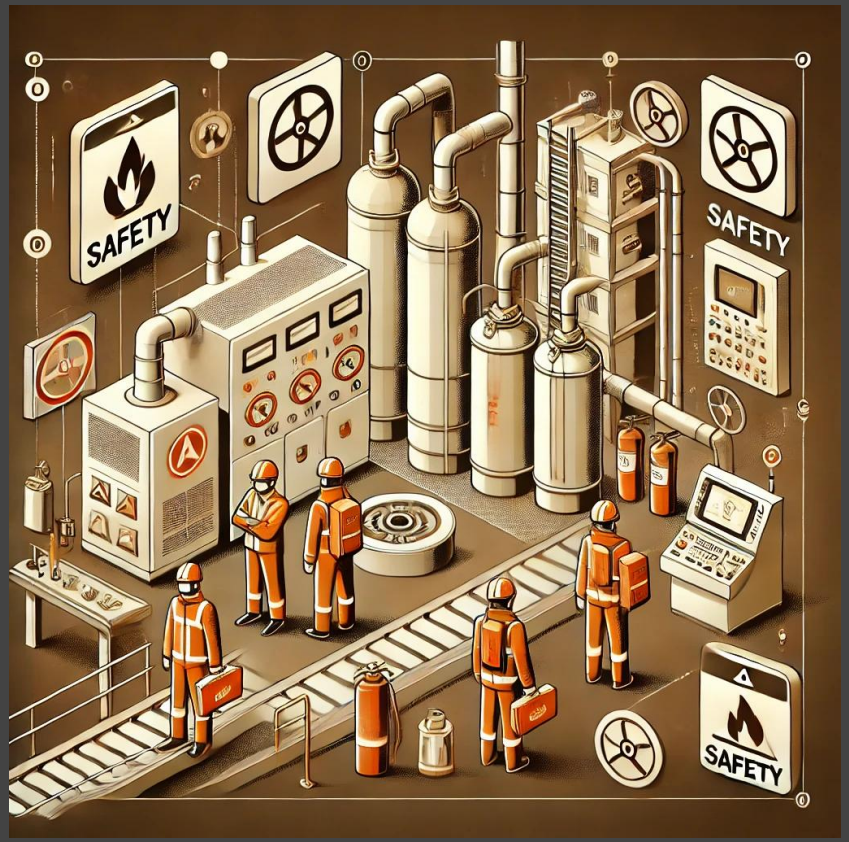
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

SICUREZZA INDUSTRIALE

LA VALUTAZIONE DEL RISCHIO

Vol. III



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

GLI STRUMENTI DI RISK ASSESSMENT

Principali metodologie per l'identificazione e la valutazione dei rischi

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

CHECK LIST

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

CHECK LIST

CARATTERISTICHE

Consiste in una lista di voci di controllo basate sulle esperienze precedenti e da utilizzare in caso di determinate analisi per evitare situazioni già verificatesi, per attivare i procedimenti necessari o confrontare la rispondenza di apparecchiature, materiali, procedure e sistemi di sicurezza con standard di buona tecnica ingegneristica e normative vigenti. Con questo metodo è assicurato il livello minimo richiesto nella valutazione dei rischi per qualsiasi tipo di lavoro e può essere applicato ad ogni livello di sviluppo dell'impianto o della fase di progettazione dello stesso.

VANTAGGI

Si tratta di uno dei metodi più semplici e meno costosi per la valutazione dei rischi; molto utile per rilevare gli errori di progettazione più comuni e di grande aiuto per tecnici con poca esperienza in questo campo.

SVANTAGGI

Ha il limite di essere fortemente dipendente dall'esperienza acquisita dal suo o dai suoi autori per cui non è in grado di identificare rischi non esplicitamente già previsti.

APPLICAZIONE

Semplice e frequente, può evidenziare una situazione che richiede una valutazione più dettagliata.

COMMENTI

Di checklists ne esistono più tipi, ognuna utilizzabile per scopi specifici e dovrebbero essere regolarmente verificate e aggiornate. Molte organizzazioni utilizzano questa metodologia dalla fase di progettazione dell'impianto alla chiusura dello stesso.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

L'analisi del rischio con il metodo delle check-list è una tecnica strutturata e sistematica utilizzata per identificare e valutare i rischi associati a processi, attività o impianti. Questo approccio prevede l'uso di liste predefinite di domande o punti di controllo per garantire che tutti gli aspetti critici siano valutati in modo completo e consistente. Vediamo più in dettaglio come funziona.

1. Definizione del Metodo delle Check-list

Il metodo delle check-list consiste nel creare elenchi di punti di controllo basati su standard, normative, esperienze precedenti e buone pratiche. Queste liste vengono utilizzate durante l'analisi per valutare se i requisiti di sicurezza e di gestione del rischio sono stati rispettati e se sono presenti pericoli potenziali. L'obiettivo principale è assicurare che tutti i rischi siano identificati, anche quelli che potrebbero essere trascurati durante una valutazione meno strutturata.

2. Struttura della Check-list

Una check-list ben progettata deve includere:

- **Domande specifiche** su aspetti tecnici, gestionali e organizzativi;
- **Punti critici di verifica** per valutare le condizioni di sicurezza;
- **Indicatori di rischio** associati a specifici contesti;
- **Sezioni categorizzate** (es. ambiente, sicurezza operativa, gestione del personale) per facilitare l'identificazione dei pericoli in ciascuna area.

3. Fasi di Implementazione

- **Preparazione della check-list**:
  - Sviluppare la lista in base al contesto operativo e alle normative applicabili.
  - Raccogliere input da esperti del settore, personale coinvolto e documenti tecnici.
- **Raccolta di informazioni**:
  - Effettuare sopralluoghi, analizzare documentazione, condurre interviste con il personale e raccogliere i dati necessari per completare la check-list.
- **Valutazione e identificazione dei rischi**:
  - Rispondere a ogni punto della lista e segnalare eventuali condizioni di rischio.
  - Classificare i rischi in base alla probabilità e alla gravità.
- **Sviluppo di azioni correttive**:
  - Identificare misure per eliminare, ridurre o controllare i rischi.
  - Stabilire priorità e piani di attuazione.
- **Revisione e aggiornamento**:
  - Rivedere periodicamente la check-list per aggiornamenti e modifiche normative o per tenere conto di cambiamenti operativi.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

4. Vantaggi del Metodo delle Check-list

Standardizzazione: Fornisce un approccio standardizzato, riducendo la soggettività e assicurando una copertura completa di tutte le aree critiche.
Facilità d'uso: È uno strumento semplice che può essere utilizzato da personale con diversi livelli di competenza.
Tracciabilità: Consente di documentare e tracciare facilmente i punti di controllo e le verifiche effettuate.
Facilità di aggiornamento: La check-list può essere modificata e ampliata con nuove domande in base ai cambiamenti operativi o normativi.

5. Limitazioni del Metodo delle Check-list

Rigidità: Una check-list predefinita può non considerare rischi nuovi o specifici del contesto.
Focalizzazione limitata: L'analisi è spesso limitata agli aspetti inclusi nella lista, trascurando potenziali rischi non codificati.
Dipendenza dall'esperienza: L'efficacia della check-list dipende molto dall'esperienza di chi la progetta e la utilizza.

6. Applicazioni Pratiche

Le check-list sono utilizzate in vari settori, tra cui:
Sicurezza sul lavoro: Per identificare rischi legati a macchinari, dispositivi di protezione individuale e procedure operative.
Sicurezza industriale: Per verificare il rispetto delle normative tecniche e di sicurezza degli impianti.
Progettazione ingegneristica: Per valutare la conformità dei progetti a standard di sicurezza.
Gestione di emergenze: Per controllare la prontezza e la risposta del personale in caso di situazioni critiche.

7. Esempio di Check-list per la Sicurezza sul Lavoro

Di seguito un esempio di domande per una check-list di sicurezza in un ambiente industriale:
Le uscite di emergenza sono chiaramente segnalate e libere da ostacoli?
Il personale è adeguatamente formato sui rischi connessi all'uso di macchinari?
Sono presenti misure per prevenire l'esposizione a sostanze pericolose?
Le attrezzature di sicurezza (es. estintori, allarmi) sono in buone condizioni e facilmente accessibili?
Sono stati condotti audit di sicurezza regolari nell'ultimo anno?

Conclusione

Il metodo delle check-list è uno strumento pratico e versatile che, sebbene presenti alcune limitazioni, rappresenta una soluzione efficace per garantire una valutazione del rischio accurata e sistematica. Per un uso ottimale, è fondamentale adattare la check-list alle specificità del contesto e integrarla con altre tecniche di analisi del rischio, come l'analisi HAZOP o l'analisi FMEA.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

CHECK LIST

SINTESI

E' una lista di voci di controllo basata su esperienze precedenti

E' da utilizzare per situazioni già verificatesi

Serve per confrontare la rispondenza di sistemi e procedure con standard di buona tecnica e normative vigenti

VANTAGGI

Metodo semplice e poco costoso

Non richiede elevata esperienza nella valutazione

SVANTAGGI

Non identifica rischi che non siano esplicitamente previsti

Dipende dall'esperienza di chi l'ha predisposto

LE TIPOLOGIE

- Liste di controllo
- Generali vs. Specifiche
- Campi di applicazione:
  - fasi di progetto, pre - commissioning e controlli periodici
  - situazioni di pericolo comune

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempi di check-list per la sicurezza e la conformità in un ambiente metalmeccanico:

N.	Punti di Controllo	Stato (OK / Non OK)	Rating di Rischio	Azioni Correttive	Responsabile	Scadenza
1	I macchinari sono dotati di protezioni adeguate?	Non OK	Alto (Probabilità: 4/5; Gravità: 5/5)	Installare nuove protezioni	Mario Rossi	1 settimana
2	Gli operatori indossano dispositivi di protezione individuale (DPI)?	OK	Basso (Probabilità: 1/5; Gravità: 2/5)	N/A	N/A	N/A
3	Le vie di fuga sono libere e chiaramente segnalate?	Non OK	Medio (Probabilità: 3/5; Gravità: 4/5)	Rimuovere ostacoli e migliorare la segnaletica	Anna Verdi	3 giorni
...	...	...	...	...	...	...

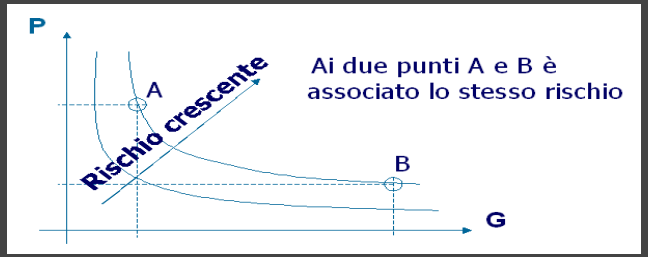
N.	Punti di Controllo	Stato (OK / Non OK)	Azioni Correttive	Responsabile	Scadenza
1	I macchinari sono dotati di protezioni adeguate?				
2	Gli operatori indossano dispositivi di protezione individuale (DPI)?				
3	Le vie di fuga sono libere e chiaramente segnalate?				
4	Gli impianti di aspirazione e ventilazione funzionano correttamente?				
5	Gli strumenti manuali e le attrezzature sono in buone condizioni e periodicamente ispezionati?				
6	I materiali infiammabili sono conservati in maniera sicura e lontano da fonti di calore?				
7	I lavoratori sono stati formati sui rischi specifici dell'ambiente metalmeccanico?				
8	Le gru, i paranchi e altri mezzi di sollevamento sono utilizzati correttamente e in buono stato?				
9	Le segnalazioni di sicurezza sono ben visibili e rispettate?				
10	Sono presenti e funzionanti sistemi di estinzione incendi nelle aree critiche?				

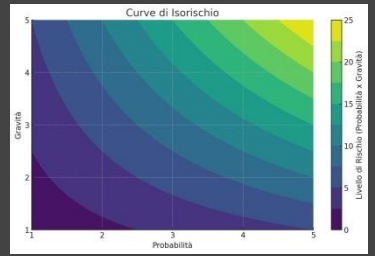
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

CHECK LIST

IL RATING DEL RISCHIO $R = G \times P$





Le curve a pari Livello di Rischio sono quindi delle iperboli equilatere
Nulla vieterebbe, in linea di principio, di utilizzare altre funzioni

Probabilità

Livello 4 = altamente probabile
-esiste una correlazione diretta tra la mancanza rilevata ed il verificarsi del danno ipotizzato per i lavoratori
-si sono già verificati danni per la stessa mancanza rilevata in situazioni simili
-il verificarsi del danno alla mancanza rilevata non susciterebbe alcun stupore (in altre parole l'evento sarebbe largamente atteso)

-Livello 3 = probabile
-la mancanza rilevata può provocare un danno anche se non in modo automatico o diretto già noto, all'interno dell'unità produttiva, qualche episodio in cui la mancanza rilevata ha fatto seguito a un danno
-il verificarsi del danno ipotizzato, susciterebbe una moderata sorpresa

-Livello 2 = poco probabile
-la mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi sono noti solo rarissimi episodi già verificatisi
-il verificarsi del danno ipotizzato, susciterebbe grande sorpresa

-Livello 1 = improbabile
-la mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili e indipendenti
-non sono noti episodi già verificatisi
-il verificarsi del danno ipotizzato susciterebbe incredulità

Magnitudo

Livello 4 = gravissimo
- infortunio o episodio di esposizione acuta con effetti letali o di
- invalidità totale
- esposizione cronica con effetti letali e/o totalmente invalidanti

Livello 3 = grave
- infortunio o episodio di esposizione acuta con effetti di
- invalidità parziale
- esposizione cronica con effetti irreversibili e/o parzialmente invalidanti

Livello 2 = medio
-infortunio o episodio di esposizione acuta con effetti di inabilità reversibile
- esposizione cronica con effetti reversibili

Livello 1 = lieve
- infortunio o episodio di esposizione acuta con effetti di inabilità rapidamente reversibile
- esposizione cronica con effetti rapidamente reversibili

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

CHECK LIST

4	8	12	16
3	6	9	12
2	4	6	8
1	2	3	4

Rating del Rischio

R > 8	Azioni correttive indilazionabili
4 < R < 8	Azioni correttive da programmare con urgenza
2 < R <3	Azioni correttive da programmare a breve medio termine
R = 1	Azioni correttive da programmare con minore urgenza

Assenza di rischio
trascurabilità del rischio

↓

Non c'è motivo di intervenire
Mantenimento a livello di attenzione

Esposizioni entro i limiti
previsti dalla norma\

↓

Previsione di controlli periodici

Previsione di esposizione nei
limiti ma comunque allarmante

↓

Adozione di misure di
prevenzione e protezione

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

La sicurezza reale e quella percepita sono due concetti fondamentali nella gestione del rischio e nella valutazione della sicurezza, in particolare nel contesto lavorativo e sociale. Questi due tipi di sicurezza spesso divergono e possono influenzare il comportamento e le decisioni degli individui in modo significativo.

1. Sicurezza Reale

La **sicurezza reale** rappresenta l'effettivo livello di sicurezza, determinato oggettivamente sulla base di dati, misurazioni, e analisi del rischio. Essa è basata su evidenze fattuali, come la frequenza degli incidenti, i dati storici e l'efficacia delle misure di protezione adottate.

- **Misurazione oggettiva**: Deriva dall'uso di statistiche e modelli matematici.
- **Evidenze**: Incidenti passati, dati raccolti tramite audit, analisi delle performance di sistemi di sicurezza.

Esempio: L'installazione di barriere protettive e l'uso di dispositivi di protezione individuale (DPI) riducono statisticamente la possibilità di infortuni in un ambiente industriale.

2. Sicurezza Percepita

La **sicurezza percepita**, invece, è il livello di sicurezza che una persona crede di avere. Questo concetto è più soggettivo e può essere influenzato da vari fattori psicologici, sociali e ambientali.

- **Fattori emotivi**: La paura o la confidenza possono alterare la percezione del rischio.
- **Comunicazione**: L'informazione (o disinformazione) ricevuta influisce notevolmente sulla percezione del rischio.

Esempio: In una fabbrica, anche se tutte le misure di sicurezza sono correttamente adottate, un dipendente potrebbe sentirsi ancora in pericolo se non comprende il funzionamento dei sistemi di protezione.

3. Differenze e Divergenze tra Sicurezza Reale e Percepita

Le differenze tra sicurezza reale e percepita possono portare a comportamenti inappropriati o inefficaci:

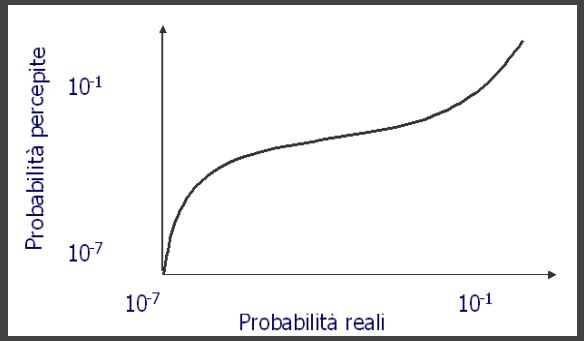
- **Sottovalutazione del rischio**: Se la sicurezza percepita è maggiore di quella reale, le persone potrebbero adottare comportamenti rischiosi perché credono di essere più sicure di quanto non siano in realtà.
- **Eccesso di precauzione**: Se la sicurezza percepita è inferiore a quella reale, potrebbe esserci un eccesso di precauzione, con conseguente impatto sull'efficienza e sui costi operativi.

Ad esempio, anche se un impianto è dotato di tutte le protezioni necessarie, la mancanza di una comunicazione chiara potrebbe portare i lavoratori a non sentirsi completamente al sicuro, compromettendo l'efficacia delle misure di sicurezza.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

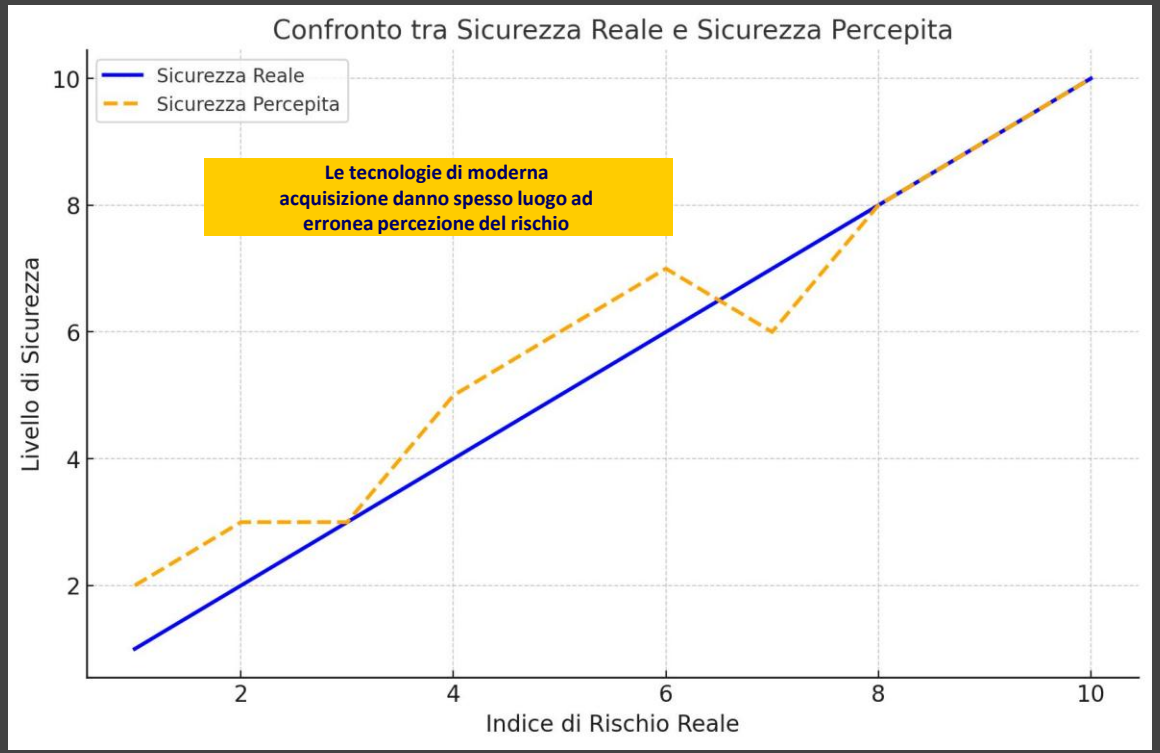
Sicurezza Reale e Percepita

Per rappresentare visivamente la relazione tra sicurezza reale e percepita, possiamo utilizzare un **grafico a dispersione** (scatter plot) o una **linea comparativa** che mostri come la percezione del rischio possa variare rispetto al rischio reale. Creerò un grafico per illustrare questo concetto.



Un approccio equilibrato alla sicurezza è sviluppato soltanto se il rischio reale coincide (o quasi) con quello percepito

Occorre approfondire le modalità di percezione del rischio e correggere le distorsioni con opera di informazione



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Migliorare la **sicurezza percepita** è un aspetto fondamentale per garantire che le persone si sentano al sicuro nei loro ambienti, non solo in termini di numeri e misure, ma anche psicologicamente. La sicurezza percepita può avere un impatto significativo sul comportamento dei lavoratori, sulla loro produttività e sul benessere generale. Vediamo alcune strategie per migliorare la sicurezza percepita.

1. Comunicazione Chiara e Costante

- **Informare e Coinvolgere il Personale**: Comunicare chiaramente le misure di sicurezza adottate è essenziale. Il personale deve sapere esattamente quali sono le misure di protezione implementate, perché sono importanti e come funzionano.
- **Trasparenza sulle Iniziative di Sicurezza**: Aggiornare i lavoratori su qualsiasi miglioramento o cambiamento nelle procedure di sicurezza, e spiegare come tali azioni migliorano la loro protezione, aiuta a creare fiducia.

Rispondere alle Preoccupazioni: Creare un canale aperto per ricevere e rispondere alle preoccupazioni di sicurezza percepite dai dipendenti. Questo dialogo aperto aiuta a ridurre l'ansia e a correggere eventuali idee sbagliate.

2. Formazione e Sensibilizzazione

- **Formazione su Misure di Sicurezza e Rischi**: Fornire una formazione continua per spiegare i rischi presenti nell'ambiente e le misure per mitigarli. La conoscenza crea una maggiore comprensione e quindi una percezione più realistica della sicurezza.
- **Simulazioni e Esercitazioni Pratiche**: Eseguire esercitazioni pratiche, come simulazioni di evacuazione o esercizi per gestire situazioni di emergenza, aiuta a rafforzare la fiducia nelle procedure di sicurezza e riduce il senso di vulnerabilità.
- **Comportamenti Sicuri**: Educare il personale sull'importanza di adottare comportamenti sicuri. Quando le persone capiscono che possono contribuire attivamente alla propria sicurezza, la loro percezione di essere al sicuro aumenta.

3. Ambiente di Lavoro Visivamente Sicuro

- **Segnaletica Chiara e Ben Visibile**: Utilizzare segnaletica di sicurezza ben visibile e chiara per indicare aree pericolose, vie di fuga e dispositivi di sicurezza. Una buona segnaletica contribuisce a creare un ambiente che "appare" più sicuro.
- **Ordine e Pulizia**: Mantenere l'ambiente di lavoro pulito e ben organizzato riduce la percezione del rischio. Un luogo di lavoro disordinato può far percepire un maggiore senso di pericolo e disorganizzazione.
- **Manutenzione e Controllo Visivo degli Equipaggiamenti**: Equipaggiamenti ben mantenuti e ispezioni regolari visibili aumentano la fiducia nelle attrezzature di sicurezza. L'aspetto fisico delle attrezzature e il modo in cui vengono curate può influenzare fortemente la percezione della loro affidabilità.

4. Partecipazione Attiva dei Lavoratori

- **Coinvolgimento nel Processo di Valutazione del Rischio**: Quando i lavoratori sono coinvolti nell'analisi del rischio e nella definizione delle soluzioni, si sentono parte del processo di sicurezza e sviluppano una percezione più positiva del loro ambiente.
- **Programmi di Segnalazione di Rischi**: Incoraggiare il personale a segnalare situazioni o comportamenti a rischio contribuisce a creare una cultura di sicurezza proattiva. Le persone che hanno un ruolo attivo nella segnalazione percepiscono un controllo maggiore, aumentando la loro sicurezza percepita.

5. Supporto Psicologico e Gestione dello Stress

- **Supporto Psicologico**: Offrire supporto psicologico per ridurre l'ansia o le paure dei lavoratori nei confronti dei rischi percepiti. La consulenza professionale può essere utile per affrontare situazioni di stress legate alla sicurezza.
- **Promuovere il Benessere sul Lavoro**: Programmi di benessere aziendale possono contribuire a migliorare la percezione generale di sicurezza, poiché migliorano il morale e il comfort emotivo dei dipendenti.

6. Cultura della Sicurezza

- **Esempio da Parte dei Responsabili**: I leader devono essere i primi a rispettare e promuovere le norme di sicurezza. Un buon esempio da parte della direzione rafforza la percezione della serietà delle misure adottate.
- **Riconoscere i Comportamenti Sicuri**: Riconoscere pubblicamente i dipendenti che adottano comportamenti sicuri rinforza l'importanza della sicurezza e incoraggia gli altri a fare lo stesso.
- **Cultura della Segnalazione senza Ritorsioni**: Creare un ambiente in cui i lavoratori possono segnalare problemi di sicurezza senza paura di conseguenze è essenziale per costruire una sicurezza percepita positiva.

7. Tecnologia per il Monitoraggio della Sicurezza

- **Utilizzo di Sistemi di Monitoraggio in Tempo Reale**: Implementare tecnologie come sistemi di monitoraggio video o sensori che verificano il rispetto delle misure di sicurezza aiuta i lavoratori a sentirsi più protetti, sapendo che vi è un sistema continuo di verifica e controllo.
- **Feedback in Tempo Reale**: Tecnologie che forniscono feedback in tempo reale, come sistemi di allarme per anomalie o DPI con sensori integrati, possono aumentare la percezione di protezione.

Conclusione

Migliorare la sicurezza percepita richiede un approccio multidimensionale che include comunicazione, formazione, coinvolgimento attivo, supporto psicologico e miglioramenti dell'ambiente fisico. Quando le persone capiscono le misure di sicurezza in atto, sono coinvolte nei processi e vedono che i loro ambienti sono ben gestiti, la loro percezione di essere al sicuro migliora. Di conseguenza, questo porta a comportamenti più sicuri, migliorando l'efficacia complessiva delle misure di sicurezza.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

STRUMENTI OPERATIVI

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

STRUMENTI OPERATIVI

Identificazione dei pericoli → **FMEA / FMECA**

Identificazioni degli effetti conseguenti a guasti di componenti o dispositivi di sicurezza dei pericoli → **HaZop**

Identificazioni degli effetti conseguenti a guasti di componenti o dispositivi di sicurezza dei pericoli →

- **Fault Tree Analysis**: combinazione di eventi che comportano un effetto indesiderato (Top Event)
- **Event Tree Analysis:** sequenze incidentali originate da un Top Event,in concomitanza di eventi che ne condizionano l'evoluzione

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FME(C)A

Failure Modes Effects and Criticality Analysis

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

FMEA (Failure Modes and Effects Analysis) è una metodologia sistematica utilizzata per identificare e valutare i **modi di guasto** (failure modes) di un sistema, un processo, un prodotto o un componente. L'obiettivo è prevenire guasti o mitigare i loro effetti, identificando cause, conseguenze e misure preventive. L'analisi si concentra principalmente su tre parametri:

1. **Gravità (Severity)**: valuta l'impatto del guasto se si verifica.
2. **Occorrenza (Occurrence)**: misura la probabilità che il guasto si verifichi.
3. **Rilevabilità (Detection)**: valuta quanto sia facile rilevare il guasto prima che causi problemi.

Questi tre parametri sono usati per calcolare un indice chiamato **RPN (Risk Priority Number)**, che viene usato per determinare le priorità delle azioni correttive. Il RPN è dato dalla formula:

$$RPN = Gravita` \times Occorrenza \times Rilevabilita`$$

Obiettivo della FMEA: l'obiettivo primario è ridurre il rischio associato a potenziali guasti attraverso azioni preventive o mitigative, migliorando l'affidabilità e la sicurezza del sistema.

FMECA (Failure Modes, Effects, and Criticality Analysis) è una variante avanzata della FMEA che aggiunge un'analisi di **criticità** per valutare l'importanza relativa dei diversi guasti in base alla loro **probabilità e impatto**. È particolarmente utile nei settori in cui la sicurezza è cruciale, come l'aerospaziale o il militare.

In aggiunta ai parametri di base della FMEA (gravità, occorrenza, rilevabilità), la FMECA include:

- **Criticità**: misura la gravità del guasto considerando non solo la sua probabilità ma anche l'impatto potenziale in termini di sicurezza, costi e tempi di fermo. La criticità può essere valutata in diversi modi, ad esempio con la matrice di rischio o con altre tecniche quantitative.

Obiettivo della FMECA: oltre a prevenire i guasti, come nella FMEA, l'obiettivo della FMECA è focalizzarsi sui guasti più **critici** per la sicurezza o per la missione, gestendo le risorse in modo più efficiente per prevenire problemi con maggiore impatto.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Definizioni

La gravità è l'impatto relativo alla sicurezza e alla prestazione funzionale

S = 10 → Incidenti di multipla fatalità o un guasto con gravi conseguenze

S = 1 → Danni trascurabili

La frequenza è la probabilità di accadimento

F = 10 → Evento certo

Indice di criticità (IdC) = O • G • R

La rilevabilità è indice di quanto il difetto può essere individuato nel processo

R =10 → Evento non rilevabile

R=1 → Evento rilevabile

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

DIFFERENZE FRA FMEA E FMECA

La principale differenza tra FMEA e FMECA risiede nell'approfondimento dell'analisi e nella valutazione della criticità:

1. **Criticità**: FMECA include un'analisi di criticità che permette di dare priorità ai guasti più rilevanti dal punto di vista della sicurezza o delle prestazioni, mentre la FMEA si limita a identificare i guasti e calcolare il rischio in base al RPN.
2. **Applicazione**: FMEA è generalmente più semplice e può essere utilizzata in contesti industriali più ampi per migliorare processi, prodotti o sistemi. La FMECA è più specifica e viene utilizzata in ambiti dove la sicurezza o la criticità sono aspetti fondamentali (ad esempio, industria aerospaziale, automotive, difesa).
3. **Output**: FMEA genera un RPN che dà una visione del rischio combinato di ogni guasto, mentre FMECA classifica i guasti in base alla loro criticità, consentendo decisioni più mirate.

In sintesi, mentre sia FMEA che FMECA mirano a identificare e prevenire i guasti, la FMECA si distingue per un'analisi più approfondita, con una valutazione quantitativa della criticità. Questo la rende particolarmente utile in settori dove la sicurezza è una priorità assoluta.

CARATTERISTICHE

Metodologia altamente strutturata che consiste in una tabulazione dei singoli componenti dell'impianto, delle relative modalità di guasto e dei corrispondenti effetti. Di ogni componente studia inoltre gli eventi iniziatori del "peggior caso" verificabile.

VANTAGGI

Le sue caratteristiche di completezza e rigorosità fanno sì che si presti particolarmente allo studio di impianti di tipo componentistico, costituiti cioè da 10 o più "items", può fornire informazioni utili all'applicazione di metodologie sistemistiche (FTA, ecc).

SVANTAGGI

Utilizzato da solo non è sufficiente ad identificare le possibili interazioni di guasto tra i vari sistemi dell'impianto. Non è adatto alla identificazione di cause di processo, di utilities, ecc. A volte, la valutazione quantitativa dei singoli livelli si dimostra complessa e il risultato è un giudizio troppo soggettivo.

APPLICAZIONE

Rara, può essere eseguita da una squadra multidisciplinare di professionisti o anche da due soli analisti. Applicata dettagliatamente risulta essere onerosa per cui può essere sostituita da PHA (Preliminary Hazard Hanalysis) o "What if". In media, ad ogni analista è sufficiente poco tempo per 2 - 4 operazioni di controllo.

Prof. Claudio Pantanali, PhD cpantanali@units.it

- E’ un potente strumento di analisi nel campo di verifica (affidabilistico e/o della sicurezza) della qualità di un progetto.
- E’ una tecnica affidabilistica di tipo induttivo: si analizza il guasto e poi gli eventi che questo può causare.
- È una tecnica di tipo bottom-up: si parte dalla struttura elementare e si procede verso i livelli superiori, indicando le modalità di guasto e le conseguenze che ne derivano.
- La tecnica è qualitativa.
- L’analisi inizia a livello di componente:

    1.per determinare cosa potrebbe "andar male“

    2.analizza le cause

    3.valuta quali sono gli effetti sul sistema.

CAMPI DI APPLICAZIONE

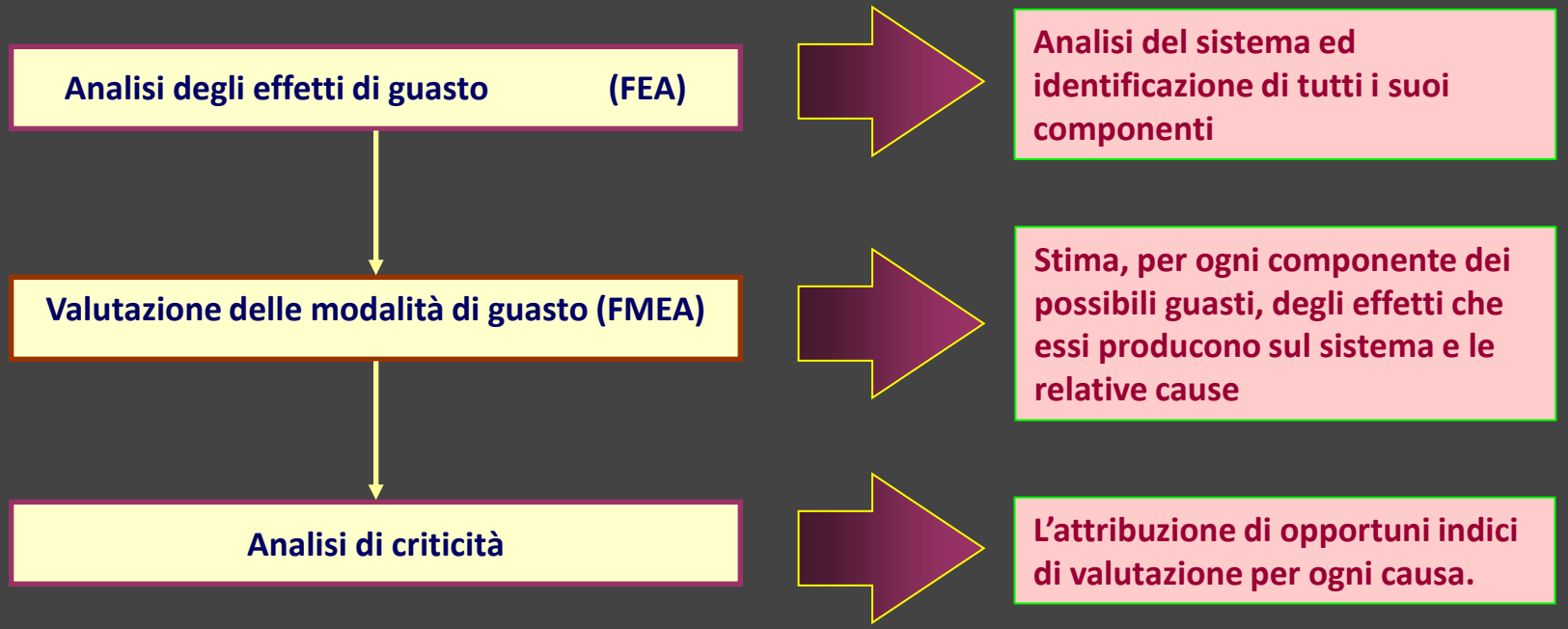
E’ il metodo più diffuso di analisi e di validazione del progetto di un prodotto industriale (meccanico, elettronico, ecc.). E’ esplicitamente prevista dalla norma UNI EN 29004 relativa alla garanzia di qualità della progettazione.

La disponibilità di informazioni relative ai modi in cui un oggetto o un impianto può danneggiarsi consente di analizzare e migliorare altre caratteristiche del prodotto non connesse direttamente alla sicurezza nella fase d’uso.

L'aggiunta di una Analisi di Criticità (FMECA, Failure Mode, Effects and Criticality Analysis) permette di quantificare la gravità degli effetti di ciascun modo di guasto e, di classificare tutti i modi di guasto previsti in base ad un indice di criticità.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Fasi di sviluppo



Prof. Claudio Pantanali, PhD cpantanali@units.it

INFORMAZIONI PRINCIPALI

1. **Numero di identificazione del componente: permette un'impostazione sistematica del problema in esame.**
2. **Funzioni del componente: la descrizione delle funzioni che i vari componenti devono svolgere è importante per capire il non funzionamento del sistema, ed individuare quindi i "modi di guasto".**
3. **Modi di guasto: individuare i modi di guasto richiede l'individuazione delle cause che possano impedire lo svolgimento corretto delle funzioni del componente o del sistema.**
4. **Cause di guasto: individuare le cause all'origine dei guasti contribuisce ad eliminarle con la revisione del progetto.**
5. **Effetti di guasto: individuare l'effetto che il guasto del componente produce sul sistema dà un idea del rischio che viene generato dal guasto.**
6. **Azioni Correttive: individuare metodi e strumenti per ridurre il rischio.**

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

ESEMPIO

Prendiamo in considerazione lo stesso cuscinetto a sfera montato su un albero rotante in una linea di produzione. Questo cuscinetto consente la rotazione dell'albero riducendo l'attrito. L'analisi identificherà i possibili modi di guasto, le loro cause, gli effetti, e come priorizzare le azioni correttive calcolando l'RPN.

Modo di Guasto	Cause del Guasto	Effetti del Guasto	Gravità (S)	Occorrenza (O)	Rilevabilità (D)	RPN
Bloccaggio del cuscinetto	Lubrificazione inadeguata, accumulo di sporco	Arresto della macchina, possibile rottura dell'albero	9	5	4	180
Usura eccessiva	Fatica del materiale, sovraccarico	Vibrazioni, ridotta efficienza, usura di altri componenti	7	6	6	252
Deformazione della pista	Sovraccarico accidentale, errato montaggio	Rigidità eccessiva, maggiore attrito, danno a componenti vicine	6	3	5	90
Corrosione	Contaminazione con acqua o umidità	Riduzione della vita utile, vibrazioni e rumorosità	5	4	3	60

L'**RPN (Risk Priority Number)** viene calcolato moltiplicando i seguenti tre fattori:

1.Gravità (Severity, S): quanto sono gravi gli effetti del guasto?

1. Varia da **1** (nessun effetto) a **10** (effetto catastrofico).
2. Nel nostro esempio, il bloccaggio del cuscinetto è critico e può fermare l'intera linea di produzione. Pertanto, il valore è alto, **9**.

2.Occorrenza (Occurrence, O): quanto è probabile che il guasto si verifichi?

1. Varia da **1** (molto improbabile) a **10** (molto frequente).
2. Se non viene effettuata la manutenzione periodica, la probabilità di un guasto per lubrificazione inadeguata è significativa, quindi scegliamo **5**.

3.Rilevabilità (Detection, D): quanto è facile rilevare il guasto prima che causi problemi significativi?

1. Varia da **1** (molto facile da rilevare) a **10** (molto difficile da rilevare).
2. Nel caso di un bloccaggio del cuscinetto, non ci sono sensori dedicati per rilevarlo prima che si manifestino problemi. Pertanto, la rilevabilità è media, **4**.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Per ciascun modo di guasto, il **RPN** viene calcolato come: **RPN=S × O × D**

1.Bloccaggio del cuscinetto:

1. S = 9, O = 5, D = 4
2. RPN = 9×5×4=1809 \times 5 \times 4 = 1809×5×4=180

2.Usura eccessiva:

1. S = 7, O = 6, D = 6
2. RPN = 7×6×6=2527 \times 6 \times 6 = 2527×6×6=252

3.Deformazione della pista:

1. S = 6, O = 3, D = 5
2. RPN = 6×3×5=906 \times 3 \times 5 = 906×3×5=90

4.Corrosione:

1. S = 5, O = 4, D = 3
2. RPN = 5×4×3=605 \times 4 \times 3 = 605×4×3=60

L'RPN è usato per determinare la **priorità delle azioni correttive**. Più alto è il valore dell'RPN, più urgente è il bisogno di intervenire. In questo esempio:

- **Usura eccessiva** ha l'RPN più alto (**252**), indicando che è una delle principali cause su cui intervenire. Sono necessarie azioni correttive, come un'ispezione più frequente e il miglioramento del design per ridurre il carico.
- **Bloccaggio del cuscinetto** ha un RPN di **180**: anche in questo caso, l'intervento è urgente per evitare fermi produttivi e danni.
- **Deformazione della pista** e **corrosione** hanno RPN più bassi (90 e 60), suggerendo che i guasti sono relativamente meno critici rispetto agli altri due casi.

Azioni Correttive

Per ridurre l'RPN, possiamo intervenire su uno o più dei parametri:

- **Ridurre Occorrenza (O)**: ad esempio, un programma di **manutenzione preventiva** riduce la probabilità di guasti.
- **Migliorare la Rilevabilità (D)**: installare **sensori di vibrazione** per monitorare il comportamento del cuscinetto potrebbe rendere più facile identificare l'usura precoce.
- **Ridurre la Gravità (S)**: a volte è possibile riprogettare il sistema in modo tale che il guasto di un componente non abbia un impatto catastrofico sull'intero processo.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop
Hazard & Operability Analysis

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop

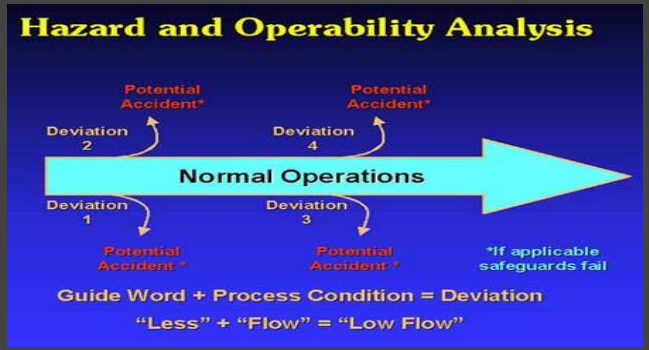
Hazard & Operability Analysis

- E' stata sviluppata inizialmente per l'identificazione dei pericoli connessi con tecnologie innovative.
- Consente di identificare e valutare pericoli inerenti la sicurezza di sezioni di processo che possono compromettere la capacità dell'impianto di raggiungere le prestazioni predefinite.

obiettivi

HAZOP GUIDE WORDS	
No or Not	Complete negation of the intention from the design.
More	Quantitative increase in whatever is being identified.
Less	Quantitative decrease in whatever is being identified.
As Well As	Qualitative modification, or a qualitative increase.
Part Of	Qualitative modification or decrease.
Other Than	Complete substitution.
Early	Something occurred earlier than intended (clock time).
Late	Something occurred later than intended (clock time).
Before	Step was performed before it should have in the process sequence.
After	Step was performed after it should have in the process sequence.

- Scopo dell'HAZOP è la revisione di processi industriali e di procedure operative in modo da definire se le deviazioni del processo dalle condizioni di progetto possono determinare conseguenze indesiderabili.
- Il risultato è l'individuazione delle cause potenziali, delle conseguenze delle deviazioni, delle misure di sicurezza esistenti a protezione.
- Possono essere formulate raccomandazioni a sviluppare studi più approfonditi su aree dove non è stato possibile giungere a conclusioni per mancanza di dettagliate informazioni.



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop

Hazard & Operability Analysis

caratteristiche

1. Identifica gli eventi iniziatori della condizione peggiore ipotizzabile.
2. E' una tecnica deduttiva.
3. Il risultato consiste nell'identificazione dei rischi e dei problemi operativi.
4. E' particolarmente adatta per l'industria di processo e ottima dal punto di vista economico se applicata ad un nuovo impianto.
5. Il team deve essere composto da 5-7 tecnici.

1. Identifica gli eventi iniziatori della condizione peggiore ipotizzabile.
2. E' una tecnica deduttiva.
3. Il risultato consiste nell'identificazione dei rischi e dei problemi operativi.
4. E' particolarmente adatta per l'industria di processo e ottima dal punto di vista economico se applicata ad un nuovo impianto.
5. Il team deve essere composto da 5-7 tecnici.

risorse richieste

Accurati ed aggiornati diagrammi P&I o documenti tecnici equivalenti ed altre dettagliate informazioni inerenti i processi e le procedure operative

Una profonda conoscenza del processo, della strumentazione, e delle modalità di conduzione dell'impianto. Tali informazioni sono generalmente fornite dai membri del team con attinenza alle relative aree di competenza.

Prof. Claudio Pantanali, PhD cpantanali@units.it

le fasi di sviluppo

Il team-leader guida lo studio funzionale dei parametri di processo dell'impianto utilizzando un set di parole chiave prefissate (le parole guida) applicate in punti cruciali del processo (i nodi di studio)

Si ricorrerà a checklists o all'esperienza maturata sul processo per sviluppare la lista necessaria di deviazioni da considerare

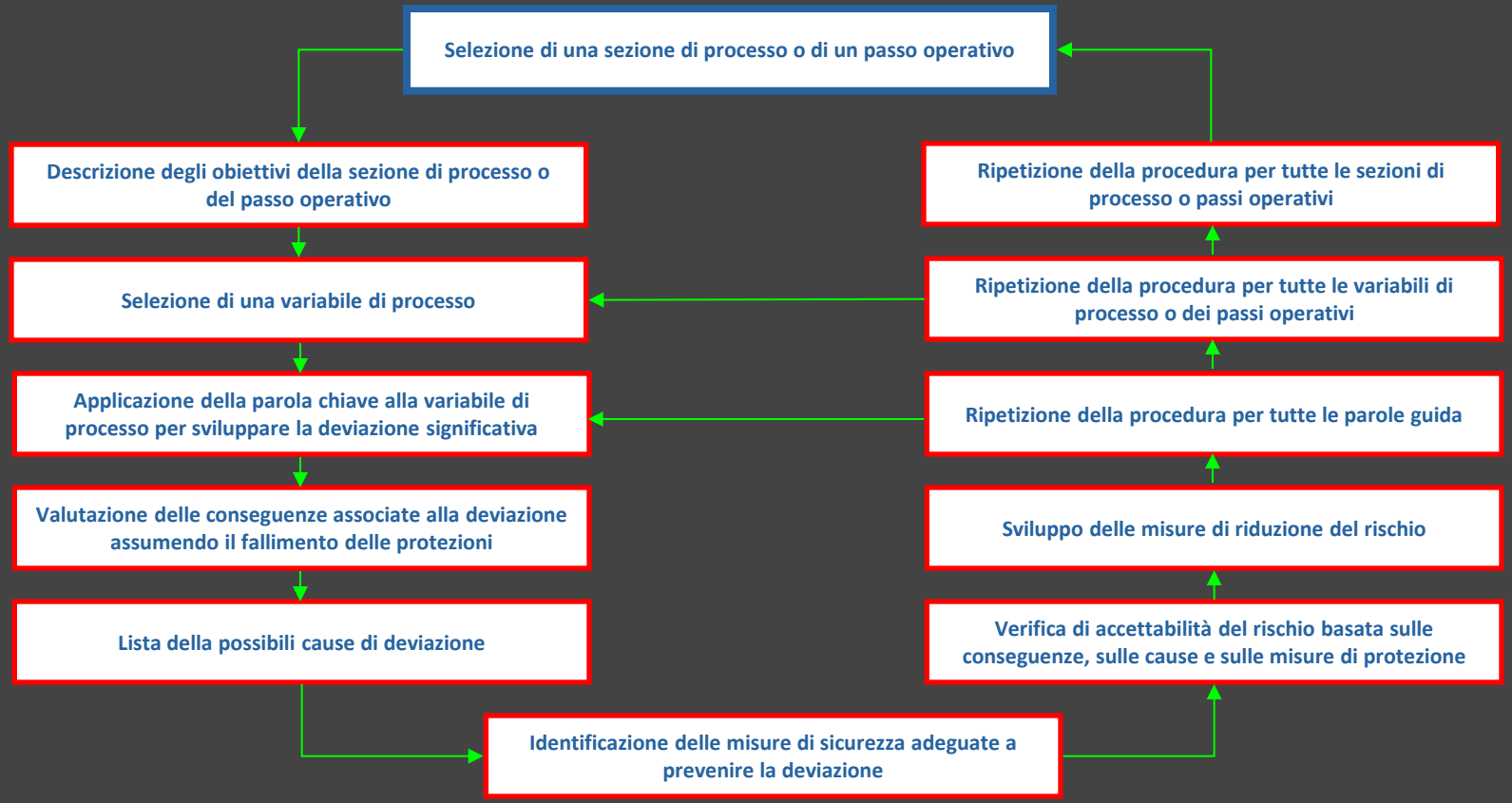
Le parole guida sono combinate con specifici parametri di processo per identificare potenziali deviazioni dalle condizioni di progetto

Il team concorda le cause delle deviazioni (p.e sovrappressioni delle pompe) e sulle misure di sicurezza applicabili alle deviazioni (p.e. una valvola di sfiato su una condotta di scarico)

Se le cause e le conseguenze sono significative e le misure di sicurezza inadeguate si prevede un'analisi retroattiva (follow-up)

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

il diagramma di flusso



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop

Hazard & Operability Analysis

L'analisi di pericolo e funzionalità (*Hazard Operability analisys*) è una metodologia di valutazione del pericolo qualitativa elaborata inizialmente per essere applicata in fase di progettazione dei processi, allo scopo di individuare e limitare preventivamente tutti i possibili problemi operativi. Nel tempo la tecnica è stata impiegata con successo anche a processi già in fase produttiva.

L'Hazop viene condotto da un team multidisciplinare in cui sono presenti da un lato un gruppo di esperti nella applicazione della metodologia e dall'altro una rappresentanza qualificata di responsabili del progetto, di tecnologi del processo, della sicurezza di impianto, dei sistemi di controllo e della strumentazione e della manutenzione.

Le attività del gruppo sono dirette e coordinate da un Team leader di adeguata esperienza e competenza che, durante una serie di incontri, analizzano tutta la documentazione disponibile del processo, come:

- calcoli di progetto;
- manuale operativo dell'impianto;
- fogli specifiche di tutte le apparecchiature (pompe, scambiatori di calore, ecc.), con dati operativi, temperature, pressioni, portate e materiali trattati;
- processi e reazioni;
- sostanze e materiali a stoccaggio e trattati nel processo;
- eventuali informazioni sulla frequenza di guasti e manutenzione delle apparecchiature;
- elenco delle linee trasferimento liquidi e gas e classi delle tubazioni;
- elenco delle valvole di sicurezza, fogli specifiche e pressioni di intervento;
- caratteristiche ambientali del territorio circostante.

Lo scopo dell'Hazop è quello di identificare tutte le possibili deviazioni dalle normali condizioni operative del processo e, qualora venissero verificate conseguenze significative, si segnala il potenziale pericolo.

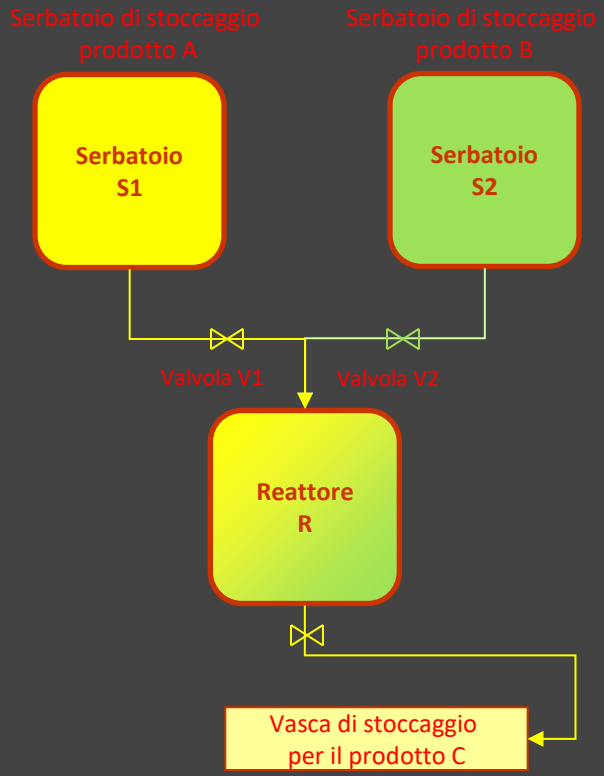
I responsabili del processo dovranno tenere conto delle informazioni prodotte dall'Hazop per intraprendere tutte le necessarie azioni di limitazione del rischio

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FMECA (Failre Modes Effects and Criticality Analysis)

Esempio

Identificazione	linea di collegamento fra serbatoio S1 e reattore R.
Componente	Valvola V1 di comunicazione posta tra contenitore della sostanza A e reattore
Descrizione	Stato di conduzione normale è : valvola V1 normalmente aperta per permettere il deflusso della sostanza A
Modi di guasto	valvola V1 rimane completamente aperta quando era richiesta la chiusura
Effetti	• flusso verso il reattore della sostanza A quando questo non richiesto • alta pressione nel reattore R • alta temperatura nel reattore R • prodotto finale non buono perché ricco della sostanza A • alto livello nel serbatoio finale F di raccolta • pericolo per la presenza della sostanza A nella zona di lavoro.
Sistema di protezione	• misuratore di portata posto sulla linea, capace di registrare incrementi indesiderati della sostanza A e avvertire per mezzo di allarme; • sistema di aerazione capace di espellere dalla zona lavoro la presenza della sostanza A quando questa si disperde in aria
Intervento	Aggiunta valvola di sfiato verso l'esterno sul reattore; Aggiunta misuratore di temperatura collegato ad un allarme, ecc



Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop

Hazard & Operability Analysis

La procedura operativa dell'Hazop

Tra i documenti da analizzare una particolare importanza assume il Piping & Instrumentation Diagram (P&I), ovvero lo schema di marcia del processo. Come già è noto, il P&I non si limita a fornire solamente informazioni sulle apparecchiature principali e i circuiti di regolazione automatica, in maniera da illustrare soltanto i principi generali del processo, ma riporta in dettaglio assolutamente tutti i dispositivi e le apparecchiature presenti nell'impianto. In particolare, tutto il sistema delle valvole di sicurezza alla sovrapressione, le linee di blow down, le linee dei servizi come il vapore di rete, l'acqua industriale, i gas tecnici, e le linee eventualmente necessarie solo nelle procedure di avviamento o arresto dell'impianto.
In questo modo sarà possibile studiare il processo senza rischiare di trascurare dispositivi ed elementi di linea apparentemente insignificanti durante la conduzione regolare del processo, ma il cui malfunzionamento può innescare una sequenza di eventi negativi. Il team Hazop, utilizzando una terminologia specifica, applica la seguente procedura standard.

Individuazione di un nodo

Il processo viene suddiviso in stadi operativi elementari, definiti nodi, che possono essere apparecchiature come reattori, scambiatori di calore o anche linee di trasferimento. Ad ogni nodo possono essere associati tutti i dispositivi necessari al suo funzionamento, come valvole o circuiti di regolazione. Il livello di dettaglio di un nodo viene scelto dal team leader, in base alla sua esperienza. Tuttavia, l'insieme dei nodi deve essere scelto in modo tale che nessuno dei dispositivi o apparecchiature presenti nel P&I ne rimanga escluso.

Prof. Claudio Pantanali, PhD cpantanali@units.it

Dichiarazione delle intenzioni progettuali del nodo

Questa comprende sia i compiti che il nodo deve assolvere che i parametri di progetto ed i loro range operativi. Ad esempio, se il nodo è costituito da una linea di scarico di sovrapressione comandata da una valvola le intenzioni progettuali includono la pressione alla quale la valvola si deve aprire e i limiti di portata che la linea può scaricare.
In questo modo il team stabilisce se una determinata condizione è all'interno dei limiti di operabilità o può dare luogo ad una deviazione dalle condizioni regolari.

Individuazione dei parametri coinvolti nelle intenzioni progettuali del nodo

Una lista dei possibili parametri operativi è riportata nella Tab. 2. Tuttavia l'elenco non si deve intendere esaustivo e sta all'esperienza del team non tralasciare parametri che potrebbero essere fondamentali nella individuazione delle *deviazioni.*

Parametri coinvolti nella descrizione del nodo			
Parametri operativi	**Azioni**	**Parametri fisici e chimico/fisici**	**Parametri di controllo**
Portata	Agitazione	Viscosità	Misura
Pressione	Miscelazione	Dimensioni particelle	Controllo
Temperatura	Separazione	Tempo	Sequenza
Livello	Addizione	Fase	Segnale
	Reazione	Velocità	Avvio/Arresto
	Trasferimento	Composizione	Comunicazione
		pH	Servizio

Esempio di possibili parametri per l'analisi Hazop.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Applicazione delle parole guida ai parametri operativi e ricerca delle deviazioni

Il punto principale della metodologia Hazop consiste nell'applicare ai parametri di processo un certo di numero di parole chiave e investigare se la combinazione può dare luogo ad una deviazione dalle normali condizioni operative. Se la deviazione costituisce un pericolo potenziale il team produce delle raccomandazioni.
Le parole chiave sono riportate in tabella.

Parole guida e significato	
Assenza (no, none)	Nessuna intenzione progettuale si è ottenuta (assenza di flusso, di scambio termico..).
Aumento (more)	Riferito al parametro operativo considerato (aumento di temperatura, pressione, ecc.).
Diminuzione (less)	Riferito al parametro operativo considerato (diminuzione di temperatura, pressione, ecc.).
Diverso da (other than)	Ad esempio, una composizione differente da quella prevista.
Più di (more than)	Più componenti o attività di quelli previsti.
Altro (other than)	Si ha un'altra attività rispetto alle previste intenzioni progettuali.
Parte di	Si è ottenuta solo una parte delle intenzioni progettuali.
Inverso	Si verifica l'opposto delle intenzioni progettuali (esempio: il flusso è opposto).
Altrove	Applicabile a portate, destinazioni.
Prima/dopo	La sequenza operativa è errata (in particolare per operazioni discontinue).
Prima/dopo	Il tempo delle operazioni è differente.
Più veloce/più lento	L'intenzione è raggiunta troppo presto/troppo tardi.

Parole guida standard della procedura Hazop.

Non tutte le combinazioni tra parole guida e parametri scelti hanno un reale significato.

Ad esempio, la condizione "assenza di temperatura", ottenuta associando la parola guida "assenza" ed il parametro "temperatura", non ha significato fisico, mentre ha perfettamente senso la combinazione "assenza di portata".

Questa se riferita ad una portata di acqua di raffreddamento può dare luogo ad una deviazione potenzialmente pericolosa.

Prof. Claudio Pantanali, PhD cpantanali@units.it

Individuazione delle cause di deviazione

Individuata una deviazione, ad esempio l'assenza di portata di acqua di raffreddamento, il team deve ricercarne tutte le possibili cause, considerando sia i possibili guasti delle apparecchiature che gli errori umani.
La raccolta di dati storici può essere di grande aiuto nell'approfondire solo le cause realistiche, anche non si deve mai trascurare l'analisi approfondita del caso e l'esperienza dei componenti del team. Quando tutte le cause che producono la deviazione sono state analizzate si passa allo studio di un'altra combinazione "parola guida-parametro".

Valutazione delle conseguenze

Le conseguenze di ogni causa di deviazione deve essere analizzata per controllare se i parametri di processo escono al di fuori dei range operativi delle intenzioni progettuali, valutando, eventualmente, anche i tempi in cui i range operativi vengono superati. Questo allo scopo di considerare anche l'intervento degli operatori e
delle apparecchiature di controllo e salvaguardia.
Una volta che le conseguenze sono ritenute rilevanti, anche considerando i sistemi di salvaguardia e protezione esistente, il team registra la deviazione come rilevante ed emette delle raccomandazioni per i responsabili del processo.

Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop

Hazard & Operability Analysis

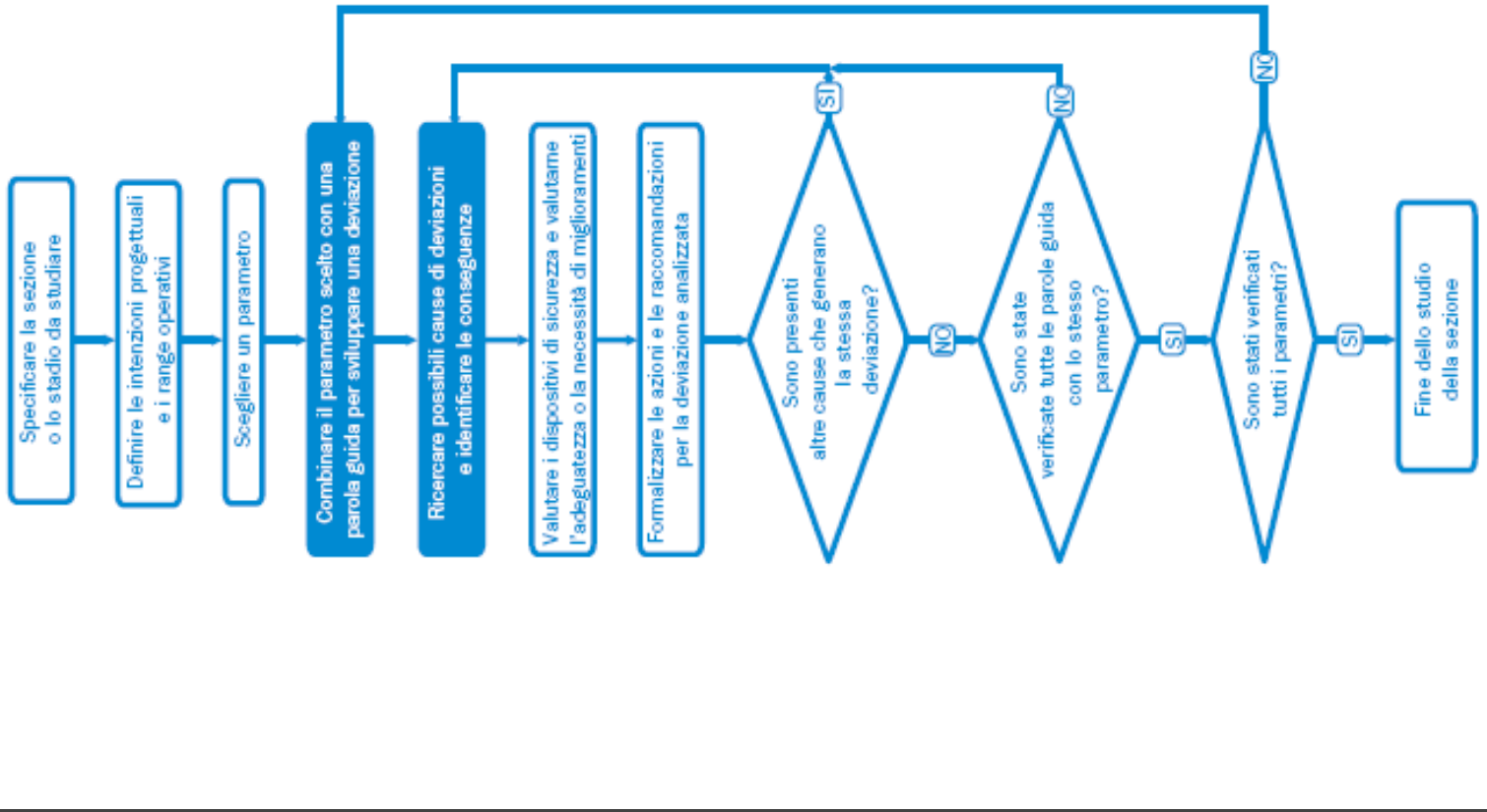


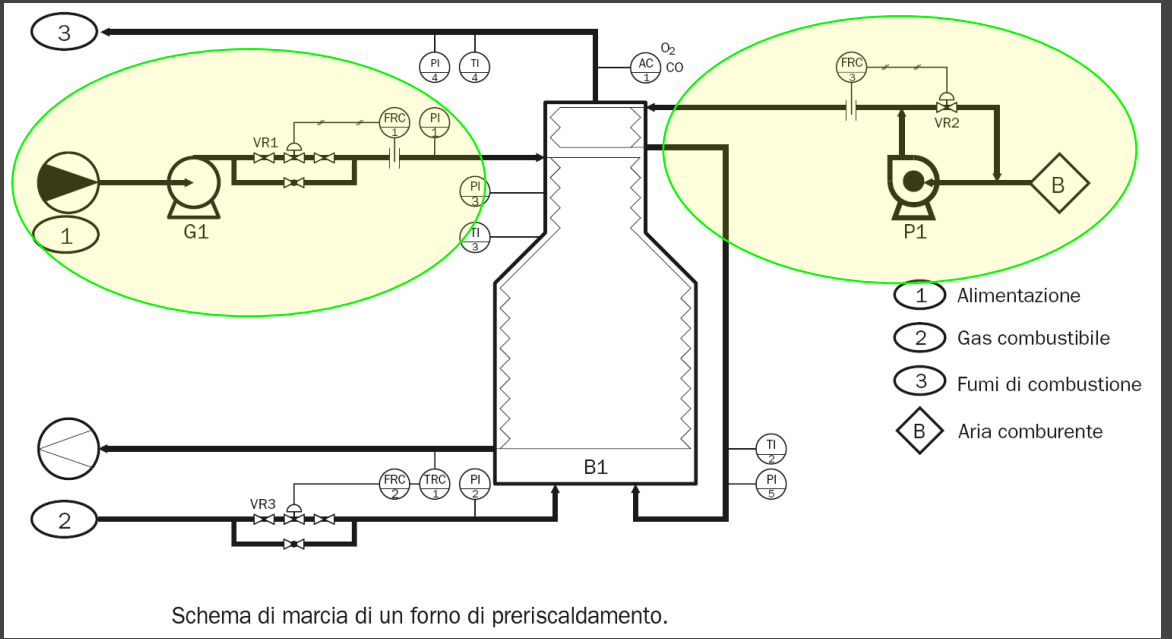
Diagramma di flusso della metodologia Hazop.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

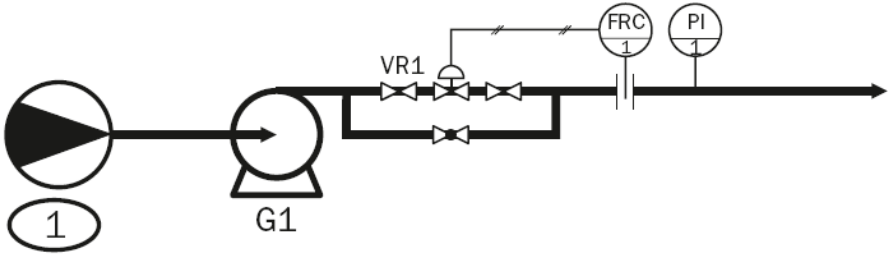
ESEMPIO DI APPLICAZIONE DELL'HAZOP

Con l'esempio seguente si vuole semplicemente presentare la metodologia senza la pretesa di rappresentare in ogni dettaglio un realistico studio di caso. Il numero e il tipo dei documenti necessari non consente una trattazione esaustiva, che andrebbe, peraltro, oltre gli obiettivi di questo corso. Basti pensare che il P&I diagram di un processo semplice come la distillazione vacuum ha una lunghezza di 7 metri, mentre quello del cracking catalitico di circa 10 metri. Per questi motivi, nel prossimo esempio si fornirà una versione solo leggermente più completa di un consueto schema di processo. Come esempio di applicazione si è scelto il forno di riscaldamento di una carica che deve essere destinata ad una reazione endotermica. Il forno utilizza un combustibile gassoso, come gas naturale o gas di raffineria, ed è presente un controllore della temperatura in uscita della carica (variabile controllata) che comanda la valvola di regolazione della portata del combustibile. Processi simili sono comuni nell'industria petrolifera e petrolchimica, come, ad esempio, l'idrodesolforazione della virgin naphta da inviare a reforming e il platforming stesso, dove la virgin naphta proveniente dall'impianto di desolforazione viene preriscaldata sino alla temperatura in cui il platino del catalizzatore è attivo. Si ipotizza che una portata di 250 m3/h deve essere riscaldata da 150 °C a 325 °C.



Schema di marcia di un forno di preriscaldamento.

La procedura Hazop prevede al primo punto la suddivisione del processo in diversi nodi che andranno affrontati singolarmente. Come primo nodo si consideri la linea di trasferimento dell'alimentazione dalla pompa G1 alla zona convettiva del forno B1



Nodo 1 del processo "Forno di preriscaldamento".

Definito il Nodo 1 si applicano i passi della procedura illustrati in precedenza. Solo a scopo esplicativo nella tabella seguente vengono riportati gli stessi blocchi del flow sheet, mentre nella pratica la metodologia Hazop viene presentata come tabella.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Applicazione del Flow sheet Hazop al nodo "Transfer line alimentazione"

L'applicazione di altre parole guida allo stesso parametro non fornisce altre deviazioni degne di considerazione ad eccezione di flusso-inverso che richiede semplicemente l'applicazione di una valvola di ritegno sulla mandata della pompa G1.

Passando all'analisi di altri parametri, l'unico che può dare deviazioni significative è la pressione.

Tuttavia l'aumento di pressione fino alla rottura delle tubazioni all'interno del forno può essere causato solo dalla chiusura di una valvola a valle del forno e conseguente assenza di flusso.

Quindi tutte le cause e le conseguenze e le azioni correttive sono già state considerate nel caso precedente.

Nodo 1	Linea trasferimento dell'alimentazione dalla pompa G1 al forno B1.
Intenzioni progettuali	Trasportare la portata $F = 250\ m^3/h$, sotto controllo di portata, all'interno del forno B1 tramite la pompa G1.
Scelta parametro 1	Portata
Parola guida 1	Assenza (no)
Deviazione 1 Ottenuta dalla combinazione parametro-parola guida.	Assenza di flusso nella linea di trasferimento.
Analisi della deviazione ed individuazione delle cause.	L'analisi del P&I porta alle seguenti possibili cause di deviazione: ■ il motore della pompa non funziona; ■ la valvola di regolazione VR1 è bloccata in posizione chiusa; ■ la tubazione o la flangia tarata (il misuratore di portata) sono ostruite; ■ c'è un problema a monte della linea di trasferimento.
Valutare le possibili conseguenze della deviazione.	■ Il fluido nel serpentino del forno si surriscalda e va incontro a reazioni di decomposizione termica (cracking); ■ il serpentino nel forno rimane senza liquido si surriscalda e si danneggia; ■ il serpentino si rompe e rilascia liquido infiammabile nella zona radiante, dove sono presenti fiamme libere: di conseguenza si sviluppa un incendio; ■ perdita di produzione nelle unità a valle del processo.
Valutazione dei dispositivi di sicurezza presenti e proposta di adeguamenti.	■ Installare un allarme di bassa portata; ■ utilizzare una valvola di controllo del tipo aria chiude che, in caso di guasto alla rete aria compressa strumentale, mette in sicurezza il forno B1 aprendo la valvola VR1; ■ a monte della linea di trasferimento, installare un allarme di basso livello nel serbatoio che alimenta la pompa G1.
Raccomandazioni.	Installare un sistema strumentato di sicurezza che, al verificarsi della deviazione, provveda a: ■ bloccare l'ingresso del combustibile ai bruciatori del forno; ■ continuare l'immissione di aria ai bruciatori; ■ utilizzare più misuratori di portata sulla linea di alimentazione; ■ utilizzare allarmi sonori e visivi attivati dalla bassa portata di alimentazione; ■ aprire la valvola a serrande del camino del forno.

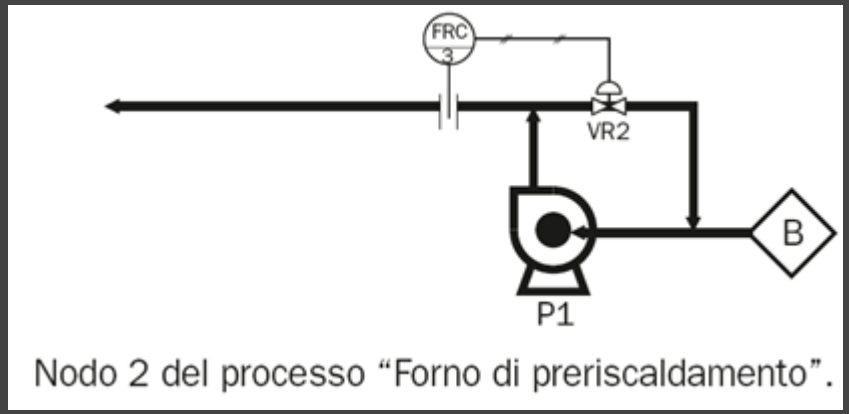
HaZop

Hazard & Operability Analysis

Composizione del Team							
P&I n°:			Foglio:				
Nodo: 2			Linea di trasferimento dell'aria dal ventilatore P1 al forno B1				
Intenzioni progettuali			Trasferimento della portata di aria necessaria alla combustione completa ed efficiente del combustibile, in modo che l'analizzatore dei fumi rilevi valori corretti di O_2 e CO.				
No	Parametro	Parola guida	Deviazione	Cause	Conseguenze	Protezioni presenti	Azioni
2	Portata	Assenza (No)	Assenza di portata di aria comburente.	Il motore del compressore non funziona.	La fiamma si spegne mentre il gas combustibile continua a fluire.	Sistema motore al compressore più affidabile.	Installare più sistemi di rilevazione della portata nella linea aria comburente.
				Il motore funziona ma l'accoppiamento con il compressore si è rotto.	La camera della fornace non è a tenuta e aria potrebbe essere presente. Se l'aria non viene fornita al bruciatore ed il gas combustibile si accumula nella camera l'aria presente e le superfici calde potrebbero determinare una esplosione.	Il controllore dell'aria deve essere di tipo aria apre che in mancanza di aria strumentale chiude la valvola ed evita la mancanza di aria al bruciatore.	Bloccare la portata di combustibile in assenza di portata aria comburente.
				La valvola VR2 di controllo portata a riciclo si è aperta completamente.	L'esplosione può provocare danni alle persone, alle apparecchiature e mancata produzione.		Utilizzare un sistema strumentato di sicurezza con un sistema di allarmi anche sonori e visivi.
				La tubazione si è intasata per qualche motivo.			Accorciare i tempi di intervento del sistema di sicurezza.
							Utilizzare schermi e reti di sicurezza nella aspirazione del compressore e verificare anche visivamente l'assenza di ostruzioni che coprono la rete di aspirazione.

Tab. 5 ▶ Applicazione del Flow sheet Hazop al nodo "Transfer line aria comburente".

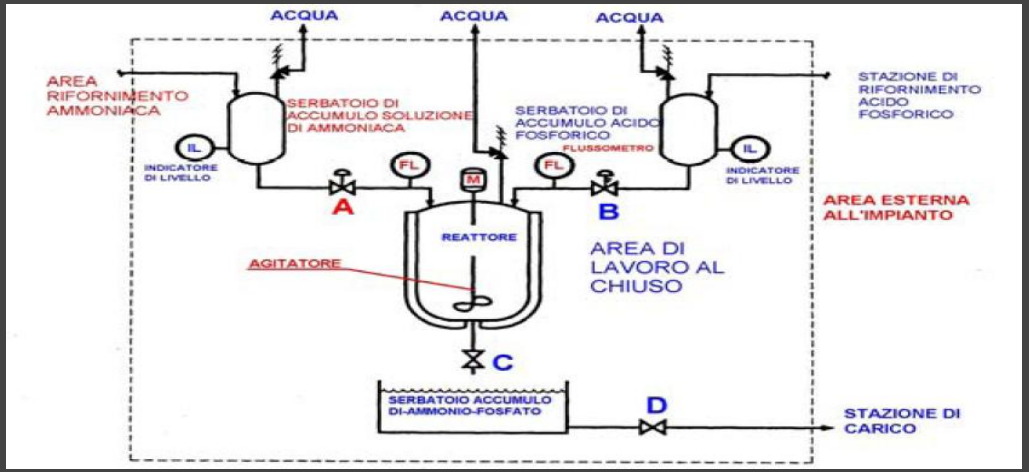
È possibile passare all'analisi del secondo nodo, costituito dalla linea di alimentazione dell'aria, illustrata in figura:



Nodo 2 del processo "Forno di preriscaldamento".

ancora un esempio applicativo

Impianto di Processo Continuo: Produzione di Di-Ammonio-Fosfato (DAF).



Nell'impianto si effettua la miscelazione di soluzione di Ammoniaca e di soluzione di Acido Fosforico

- Eccesso di acido fosforico: reazione sicura.
- Il DAF non è un prodotto tossico – nocivo

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop
Hazard & Operability Analysis

Sezione di processo: Alimentazione di acido fosforico al reattore DAF
Obiettivo Progettuale: Alimentare acido fosforico al reattore DAF ad un opportuno tasso
Parola Guida: NO
Parametro di Processo: FLUSSO
Deviazione: NO-FLUSSO

Conseguenze:
1. Eccesso di ammoniaca nel reattore
2. Ammoniaca non reagita nel serbatoio di accumulo
3. Rilascio di ammoniaca non reagita dal serbatoio di accumulo nell'area di lavoro
4. Mancata produzione del reattore

Cause
- Mancato rifornimento di reagente nel serbatoio di acido fosforico
- Indicatore/controllore di flusso guasto
- Controllore di flusso mal regolato dall'operatore
- Valvola di controllo, B, dell'acido fosforico chiusa
- Intasamento della linea
- Perdita o rottura della linea

Azioni:
- Valutare la possibilità di includere dispositivi di allarme/arresto del sistema in caso di flussi ridotti di acido fosforico nel reattore
- Assicurarsi che gli intervalli di manutenzione e verifica della valvola B siano adeguati
- Considerare la possibilità di utilizzare un serbatoio chiuso per l'accumulo del DAF

Prof. Claudio Pantanali, PhD cpantanali@units.it

HaZop
Hazard & Operability Analysis

Team:			Numero di report: 1		
Data Meeting: 8 Aprile 2002			Numero di revisione: 1		
Item N.	**Deviazione**	**Causa**	**Conseguenza**	**Mis. di Sicur.**	**Azione**
1.0 Serbatoio di accumulo di ammoniaca. Stoccaggio in condizioni di sicurezza a pressione e temperatura ambiente.					
1.1	Elevato Livello	Mancato scarico di ammoniaca dal serbatoio.	Potenziale rilascio di ammoniaca in atmosfera.	Indicatore di livello sul serbatoio.	Revisione del processo di alimentazione di ammoniaca per assicurare volume sufficiente.
		Malfunz. indicatore di livello.		Valvola di sic. per scarico in atmosfera.	Inviare lo scarico di sicurezza in un depuratore (scrubber).
					Inserire un allarme di livello indipendente per il serbatoio.

Item N.	**Deviazione**	**Causa**	**Conseguenza**	**Mis. di Sicur.**	**Azione**
3.0 Serbatoio di accumulo della soluzione acida. Contenimento soluzione a condizioni di temperatura e pressione ambiente.					
3.7	Bassa concentraz. di acido fosforico	Bassa concentraz. dell'acido da fornitore.	Presenza di ammoniaca non reagita nel reattore e conseguente invio nel serbatoio di accumulo con possibilità di rilascio nell'area di lavoro.	Procedura di controllo delle fasi di scarico e trasferimento dell'acido.	Procedure di scarico opportune e sistema di identificazione (labelling)
		Errore nella procedura di carico del serbatoio.		Sensore di presenza di ammoniaca e sistema di allarme.	Verificare la concentrazione di acido fosf. prima del processo.
					Assicurare l'adeguata ventilazione dei locali.

Prof. Claudio Pantanali, PhD cpantanali@units.it

SINTESI

Obiettivi: identificazione sistematica delle cause e delle conseguenze dovute a possibili deviazioni del funzionamento dai valori di progetto. Definizione delle azioni da intraprendere per l'evidenziazione ed il contenimento delle conseguenze.

Metodologia: analisi sistematica di specifici punti dell'impianto (componenti o procedure operative). Per ciascuno si considerano le possibili deviazioni dai valori di progetto.

Pro: affidabilità, qualità e completezza. È la tecnica più completa.
Capacità di individuare anche sorgenti di rischio legate a sequenze di eventi. Output chiaro e completo.

Contro: composizione eterogenea del team con conoscenze relative a: progettazione, processo, materiali, chimica, tossicologia. Risorse umane. Tempi e costi elevati.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA
Event Tree Analysis

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

- **E' un processo induttivo nel quale lo studio ha inizio con un evento iniziale e prosegue con la definizione delle possibili conseguenze dell'evento fino ai potenziali incidenti considerando sia il funzionamento corretto sia quello errato delle diverse funzioni di sicurezza coinvolte.**

- **Valuta la potenzialità di un incidente risultante da un guasto o da una rottura di tipo generale degli impianti di processo.**

- **L'Albero degli Eventi parte dalla causa iniziale di un eventuale incidente e procede fino a determinarne tutte le possibili conseguenze finali:**
  - **ripristino delle condizioni di funzionamento degli impianti**
  - **interruzione del funzionamento degli impianti**
  - **guasto degli impianti ed eventuali disastri…**

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

L'**Event Tree Analysis (ETA)**, o **analisi dell'albero degli eventi**, è una tecnica di analisi del rischio utilizzata per valutare le possibili conseguenze di eventi iniziali, specialmente nei contesti di sicurezza e gestione delle emergenze. L'ETA si concentra sugli eventi potenziali a partire da un singolo evento iniziale e cerca di comprendere le diverse sequenze di eventi che potrebbero portare a diversi risultati, alcuni dei quali potrebbero essere indesiderati o disastrosi.

L'Event Tree Analysis è uno strumento grafico e analitico che permette di rappresentare i diversi percorsi che possono essere intrapresi a partire da un singolo **evento iniziale**, denominato anche "evento scatenante". Attraverso una serie di **biforcazioni** (o diramazioni), l'analisi mostra la serie di azioni o mancate azioni che possono portare a risultati finali differenti.

Questo approccio è particolarmente utile in sistemi complessi dove un evento può avere diverse possibili reazioni o dove l'efficacia dei dispositivi di sicurezza deve essere verificata. L'ETA è ampiamente utilizzato in settori come l'industria nucleare, petrolifera, chimica e l'aviazione, dove la sicurezza è una priorità assoluta e gli scenari di rischio sono numerosi e interconnessi.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

PRINCIPALI CARATTERISTICHE

- Costruisce le possibili evoluzioni di una condizione potenzialmente pericolosa
- Individua un percorso evolutivo per ogni fase considerata

Vantaggi

- Evidenzia lo sviluppo cronologico degli incidenti in base alle risposte dei dispositivi di sicurezza
- Consente di individuare le scelte critiche che influenzano maggiormente l'evento iniziatore

Svantaggi:

- Nel caso di cause comuni di guasto o di sviluppi contemporanei, presenta difficoltà di elaborazione
- La valutazione di alcune opzioni può essere fortemente soggettiva

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

CARATTERISTICHE

Partendo da una condizione potenzialmente pericolosa o da un incidente particolarmente complesso, generati da una deficienza del sistema o da errore umano, ne costruisce, per metodo induttivo, le possibili evoluzioni in forma dicotomica, assegnando ad ogni scelta una determinata probabilità di accadimento. In questo modo si ottiene un duplice percorso evolutivo per ogni fase da considerare e il risultato è un certo numero di scenari incidentali proporzionale, geometricamente, alla quantità di proposizioni inserite.

VANTAGGI

Riuscendo ad evidenziare lo "sviluppo cronologico" degli incidenti susseguenti un evento iniziale, in base a risposte positive o fallimentari dei dispositivi di sicurezza, si capisce come questo tipo di analisi sia utile ai fini dell'identificazione delle scelte critiche che più contribuiscono allo sviluppo negativo dell'evento iniziatore o, al contrario, ad una sua attenuazione (per es., nuovi interventi).

SVANTAGGI

Nel caso di sviluppi paralleli e contemporanei o cause comuni di guasto, si possono presentare difficoltà di elaborazione. La valutazione quantitativa di alcune opzioni rischia di essere molto soggettiva. L'incertezza dei risultati ottenuti dipende dalla stessa incertezza presente in ogni singola possibilità introdotta e quindi aumenta ampliando il loro numero.

APPLICAZIONE

E' limitata ed è auspicabile non adottare un numero troppo alto di opzioni per non complicare eccessivamente l'albero, se però si tratta di "cause comuni di guasto", allora devono essere considerate attentamente.

COMMENTI

Può essere utilizzata anche come sistema diagnostico e decisionale. Questa analisi può essere eseguita da un analista, preferibilmente da un gruppo di 2-4 persone. Un'unità di processo di piccole dimensioni può richiedere pochi giorni, mentre sono necessarie molte settimane per quelle più grandi e complesse.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

Come funziona l'ETA?

Il processo di analisi dell'albero degli eventi può essere suddiviso in alcuni passaggi fondamentali:

1.Definizione dell'Evento Iniziale:

1. L'analisi parte da un **evento iniziale**, che può essere un guasto o un evento inaspettato, ad esempio il guasto di un componente o la perdita di pressione in un impianto.

2.Identificazione delle Funzioni di Sicurezza:

1. Si identificano tutte le funzioni o le misure di sicurezza che possono intervenire per mitigare l'evento iniziale, come sistemi di protezione, barriere di sicurezza o azioni correttive umane.

3.Creazione dell'Albero degli Eventi:

1. A partire dall'evento iniziale, si costruisce un **diagramma ad albero**. Ad ogni punto in cui una misura di sicurezza può intervenire, si creano due possibili rami:
    1. **Successo** della misura di sicurezza.
    2. **Fallimento** della misura di sicurezza.
2. Ogni diramazione porta a ulteriori sviluppi, creando così un percorso completo che descrive tutte le possibili sequenze di eventi.

4.Determinazione delle Probabilità:

1. Ogni ramo dell'albero viene associato a una **probabilità di successo o fallimento**, spesso basata su dati storici, analisi ingegneristiche o stime probabilistiche.
2. Calcolare le probabilità totali di ogni possibile esito aiuta a quantificare il rischio associato all'evento iniziale.

5.Valutazione dei Risultati Finali:

1. Le diverse combinazioni di successo o fallimento delle misure di sicurezza portano a vari **esiti finali**, ciascuno con una propria probabilità e con conseguenze diverse (danno alla sicurezza, perdita economica, impatti ambientali, ecc.).
2. Ogni esito viene quindi classificato e valutato in termini di gravità e frequenza per fornire una visione del rischio totale associato all'evento iniziale.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

Esempio di ETA

Immagina un evento iniziale come una **perdita di gas in un impianto chimico**. L'albero degli eventi potrebbe seguire il seguente percorso:

1.Rilevazione del gas:

1. Successo: il sistema rileva correttamente la perdita di gas.
2. Fallimento: il sistema non rileva la perdita.

2.Attivazione del Sistema di Ventilazione:

1. Se il gas viene rilevato, potrebbe esserci il successo o il fallimento del sistema di ventilazione per disperdere il gas.

3.Allarme e Evacuazione:

1. Se il sistema di ventilazione funziona o fallisce, si può avere un allarme che avvia la procedura di evacuazione.

Ogni uno di questi passaggi è rappresentato da una biforcazione dell'albero, e il risultato finale può variare da una mitigazione totale dell'incidente a un'esplosione potenzialmente devastante.

Vantaggi dell'ETA

1.Analisi di scenari complessi: L'ETA è utile per esaminare i vari scenari di un evento, specialmente quando le conseguenze sono incerte.
2.Valutazione del livello di sicurezza: Permette di valutare l'efficacia delle misure di sicurezza, identificando punti deboli o componenti critici del sistema.
3.Supporto per decisioni preventive: Fornisce informazioni importanti per migliorare i sistemi di sicurezza, riducendo la probabilità di eventi disastrosi.

Limiti dell'ETA

1.Richiede Dati Affidabili: L'accuratezza dell'analisi dipende fortemente dalla disponibilità e dalla qualità dei dati probabilistici sui guasti.
2.Semplicità delle Assunzioni: L'ETA assume spesso che i diversi eventi siano indipendenti tra loro, il che potrebbe non essere sempre vero in sistemi complessi e interconnessi.
3.Difficoltà di Modellazione di Sistemi Complessi: In un sistema molto grande, l'albero può diventare estremamente complesso e difficile da gestire, specialmente se ci sono molteplici eventi dipendenti.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Event Tree Analysis: Perdita di Gas in un Impianto Chimico

1. Evento Iniziale: Perdita di Gas
   - ├── Sistema di Rilevazione del Gas Funziona?
     - ├── Sì
       - ├── Sistema di Ventilazione Funziona?
         - ├── Sì: Gas Disperso → Incidente Evitato
         - └── No
           - ├── Allarme e Evacuazione Funzionano?
             - ├── Sì: Evacuazione Riuscita → Nessuna Vittima
             - └── No: Evacuazione Fallita → Esplosione con Vittime
       - └── No
         - ├── Allarme e Evacuazione Funzionano?
           - ├── Sì: Evacuazione Riuscita → Nessuna Vittima
           - └── No: Evacuazione Fallita → Esplosione con Vittime
     - └── No
     - ├── Nessuna Azione Intrapresa → Esplosione con Gravi Conseguenze

Esempio del rilascio di gas in un impianto chimico.

Immaginiamo questo schema come un diagramma ad albero che si espande dall'evento iniziale verso più risultati possibili, a seconda di come le diverse misure di sicurezza rispondono.

Descrizione dei Passaggi

1.Evento Iniziale: Rilascio di Gas in Impianto Chimico:

1. Questo è l'evento scatenante che può portare a diversi scenari.

2.Sistema di Rilevazione del Gas:

1. **Successo**: Il gas viene rilevato correttamente.
   1. Si passa alla successiva funzione di sicurezza (sistema di ventilazione).
2. **Fallimento**: Il gas non viene rilevato.
   1. Non viene intrapresa alcuna azione, con un potenziale rischio di esplosione e gravi conseguenze.

3.Sistema di Ventilazione Attivato (nel caso in cui il gas sia stato rilevato):

1. **Successo**: Il sistema di ventilazione si attiva correttamente e disperde il gas.
   1. **Risultato**: L'incidente viene evitato.
2. **Fallimento**: Il sistema di ventilazione non si attiva.
   1. Si passa alla valutazione dell'allarme e dell'evacuazione.

4.Allarme e Evacuazione (nel caso in cui la ventilazione fallisca):

1. **Successo**: Le persone nell'impianto sono evacuate correttamente.
   1. **Risultato**: Nessuna vittima, l'incidente è sotto controllo.
2. **Fallimento**: L'evacuazione fallisce.
   1. **Risultato**: Esplosione potenziale con conseguenze per le persone.

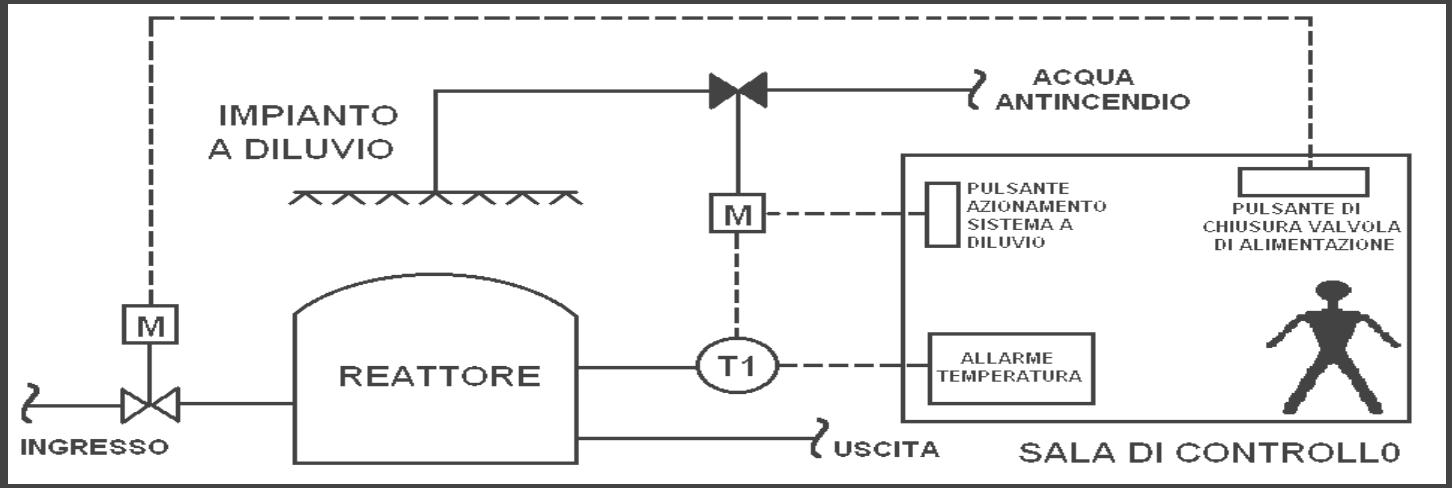
Conclusioni

- **Successo a Ogni Livello**: Se tutte le misure di sicurezza hanno successo, l'incidente viene evitato senza conseguenze.
- **Fallimenti in Serie**: Se ci sono fallimenti consecutivi nelle misure di sicurezza, l'esito finale può essere disastroso, con potenziali esplosioni e vittime.
- **Importanza delle Misure di Sicurezza**: L'analisi evidenzia come ogni funzione di sicurezza, dal rilevamento all'evacuazione, sia critica per la gestione efficace dell'evento.

Questo tipo di schema può essere facilmente tradotto in un diagramma visivo dove ogni nodo rappresenta una biforcazione con due rami (successo o fallimento), rendendo visibili tutte le possibili conseguenze di un evento iniziale.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ALTRO ESEMPIO

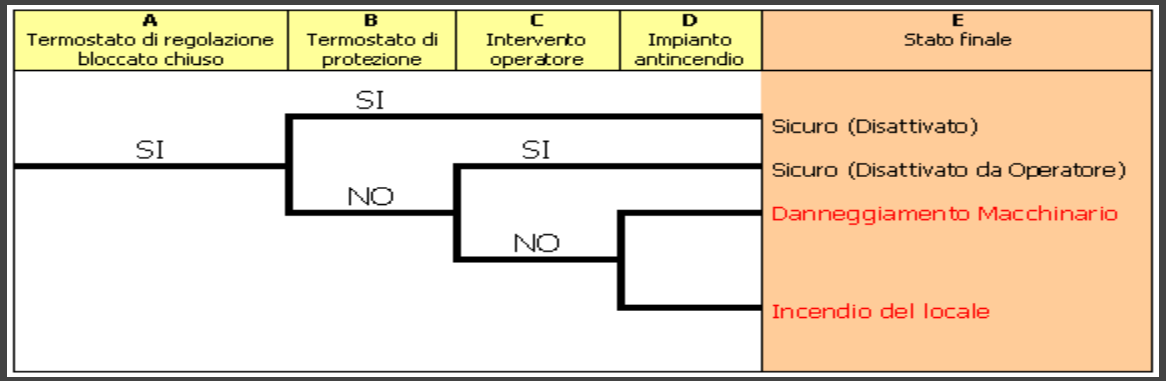


Si sviluppa l'albero degli eventi relativo alla **perdita di acqua di raffreddamento** individuata come causa di possibile danneggiamento del reattore nel caso considerato per la costruzione dell'albero dei guasti.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

Ogni ramo rappresenta una singola ed unica sequenza di incidente cioè un set di relazioni che correlano le varie funzioni di sicurezza.



1. La descrizione delle diverse sequenze evolutive dell'evento iniziale consente di definire una scala di priorità per i diversi incidenti basata sull'efficacia delle procedure adottate.
2. E' possibile identificare e valutare gli eventi contraddistinti da maggior rischio per adottare misure di intervento ottimali (p.e. procedure operative di intervento e/o da diverse configurazioni dei sistemi di sicurezza).

Ogni ramo finale è individuato da una combinazione unica di eventi successivi che determinano lo stato finale (condizioni di sicurezza o di pericolo).

Prof. Claudio Pantanali, PhD cpantanali@units.it

CARATTERISTICHE DEL SISTEMA

Le **funzioni di sicurezza** adottate per intervenire in corrispondenza dell'evento principale sono:

1. avvertimento dell'operatore mediante allarme di temperatura tarato sul valore **T1**;
2. ristabilimento del flusso di acqua di raffreddamento del reattore di ossidazione;
3. arresto automatico del sistema in corrispondenza della temperatura **T2** (T2 >T1).

L'ordine con cui sono riportate costituisce anche la sequenza con la quale le funzioni di sicurezza sono chiamate ad intervenire.

Il sistema d'allarme ed il sistema di arresto automatico dispongono di sensori di temperatura diversi. L'allarme di temperatura è l'unico ad avvisare l'operatore dell'anomalia di funzionamento del reattore.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

COSTRUZIONE DELL'ALBERO

1. La prima funzione di sicurezza consiste nell'**allarme di temperatura eccessiva**. Tale funzione interviene avvisando l'operatore, nel caso il sistema d'allarme funzioni correttamente. Pertanto, un punto di divisione (P1) (**branch point**) è necessario per definire l'efficacia di intervento di tale funzione di sicurezza.
2. La seconda funzione di sicurezza consiste **nell'intervento dell'operatore**.
3. Nel caso di mancato funzionamento del sistema d'allarme, la reazione dell'operatore deve essere esclusa. Il ramo inferiore dell'albero degli eventi, inoltre non presenta punto di divisione sul ramo superiore conseguente al corretto funzionamento del sistema d'allarme ed all'ulteriore corretto intervento dell'operatore.
4. La terza funzione di sicurezza, **l'intervento del sistema di arresto automatico.**

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

Un **branch point** (o **punto di biforcazione**) è un termine usato principalmente nell'analisi del rischio e nella modellazione di sistemi complessi, come nelle tecniche di analisi come l'**Event Tree Analysis (ETA)**. È un punto chiave in un diagramma ad albero in cui un evento può svilupparsi in **diverse direzioni** in base al successo o al fallimento di un particolare sistema o processo. Questi punti rappresentano le decisioni o le reazioni a un evento iniziale e descrivono tutte le possibili sequenze di eventi che ne derivano.

Definizione di Branch Point

In modo specifico, un **branch point** è un nodo in cui si verificano diverse **possibili alternative**. Ogni alternativa rappresenta un possibile sviluppo o un esito a seguito di un evento iniziale. Questi sviluppi dipendono dalle condizioni e dalle risposte del sistema o dalle misure di sicurezza. Ogni alternativa si espande in un nuovo ramo che porta a un nuovo insieme di eventi o di risultati finali.

Nella rappresentazione dell'**Event Tree Analysis**, il branch point è il luogo in cui l'**albero degli eventi** si biforca in due (o più) possibili risultati:

- **Successo**: Il sistema o la misura di sicurezza funziona correttamente.
- **Fallimento**: Il sistema o la misura di sicurezza non funziona.

Queste biforcazioni descrivono come il sistema potrebbe reagire a un evento, rappresentando una scelta tra diversi percorsi di sviluppo.

Esempio di Branch Point

Immaginiamo il caso di una perdita di gas in un impianto chimico. In questo scenario, un **branch point** potrebbe essere il funzionamento del **sistema di rilevazione del gas**. Questo è il punto in cui l'evento iniziale (la perdita di gas) può svilupparsi in due modi diversi:

1.Successo del Sistema di Rilevazione del Gas:

1. Il sistema rileva correttamente la perdita di gas.
2. Si attivano le successive misure di sicurezza (ad esempio, ventilazione e allarme).

2.Fallimento del Sistema di Rilevazione del Gas:

1. Il sistema non rileva il gas.
2. Nessuna azione viene intrapresa, e il gas rimane disperso, aumentando il rischio di esplosione.

In questo esempio, il **branch point** è il momento in cui si determina se il sistema di rilevamento riesce a rilevare il gas o meno. Da questo punto di biforcazione partono due possibili ramificazioni, ognuna delle quali rappresenta un possibile sviluppo della situazione con conseguenze molto diverse.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Un **branch point** (o **punto di biforcazione**) è un termine usato principalmente nell'analisi del rischio e nella modellazione di sistemi complessi, come nelle tecniche di analisi come l'**Event Tree Analysis (ETA)**. È un punto **Importanza dei Branch Point**

I **branch point** sono fondamentali nelle analisi di rischio e sicurezza per diversi motivi:

1.Visualizzazione degli Scenari:

1. I branch point aiutano a visualizzare tutte le **possibili sequenze di eventi** a partire da un singolo evento iniziale. Questo consente di identificare tutte le possibili combinazioni di successo e fallimento dei sistemi coinvolti.

2.Analisi delle Misure di Sicurezza:

1. I branch point mostrano come le diverse misure di sicurezza intervengono in risposta a un evento iniziale e valutano quanto efficacemente riescano a prevenire un esito indesiderato.

3.Quantificazione del Rischio:

1. Assegnando delle probabilità di successo o fallimento a ciascun branch point, è possibile quantificare il rischio complessivo associato a ciascun percorso, contribuendo alla definizione delle priorità nelle strategie di mitigazione.

4.Identificazione dei Punti Critici:

1. I branch point permettono di identificare i **punti critici** all'interno del sistema, ovvero i punti in cui un singolo fallimento potrebbe portare a conseguenze disastrose. Questi punti diventano il focus di interventi preventivi per ridurre il rischio.

Diagramma di un Branch Point nell'Albero degli Eventi

In un **diagramma ad albero degli eventi**, il branch point viene rappresentato come un nodo che si **biforca** in due o più direzioni, a seconda delle possibili alternative di successo o fallimento. Ogni nodo ha dei rami che rappresentano le opzioni disponibili:

•Una linea orizzontale che si dirama verso destra con diverse **biforcazioni** indica le possibili azioni o le risposte a un evento.

•Ogni ramo porta a ulteriori punti di decisione o a esiti finali.

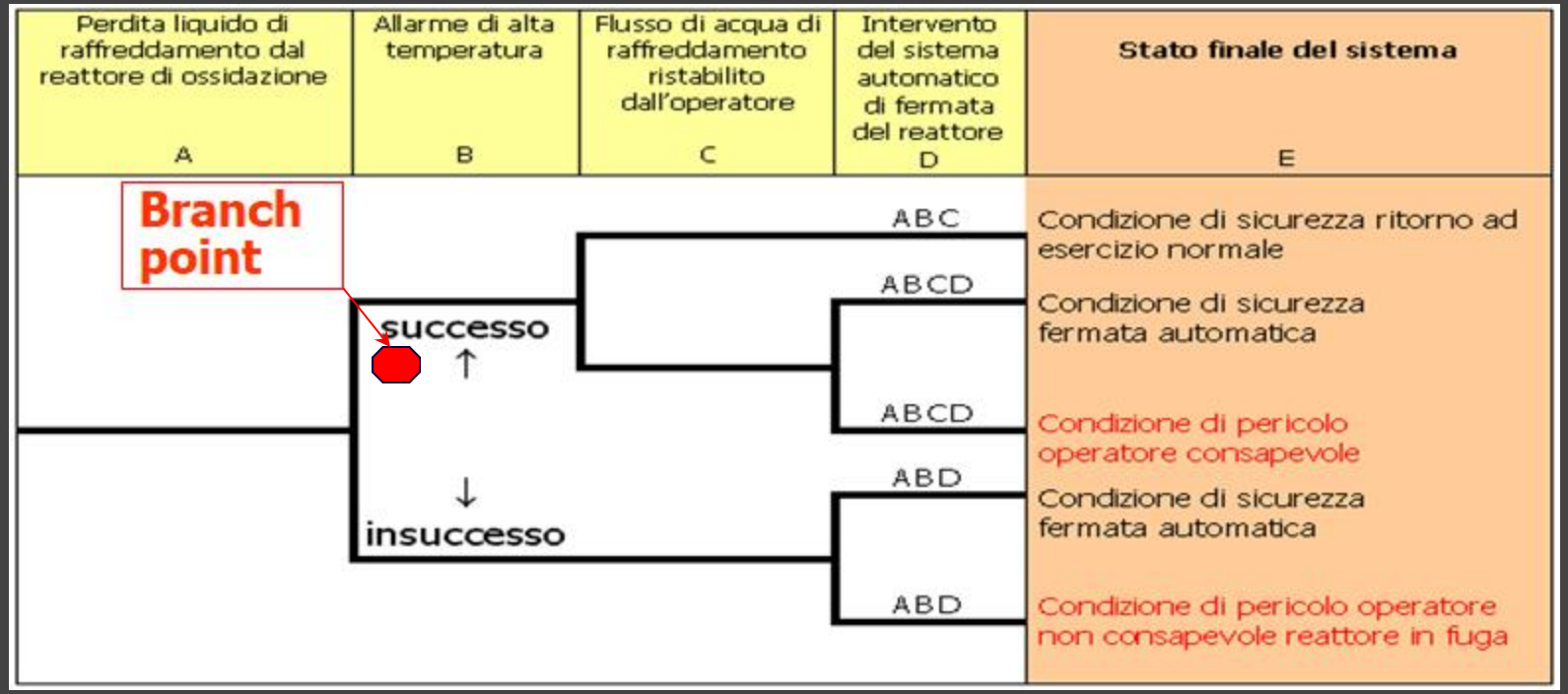
Conclusione

Il **branch point** è un concetto centrale nelle tecniche di analisi del rischio come l'Event Tree Analysis, poiché rappresenta i punti cruciali dove si determinano i possibili sviluppi di un evento iniziale. Aiuta a modellare la risposta del sistema e ad analizzare l'efficacia delle misure di sicurezza adottate. Comprendere e rappresentare adeguatamente i branch point permette ai progettisti e ai gestori del rischio di valutare meglio la resilienza del sistema, di identificare i punti deboli e di adottare le misure necessarie per migliorare la sicurezza.

Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA (Event Tree Analysis)

RISULTATO FINALE



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ETA vs. FTA

L'**Event Tree Analysis** è spesso confrontata con l'**FTA (Fault Tree Analysis)**. Mentre l'ETA parte da un evento iniziale e analizza le possibili conseguenze, l'FTA parte da un **evento indesiderato** e cerca di identificare le **cause** che potrebbero portare a quell'evento. Quindi, l'ETA è un approccio "dal basso verso l'alto" (bottom-up), mentre l'FTA è "dall'alto verso il basso" (top-down).

Applicazioni

L'ETA è utilizzata in vari settori, tra cui:

- **Industria nucleare**: per valutare gli scenari di emergenza in caso di guasti ai reattori.
- **Settore petrolchimico**: per analizzare le conseguenze di perdite di gas o di altri materiali pericolosi.
- **Aviazione**: per esaminare le risposte alle situazioni di emergenza, come guasti a sistemi critici.
- **Sistemi di trasporto**: per valutare l'efficacia delle misure di sicurezza in caso di incidenti stradali o ferroviari.

Conclusione

L'**Event Tree Analysis** è un potente strumento di valutazione del rischio che permette di esplorare sistematicamente le conseguenze degli eventi indesiderati e di identificare percorsi critici in cui le misure di sicurezza possono essere migliorate. Fornendo una visione dettagliata delle diverse sequenze di eventi, l'ETA consente ai gestori della sicurezza di implementare strategie di mitigazione più efficaci, migliorando la resilienza dei sistemi complessi e minimizzando i rischi per persone, ambiente e infrastrutture.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA
(Fault Tree Analysis)

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

GENERALITA‘

Oltre alla metodologia FMEA uno dei metodi più diffusi e conosciuti per l'analisi del rischio, è il **Fault Tree Analysis** (FTA) o ***albero dei guasti***. Diversamente dall'FMEA tuttavia, l'FTA va annoverato tra i metodi di analisi di tipo **deduttivo** in quanto, partendo da un'analisi generale e complessiva del tipo di guasto (o evento indesiderato sul sistema), arriva ad individuare i guasti sui componenti.

Al contrario l' FMEA **partendo dal particolare** ovvero dai guasti sui singoli componenti, giunge all'individuazione del guasto **sul sistema**.

Tutti i metodi sul controllo dei processi come l' FTA nascono intorno agli anni '60 presso i laboratori Bell Telephone sostenuto dalla teoria dell’affidabilità ed, in particolare, dall’algebra booleana. Dagli anni ’60 in poi FTA ha trovato sempre più occasioni di applicazione, nel mondo manifatturiero come anche più di recente in quello dei servizi, risultando oggi uno dei metodi più semplici ed efficaci nell’analisi dell’affidabilità e sicurezza dei sistemi.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

SINTETICAMENTE

Obbiettivi: costruzione delle possibili evoluzioni di una condizione potenzialmente pericolosa; identificazione di un percorso evolutivo per ogni fase considerata.

Metodologia: approccio ordinato e sistematico che consente di valutare correttamente i molti fattori che potrebbero influenzare il corso dei potenziali incidenti.

Pro: capacità di rilevare lo sviluppo cronologico degli incidenti susseguenti un evento iniziale, in base alle risposte dei dispositivi di sicurezza; capacità di identificazione delle scelte critiche che incidono sullo sviluppo dell'evento iniziatore.

Contro: difficoltà di elaborazione nel caso di sviluppi paralleli e contemporanei o cause comuni di guasto; soggettività nella valutazione di alcune opzioni

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

La FTA permette, in modo grafico e logico, di collegare fra loro i guasti dei componenti di un sistema. Lo scopo principale, al contrario della FMEA, non è però quello di individuare le cause dei guasti bensì, partendo da un guasto sul sistema (Evento indesiderato), di metterlo in relazione funzionale con i guasti sui componenti (Eventi base).
Prima di affrontare nel dettaglio la tecnica, possono risultare utili alcune definizioni, che torneranno utili nel seguito.
Evento indesiderato o evento top (TOP EVENT)
Rappresenta il guasto relativo al sistema funzionale sotto esame. L'evento top indesiderato può essere combinazione di numerose cause. Esso avrà, cioè, un numero n di eventi (nodi del sistema) che lo precedono e lo determinano ma nessun evento che lo succede.

Combinazione di cause: è il presentarsi simultaneo di guasti degli elementi funzionali che portano all'evento top indesiderato. La più piccola combinazione di guasti ne contiene almeno un numero necessario a causare l'evento top.
Unità esaminata: l'oggetto da esaminare, identificato dalle sue caratteristiche funzionali e costruttive. Unità esaminate possono ad esempio essere sistemi, componenti ed elementi funzionali.
Componente: è l'unità esaminata di livello più basso alla quale può essere assegnato uno o più elementi funzionali.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

CARATTERISTICHE

L'FTA parte da un evento incidentale procedendo per metodo deduttivo alla stesura di una sequenza logica di cause iniziali e intermedie che ne determinano, singolarmente o per interconnessione, la possibilità di accadimento. Il grafico che ne risulta è una rappresentazione ad "albero" composto da vari livelli alla fine di ciascuno dei quali gli eventi intermedi si trasformano a loro volta in cause iniziali con una loro probabilità di accadimento. La frequenza dell'evento principale dipende da quella dei vari insiemi. Minore è il numero degli eventi intermedi, maggiore è la probabilità di verificarsi dell'evento finale.

VANTAGGI

Analizza l'evento principale studiando le possibili combinazioni degli eventi intermedi individuando i punti "a rischio" che più contribuiscono al verificarsi dell'incidente e quindi anche le misure preventive più idonee per ridurne la probabilità.
E' una tecnica molto utile per lo studio degli errori umani e delle "cause" comuni di guasto.

SVANTAGGI

Se applicato dettagliatamente può essere molto oneroso perciò, è consigliabile effettuarne l'applicazione agli eventi più rappresentativi.

APPLICAZIONE

Limitata. L'analista addetto deve consultarsi frequentemente con tecnici e operatori.

COMMENTI

Il risultato, di tipo qualitativo, ma potenzialmente anche quantitativo, è un'elencazione degli scenari dei fallimenti dell'apparecchiatura e/o dell'operatore relativa ad un determinato evento.
Il tempo necessario a questo tipo di analisi può essere di un giorno, se si tratta di una piccola unità di processo, o di più settimane se l'apparecchiatura è grande e complessa.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

L'analisi degli alberi di guasto o **FTA**(*Fault Tree Analysis*) è stata introdotta per la prima volta nel **1962** nei Bell Telephone Laboratories in relazione allo studio della sicurezza del sistema di controllo del missile Minuteman; negli anni successivi questo metodo è stato sviluppato dalla Boeing Company ed è stato utilizzato sempre più diffusamente nell'industria aerospaziale e nucleare e in generale per lo studio di sistemi complessi di grosse dimensioni, cosi come di recente anche dalle Banche.

Essa è particolarmente adatta per l'analisi di *sistemi altamente ridondanti*, mentre per sistemi particolarmente *vulnerabili a singoli guasti* che possono provocare un incidente è meglio utilizzare tecniche di tipo diverso come **FMEA** (*Failure Modes and Effects Analysis*) o **HAZOP**(*Hazard and Operability Analysis*).

Questo metodo può essere applicato:

sia durante la fase di progettazione di un nuovo impianto(o sistema),
sia in fase di verifica di un impianto(o sistema).

Lo scopo è quello di migliorare la *sicurezza del sistema* poiché permette di individuare importanti caratteristiche come:

- *i punti deboli del sistema;*
- *false ridondanze;*
- *o gli effetti di un dato componente sull'affidabilità complessiva.*

Il metodo FT ci permette anche di poter:

1. effettuare delle *predizioni*: studiando gli stati delle componenti di un sistema arrivando ad ottenere informazioni sullo stato dell'intero sistema(in questo ambito rientra lo studio dell'*Affidabilità*);
2. effettuare un'*analisi diagnostica*: partendo da un analisi *"generale"* e complessiva dello stato dell'intero sistema, arrivando ad individuarne gli stati sui suoi componenti.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

L'**FTA (Fault Tree Analysis)**, o **analisi dell'albero dei guasti**, è una tecnica strutturata per identificare e analizzare le possibili cause di un evento indesiderato (come un incidente o un guasto di sistema). Questa tecnica è particolarmente utilizzata per comprendere come e perché si verificano eventi critici, attraverso la scomposizione di tali eventi in singoli guasti di componenti o errori umani. È una delle principali metodologie di analisi del rischio nei contesti di sicurezza industriale, progettazione di sistemi critici, e nei settori dell'aviazione, dell'energia nucleare, chimica, e altri settori ad alto rischio.

L'FTA è un metodo **top-down** per analizzare e capire i **meccanismi di guasto** che portano a un evento critico, chiamato anche **evento indesiderato** o **Top Event**. L'obiettivo principale dell'analisi FTA è quello di individuare tutte le possibili cause che possono portare al verificarsi dell'evento indesiderato e fornire informazioni che possono essere utilizzate per ridurre la probabilità del guasto.

Concetti Chiave dell'FTA

1.Evento Iniziale (Top Event):

- L'analisi FTA parte dalla definizione di un **evento indesiderato** che si vuole prevenire, come il guasto di un sistema critico o un incidente grave.

2.Evento Intermedio:

- Gli eventi intermedi sono una combinazione di eventi di base o altri eventi intermedi che contribuiscono al verificarsi del Top Event. Gli eventi intermedi descrivono come si combinano vari guasti per portare al guasto principale.

3.Eventi di Base:

- Gli eventi di base sono le cause fondamentali di un guasto, che non possono essere ulteriormente scomposte. Possono essere componenti che si rompono, errori umani o condizioni esterne sfavorevoli.

4.Porte Logiche (Gate):

- Per costruire un albero dei guasti, si utilizzano delle **porte logiche** per rappresentare il modo in cui diversi guasti contribuiscono al Top Event:
  1. **AND Gate**: indica che l'evento critico si verifica solo se **tutti gli eventi** a monte si verificano contemporaneamente.
  2. **OR Gate**: indica che l'evento critico si verifica se **almeno uno** degli eventi a monte si verifica.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Come si Costruisce un Fault Tree?

Il processo per costruire un **Fault Tree** parte dalla definizione del Top Event e poi "discende" in modo iterativo per scomporre le cause. Ecco i passaggi fondamentali per sviluppare un'analisi dell'albero dei guasti:

1.Definizione dell'Evento Indesiderato (Top Event):

- Si identifica l'evento di guasto o la condizione indesiderata che si vuole analizzare. Ad esempio, il guasto di un sistema di raffreddamento in una centrale nucleare.

2.Identificazione degli Eventi Intermedi:

- Si scompone il Top Event in **eventi intermedi**, cercando di capire quali fattori potrebbero contribuire al guasto finale. Ad esempio, il guasto di una pompa o la perdita di alimentazione elettrica.

3.Identificazione degli Eventi di Base:

- Ogni evento intermedio viene ulteriormente scomposto per individuare le cause fondamentali (eventi di base). Queste possono includere errori di componenti, errori operativi, o fattori ambientali.

4.Utilizzo delle Porte Logiche:

- Si utilizzano **porte logiche AND e OR** per collegare gli eventi intermedi e di base e rappresentare le relazioni tra loro. Le porte AND indicano che tutte le cause devono essere presenti affinché si verifichi l'evento a valle, mentre le porte OR indicano che basta una sola delle cause.

5.Analisi del Fault Tree:

- Una volta costruito l'albero, si procede con l'**analisi del rischio**, che può includere il calcolo delle probabilità di guasto per determinare la probabilità complessiva che si verifichi l'evento indesiderato.

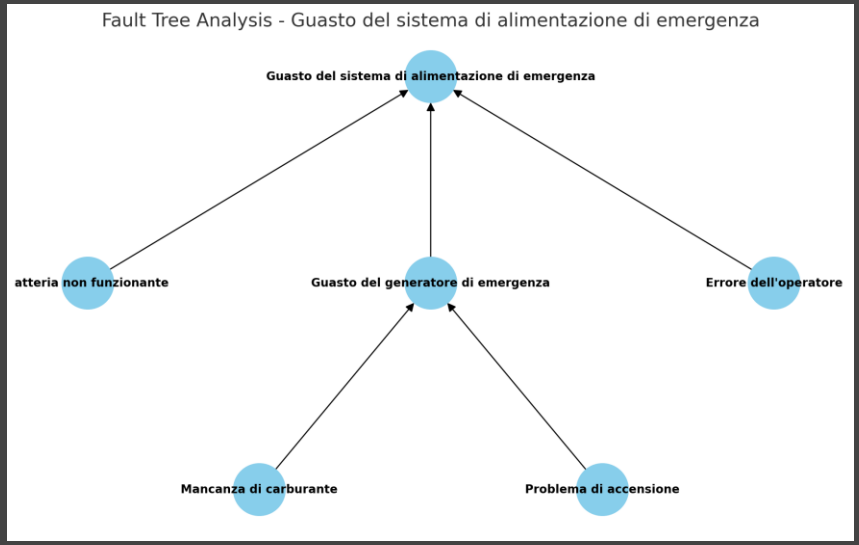
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempio di Fault Tree Analysis

Supponiamo di voler analizzare il **guasto di un sistema di alimentazione elettrica** di emergenza.

- **Top Event**: Guasto del sistema di alimentazione elettrica di emergenza.
  - **OR Gate**: Il guasto può derivare da una di queste cause:
    - **Batteria non Funzionante** (Evento di base)
    - **Guasto Generatore di Emergenza** (Evento di base)
    - **Errore dell'Operatore** (Evento di base)

  - Se approfondiamo il guasto del generatore di emergenza:
    - **AND Gate**: Il generatore può fallire se si verificano entrambe queste condizioni:
      - **Mancanza di Carburante** (Evento di base)
      - **Problema di Accensione** (Evento di base)



Analisi delle Probabilità

Dopo aver costruito l'albero dei guasti, una delle parti più importanti è la determinazione delle **probabilità** di ciascun evento. Questo viene spesso fatto tramite l'utilizzo di **dati storici**, stime ingegneristiche e dati di affidabilità. Le probabilità degli eventi di base vengono combinate utilizzando le porte logiche per determinare la probabilità complessiva del Top Event.

- Per le **porte AND**, la probabilità dell'evento è il **prodotto** delle probabilità dei singoli eventi.
- Per le **porte OR**, la probabilità dell'evento è calcolata come la **somma** delle probabilità meno la probabilità congiunta (per evitare il doppio conteggio).

Prof. Claudio Pantanali, PhD cpantanali@units.it

Vantaggi dell'FTA

1.Approccio Sistematico: Permette di esaminare sistematicamente tutte le possibili cause di un evento indesiderato.

2.Facilità di Visualizzazione: L'approccio grafico aiuta a rappresentare chiaramente la catena dei guasti e come questi si combinano per causare un evento.

3.Supporto alle Decisioni di Progettazione: Identificando i punti deboli e i componenti critici, l'FTA aiuta gli ingegneri a migliorare la sicurezza e l'affidabilità dei sistemi.

Limiti dell'FTA

1. **Richiede una Buona Conoscenza del Sistema**: L'efficacia dell'FTA dipende molto dalla comprensione dettagliata del sistema e dall'identificazione accurata dei guasti.
2. **Non Tratta Bene le Interdipendenze**: L'FTA assume spesso che i guasti siano **indipendenti** tra loro, mentre in realtà molti sistemi complessi hanno componenti che dipendono l'uno dall'altro.
3. **Complessità**: Per sistemi molto grandi e complessi, l'albero può diventare estremamente ampio e difficile da gestire.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Differenze tra FTA e ETA

L'**FTA** e l'**ETA (Event Tree Analysis)** sono entrambe tecniche di analisi del rischio, ma hanno approcci diversi:

- L'FTA è un metodo **top-down**, che parte dall'evento indesiderato e cerca di determinare le sue cause. In altre parole, si parte dall'**evento negativo** e si va a ritroso per capire perché è successo.
- L'ETA è un metodo **bottom-up**, che parte da un **evento iniziale** (come un guasto o un incidente) e analizza le possibili conseguenze o sviluppi. Serve per esplorare cosa potrebbe accadere una volta che si verifica un determinato evento.

Applicazioni dell'FTA

L'FTA è utilizzato in molte industrie, tra cui:

- **Industria Nucleare**: Per identificare potenziali cause di incidenti in impianti nucleari.
- **Settore Aerospaziale**: Per garantire la sicurezza dei sistemi aeronautici.
- **Industria Chimica e Petrolifera**: Per analizzare guasti potenzialmente pericolosi che potrebbero portare a esplosioni o perdite.
- **Automotive**: Per l'analisi di guasti di componenti critici nei veicoli.

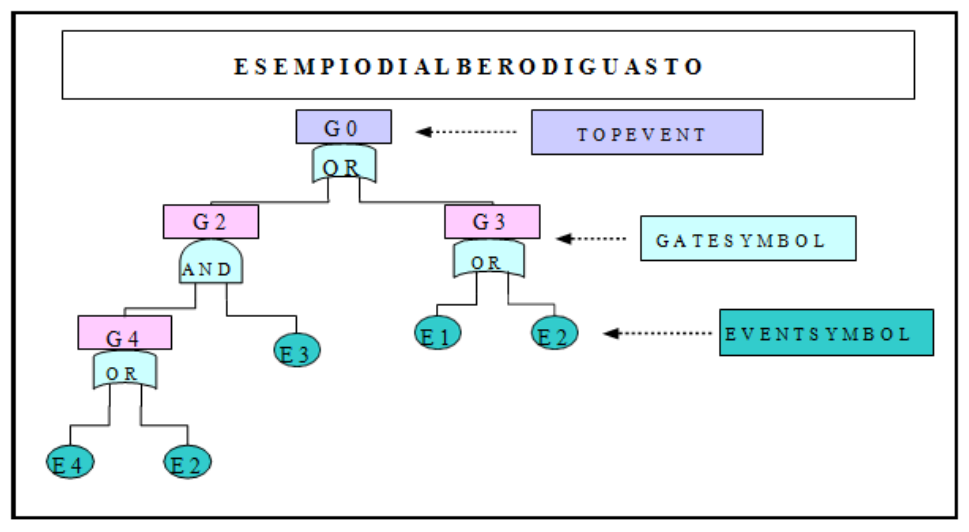
Conclusione

L'**FTA (Fault Tree Analysis)** è uno strumento estremamente potente per analizzare i sistemi complessi, identificare le cause dei guasti e migliorare la sicurezza complessiva. L'approccio grafico e strutturato consente di comprendere meglio le possibili interazioni tra i componenti e i rischi associati a ciascun guasto, rendendolo uno strumento fondamentale in settori critici. Tuttavia, richiede esperienza e una buona conoscenza del sistema per essere efficace, e presenta alcune limitazioni, soprattutto nella gestione di sistemi molto interdipendenti.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

La tecnica degli alberi di guasto richiede la decomposizione del sistema in un diagramma logico, detto ***Albero di Guasto*** (*Fault Tree* o FT), in cui certi eventi primari conducono ad uno specifico evento che rappresenta l'avaria totale del sistema, detto *Top-Event* poiché si trova in *cima all'albero di guasto*



Più semplicemente un FT illustra lo stato del sistema (Top Event) in base agli stati (funzionamento o guasto) delle componenti del sistema (Basic Event). Un esempio di albero di guasto è presentato nella figura.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

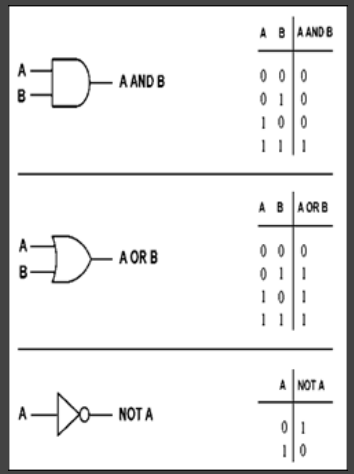
Iniziando dal *Top-Event*, l'albero di guasto è costruito ramificandosi verso livelli più bassi costituiti da eventi intermedi che potrebbero determinare il *Top Event*; cioè si ricostruisce la sequenza degli eventi fino ad arrivare agli eventi di base di cui sono note le probabilità di accadimento.

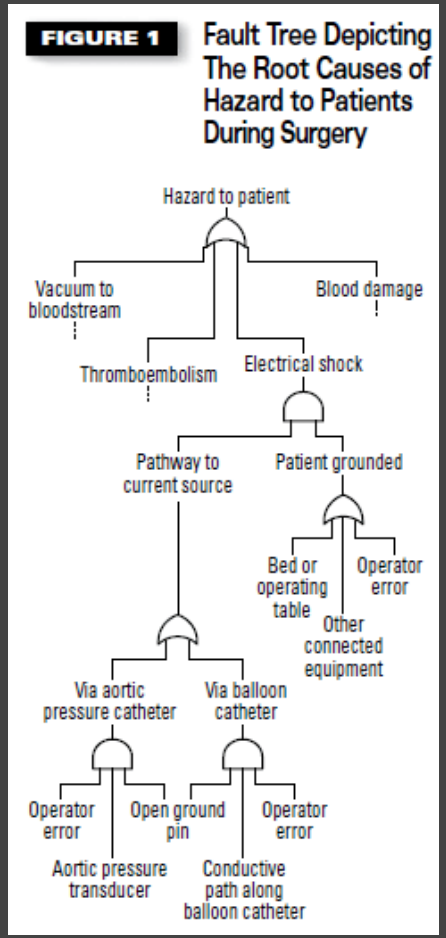
Una volta che l'albero di guasto è stato costruito, la probabilità del *Top-Event* può essere determinata calcolando la probabilità degli eventi intermedi con l'approccio *Top-Down*. Le connessioni tra gli eventi intermedi sono rappresentate tramite ***gates,*** dove l'output di un *gate* è determinato dagli input che a lui arrivano.

La *Fault Tree Analysis* si articola nei seguenti passi:

- *definizione del Top Event*;
- *costruzione dell'Albero di Guasto*;
- *analisi qualitative*;
- *eventuali analisi quantitative dell'Albero di Guasto*.

Ogni passo è fondamentale e sintetizzati a seguire.





Prof. Claudio Pantanali, PhD cpantanali@units.it

1.Guasto di un Sistema di Raffreddamento in una centrale nucleare: In questo caso, il Top Event è il guasto del sistema che fornisce raffreddamento al reattore, un evento con potenziali conseguenze catastrofiche.
2.Esplosione in un Impianto Chimico: L'esplosione potrebbe essere il Top Event e l'obiettivo dell'analisi è identificare tutte le possibili cause che potrebbero portare a tale esplosione.
3.Guasto del Sistema di Alimentazione di Emergenza: Come nell'esempio dell'albero dei guasti discusso, il guasto del sistema di alimentazione di emergenza può essere un Top Event, e si vuole analizzare cosa può causare questo guasto e quali sono i percorsi possibili che lo portano a verificarsi.
Rappresentazione del Top Event nell'Albero dei Guasti
In un **Fault Tree**, il **Top Event** è posizionato nella parte **superiore** del diagramma, da cui si sviluppa l'intero albero verso il basso per rappresentare le cause sottostanti. Il Top Event è collegato ad altri eventi intermedi o eventi di base attraverso delle **porte logiche** (come AND e OR) per rappresentare la combinazione di fattori che possono portare al guasto.
Importanza del Top Event
•**Punto di Partenza per la Mitigazione**: Il Top Event è l'evento che l'azienda o l'ente vuole evitare, quindi l'analisi dell'albero dei guasti viene utilizzata per identificare i fattori di rischio e implementare azioni di mitigazione che possano ridurre la probabilità che si verifichi.
•**Quantificazione del Rischio**: L'FTA aiuta a stimare la **probabilità** che il Top Event si verifichi, valutando la combinazione delle probabilità di tutti i guasti a monte.
•**Identificazione delle Cause Radice**: Attraverso l'analisi, si identificano tutti i fattori che contribuiscono al Top Event, fornendo una visione chiara delle **cause radice** e dei punti di vulnerabilità del sistema.
In sintesi, il **Top Event** rappresenta l'elemento centrale dell'analisi FTA ed è l'evento negativo che si desidera prevenire. L'analisi mira a scomporre questo evento in tutte le possibili cause che lo possono determinare, permettendo di migliorare la sicurezza, l'affidabilità e la gestione dei rischi del sistema.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

Il **Top Event** (o **Evento Principale**) è il punto di partenza di un'analisi **Fault Tree Analysis (FTA)**, rappresenta l'**evento indesiderato** che si desidera prevenire o analizzare. In altre parole, è il guasto o l'incidente critico per il quale si vogliono determinare tutte le possibili cause sottostanti. L'obiettivo di un'analisi dell'albero dei guasti è comprendere come e perché si possa verificare il Top Event, identificando e analizzando tutti i guasti e le condizioni che potrebbero contribuire a causarlo.

Caratteristiche del Top Event

•**Evento Critico**: Il Top Event rappresenta un evento di particolare interesse, generalmente con conseguenze significative per la sicurezza, la produzione o l'affidabilità del sistema.

- **Inizio dell'Analisi FTA**: Nell'analisi dell'albero dei guasti, l'analisi parte sempre dal Top Event e poi discende verso il basso per scoprire le cause possibili. Si utilizza un approccio "top-down".
- **Focus sulla Prevenzione**: Il Top Event viene scelto perché è un evento che si desidera evitare. Può rappresentare un incidente come un'esplosione, un guasto a un sistema critico, un'interruzione della produzione o qualunque altra condizione con un impatto significativo.

Come abbiamo sopra visto l'albero di guasto è un modello grafico che: *visualizza combinazioni di eventi che possono portare ad un evento finale indesiderato*, che normalmente coincide con *la rottura* o *il malfunzionamento* del sistema visto nel suo complesso, ed è chiamato *Top-Event.*

La descrizione del Top Event risponde alle seguenti domande:

- *What:* descrive l'evento critico sul quale è focalizzato l'analisi;
- *Where:* descrive dove l'evento critico avviene;
- *When:* descrive quando l'evento critico si verifica.

La definizione del Top-Event è indubbiamente una delle fasi più delicate nella FTA.
Se un Top Event non è *definito con precisione*, si ha il rischio che l'Albero di Guasto che ne risulta sarà eccessivamente: *grande, complesso* e *non ben focalizzato sul problema che vuole analizzare*.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempi di Top Event

1. **Guasto di un Sistema di Raffreddamento** in una centrale nucleare: In questo caso, il Top Event è il guasto del sistema che fornisce raffreddamento al reattore, un evento con potenziali conseguenze catastrofiche.
2. **Esplosione in un Impianto Chimico**: L'esplosione potrebbe essere il Top Event e l'obiettivo dell'analisi è identificare tutte le possibili cause che potrebbero portare a tale esplosione.
3. **Guasto del Sistema di Alimentazione di Emergenza**: Come nell'esempio dell'albero dei guasti discusso, il guasto del sistema di alimentazione di emergenza può essere un Top Event, e si vuole analizzare cosa può causare questo guasto e quali sono i percorsi possibili che lo portano a verificarsi.

Rappresentazione del Top Event nell'Albero dei Guasti

In un **Fault Tree**, il **Top Event** è posizionato nella parte **superiore** del diagramma, da cui si sviluppa l'intero albero verso il basso per rappresentare le cause sottostanti. Il Top Event è collegato ad altri eventi intermedi o eventi di base attraverso delle **porte logiche** (come AND e OR) per rappresentare la combinazione di fattori che possono portare al guasto.

Importanza del Top Event

- **Punto di Partenza per la Mitigazione**: Il Top Event è l'evento che l'azienda o l'ente vuole evitare, quindi l'analisi dell'albero dei guasti viene utilizzata per identificare i fattori di rischio e implementare azioni di mitigazione che possano ridurre la probabilità che si verifichi.
- **Quantificazione del Rischio**: L'FTA aiuta a stimare la **probabilità** che il Top Event si verifichi, valutando la combinazione delle probabilità di tutti i guasti a monte.
- **Identificazione delle Cause Radice**: Attraverso l'analisi, si identificano tutti i fattori che contribuiscono al Top Event, fornendo una visione chiara delle **cause radice** e dei punti di vulnerabilità del sistema.

In sintesi, il **Top Event** rappresenta l'elemento centrale dell'analisi FTA ed è l'evento negativo che si desidera prevenire. L'analisi mira a scomporre questo evento in tutte le possibili cause che lo possono determinare, permettendo di migliorare la sicurezza, l'affidabilità e la gestione dei rischi del sistema.

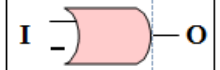
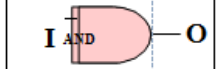
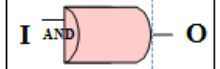
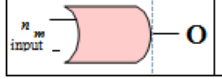
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

COSTRUZIONE DELL'ALBERO DI GUASTO

Un Albero di Guasto è un albero a struttura rovesciata, ovvero con la radice in alto, nel quale, movendoci dall'alto verso il basso, troviamo come primo componente il *Top Event* e, scendendo di livello in livello, arriviamo alle foglie dell'albero che sono costituite dagli eventi di base *(cut set)*

Per rappresentare la sequenza di eventi che devono verificarsi per arrivare all'accadimento del *Top Event*, sono presenti nell'albero, a vari livelli, dei nodi costituiti da *gates* che rappresentano graficamente le relazioni che intercorrono tra i rami che convergono in ciascun nodo.

I gates maggiormente usati sono

GATE SYMBOL	GATE NAME	CASUAL RELATION
	AND gate	Il guasto si verifica se tutti gli elementi in input si guastano
	OR gate	Il guasto si verifica se almeno un elemento di input si guasta
	PRIORITY AND gate	Il guasto si verifica se tutti gli eventi di input si guastano seguendo un preciso ordine
	EXCLUSIVE OR gate	Il guasto si verifica se uno, e solo uno, degli eventi di input si guastano
	m-OUT OF-n gate	Il guasto si verifica se m degli n eventi di input si guastano

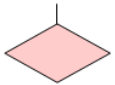
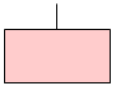
I = INPUT \ O =OUTPUT

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

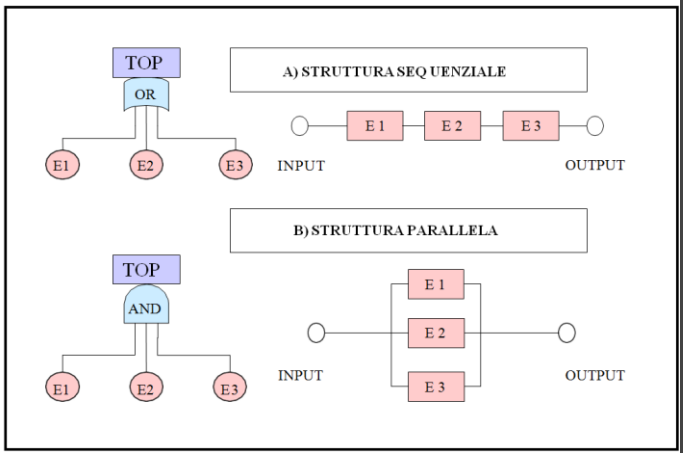
In questa presentazione si considerano solamente *sistemi binari*, ovvero sistemi in cui ogni componente ed in ultima analisi anche l'intero sistema può assumere unicamente le due condizioni "*funzionante/non funzionante*".

La simbologia usata, in questa analisi e per tutti i sistemi in generale, è riportata nella figura

EVENT SYMBOL	NOME	SIGNIFICATO
	Cerchio	Basic Event con sufficienti dati
	Diamante	Evento non sviluppato
	Rettangolo	Evento rappresentato da un gate
	Casa	E vento che può occorrere o non occorrere
	Triangolo	Simbolo di trasferimento

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)



OR → rappresenta una *Struttura Sequenziale*
AND → rappresenta una *Struttura Parallela*

Durante la definizione dell'albero è inoltre importante considerare la presenza di eventuali *cause comuni di guasto*.

Se il malfunzionamento o la rottura di un componente del sistema considerato infatti, provoca la perdita di più funzioni del sistema stesso, i due o più effetti provocati non sono indipendenti tra loro e questo fatto può portare ad una notevole variazione dell'espressione della possibilità di guasto totale, ovvero del *Top Event*.

Di conseguenza si seguono delle regole standard per la costruzione dell'Albero di , cioè:

- Definire la complessità e i confini del sistema che si vuol analizzare;
- Definire il Top-Event, nel modo più accurato possibile;
- Identificare le cause che provocano il Top-Event, associando gli opportuni gates o events symbol e identificare i nodi;
- Identificare le ultime ramificazioni dell'albero significa trovare i Basic Event e significa che l'analisi si è conclusa.

La costruzione dell'albero richiede molta attenzione, gli errori più comuni sono:
- Identificazione errata, quindi soluzioni ambigue e senza significato;
- Uso della nomenclatura in modo inappropriata o anche poco precisa;
- Uso di sottosistemi significativi per poter analizzare il sistema nel suo complesso.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

ANALISI QUALITATIVA

L'occorrere del TOP Event (in questo ambito corrisponde al *fallimento del sistema*) è spesso dovuto alle differenti combinazioni dei Basic Event.
Un FT fornisce utili informazioni per quanto riguarda queste combinazioni.
In questo contesto il concetto di *Cut Sets* è molto importante.

Un *Cut Sets* in un FT è un insieme di Basic Event i quali, se occorrono simultaneamente, fanno si che anche il Top Event occorra.

Un Cut Set è detto ***Minimal*** se *l'insieme non può essere ridotto senza perdere il suo status di Cut Set*.
l loro studio permette di effettuare analisi sui Basic Event molto più approfondite di quelle che si ottengono dallo studio delle singole componenti.

Ad esempio: Permette di trattare simultaneamente un certo numero di guasti (quando i Cut Sets contengono più di un elemento);permette di identificare e di trattare più facilmente le cause comuni di guasto; permette un'integrazione più immediata delle cause che portano il sistema a fallire.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Un **Cut Set** (insieme di taglio) è un concetto fondamentale utilizzato nella **Fault Tree Analysis (FTA)** per individuare le combinazioni di guasti di base che possono causare il **Top Event**. In altre parole, il **Cut Set** rappresenta un insieme di eventi di guasto che, se accadono contemporaneamente, portano inevitabilmente al verificarsi dell'evento indesiderato (il Top Event). L'analisi degli insiemi di taglio è utile per comprendere meglio i percorsi critici che possono portare a un guasto totale del sistema e per sviluppare strategie di mitigazione.

Definizione di Cut Set

Un **Cut Set** è una **combinazione di eventi di base** (guasti elementari) che, se accadono insieme, portano al verificarsi del **Top Event**. In altre parole, è un percorso che conduce dall'evento di base (guasto o malfunzionamento di un componente) al guasto complessivo del sistema.

- Ogni **Cut Set** rappresenta un **percorso di guasto** che può causare il Top Event.
- I **Cut Set** sono importanti per identificare i componenti o i gruppi di componenti che possono essere critici per la sicurezza del sistema.

Minimo Cut Set

Un concetto correlato è quello del **Minimo Cut Set** (Minimal Cut Set). Un **Minimo Cut Set** è il più piccolo insieme possibile di eventi di guasto che, se accadono insieme, portano al verificarsi del Top Event. Se anche uno degli eventi di un Minimo Cut Set non si verifica, il Top Event non avviene.

- **Minimalità**: Il concetto di "minimo" implica che nessun evento può essere rimosso dal Cut Set senza perdere la capacità di causare il Top Event.
- **Importanza nella Mitigazione**: Il Minimo Cut Set aiuta a identificare le parti del sistema su cui è necessario intervenire per evitare il verificarsi dell'evento indesiderato. Concentrandosi su questi, è possibile migliorare l'affidabilità generale del sistema.

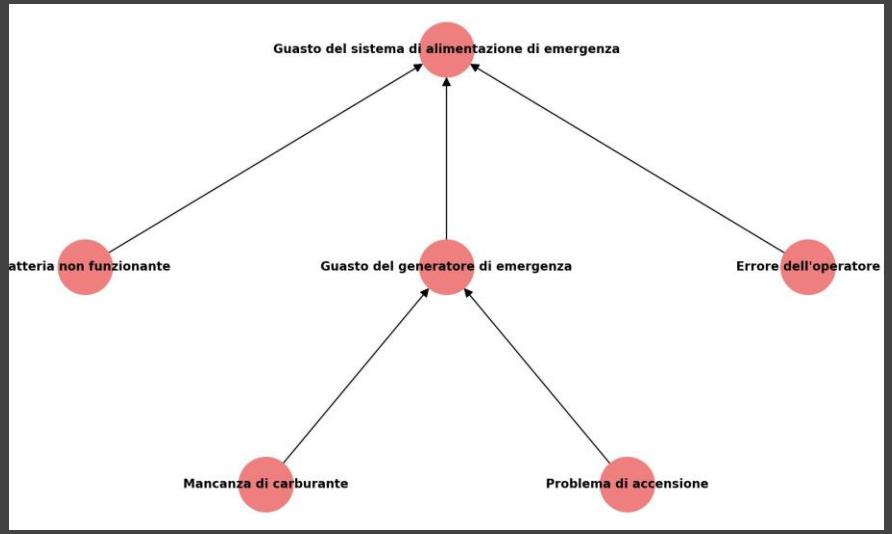
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempio di Cut Set

Immaginiamo un sistema di alimentazione di emergenza che può guastarsi per diversi motivi. Il **Top Event** è il **guasto del sistema di alimentazione di emergenza** e le cause di questo guasto possono essere combinate come segue:

1. **Guasto della Batteria** (evento di base).
2. **Guasto del Generatore di Emergenza** (evento di base), che può verificarsi a causa di:
   - **Mancanza di Carburante**.
   - **Problema di Accensione**.

Possibili **Cut Set** per il guasto del sistema di alimentazione di emergenza potrebbero essere:
- **Cut Set 1**: Guasto della Batteria.
- **Cut Set 2**: Mancanza di Carburante e Problema di Accensione (entrambi devono verificarsi per causare il guasto del generatore).



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Utilizzo del Cut Set nell'FTA

L'analisi degli **insiemi di taglio** è uno degli obiettivi principali della Fault Tree Analysis. È particolarmente utile per:

1. **Valutazione della Sicurezza del Sistema**:
   - Gli insiemi di taglio aiutano a identificare i componenti critici del sistema. Se questi componenti falliscono, possono portare direttamente al Top Event.
2. **Quantificazione del Rischio**:
   - Ogni **evento di base** in un Cut Set ha una certa **probabilità di guasto**. L'analisi dei Cut Set permette di combinare queste probabilità per stimare la probabilità complessiva che si verifichi il Top Event.
3. **Prioritizzazione delle Azioni di Mitigazione**:
   - I Cut Set aiutano a capire quali componenti o sottosistemi sono più critici per la sicurezza del sistema. L'attenzione può essere concentrata su di essi per ridurre il rischio di guasto complessivo.
4. **Identificazione dei Punti Deboli**:
   - I **Minimal Cut Set** identificano le combinazioni minime di eventi di guasto che causano il Top Event, evidenziando i punti deboli che possono essere risolti con modifiche progettuali o con l'aggiunta di ridondanza.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Analisi del Cut Set: Esempio Pratico

Consideriamo un impianto industriale con un sistema di sicurezza composto da un sensore di temperatura, una valvola di sicurezza e un sistema di allarme. L'evento indesiderato, o **Top Event**, è un aumento incontrollato della temperatura, e questo evento può verificarsi se:

- Il **sensore di temperatura non rileva** l'aumento della temperatura.
- La **valvola di sicurezza non si apre**.
- Il **sistema di allarme non avvisa** l'operatore.

Cut Set per questo sistema potrebbero essere:

1.Guasto del Sensore di Temperatura e della Valvola di Sicurezza.

2.Guasto della Valvola di Sicurezza e del Sistema di Allarme.

Un **Minimo Cut Set** sarebbe quello composto da:

- **Guasto del Sensore di Temperatura**, in combinazione con uno dei due altri componenti (la valvola o l'allarme). Questo è un esempio di come una combinazione minima di eventi può condurre al Top Event.

Importanza dei Minimo Cut Set

I **Minimal Cut Set** hanno un'importanza cruciale per:

- **Ridurre la Complessità del Sistema**: Gli ingegneri possono concentrare le loro risorse sui percorsi più critici per evitare l'evento indesiderato.
- **Valutare la Robustezza del Sistema**: Capire quali singoli componenti o gruppi di componenti devono essere migliorati per aumentare la robustezza complessiva.

Tecniche per Trovare i Cut Set

Esistono diversi approcci per determinare i Cut Set durante l'analisi dell'albero dei guasti:

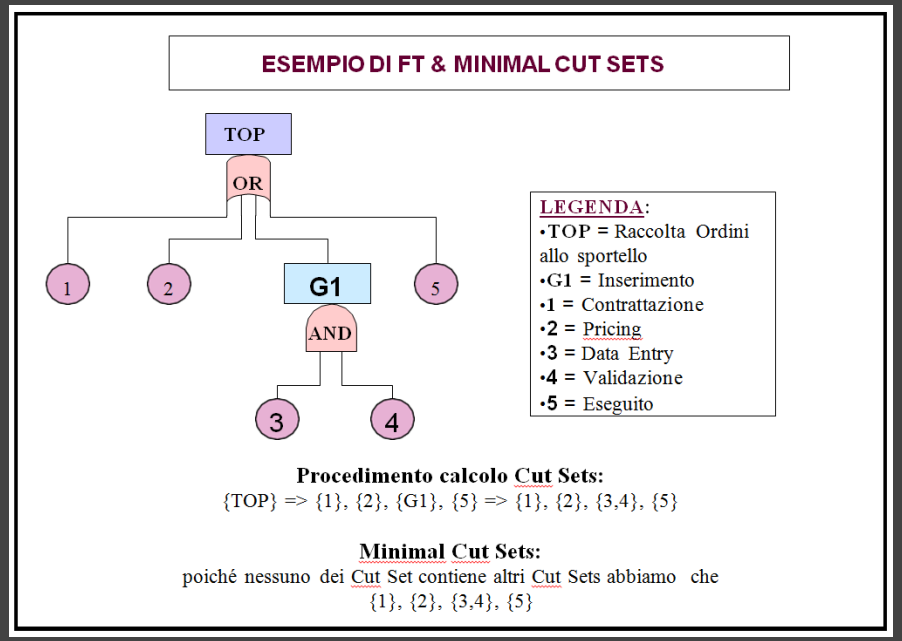
- **Analisi Manuale**: In sistemi semplici, gli ingegneri possono disegnare manualmente l'albero e identificare i Cut Set.
- **Software di Analisi del Rischio**: Nei sistemi più complessi, viene utilizzato software specializzato per identificare tutti i possibili Cut Set e calcolarne la probabilità.

Conclusione

In sintesi, i **Cut Set** e i **Minimal Cut Set** sono strumenti fondamentali nella Fault Tree Analysis per comprendere come i guasti elementari si combinano per causare un evento indesiderato (Top Event). Analizzando i Cut Set, gli ingegneri possono identificare i percorsi critici verso il guasto e implementare strategie di mitigazione che migliorino l'affidabilità e la sicurezza del sistema. Concentrarsi sui Minimal Cut Set è particolarmente utile per identificare i punti deboli e intervenire in modo mirato per ridurre il rischio complessivo.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)



La figura mostra un *FT* ed i relativi *Minimal Cut Sets.*
Vediamo che il **nodo G1** si guasta solo se entrambi i Basic Event (E3 e E4) si guastano, quindi un inserimento sbagliato dei dati si ha sia perché c'è stato un errore nella fase di *Data Entry*, sia perché c'è stato un errore nella fase di *Validazione* dei dati.

Possiamo aggiungere che il Top Event è in stato di *guasto* se, o E1, o il nodo G1 oppure E5 si guastano, ossia si ha errore nella *Raccolta Ordini* perché c'è un errore o nella fase di *Contrattazione*, o nella fase di *Pricing*, o in quella di *Inserimento*, o in quella di *Eseguito,* o contemporaneamente c'è errore in più di ognuna di queste.

I **Minimal Cut Set** risultano molto importanti nello studio dell'*Affidabilità (probabilità che ad un determinato tempo t il sistema sia funzionante)* di un sistema perché permettono di effettuare analisi, oltre che sui Basic Event, anche sul Top Event.
Per l'approfondimento di questo aspetto, rimandiamo ai paragrafi successivi.

Prof. Claudio Pantanali, PhD cpantanali@units.it

FTA (Fault Tree Analysis)

ANALISI QUANTITATIVA

Una volta che i Minimal Cut Sets sono stati ottenuti, si possono ottenere delle valutazioni basate sulla *probabilità* di ottenere determinati stati del sistema ed avere, così, dei risultati quantitativi. La procedura per ottenere queste valutazioni è la seguente:

- *determinare la probabilità di guasto di ogni Basic Event*;
- *determinare la probabilità di guasto del Minimal Cut Set;*
- *determinare la probabilità di guasto del Top Event, ossia di tutto il sistema*.

Con la stessa procedura si possono ottenere altre statistiche non meno importanti: l'*Affidabilità*, la *Disponibilità*, ecc.

Tutti questi indicatori si ottengono facilmente a partire dalla *Funzione di Struttura* del sistema.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Analisi quantitativa

Analisi quantitativa dei **Cut Set minimi (Minimal Cut Set)** è un passo fondamentale della **Fault Tree Analysis (FTA)** per determinare la **probabilità complessiva** che si verifichi l'evento indesiderato (Top Event). L'analisi si basa sull'assegnazione di **probabilità di guasto** ai singoli eventi di base e poi sul calcolo di tali probabilità lungo le combinazioni rappresentate dai Cut Set minimi. Questo processo consente di quantificare il rischio complessivo e di identificare i percorsi più critici che possono portare al guasto.

Obiettivo dell'Analisi Quantitativa con Cut Set Minimi

- **Calcolare la probabilità complessiva del Top Event**, cioè l'evento critico che si desidera prevenire.
- **Identificare il contributo dei singoli Cut Set minimi** alla probabilità totale del guasto. Questo permette di identificare quali percorsi contribuiscono maggiormente al rischio e su quali occorre concentrare l'attenzione.

Processo di Analisi Quantitativa

1.Identificazione dei Minimal Cut Set:

- Si inizia identificando tutti i **Minimal Cut Set** dell'albero dei guasti. Questi sono i più piccoli insiemi di eventi di base che, se si verificano, portano al verificarsi del Top Event.

2.Assegnazione delle Probabilità agli Eventi di Base:

- A ogni evento di base viene assegnata una **probabilità di guasto** (tipicamente indicata come "P"). Queste probabilità si basano su dati storici, analisi statistiche, affidabilità dei componenti, ecc.

3.Calcolo della Probabilità dei Minimal Cut Set:

- Ogni Minimal Cut Set è formato da una combinazione di eventi di base. La probabilità che il Minimal Cut Set si verifichi dipende dalle porte logiche che lo collegano:
    1. **Porta AND**: La probabilità che il Cut Set si verifichi è il **prodotto** delle probabilità dei singoli eventi.
    2. **Porta OR**: La probabilità è calcolata come la **somma** delle probabilità dei singoli eventi meno la probabilità congiunta (per evitare il doppio conteggio).

4.Calcolo della Probabilità del Top Event:

- La probabilità del Top Event può essere calcolata combinando le probabilità di tutti i Minimal Cut Set utilizzando la **formula dell'unione** per evitare il doppio conteggio. Se assumiamo che gli eventi di base siano statisticamente indipendenti, la probabilità del Top Event può essere calcolata come la **somma delle probabilità** dei Cut Set minimi.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempio Pratico di Analisi Quantitativa

Supponiamo di avere il seguente **Fault Tree** per un sistema di alimentazione di emergenza, e di voler calcolare la probabilità complessiva del guasto:

•**Top Event**: Guasto del sistema di alimentazione di emergenza.

•**Minimal Cut Set**:

- **Cut Set 1**: Guasto della Batteria (P1)
- **Cut Set 2**: Mancanza di Carburante (P2) e Problema di Accensione (P3) — Porta AND

Diamo ora delle **probabilità** di guasto ai singoli eventi:

- **P1 (Guasto della Batteria)** = 0,02
- **P2 (Mancanza di Carburante)** = 0,01
- **P3 (Problema di Accensione)** = 0,03

Calcolo delle Probabilità dei Minimal Cut Set:

- **Cut Set 1**: La probabilità che il guasto della batteria porti al Top Event è semplicemente **P1** = 0,02.
- **Cut Set 2** (Mancanza di Carburante e Problema di Accensione): Essendo una **porta AND**, la probabilità del guasto è il prodotto delle probabilità dei singoli eventi:

$$P_{\text{Cut Set 2}} = P2 \times P3 = 0,01 \times 0,03 = 0,0003$$

Calcolo della Probabilità del Top Event: La probabilità complessiva del **Top Event** (guasto del sistema di alimentazione di emergenza) si ottiene sommando le probabilità dei due Minimal Cut Set, considerando che si tratta di eventi indipendenti:

$$P_{\text{Top Event}} = P_{\text{Cut Set 1}} + P_{\text{Cut Set 2}}$$

$$P_{\text{Top Event}} = 0,02 + 0,0003 = 0,0203$$

Quindi, la probabilità complessiva che si verifichi il guasto del sistema di alimentazione di emergenza è **0,0203**, ovvero circa il **2,03%**.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Analisi quantitativa

Importanza dell'Analisi Quantitativa dei Cut Set Minimi

1.Identificazione dei Percorsi Critici:

- Attraverso l'analisi quantitativa, è possibile capire quali Cut Set contribuiscono maggiormente al rischio complessivo. Questo consente di identificare i percorsi critici e implementare contromisure mirate per ridurre il rischio.

2.Valutazione dell'Affidabilità del Sistema:

- Conoscere la probabilità complessiva del Top Event aiuta a valutare l'affidabilità del sistema e a prendere decisioni informate sulle azioni da intraprendere per migliorare la sicurezza.

3.Ottimizzazione dei Costi:

- Capire quali eventi contribuiscono maggiormente al rischio permette di ottimizzare i costi delle azioni di mitigazione, concentrando risorse solo dove è davvero necessario.

4.Supporto nella Progettazione:

- Durante la progettazione di nuovi sistemi, l'analisi quantitativa dei Cut Set aiuta a definire standard di sicurezza e ridondanza più efficaci per ridurre al minimo le probabilità di guasto.

Tecniche Avanzate per l'Analisi Quantitativa

•**Monte Carlo Simulation**: Spesso, per sistemi molto complessi, si utilizzano simulazioni Monte Carlo per stimare la probabilità di guasto. Questo metodo è particolarmente utile quando gli eventi di base non sono indipendenti.

•**FTA Software Tools**: Esistono vari strumenti software specifici per condurre analisi quantitative complesse. Questi strumenti facilitano il calcolo delle probabilità per sistemi con molti eventi e porte logiche.

Conclusione

L'**analisi quantitativa dei Cut Set minimi** è una tecnica potente per quantificare il rischio di eventi critici in un sistema. Identificando e calcolando la probabilità che si verifichino i percorsi di guasto, gli ingegneri possono determinare quali azioni intraprendere per migliorare la sicurezza e l'affidabilità del sistema. Questo processo contribuisce non solo alla riduzione del rischio, ma anche a una maggiore efficienza economica nella gestione delle risorse dedicate alla sicurezza.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

LA FUNZIONE DI STRUTTURA

L'algebra booleana è il primo strumento matematico utilizzato per una iniziale analisi di un Fault Tree:

una variabile booleana è una variabile che prende i suoi valori nell'insieme {0,1} e quindi ben si presta alla rappresentazione di un evento del tipo buon funzionamento/guasto.
Indicato con *H* l'insieme {0,1}, una funzione ϕ definita su $\mathbf{H^n}$ a valori in *H* è detta *funzione booleana*.

La funzione booleana che per eccellenza permette un'analisi del Fault Tree è la ***Funzione di Struttura***: essa traduce in formule matematiche la relazione tra il Top Event ed i Basic Event dell'Albero di Guasto: il suo scopo essenziale è quello di descrivere in maniera compatta(con ϕ = 0 o con ϕ = 1) il guasto/fallimento del sistema per tutti i possibili stati dei suoi componenti.

Questa nozione si comprende meglio se si considera un sistema ***S*** costituito da ***n*** componenti $\boldsymbol{C_1,\ldots,C_n}$ e sia $\boldsymbol{x_i}$ la variabile booleana che vale 0 se e soltanto se si verifica un guasto nel componente $\boldsymbol{C_i}$: indicata con $\boldsymbol{x_S}$ la variabile di uscita del sistema (ovvero), si ha che $\mathbf{x_S}$ è una funzione booleana dipendente dalla variabili booleane $\mathbf{x_i}$, vale a dire:

$$x_S = \Phi\left(x_1 \ldots . x_n\right)$$

Con il termine *Fault Tree* relativo al sistema *S* si intende quindi sia la funzione ϕ che una sua rappresentazione nel senso della teoria dei grafi: il Fault Tree mostra quindi la struttura logica di come i guasti dei componenti si ripercuotano sul guasto dell'intero sistema.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Nella **Fault Tree Analysis (FTA)**, il concetto di **funzione di struttura** (in inglese "**structure function**") è un elemento chiave per descrivere la relazione logica tra i vari componenti di un sistema e per modellare il modo in cui le combinazioni di guasti dei componenti portano all'evento indesiderato (il **Top Event**). La funzione di struttura rappresenta matematicamente la logica dell'albero dei guasti e viene utilizzata principalmente per calcolare le probabilità di guasto, comprendere meglio la resilienza del sistema e valutare le prestazioni complessive.

Cos'è la Funzione di Struttura?

La **funzione di struttura** è una **rappresentazione matematica** del sistema e descrive come lo stato dei componenti individuali influisce sullo stato del sistema complessivo. In altre parole, definisce quali combinazioni di componenti in stato di guasto (o funzionanti) causano il guasto del sistema nel suo insieme.

La funzione di struttura è tipicamente rappresentata come una funzione logica, in cui i vari componenti sono rappresentati con variabili che indicano se un componente è **in funzione** o **in guasto**:

- **Stato "1"** indica che il componente è in funzione (buono).
- **Stato "0"** indica che il componente è in guasto (malfunzionante).

La funzione di struttura quindi mappa ogni possibile combinazione di stati dei componenti al **risultato del sistema**:

- **1** significa che il sistema è in funzione.
- **0** significa che il sistema è in guasto.

Notazione della Funzione di Struttura

Nella **funzione di struttura** vengono utilizzate porte logiche come **AND** e **OR** per descrivere il funzionamento del sistema:

- **Porte AND**: Il sistema funziona solo se **tutti i componenti coinvolti funzionano**. Se uno dei componenti fallisce, l'intero sistema fallisce.
- **Porte OR**: Il sistema funziona se **almeno un componente funziona**. Il sistema fallisce solo se tutti i componenti falliscono.

La funzione di struttura è una funzione booleana che descrive la relazione tra gli ingressi (componenti del sistema) e l'uscita (funzionamento del sistema).

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempio di Funzione di Struttura

Immaginiamo un semplice sistema con tre componenti A, B e C, e il **Top Event** (guasto del sistema) è modellato attraverso le seguenti relazioni:

- Il guasto del sistema si verifica se **entrambi** i componenti A e B falliscono.
- Inoltre, se **C fallisce** da solo, il sistema è comunque in guasto.

In questo caso, la **funzione di struttura** può essere espressa come:

$$\Phi(A, B, C) = (A \cdot B) + C$$

Dove:

- **A**, **B**, **C** rappresentano i componenti.
- · rappresenta l'operatore **AND**.
- **+** rappresenta l'operatore **OR**.

Nel contesto della funzione booleana, la funzione rappresenta come il guasto dei componenti porta al guasto complessivo del sistema.

Utilizzo della Funzione di Struttura nell'FTA

La funzione di struttura viene utilizzata per diverse analisi all'interno della Fault Tree Analysis, tra cui:

1.Valutazione della Affidabilità del Sistema:

- La funzione di struttura permette di calcolare la probabilità di guasto del sistema dato che si conosce la probabilità di guasto di ciascun componente. Utilizzando la funzione di struttura, è possibile modellare il comportamento del sistema sotto diverse condizioni operative.

2.Quantificazione del Rischio:

- Con la funzione di struttura e la probabilità di guasto di ciascun componente, si possono calcolare le **probabilità di guasto** del sistema nel suo complesso. Questo permette di avere una visione quantitativa del rischio associato a un determinato sistema.

3.Analisi di Sensibilità:

- La funzione di struttura permette di comprendere come il guasto di un singolo componente influisce sul guasto complessivo del sistema. Attraverso questa funzione è possibile eseguire analisi di sensibilità, ossia valutare l'importanza di ogni componente per la sicurezza del sistema.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA

Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempio Pratico: Sistema di Alimentazione di Emergenza

Consideriamo l'esempio di un **sistema di alimentazione di emergenza** composto dai seguenti componenti:

- **Batteria (A)**.
- **Generatore di emergenza (B)**.
- **Errore dell'operatore (C)**.

Supponiamo che il **Top Event** (guasto del sistema di alimentazione di emergenza) si verifichi nei seguenti casi:

•**Batteria e Generatore** devono fallire contemporaneamente per causare il guasto (AND).

•Inoltre, se si verifica un **errore dell'operatore** (C), il sistema va in guasto indipendentemente dallo stato degli altri componenti.

In questo caso, la funzione di struttura sarebbe:

$$\Phi(A, B, C) = (A \cdot B) + C$$

Dove:

- **(A \cdot B)**: Il sistema fallisce se entrambi i componenti A e B falliscono (porta AND).
- **+ C**: Se si verifica l'errore dell'operatore, il sistema fallisce comunque (porta OR).

Questa funzione logica permette di modellare il comportamento del sistema e aiuta a capire come i guasti dei singoli componenti contribuiscano al guasto complessivo.

Probabilità Utilizzando la Funzione di Struttura

Per utilizzare la funzione di struttura per calcolare la probabilità del Top Event, occorre conoscere la probabilità di guasto di ogni singolo componente. Ad esempio, se le probabilità di guasto sono:

- **P(A)** = 0,02 (Batteria)
- **P(B)** = 0,01 (Generatore)
- **P(C)** = 0,03 (Errore dell'operatore)

Prof. Claudio Pantanali, PhD cpantanali@units.it

Per calcolare la probabilità del Top Event, si può utilizzare la funzione logica per combinare le probabilità:

1. Calcolo della probabilità di guasto dell'AND ($A \cdot B$):

$$P(A \cdot B) = P(A) \times P(B) = 0,02 \times 0,01 = 0,0002$$

2. Calcolo della probabilità del Top Event utilizzando l'OR ($(A \cdot B) + C$):

$$P_{\text{Top Event}} = P(A \cdot B) + P(C) - P(A \cdot B) \cdot P(C)$$

$$P_{\text{Top Event}} = 0,0002 + 0,03 - (0,0002 \times 0,03) = 0,030194$$

Quindi la probabilità complessiva di guasto del sistema è circa 3,02%.

Vantaggi dell'Uso della Funzione di Struttura

1. **Chiarezza nella Rappresentazione**: La funzione di struttura rappresenta chiaramente la relazione tra i componenti e il sistema, permettendo una facile visualizzazione delle relazioni tra guasti e Top Event.
2. **Calcolo del Rischio**: Facilita il calcolo delle probabilità complessive di guasto del sistema, fornendo un mezzo quantitativo per stimare l'affidabilità.
3. **Supporto per la Ridondanza**: La funzione di struttura può essere utilizzata per valutare come l'aggiunta di ridondanza (componenti alternativi) influenzi la probabilità di guasto complessiva.

Conclusione

La **funzione di struttura** è un elemento essenziale nell'analisi **Fault Tree Analysis (FTA)** perché consente di descrivere in modo logico e matematico come i guasti dei vari componenti del sistema contribuiscano al guasto complessivo (Top Event). Attraverso l'uso delle porte logiche AND e OR, la funzione di struttura rappresenta la relazione tra i guasti e aiuta a quantificare la probabilità complessiva di guasto, fornendo una base importante per le decisioni di progettazione e mitigazione dei rischi.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Esempio

Costruzione dell'Albero dei Guasti

Campo di applicazione

- In fase di progetto: può essere usato per identificare i modi di guasto non usuali, con riduzione del rischio.
- In fase operativa: è uno strumento utile per valutare la probabilità di modi di guasto di tipo comune, inclusi gli interventi dell'operatore, sia autonomi che per l'inosservanza delle procedure.
- In generale: può essere usato quando si vuole determinare la probabilità di verificarsi di determinati incidenti e/o scenari.

Tipo e natura dei risultati

Con sufficienti dati di base, la procedura può dare risultati sia qualitativi che quantitativi. In ogni caso consente di individuare le combinazioni di guasto ed errore umano che originano specifici Eventi Critici (elenco degli eventi elementari concomitanti che possono provocare il danno) nonché la relativa importanza come contributo al rischio (influenza dei vari eventi elementari nel determinare il danno).

Requisiti

La preparazione di un albero dei guasti presuppone l'esatta conoscenza sia del funzionamento del sistema e dei suoi componenti in situazione di normale attività sia dei suoi modi di guasto e dei relativi effetti, dati questi ricavabili, ad esempio, da un precedente studio HAZOP, FMEA o FMECA.

Ogni albero deve essere predisposto da un singolo analista, con la collaborazione di operatori ed altro personale con esperienza nel funzionamento dei componenti e dei sistemi inclusi nell'analisi, in modo da avere le informazioni sui guasti che contribuiscono all'incidente.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

Costruzione grafica

L'albero dei guasti viene costruito per mezzo di grafici che uniscono gli eventi alle cause con simboli specifici rappresentanti funzioni logiche (Figura)
Il punto di partenza del grafico è l'Evento Critico da cui si risale alla/e possibile/i causa/e che lo possono produrre.

Esempio applicativo del metodo FTA

Si consideri l'elenco dei guasti che possono portare all'interno di un cantiere temporaneo e mobile all'Evento Critico di morte o lesione di un operaio per effetto, di un evento intermedio quale l'investimento da parte di un automezzo. Nella costruzione grafica dell'albero dei guasti occorre valutare le cause scatenanti dovute all'insorgere sia di guasti primari legati al cattivo funzionamento delle apparecchiature (nel caso specifico, l'automezzo) che di guasti secondari legati ad influenze esterne inaccettabili, come per esempio condizioni ambientali o errori di natura umana.

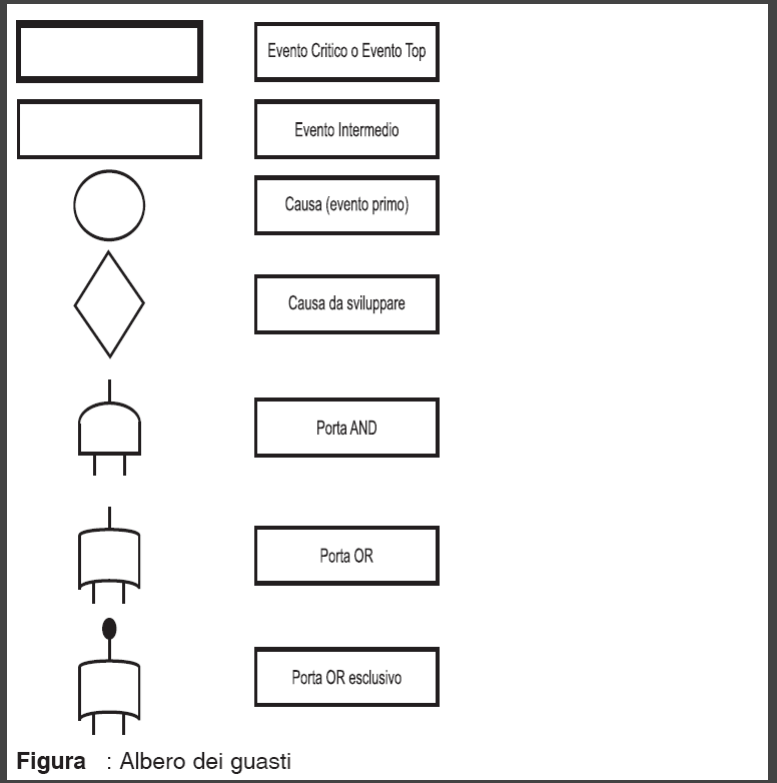


Figura : Albero dei guasti

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

HEA (Human Error Analysis)

Valutazione dei guasti o malfunzionamenti che possono avere causato l'Evento Critico

Si può iniziare cercando di rispondere alla domanda: "cosa deve succedere per avere l'incidente ipotizzato?".

Fra le cause possiamo considerare:
- scarso addestramento del personale presente in cantiere;
- non rispetto delle procedure di sicurezza;
- scarsa attenzione;
- manutenzione inadeguata dell'automezzo;
- mancata valutazione dei rischi interferenti.

Tali eventi ipotetici possono essere suddivisi in categorie distinte per semplificare la costruzione dell'albero.
Per stabilire quali eventi entrano in una categoria e quali no può essere scelto il criterio della connessione degli eventi che le compongono. In questo modo, se ciò è possibile, si individuano delle sequenze incidentali che possono essere analizzate indipendentemente. Queste sequenze, la cui corretta scelta dovrà però essere comprovata a posteriori, possono a loro volta essere suddivise in fasi distinte separatamente analizzate.

Nel nostro caso si possono fare le seguenti suddivisioni:
- eventi connessi con il malfunzionamento dell'automezzo;
- eventi connessi con difetti procedurali;
- eventi connessi con difetto di controllo d'applicazione delle procedure;
- eventi connessi con difetto d'istruzione del personale;
- eventi connessi con errori umani accidentali.

DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

HEA (Human Error Analysis)

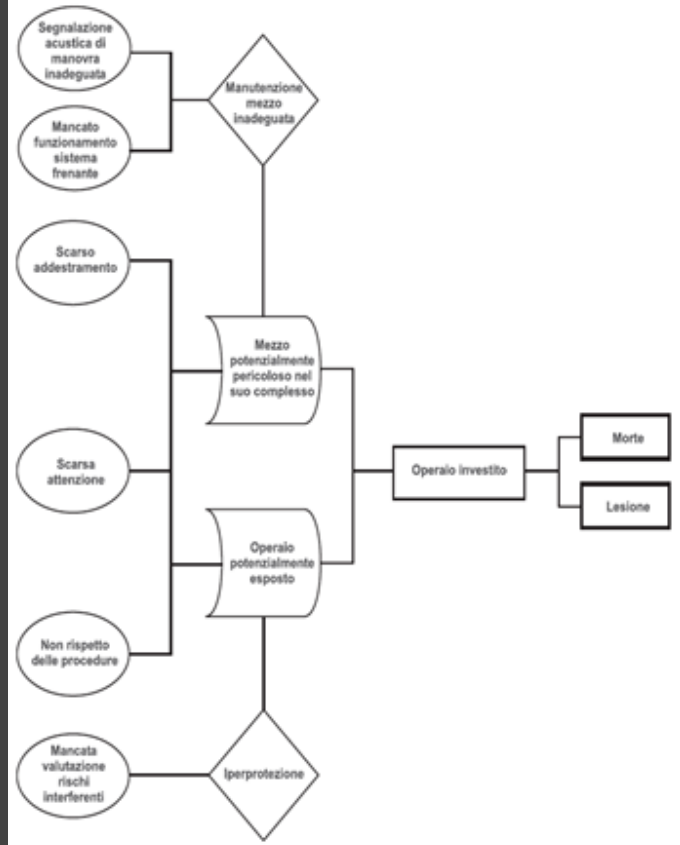
Alla luce di quanto detto è possibile rappresentare l'albero dei guasti per il caso specifico proposto (Figura).Tutti gli eventi intermedi segnati possono essere ulteriormente sviluppati, inoltre appare opportuno fare alcune riflessioni in merito all'errore accidentale. Se le procedure sono corrette e correttamente applicate da operatori istruiti e controllati, gli eventi connessi con difetti procedurali, connessi con difetto di controllo d'applicazione delle procedure e gli eventi connessi con difetto d'istruzione del personale, avranno probabilità assimilabile a "0" mentre l'evento connesso con errori umani accidentali, pur avendo probabilità in questo caso molto bassa, sarà preponderante.

Conclusioni

Si può aggiungere che la metodologia FTA è una metodologia completa che permette di valutare gli apporti al rischio, connesso con l'evento critico, di tutte le cause prime ipotizzabili siano esse legate ad errori umani, omissioni di controllo, non adeguatezza delle procedure operative o alle apparecchiature. Essa inoltre permette di definire quale delle tre azioni tipiche di: prevenzione, attenuazione, protezione, è da porre in essere per rendere il rischio accettabile.

Nell'esempio illustrato si è cercato di mostrare ciò evidenziando anche l'impatto che ha sul rischio il progetto del sistema. L'unico limite della metodologia è rappresentato dal fatto che una analisi accurata è possibile solo se si conosce in modo approfondito il sistema in analisi. Lo studio e l'implementazione di tale metodologia è sicuramente una linea di ricerca che può ridurre gli attuali limiti del metodo e può far si che lo stesso diventi uno strumento agevole per prevenire i rischi dei lavoratori.

Figura : Albero dei guasti specifico



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it