UNIVERSITÀ DEGLI STUDI DI FIRENZE

Scuola di Scienza Matematiche, Fisiche, e naturali

HAZARD ANALYSIS DELL' AXLE COUNTER

ANDREA CHIMENTI - FILIPPO FALDETTA

1. Introduzione

Questo documento descrive il lavoro svolto sull' hazard analysis dell' Axle Counter preso in considerazione.
L' Axle Counter è uno strumento (indoor) utilizzato in ambito ferroviario che ha lo scopo di contare gli assi dei treni in una determinata sezione ferroviaria onde evitare sconfinamenti.
Questa analisi serve ad identificare i requisiti di safety, analizzando i rischi associati e le eventuali situazioni pericolose. Dopo aver identificato i vari hazard relativi al sistema, abbiamo determinato delle mitigazioni con lo scopo di ridurre la frequenza di eventi catastrofici.

1.1 Metodologia Utilizzata

Avendo avuto una accurata descrizione ad alto livello del sistema abbiamo deciso di utilizzare per identificare gli hazard, la metodologia **top-down.**
Per comprendere quindi le relazioni che collegano il sistema abbiamo costruito un modello logico funzionale che descrivesse il sistema.
Da questo abbiamo ricavato le varie funzionalità del sistema, che abbiamo elencato in una tabella (file ElencoFunzionalita.xls) da cui è partita l'analisi dei rischi.
Per effettuare la **functional hazard analysis** sono state elencate da prima le funzionalità dei componenti interni al sistemi che avevano influenza sulla safety. Successivamente abbiamo identificato nel dettaglio i rischi, identificato mitigazioni per gli hazards che in fase di pre-mitigazione risultavano non accettabili ed effetuato una valutazoine dell'hazard post-mitigazione.
Operando in questa maniera abbiamo compilato una tabella (file FuctionHazardAnalysis.xls) in cui nello specifico abbiamo compilato i seguenti campi:

- **ID:** identificativo associato a un determinato hazard.
- **Blocco:** componente relativo alla funzionalità analizzata.
- **Funzionalità:** ID associato alla funzionalità analizzazta, riscontrabile nella tabella ElencoFunzionalita.xls.
- **Hazop:** keyword applicata alla funzionalità del sistema.

- **Hazard potenziale:** rischio potenziale per la safety del sistema.
- **Cause:** cause del rischio che descrivolo lo scenario di generazione dell'hazard.
- **Conseguenze:** possibili conseguenze dell'hazard.
- **Frequenza:** frequenza dell'hazard.
- **Severità:** severità dell'hazard.
- **Livello di rischio:** livello di rischio ottenuto dalla risk matrix combinando frequenza e severità
- **Mitigazione:** azione di protezione atta a mitigare quello specifico hazard così da aumentare la safety del sistema.
- **Status:** stato dell'hazard prima di applicare la mitigazione.
- **Frequenza post-mitigazione:** frequenza associata dopo la mitigazione
- **Severità post-mitigazione:** severità associata dopo la mitigazione (rimane indifferente in quando intrinseca allo scenario di pericolo).
- **Livello di rischio post-mitigazione:** livello di rischio ottenuto dalla risk matrix combinando frequenza post-mitigazione e severità post-mitigazione.
- **Status post-mitigazione:** status dell'hazard dopo aver applicato la mitigazione.

Le **Hazop** utilizzate sono:

- **Not:** funzionalità non attivata.
- **Reverse:** semantica della funzionalità opposta rispetto a quella progettata
- **Part of:** funzionalità che ha avuto successo solo in parte
- **Other than:** keyword riferita a casi non presi in considerazione in precedenza.

La **frequenza** è stata attribuita in base a questa tabella:

Frequenza	**Definizione**
Frequente	probabile che si verifichi frequentemente. Il pericolo sarà continuamente sperimentato.
Probabile	Si verificherà più volte. Ci si può aspettare che il rischio si verifichi spesso.
Occasionale	Probabile che si verifichi molte volte nel ciclo di vita del sistema.
Remoto	Probabile che si verifichi a volte nel ciclo di vita del sistema. E ragionevole aspettardi che il pericolo si verifichi.
Improbabile	Improbabile che si verifichi ma possibile. Si può presumere che il rischio possa verificari eccezionalmente
Eccezionale	Estremamente improbabile che si verifichi. Si può presumere che il pericolo possa non verificarsi.

La **severità** è stata attribuita in base a questa tabella:

Categoria	**Severità per le conseguenze alle persone, all'ambiente o al servizio**
Insignificante	Possibili danni minori.
Marginale	Diverse danni minori e/o significante minaccia per l'ambiente
Critico	Singolo fatale e/o grave danno e/o significante danno all'ambiente
Catastrofico	Fatale e/o multipli danni severi e/o maggiori danni all'ambiente

Il **livello di rischio** è stata attribuita in base alla **risk matrix** seguente:

Frequente	Indesiderabile	Intollerabile	Intollerabile	Intollerabile
Probabile	Tollerabile	Indesiderabile	Intollerabile	Intollerabile
Occasionale	Tollerabile	Indesiderabile	Indesiderabile	Intollerabile
Remoto	Trascurabile	Tollerabile	Indesiderabile	Indesiderabile
Improbabile	Trascurabile	Trascurabile	Tollerabile	Tollerabile
Eccezionale	Trascurabile	Trascurabile	Trascurabile	Trascurabile
	Insignificante	**Marginale**	**Critico**	**Catastrofico**

Dove gli elementi della risk matrix hanno il seguente significato:

Livello di rischio	Riduzione e controllo del rischio
Intollerabile	Deve essere eliminata.
Indesiderabile	Sono accettati solo quando la riduzione del rischio non è praticabile e con l'accordo dell'autorità ferroviaria o dell'autorità di regolamentazione della sicurezza, a seconda dei casi.
Tollerabile	Accettabili con adeguati controlli e l' accordo con le autorità di regolamentazione della sicurezza.
Trascurabile	Accettabili senza nessun accertamento.

Lo **status** invece è stato attribuito in base alla seguente tabella:

STATUS	Definizione
Aperto	L'azione per chiudere un hazard non è stata formalmente concordata
Chiuso	L'azione per chiudere un hazard è stata formalmente completata e autorizzata
Risolto	L'azione per chiudere un hazard è stata formalmente concordata, ma non è stata completata o documentata
Cancellato	L'oggeto non è considerato un hazard o è contenuto in un altro hazard identificato
Trasferito	L'oggetto non è considerato un hazard che cade debtro i limite del sistema preso in considerazione

Per quando riguarda la **interface hazard analysis**, abbiamo utilizzato lo stesso procedimento effettuato per la function hazard analysis, in questo caso però non abbiamo effettuato un elenco di funzionalità delle varie interfacce ma, avendo notato che le possibili problematiche erano dovute o dai collegamenti fra le interfacce e il sistema o direttamente dalle componente del sistema, abbiamo lavorato con questa osservazione. Successivamente, abbiamo prodotto una tabella (file InterfaceHazardAnalysis.xls) in cui sono stati analizzati in dettaglio ogni rischio, con gli stessi parametri della tabella associata alla fuctional hazard analysis; fatta eccezione per la voce **Funzionalità** in cui in questo caso non sono stati utilizzati degli ID ma direttamente il titolo utilizzato nel modello logico funzionale e per la sostituzione della Haztop 'reverse' con 'late' (ritardo della funzionalità).

2. Modello logico funzionale

Per analizzare al meglio il dispositivo XYZ abbiamo prodotto un modello logico funzionale per descriverne la struttura ed i flussi di dati.
Specifichiamo di seguito, per una migliore comprensione, le convenzioni utilizzate:

- **rettangoli:** componenti del sistema
- **rettangoli tratteggiati:** interfacce (sistemi esterni)
- **ellissi:** funzionalità
- **frecce:** flussi della trasmissione dei dati

Vogliamo puntualizzare che nel nostro modello logico abbiamo associato i rettangoli tratteggiati a sistemi esterni piuttosto che alle interfacce.
Questo è stato fatto poiché un'effettiva analisi delle interfacce avrebbe richiesto conoscenze ingegneristiche che non abbiamo.
Abbiamo quindi incluso le interfacce nei sistemi esterni ai fini delle analisi per poterle effettuare ad un livello progettuale più alto.

2.1 Componenti e funzionalità

Per semplificare la comprensione del dispositivo elenchiamo le componenti e, tramite i flussi, ne spiegheremo il funzionamento.
Il dispositivo è composto in 7 unità distinte ognuna delle quali provvede ad un certo numero di funzionalità che sono le stesse riportate nel file ElencoFunzionalita.xls:

- Processing Unit
  - elabora dei segnali dei sensori
  - conteggia degli assi
  - decide lo stato della sezione
  - controlla dell'output della sezione
  - comunica con altri dispositivi XYZ

- Input Unit:
  - inoltra i segnali da parte dei sensori
- Output Unit
  - inoltra l’output della processing unit al sistema di interlocking
- Connection Unit
  - gestisce la comunicazione tra dispositivi XYZ
- Power Unit
  - accumula energia per casi di emergenza
  - fornisce energia al dispositivo
- Diagnostic Unit
  - fornisce un log agli utenti
  - acquisisce informazioni circa lo stato del dispositivo
  - genera log
  - salva log
  - aggiorna data e ora con un server
  - salvataggio informazioni circa temperatura del dispositivo ed energia residua
  - percepisce i cambi di stato
- Monitoring Unit
  - permette il monitoraggio remoto
  - acquisisce informazioni dalla diagnostic unit
  - sincronizza data e ora
  - accumula energia per il funzionamento del singolo componente per i casi di emergenza

Queste unità vanno a comporre l’Axle Counter.
Alcune di esse, come verrà descritto al paragrafo successivo, comunicano con alcune interfaccie che possiedono a loro volte delle proprie funzionalità.
Esse sono:

- **Users** (controlla più Axle Counter diversi)
  - legge da display il log di sitema
  - richiede da tastiera il log di sistema
  - avvisi da led che arrivano
  - salvattaggio con USB del log
  - interroga il server sul sistema
- **XYZ1** (un Axle Counter che comunica con il nostro Axle Counter)
  - comunica con altri XYZ
- **Sensori**
  - genera un segnalle al passaggio dell’asse

- **Interlocking** (apparato centrale che gestisce la safety)
  - mantiene la safety

L’interlocking al suo interno possiede un unità specifica che interagisce con l’Axle counter:

- **Power Unit** (dell’Interlocking)
  - fornisce energia alla Power Unit dell’ Axle Counter

2.2 Flussi di dati

I primi dati vengono ricevuti dai sensori tramite la Input Unit e da qui arrivano alla Processing Unit, dove vengono elaborati e sfruttati per contare gli assi.

Conseguentemente, la Processing Unit decide lo stato della sezione che viene inoltrato alla Output Unit, alla Connection Unit ed alla Diagnostic Unit.
La Output Unit inoltra i dati al sistema di Interlocking per coordinare le varie azioni.

La Connection Unit dopo aver ricevuto i dati dalla Processing Unit li utilizza per comunicare con gli altri dispositivi XYZ.
La Diagnostic Unit, ricevuti i dati, li elabora per fornire un log di sistema.
I dati elaborati dalla Diagnostic Unit sono utilizzati dalla Monitoring Unit e dagli Users che ne richiedono le informazioni.

La Monitoring Unit sfrutta i dati per permettere agli utenti il monitoraggio del funzionamento del dispositivo ed inoltre riceve energia dalla Power Unit che a sua volta la riceve dalla Power Unit dell’ Interlocking.

Per capire con più chiarezza il flusso dei dati è sufficente consultare il modello da noi realizzato che si trova nel file ModelloLogicoFunzionaleConFlusso.pdf e controllare le freccie.

3. Report hazard analysis

Per analizzare il dispositivo è stato, innanzitutto, necessario definirne il funzionamento. Ciò è stato fatto analizzando le specifiche fornite dal documento fornito con la descrizione del sistema e derivandone un modello logico funzionale per evidenziarne le componenti, le relative funzionalità ed i flussi di dati.
Questo modello è stato costruto da prima senza considerare i flussi di dati e a portato all'elaborazione del file ModelloLogicoFunzionale.pdf, successivamente abbiamo aggiunto il flusso di dati tramite delle freccie elaborando il file ModelloLogicoFunzionaleConFlusso.pdf.

Abbiamo quindi proceduto a elencare in una tabella le funzionalità del dispositivo in analisi, assegnando ad ognuna un codice identificativo, una tipologia ed una breve descrizione (file ElencoFunzionalita.xls).
La tipologia di tutte le funzionalità che caratterizzano l'analisi è quella elettrica, in quanto non rientra nelle competenze da informatici analizzare proprietà meccaniche del sistema.

In seguito abbiamo effettuato l'Hazard Analysis delle funzionalità (causanti dai possibili hazards) usando le parole chiave assegnate e abbiamo inserito i risultati in una tabella nella quale, per ogni hazard potenziale, indichiamo funzionalità, blocco di appartenenza di quest'ultima, ID dell'hazard e della funzionalità, cause, conseguenze, frequenza pre e post mitigazione, severità pre e post mitigazione, livello di rischio, mitigazione e status pre e post mitigazione; allo stesso modo abbiamo analizzato le interfacce.
Da questo lavoro sono stati fatti i file FunctionHazardAnalysis.xls e InterfaceHazardAnalysis.xls.

La compilazione delle tabelle per quanto riguarda frequenza e severità, non avendo a disposizione dati effettivi con cui valutarle, è stata fatta sulla base di nostre ipotesi.
Più nello specifico dopo aver analizzato il campo ‘cause’ e le varie tabelle con la descrizione dei vari campi per frequenza e severità abbiamo deciso di dare quei valori a quegli specifici campi.
Per quanto riguarda la frequenza, i campi sono stati assegnati dal fatto che eventi come il mancato conteggio di un asse, essendo un azione ripetuta più volte nel tempo può essere considerata con una frequenza abbastanza elevata poiché aumenta la probabilità di un errore, mentre la mancata conoscenza dei settori adiacenti, essendo un informazione che cambia meno spesso nel tempo avrà una frequenza minore.
Per quanto riguarda la severità ci siamo basati sulle conseguenze che determinati hazard possono portare, più la conseguenza è rilevante per la safety più il livello di severità sarà alto.