggiunti e se i processi sono stati eseguiti correttamente.
- si confrontano i risultati ottenuti con gli indicatori di performance stabiliti e si identificano eventuali scostamenti.

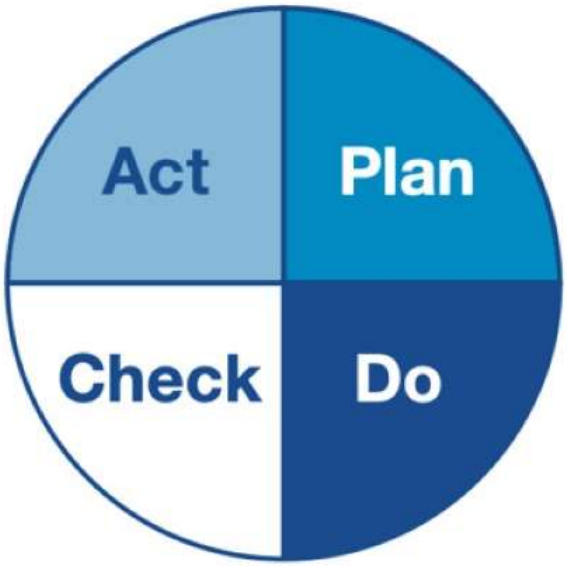




Act (Agire):

- In base ai risultati della fase di verifica, si intraprendono azioni correttive per migliorare i processi e le performance.
- Se gli obiettivi non sono stati raggiunti, si rivedono le attività pianificate e si apportano le modifiche necessarie.
- Se gli obiettivi sono stati raggiunti, si standardizzano i processi migliorati e si definiscono nuovi obiettivi per il ciclo successivo.

INTEGRAZIONE TRA PDCA E APPROCCIO PRESTAZIONALE



- Il ciclo di Deming è uno strumento fondamentale per l'implementazione dell'approccio prestazionale.
- Il PDCA fornisce un framework strutturato per la pianificazione, l'attuazione, la verifica e il **miglioramento continuo dei processi**, consentendo alle organizzazioni di raggiungere i propri obiettivi di performance.

VANTAGGI DELL'APPROCCIO PRESTAZIONALE BASATO SUL CICLO DI DEMING

- **Miglioramento continuo:** Il ciclo PDCA promuove un processo di miglioramento continuo, in cui le performance vengono costantemente monitorate e migliorate.
- **Flessibilità:** L'approccio prestazionale consente di adattare le misure e le azioni in base alle specifiche esigenze e al contesto dell'organizzazione.
- **Orientamento ai risultati:** L'attenzione è focalizzata sul raggiungimento di obiettivi specifici e misurabili, garantendo che le risorse siano utilizzate in modo efficace.
- **Coinvolgimento del personale:** Il ciclo PDCA coinvolge il personale a tutti i livelli dell'organizzazione, promuovendo la partecipazione e la responsabilità nel raggiungimento degli obiettivi.
- **Efficienza:** L'approccio prestazionale consente di ottimizzare i processi e le risorse, riducendo i costi e gli sprechi.

ESEMPIO DI APPLICAZIONE DEL CICLO DI DEMING (1/4)



- **Scenario:** Aumento degli incidenti ai passaggi a livello, alcuni con gravi conseguenze.
  - **Pianificazione (Plan)**
    - **Obiettivo:** Ridurre del 20% il numero di incidenti ai passaggi a livello entro 12 mesi.
    - **Raccolta dati:** Analizzare i dati sugli incidenti ai passaggi a livello degli ultimi anni, identificando le cause più comuni (ad esempio, mancato rispetto del codice della strada da parte degli automobilisti, malfunzionamento dei sistemi di segnalamento, scarsa visibilità).
    - **Definizione delle azioni:**
      - Migliorare la segnaletica e la visibilità dei passaggi a livello.
      - Implementare campagne di sensibilizzazione per aumentare la consapevolezza degli automobilisti sui rischi ai passaggi a livello.
      - Installare sistemi di rilevamento automatico degli ostacoli sui binari.
      - Verificare e migliorare l'affidabilità dei sistemi di segnalamento.
      - Collaborare con le autorità locali per migliorare la sicurezza stradale in prossimità dei passaggi a livello.

ESEMPIO DI APPLICAZIONE DEL CICLO DI DEMING (2/4)

- **Esecuzione (Do)**
  - **Implementazione delle azioni:** Mettere in atto le azioni definite nella fase di pianificazione. Ad esempio:
    - Installare nuove segnaletiche e illuminazione nei passaggi a livello.
    - Avviare campagne di sensibilizzazione attraverso i media e le scuole.
    - Installare sistemi di rilevamento ostacoli in alcuni passaggi a livello.
    - Effettuare controlli e manutenzione più frequenti dei sistemi di segnalamento.
    - Organizzare incontri con le autorità locali per discutere interventi di miglioramento della sicurezza stradale.
  - **Raccolta dati***:* Continuare a monitorare il numero e la tipologia di incidenti ai passaggi a livello durante il periodo di implementazione delle azioni.

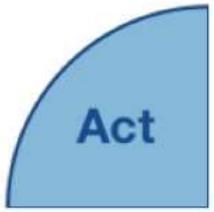


ESEMPIO DI APPLICAZIONE DEL CICLO DI DEMING (3/4)

- **Verifica (Check)**
  - **Analisi dei risultati:** Dopo un periodo di tempo (ad esempio, 6 mesi);
    - analizzare i dati raccolti per verificare se le azioni implementate hanno avuto l'effetto desiderato.
    - Confrontare il numero di incidenti attuali con quelli del periodo precedente e valutare se si è raggiunto l'obiettivo parziale di riduzione degli incidenti.
  - **Identificazione dei problemi:**
    - Identificare eventuali problemi o difficoltà incontrate durante l'implementazione delle azioni, nonché eventuali effetti collaterali indesiderati (ad esempio, costi eccessivi per l'installazione dei sistemi di rilevamento ostacoli).



ESEMPIO DI APPLICAZIONE DEL CICLO DI DEMING (4/4)



- **Azione (Act)**
  - **Azione correttiva:** In base ai risultati della fase di verifica, intraprendere azioni correttive per migliorare ulteriormente i processi. Ad esempio:
    - Se le campagne di sensibilizzazione non hanno dato i risultati sperati, rivedere le strategie di comunicazione e coinvolgere maggiormente le associazioni di automobilisti.
    - Se i sistemi di rilevamento ostacoli si sono rivelati troppo costosi, cercare soluzioni alternative più economiche.
    - Se i controlli sui sistemi di segnalamento non sono stati sufficienti, aumentare la frequenza e il rigore delle verifiche.
  - **Standardizzazione:** Una volta raggiunti gli obiettivi desiderati, standardizzare i processi migliorati, documentandoli e integrandoli nelle procedure operative.
  - **Nuovo ciclo:** Ricominciare il ciclo PDCA con nuovi obiettivi di miglioramento, ad esempio ridurre ulteriormente il numero di incidenti o migliorare la sicurezza in specifici tipi di passaggi a livello.

DEFINIZIONE DI RISCHIO

Rischio = Frequenza × Gravità x Vulnerabilità x Esposizione

N O R M A I T A L I A N A CEI

Norma Italiana

CEI EN 50126

Data Pubblicazione	*Edizione*
2000-03	Prima
Classificazione	*Fascicolo*
9-58	5594

Titolo

Applicazioni ferroviarie, tranviarie, filotranviarie, metropolitane

La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS)

- La norma **EN 50126**, definisce il rischio come:
- combinazione della **probabilità di un evento pericoloso** e della **gravità delle sue conseguenze**
- evento pericoloso = qualsiasi evento che possa causare danni a persone, beni o all'ambiente.

ELEMENTI CHIAVE

- **Evento pericoloso (Hazard):**
  - Qualsiasi evento che possa causare danni, come ad esempio un deragliamento, una collisione, un incendio, un'esplosione, un guasto di un sistema di segnalamento, un errore umano, un atto vandalico, un evento naturale.
- **Probabilità:**
  - La probabilità che l'evento pericoloso si verifichi.
- **Gravità (Severity):**
  - L'entità dei danni che possono derivare dall'evento pericoloso, che possono essere di diversa natura (lesioni a persone, danni materiali, interruzioni del servizio, impatto ambientale).

HAZARD – ESEMPI

Hazard log – Registro Eventi Pericolosi

Evento Pericoloso	ID Evento Pericoloso	Indicatore sull'occorrenza dell'EP	Obiettivo	Evento incidentale	Macrocausa (Umana/ Tecnica/ Esterna)	Misure di sicurezza parmamenti		
						Tipologia misura di sicurezza (Preventiva/ protettiva)	Descrizione	Resp.
Errata comunicazione regolatore della circolazione / Agente di condotta	EP.01	N°errate comunicazioni tra AdC e GI che avrebbero potuto portare ad una collisione	0	Collisione di treno con veicolo ferroviario	Umana	Preventiva	Formazione dell'agente di condotta [redacted]	Resp. FSR
							Idoneità sanitaria dell'agente di condotta [redacted]	Resp. Personale di Produzione
							Programmazione turni nel rispetto dei vincoli legislativi e contrattuali	Resp. Personale di Produzione
							Conoscenza della lingua italiana	Resp. FSR
						Protettiva	Procedura di gestione emergenze	Resp. SGS
					Esterna	Preventiva	Formazione del regolatore della circolazione	RFI

Gli **Hazard** sono individuati sia attraverso tecniche di **Brainstorming** che ricavati dalla **Fault Tree Analysis (FTA)** degli eventi incidentali

STIMA DELLA PROBABILITÀ

- Per ogni **Evento pericoloso (Hazard)** si stima relativo il **livello di probabilità.**
- I **Livelli di Probabilità** sono stabiliti utilizzando le indicazioni fornite dalla EN 50126

Livello di probabilità	Condizione	Frequenza indicativa
Frequente	Probabile che accada frequentemente. La situazione pericolosa si presenterà continuamente.	1/50
Probabile	Accadrà parecchie volte. Ci si può aspettare che la situazione pericolosa si presenti spesso.	1/100
Occasionale	Probabile che accada parecchie volte. Ci si può aspettare che la situazione pericolosa si presenti parecchie volte	1/500
Remoto	Probabile che accada qualche volta nella vita del sistema. Ci si può ragionevolmente aspettare che la situazione pericolosa si presenti.	1/10.000
Improbabile	Improbabile che accada ma possibile. Si può assumere che la situazione pericolosa possa presentarsi eccezionalmente.	1/100.000
Inverosimile	Estremamente improbabile che accada. Si può assumere che la situazione pericolosa possa non presentarsi.	1/1.000.000

La **frequenza indicativa** è da intendersi come numero di occorrenze dell'evento o dell'elemento di interesse su un numero di volte che si realizza l'attività presupposto nel corso della vita utile del sistema oggetto di osservazione, stimata in 30 anni.

LIVELLO DI PROBABILITÀ STIMATA PER OGNI HAZARD

Evento Pericoloso		Probabilità dell'EP
EP1	Errata comunicazione regolatore della circolazione/Agente di Condotta	*remoto*
EP2	Errore dell'Agente di Condotta	*remoto*
EP3	Errore del regolatore della circolazione	*remoto*
EP4	Bassa aderenza	*improbabile*
EP5	Errore del segnalamento	*improbabile*
EP6	Veicolo non correttamente immobilizzato/stazionato	*improbabile*
EP7	Frenatura anomala	*improbabile*
EP8	Errore del sistema di segnalamento	*improbabile*
EP9	Anormalità segnalamento di coda	*improbabile*
EP10	Rottura/difetti dei binari	*remoto*
EP11	Elementi del carrello dei veicoli daneggiati	*remoto*
EP12	Ruote danneggiate	*improbabile*
EP13	Assili danneggiati	*improbabile*
EP14	Guasto odometria	*improbabile*
EP15	Eventi sismici	*inverosimile*
EP16	Criticità idrogeologiche	*inverosimile*
EP17	Terrorismo/vandalismo	*improbabile*
EP18	Presenza animali in linea	*remoto*

Sulla base dell'esperienza di ogni singolo componente del GdL, attraverso l'attività di Brainstorming si identifica la Probabilità di ogni Hazard.

STIMA DELLA GRAVITÀ

- Per ogni **Evento pericoloso (Hazard)** si stima il **livello di gravità** associato.
- Il metodo maggiormente utilizzato è il **Worst Case Scenario**

Livello di gravità	Condizione
Insignificante	Danno leggero
Marginale	Ferimento leggero di una o più persone e/o importante minaccia per l'ambiente e danno grave
Critico	Lesione grave di una persona o importante danno all'ambiente
Catastrofico	Morte o ferimento grave di una o più persone e danni ingenti

Il **livelli di gravità** sono stabiliti utilizzando le indicazioni fornite dalla EN 50126

LIVELLO DI GRAVITÀ STIMATA PER OGNI HAZARD

Evento Pericoloso		Livello di Gravità
EP1	Errata comunicazione regolatore della circolazione/Agente di Condotta	*Catastrofico*
EP2	Errore dell'Agente di Condotta	*Catastrofico*
EP3	Errore del regolatore della circolazione	*Catastrofico*
EP4	Bassa aderenza	*Catastrofico*
EP5	Errore del segnalamento	*Catastrofico*
EP6	Veicolo non correttamente immobilizzato/stazionato	*Catastrofico*
EP7	Frenatura anomala	*Catastrofico*
EP8	Errore del sistema di segnalamento	*Catastrofico*
EP9	Anormalità segnalamento di coda	*Catastrofico*
EP10	Rottura/difetti dei binari	*Catastrofico*
EP11	Elementi del carrello dei veicoli daneggiati	*Catastrofico*
EP12	Ruote danneggiate	*Catastrofico*
EP13	Assili danneggiati	*Catastrofico*
EP14	Guasto odometria	*Catastrofico*
EP15	Eventi sismici	*Catastrofico*
EP16	Criticità idrogeologiche	*Catastrofico*
EP17	Terrorismo/vandalismo	*Catastrofico*
EP18	Presenza animali in linea	*Critico*
EP19	Presenza elementi di altro veicolo ferroviario in linea	*Critico*

Il livello di gravità (massimo) associato è in genere frutto di un'attività di Brainstorming.

DETERMINAZIONE DEL RISCHIO

- Incrociando il livello di gravità e la frequenza di accadimento si individua la cosiddetta **MATRICE DEI RISCHI**

Frequenza di accadimento di una situazione pericolosa	**Livello di rischio**			
Frequente	indesiderabile	**intollerabile**	**intollerabile**	**intollerabile**
Probabile	indesiderabile	indesiderabile	**intollerabile**	**intollerabile**
Occasionale	indesiderabile	indesiderabile	indesiderabile	**intollerabile**
Remoto	Tollerabile	indesiderabile	indesiderabile	indesiderabile
Improbabile	Trascurabile	Tollerabile	Tollerabile	indesiderabile
Inverosimile	Trascurabile	Trascurabile	Trascurabile	Trascurabile
	Insignificante (IV)	Marginale (III)	Critico (II)	Catastrofico (I)
	Livello di gravità delle conseguenze della situazione pericolosa			

INACCETTABILE

LIVELLO DI RISCHIO ASSOCIATO AD OGNI HAZARD

Evento Pericoloso		Gravità dell'EP	Probabilità dell'EP	Livello di rischio neutro
EP1	Errata comunicazione regolatore della circolazione/Agente di Condotta	*Catastrofico*	remoto	Inaccettabile
EP2	Errore dell'Agente di Condotta	*Catastrofico*	*remoto*	Inaccettabile
EP3	Errore del regolatore della circolazione	*Catastrofico*	*remoto*	Inaccettabile
EP4	Bassa aderenza	*Catastrofico*	improbabile	Inaccettabile
EP5	Errore del segnalamento	*Catastrofico*	*improbabile*	Inaccettabile
EP6	Veicolo non correttamente immobilizzato/stazionato	*Catastrofico*	*improbabile*	Inaccettabile
EP7	Frenatura anomala	*Catastrofico*	*improbabile*	Inaccettabile
EP8	Errore del sistema di segnalamento	*Catastrofico*	*improbabile*	Inaccettabile
EP9	Anormalità segnalamento di coda	*Catastrofico*	*improbabile*	Inaccettabile
EP10	Rottura/difetti dei binari	*Catastrofico*	*remoto*	Inaccettabile
EP11	Elementi del carrello dei veicoli daneggiati	*Catastrofico*	*remoto*	Inaccettabile
EP12	Ruote danneggiate	*Catastrofico*	*improbabile*	Inaccettabile
EP13	Assili danneggiati	*Catastrofico*	*improbabile*	Inaccettabile
EP14	Guasto odometria	*Catastrofico*	*improbabile*	Inaccettabile
EP15	Eventi sismici	*Catastrofico*	*inverosimile*	Tollerabile

Il livello di rischio **neutro** dato dalla combinazione del livello di probabilità **stimato** e livello di gravità nel caso di scenario **peggiore**.

Nella pratica al **livello di probabilità** si associano **elementi di inferenza** e/o di attivazione che possono amplificare il livello quindi il rischio .

elementi di inferenza = condizioni atmosferiche, elementi topografici (gallerie, ponti, viadotti, ecc...);

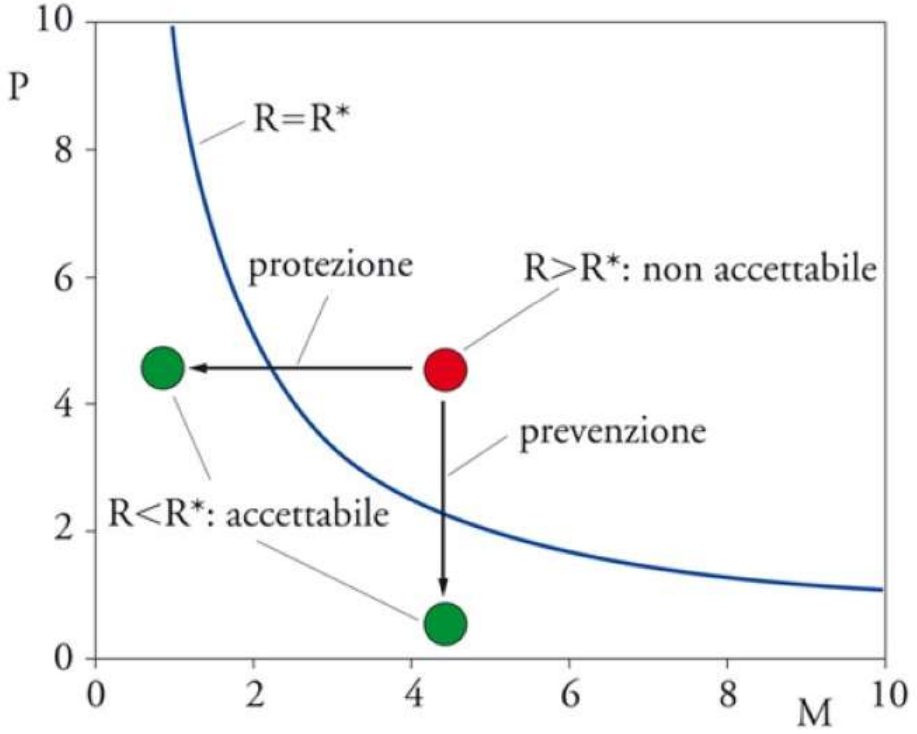
elementi di attivazione = velocità di marcia, numero di passeggeri;

Inferenza sulla probabilità può amplificare.

Inferenza sulla gravità in genere riduce.

MISURE DI SICUREZZA

- Le **misure di sicurezza** di tipo permanente o provvisorio hanno lo scopo di mitigare il livello di rischio associato al singolo Hazard e portarlo nella zona di accettabilità



MISURE DI PREVENTIVE

- **Misure sui sistemi**:
  - Miglioramento degli apparati tecnici;
  - Monitoraggio delle prestazioni degli apparati;
- **Misure procedurali:**
  - Definizione di **procedure operative** chiare e dettagliate per tutte le attività.
  - Formazione e addestramento del personale per garantire la competenza e la consapevolezza dei rischi.
  - Controlli e ispezioni regolari per verificare il rispetto delle procedure e l'efficacia delle misure di sicurezza.
- **Misure sul fattore umano:**
  - **Organizzazione** - definizione chiara di ruoli e responsabilità;
  - Implementazione di un sistema di gestione della sicurezza che preveda la valutazione dei rischi, la definizione di obiettivi di sicurezza, il monitoraggio delle prestazioni e il miglioramento continuo.
  - Comunicazione efficace tra le diverse figure coinvolte (ad esempio, personale di bordo, personale di terra, controllori del traffico).

MISURE PROTETTIVE

Esempi di misure protettive:

- **Misure ingegneristiche**:
  - Barriere fisiche di sicurezza, ad esempio per impedire l'accesso a zone pericolose.
  - Materiali resistenti al fuoco per ridurre il rischio di incendi.
  - Sistemi di evacuazione di emergenza per facilitare l'allontanamento delle persone in caso di pericolo.
- **Misure procedurali**:
  - Piani di emergenza per gestire situazioni di crisi (ad esempio, incidenti, deragliamenti, incendi).
  - Procedure di evacuazione per garantire l'allontanamento sicuro delle persone in caso di pericolo.
  - Utilizzo di dispositivi di protezione individuale (DPI) per proteggere i lavoratori da specifici rischi (ad esempio, caschi, guanti, scarpe antinfortunistiche).
- **Misure organizzative**:
  - Organizzazione di squadre di emergenza per intervenire in caso di incidenti.
  - Definizione di protocolli di comunicazione per allertare i soccorsi in caso di necessità.

LIVELLO DI RISCHIO FINALE

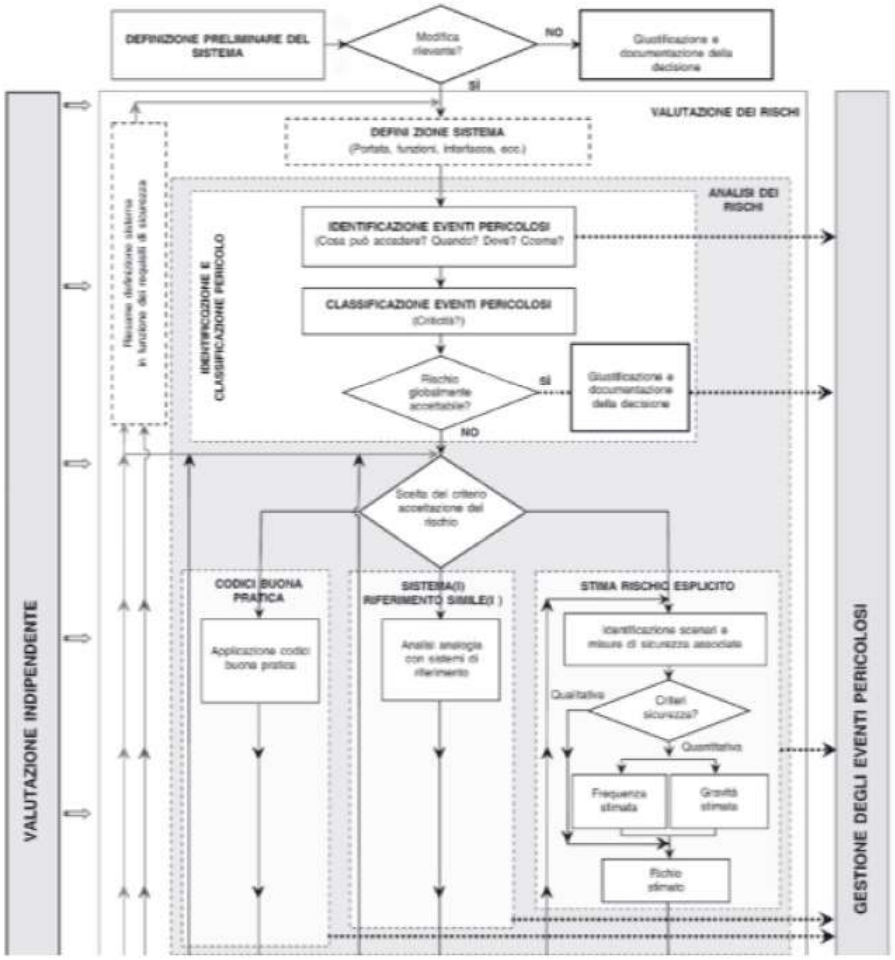
- Le misure di sicurezza riducono il livello di rischio associato.
- Le mitigazioni associate possono essere pure esportate mediante le cosiddette **SRACs (Safety Relevant Application Conditions)**

Evento Pericoloso		Gravità dell'EP	Probabilità dell'EP	Livello di rischio neutro
EP1	Errata comunicazione regolatore della circolazione/Agente di Condotta	*Catastrofico*	remoto	Inaccettabile
EP2	Errore dell'Agente di Condotta	*Catastrofico*	*remoto*	Inaccettabile
EP3	Errore del regolatore della circolazione	*Catastrofico*	*remoto*	Inaccettabile
EP4	Bassa aderenza	*Catastrofico*	improbabile	Inaccettabile
EP5	Errore del segnalamento	*Catastrofico*	*improbabile*	Inaccettabile
EP6	Veicolo non correttamente immobilizzato/stazionato	*Catastrofico*	*improbabile*	Inaccettabile
EP7	Frenatura anomala	*Catastrofico*	*improbabile*	Inaccettabile
EP8	Errore del sistema di segnalamento	*Catastrofico*	*improbabile*	Inaccettabile
EP9	Anormalità segnalamento di coda	*Catastrofico*	*improbabile*	Inaccettabile
EP10	Rottura/difetti dei binari	*Catastrofico*	*remoto*	Inaccettabile
EP11	Elementi del carrello dei veicoli daneggiati	*Catastrofico*	*remoto*	Inaccettabile

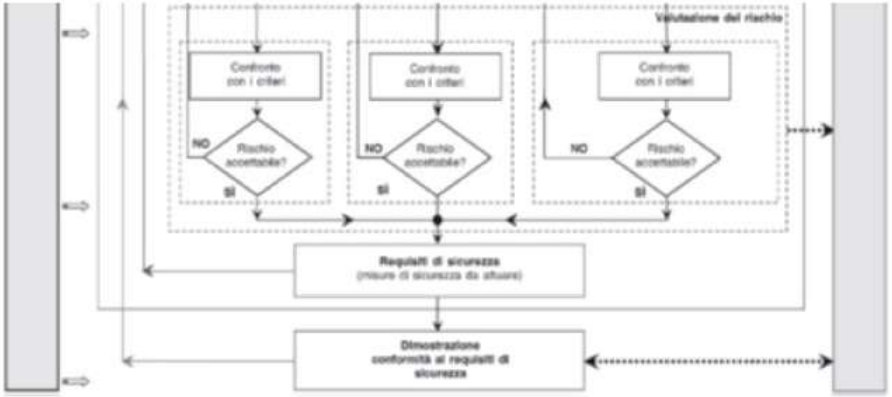
mitigazione

Livello di rischio
Tollerabile
Tollerabile
Tollerabile
Tollerabile
Tollerabile
Trascurabile
Tollerabile
Tollerabile
Tollerabile
Trascurabile
Tollerabile

PROCEDIMENTO DI GESTIONE DEI RISCHI NEL REG 402/2013

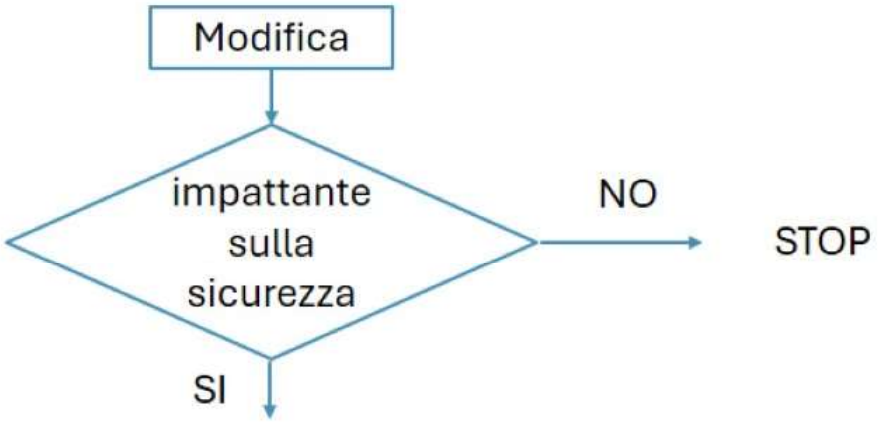


- Regolamento di Esecuzione (UE) n.402/2013 integrato con Regolamento di Esecuzione (UE) n.1136/2015 relativo al metodo comune di sicurezza per la determinazione e valutazione dei rischi (il Regolamento 402/2013 è richiamato anche del Decreto ANSFISA del 28 dicembre 2023)



PERCHE' SI PARLA DI MODIFICA E QUAL È IL PRIMO PASSO ?

- In linea di principio ogniqualvolta che si interviene sul sistema complesso, sia attraverso l'inserimento di un **sottosistema**, sia attraverso l'inserimento di una nuova **procedura operativa** o **organizzativa**, di fatto si sta apportando una **modifica** al sistema stesso.



MODIFICHE (GENERALMENTE) NON IMPATTANTI

elenco non è esaustivo

- **Sostituzione di un componente "alla pari" (like-for-like):** La sostituzione di un componente guasto con uno identico, dello stesso produttore e modello, senza alcuna variazione di funzionalità, software o interfaccia, è considerata non significativa. Ad esempio: la sostituzione di una lampadina di un segnale con una lampadina identica o la sostituzione di un relè guasto con un relè identico.
- **Modifiche minime a procedure operative:** L'aggiornamento di un manuale operativo che chiarisce un passaggio ambiguo senza cambiare la sostanza della procedura.
- **Sostituzione di hardware senza modifiche software:** La sostituzione di un computer di controllo con un modello più recente che esegue lo stesso software (con le stesse funzionalità e lo stesso livello di sicurezza) è considerata non significativa, a condizione che non ci siano cambiamenti nelle interfacce fisiche o nel comportamento del sistema.
- **Interventi di manutenzione ordinaria:** Le attività di manutenzione programmata, come la lubrificazione di un apparato di scambi o la pulizia di un sensore, che rientrano nelle normali procedure operative e di manutenzione, sono intrinsecamente non significative.
- **Piccole modifiche a infrastrutture non critiche per la sicurezza:** La riverniciatura di un ponte, la sostituzione di una ringhiera non strutturale o la sistemazione di un sentiero di servizio a lato binario sono modifiche che non influiscono sui sistemi di sicurezza e sono quindi non significative.

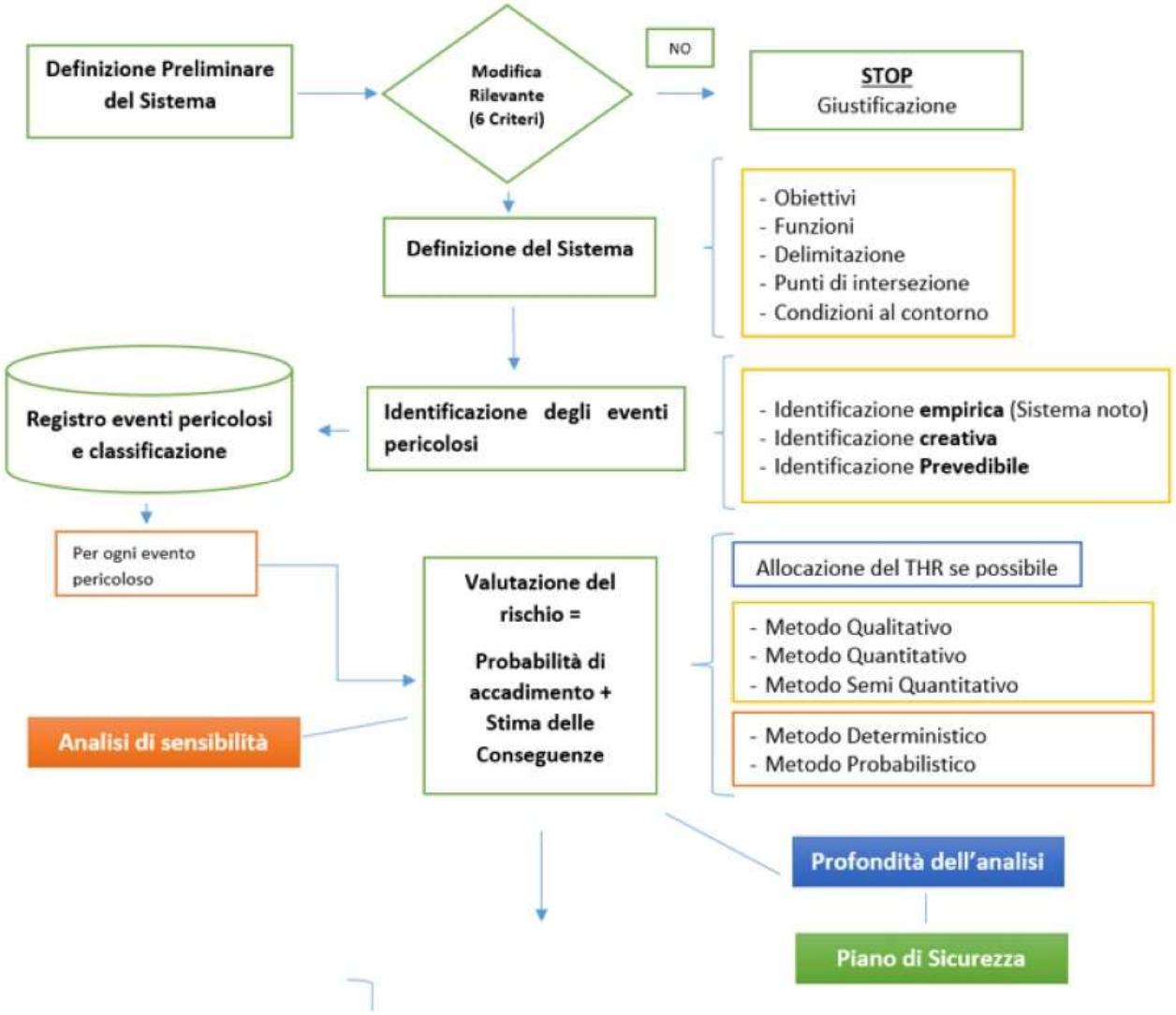
MODIFICHE NON IMPATTANTI - ECCEZIONI E AVVERTENZE

- **Non è "alla pari":** Se un nuovo componente ha un comportamento leggermente diverso, anche se le sue specifiche sono le stesse, potrebbe avere un impatto imprevisto.
- **Interagisce con un sistema complesso:** Anche una piccola modifica potrebbe avere conseguenze a cascata su altri sottosistemi complessi (effetto "farfalla").
- **Riguarda un sistema con un passato di guasti:** Se il sistema che si sta modificando ha una storia di problemi o guasti ripetuti, anche una modifica minore potrebbe essere considerata significativa per evitare ulteriori rischi.
- Per questo motivo, il Regolamento 402/2013 richiede che il proponente documenti il proprio giudizio di "non significatività" per ogni modifica.
- In caso di dubbio, è sempre più sicuro classificare la modifica come significativa e avviare il processo di valutazione del rischio formale

MODIFICA IMPATTANTE SULLA SICUREZZA

- **Modifiche che impattano sulla sicurezza (e che quindi richiedono una valutazione approfondita)**
  - **Introduzione di un nuovo tipo di materiale rotabile:** L'immissione in servizio di un treno con caratteristiche tecniche significativamente diverse da quelli esistenti (ad esempio, maggiore velocità, diversa tecnologia di frenatura) richiede una valutazione accurata dei rischi e delle interazioni con l'infrastruttura e gli altri treni.
  - **Modifiche significative all'infrastruttura:** La costruzione di una nuova linea ferroviaria, la modifica di tracciati esistenti (ad esempio, rettifiche di curve, creazione di gallerie), o l'installazione di nuovi sistemi di segnalamento possono introdurre nuovi pericoli e alterare le condizioni di sicurezza esistenti.
  - **Cambiamenti nelle procedure operative:** Modifiche alle regole di circolazione dei treni, alle procedure di manutenzione, o all'organizzazione del lavoro del personale possono avere un impatto diretto sulla sicurezza, soprattutto se coinvolgono attività critiche come la gestione del traffico o la manutenzione dell'infrastruttura.
  - **Introduzione di nuove tecnologie:** L'implementazione di sistemi di controllo automatico dei treni (ATC), sistemi di segnalamento di nuova generazione (ERTMS), o altre tecnologie innovative può portare

PROCESSO DI GESTIONE DEI RISCHI



MODIFICA RILEVANTE SULLA SICUREZZA

L'art. 4 del Reg.402/2013

- I criteri di rilevanza sono i seguenti:
  - **Conseguenza del guasto:** il peggiore scenario plausibile che potrebbe verificarsi in caso di guasto del sistema sottoposto a valutazione, tenuto conto dell'esistenza di barriere di sicurezza al di fuori del sistema in questione. Se la modifica introdotta riduce la sicurezza del sottosistema, dunque, la stessa deve essere considerata "rilevante".
  - **Innovazioni applicate per attuare la modifica:** sono comprese sia le innovazioni nel settore ferroviario sia le novità che riguardano l'organizzazione che mette in atto la modifica. L'introduzione di una soluzione tecnica innovativa impone la rilevanza della stessa.
  - **Complessità della modifica:** Una modifica che interessa più sottosistemi e le interazioni fisiche e funzionali tra gli stessi deve essere considerata rilevante.
  - **Monitoraggio:** l'impossibilità di monitorare la modifica realizzata in tutto il ciclo di vita del sistema e di intervenire opportunamente. Una modifica che non può essere periodicamente controllata deve essere considerata rilevante.
  - **Reversibilità:** l'impossibilità di ripristinare la situazione esistente prima della modifica del sistema. Se l'introduzione della modifica impedisce il ripristino della situazione precedente, la modifica deve essere considerata rilevante.
  - **Complementarità:** la valutazione della rilevanza della modifica alla luce di tutte le modifiche recenti riguardanti la sicurezza apportate al sistema sottoposto a valutazione e non ritenute rilevanti.

MODIFICA RILEVANTE SULLA SICUREZZA

L'art. 4 del Reg.402/2013

La somma di modifiche non rilevanti potrebbero dare luogo ad una modifica rilevante

- La rilevanza della modifica deve essere valutata in considerazione di eventuali altre modifiche recenti che hanno interessato lo stesso sistema, e considerate non rilevanti.
- Una modifica non rilevante sommata a una serie di modifiche non rilevanti apportate allo stesso sottosistema potrebbe determinare una modifica rilevante.
- Una modifica deve essere classificata come rilevante anche se solo uno dei precedenti sei criteri è verificato.

ESEMPIO DI CLASSIFICAZIONE

- **Scenario:** L'esercente che gestisce una linea di metropolitana prevede di introdurre una nuova generazione di treni, con le seguenti caratteristiche principali:
  - **Sistema di trazione**: I nuovi treni utilizzano una tecnologia di trazione elettrica più efficiente e performante rispetto ai treni attualmente in servizio.
  - **Sistema di controllo della marcia**: I nuovi treni sono dotati di un sistema di controllo della marcia di ultima generazione (SCMT, ERTMS/ETCS, ecc..), che consente una gestione più precisa e automatizzata della circolazione.
  - **Interfaccia uomo-macchina (HMI)**: La cabina di guida dei nuovi treni è dotata di un'interfaccia HMI più moderna e interattiva, che fornisce al macchinista informazioni più dettagliate e in tempo reale sullo stato del treno e della linea.

CLASSIFICAZIONE DELLA MODIFICA

- L'introduzione di questa nuova generazione di treni è considerata **rilevante** ai fini della sicurezza per diverse ragioni:
  - **Impatto sull'infrastruttura**: La nuova tecnologia di trazione potrebbe richiedere modifiche all'alimentazione elettrica della linea (ad esempio, adeguamento della potenza erogata o della tensione). Il sistema di controllo della marcia del treno potrebbe richiedere l'installazione di nuove apparecchiature di segnalamento a terra e a bordo dei treni.
  - **Interazione con i treni esistenti**: I nuovi treni dovranno coesistere sulla stessa linea con i treni attualmente in servizio, che utilizzano tecnologie di trazione e di controllo della marcia diverse. È necessario garantire la compatibilità e l'interoperabilità tra i diversi sistemi per evitare interferenze o conflitti.
  - **Formazione del personale**: L'introduzione di nuove tecnologie e di una nuova interfaccia HMI richiede una formazione adeguata del personale di bordo (macchinisti) e del personale di terra (operatori del centro di controllo) per garantire la corretta comprensione e utilizzo dei nuovi sistemi e procedure.
  - **Procedure operative**: L'introduzione dei nuovi treni potrebbe richiedere modifiche alle procedure operative, ad esempio per quanto riguarda la gestione del traffico, la manutenzione, o le situazioni di emergenza.
  - **Potenziali conseguenze in caso di errore**: Un errore nell'utilizzo dei nuovi sistemi, un malfunzionamento delle apparecchiature, o un'interazione non corretta con i sistemi esistenti possono avere conseguenze gravi per la sicurezza, come ad esempio collisioni, deragliamenti, o interruzioni del servizio.

MOTIVAZIONE DELLA CLASSIFICAZIONE

- La decisione di classificare la modifica come rilevante è motivata dai seguenti fattori:
  - **Innovazione tecnologica**: L'introduzione di nuove tecnologie di trazione, di controllo della marcia e di interfaccia uomo-macchina rappresenta un'innovazione tecnologica significativa, che può introdurre nuovi rischi e richiedere una valutazione approfondita.
  - **Complessità del sistema**: Il sistema di trasporto metropolitano è un sistema complesso, in cui diversi elementi (infrastruttura, materiale rotabile, segnalamento, personale) interagiscono tra loro. Una modifica a uno di questi elementi può avere effetti a cascata su altri elementi, aumentando la complessità e il rischio di incidenti.
  - **Impatto potenziale sulla sicurezza**: Un incidente che coinvolge un treno della metropolitana può avere conseguenze gravi, sia in termini di perdite di vite umane che di danni materiali e interruzioni del servizio.

DEFINIZIONE DEL SISTEMA



La definizione del sistema deve riguardare quanto meno i seguenti punti:

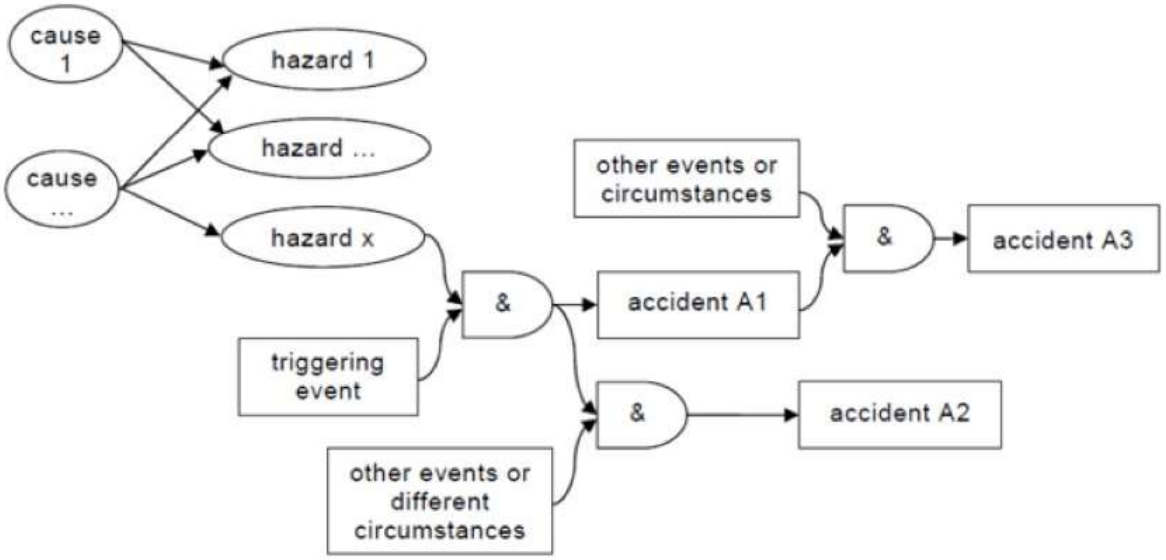
- gli **obiettivi del sistema** (finalità prevista);
- le **funzioni e gli elementi del sistema**, se del caso (compresi, tra gli altri, elementi umani, tecnici ed operativi);
- la **delimitazione del sistema**, anche in riferimento ai sistemi che interagiscono con esso;
- **punti d'interazione** materiali (sistemi che interagiscono) e funzionali (input ed output funzionali);
- le **condizioni ambientali del sistema** (ad esempio, flusso termico ed energetico, urti, vibrazioni, interferenze elettromagnetiche, utilizzo operativo);
- 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;
- le ipotesi che determinano i **limiti della valutazione dei rischi.**

PUNTI DI INTERAZIONE

- Per ciascun punto d'interazione del sistema da valutare, e fatte salve le specifiche definite nelle specifiche tecniche di interoperabilità relativamente ai punti d'interazione, gli operatori del settore ferroviario cooperano per individuare e gestire congiuntamente gli eventi pericolosi e le relative misure di sicurezza. Il proponente coordina la gestione dei rischi condivisi nei punti di interazione.
- L'operatore che, per adempiere un requisito di sicurezza, ritiene necessaria una misura di sicurezza che non è in grado di applicare personalmente trasferisce ad un altro operatore, previo accordo di quest'ultimo, la gestione del relativo evento pericoloso secondo le modalità definite al punto 4
- L'operatore che mette in atto la misura di sicurezza informa tutti gli operatori interessati dal problema nell'ambito del sistema da valutare o, per quanto ne sia a conoscenza, nell'ambito di altri sistemi che si avvalgono della stessa misura di sicurezza.
- Qualora non sia possibile giungere ad un accordo tra due o più soggetti, il proponente è tenuto a trovare una soluzione idonea.
- Quando un operatore non è in grado di soddisfare un requisito stabilito in una norma nazionale notificata, il proponente chiede il parere dell'autorità competente

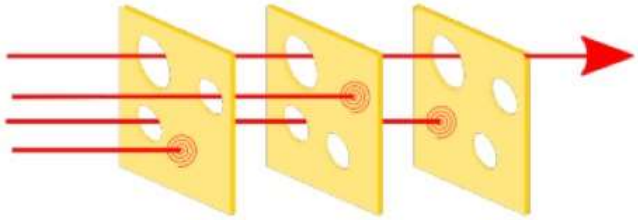
IDENTIFICAZIONE DEGLI EVENTI PERICOLOSI – HAZARD

Hazard: 'a condition that could lead to an accident'





Reason's swiss-cheese model



«Barriers»

IDENTIFICAZIONE DEI PERICOLI – HAZARD

- Si identificano tutti i punti deboli e le relative conseguenze al confine dello specifico sistema individuato.
- L'identificazione è **SISTEMATICA**, durante l'intero ciclo di vita e avviene a cura di un gruppo di esperti.
- L'identificazione può avvenire in modo empirico e in modo creativo. Si aggiunge una ulteriore modalità che è quella degli incidenti prevedibili.

IDENTIFICAZIONE EMPIRICA

- **Identificazione empirica -> sistema noto**
  - Come tutti i metodi empirici si basano sulla conoscenza storica, quanti si fonda sull'esperienza maturata nell'individuare eventi pericolosi.
  - È applicabile in attività ordinarie, di cui si conosce molto.
  - Poco applicabile in attività nuove che richiedono un approccio creativo.

Tra i metodi empirici ci sono:

- **FMECA (Failure Method Effects and Critical Analisys)**: Analisi dei modi di guasto e degli effetti dei guasti. (guasti componenti)
- **Analisi delle attività per le interfacce uomo-macchina (errori umani)**

IDENTIFICAZIONE CREATIVA
IDENTIFICAZIONE PREVEDIBILE

- **Identificazione creativa**
  - Si fonda su **BRAINSTORMING** tra esperti con esperienze trasversali.
  - Tra i metodi creativi ci sono:
  - HAzOP
- **Identificazione degli incidenti prevedibili**
  - Si fonda sull'analisi di archivi storici di incidenti occorsi (tra treni, a bordo, in stazione, ecc....), con l'individuazione del fattore scatenante.

PROCESSO DI IDENTIFICAZIONE DEI PERICOLI

- Il regolamento prevede che l'identificazione dei pericoli sia un processo **sistematico** e **completo**, che tenga conto di tutti i fattori rilevanti. In particolare, il punto 2.2 suggerisce di considerare:
  - **Fattori tecnici**: Malfunzionamenti di attrezzature, guasti di componenti, errori di progettazione, difetti di costruzione o manutenzione.
  - **Fattori umani**: Errori del personale (macchinisti, controllori del traffico, manutentori), comportamenti non sicuri, carenza di formazione, stress, fatica.
  - **Fattori ambientali**: Eventi naturali (tempeste, alluvioni, frane), condizioni meteorologiche avverse (ghiaccio, neve, nebbia), incendi, terremoti.
  - **Fattori organizzativi**: Inadeguatezza delle procedure, carenza di supervisione, problemi di comunicazione, turni di lavoro eccessivi.
  - **Interazioni tra fattori**: Combinazioni di fattori diversi che possono aumentare il rischio di incidenti (ad esempio, errore umano + guasto tecnico + condizioni ambientali avverse).

TECNICHE DI IDENTIFICARE DEI PERICOLI - HAZARD

- Il proponente individua un Expert-Group (fattori tecnici, umani, ecc....)
- L'EG utilizza principalmente la tecniche di **Brainstorming** combinandola a:
  - **Fault Tree Analysis (FTA)** partendo da eventi incidentali occorsi;
  - **What – If Strutturata** usata anche per individuare misure di sicurezza;
  - **FMECA:** Analisi dei Modi, degli Effetti e della criticità dei Guasti
  - **Analisi storiche** di dati a disposizione sugli inconvenienti (near miss) ed incidenti;
  - Indicazioni fornite dall'ANSFISA anche nella Relazione Annuale della Sicurezza;
  - Caratteristiche specifiche indicate nei Fascicoli di Linea del GI o Esercente;
  - Altra legislazione specifica (antisismica, idrogeologica, gallerie, Direttiva Seveso, ecc..);

FAULT TREE ANALYSIS (FTA)

- L'analisi mediante Albero dei Guasti è un metodo diffusamente accettato di presentare l'interazione tra guasti di sistemi, sottosistemi e componenti ed è descritta nella IEC 61025.
- L'analisi mediante Albero dei Guasti può essere usata **qualitativamente**, sia per i guasti casuali sia per quelli sistematici, e **quantitativamente**, quando il guasto può essere quantificato, al fine di individuare nuovi eventi guasto da analizzare mediante l'analisi degli Eventi Guasto e mediante l'Analisi dei Modi, degli Effetti e della Criticità dei Guasti (FMECA).
- L'analisi mediante Albero dei Guasti determina le cause di un guasto di un sistema dall'esame delle relazioni logiche tra guasti di altri sotto-sistemi, componenti e in alcuni casi procedure operative.
- Le operazioni logiche sono rappresentate, nel diagramma, dai simboli dell'algebra Booleana.
  - OR nel caso di eventi indipendenti che dovrebbero verificarsi insieme per determinare un guasto
  - AND sono entrambe utilizzate nell'ambito di un albero dei guasti

FTA

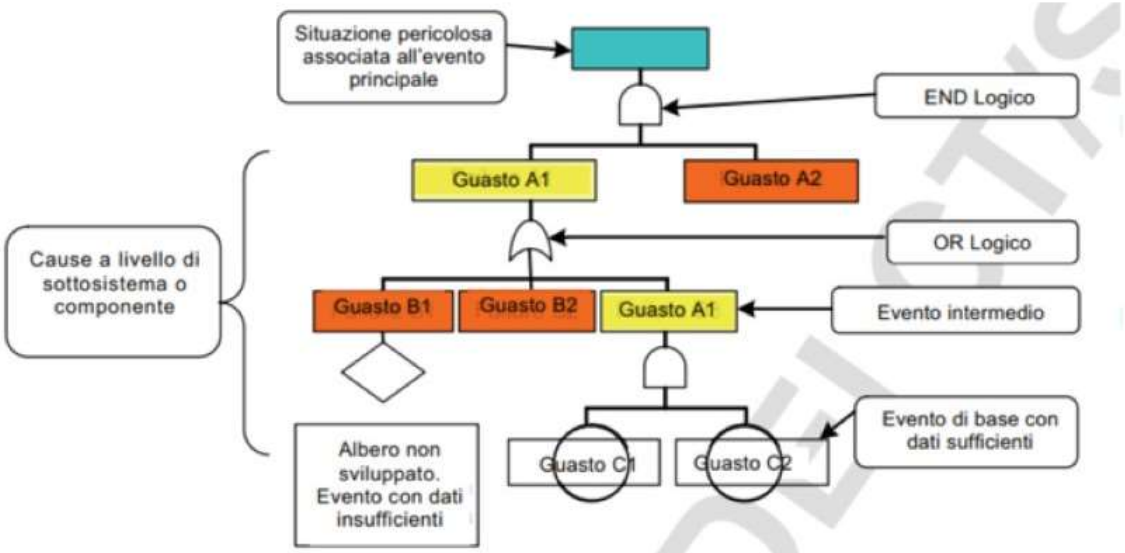


Figura E.4 – Analisi mediante Albero dei Guasti – Esempio

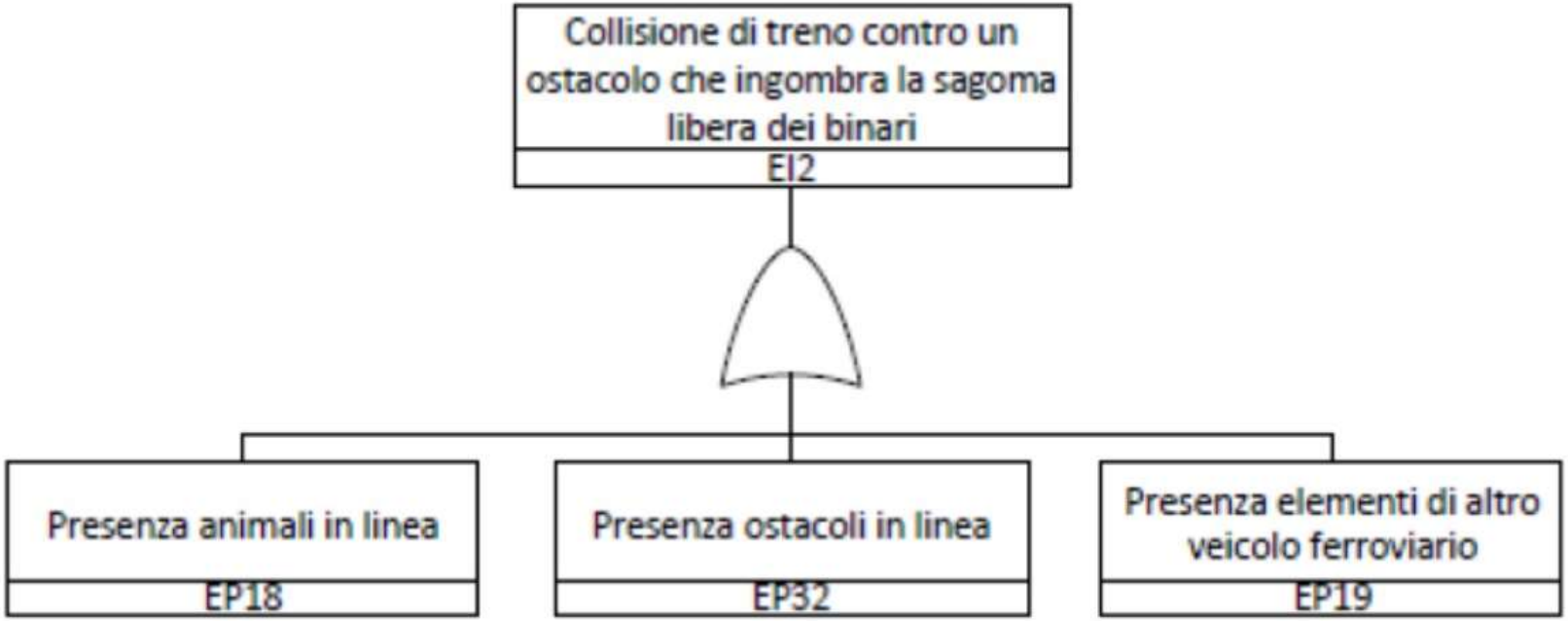
L'FTA si concentra sull'identificazione delle cause che possono portare a un evento indesiderato

L'albero dei guasti rappresenta graficamente le relazioni logiche tra le diverse cause.

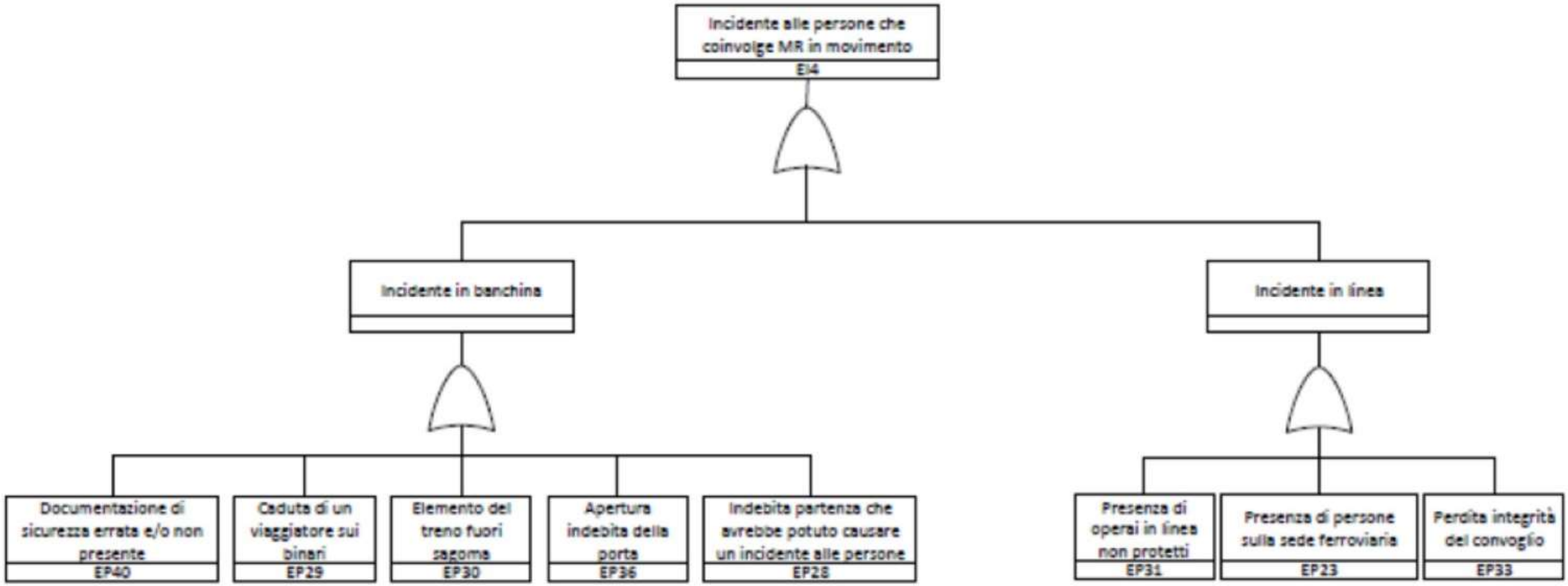
FTA

- Una particolare attenzione dovrebbe essere prestata, oltre che alle caratteristiche fisiche, tecniche e funzionali dei componenti, anche ai processi operativi attuati.
- **una manutenzione inadeguata può determinare il guasto di componenti che generalmente sono individuati come indipendenti**
- Le specifiche di manutenzione congiunta sono un esempio di processo operativo che può essere assimilato ad un modo comune di guasto;
- Altri esempi sono le precauzioni contro l'accesso non autorizzato nelle aree ferroviarie, o gli effetti atmosferici come le fulminazioni."

ESEMPI - FTA


Collisione di treno contro un ostacolo che ingombra la sagoma libera dei binari
EI2
Presenza animali in linea
EP18
Presenza ostacoli in linea
EP32
Presenza elementi di altro veicolo ferroviario
EP19

ESEMPI - FTA


Incidente alle persone che coinvolge MR in movimento
EI4
Incidente in banchina
Incidente in linea
Documentazione di sicurezza errata e/o non presente
EP40
Caduta di un viaggiatore sui binari
EP29
Elemento del treno fuori sagoma
EP30
Apertura indebita della porta
EP36
Indebita partenza che avrebbe potuto causare un incidente alle persone
EP28
Presenza di operai in linea non protetti
EP31
Presenza di persone sulla sede ferroviaria
EP23
Perdita integrità del convoglio
EP33

ESEMPI - FTA


Incendio di un treno
EI3
Treno frenato
EP37
Cortocircuito in apparato del treno
EP24
Innesco di incendio causato da viaggiatore
EP25
Innesco incendio in motore termico
EP27
Incendio provocato dall'esterno
EP38

ANALISI WHAT-IF STRUTTURATA

E' una forma predittiva di revisione della sicurezza ed è preferibilmente utilizzata nell'analisi di non conformità in precedenza evidenziata nel Hazard Log.

Questo metodo si basa sulla formulazione di domande ipotetiche ("***Cosa succederebbe se...***") per esplorare possibili scenari di pericolo.

L'analisi è gestita in accordo ai seguenti principi:

- Analizzare gli eventi e le deviazioni dagli stati normali
- Effettuare una prima approssimazione preliminare dei rischi
- Contro-misure possibili

Esempio pratico:
Durante una revisione delle procedure operative, il responsabile della sicurezza potrebbe chiedere: "Cosa succederebbe se un macchinista dovesse avere un malore durante la guida del treno?". Questo può portare all'identificazione di pericoli legati alla gestione di situazioni di emergenza e alla definizione di procedure adeguate.

OUTPUT

Al termine della sessione "What-if?", il team genera:

- Un elenco di potenziali pericoli e scenari problematici,
- Un elenco di valutazione delle misure di sicurezza esistenti
- Un elenco di suggerimenti per ulteriori miglioramenti.
- Queste informazioni potrebbero poi essere utilizzate per aggiornare le procedure operative, rafforzare la formazione del personale o implementare nuove misure di sicurezza.
- Questo è un esempio di come la tecnica "What-if?" possa essere applicata in modo pratico per identificare rischi e stimolare il miglioramento continuo della sicurezza nel contesto della manutenzione ferroviaria.

ESEMPIO DI APPLICAZIONE ''WHAT-IF''

- Hazard = **AVARIA SOSPENSIONE PNEUMATICA**
- Rischio associato = **INACCETTABILE**
- Dall'applicazione dell'analisi "**WHAT-IF**" viene predisposto una misura mitigativa procedurale che rende il rischio **TOLLERABILE**.
- Misura di sicurezza = l'anomalia viene segnalata tramite il lampeggiamento sul quadro di segnalazione principale del pittogramma "**AVARIA SOSPENSIONE PNEUMATICA**"
- Il Personale di Condotta (PdC) applica la procedura che prevede l'avviso al Personale di Bordo (PdB) e l'applicazione della guida di depannage alla prima fermata.
- Il PdC identifica il carrello con la sospensione in avaria isolandola come previsto dalla guida di depannage.
- La procedura messa in opera dal PdB in caso di anormalità di sospensione, prevede che la chiusura delle porte deve essere effettuata dalla porte la più vicina alla sospensione in avaria verificando il rientro del gradino mobile.
- In caso di non rientro del gradino mobile della porta corrispondente al carrello con la sospensione isolata, viene applicata la **procedura di rientro manuale del gradino mobile** con isolamento della porta da parte del PdB.

FMECA - FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS

- Analisi dei modi e degli effetti dei guasti. Metodo per l'individuazione e le modalità di guasto di ogni oggetto sotto analisi.
- L'oggetto può essere un sistema complesso o un singolo componente fisico e include sia componenti fisici che processi, funzioni, hardware, software e errori umani.
- È una tecnica bottom-up in quanto l'individuazione di un guasto complesso parte dall'individuazione di guasti elementari.
- Attraverso la metodologia FMECA è possibile effettuare la verifica di robustezza dei software, vale a dire testare la capacità di un software di mantenere il requisito di sicurezza anche in presenza di eventuali guasti. (fail-safe)

FMECA

Si tratta di un processo strutturato e sistematico che si articola in diverse fasi:

1. **Definizione del sistema:**
   - Si definisce l'ambito dell'analisi, identificando i componenti e le funzioni del sistema.
   - Si crea un diagramma a blocchi o un albero di guasto per rappresentare le interconnessioni tra i componenti.
2. **Identificazione dei modi di guasto:**
   - Per ciascun componente, si identificano tutti i possibili modi in cui può guastarsi (ad esempio, rottura, blocco, usura).
   - Si utilizzano diverse fonti di informazione, come dati storici, manuali tecnici e pareri di esperti.

FMECA

3. Analisi degli effetti dei guasti:

- Per ciascun modo di guasto, si analizzano le conseguenze a livello locale (sul componente stesso) e a livello globale (sull'intero sistema).
- Si valutano gli effetti in termini di sicurezza, prestazioni, costi e impatto ambientale.

4. Valutazione della criticità:

- Si assegna un punteggio a ciascun modo di guasto in base a tre parametri:
  - Probabilità di occorrenza: Quanto è probabile che il guasto si verifichi?
  - Gravità delle conseguenze: Quanto sono gravi le conseguenze del guasto?
  - Rilevabilità del guasto: Quanto è facile rilevare il guasto prima che si verifichino conseguenze gravi?
- Si calcola il Risk Priority Number (RPN) moltiplicando i tre punteggi.

FMECA

5. Definizione delle azioni correttive:

- Per i modi di guasto con RPN elevato, si definiscono azioni correttive per ridurre la probabilità di occorrenza, la gravità delle conseguenze o aumentare la rilevabilità.
- Esempi di azioni correttive: manutenzione preventiva, ridondanza dei componenti, sistemi di monitoraggio avanzati.

- **Vantaggi del metodo FMECA:**
  - Identificazione sistematica dei possibili modi di guasto.
  - Valutazione approfondita degli effetti e della criticità dei guasti.
  - Prioritizzazione delle azioni correttive in base al rischio.
  - Miglioramento della sicurezza e dell'affidabilità dei sistemi.
  - Supporto alla progettazione di sistemi più robusti e resilienti.

REGISTRO EVENTI PERICOLI – HAZARD LOG

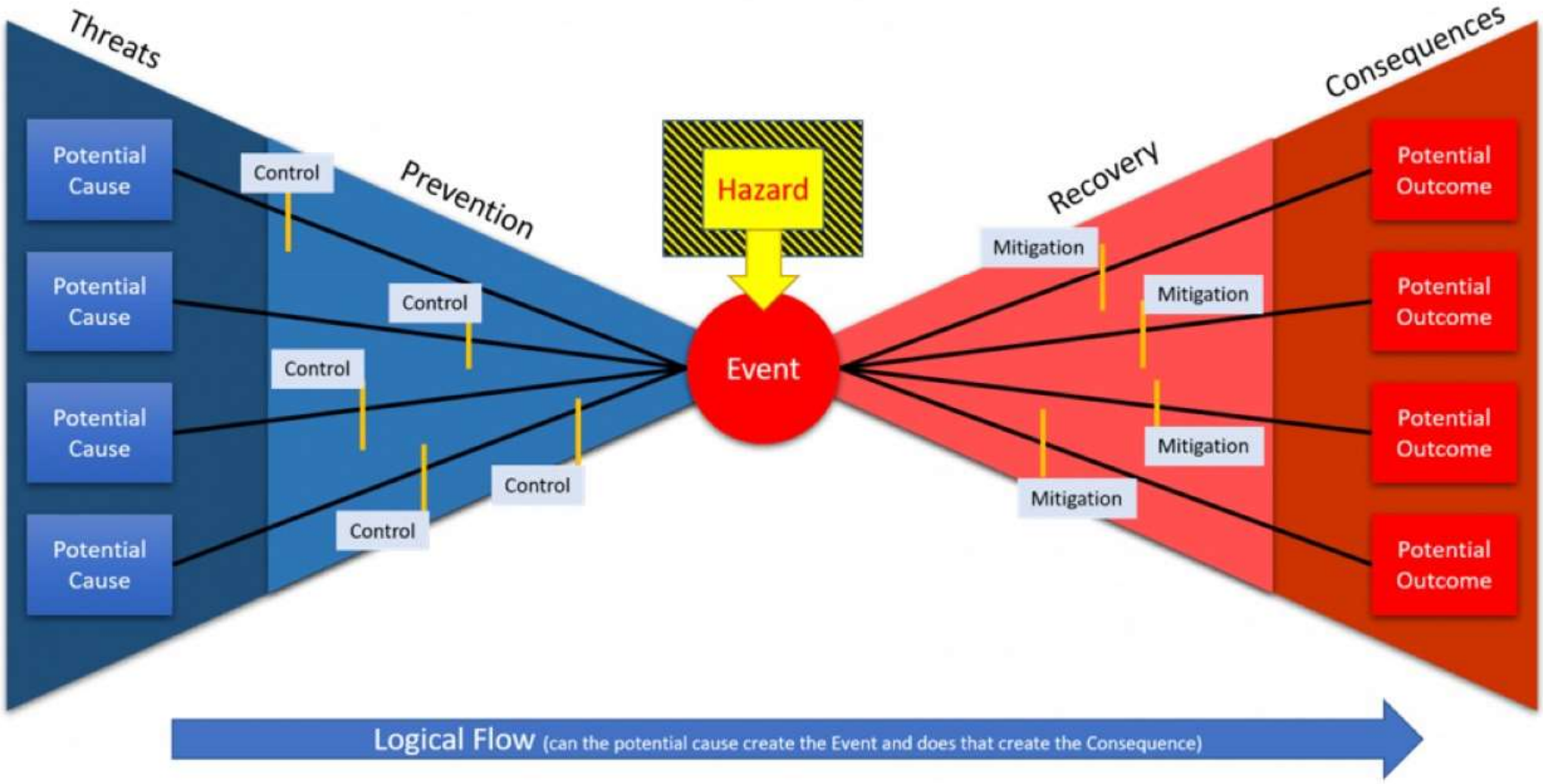
- Registro contenente tutti gli eventi pericolosi individuati (anche quelli considerati non rilevanti ai fini della sicurezza) nella fase preliminare e riscontrati durante il ciclo di vista del sistema (Documento vivo)
- Elementi essenziali contenuti nel Registro

Descrizione della situazione pericolosa	Livello di rischio calcolato tenendo conto delle frequenza (probabilità stimata) e delle possibili conseguenze	Esempi di Misure intraprese per ridurre il rischio	Livello di rischio resid dopo le misure riduzione
	Trascurabile Tollerabile Indesiderabile intollerabile	Misure di progetto Misure manutentive Misure in esercizio	Trascurabile Tollerabile Indesiderabile intollerabile

ANALISI DELLE CONSEGUENZE

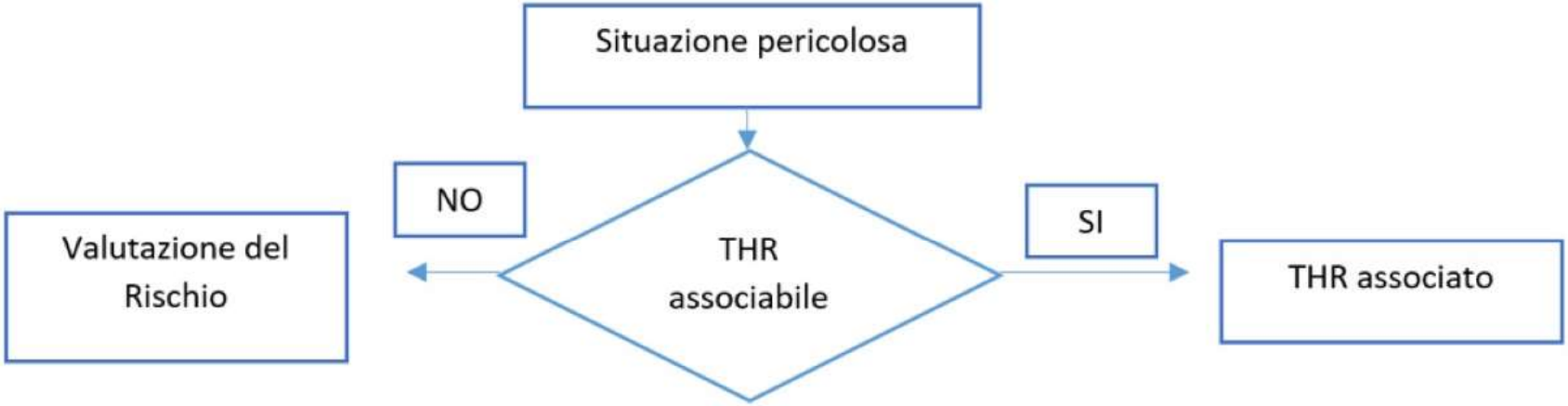
- Partendo dalle situazioni pericolose individuate si valutano tutte le possibili conseguenze dirette e indirette (come ad esempio il crollo di un ponte a seguito di un deragliamento o incendio).
- L'approccio indicato nelle EN50126-2 è quello di utilizzare il più possibile dati noti su incidenti e/o consultare esperti del settore.
- Una tecnica nota è la ETA (Event Tree Analisys) Albero degli eventi

FTA + ETA = BOWTIE



VALUTAZIONE DEL RISCHIO

- Allocazione del THR, se possibile



- THR – tasso di occorrenza di una situazione pericolosa che determinerebbe un livello di rischio inaccettabile

TASSO DI OCCORRENZA - THR

- Non sempre è fattibile associare un THR come ad esempio:
- Situazioni pericolose riconducibili e guasti o rotture di parti meccaniche / elettriche che fanno affidamento ad esempio sulla resistenza dei materiali.
- Situazioni pericolose riconducibili a mancate applicazioni di regolamenti di esercizio (personale, manutentori, ecc....)
- Quando non è possibile associare un THR -> Valutazione del rischio attraverso diversi metodi (quantitativo, qualitativo, semi quantitativo)

PROFONDITÀ DI ANALISI

- Il livello di dettaglio della valutazione del rischio dovrebbe essere proporzionato al rischio prendendo in considerazione quelle situazioni tali che le conoscenze (archivi storici, ecc…) hanno dato luogo a situazione realmente pericolose.
- Sebbene la EN 50126-1 sia applicabile all'intero sistema ferroviario e ai suoi sottosistemi, il livello di **profondità di analisi** necessario per la dimostrazione della sicurezza dipende dal livello di servizio in uso, dalle condizioni al contorno, alle interfacce e da altri fattori simili.

PIANO DELLA SICUREZZA

- Nell'ambito del Regolamento (UE) n. 402/2013 e della norma EN 50126, il concetto di "**PIANO DI SICUREZZA**" è strettamente legato al processo di gestione del rischio e alla sua documentazione.
- Non è un documento autonomo, ma piuttosto un elemento chiave all'interno del più ampio Dossier di Sicurezza (Safety Case).
- Un Piano di Sicurezza (Safety Plan) è un documento operativo che descrive in dettaglio come il processo di gestione della sicurezza verrà gestito e implementato durante l'intero ciclo di vita di un progetto (es. un nuovo veicolo, una modifica a un'infrastruttura).
- Come definito dalla norma EN 50126, il piano di sicurezza è l'elemento che assicura che il processo di valutazione del rischio non sia un'attività "una tantum", ma un'attività continua e gestita.
- Il piano di sicurezza serve a stabilire:
- Chi fa cosa: Chi è responsabile della sicurezza (ruoli e responsabilità).
- Cosa viene fatto: Le attività di valutazione del rischio che verranno eseguite.
- Come viene fatto: I metodi e gli strumenti utilizzati.
- Quando viene fatto: La pianificazione temporale di ogni attività.

ANALISI DI SENSIBILITA' (SENSITIVITY ANALYSIS)

- **<u>Per sostenere la decisione può essere utilizzata un'analisi di sensibilità</u>**
- **Analisi di sensibilità**: metodo per determinare la robustezza di una valutazione. Valutare il **GRADO DI INCERTEZZA** (incertezza intrinseca nel processo di valutazione) ed eventuali fattori che possono amplificarne lo scostamento.
- Attraverso l'analisi di sensibilità è possibile aumentare la confidenza circa Il **RISCHIO GLOBALE ASSOCIATO**

Come?

- Attraverso **MODELLI** che si basano sul principio:
- Valutare l'impatto sulle variabili di uscita a fronte di variazioni su una o più variabili di ingresso.
- Ci sono diverse tecniche:
  - Analisi One a time
  - Stress test
  - Analisi per scenari

MODELLI DI ANALISI

METODI DI VALUTAZIONE DEL RISCHIO

Esistono diversi metodi di valutazione del rischio i quali si suddividono principalmente in:

- **Metodi QUALITATIVI**
- **Metodi IBRIDI o SEMIQUALITATIVI**
- **Metodi QUANTITATIVI**
  - **Metodo Deterministico**
  - **Metodo Probabilistico**

METODI QUALITATIVI

- Con buona probabilità una **VALUTAZIONE QUALITATIVA** è sufficiente per la maggior parte delle situazioni pericolose.
- **CONFIDA SUL GIUDIZIO DI ESPERTI**
- **SU GUASTI SISTEMATICI**
- **SU RISCHI GESTITI DA NORME TECNICHE, CODICI DI BUONA PRATICA, SISTEMA DI RIFERIMENTO SIMILE**
- **NON VI È UNA COMPLETA ASSENZA DI QUANTIFICAZIONE MA SONO GENERALMENTE UTILIZZATE STIME DELL'ORDINE DI GRANDEZZA**
- **GUASTO SISTEMATICO** (EN 61508 e EN50126):
- Guasto connesso in modo deterministico ad una certa causa che può essere eliminato solo attraverso una modifica di Progetto/Processo/Organizzazione

METODI IBRIDI O SEMIQUALITATIVI

- Valutazione separata della frequenza, delle conseguenze e assegnazione del livello di rischio residuo attraverso l'uso della matrice dei rischi, introdotta in Italia dalla CENELEC 50126 ed estesa al sistema ferroviario dalla disp. RFI 13/2001 e modificata dalla disp. RFI 51/2007.
- La norma CENELEC 50126 ha fornito gli elementi per definire **qualitativamente**: frequenza e conseguenze, a cui associare degli intervalli numerici (da qui il concetto **semi-quantitativo**)

METODI IBRIDI O SEMIQUALITATIVI

- **Stima delle Frequenze**
- Per frequenza di accadimento si intende il numero di eventi per anno.

Classe di Frequenza	F	Intervallo di Frequenza
Frequente	F≥4	Da 1 ogni 20gg a 1 ogni 3 mesi
Probabile	0,8≤F≤4	
Occasionale	0,143≤F≤0,8	
Remoto	0,029≤F≤0,143	
Improbabile	0,006≤F≤0,029	
Inverosimile	F≤0,006	Meno di 1 ogni 175 anni

METODI IBRIDI O SEMIQUALITATIVI

- **Stima delle conseguenze**
- Partendo dalla FWSI (fatalities ans Weighted Serious Injures) -> unità di misura di 1 decesso in seguito ad un incidente ferroviario.
- È stato definito
- 1 morto -> FWSI =1
- 10 Feriti Gravi = 1 Morto -> 1 Ferito Grave = 0,1 FWSI
- 10 Feriti lievi = 1 Ferito Grave -> 1 Ferito Lieve = 0,01 FWSI

Conseguenza	**FWSI = G**
Catastrofico	$G \geq 2$
Critico	$0,1 \leq G < 2$
Marginale	$0,01 < G < 0,1$
insignificante	$G \leq 0,01$

- Partendo da queste assunzioni per ciascuno dei livelli di gravità qualitativi definiti dalla EN50126 è possibile associare un valore quantitativo.
- Nel fare questa associazione con la scala di gravità si tiene conto anche di quanto disposto al Reg UE 1136/2015 che modifica il Reg UE 402/2013 definisce un **incidente catastrofico** un incidente che produce almeno 2 morti o 20 feriti gravi
- Per quanto riguarda i danni all'ambiente, al materiale rotabile, all'infrastruttura e al sistema si associa
- FWSI = 0,1 - 1 Ferito grave = danno ambiente a cose pari a 150 mila Euro e 6 ore di interruzione

METODI QUANTITATIVI

- Il metodo semi-quantitativo presenta ovviamente dei limiti che sono:
- È possibile stimare solo eventi classificati al più come remoti, non potendo fare riferimento a serie storiche più ampie (più di 175 anni nell'ipotesi di inverosimile)
- È possibile rivedere il rischio residuo associato ad una misura mitigativa solo dopo la sua applicazione. Non avendo dati a supporto
- La valutazione del rischio di tipo quantitativo, rispetto a quello qualitativo ha una minor margine di incertezza. Il motivo è l'utilizzo di numerosi dati oggettivi e validati.

METODI QUANTITATIVI - VANTAGGI

- maggiore accuratezza rispetto alla valutazione qualitativa del rischio, a condizione che i dati siano disponibili e sufficientemente accurati;
- identificazione dei difetti nella progettazione o di carenze nei sistemi di sicurezza;
- integrazione di tutti i contributi di rischio alla determinazione di indicatori globali (danno atteso o rischio totale, rischio individuale e rischio sociale o collettivo);
- favorisce l'identificazione di malfunzionamenti nascosti a causa di analisi più dettagliate;
- fornisce una migliore comprensione delle conseguenze di un pericolo

METODI QUANTITATIVI - SVANTAGGI

- Costoso
- Necessita di molti dati

Il metodo quantitativo risulta necessario nell'ipotesi di:

- situazioni pericolose che indurrebbero ad eventi catastrofici o di particolare rilievo
- quando c'è un chiaro dettato normativo ad imporlo. Vedi nel caso del DM Gallerie oppure requisiti fissati per il segnalamento (EN50129).
- Nel caso di sistemi nuovi per i quali non si ha sufficiente esperienza.
- Un metodo quantitativo è la combinazione del metodo FTA e ETA da cui si ottiene il diagramma bow-tie.

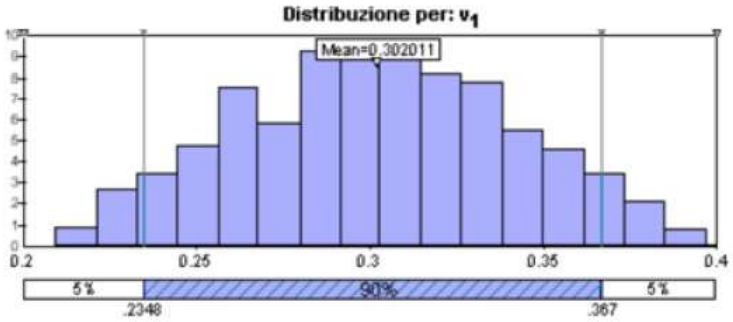
METODO DETERMINISTICO

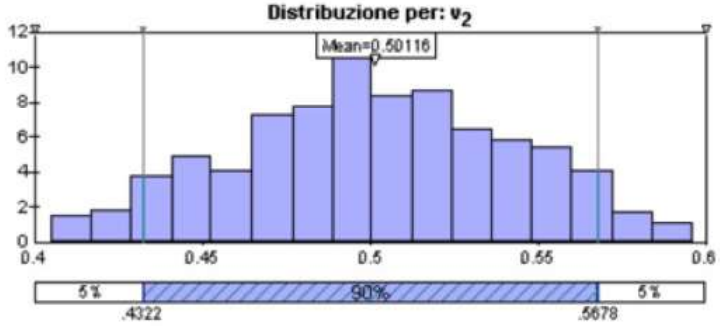
- L'approccio deterministico è basato su 2 concetti:
  - **PREVEDERE** il verificarsi di un guasto
  - **PREVENIRE** il verificarsi di un evento indesiderato
- **INPUT**: I dati di input di un Modello deterministico sono valori fissati sulla base di ipotesi di scenario preventivo.

- **QUANDO SI USA L'APPROCCIO DETERMINISTICO?**
- Quando si hanno a disposizione poche osservazioni. La valutazione è basata su una **PREVISIONE** dei tassi di guasto
- **Detto approccio è alla base del DPR 753/80 il quale prescrive che gli operatori ferroviari, nel gestire la propria parte di sistema devono adottare tutte le misure e le cautele tecniche atte ad evitare sinistri.**

METODO PROBABILISTICO

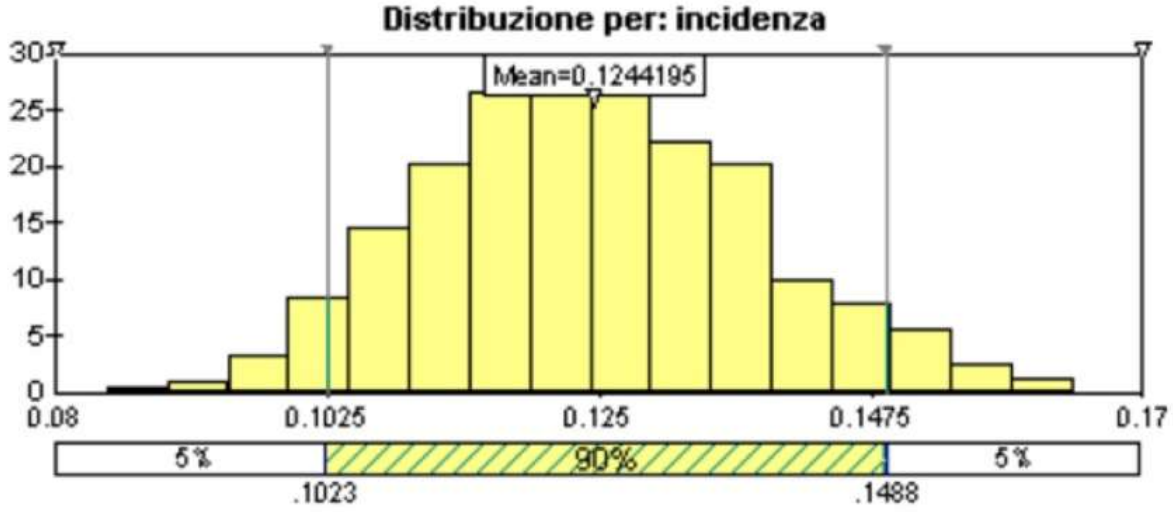
- L'approccio probabilistico è basato sulla conoscenza delle **distribuzioni** di affidabilità di sottosistemi e componenti.
- Prendendo a riferimento le solite 2 variabili v1 e v2 di queste conosciamo la **distribuzione**





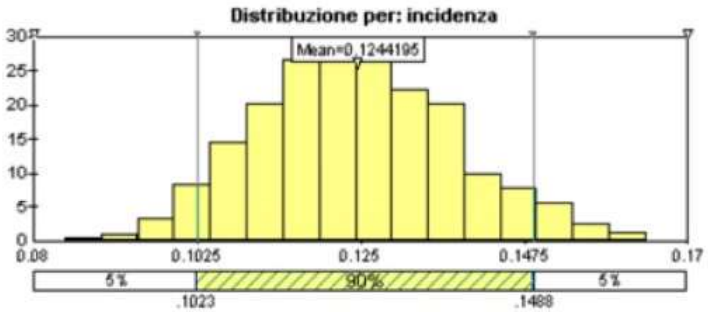
METODO PROBABILISTICO

- L'incidenza i è simulata con il metodo "MONTECARLO" che tiene conto delle 2 distribuzioni v1 e v2



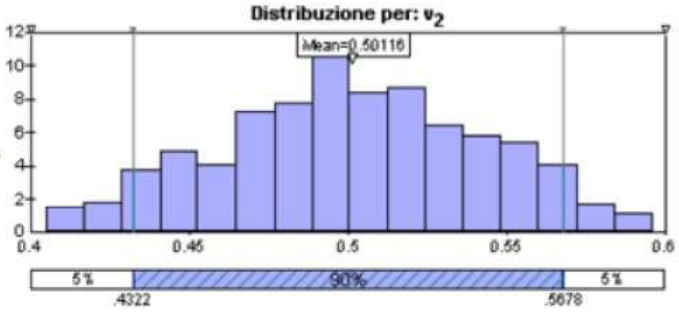
METODO PROBABILISTICO

- L'incidenza i è simulata con il metodo "MONTECARLO" che tiene conto delle 2 distribuzioni v1 e v2



IN: Distribuzione dell'incidenza

Metodo Probabilistico



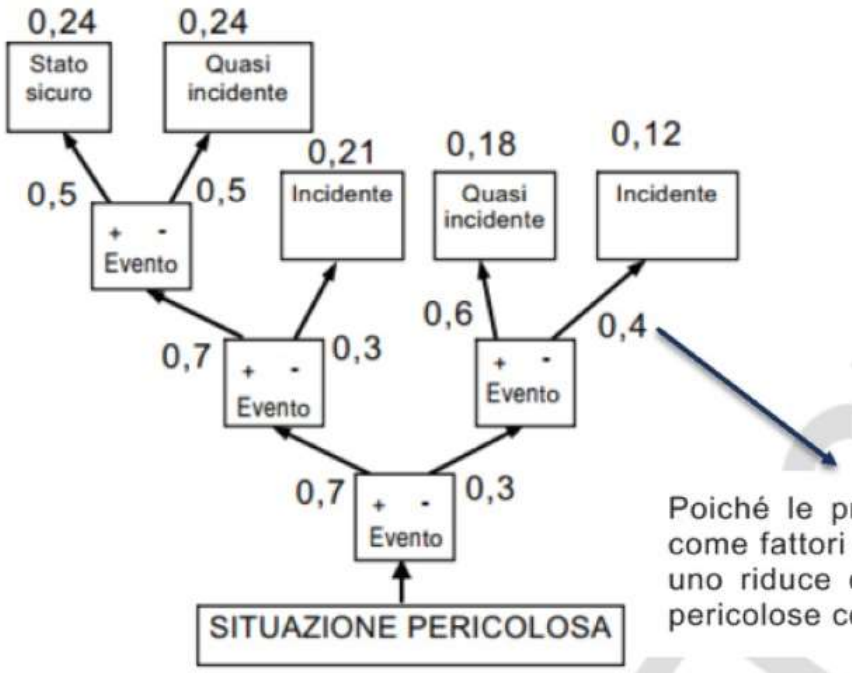
OUT: Distribuzione del rischio

- Con l'avvento dei sistemi più complessi, che adottano sistemi computerizzati o comunque sistemi con tassi di guasto non prevedibili, è stato giocoforza necessario individuare un approccio di tipo "risck based" di natura probabilistica.
- Una tecnica che utilizza l'approccio probabilistico è la FTA.

APPROCCIO MISTO DETERMINISTICO/PROBABILISTICO

- Ci sono sottosistemi ferroviari per i quali è difficile applicare un approccio probabilistico, vedi ad esempio la resistenza a fatica di alcuni componenti meccanici, ragion per cui in questo caso si utilizza un mix di approccio deterministico/probabilistico.
- In pratica si utilizza l'approccio deterministico fino ad un certo livello del sistema, per poi procedere in profondità con l'approccio probabilistico.
- Altro esempio tipico esempio di mix di approccio deterministico/probabilistico è sui sistemi computerizzati costituiti da HW e SW. Mentre sul HW è possibile adottare un approccio probabilistico perché sono noti i tassi di guasto dei singoli componenti, sui SW invece è necessario utilizzare un approccio di tipo deterministico. Una raccomandazione sull'utilizzo dei metodi di sviluppo dei SW è data dalla EN 50128.

ANALISI DELL'ALBERO DEGLI EVENTI (ETA)



- Attraverso il metodo ETA si individuano, partendo dall'evento iniziale, tutti i possibili scenari e quindi eventi successivi.
- L'ETA analizza il tasso di occorrenza di un evento e della sequenza di eventi successivi, fino a calcolare la probabilità di occorrenza dell'evento finale (incidente, deragliamento, svio, incendio, ecc.....)

Poiché le probabilità degli eventi intermedi sono inferiori all'unità, questi eventi sono noti come fattori di riduzione del rischio (la moltiplicazione per un fattore di probabilità inferiore ad uno riduce ovviamente la probabilità che si verifichi un incidente – non tutte le situazioni pericolose conducono automaticamente ad un incidente).

DIAGRAMMA BOW-TIE

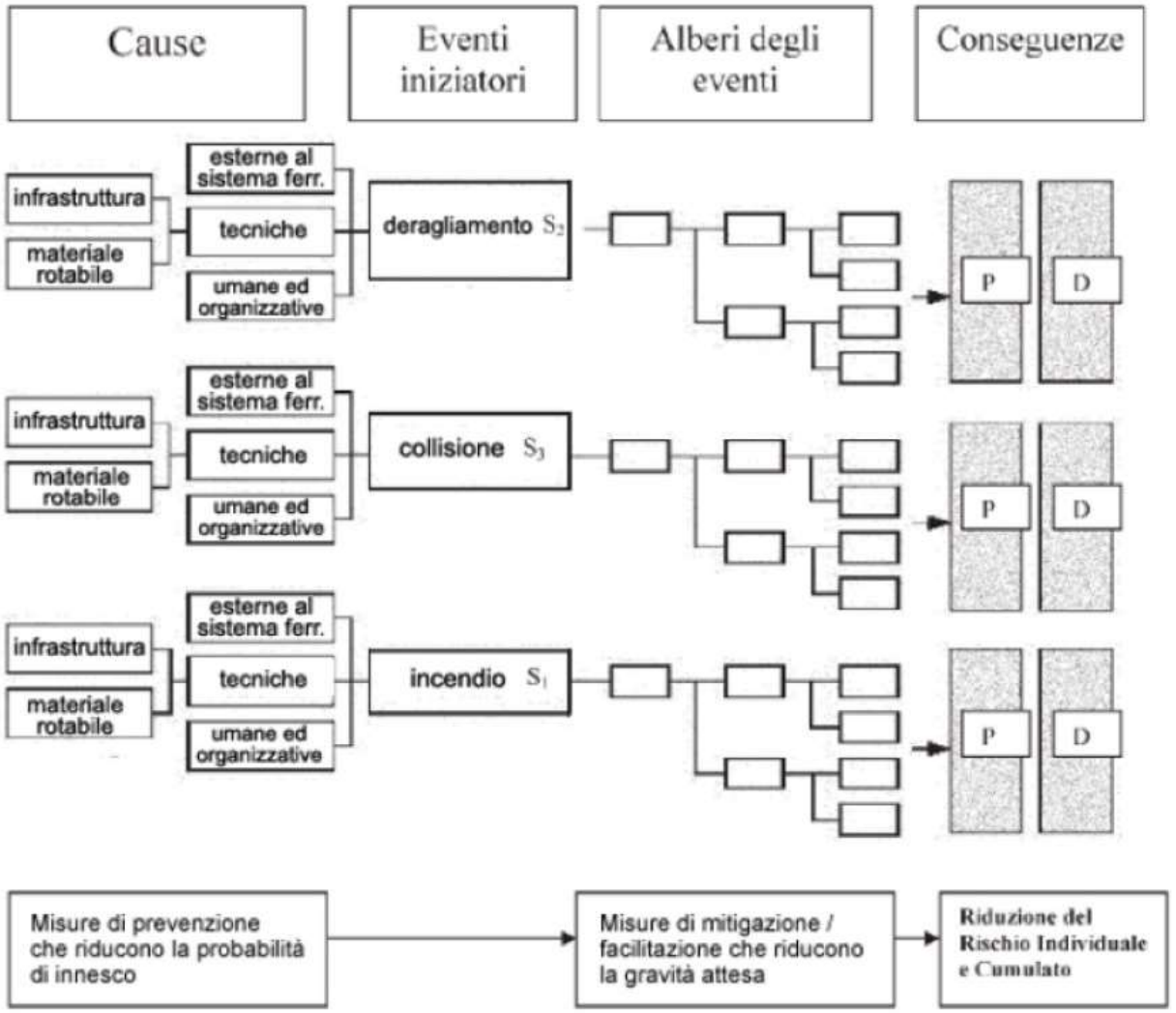


Tavola 3.4.I: Schema della procedura estesa

RISCHIO TOTALE E RISCHIO INDIVIDUALE

- Attraverso questo metodo è possibile quantificare il Rischio Totale **RT** e il Rischio individuale **Ri** (del singolo evento iniziatore), moltiplicando la Probabilità di occorrenza del singolo evento con il danno stimato

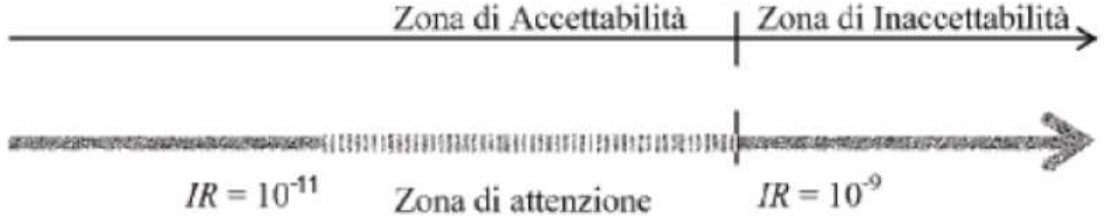
$$R_i = P_i D_i \qquad RT = \sum_i P_i D_i$$

- Partendo da questi indicatori, così come descritto nel DM Gallerie si può ottenere il **livello del rischio atteso individuale (IR)**, normalizzando il valore del rischio totale rispetto alla popolazione esposta in un intervallo di tempo prefissato (un anno) e per Km percorso
- ***IR = numero di fatalità/pass * Km * anno***
- È altresì definito anche il **livello di Rischio Cumulato (CR)** sulla base della distribuzione di probabilità cumulata del livello di danno riferita sempre all'anno.
- ***CR = numero di fatalità/Km * anno***
- L'IR e CR costituiscono le grandezze di riferimento per l'accettabilità del livello di rischio.

SOGLIE DI ACCETTABILITÀ - IR

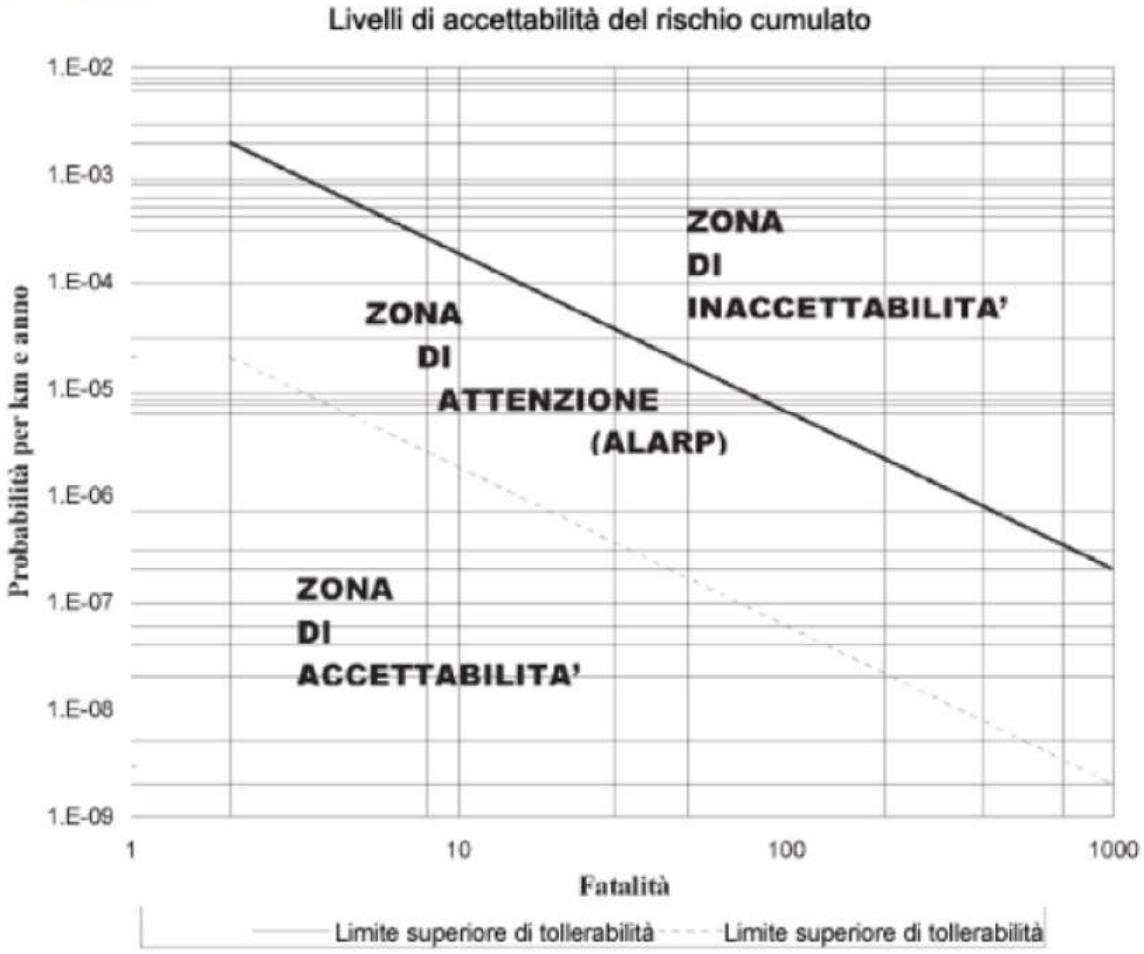
- Le soglie limite, laddove esistenti, sono imposte dalle norme tecniche, dalle STI o dalla normativa nazionale.
- In particolare nel DM Gallerie sono imposte nelle soglie di accettabilità relative al IR.
- La soglia di accettabilità IR è la seguente:

- Abbiamo un limite di inaccettabilità, un limite di accettabilità e una fascia cosiddetta di ALARP (As Low As Reasonably Practicable).
- La zona di ALARP è considerata la più bassa possibile al di sotto della quale qualsiasi sforzo ulteriore di riduzione del rischio non sarebbe giustificato in termini di benefici attesi.



SOGLIE DI ACCETTABILITÀ - CR

- Analogamente la soglia di accettabilità CR



CLASSIFICAZIONE DEGLI HAZARD

Evento Pericoloso		Gravità dell'EP	Probabilità dell'EP	Livello di rischio neutro
EP1	Errata comunicazione regolatore della circolazione/Agente di Condotta	*Catastrofico*	remoto	Inaccettabile
EP2	Errore dell'Agente di Condotta	*Catastrofico*	*remoto*	Inaccettabile
EP3	Errore del regolatore della circolazione	*Catastrofico*	*remoto*	Inaccettabile
EP4	Bassa aderenza	*Catastrofico*	improbabile	Inaccettabile
EP5	Errore del segnalamento	*Catastrofico*	*improbabile*	Inaccettabile
EP6	Veicolo non correttamente immobilizzato/stazionato	*Catastrofico*	*improbabile*	Inaccettabile
EP7	Frenatura anomala	*Catastrofico*	*improbabile*	Inaccettabile
EP8	Errore del sistema di segnalamento	*Catastrofico*	*improbabile*	Inaccettabile
EP9	Anormalità segnalamento di coda	*Catastrofico*	*improbabile*	Inaccettabile
EP10	Rottura/difetti dei binari	*Catastrofico*	*remoto*	Inaccettabile
EP11	Elementi del carrello dei veicoli daneggiati	*Catastrofico*	*remoto*	Inaccettabile

mitigazione

Livello di rischio
Tollerabile
Tollerabile
Tollerabile
Tollerabile
Tollerabile
Trascurabile
Tollerabile
Tollerabile
Tollerabile
Trascurabile
Tollerabile

PROFONDITÀ DI ANALISI

- Il livello di dettaglio della valutazione del rischio dovrebbe essere proporzionato al rischio prendendo in considerazione quelle situazioni tali che le conoscenze (archivi storici, ecc…) hanno dato luogo a situazione realmente pericolose.
- Sebbene la EN 50126-1 sia applicabile all'intero sistema ferroviario e ai suoi sottosistemi, il livello di **profondità di analisi** necessario per la dimostrazione della sicurezza dipende dal livello di servizio in uso, dalle condizioni al contorno, alle interfacce e da altri fattori simili.

PIANO DELLA SICUREZZA

- Nell'ambito del Regolamento (UE) n. 402/2013 e della norma EN 50126, il concetto di "**PIANO DI SICUREZZA**" è strettamente legato al processo di gestione del rischio e alla sua documentazione.
- Non è un documento autonomo, ma piuttosto un elemento chiave all'interno del più ampio Dossier di Sicurezza (Safety Case).
- Un Piano di Sicurezza (Safety Plan) è un documento operativo che descrive in dettaglio come il processo di gestione della sicurezza verrà gestito e implementato durante l'intero ciclo di vita di un progetto (es. un nuovo veicolo, una modifica a un'infrastruttura).
- Come definito dalla norma EN 50126, il piano di sicurezza è l'elemento che assicura che il processo di valutazione del rischio non sia un'attività "una tantum", ma un'attività continua e gestita.
- Il piano di sicurezza serve a stabilire:
- Chi fa cosa: Chi è responsabile della sicurezza (ruoli e responsabilità).
- Cosa viene fatto: Le attività di valutazione del rischio che verranno eseguite.
- Come viene fatto: I metodi e gli strumenti utilizzati.
- Quando viene fatto: La pianificazione temporale di ogni attività.

ANALISI DI SENSIBILITA' (SENSITIVITY ANALYSIS)

- **<u>Per sostenere la decisione può essere utilizzata un'analisi di sensibilità</u>**
- **Analisi di sensibilità**: metodo per determinare la robustezza di una valutazione. Valutare il **GRADO DI INCERTEZZA** (incertezza intrinseca nel processo di valutazione) ed eventuali fattori che possono amplificarne lo scostamento.
- Attraverso l'analisi di sensibilità è possibile aumentare la confidenza circa Il RISCHIO GLOBALE ASSOCIATO

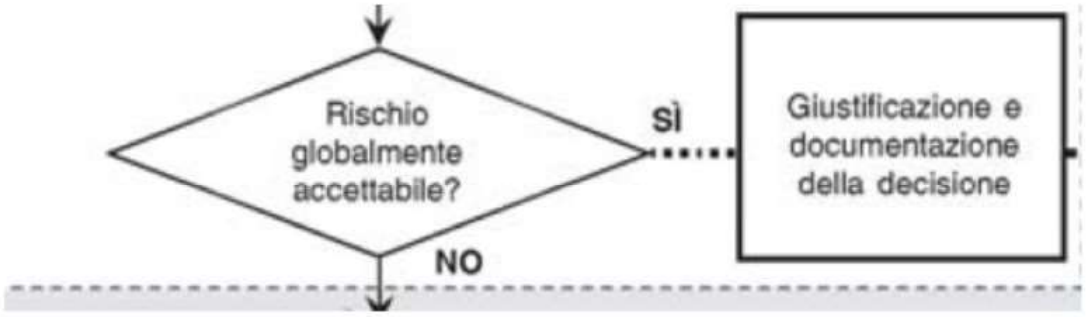
Come?

- Attraverso **MODELLI** che si basano sul principio:
- Valutare l'impatto sulle variabili di uscita a fronte di variazioni su una o più variabili di ingresso.
- Ci sono diverse tecniche:
  - Analisi One a time
  - Stress test
  - Analisi per scenari

MODELLI DI ANALISI

RISCHIO GLOBALMENTE ACCETTABILE?

- In linea di principio il rischio connesso ad un evento pericoloso può considerarsi **globalmente accettabile** se è talmente esiguo da non giustificare la messa in atto di alcuna misura di sicurezza supplementare.
- La consulenza tecnica deve verificare che tutti i rischi ritenuti globalmente accettabili non superino, cumulativamente, una determinata quota del rischio complessivo



SIL (SAFETY INTEGRITY LEVEL)

- Il livello di integrità della sicurezza rappresenta la fiducia di un singolo componente di mantenere accettabile il rischio di sicurezza legato ad un suo malfunzionamento.
- Il SIL si esprime in termini di:
  - PFD (Probability of Failure on Demand): probabilità di guasto legato al mancato intervento nel singolo caso;
  - PFH (Probability of Failure per Hour): probabilità di guasto legato al mancato intervento calcolato in un'ora di funzionamento.

Safety Integrity Level (SIL)	Average Probability of Failuire on Demand (PFD_{AVG})	Average Probability of Failuire per Hour (PFH_{AVG})
SIL 4	$10^{-5} \leq x \leq 10^{-4}$	$10^{-9} \leq x \leq 10^{-8}$
SIL 3	$10^{-4} \leq x \leq 10^{-3}$	$10^{-8} \leq x \leq 10^{-7}$
SIL 2	$10^{-3} \leq x \leq 10^{-2}$	$10^{-7} \leq x \leq 10^{-6}$
SIL 1	$10^{-2} \leq x \leq 10^{-1}$	$10^{-6} \leq x \leq 10^{-5}$

Tabella 2-1: SIL e Probability of Failuire on Demand

SIL (SAFETY INTEGRITY LEVEL)

- Il SIL si definisce per singolo componente e/o per singola funzione di sicurezza, quindi al fine di individuare il SIL per l'intero sistema è necessario valutare tutte le possibili combinazioni.

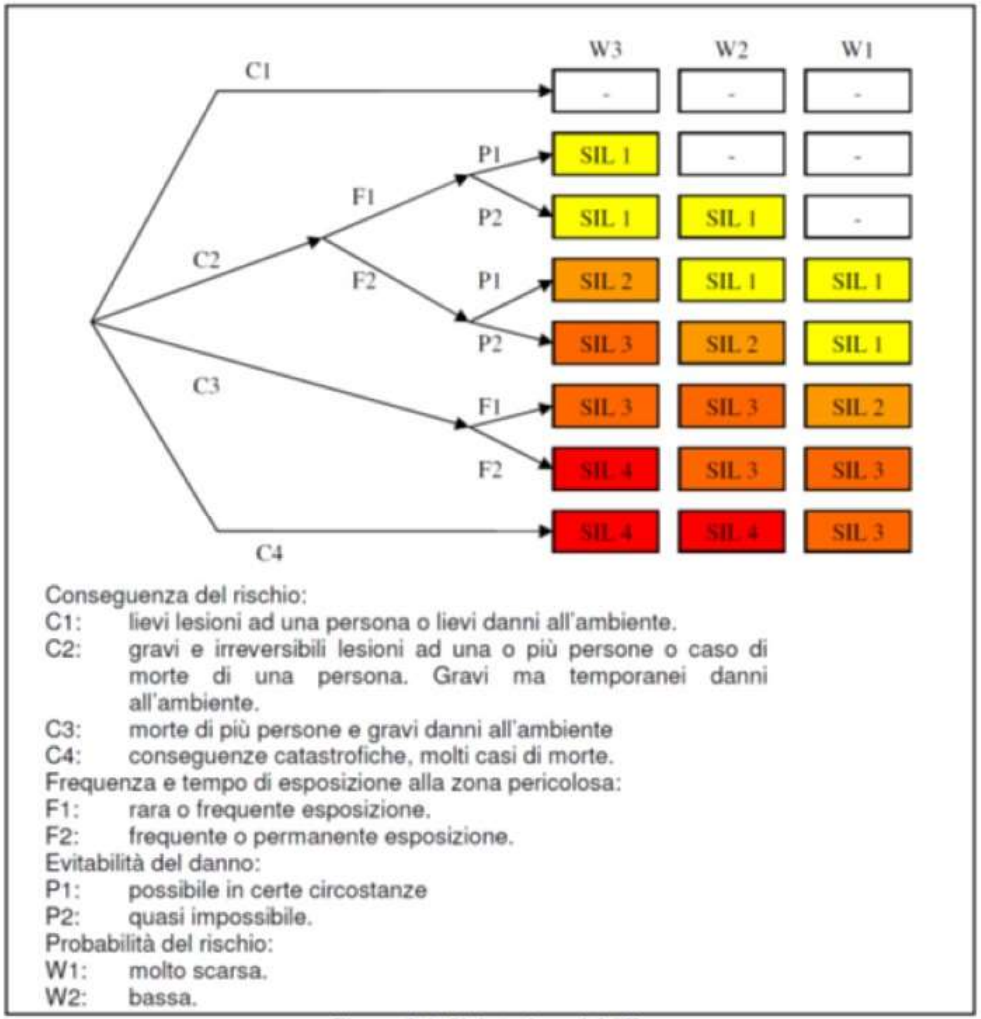
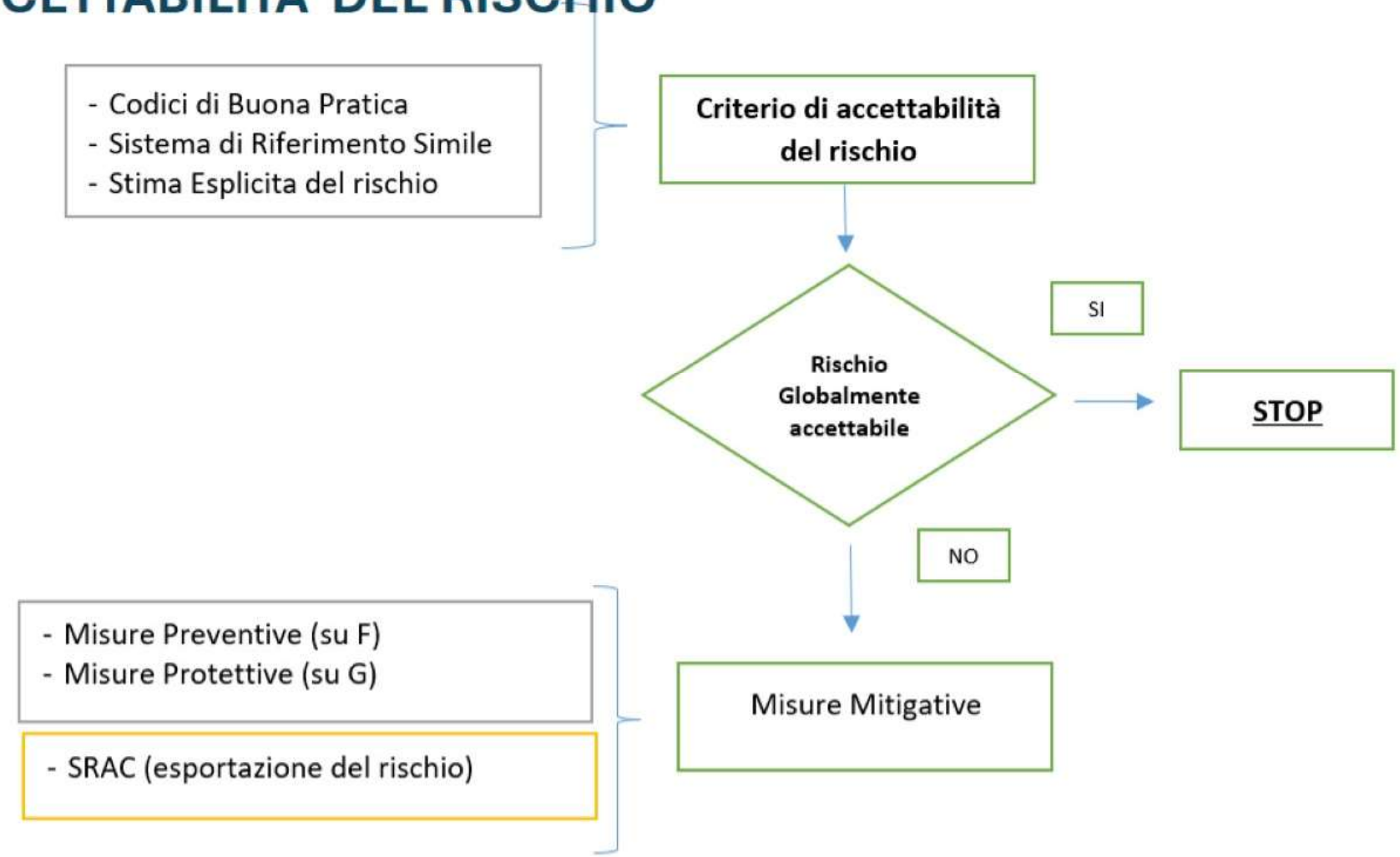


Figura 2-1: Valutazione del SIL

SIL (SAFETY INTEGRITY LEVEL)

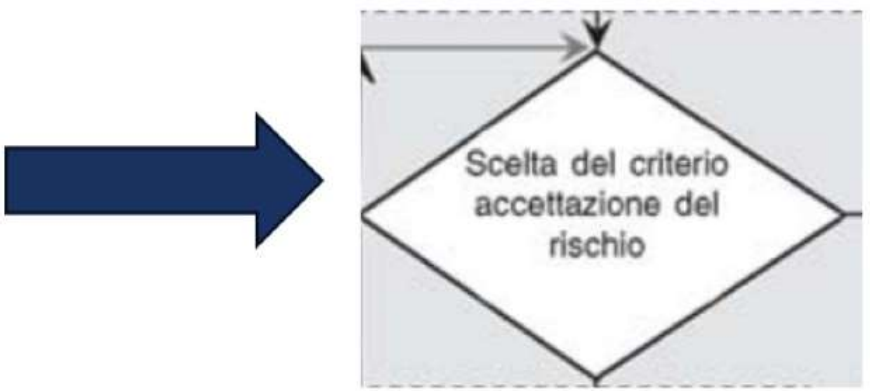
- La norma si rivolge a tutti i sistemi correlati alla sicurezza (trasporti, produzione, ...) e copre tutte le fasi di vita del sistema di sicurezza, dalla fase di progetto a quella di esercizio e manutenzione fino allo smaltimento.
- Lo specifico SIL da raggiungere non è imposta dalla IEC 61508, ma è frutto di un'analisi del rischio del sistema tecnico in oggetto e una valutazione del rischio accettabile, come combinazione della probabilità e del livello di pericolo.
- In ambito ferroviario i criteri di accettabilità del rischio, così come per tutte le funzioni di sicurezza, sono disciplinate dalla EN50126.
- Nel caso specifico di implementazioni SW la norma di riferimento è la EN50128.
- Nel caso di segnalamento ferroviario la norma di riferimento è la EN50129.

CRITERI DI ACCETTABILITA' DEL RISCHIO



CRITERI DI ACCETTABILITA' DEL RISCHIO

- Gli eventi pericolosi che si considerano associati ad un rischio **globalmente accettabile** non devono essere esaminati più a fondo, ma devono comunque essere inseriti nel **registro degli eventi pericolosi.**
- In linea di principio il rischio connesso ad un evento pericoloso può considerarsi globalmente accettabile se è talmente esiguo da non giustificare la messa in atto di alcuna misura di sicurezza supplementare.
- Laddove si individuano più rischi accettabili è necessario valutare che globalmente non superino, cumulativamente, una determinata quota del rischio complessivo.



CRITERI DI ACCETTABILITA' DEL RISCHIO NEL REG. 402/2013

- In linea di principio il rischio connesso ad un evento pericoloso può considerarsi globalmente accettabile se è talmente esiguo da non giustificare la messa in atto di alcuna misura di sicurezza supplementare.
- L'accettabilità dei rischi viene determinata sulla base di uno o più dei seguenti criteri di accettazione:
  - **applicazione di codici di buona pratica;**
  - **uso di un sistema di riferimento simile;**
  - **stima e determinazione accurata dei rischi**
- I criteri di accettazione dei rischi devono permettere di individuare le possibili misure di sicurezza che rendano accettabili i rischi del sistema da valutare.
- Le misure di sicurezza selezionate, fra quelle possibili, al fine di contenere il rischio o i rischi costituiscono i requisiti di sicurezza che il sistema deve soddisfare.

CRITERI DI ACCETTABILITA' DEL RISCHIO NEL REG. 402/2013

- Il metodo scelto per dimostrare la conformità ai requisiti di sicurezza nonché la dimostrazione stessa devono essere valutati in maniera indipendente da un organismo di valutazione (CSM Assessor);
- se, nel corso della dimostrazione della conformità ai requisiti di sicurezza, viene rilevata un'inadeguatezza nelle misure di sicurezza intese ad adempiere i requisiti di sicurezza oppure emerge un nuovo evento pericoloso, il proponente deve procedere ad una nuova valutazione e determinazione dei rischi

CODICI DI BUONA PRATICA

- Il proponente esamina, con la collaborazione di altri operatori interessati, se uno, più o tutti gli eventi pericolosi individuati sono adeguatamente disciplinati da codici di buona pratica pertinenti.
- I codici di buona pratica utilizzabili devono godere di un ampio riconoscimento nel settore ferroviario; in caso contrario, tali codici devono essere corredati delle necessarie motivazioni e devono essere ritenuti accettabili dall'organismo di valutazione.
- **I codici di buona pratica** devono quanto meno:
  - godere di un ampio riconoscimento nel settore ferroviario; in caso contrario, tali codici devono essere corredati delle necessarie motivazioni e devono essere ritenuti accettabili dall'organismo di valutazione;
  - essere pertinenti ai fini del controllo degli eventi pericolosi considerati nel sistema da valutare.
  - un "codice di buona pratica" si riferisce a un insieme di standard, linee guida o regole tecniche riconosciute a livello internazionale.

CODICI DI BUONA PRATICA - ESEMPI

- **EN 14363**: Prove e simulazioni per l'accettazione delle caratteristiche di marcia dei veicoli ferroviari - Prove di comportamento dinamico e statico;
- **EN 12663-1:** Resistenza meccanica della cassa, del telaio, degli organi della sospensione, ...
- **EN 13848:** Qualità geometrica del binario;
- **EN 50152:** Installazioni fisse per la trazione elettrica nel settore ferroviario, tranviario, filoviario e metropolitano.
- **Norma nazionali**
- Le buone pratiche di altri settori (ad esempio energia nucleare, industria militare e aviazione) si possono applicare, previa verifica di accettabilità da parte di un organismo di valutazione, anche ai sistemi ferroviari per determinate applicazioni tecniche, a condizione che l'operatore interessato dimostri che le buone pratiche in questione siano efficaci nel controllo dei relativi eventi pericolosi ferroviari

SISTEMA DI RIFERIMENTO SIMILE

- Un **Sistema di riferimento simile** è un sistema ferroviario esistente, con caratteristiche e operazioni simili a quello che si sta analizzando. Deve quindi almeno:
  - avere già **dimostrato**, nella pratica, di garantire un livello di sicurezza accettabile;
  - presentare funzionalità e punti di interazione analoghi a quelli del sistema da valutare;
  - essere utilizzato in circostanze operative analoghe a quelle del sistema da valutare;
  - essere utilizzato in condizioni ambientali analoghe a quelle del sistema da valutare.

COME SCEGLIERE UN SISTEMA DI RIFERIMENTO SIMILE?

- La scelta del sistema di riferimento simile deve essere fatta con attenzione, considerando diversi fattori:
  - **Tipo di servizio:** Il sistema di riferimento dovrebbe operare un servizio simile (ad esempio, trasporto passeggeri ad alta velocità, trasporto merci, trasporto regionale).
  - **Tecnologia:** Dovrebbe utilizzare tecnologie simili (ad esempio, sistemi di segnalamento, materiale rotabile).
  - **Contesto operativo:** Dovrebbe operare in un contesto simile (ad esempio, densità di traffico, caratteristiche del territorio, condizioni climatiche).
  - **Normative e standard:** Dovrebbe essere soggetto a normative e standard di sicurezza simili.

STIMA E DETERMINAZIONE ACCURATA DEI RISCHI

- Se nessuno dei 2 precedenti criteri sono in grado di individuare un rischio globalmente accettabile allora si procede con la **Stima accurata dei rischi** eseguita con uno dei metodi quantitativi, qualitativi o ibridi.

Per quanto riguarda i criteri di accettabilità del rischio, la EN 50126 individua 3 principi:

- **ALARP:** definisce un limite di accettabilità, uno di inaccettabilità e una zona di ALARP da tenere sotto controllo in cui il rischio è accettabile in quanto definito il più basso possibile.
- **MEM**: Minima Mortalità Endogena. Utilizzata dai tedeschi in cui si prende a riferimento il rischio di mortalità dovuta ad esempio ad un incidente ferroviario con quello stimato di morte "naturale". Si ritiene quindi che il rischio da incidente è tollerato se minore di quello causato da morte "naturale"
- **GAMAB:** che richiede che i nuovi sistemi di sicurezza presentino almeno le prestazioni ottenute con i sistema equivalente esistente.

STIMA E DETERMINAZIONE ACCURATA DEI RISCHI

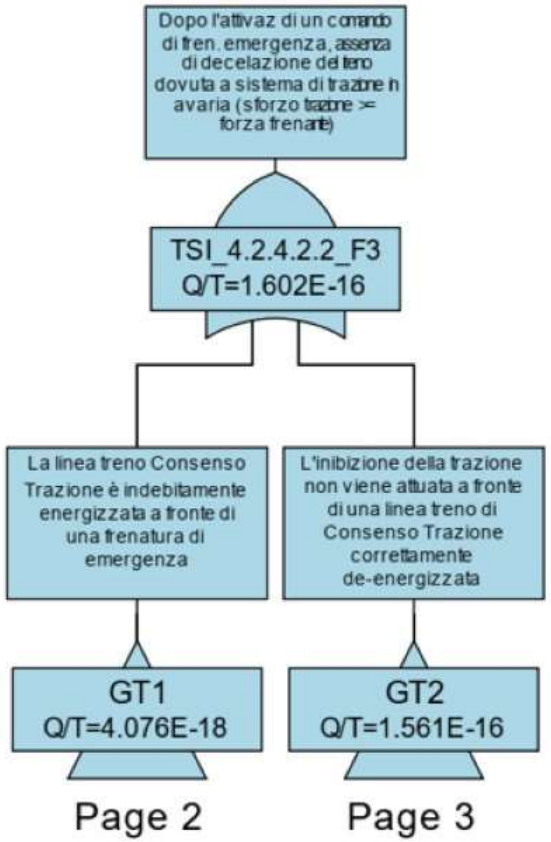
- Se gli eventi pericolosi non sono coperti dall'applicazione dei codici di buona pratica o dalla stima accurata del rischio, oppure la norma ce lo impone (vedi ad esempio il DM Gallerie), l'accettabilità dei rischi deve essere dimostrata mediante una **stima e una determinazione accurate dei rischi stessi.**
- I rischi derivanti dagli eventi pericolosi devono essere stimati sotto il profilo **quantitativo** o **qualitativo** o, se necessario, sia **quantitativo** che **qualitativo**, tenendo conto delle misure di sicurezza in essere.
- La norma **EN 50126** non prescrive metodologie specifiche per la stima dei rischi, ma suggerisce di utilizzare approcci che siano adeguati al contesto specifico del sistema ferroviario in esame.
- I metodi maggiormente utilizzati:
  - **FTA - ETA**

STIMA E DETERMINAZIONE ACCURATA DEI RISCHI

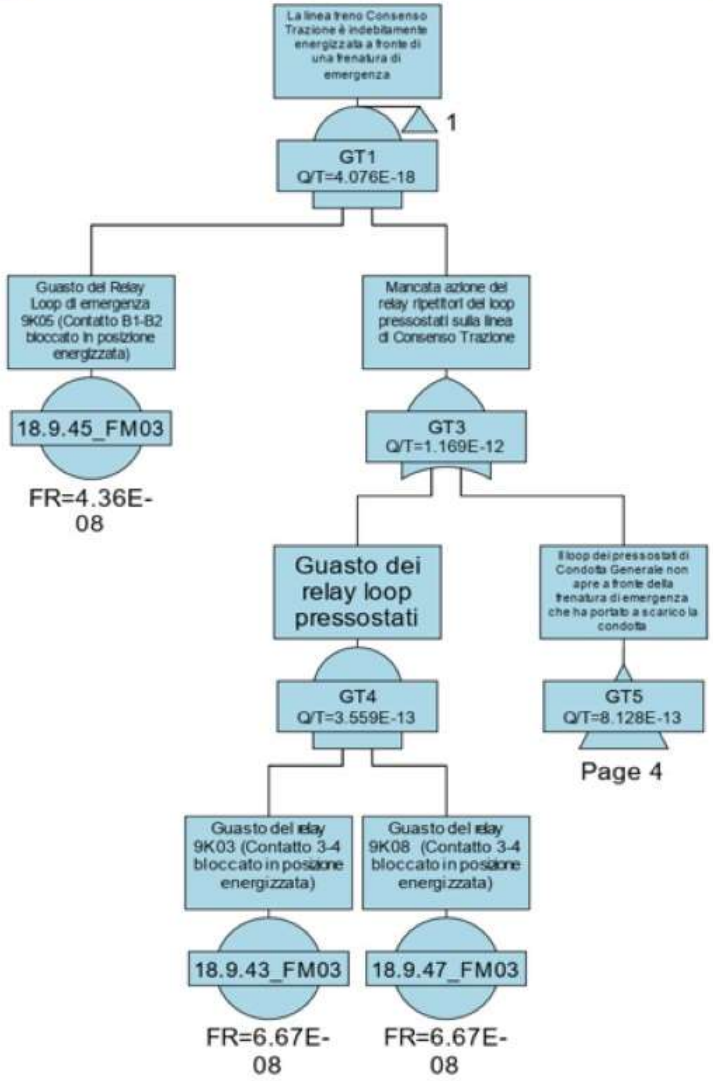
Dopo l'attivazione di un comando di frenatura d'emergenza, assenza di decelerazione del treno dovuta al sistema di trazione in avaria (sforzo di trazione ≥ forza frenante)

Funzione di sicurezza	Livelli di gravità	Requisiti in termini di frequenza di occorrenza	Risultati analisi FTA [guasti/h]	Conforme/non conforme
F2	Catastrofico	Inverosimile	$2{,}798\ 10^{-11}$	CONFORME
F3	Catastrofico	Inverosimile	$1.602\ 10^{-16}$	CONFORME
F6	Catastrofico	Inverosimile	$8{,}47\ 10^{-12}$	CONFORME
F7	Catastrofico	Inverosimile	$1{,}742\ 10^{-9}$	CONFORME
F8	Catastrofico	Inverosimile	$3{,}306\ 10^{-9}$	CONFORME
F9	Catastrofico	Inverosimile	$7.579\ 10^{-12}$	CONFORME
F10	Catastrofico	Inverosimile	$8.464\ 10^{-14}$	CONFORME
F11_1 F11_2	Critico Catastrofico	Remoto Inverosimile	$5{,}139\ 10^{-8}$ $3{,}912\ 10^{-10}$	CONFORME
F12	Catastrofico	Nessuno	NA	CONFORME

FTA- F3


Dopo l'attivaz di un comando di fren. emergenza, assenza di decelazione del treno dovuta a sistema di trazione in avaria (sforzo trazione >= forza frenante)
TSI_4.2.4.2.2_F3
Q/T=1.602E-16
La linea treno Consenso Trazione è indebitamente energizzata a fronte di una frenatura di emergenza
L'inibizione della trazione non viene attuata a fronte di una linea treno di Consenso Trazione correttamente de-energizzata
GT1
Q/T=4.076E-18
GT2
Q/T=1.561E-16
Page 2
Page 3

FTA- F4


La linea treno Consenso Trazione è indebitamente energizzata a fronte di una frenatura di emergenza
1
GT1
Q/T=4.076E-18
Guasto del Relay Loop di emergenza 9K05 (Contatto B1-B2 bloccato in posizione energizzata)
18.9.45_FM03
FR=4.36E-08
Mancata azione dei relay ripetitori del loop pressostati sulla linea di Consenso Trazione
GT3
Q/T=1.169E-12
Guasto dei relay loop pressostati
GT4
Q/T=3.559E-13
Guasto del relay 9K03 (Contatto 3-4 bloccato in posizione energizzata)
18.9.43_FM03
FR=6.67E-08
Guasto del relay 9K08 (Contatto 3-4 bloccato in posizione energizzata)
18.9.47_FM03
FR=6.67E-08
Il loop dei pressostati di Condotta Generale non apre a fronte della frenatura di emergenza che ha portato a scarico la condotta
GT5
Q/T=8.128E-13
Page 4

NEAR MISS

- I **near miss**, o "quasi incidenti", sono eventi che si verificano in un sistema ferroviario (o in qualsiasi altro ambiente) che hanno il **potenziale di causare danni**, ma che fortunatamente **non lo fanno**. Questo può accadere per una serie di motivi, come ad esempio:
  - **Circostanze fortunate**: L'evento si verifica in un momento o in un luogo in cui non ci sono persone o beni esposti al pericolo.
  - **Intervento tempestivo**: Un'azione rapida e efficace (da parte di un operatore, di un sistema di sicurezza, ecc.) impedisce che l'evento si sviluppi in un incidente.
  - **Combinazione di fattori non dannosi**: Si verificano diverse anomalie o eventi inattesi, ma la loro combinazione non porta a conseguenze negative.

ESEMPI DI NEAR MISS NEL SETTORE FERROVIARIO

- Un treno merci transita su uno scambio deviato per errore, ma il macchinista se ne accorge in tempo e riesce a fermare il treno prima che deragli.
- Un operaio sta lavorando sui binari e un treno si avvicina inaspettatamente, ma l'operaio si sposta rapidamente evitando l'impatto.
- Un sistema di segnalamento presenta un'anomalia, ma il controllore del traffico se ne accorge e adotta le misure necessarie per garantire la sicurezza della circolazione.
- Un incendio divampa a bordo di un treno, ma viene spento rapidamente dal personale prima che si propaghi e causi danni significativi.

IMPORTANZA DEI NEAR MISS NELL'IDENTIFICAZIONE DEI PERICOLI

- I near miss sono **indicatori preziosi di potenziali pericoli** presenti nel sistema ferroviario. Anche se non hanno causato danni, essi rappresentano un campanello d'allarme e segnalano la presenza di condizioni o situazioni che potrebbero portare a incidenti in futuro.
- L'analisi dei near miss consente di:
  - **Identificare pericoli nascosti**: Spesso i near miss rivelano pericoli che non erano stati considerati durante la valutazione dei rischi.
  - **Comprendere le cause degli incidenti**: Analizzando i near miss, è possibile individuare le cause profonde che possono portare a incidenti, come ad esempio errori umani, carenze procedurali, o problemi tecnici.
  - **Migliorare le misure di sicurezza**: Le informazioni ottenute dai near miss possono essere utilizzate per migliorare le misure di sicurezza esistenti e prevenire incidenti futuri.

COME GESTIRE I NEAR MISS

- Per sfruttare appieno il valore dei near miss, è necessario implementarli in un sistema di segnalazione e analisi efficace. Tale sistema dovrebbe prevedere:
  - **Segnalazione facile e accessibile**: Il personale deve essere incoraggiato a segnalare i near miss in modo semplice e senza timore di conseguenze negative.
  - **Raccolta e analisi dei dati**: Le informazioni sui near miss devono essere raccolte e analizzate in modo sistematico per identificare trend, pattern e cause comuni.
  - **Definizione di azioni correttive**: Sulla base dell'analisi dei near miss, devono essere definite e implementate azioni correttive per eliminare o ridurre i pericoli identificati.
  - **Diffusione delle informazioni**: Le informazioni sui near miss e le azioni correttive adottate devono essere condivise con tutto il personale per favorire l'apprendimento e il miglioramento continuo della sicurezza.

LA PIRAMIDE DI HEINRICH

- La piramide di Heinrich è un modello sviluppato da Herbert William Heinrich negli anni '30.
- Strumento fondamentale per la gestione della sicurezza nel settore ferroviario. Essa sottolinea l'importanza di concentrarsi sulla prevenzione dei near miss per ridurre il rischio di infortuni più gravi.
- Attraverso un'analisi accurata dei near miss e l'implementazione di misure di sicurezza adeguate, è possibile creare un sistema più sicuro.

LA STRUTTURA DELLA PIRAMIDE

- La piramide è suddivisa in diversi livelli, ognuno dei quali rappresenta una diversa categoria di eventi:
  - **Vertice**: Infortuni mortali o gravi (con conseguenze permanenti o decessi).
  - **Livelli intermedi**: Infortuni minori (con lesioni che richiedono cure mediche ma non causano disabilità permanenti).
  - **Base**: Near miss (eventi che avrebbero potuto causare danni, ma che non lo hanno fatto).
- La piramide di Heinrich si basa sull'idea che gli infortuni gravi sono eventi rari, ma che sono preceduti da un numero molto maggiore di infortuni minori e near miss. Questi ultimi, pur non causando danni diretti, sono indicatori di potenziali pericoli presenti nel sistema e che potrebbero portare a conseguenze ben più gravi se non corretti.



LA PROPORZIONE

- Heinrich, attraverso le sue ricerche, stimò una proporzione di 1 infortunio grave ogni 29 infortuni minori e 300 near miss.
- Questa proporzione, sebbene possa variare a seconda del settore e delle specifiche condizioni di lavoro, evidenzia l'importanza di concentrarsi sulla prevenzione dei near miss per ridurre il rischio di infortuni più gravi.



COME UTILIZZARE LA PIRAMIDE DI HEINRICH

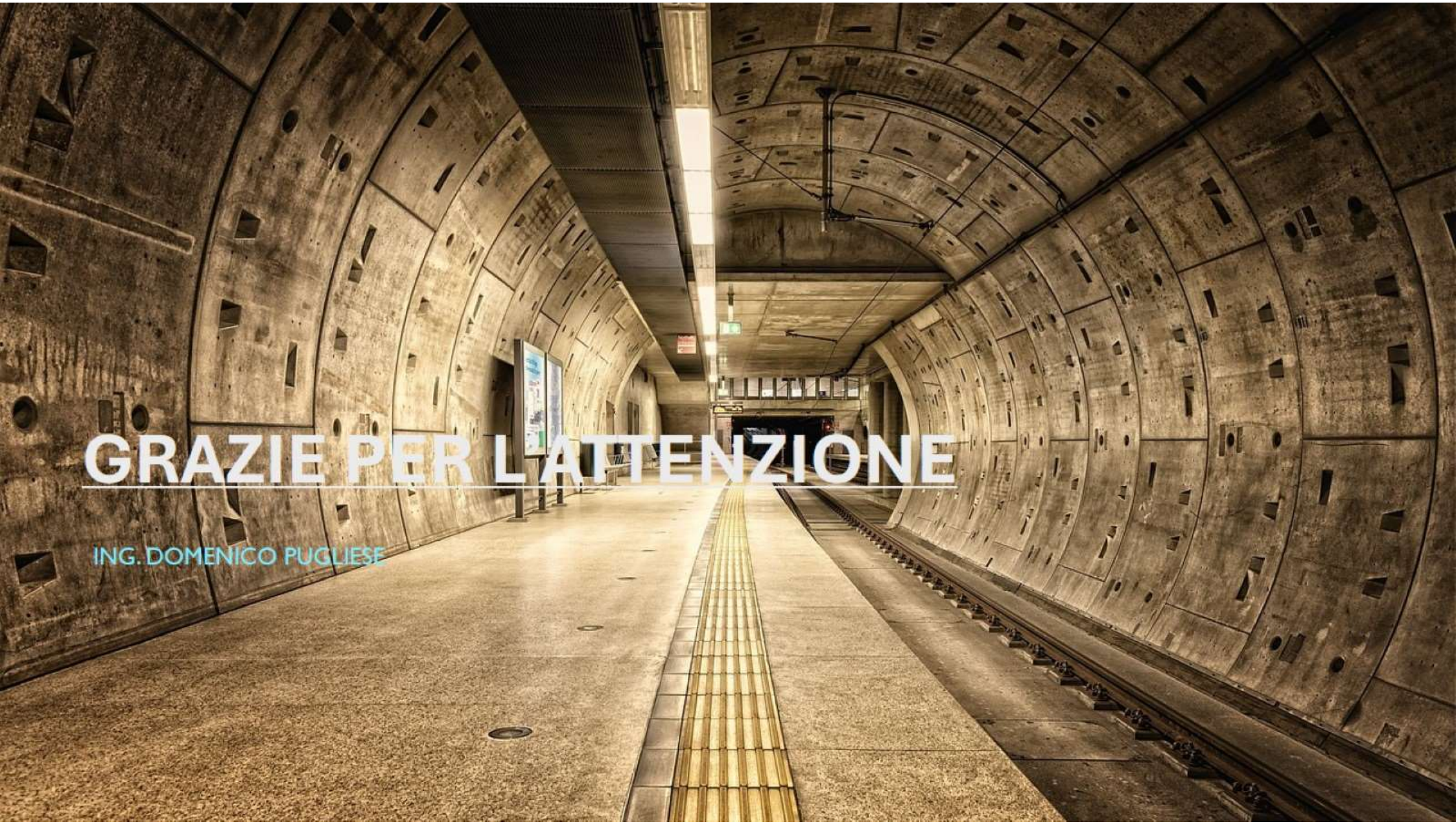
- La piramide di Heinrich è uno strumento prezioso per la gestione della sicurezza nel settore ferroviario.
- Essa può essere utilizzata per:
  - **Identificare i pericoli**: Analizzare i near miss per individuare le situazioni di pericolo che potrebbero portare a infortuni.
  - **Valutare i rischi**: Stimare la probabilità e la gravità dei rischi associati a ciascun pericolo identificato.
  - **Definire le misure di sicurezza**: Implementare misure preventive e protettive per ridurre o eliminare i rischi.
  - **Monitorare l'efficacia delle misure**: Verificare periodicamente l'efficacia delle misure di sicurezza adottate e aggiornarle se necessario.

ESEMPIO PRATICO NEL SETTORE FERROVIARIO

- **Near miss**: Un macchinista frena bruscamente per evitare un pedone che attraversa i binari in un punto non autorizzato.
- **Infortunio minore**: Un lavoratore si sloga una caviglia mentre effettua la manutenzione di un tratto di binario.
- **Infortunio grave**: Un treno deraglia a causa di un guasto ai binari, causando gravi lesioni ai passeggeri.
- Analizzando i near miss, si potrebbe individuare una carenza di segnaletica in prossimità del tratto di binario dove è avvenuto l'evento, oppure una scarsa informazione sui rischi legati all'attraversamento dei binari in punti non autorizzati. Implementando misure correttive (ad esempio, migliorando la segnaletica, aumentando i controlli), si potrebbe ridurre il rischio di incidenti più gravi.

ULTIMO STEP – REDAZIONE DEL DOSSIER DI SICUREZZA

- La dimostrazione documentata che un sistema soddisfa i requisiti RAMS durante l'intero ciclo di vita.
- La EN 50129 sebbene si occupi di segnalamento fornisce gli elementi per la corretta redazione del dossier di sicurezza anche per aspetti diversi.
- In particolare dossier di sicurezza si sviluppano per le seguenti categorie:
- **Prodotto generico:** (inteso come raggruppamento di compenti interconnessi per formare un sistema/sottosistema/apparecchiatura)
- **Applicazione generica:** applicazione che sviluppa funzioni comuni, configurabile per applicazioni specifiche
- **Applicazione specifica:** applicazione sviluppata per una data funzione. Un applicazione specifica può essere frutto di una configurazione di un'applicazione generica oppure sviluppata in modalità stand alone.


GRAZIE PER L'ATTENZIONE
ING. DOMENICO PUGLIESE