

10S.1) System Safety:

SEMINARIO: TECNICHE ED ESEMPI DI SYSTEM SAFETY:


Agenda:

- Introduzione;
- HAZOP;
- FMEA;
- EVENT TREE ANALYSIS;
- FATTORE UMANO;
 - o Swiss chesse;
 - o Human Behaviour Theory.

1/5. Introduzione:

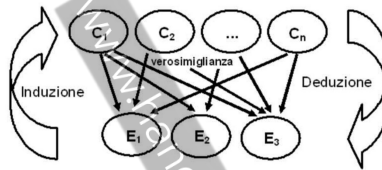
- > **OBJ:** identificazione dei meccanismi attraverso i quali possono accadere incidenti.
 - Modo in cui il sistema opera;
 - Limitazione componenti.

Storia S.S.:

- > Nasce:
 - IDEA: anni '40, con la missilistica in senso moderno (lancio primi vettori e sbarco luna);
 - DISCIPLINA: anni '50-'60 con  stima /quantificazione rischio associato a incidenti industriali/ aeronautici/ aerospaziali.
- > **OBJ:** prevedere/ mitigare eventi catastrofici o assicurare l'affidabilità dello stesso sistema.

Valutazione del rischio:

- > **DEF:** Classificazione riferita alla sequenza nell'analisi di processo:
- > Categorie tecniche:
 - **DEDUTTIVE:** Cause (eventi primari) => Conseguenze (**fmea, event tree**);
 - **INDUTTIVE:** conseguenze => Cause (**Fault tree**);
 - **MISTE:** Cause <=> conseguenze (**fmeca**)



2/5. Hazard and Operability Analysis (HAZOP):

Introduzione all'HAZOP:

- > **DEF:** Analisi di pericolo e operabilità.
- > **OBJ:** individuazione delle modalità di guasto di un componente, sottosistema o sistema.
 - **NECESSITÀ:** comprendere le cause di incidenti/pericoli per i quali non era nota la genesi e che risultavano anomali.
 - Eseguita da un gruppo di esperti;
 - Nasce anni '60 in Inghilterra > Manchester.
 - **STANDARD:** standard IEC 61882 : 2001 – "Hazard and Operability studies (HAZOP studies) – Application guide"
- > Per ogni tipologia di guasto si devono individuare le cause e le possibili conseguenze, in termini di variazione rispetto alle deviazioni dalle condizioni di progetto

Applicazioni principali:

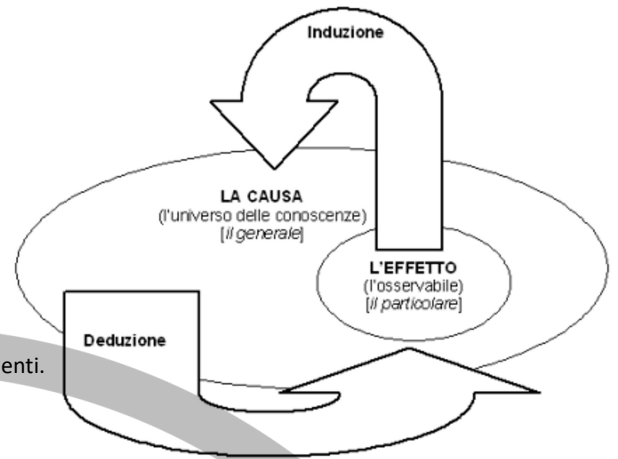
-> I campi in cui viene applicata l'analisi HAZOP sono: Nucleare, Settore Oil & Gas, Impianti di processo e industriali di grandi dimensioni ad alto rischio (es. Seveso), Settore Farmaceutico, Settore agroalimentare e agrochimico, Impianti per la produzione di energia (sia tradizionali che ad energie alternative: eolico, idroelettrico, biomasse, ecc.), Settore navale, Settore aeronautico e aerospaziale.

Procedura:

- > Prima di procedere all'analisi vera e propria, è necessario seguire una procedura preliminare:
 1. esame attento e minuzioso del progetto, in modo da fornire una descrizione delle variabili il più completa possibile
 2. Indagine, sistematica, su ogni parte per identificare se, in che modo e in base a quale principio le deviazioni dalle specifiche di progetto agiscono sul sistema
 3. Informazioni sullo stato attuale di funzionamento e sulle possibili configurazioni critiche.
 4. Scomposizione dell'impianto in una serie di sottosistemi a cui verrà poi applicata singolarmente la procedura.

Documentazione:

- > E' necessario reperire la seguente documentazione prima di procedere:
 - Progetti e schemi tecnici
 - Planimetrie del sito/impianto e schemi funzionali
 - Diagramma di flusso del processo
 - Procedure operative e di manutenzione
 - Limiti operativi e dettagli tecnici (es. portate, pressioni massime)
 - Documentazione relativa a passati incidenti, infortuni, near miss
 - Schemi HAZOP di impianti simili



10S.2) System Safety:

Pregi e difetti:

✓ Vantaggi:

- Identificare le "falle" e/o i punti deboli del sistema;
- Permette una analisi completa dati tutti gli stati dei nodi, con scarsa interpretabilità da parte degli analisti;
- Permette di superare "pregiudizi" e/o schemi preesistenti;
- È efficace in ogni fase di funzionamento (manutenzione o emergenza);
- Mezzo di addestramento (es. addetti alla conduzione dell'impianto);
- Permette di ottenere miglioramenti progettuali a costo ridotto;
- Metodologia è semplice e facilmente replicabile.

✗ Svantaggi:

- Non "vede" le interrelazioni fra componenti;
- Considera solo semplici tipologie di guasto/funzionamento;
- Non prende in considerazione componenti complessi con l'essere umano;
- Prende in considerazione solo ciò che "appare" esplicitamente da disegni, progetti, schemi funzionali;
- Non permette di calcolare Probabilità e Magnitudo dei danni.

3/5. Failure model and Effects Analysis - Fmea:

Introduzione:

-> **DEF:** analisi che indaga i modi in cui le componenti di un sistema possono guastarsi e gli effetti prodotti sull'intero sistema.

-> **OBJ:** prevedere e classificare i possibili guasti in base all'impianto, sul successo della missione e sulla sicurezza del personale e degli equipaggiamenti nel settore aeronautico.

- Applicazione: settori industriali e non (missioni Apollo), applicazioni di gestione della qualità.
- **RISULTATI**> qualitativi,

-> **FMECA:** Failure Model Effects and Critical Analysis: aggiunge una valutazione quantitativa delle probabilità di accadimento degli eventi e della gravità (magnitudo) delle conseguenze.

- I risultati sono solitamente presentati in forma di schema cartaceo, in cui vengono rappresentati tutti i singoli elementi componenti il sistema.
- Possibile ottenere una graduatoria di priorità basata su gravità dei danni tramite l'**Indice di Priorità di Rischio (IPR)**.

Procedura:

- **Identificazione** di tutti i **possibili malfunzionamenti** dei componenti del sistema;
- **Descrizione effetti e cause** possibili (\-/ malfunzionamento);
- Definizione delle **probabilità** (P), delle **severità** (G) del danno e della **rilevabilità** della cause (R), dei range dei tre parametri P, G, R ed i relativi **criteri di assegnazione**;
- **Calcolo dell'Indice di Priorità di Rischio** ($IPR = P \cdot G \cdot R$) per ogni modo di malfunzionamento;
- Definizione degli **interventi** da intraprendere in modo da portare l'IPR sotto un valore di soglia prefissato.

Note applicative:

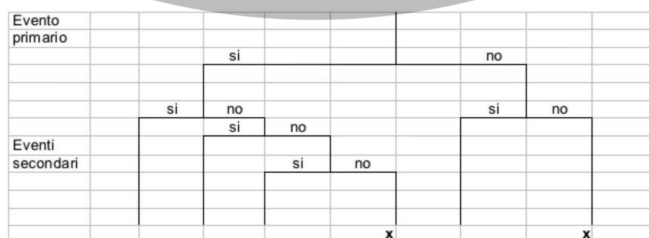
- Utilizzata ad ampio spettro nella Risk Analysis/Risk Management;
- FMEA utilizzata con successo nell'analisi dei rischi in ambito Direttivo Mancchine;
- Utile nella fase di **progettazione di nuovi impianti**, prodotti. Componenti oppure nel prevedere nuovi impieghi.
- ✓ Permette di **INSERIRE** gli aspetti intangibili ed "**FATTORE UMANO**" nell'analisi.

4/5. Event Tree Analysis:

Introduzione:

-> **DEF:** Event Tree: l'albero degli eventi si utilizza quando lo scopo dell'analisi è lo studio delle sequenze incidentali che coinvolgono l'impianto/l'ambiente interno ed esterno.

-> È complementare all'albero dei guasti (presenta il diagramma cause-conseguenze).



Processo:

- Partenza: da un particolare evento iniziale e procede bottom-up;
- Costituito definendo prima un evento primario e poi gli eventi-conseguenti + processi che fluiscono da questo;
- Ogni evento ha un cammino per il successo e uno per l'insuccesso => 2^n .
- Evento iniziale espresso in termini di frequenza, mentre i secondari in termini di probabilità;

10S.3) System Safety:

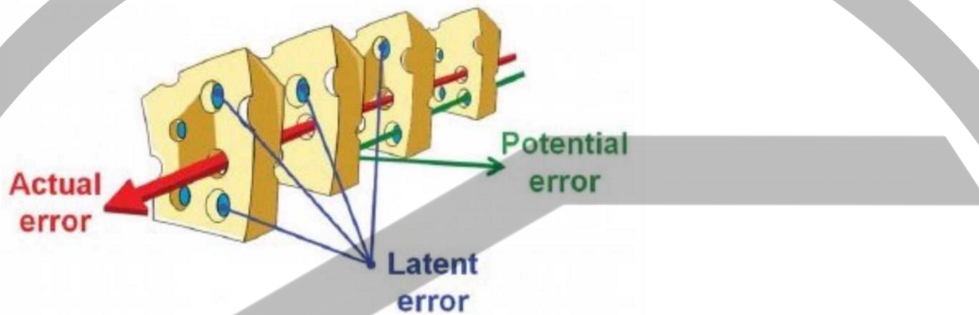
- Si costruisce indicando tutte le funzioni e i sistemi di sicurezza sull'impianto per impedire/ mitigare le conseguenze ad una causa iniziale;

Caratteristiche:

- Partenza da un particolare evento iniziale e procede bottom-up;
- Costituito definendo prima un evento primario e poi gli eventi-conseguenti + processi che fluiscono da questo;
- Elementi principali: definizione degli eventi e vertici logici;
- È vicino alla tecnica qualitative della fmea e fmeca;
- Permette una quantificazione delle frequenze degli eventi;
- Ogni evento ha un cammino per il successo e uno per l'insuccesso => 2^n .
- Evento iniziale espresso in termini di frequenza, mentre i secondari in termini di probabilità;
- Mostra gli effetti di un guasto;
- Indica se il sistema considerato contribuisce in riferimento alla totalità dei pericoli;

5/5.Fattore Umano:

Teoria del formaggio svizzero (James Reason):



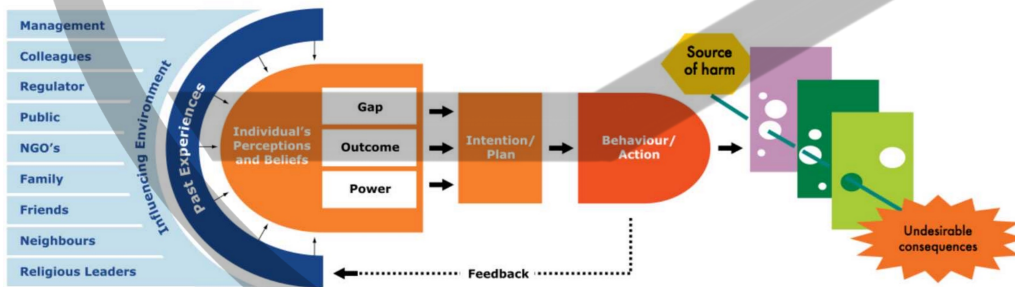
-> In tutte le attività che si susseguono per raggiungere un determinato outcome ogni procedura può essere esposta ad un rischio di non essere completata adeguatamente.

Le "fette" rappresentano le difese del sistema. I "buchi" sono invece i difetti del sistema, l'assenza di meccanismi di controllo che possono determinare, insieme ad altre carenze, ad un evento avverso.

L'allineamento dei buchi, come nella figura porta al decesso del paziente:

- Mancata anamnesi su allergia ad un farmaco
- Il medico prescrive il farmaco
- Il farmacista non verifica se sia stata accertata l'idiosincrasia al preparato
- L'infermiera somministra il farmaco
- Il paziente muore

Ad ogni livello, se una delle difese è messa in atto, l'evento avverso non avviene. Se invece, le fette consentono un allineamento dei "buchi" si può verificare un evento avverso.



-> La teoria di Reason esplicita azioni o comportamenti errati come conseguenze di precondizioni (ambientali, circostanziali o psicologiche), a loro volta influenzate da cause indirette, nascoste o non direttamente legate agli eventi di guasto.

—> Per J. Se è presente un comportamento sbagliato e questo è una barriera stessa all'evento.

