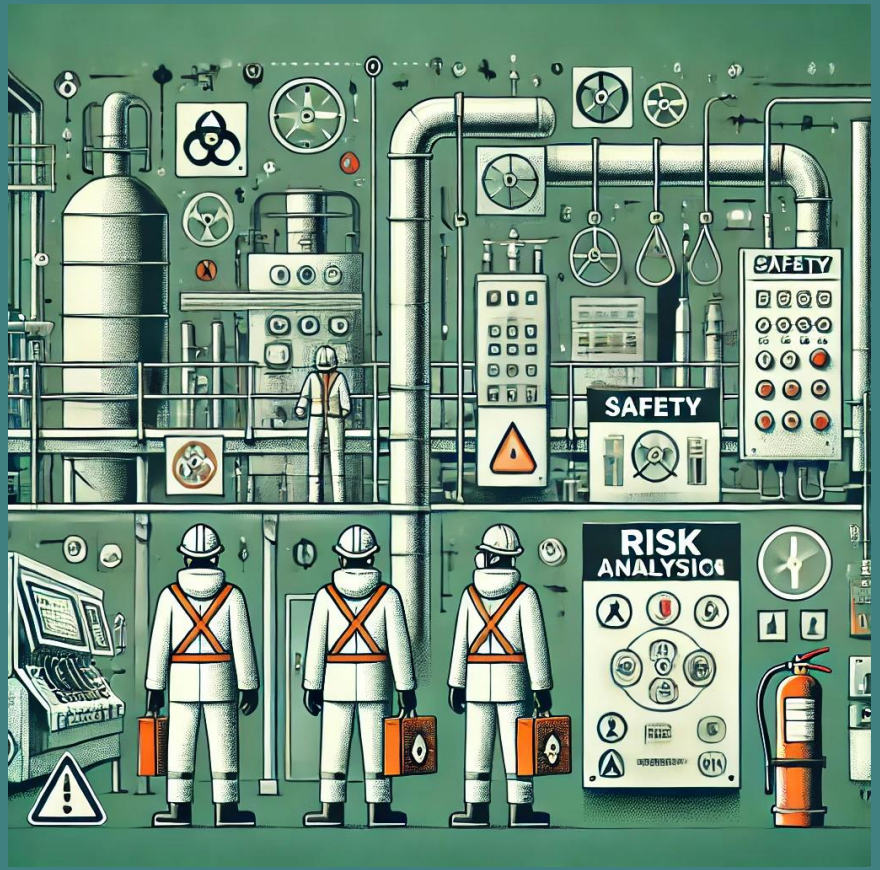
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

# SICUREZZA INDUSTRIALE

# LA VALUTAZIONE DEL RISCHIO

Vol. IV

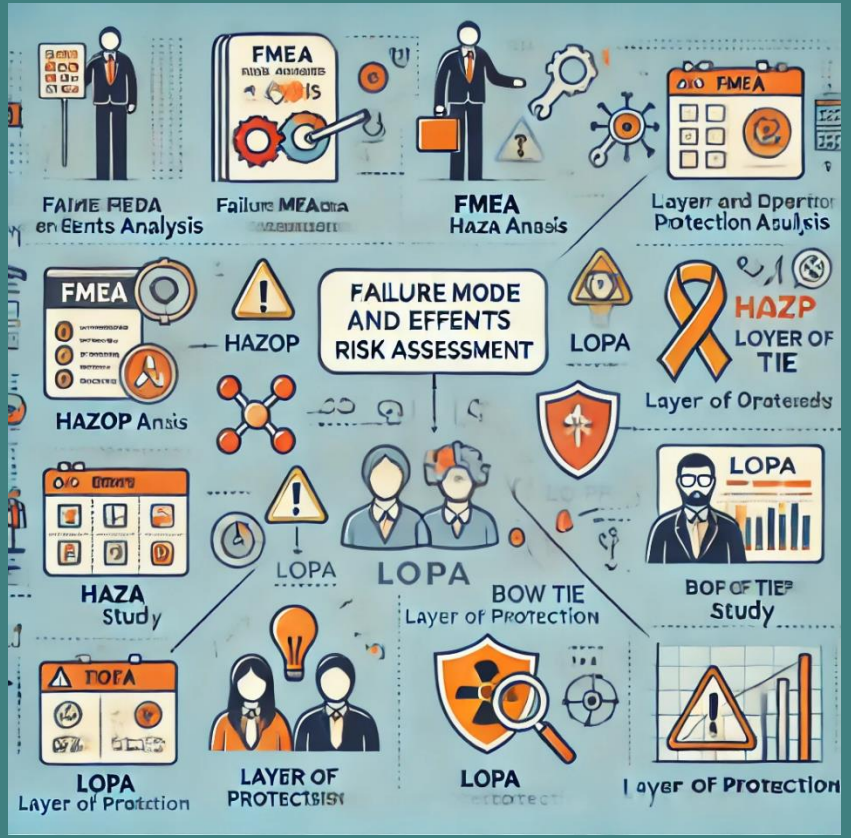


DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it



# 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



# HEA

## Human Error Analysis

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

# Human Error Analysis

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

***CARATTERISTICHE***

Si tratta, in sostanza, di un insieme di più tecniche che descrive le condizioni fisiche e ambientali in cui l'operatore svolge i propri compiti, valutandone gli errori, tenuto conto anche delle capacità e delle abilità a lui richieste. I dati raccolti sono poi utilizzati sia per l'individuazione degli elementi ergonomici che più influiscono che per la creazione di un data-base utilizzabile in altre tecniche quali l'ETA e l'FTA.
Qui l'errore umano è inteso nel suo senso più ampio in quanto sono studiati anche gli errori di gestione, di revisione o di progettazione e non solo quelli operativi o di manutenzione.

***VANTAGGI***

Permette la comprensione dell'influenza dei fattori umani nello svolgimento di operazioni normali o di emergenza come cause iniziali o come concause incidentali e inoltre permette di riconoscerne il meccanismo di formazione.
Conseguentemente, vengono anche fatte proposte di modificazione al sistema per ridurne l'incidenza.

***SVANTAGGI***

La materia è in una fase iniziale rispetto al livello raggiunto dalle altre metodologie inoltre, coinvolgendo argomenti e situazioni non facilmente razionalizzabili, è ancora soggetta a molte incertezze.

***APPLICAZIONE***

E' rara e richiede molta attenzione.
Il tempo necessario ad identificare l'origine di un errore varia secondo i compiti richiesti all'operatore, ma l'analisi può in ogni caso essere completata in poco tempo.
I dati necessari all'analista sono quelli relativi alle procedure dell'impianto, altri desumibili da interviste rivolte al personale e la conoscenza della planimetria e dei comandi dell'impianto.

***COMMENTI***

Si può utilizzare anche nella progettazione di strumenti o ambienti di lavoro, nella gestione del personale, nello studio dei procedimenti operativi, ecc.

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

# Human Error Analysis

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

L'analisi dell'errore umano (Human Error Analysis, HEA) è una tecnica utilizzata per identificare, comprendere e ridurre gli errori umani in processi e sistemi. L'obiettivo è prevenire gli incidenti derivanti da errori umani, migliorando così la sicurezza, l'affidabilità e l'efficienza di un'organizzazione. L'errore umano può verificarsi a causa di vari fattori, come mancanza di formazione, carenze nelle procedure, pressione psicologica o ambienti di lavoro non ideali.
Ecco i principali aspetti e tecniche utilizzate nell'analisi dell'errore umano:

## Tipi di Errori Umani

- **Errori Attivi**: Questi errori hanno effetti immediati e sono generalmente compiuti da operatori che interagiscono direttamente con un sistema. Ad esempio, un operatore che preme un pulsante sbagliato.
- **Errori Latenti**: Questi errori sono meno visibili e possono rimanere nascosti per molto tempo prima di manifestarsi. Spesso sono legati a decisioni di progettazione o problemi nelle procedure che diventano apparenti solo quando una situazione specifica si verifica.

## Tecniche di Analisi degli Errori Umani

### HEART (Human Error Assessment and Reduction Technique):

- HEART è una tecnica utilizzata per stimare la probabilità di errore umano in una data attività.
- Consente di identificare fattori di stress e altre condizioni che potrebbero influenzare negativamente la performance degli operatori.
- Attraverso HEART, è possibile determinare azioni per ridurre il rischio, come migliorare la formazione o ridurre le condizioni di stress.

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Human Error Analysis



**THERP (Technique for Human Error Rate Prediction)**:

- Questa tecnica si basa su un approccio quantitativo per prevedere la probabilità di errore umano in un'operazione.
- THERP scompone un'attività in singole operazioni e stima la probabilità che ogni passo venga completato senza errori, fornendo una valutazione complessiva della probabilità di errore.

**Analisi dei Compiti (Task Analysis)**:

- Questa tecnica implica la suddivisione di un processo in attività più piccole per identificare i passaggi in cui potrebbe verificarsi un errore.
- Comprende anche l'identificazione dei requisiti cognitivi e fisici di ogni attività, come la complessità del processo, le condizioni ambientali e le capacità degli operatori.

**Fattori Umani e Ergonomia**:

- Uno dei principali obiettivi dell'HEA è garantire che il sistema, il luogo di lavoro e le procedure siano adeguati per l'utente umano.
- Questo può includere la progettazione di interfacce uomo-macchina intuitive, il miglioramento dell'ergonomia dell'ambiente di lavoro, e la riduzione dei fattori di distrazione.

**Human Reliability Analysis (HRA)**:

- HRA valuta il contributo dell'errore umano alla probabilità complessiva di un incidente.
- Questa tecnica è utile nei settori ad alto rischio, come l'industria nucleare, il settore petrolchimico e l'aviazione, dove l'errore umano può avere conseguenze gravi.

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Human Error Analysis



## Errori umani – tipologie

Esistono vari metodi per caratterizzare l'errore umano:
alcuni di essi distinguono l'errore a seconda che si origini all'interno o all'esterno dell'individuo (ad es. dovuto a processi di distrazione o a eventi che influenzano la persona), altri analizzano le problematiche relative alla percezione del problema ovvero alla sua possibile gestione.
Considerando l'interazione tra pianificazione ed esecuzione, gli errori umani possono essere classificati secondo Rasmussen, come *skill based*, *rule based* e *knowledge based (SKR)* [Rasmussen, 1983, Rasmussen, 1998] e sono semplificati secondo lo schema proposto in figura.

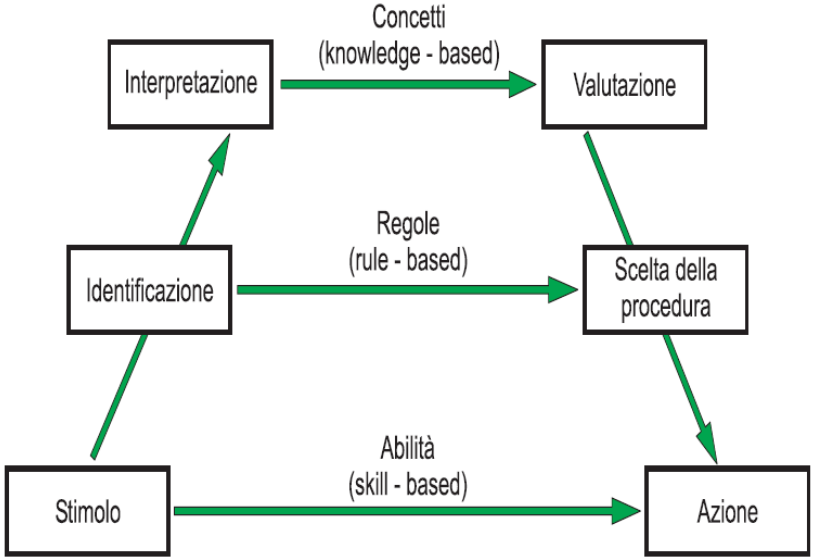
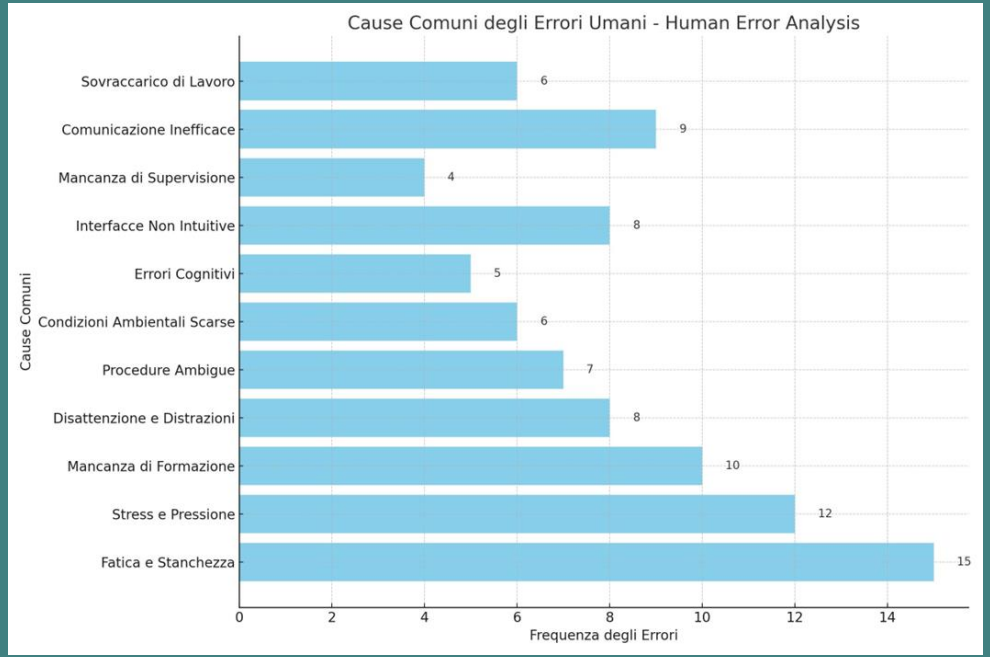



**Figura 1**: Schema semplificato degli errori secondo Rasmussen



Prof. Claudio Pantanali, PhD cpantanali@units.it

# Human Error Analysis



Le cause più comuni degli errori umani sono molteplici e spesso dipendono dall'interazione di fattori individuali, organizzativi e ambientali. Ecco alcune delle cause principali degli errori umani:

**1. Fatica e Stanchezza**

- **Turni Lunghi**: Lavorare per lunghi periodi senza pause adeguate porta a una diminuzione della concentrazione e della prontezza mentale.
- **Privazione del Sonno**: Una mancanza di sonno sufficiente o di buona qualità riduce significativamente la capacità di prendere decisioni accurate.

**2. Stress e Pressione**

- **Scadenze Stringenti**: La pressione del tempo per completare i compiti può portare a decisioni affrettate e scarsa attenzione ai dettagli.
- **Conflitti Lavorativi o Personali**: Lo stress causato da questioni personali o ambienti di lavoro conflittuali può compromettere la capacità di concentrarsi e pensare chiaramente.

**3. Mancanza di Formazione Adeguata**

- **Conoscenze Insufficienti**: La mancanza di formazione o esperienza adeguata può portare a errori, soprattutto in situazioni complesse o nuove.
- **Processi Sconosciuti**: L'assenza di istruzioni o una formazione non aggiornata sui processi può causare errori operativi.

**4. Disattenzione e Distrazioni**

- **Distrazioni Esterne**: Rumori, comunicazioni continue, dispositivi tecnologici e altre interruzioni ambientali possono distogliere l'attenzione.
- **Noia o Lavori Ripetitivi**: Attività ripetitive o monotone possono causare disattenzione e un aumento del rischio di errori.

**5. Ambiguità nelle Procedure**

- **Procedure Non Chiare**: Documentazione poco chiara, contraddittoria o non disponibile può creare confusione e causare errori.
- **Mancanza di Standardizzazione**: Procedure variabili o non standardizzate possono rendere difficile la comprensione di ciò che va fatto.

**6. Condizioni Ambientali Scarse**

- **Illuminazione Inadeguata**: Un'illuminazione insufficiente può rendere difficile vedere dettagli importanti.
- **Temperature Estreme**: Ambienti troppo caldi o troppo freddi possono influire sulla capacità di concentrazione e sulla coordinazione fisica.
- **Rumore Elevato**: Rumori intensi possono ridurre la capacità di comunicazione e di concentrazione.

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Human Error Analysis



**7. Errori Cognitivi**
- Bias Cognitivi: Errori nella percezione e nel giudizio, come il bias di conferma (prestare attenzione solo alle informazioni che confermano ciò che si pensa), possono portare a decisioni sbagliate.
- Memoria Limitata: L'incapacità di ricordare informazioni critiche, soprattutto se il carico di lavoro è elevato, può causare errori operativi.

**8. Interfacce di Controllo Non Intuitive**
- Strumenti Complessi o Non User-Friendly: Se gli strumenti o le interfacce di controllo non sono progettati in modo ergonomico e intuitivo, l'operatore può avere difficoltà nell'interazione corretta.
- Mancanza di Feedback: Un sistema che non fornisce un feedback chiaro può lasciare gli operatori incerti sul successo o il fallimento delle loro azioni.

**9. Mancanza di Supervisione o Controlli Inadeguati**
- Supervisione Insufficiente: La mancanza di supervisione o la supervisione inadeguata può far sì che errori minori non vengano notati finché non diventano più significativi.
- Sistemi di Controllo Mal Funzionanti: Sistemi di controllo progettati male possono non rilevare errori in tempo utile, portando a conseguenze più gravi.

**10. Comunicazione Inefficace**
- Malintesi: I problemi di comunicazione tra i membri del team, sia verbali che scritti, possono portare a interpretazioni errate delle istruzioni o delle situazioni.
- Messaggi Ambigui: Comunicazioni non specifiche o ambigue possono causare confusione, con errori conseguenti nell'esecuzione del compito.

**11. Sovraccarico di Lavoro**
- Multitasking: Essere costretti a svolgere più compiti contemporaneamente può portare a una riduzione della qualità dell'attenzione dedicata a ciascun compito.
- Carico di Lavoro eccessivo: Troppi compiti in un breve periodo possono portare a errori dovuti a decisioni affrettate o dimenticanze.

Per ridurre gli errori umani, è essenziale implementare misure come:
- Formazione Continua: Assicurare che tutto il personale riceva la formazione necessaria e aggiornata.
- Progettazione Ergonomica: Ottimizzare le interfacce e l'ambiente di lavoro per ridurre lo stress e facilitare l'operatività.
- Procedure Chiare e Semplici: Garantire che le istruzioni operative siano standardizzate e di facile comprensione.
- Pianificazione di Turni Adeguati: Minimizzare la fatica assicurando che i dipendenti non lavorino turni eccessivamente lunghi senza pause.

Gli errori umani possono essere ridotti, ma richiedono un approccio combinato di miglioramento dei sistemi, progettazione adeguata dell'ambiente e supporto continuo agli operatori.

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Human Error Analysis



Nel campo della sicurezza sul lavoro viene spesso invocato l'errore umano come generica chiave di interpretazione di molti incidenti, ma dagli studi sull'errore umano e sulle condizioni in cui si verifica si è visto come questo, nella maggior parte dei casi, sia in realtà un "errore organizzativo", dove la componente umana agisce in seguito a una non adeguata progettazione della sua attività.

In questo ambito viene anche studiato il fattore organizzativo nell'induzione di situazioni di stress, che può essere all'origine di una non irrilevante percentuale di eventi classificati come dovuti ad "errore umano". Le costrizioni organizzative giocano un ruolo importante nell'induzione degli errori, in quanto sono in grado di ridurre la soglia di attenzione necessaria per svolgere le operazioni in sicurezza.

Per l'analisi del rischio, in questa presentazione, è stato scelto l'approccio SRK *(skill-ruleknowledge).*

Risulta pertanto di interesse nozionistico menzionare i modelli di valutazione di *II generazione* che si sono soffermati sulla dipendenza dell'affidabilità umana da fattori personali e contestuali.

Tali metodologie mirano alla valutazione qualitativa del comportamento dell'operatore ed alla ricerca di modelli che ne descrivano l'interazione con il processo produttivo.

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Human Error Analysis



Si parla dunque di *modelli cognitivi*, che rappresentano il processo logico-razionale dell'operatore e ne sintetizzano la dipendenza dai fattori personali (quali stress, incompetenza, etc.) e dalla situazione contingente (conduzione normale del sistema, condizioni anomale o, addirittura, emergenza) e *modelli di interfaccia uomo-macchina*, che rispecchiano il sistema di controllo del processo produttivo.

L'utilizzo dei *modelli cognitivi* e dei *modelli di interfaccia uomo-macchina* ha evidenziato la necessità di individuare chiaramente il *dominio* dell'analisi, la cui applicazione appare strettamente legata al contesto lavorativo inteso nel senso più ampio del termine, ossia come ambiente costituito da sistemi tecnologici, organizzativi, gestionali, nonché da relazioni interpersonali.

Una definizione esaustiva del *dominio* di applicazione della *HRA* può essere quella data nell'ambito della Metodologia *Cognitive Reliability and Error Analysis Method-CREAM* [Mosleh, 2004], nel quale esso è definito come

*sistema integrato uomo-tecnologia-organizzazione (MTO integrated system),*

ossia come squadra di operatori *(Men)* che collaborano al fine di raggiungere il medesimo obiettivo, intervenendo sul processo meccanico *(Technology)* in seno ad un sistema di organizzazione e di gestione dell'azienda *(Organisation)*.

L'identificazione del *sistema integrato MTO*, come *dominio* dell'analisi, da una parte, risolve l'esigenza di rendere la *HRA* coerente al campo di applicazione, da quell'altra identifica i confini all'interno dei quali ricercare le variabili indipendenti che influenzano l'affidabilità dell'operatore.

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

# Human Error Analysis

## Esempio di Human Error Analysis

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

Supponiamo di voler analizzare gli errori potenziali in un contesto di impianto chimico in cui gli operatori devono aprire manualmente una valvola di sicurezza.

**Attività**: Aprire una valvola di sicurezza in caso di pressione elevata.

**Possibili Errori**:

- Non aprire la valvola nel momento giusto (errore di temporizzazione).
- Aprire la valvola sbagliata (errore di selezione).
- Non riuscire a verificare la pressione prima di aprire la valvola (errore di controllo).

**Cause Potenziali degli Errori**:

- Mancanza di chiarezza nelle istruzioni operative.
- Etichettatura scorretta delle valvole.
- Stanchezza dell'operatore a causa di turni lunghi.

**Azioni Correttive**:

- Revisionare e migliorare le istruzioni operative.
- Etichettare chiaramente le valvole con codici colore.
- Ridurre i turni o inserire pause regolari per ridurre la fatica.

Benefici dell'Analisi dell'Errore Umano

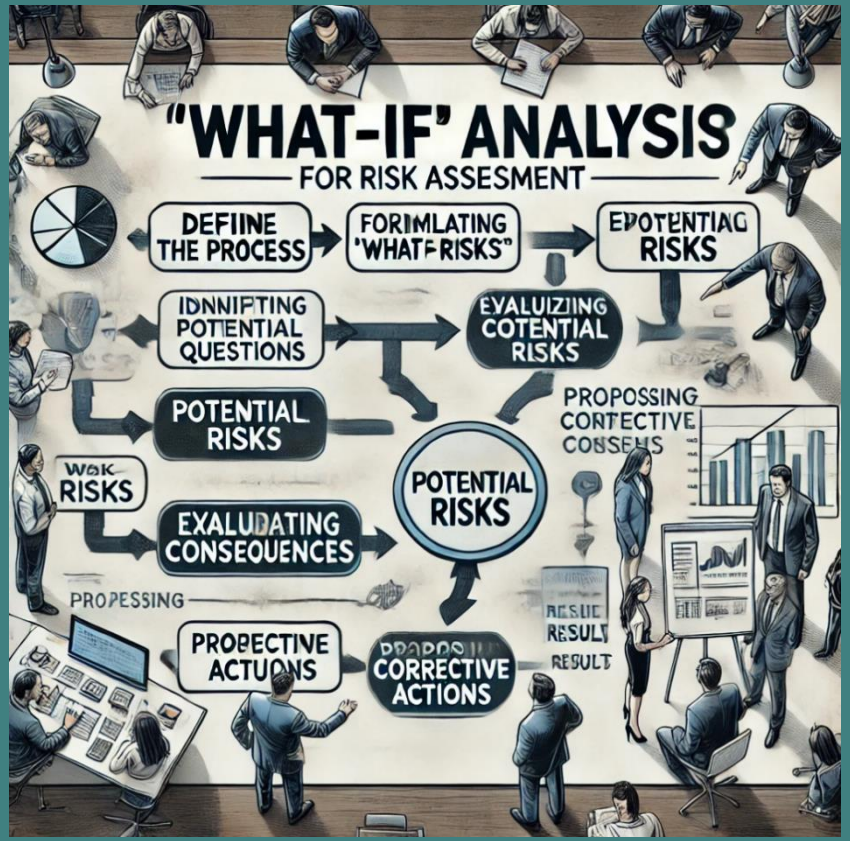
- Prevenzione degli Incidenti: L'identificazione e la mitigazione degli errori umani aiutano a ridurre la probabilità di incidenti.
- Miglioramento delle Procedure: Spesso gli errori umani sono causati da problemi nelle procedure. L'analisi permette di rivedere e migliorare questi aspetti.
- Formazione: Identificare le carenze permette di fornire una formazione mirata per migliorare la performance degli operatori.

L'analisi dell'errore umano è una componente critica nella gestione della sicurezza industriale, specialmente nei settori dove i rischi possono avere conseguenze gravi. La comprensione delle cause degli errori umani e la progettazione di sistemi resilienti contribuiscono notevolmente alla sicurezza complessiva dei processi.

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



# WHAT IF analysis



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

# WHAT IF

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

Cosa sarebbe successo se Helen Quilley, la protagonista di *Sliding doors* avesse preso la metropolitana?

E se invece l'avesse persa?
Che direzioni avrebbe imboccato la sua vita in una o l'altra situazione?
Non è una novità: **il segreto di una scelta giusta sta nel prendere le decisioni migliori.**

E per prenderle occorre analizzare e valutare una serie di variabili.
Poter prevedere quello che può accadere non è solo un qualcosa che succede sul grande schermo o nei romanzi di fantascienza.

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

# WHAT IF

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

Il metodo "cosa - se" ("WHAT - IF" Method) è un metodo induttivo. Per applicazioni relativamente semplici, si prendono in esame la progettazione, il funzionamento e l'uso di una macchina. In corrispondenza di ogni passo, vengono formulate le domande "cosa - se" ("WHAT - IF" Method) e ad esse vengono fornite delle risposte per valutare gli effetti dei guasti dei componenti o degli errori procedurali sulla creazione di pericoli sulla macchina.
Per applicazioni più complesse, è possibile applicare nel modo migliore il metodo "cosa - se" ("WHAT - IF" Method) attraverso l'uso di una "lista di controllo" ("check - list"), e distribuendo il lavoro allo scopo di affidare alcuni aspetti dell'uso della macchina alle persone che hanno la maggiore esperienza o capacità nella valutazione di tali aspetti.
Si valutano le tecniche utilizzate dall'operatore e la sua conoscenza del lavoro. Si valuta l'adeguatezza dell'attrezzatura, la progettazione della macchina, il suo sistema di comando e il suo equipaggiamento di sicurezza. Si esaminano gli effetti del materiale che viene lavorato, e si verificano le registrazioni relative al funzionamento e alla manutenzione.

**OBIETTIVI: Analisi sistematica di singole apparecchiature dell'impianto. Individuazione delle sorgenti di rischio e loro classificazione. Proposta di soluzioni alternative per ridurre le conseguenze.**

- **Campo di applicazione:** sia in fase di progetto che di gestione.
- **Metodologia:** identificazione delle componenti dell'impianto a rischio, nomina di un team multidisciplinare. Creazione della documentazione su: sostanze, processo, PFD (process flow design) e P&ID (piping & instrumentation diagram), procedure operative e manutentive, dispositivi di sicurezza.
- **Pro:** tecnica analitica e semplice, costi ridotti, qualità dei risultati.
- **Contro:** dipendenza dall'esperienza del team multidisciplinare di analisi. Carattere ancora qualitativo e non completamente quantitativo dell'analisi.

Prof. Claudio Pantanali, PhD cpantanali@units.it


**CARATTERISTICHE**

La base di partenza è una Safety Review con applicazione, nella versione più dettagliata, componente per componente. Con essa vengono considerate le sequenze di eventi imprevisti identificandone al tempo stesso le probabili conseguenze e di queste le varie combinazioni e i mezzi per ridurle; tutto questo esaminando le divergenze rispetto al disegno e alla costruzione d'origine dell'impianto. E' così chiamata perchè pone domande che iniziano con "What if"; le domande costituiscono poi vari gruppi secondo l'area studiata (per es. Sicurezza del personale, Antincendio,) e ognuna di queste è seguita da un team di 2-3 esperti.

**VANTAGGI**

Rende più completa la Safety Review, ma risulta essere meno utilizzabile come fonte d'informazioni per altri tipi d'analisi.
Fra i suoi scopi primari è compresa la stima delle conseguenze del "peggior caso" verificabile.
Ha il pregio di poter essere applicata, secondo le esigenze, più o meno dettagliatamente.

**SVANTAGGI**

Applicata dettagliatamente può essere molto onerosa senza però ottenere il grado di completezza dell'HAZOP essendo, rispetto a quest'ultima e anche all'FMECA, meno strutturata.

**APPLICAZIONE**

Rara e ci sono pochissime pubblicazioni a riguardo.
E' comunemente applicata ad impianti esistenti e nel caso di proposte di modifiche relative agli stessi.
I tempi e i costi per la sua applicazione sono proporzionali al tipo di impianto e al numero delle "aree" oggetto dello studio.

**COMMENTI**

Nell'ambito dell'industria si fa spesso riferimento a questa procedura; può rivelarsi potente se applicata da un esperto.
I dati richiesti per una sua applicazione sono costituiti dalla documentazione relativa all'impianto, alle procedure e al processo più le interviste fatte al personale operativo.

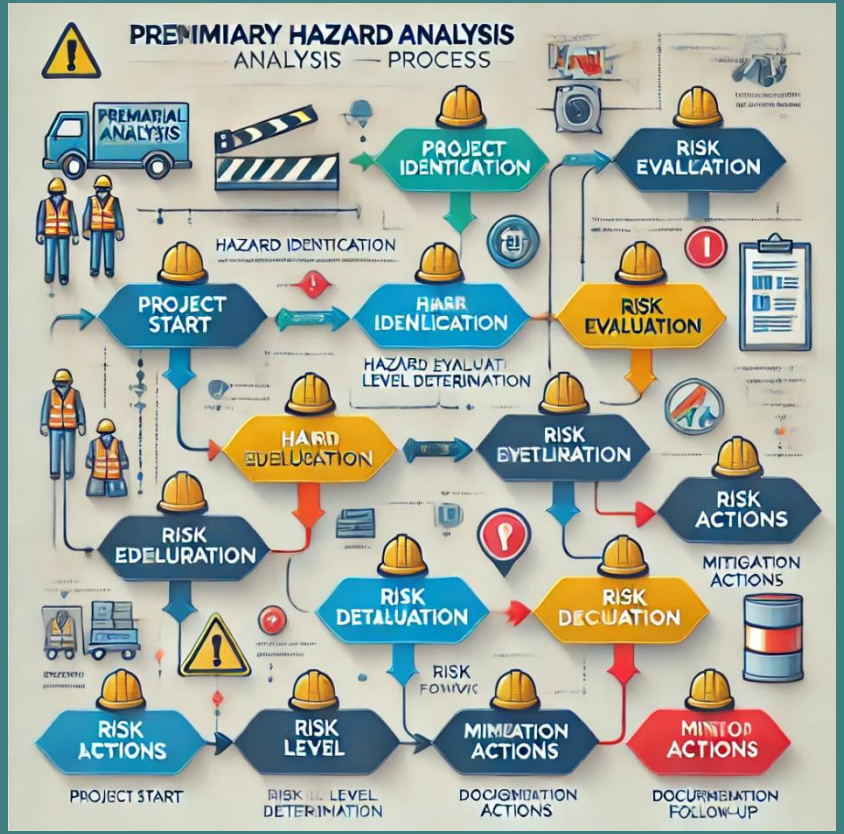
DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

# PHA

## Preliminary Hazard Analysis

## Analisi Preliminare dei Pericoli



Prof. Claudio Pantanali, PhD cpantanali@units.it

# Preliminary Hazard Analysis



## ANALISI PRELIMINARE DEI PERICOLI

Attività effettuata nella fase iniziale di progettazione (fase concettuale) di un sistema in sicurezza durante la quale, a partire da una preliminare lista di pericoli generici identificabili nel settore (PHI - Preliminary Hazard Identification), vengono individuati i possibili pericoli (Hazard), con i relativi rischi (**Risk**) di danno (Harm) in caso di funzionamento normale o in emergenza.

Una volta individuati i pericoli connessi al sistema, viene analizzata e determinata per ognuno di essi la categoria qualitativa del rischio e le relative azioni di protezione (QRC-A Qualitative Risk Categories and Actions).

In particolare, per ogni causa di hazard qualitativamente elevata ("intolerable" o "undesirable"), vengono individuati i provvedimenti (contromisure) che devono essere adottati per la riduzione dei relativi rischi, e quindi viene ridefinita la categoria qualitativa di rischio residua; i provvedimenti devono essere tali che la categoria residua non sia ancora "intolerable" o "undesirable", ma "tolerable" o "negligible".

Quindi viene effettuata la valutazione e l'accettazione del rischio (REA Risk Evaluation and Acceptance) in funzione della frequenza degli eventi pericolosi (FHE Frequency of occurrence of Hazardous Events o HFR Hazardous Failure Rate) e del livello di gravità del pericolo (HSL Hazard Severity Level).
In questa fase concettuale viene anche definito, in via preliminare tramite la Safety Integrity Level Definition (SIL-D), il livello di sicurezza che deve avere globalmente il sistema (pSysSIL Preliminary System Safety Integrity Level o pSIL) in termini di autoprotezioni (immunità) da guasti pericolosi (Safety Integrity, Inerranza*); per esempio, se vi sono dei pericoli che possono presentarsi con alto livello di probabilità (FHE) e con gravi effetti (HSL), il sistema deve avere caratteristiche tali che il proprio livello di sicurezza, per immunità da guasti pericolosi, sia pari a un fattor e sicurezza 4 (pSysSIL o pSIL 4)

* Immunità da **guasti** pericolosi. **Caratteristica** di **progettazione**, realizzazione e operativa di **un sistema** in **un** modo tale che è sempre preciso e sempre corretto, in **un** modo che non manca mai di raggiungere gli obiettivi per cui è destinato; per cui **il sistema** opera infallibilmente

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

# Preliminary Hazard Analysis

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

CARATTERISTICHE

E' utilizzata nella fase di ideazione dell'impianto o quando il progetto è ancora scarsamente dettagliato o se l'esperienza precedente non può fornire quei dati necessari alla sicurezza e alle procedure adottate.
L'analisi procede sistema per sistema o item per item dando un giudizio di criticità di tipo semi-quantitativo.

VANTAGGI

Si dimostra molto flessibile e può essere considerata un precursore per l'applicazione di altre metodologie quali l'FTA o altri. Avendo come scopo quello di riconoscere con anticipo i rischi questo si traduce in un risparmio di tempo e di denaro in quanto i rischi possono essere ridotti o quantomeno controllati già ad uno stadio iniziale. Può essere molto utile per la scelta del luogo in cui costruire l'impianto; Indica direttive da adottare in fasi successive di progettazione di dettaglio o che si riveleranno utili per la stesura delle istruzioni da fornire al futuro utilizzatore o per le operazioni di manutenzione

SVANTAGGI

- Non garantisce carattere di sistematicità, nè per l'identificazione dei rischi che per l'individuazione delle cause.
- Possibile incompletezza nella valutazione dei rischi.
- Incapacità di valutare gli effetti di guasti combinati.

APPLICAZIONE

Relativamente frequente; viene applicata più o meno dettagliatamente o autonomamente, o sulla base di una Safety Review, rendendola però più completa. Questo tipo di analisi deve essere preferibilmente condotta da 1 o 2 tecnici esperti nel settore della sicurezza.

COMMENTI

Il risultato finale consiste in una elencazione dei rischi relativi all'impianto e ai materiali (allo stato grezzo e come prodotto finito), e in una serie di consigli ai progettisti onde ridurre gli incidenti. A volte è adottata come sistema di revisione.

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

# Preliminary Hazard Analysis

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

L'Analisi Preliminare dei Pericoli (PHA - Preliminary Hazard Analysis) è una metodologia utilizzata per identificare e valutare potenziali rischi e pericoli in fase iniziale di un progetto o processo industriale. L'obiettivo principale della PHA è prevenire incidenti e garantire un ambiente di lavoro sicuro. Viene spesso utilizzata durante le fasi di progettazione, sviluppo o modifica di un sistema, per anticipare potenziali rischi prima che il progetto venga implementato.

Ecco alcune caratteristiche principali della PHA:

1. Identificazione dei Pericoli: La PHA aiuta a identificare i possibili pericoli associati a un processo, come rischi chimici, fisici, meccanici, elettrici o ambientali.

2. Analisi Qualitativa: L'analisi preliminare dei pericoli è solitamente di tipo qualitativo. Si basa sull'esperienza degli esperti, sui dati storici e su altre informazioni pertinenti per valutare i rischi senza entrare in dettaglio quantitativo.

3. Assegnazione di Livelli di Rischio: La PHA assegna un livello di rischio a ciascun pericolo identificato. Questo livello può essere determinato considerando la probabilità che un pericolo si verifichi e le conseguenze che potrebbe avere.

4. Mitigazione del Rischio: Dopo aver identificato i potenziali rischi, la PHA propone misure preventive e di mitigazione per ridurre al minimo la probabilità di incidenti o le loro conseguenze.

5. Documentazione: La PHA documenta i risultati in modo strutturato, includendo una descrizione dei pericoli, le cause potenziali, la valutazione del rischio e le misure raccomandate.

La PHA è utile per fornire una panoramica iniziale sui potenziali rischi e consente di pianificare misure preventive, come modifiche di progettazione, pratiche operative sicure o requisiti di formazione. Tuttavia, in fase successiva del progetto, si possono adottare altre metodologie di analisi più dettagliate, come HAZOP (Hazard and Operability Study) o FMEA (Failure Modes and Effects Analysis).

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

# Preliminary Hazard Analysis

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

**Contesto**: Un impianto di stoccaggio di gas naturale è in fase di progettazione. Prima di costruire il sistema, viene condotta una PHA per identificare e valutare i potenziali pericoli associati all'impianto.

**Spiegazione degli Elementi:**

1. **Pericolo**: Descrive il tipo di rischio o pericolo presente nell'impianto, come ad esempio il rilascio di gas naturale.
2. **Conseguenze Potenziali**: Identifica quali potrebbero essere le conseguenze nel caso in cui il pericolo si verifichi, come un incendio o un'esplosione.
3. **Causa Potenziale**: Elenca le possibili cause che potrebbero portare al verificarsi del pericolo, come una fuga da un giunto non sigillato.
4. **Probabilità**: Stima la probabilità che l'evento si verifichi (alta, media, bassa).
5. **Conseguenza**: Classifica la gravità dell'evento (bassa, media, elevata, catastrofica).
6. **Livello di Rischio**: Combina la probabilità e la conseguenza per determinare un livello di rischio complessivo.
7. **Azioni di Mitigazione**: Descrive le azioni da intraprendere per ridurre al minimo il rischio, come installare rilevatori di gas o eseguire manutenzione preventiva.

Questo tipo di analisi permette al team di progettazione di identificare e mitigare i pericoli prima della costruzione dell'impianto, garantendo così un ambiente più sicuro per i lavoratori e prevenendo incidenti costosi o catastrofici.

**Tabella di PHA:**

| Pericolo | Conseguenze Potenziali | Causa Potenziale | Probabilità | Conseguenza | Livello di Rischio | Azioni di Mitigazione |
|---|---|---|---|---|---|---|
| Rilascio di gas naturale | Incendio o esplosione | Fuga da un giunto non sigillato | Media | Elevata | Elevato | Installare rilevatori di gas, migliorare la qualità delle guarnizioni, formare il personale sulle procedure di emergenza. |
| Surriscaldamento serbatoio | Danneggiamento del serbatoio, rilascio | Malfunzionamento del sistema di raffreddamento | Bassa | Elevata | Moderato | Manutenzione preventiva del sistema di raffreddamento, installazione di allarmi di temperatura. |
| Sovrapressione nel serbatoio | Scoppio del serbatoio | Malfunzionamento della valvola di sicurezza | Bassa | Catastrofica | Elevato | Test regolari delle valvole di sicurezza, installazione di una valvola di sicurezza ridondante. |
| Scariche elettrostatiche | Incendio nei pressi di gas infiammabile | Mancanza di messa a terra | Media | Elevata | Elevato | Installare un sistema di messa a terra, formazione del personale sulle procedure antistatiche. |

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Preliminary Hazard Analysis



**OBIETTIVI: analisi ed identificazione delle sorgenti di pericolo con scopo l'incremento della sicurezza tramite modifiche di progetto o definizione di condizioni operative diverse.**

- **Campo di applicazione:** nelle fasi di progettazione dell'impianto o del processo in relazione alle sostanze, componenti, materiali, utilities, condizioni operative, fattori ambientali.
- **Metodologia:** analisi storica e conoscenze accumulate rispetto allo specifico processo ed alle apparecchiature coinvolte. Interazione continua tra progettisti ed esperti della sicurezza
- **Pro:** semplicità e basso costo (se opera in fase di progettazione)
- **Contro:** natura qualitativa del metodo ; dipendenza dei risultati dall'esperienza e qualificazione del team di analisi. Limitatezza dei dati disponibili.

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

# Preliminary Hazard Analysis
## I passi della valutazione del rischio

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

## 1. Preliminary Hazard List (PHL)

- Creare il gruppo di lavoro
- Studiare i casi di incidenti passati, disegni, dati disponibili riferiti a casi analoghi
- Parlare con i futuri utenti, verificare il processo o l'impianto
- Passare in rassegna tutte le norme in materia – controllare i disegni tecnici e i P&I
- Studiare i rapporti di manutenzi9one, etc.

## 2. Divisione della PHL in sottocategorie definite da una particolare tipologia di rischio

| Function | |
|---|---|
| Fails to operate | Hazards |
| Operates incorrectly | |
| Operates inadvertently | |
| Operates at wrong time | |
| Unable to stop operation | |
| Receives erroneous data | |
| Sends erroneous data | |
| Conflicting data information | |

## 3. Correlazione di rischi apparentemente indipendenti

1.Individuare, all'interno del sistema, gli elementi che, per natura delle sostanze o per condizioni operative o per esperienza, possono essere considerati pericolosi.

2.Per ogni elemento, cercare un evento/causa che costituisce una condizione potenziale pericolosa (triggering event 1) ed analizzarlo in dettaglio.

3.Cercare un evento/causa che opera da innesco per il manifestarsi di un evento incidentale (triggering event 2) ed analizzarlo in dettaglio.

4.Prevedere le conseguenze e classificarle in base alla gravità (p.e. in una scala da1 a 4)

5.Proporre misure correttive

6.Reiterare dal passo (2)

## 4. Rating del rischio

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Preliminary Hazard Analysis
esempio



Reattore di ossidazione a base di perclorato metallico alcalino

| 1) Elemento pericoloso | 2) Triggering Event 1 | 3) Condizione pericolosa creatasi | 4) Triggering Event 2 | 5) Effetti | 6) Possibili conseguenze | 7) Azioni correttive |
|---|---|---|---|---|---|---|
| **Ossidante Forte** | Contamina-zione da olio di lubrificaz. | Possibilità di reazione RedOx violenta | Energia di attivazione presente | Esplosione | Danni a persone e a cose in un raggio esteso | Mantenere l'ossidante ad adeguata distanza da tutte le possibili sorgenti di contaminazione |
| . | . | . | . | . | . | . |

Approccio induttivo

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



# Metodi basati sul concetto di barriere

Prof. Claudio Pantanali, PhD cpantanali@units.it


La gestione del rischio una volta completate analisi del contesto e valutazione dei rischi si traduce quasi interamente nella gestione delle misure di controllo del rischio, ovvero delle barriere. Gestire il rischio nel tempo, assicurandosi che esso rimanga entro certi valori di accettabilità, significa di fatto assicurarsi che le misure poste in essere dall'organizzazione
per contenere il rischio restino integre, efficaci ed efficienti nel tempo. Partendo da semplice riflessione, vengono qui presentati due metodi di analisi del rischio basati sul concetto di barriere.

Essi offrono quindi una prospettiva diversa della gestione del rischio, ponendosi come strumenti a supporto di un intero sistema di gestione del rischio che intenda adottare la prospettiva *barrier-based* che va affermandosi non solo nelle norme tecniche di adozione volontaria, ma anche nelle leggi degli stati sovrani (si pensi, come recente esempio, all'obbligo imposto dalla L. 132/2018 di redazione del Piano di Emergenza.

Interno per i gestori degli impianti di stoccaggio e lavorazione dei rifiuti, ove si parla esplicitamente di individuazione e gestione delle misure di controllo del rischio). La barriera è quindi una misura di controllo o raggruppamento di elementi di controllo che, di per sé, può prevenire lo sviluppo di una causa in un *top event* (barriera preventiva) o può mitigare le
conseguenze del top event una volta che questo si è manifestato (barriera mitigativa).

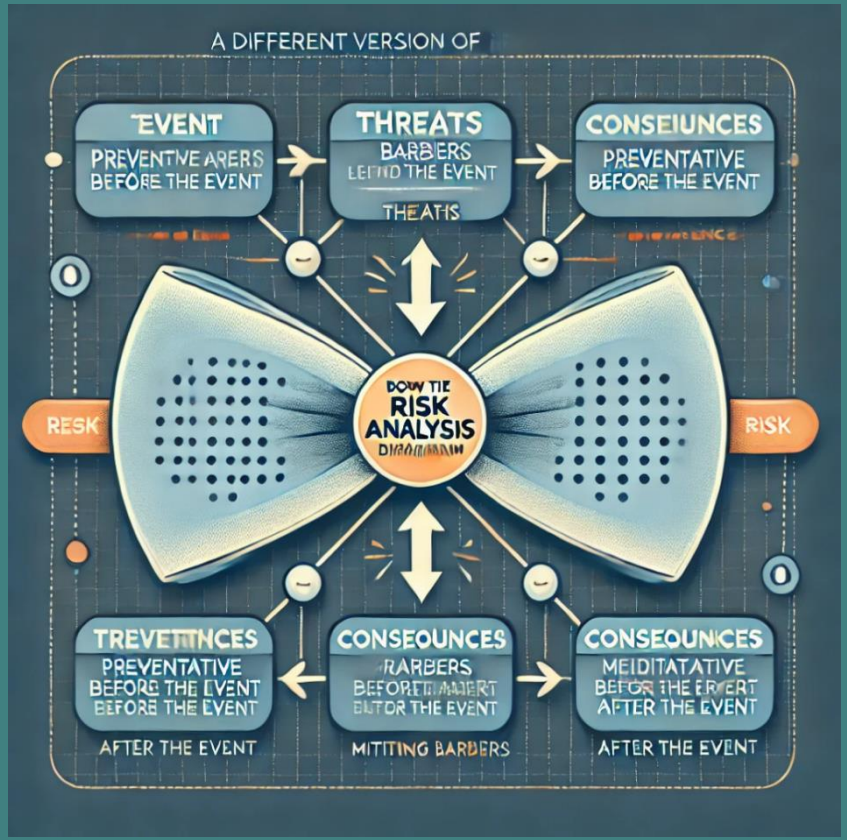
**Barriere (o Misure di Controllo)**
Le barriere sono misure o strumenti progettati per ridurre o prevenire l'accadimento di un rischio. Esistono diversi tipi di barriere che si possono applicare per minimizzare i rischi:

- **Barriere fisiche**: Come dispositivi di protezione individuale, recinzioni, o sistemi di contenimento per proteggere le persone o le attrezzature.
- **Barriere tecniche**: Sistemi di allarme, sistemi di spegnimento automatico, e altri dispositivi tecnologici progettati per ridurre il rischio.
- **Barriere organizzative**: Procedure operative, formazione del personale, e piani di risposta alle emergenze che possono aiutare a prevenire o gestire il rischio.
- **Barriere amministrative**: Linee guida, regolamenti, e altre politiche che aiutano a mantenere le attività entro limiti sicuri.

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



# BOW TIE

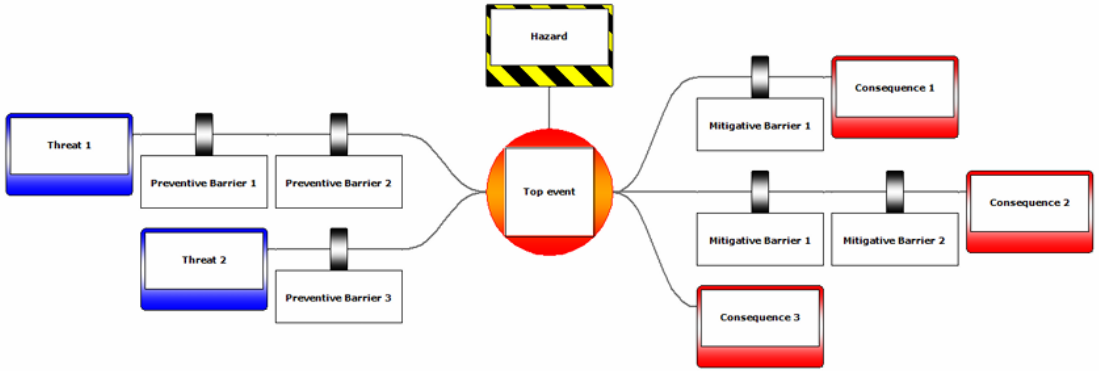


DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it

# Bow Tie

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

BowTie: **strumento** di analisi del rischio dalla caratteristica forma a «farfallino»




BowTie: **metodologia** di analisi del rischio (quantificazione frequenze)

I metodi basati sul Bow-Tie hanno origine negli anni settanta a partire dai più conosciuti diagrammi causa conseguenze (CCD) successivamente adattati (1979, David Gill, Imperial Chemical Industries) per l'impiego ai fini della investigazione post incidentale. Ottennero una vastissima diffusione nei primi anni novanta quando, a seguito dell'incidente occorso a bordo della piattaforma Piper Alpha (Mare del Nord, 6 luglio 1988, 167 morti), la società Royal Dutch/Shell Group mise a punto, codificandone il flusso di applicazione, una tecnica per migliorare la gestione, negli anni a venire, delle attività di analisi del rischio.

L'applicazione della metodologia si estese rapidamente ad altre società e ad altri campi ed in primis, nel mondo anglosassone, a tutti quei casi ove era evidente la complessità della realtà da analizzarsi e le peculiarità di alcune installazioni (es. le infrastrutture di trasporto), tipo la presenza di moltitudini di persone, sottoservizi speciali, etc.

Al momento, sono estesamente impiegati nell'analisi del rischio industriale e del rischio d'incendio

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

# Bow Tie

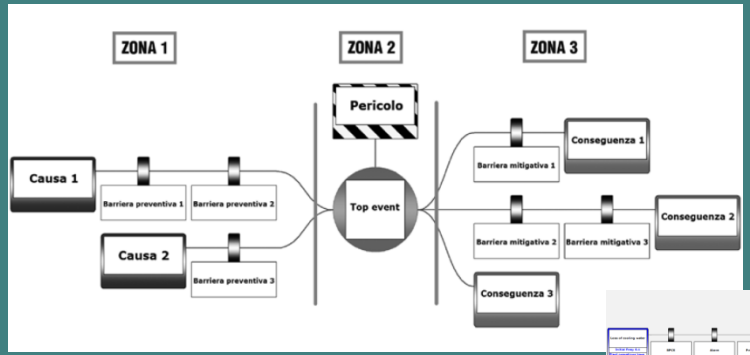
DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

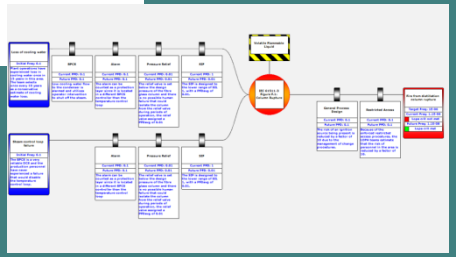
Il Bow-Tie, grazie alla sua potente capacità di comunicare le informazioni graficamente, si è affermato come la tecnica principe di analisi del rischio basata sul concetto di barriere. Ad esso, quale metodologia privilegiata dagli autori del volume per la illustrazione dei principi della ISO 31000; in questo paragrafo si vuole quindi fornire una semplice introduzione al metodo. La tecnica Bow-Tie prevede lo sviluppo di diagrammi logici di flusso sviluppati in tre zone distinte. Un esempio di diagramma Bow-Tie è riportato in Figura

La **Zona 1** (Prevenzione) è rappresentata sul lato sinistro del diagramma; identifica tutte le cause (rettangoli di colore blu) associabili all'evento indesiderato e, per ognuna di esse, evidenzia tutti gli specifici sistemi di protezione (sia impiantistici che di controllo operativo) che contribuiscono a prevenire l'evento indesiderato. La Zona 1 può essere considerata equivalente ad un albero dei guasti semplificato.

La **Zona 2** *(Top Event)* è rappresentata al centro del diagramma e identifica in modo univoco il pericolo considerato (rettangolo a strisce gialle e nere) l'evento incidentale primario detto *Top Event* (cerchio di colore rosso); tale evento può a sua volta evolvere, in base alla dinamica dell'incidente in scenari incidentali alternativi tra loro.

La **Zona 3** (Protezione) identifica tutti gli scenari incidentali potenzialmente generati (es: getto di gas incendiato, esplosione, *flash fire* ecc…) e la combinazione di tutti gli elementi che ne consentono lo sviluppo, includendo tutti i sistemi di protezione che possano mitigarne gli effetti. La Zona 3 può a tutti gli effetti essere considerata equivalente ad un albero degli eventi semplificato.



La tecnica *Bow-Tie* permette di identificare e valutare le frequenze e le conseguenze associate agli scenari e di quantificare il contributo dei sistemi protettivi e mitigativi (barriere) in condizioni di normale produzione.; tuttavia è bene prima introdurre la metodologia di analisi che è alla base della quantificazione in frequenza dei *Bow-Tie*: l'analisi LOPA.

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

# Bow Tie

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

## 1. Struttura del Bow-Tie Analysis

Il modello Bow-Tie è strutturato in tre sezioni principali:

- **Evento centrale (Top Event)**: è l'evento indesiderato o critico che si cerca di prevenire o mitigare. Questo è il punto di riferimento centrale dell'analisi.
- **Cause**: situate a sinistra del Top Event, sono i fattori o gli eventi che possono portare al verificarsi dell'evento centrale. Le cause sono legate all'evento centrale tramite barriere preventive.
- **Conseguenze:** poste a destra del Top Event, rappresentano gli impatti o le conseguenze che si verificano se l'evento centrale avviene. Le conseguenze sono associate a misure di contenimento o mitigazione.

## 2. Barriere Preventive e Mitigative

Uno degli elementi chiave del Bow-Tie Analysis è l'identificazione delle **barriere**:

- **Barriere preventive:** sono azioni o misure che possono essere implementate per impedire il verificarsi dell'evento centrale. Possono includere controlli, ispezioni, training o politiche di sicurezza.
- **Barriere mitigative:** sono misure implementate per ridurre l'impatto o le conseguenze negative dell'evento centrale nel caso in cui si verifichi. Queste includono piani di risposta alle emergenze, sistemi di rilevamento e risoluzione rapida.

Le barriere possono essere di tipo **attivo** o **passivo**. Le barriere attive richiedono un'azione specifica o un intervento umano, mentre quelle passive sono soluzioni tecniche o strutturali che funzionano senza interventi.

## 3. Vantaggi del Bow-Tie Analysis

- **Chiarezza visiva**: il diagramma facilita la comprensione rapida dei rischi, delle cause e delle misure di controllo. È particolarmente utile per presentare i rischi a team non tecnici o a stakeholder aziendali.
- **Facilità di comunicazione**: la rappresentazione visiva aiuta a discutere i rischi e le strategie di mitigazione con facilità tra team interfunzionali.
- **Identificazione delle lacune**: evidenziando le barriere esistenti e mancanti, il Bow-Tie Analysis aiuta a individuare le aree che necessitano di ulteriori controlli o miglioramenti.

Prof. Claudio Pantanali, PhD cpantanali@units.it

# Bow Tie



**4. Passaggi per Eseguire un Bow-Tie Analysis**

Ecco i passaggi generali per sviluppare un'analisi Bow-Tie:

- **Definire il Top Event**: identificare l'evento critico e collocarlo al centro dell'analisi.
- **Identificare le cause**: elencare i fattori che possono portare al verificarsi del Top Event.
- **Identificare le conseguenze**: specificare gli impatti e le conseguenze potenziali dell'evento critico.
- **Definire le barriere preventive e mitigative**: per ogni causa e conseguenza, specificare le barriere necessarie per prevenire o ridurre gli effetti dell'evento critico.
- **Valutare l'efficacia delle barriere**: analizzare se le barriere sono sufficienti o se è necessario introdurre ulteriori misure.

**5. Applicazioni del Bow-Tie Analysis**

Il Bow-Tie Analysis è usato in settori che vanno dalla sicurezza industriale e dai processi chimici alla gestione del rischio nelle attività finanziarie. Le applicazioni includono:

- **Gestione dei rischi di sicurezza** in industrie come quella petrolifera, chimica o nucleare, dove la prevenzione degli incidenti è cruciale.
- **Progetti di gestione dei rischi aziendali** nelle organizzazioni, per identificare e mitigare i rischi operativi.
- **Settori di compliance e audit** in cui i rischi sono legati alla conformità normativa o alle politiche aziendali.

**6. Limitazioni del Bow-Tie Analysis**

Sebbene sia uno strumento potente, il Bow-Tie Analysis presenta alcune limitazioni:

- **Non considera la probabilità dei rischi**: si concentra principalmente sulle cause e conseguenze, ma non analizza direttamente la probabilità di accadimento del rischio.
- **Non include l'interdipendenza tra i rischi**: i rischi complessi o sistemici potrebbero richiedere analisi supplementari.
- **Richiede un'esperienza specifica per essere implementato correttamente**: la creazione delle barriere e la definizione delle cause e conseguenze necessitano di una profonda conoscenza del contesto.

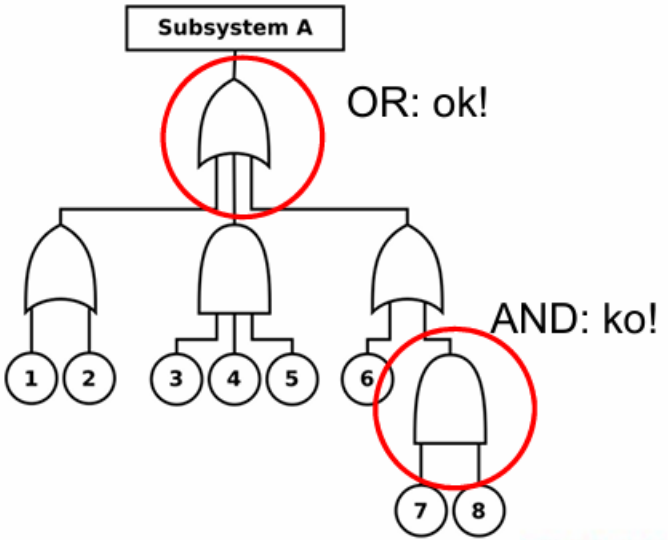
Il Bow-Tie Analysis è quindi uno strumento molto efficace per la visualizzazione e la gestione dei rischi, con un approccio basato sulle cause e sulle conseguenze, che permette di organizzare e comunicare in modo chiaro i meccanismi di rischio e le misure di protezione aziendali.

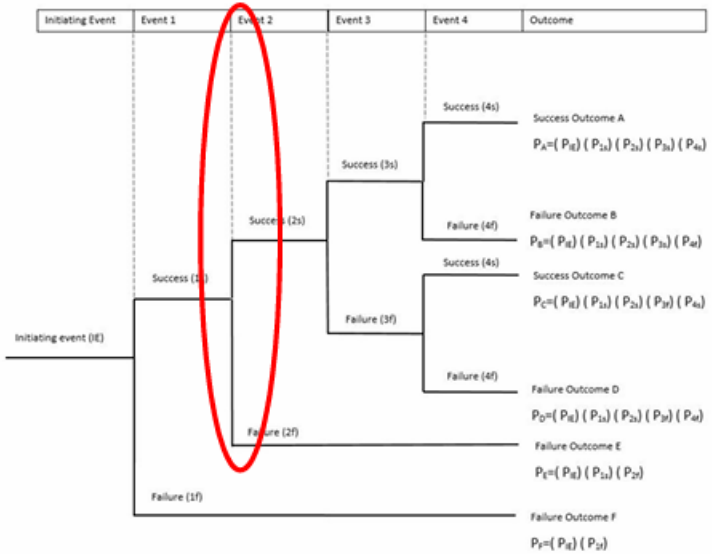
# Bow Tie



**BowTie = Albero dei guasti + Albero degli eventi**

Vero, ma occorre prestare attenzione alle combinazioni logiche delle cause e degli eventi.

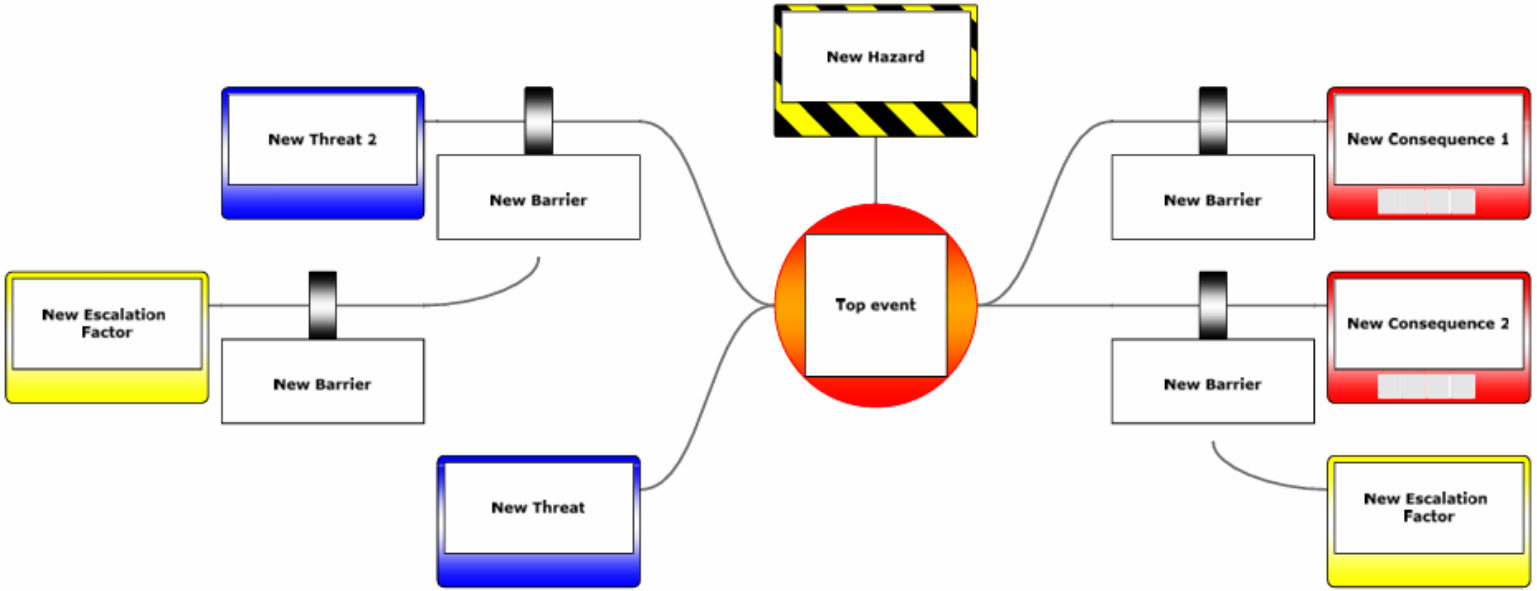


# Bow Tie



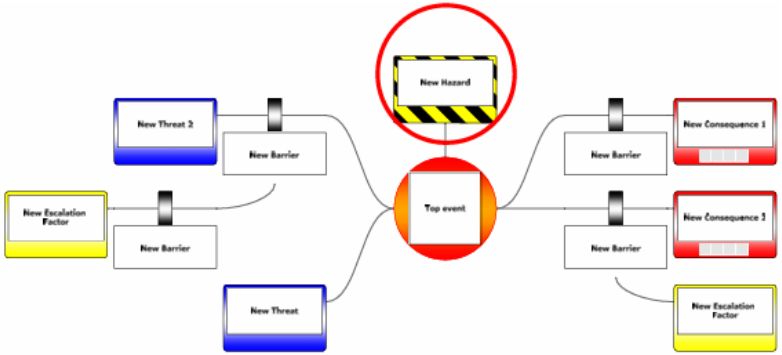
## Elementi tipici di un BowTie



# Bow Tie



## Hazard




La parola «pericolo» suggerisce qualcosa di non voluto. Indica una condizione (un'attività o uno stato di qualcosa ) **potenzialmente** in grado di generare conseguenze indesiderate È insita nelle attività produttive.

Es: idrocarburi in pressione, tensione > 440 V, ecc…

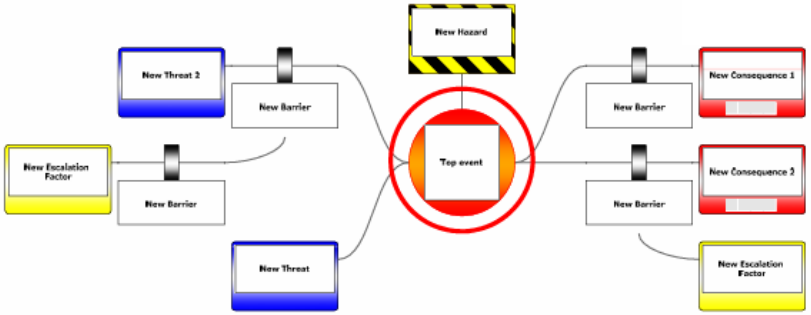
Il «pericolo» deve essere gestito: finché è sotto controllo, è tutto ok.

***Suggerimento!***
Usa la classificazione dell'**ISO 17776** sui possibili pericoli.

# Bow Tie



## Top event




Certe cause possono determinare una deviazione o una **perdita di controllo** sul pericolo. Tale evento è il top event.

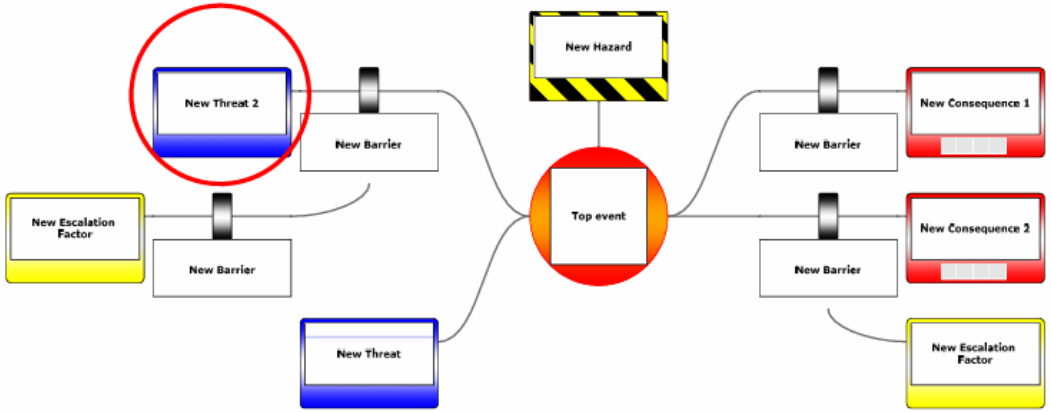
Es: Perdita di contenimento del blend, perdita di controllo elicottero, ecc…

Non è ancora un incidente grave (*major accident*), ma se non mitigato correttamente può evolvere in una o più conseguenze non volute (incendio, esplosione…).

# Bow Tie



## Cause




Le «cause» (ma in inglese *threats,* minacce) sono i fattori che **potrebbero** causare il top event.

Ogni causa individuata deve avere la potenzialità di causare **autonomamente** il top event.

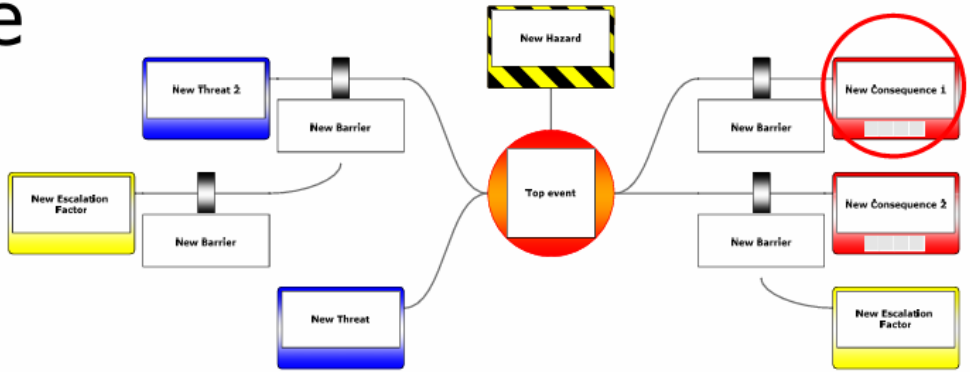
Es: corrosione, deviazioni di processo, collisioni nave, collisioni elicottero, ecc…

Le cause sono cioè **indipendenti** l'una dall'altra (nell'analisi LOPA, si combinano **solamente tramite porte OR**).

# Bow Tie



## Conseguenze




Una conseguenza è un potenziale evento risultante dalla perdita di controllo su un pericolo (cioè da un top event), che **implica direttamente una perdita o un danno**.

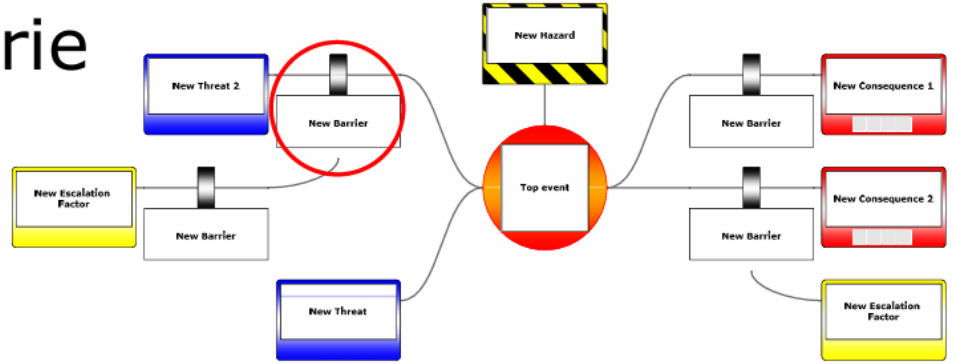
Es. pool fire in coperta, oil spill in mare, caduta elicottero in mare

Si tratta di quegli eventi che un'organizzazione vuole evitare a tutti i costi (o, meglio, ai costi giustificati da uno studio ALARP).

# Bow Tie



## Barriere primarie

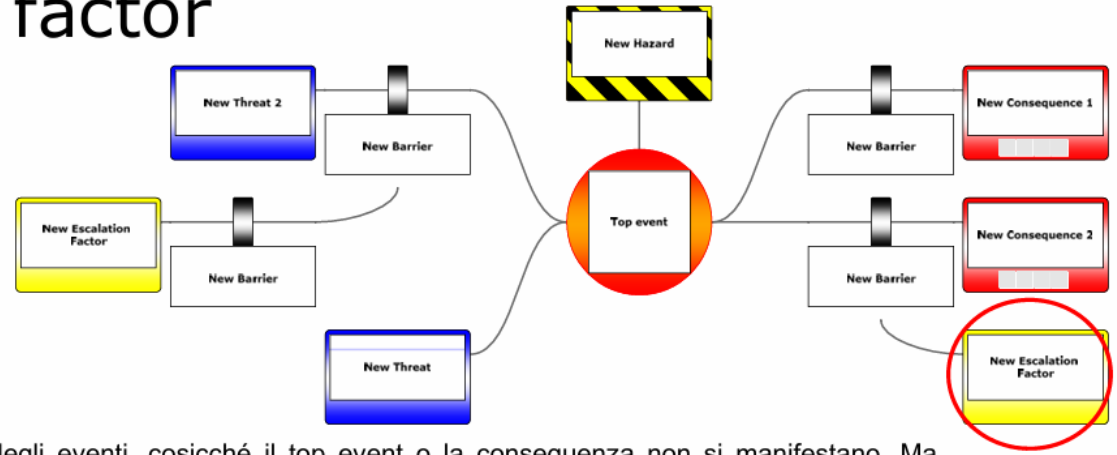



Il *risk management* è incentrato sul controllo del rischio. Ciò viene fatto piazzando le barriere (o misure di controllo) per prevenire o mitigare certi eventi.
Una barriera può essere qualsiasi misura presa contro una «forza» indesiderata, al fine di mantenere un desiderato stato.

Nei BT, si distinguono barriere preventive (sx) e barriere mitigative (dx).

Es: Piano di ispezione e manutenzione (preventiva);
Es: Bacino di contenimento (mitigativa).

# Escalation factor



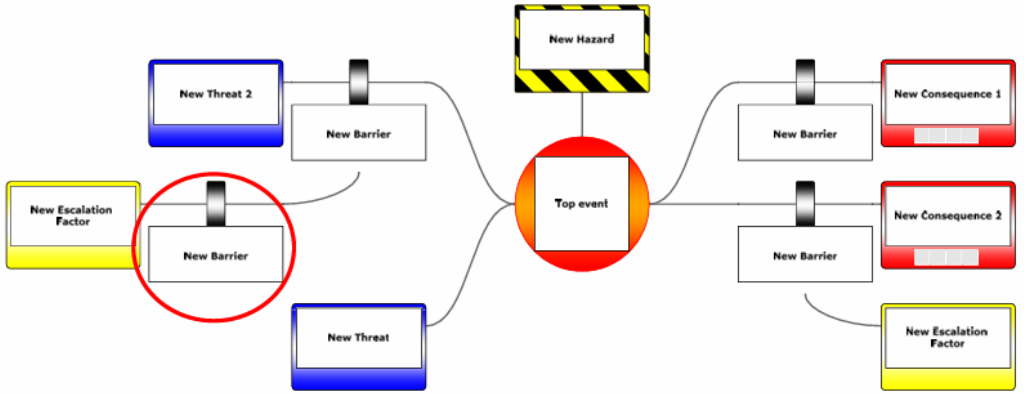

Idealmente, una barriera arresta il flusso degli eventi, cosicché il top event o la conseguenza non si manifestano. Ma nessuna barriera è efficace al 100%. Sotto certe condizioni, una barriera può fallire. Queste condizioni sono chiamate «escalation factor».

Es: condizioni meteomarine avverse (impediscono esecuzione dei piani di emergenza antinquinamento); mancanza di energia elettrica; mancanza di aria strumenti.

# Bow Tie



## Barriere secondarie




A garanzia che un escalation factor non minacci la barriera primaria, possono essere individuate le c.d. barriere secondarie.

Es: diesel generatore di emergenza, pompa antincendio di emergenza, utilizzo del disperdente previa autorizzazione ministeriale

# Definizione dei tipi di barriera


| Barrier type | Detect | Decide | Act |
|---|---|---|---|
| Passive Hardware | N/A | N/A | N/A |
| Active Hardware | Technology | Technology | Technology |
| Active Human | Human | Human | Human |
| Hardware + Human | Technology/Human | Technology/Human | Technology/Human |
| Continuous Hardware | N/A | N/A | Technology |

# Criteri di validità di una barriera

- **Pienamente funzionante**: la barriera è capace di prevenire il *top event* o di mitigare una *conseguenza*, agendo come e quando previsto, con un effetto misurabile.
- **Indipendente**: la barriera ha un impatto diretto e indipendente sulla causa, top event, o conseguenza. L'indipendenza esclude quelle barriere che condividono cause comuni di guasto o modi di fallimento.
- **Valutabile**: la barriera deve poter essere valutata per verificare le sue prestazioni attese (probabilità di fallimento della barriera, PFD).

# Analisi LOPA con i BowTie

È possibile quantificare i BT, usando l'analisi dei livelli di protezione indipendenti (LOPA).

Input: frequenze cause, Probabilità di fallimento su richiesta (PFD) barriere;
Output: frequenze top event e conseguenze.

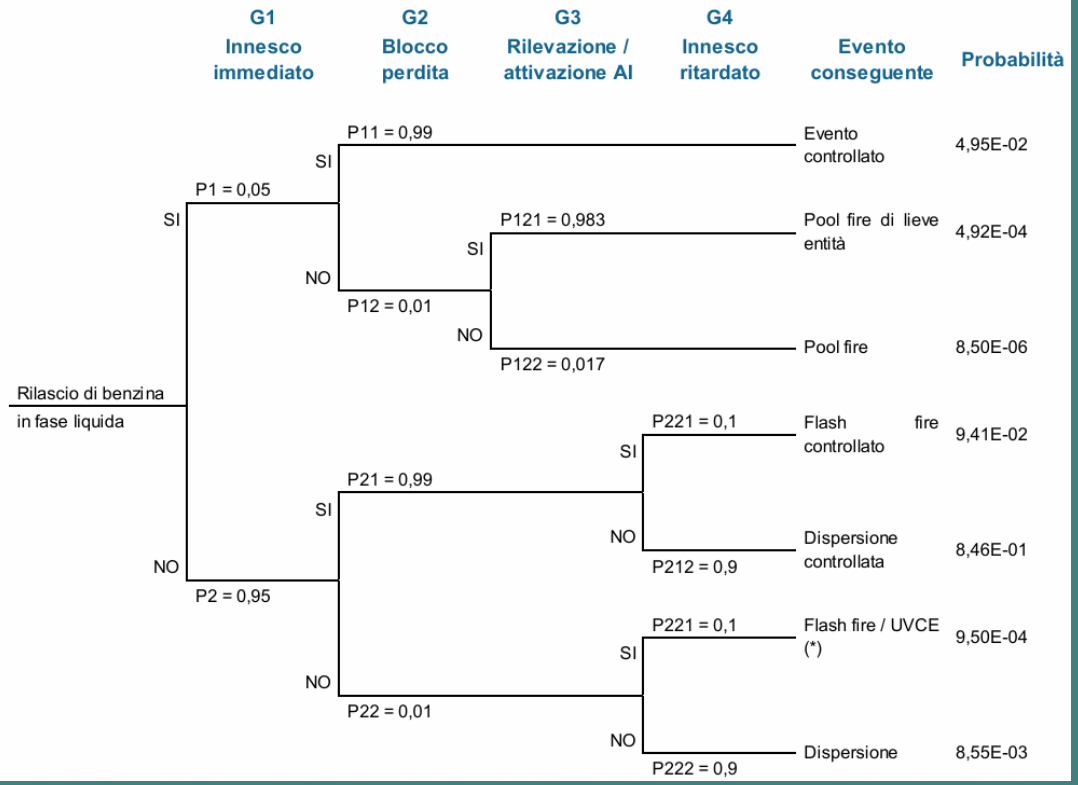
Rule-sets:

- frequenze cause in OR (somma);
- Frequenza top event = frequenza cause * PFD barriere (su ogni singola linea);
- Frequenza conseguenza = frequenza top event * PFD barriere (su ogni singola linea).

# Bow Tie

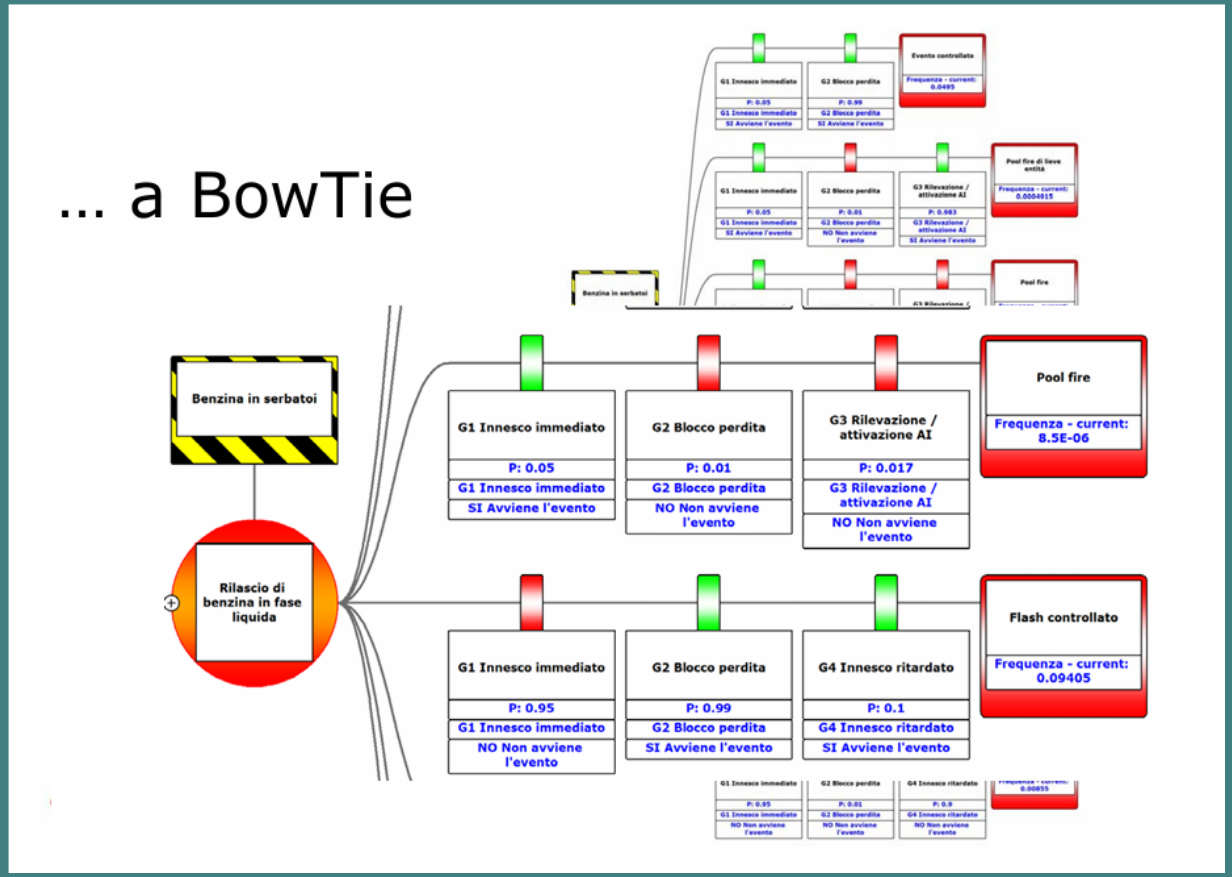


## Da albero degli eventi...



# Bow Tie

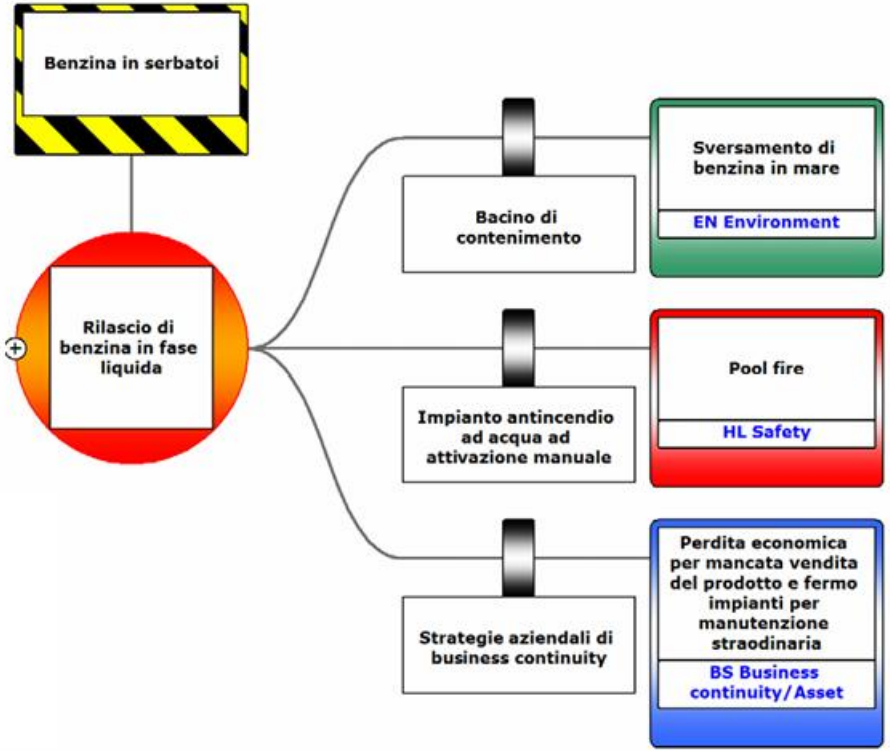



... a BowTie
Benzina in serbatoi
Rilascio di benzina in fase liquida
G1 Innesco immediato
P: 0.05
G1 Innesco immediato
SI Avviene l'evento
G2 Blocco perdita
P: 0.01
G2 Blocco perdita
NO Non avviene l'evento
G3 Rilevazione / attivazione AI
P: 0.017
G3 Rilevazione / attivazione AI
NO Non avviene l'evento
Pool fire
Frequenza - current: 8.5E-06
G1 Innesco immediato
P: 0.95
G1 Innesco immediato
NO Non avviene l'evento
G2 Blocco perdita
P: 0.99
G2 Blocco perdita
SI Avviene l'evento
G4 Innesco ritardato
P: 0.1
G4 Innesco ritardato
SI Avviene l'evento
Flash controllato
Frequenza - current: 0.09405

# Bow Tie



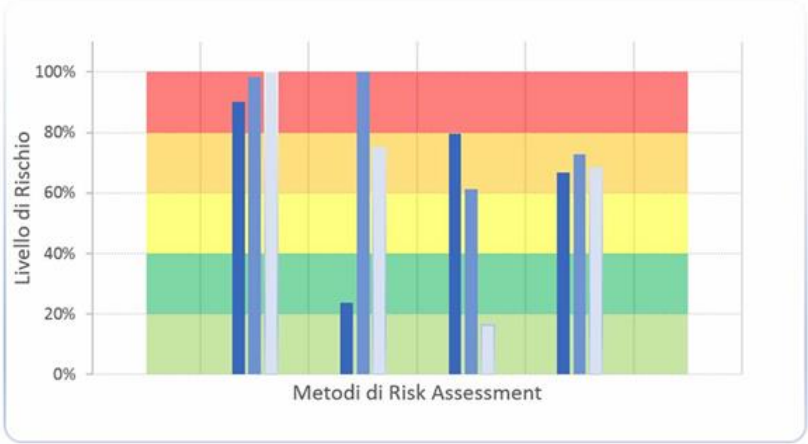
## Tipi di conseguenze in un BowTie



# Bow Tie



## Bow-Tie & Indicizzazione del Rischio



# Bow Tie



## SW&HI: Safety Weighted Hazard Index


$HP$ = f(Parametri di processo, sostanze, condizioni operative e strutturali impianto)

***Fattori di Credito A***

- Piano per le Emergenze
- Sistemi di controllo/emergenza
- Sistemi di rilevamento
- Caratterizzazione tipo processo
- Caratteristiche operatore
- Affidabilità apparecchiature

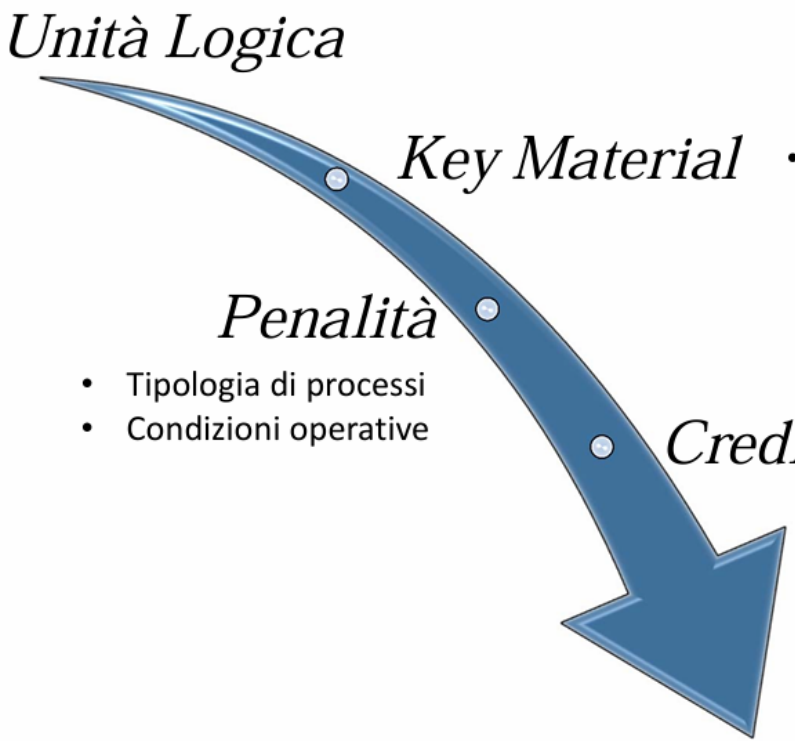
$$SW\&HI = {}^{B1}/_{A}$$

| *Indice* | *Livello di rischio* |
|---|---|
| *>20* | *Estremo* |
| 10 ÷ 20 | Alto |
| 5 ÷ 10 | Moderato |
| 1 ÷ 5 | Basso |
| 0 ÷ 1 | Lieve |

# Bow Tie



1. Suddivisione dell'impianto in Unità Logiche
2. Individuazione della sostanza 'chiave' pericolosa
3. Caratteristiche speciali della sostanza
4. Pericoli Generali dell'unità
5. Pericoli Speciali dell'unità
6. Caratterizzazione strutturale del sito




- Sostanze: pericolo di F&E, rilascio tossico

- Tipologia di processi
- Condizioni operative

- Sistemi prevenzione & protezione
- SGS Antincendio

# Bow Tie



**Penalità** →

Aumentano il livello di Rischio

- Sostanze
- Caratteristiche strutturali
- Caratteristiche del processo

**Crediti** →

Diminuiscono il livello di Rischio

- Livello di protezione delle apparecchiature e personale
- Sistemi di prevenzione/controllo
- Sisteam di gestione della sicurezza

# Bow Tie



## *Caso studio: Thyssen-Krupp*

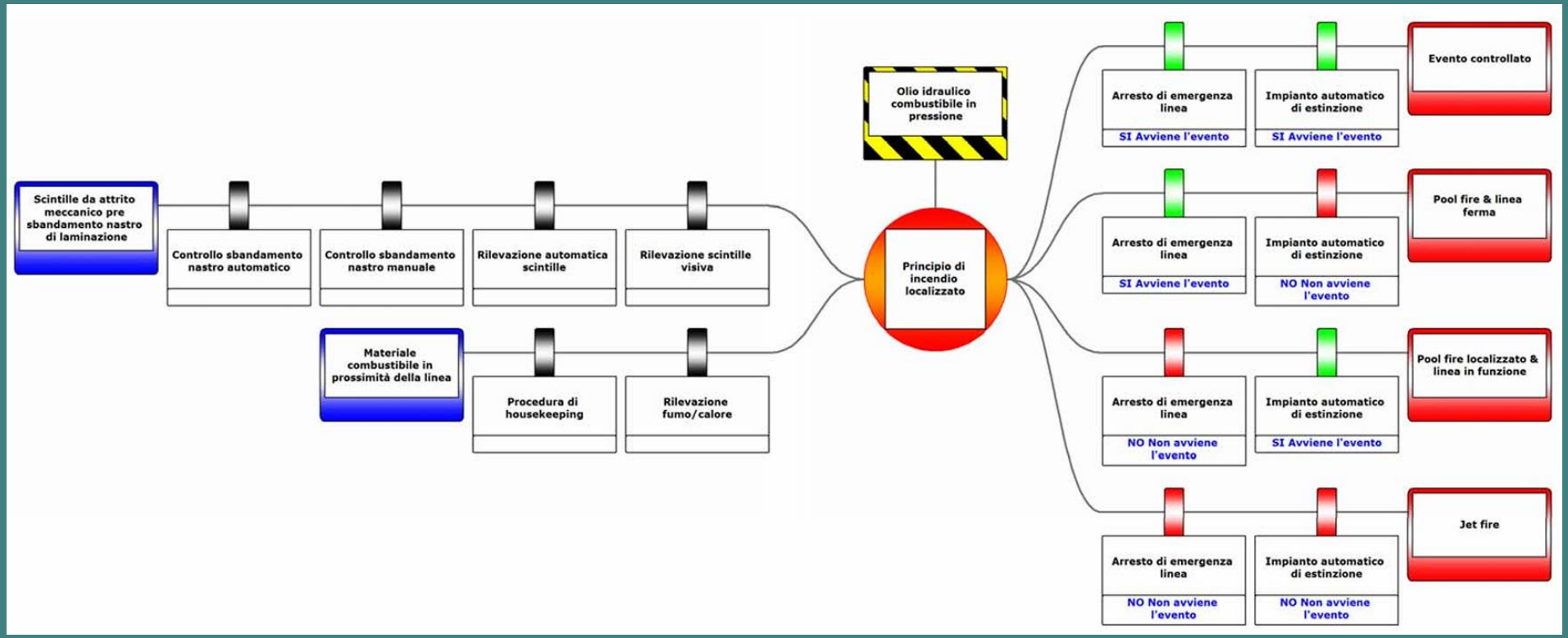
- ***Evento:*** Jet Fire
- ***Pericolo***:
  - Olio idraulico in pressione

- ***Cause dirette:*** Sbandamento nastro di laminazione, scintille meccaniche, principio di incendio materiali combustibili
- ***Stato delle Barriere*** - Assenza di addestramento personale in caso di Emergenza;
  - Assenza di HAZID
  - Assenza di Arresto automatico/sistema di spegnimento automatico

Prof. Claudio Pantanali, PhD cpantanali@units.it

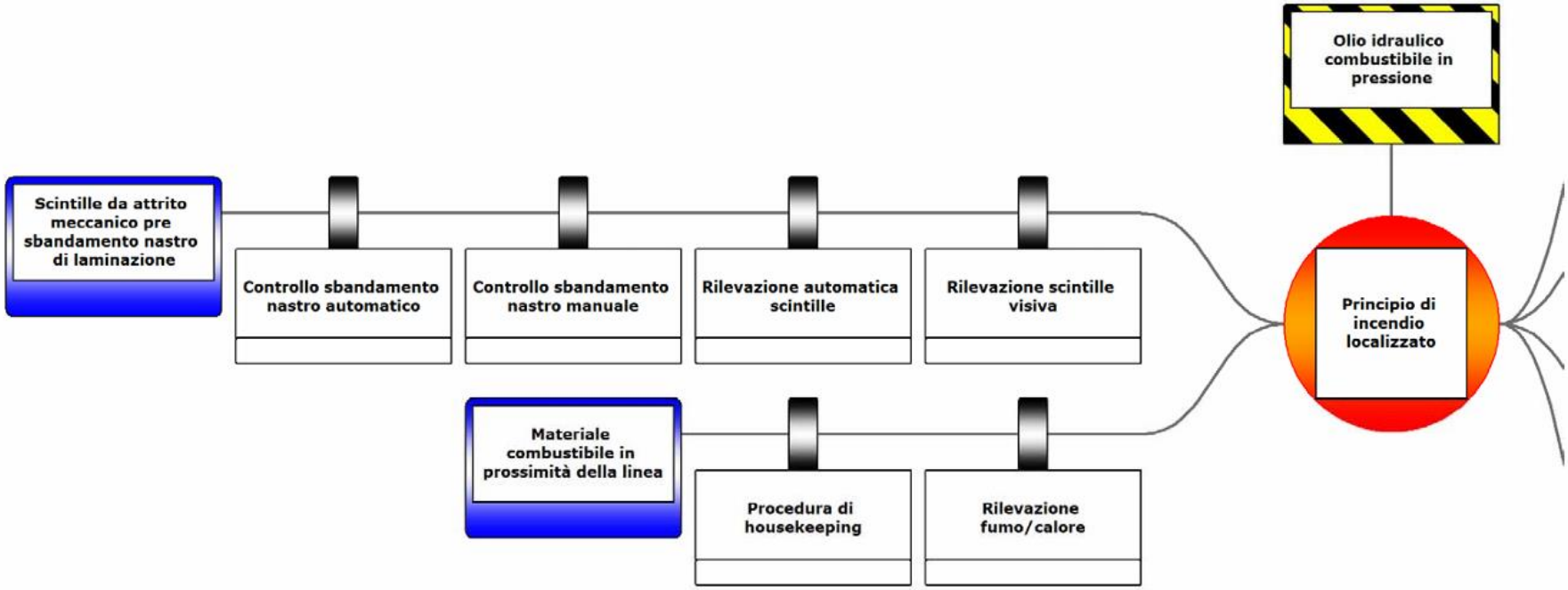
# Bow Tie





# Bow Tie

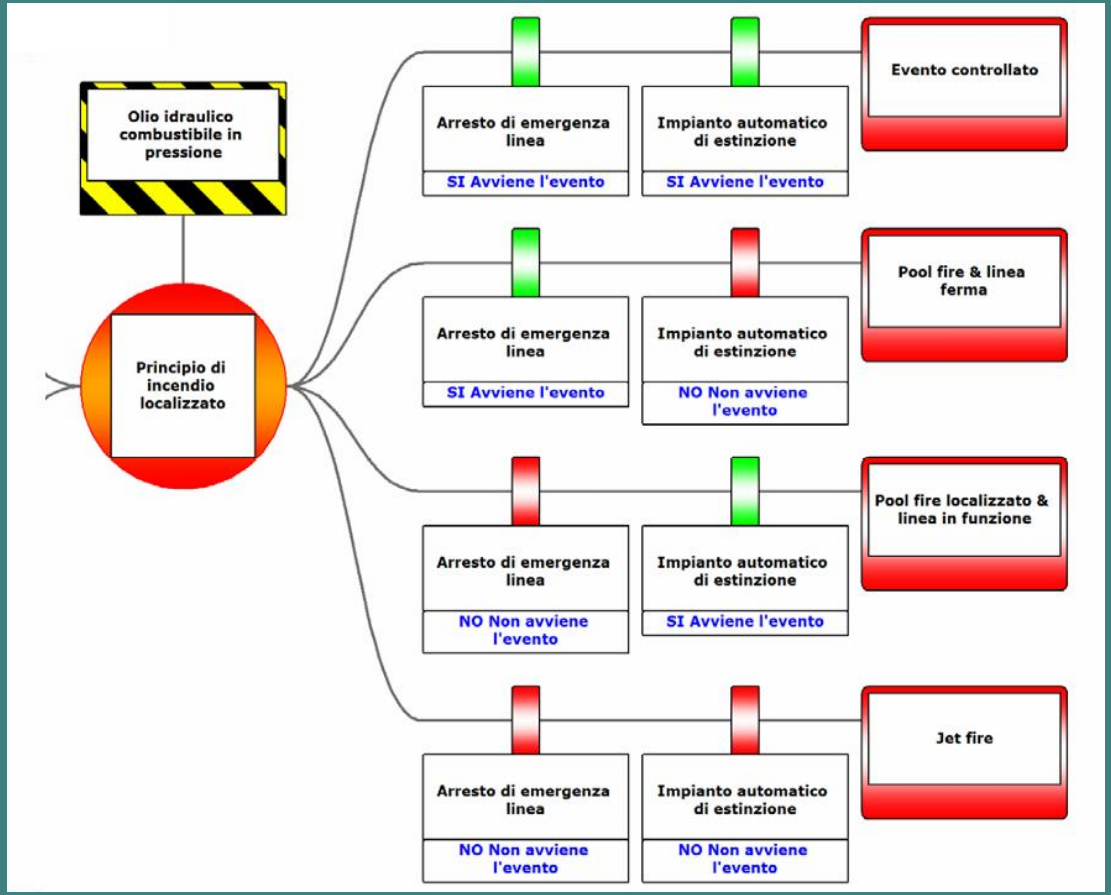



Olio idraulico combustibile in pressione
Scintille da attrito meccanico pre sbandamento nastro di laminazione
Controllo sbandamento nastro automatico
Controllo sbandamento nastro manuale
Rilevazione automatica scintille
Rilevazione scintille visiva
Principio di incendio localizzato
Materiale combustibile in prossimità della linea
Procedura di housekeeping
Rilevazione fumo/calore

Prof. Claudio Pantanali, PhD cpantanali@units.it

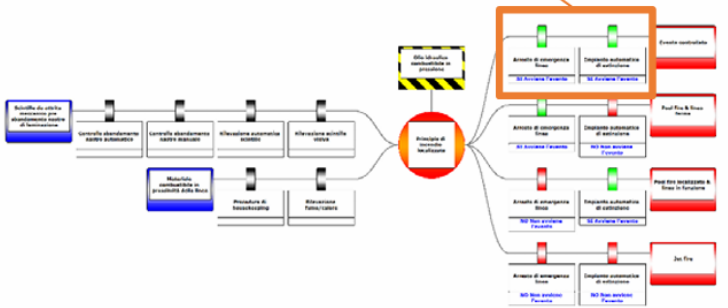
# Bow Tie





# Barriere mitigative

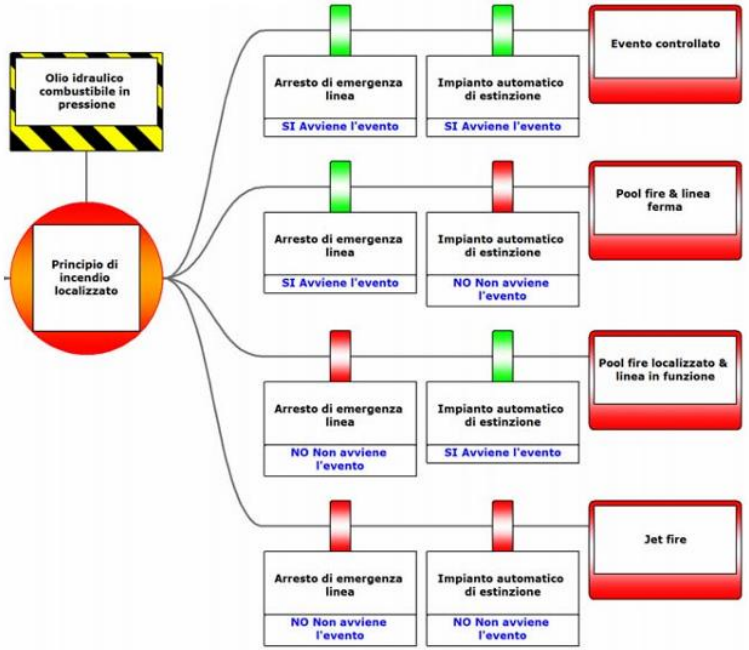
- Piano per le Emergenze
- Sistemi di controllo/emergenza
- Sistemi di rilevamento
- Automatizzazione del processo
- Caratteristiche operatore
- Affidabilità apparecchiature

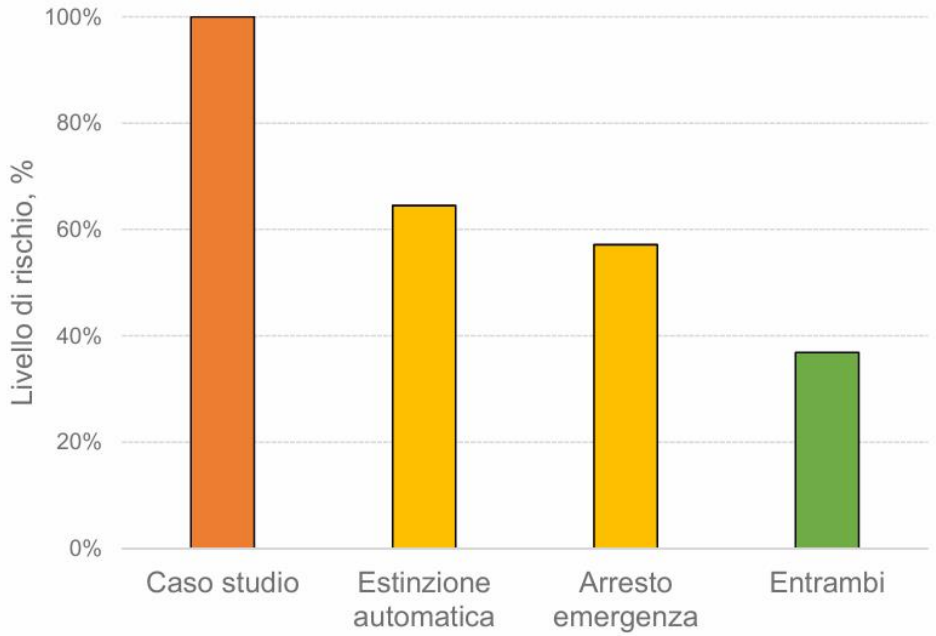



Prof. Claudio Pantanali, PhD cpantanali@units.it

# Bow Tie





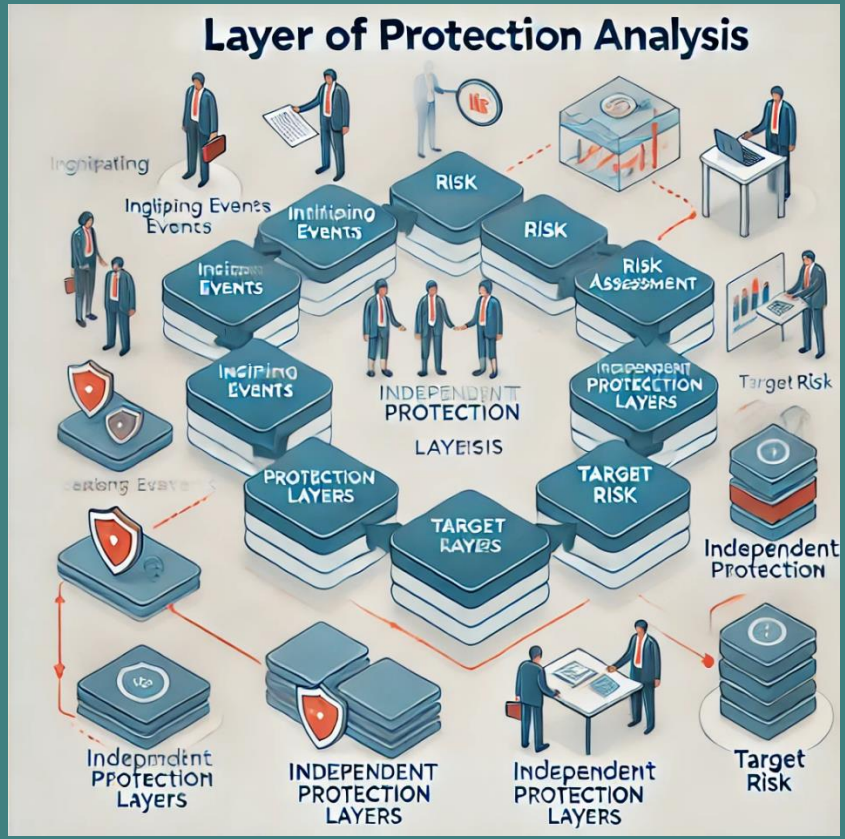



DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA
Prof. Claudio Pantanali, PhD cpantanali@units.it



# LOPA

## Layer of Protection Analysis
## Analisi dei Livelli di Protezione

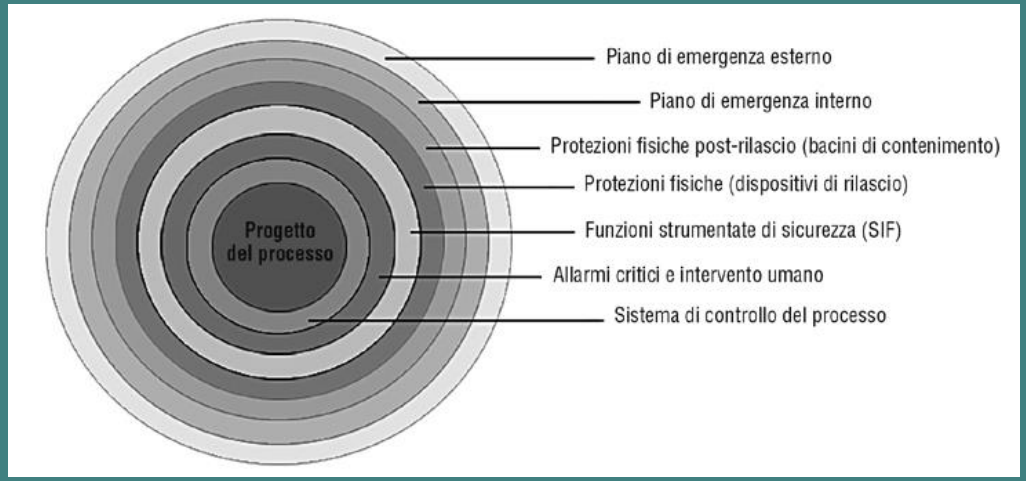


Prof. Claudio Pantanali, PhD cpantanali@units.it

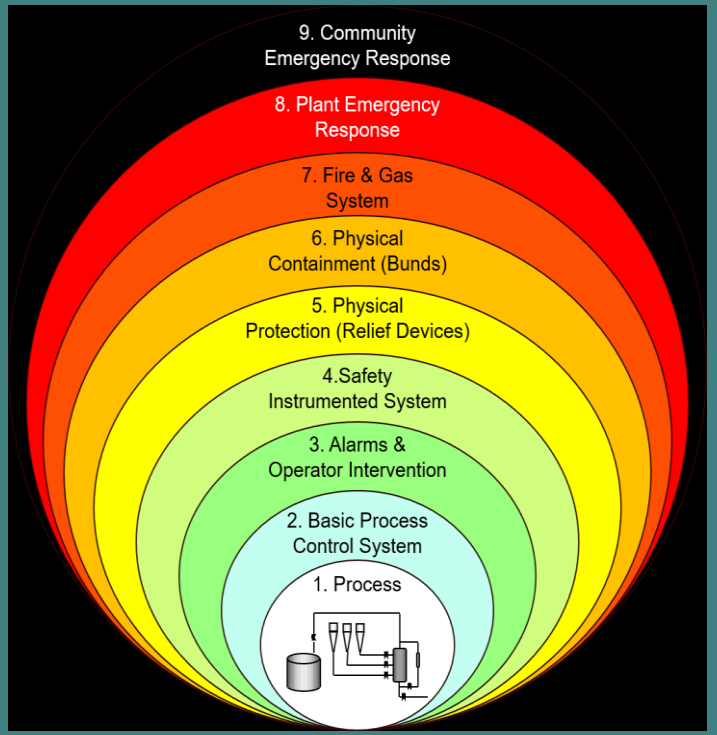
# Layer Of Protection Analysis (Analisi LOPA)



L'analisi dei livelli di protezione indipendenti (LOPA – *Layer of Protection Analysis*) è un metodo tipicamente utilizzato quale strumento di valutazione del rischio, talvolta anche utilizzato per l'investigazione di incidenti. Esso ha trovato particolare successo nell'industria di processo; in questo contesto è possibile identificare i livelli di protezione che riducono i rischi di eventi indesiderati. Essi sono raffigurati in figura.




*Livelli di protezione indipendenti nell'industria di processo*



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

# Layer Of Protection Analysis (Analisi LOPA)

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

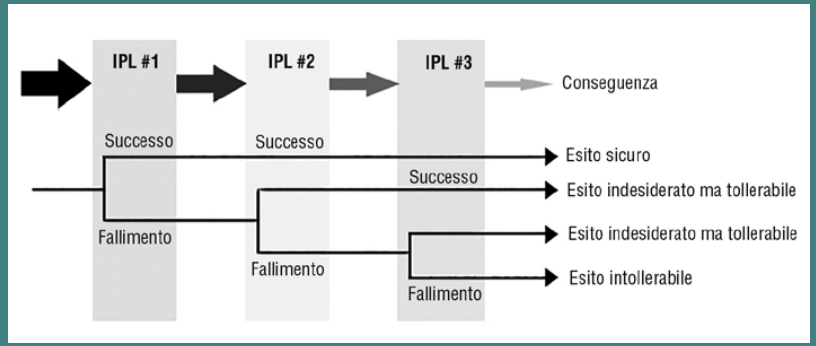
Lo scopo dell'analisi LOPA è di analizzare l'efficacia delle barriere (livelli di protezione) proposte, confrontando il livello di rischio del sistema ipotizzato privo di barriere con il livello di rischio del sistema equipaggiato con le barriere, sempre avendo come riferimento un criterio di tollerabilità del rischio.
L'analisi LOPA può utilizzare anche solo ordini di grandezza sia della frequenza degli eventi iniziatori che per la probabilità di fallimento di un livello di protezione indipendente **(IPL – *Independent Protection Layer)*,** determinando così che le barriere esistenti sono sufficienti o meno per mitigare il livello di rischio di un determinato scenario incidentale al di sotto del limite di tollerabilità.
Le barriere possono essere classificate, al pari di come è possibile fare per l'analisi *Bow-Tie*, in barriere attive o passive, o preventive e mitigative. Deve tuttavia essere chiaro che mentre tutti gli IPL sono barriere, non tutte le barriere sono IPL. In generale, una barriera è un qualunque sistema, strumento o azione che può arrestare la catena di eventi conseguente ad un evento iniziatore. Per essere anche un IPL, una barriera deve essere: efficace (avere la capacità di intervenire in tempo), indipendente (non condividere cause comuni di guasto con altre barriere), e valutabile (per dimostrare che essa soddisfi i requisiti di mitigazione del rischio). Citando ad esempio lo standard tecnico EN/IEC 61511-3 in materia di sicurezza funzionale:

- ogni IPL deve essere indipendente da qualunque altro IPL;
- ogni IPL deve essere differente da qualunque altro IPL;
- ogni IPL deve essere fisicamente separato da qualunque altro IPL;
- ogni IPL non deve condividere cause comuni di guasto con qualunque altro IPL;
- ogni IPL deve essere altamente disponibile;
- ogni IPL deve essere validato e *auditabile*.

Questo metodo può essere utilizzato lungo tutto il ciclo di vita della sicurezza di processo. È generalmente utilizzato per esaminare gli scenari provenienti da altri strumenti di PHA, come l'HAZOP, e definire i target SIL da raggiungere per soddisfare i criteri di accettabilità del rischio.
Può anche essere utilizzato nelle fasi iniziali di un progetto, allo scopo di valutare protezioni alternative, o identificare quelle critiche, ovvero quelle che mantengono il rischio all'interno della regione di tollerabilità. È anche utile per identificare i controlli amministratici critici (CAC – *Critical Administrative Control)*, ovvero le azioni o risposte dell'operatore che sono critiche per mantenere il rischio all'interno della regione di tollerabilità. È anche utilizzato per identificare gli scenari di rischio ALARP.
Risulta evidente che, in teoria, un singolo livello di protezione sia sufficiente a fermare la sequenza incidentale e prevenire quindi lo scenario di rischio.

In verità, nessun livello può essere considerato completamente affidabile (100%), nessuno è perfettamente efficace.
Questo è il motivo per cui viene generalmente identificato un insieme di livelli di protezione per fornire la richiesta mitigazione del rischio. Se il rischio non è tollerabile, IPL aggiuntivi dovrebbero essere prescritti.
Per eseguire una analisi LOPA è necessario disporre di molti dati in ingresso, quali: dati sui ratei di guasto dei componenti di un apparecchio o sistema, frequenze di cause iniziatrici, ratei di errore umano, e così via, analogamente ad altre tecniche quantitative quali FTA ed ETA.

Così strutturata, la LOPA non è un metodo pienamente quantitativo; esso è piuttosto un approccio numerico semplificato per valutare l'efficacia dei livello di protezione per un preciso scenario incidentale. Il fatto che la LOPA utilizzi dei numeri non vuol dire che fornisce misure del rischio precise: fornisce solo un'approssimazione che può essere comunque utile (se non addirittura sufficiente) a seconda del contesto. Ad esempio per stimare l'ordine di grandezza della riduzione del rischio operata da una combinazione di misure rispetto a combinazioni alternative a supporto di un successivo studio ALARP e correlate analisi costi-benefici. Quale metodologia numerica di screening essa consente di definire priorità di approfondimento e/o di implementazione nell'ambito delle attività di pianificazione della riduzione dei rischi da porsi alla base dei riesami periodici. Questa metodologia può essere vista in parallelo ad altri metodi di valutazione quantitativa del rischio, come l'albero degli eventi, come mostrato in Figura



In figura precedente, lo spessore della freccia rappresenta la frequenza dello scenario, che è ridotta progressivamente dall'efficacia delle barriere. È chiaro come LOPA e ETA condividano alcuni concetti alla base del comune ragionamento (*in primis*, come evidente, le due metodologie condividono l'individuazione delle misure di controllo quali elementi fondamentali per il riconoscimento degli insiemi di esiti possibili data una iniziale deviazione dalle normali condizioni operative atte al raggiungimento degli obiettivi prefissati). Semplificando, la LOPA consiste delle seguenti fasi:

- raccolta degli scenari sviluppati in altri studi, come l'HAZOP;
- selezione di uno scenario incidentale e valutazione delle conseguenze;
- identificazione degli eventi iniziatori e delle loro frequenze;
- identificazione degli IPL e della loro probabilità di fallimento;
- stima del rischio, combinando la frequenza degli eventi iniziatori, la probabilità di fallimento degli IPL e la severità delle conseguenze;
- valutazione del rischio ed eventuale sviluppo di un piano di azioni per mitigare ulteriormente il rischio.

L'analisi LOPA non deve essere confusa con l'HAZOP: si tratta di tecniche differenti, con obiettivi diversi. L'HAZOP è utilizzata per fare *brainstorming* sui possibili pericoli ed identificare gli scenari incidentali, il cui rischio può essere valutato solo da un punto di vista qualitativo.

Invece, durante la LOPA l'analista arricchisce queste informazioni con delle valutazioni quantitative, almeno per ordini di grandezza, quando non puramente qualitative. Come più volte accennato in questo volume non esiste una metodologia univoca per la valutazione del rischio. La selezione del metodo (ed eventuali tool a supporto) risulta essere un passaggio specifico, obbligato e fondamentale della strategia di gestione del rischio, da effettuarsi tenendo conto di risorse e competenze ma soprattutto dell'analisi iniziale dal contesto e degli obiettivi. Ciò detto spesso, anche a favore di un approccio ad approfondimento graduale, con la selezione di una metodologia per ciascun aspetto di rischio o di una combinazione di metodologie.

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

# Layer Of Protection Analysis (Analisi LOPA)

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

La valutazione del rischio tramite il metodo LOPA (Layers of Protection Analysis, ovvero Analisi degli Strati di Protezione) è una tecnica di valutazione semiquantitativa dei rischi utilizzata principalmente nell'industria di processo, come quella chimica, petrolchimica ed energetica. Questo metodo consente di valutare il rischio associato a scenari specifici, verificare se gli strati di protezione esistenti siano sufficienti e, se necessario, definire ulteriori misure per ridurre il rischio a un livello accettabile.

**Fasi della Valutazione del Rischio con il Metodo LOPA**

**1.Identificazione dell'Evento Iniziatore**:

- Si inizia con l'individuazione dell'evento scatenante, cioè un guasto, errore o malfunzionamento che potrebbe dare origine a uno scenario di rischio, come la perdita di contenimento di una sostanza pericolosa.

**2.Determinazione delle Conseguenze**:

- Viene valutata la gravità delle conseguenze nel caso in cui l'evento iniziatore si verificasse. Queste conseguenze potrebbero coinvolgere aspetti di sicurezza, salute e impatto ambientale.

**3.Stima della Frequenza dell'Evento Iniziatore**:

- Si stima la probabilità o la frequenza con cui l'evento iniziatore potrebbe verificarsi. Queste stime possono essere basate su dati storici, esperienze precedenti o analisi di affidabilità degli impianti.

**4.Identificazione degli Strati di Protezione Indipendenti (IPL)**:

- Gli strati di protezione sono le misure di sicurezza che impediscono l'escalation dell'evento iniziatore verso conseguenze gravi. Gli IPL (Independent Protection Layers) devono essere efficaci, indipendenti e credibili. Esempi di IPL includono:
  1. Sistemi di allarme e risposta dell'operatore.
  2. Sistemi di sicurezza strumentata (SIS).
  3. Sistemi di contenimento passivi e dispositivi di mitigazione.

**5.Calcolo del Rischio Residuo**:

- Si calcola il rischio residuo stimando la riduzione del rischio ottenuta dagli strati di protezione identificati. Il rischio residuo viene poi confrontato con i criteri di rischio accettabile definiti dall'organizzazione.

**6.Valutazione e Decisione**:

- Se il rischio residuo non soddisfa i criteri accettabili, è necessario implementare ulteriori strati di protezione o apportare modifiche al processo. L'obiettivo è ridurre il rischio a un livello tollerabile e garantire la sicurezza del processo.

*DIPARTIMENTO DI INGEGNERIA E ARCHITETTURA*

*Prof. Claudio Pantanali, PhD* *cpantanali@units.it*

# Layer Of Protection Analysis (Analisi LOPA)

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

## Elementi Chiave del Metodo LOPA

- **Strati di Protezione Indipendenti (IPL):** Gli strati di protezione devono essere indipendenti tra loro, in modo che il fallimento di uno non comprometta l'efficacia degli altri. Questa indipendenza è essenziale per assicurare che ogni strato sia in grado di ridurre il rischio in modo significativo.
- **Riduzione del Rischio:** Ogni IPL contribuisce a ridurre la frequenza di uno scenario di rischio. L'efficacia di ogni IPL è spesso espressa in termini di **fattore di riduzione del rischio** (Risk Reduction Factor, RRF).
- **Criteri di Accettabilità del Rischio:** Prima di iniziare l'analisi LOPA, è importante definire i livelli di rischio accettabili. Questi criteri guidano la valutazione del rischio residuo e l'implementazione di nuove misure di sicurezza.

**Esempio di Applicazione del Metodo LOPA**

Supponiamo di avere un serbatoio che contiene una sostanza chimica tossica. Un evento iniziatore potrebbe essere un guasto della valvola di scarico, che causerebbe una perdita di sostanza. La LOPA considera le seguenti informazioni:

1. **Frequenza dell'evento iniziatore:** Si stima che il guasto della valvola possa avvenire una volta ogni 10 anni.
2. **Conseguenze:** La perdita di sostanza potrebbe causare danni significativi agli operatori e all'ambiente.
3. **Strati di protezione:**
    - **Sistema di allarme e risposta dell'operatore**: Con un'efficacia del 90% (RRF = 10).
    - **Sistema di sicurezza strumentato (SIS)**: Che chiude automaticamente la valvola in caso di perdita, con un'efficacia del 99% (RRF = 100).

Il rischio residuo viene calcolato considerando la riduzione del rischio ottenuta grazie agli IPL. Se il rischio risultante è inferiore ai criteri accettabili, la situazione è considerata sicura; altrimenti, occorre aggiungere ulteriori misure di mitigazione.

## Vantaggi e Limitazioni del Metodo LOPA

**Vantaggi:**

- Struttura chiara e sistematica per la valutazione dei rischi.
- Riduzione del rischio e ottimizzazione delle risorse grazie all'individuazione delle misure più efficaci.
- Supporta la decisione riguardo l'implementazione di misure di sicurezza.

**Limitazioni:**

- Metodo semiquantitativo: i risultati dipendono dalla qualità dei dati disponibili e possono essere influenzati da incertezze.
- Può risultare complesso applicare la LOPA a scenari con numerosi eventi o con strati di protezione non ben definiti.

Il metodo LOPA rappresenta uno strumento essenziale nella gestione dei rischi per l'industria di processo, consentendo di garantire che i rischi siano ridotti a livelli accettabili attraverso un'analisi strutturata e trasparente degli strati di protezione.

# Layer Of Protection Analysis (Analisi LOPA)



Vediamo un esempio concreto per illustrare come funziona il metodo LOPA in un contesto industriale.

**Scenario di Esempio: Serbatoio di Stoccaggio con Sostanza Tossica**

Immaginiamo di avere un serbatoio che contiene ammoniaca liquida, una sostanza tossica e pericolosa per la salute degli operatori e per l'ambiente. Vogliamo valutare il rischio associato a una possibile perdita di ammoniaca dal serbatoio.

**1. Identificazione dell'Evento Iniziatore**

L'evento iniziatore considerato è la **rottura della valvola di sicurezza** del serbatoio, che potrebbe causare la fuoriuscita di ammoniaca nell'ambiente.

**2. Determinazione delle Conseguenze**

Se la valvola si rompe e l'ammoniaca fuoriesce, potrebbe verificarsi un'esposizione tossica per gli operatori presenti nell'area, con potenziali effetti sulla salute che vanno dall'irritazione delle vie respiratorie a conseguenze più gravi.

**3. Stima della Frequenza dell'Evento Iniziatore**

Basandoci su dati storici e analisi di affidabilità dell'impianto, stimiamo che la **frequenza della rottura della valvola sia di 1 volta ogni 5 anni** (0,2 volte all'anno).

**4. Identificazione degli Strati di Protezione Indipendenti (IPL)**

Identifichiamo gli strati di protezione indipendenti che potrebbero prevenire o mitigare il rischio di fuoriuscita di ammoniaca:

- **Sistema di Allarme e Intervento Operativo**: Un sensore di pressione rileva un aumento di pressione e attiva un allarme, che richiede l'intervento manuale da parte dell'operatore per chiudere la valvola difettosa.
  - **Efficienza del sistema**: Il sistema ha una probabilità di successo del 90% (Fattore di Riduzione del Rischio, RRF = 10).
- **Sistema di Sicurezza Strumentato (SIS)**: Se l'allarme non viene gestito in tempo, un sistema automatico chiude la valvola per prevenire ulteriori fuoriuscite.
  - **Efficienza del sistema**: Il SIS ha una probabilità di successo del 99% (RRF = 100).
- **Bacino di Contenimento**: Intorno al serbatoio c'è un bacino di contenimento che limita la dispersione dell'ammoniaca, riducendo il rischio di esposizione agli operatori e all'ambiente.
  - **Efficienza del sistema**: Il bacino di contenimento ha un'efficacia stimata del 95% (RRF = 20).

**5. Calcolo del Rischio Residuo**

Per calcolare il rischio residuo, consideriamo la riduzione del rischio offerta dagli strati di protezione. La frequenza dell'evento viene moltiplicata per la probabilità che ciascun IPL non funzioni. Vediamo il calcolo:

- **Frequenza iniziale dell'evento iniziatore**: 0,2 volte all'anno.
- **RRF del sistema di allarme e intervento operativo**: 10.
- **RRF del sistema di sicurezza strumentato (SIS)**: 100.
- **RRF del bacino di contenimento**: 20.

La frequenza residua si ottiene dividendo la frequenza dell'evento iniziatore per i RRF di ciascun strato di protezione:

$$\text{Frequenza Residua} = \frac{0,2}{10 \times 100 \times 20} = 0,00001 \text{ volte all'anno}$$

Quindi, la frequenza stimata di una perdita non controllata di ammoniaca è pari a **0,00001 volte all'anno**, ovvero una volta ogni 100.000 anni.

**6. Valutazione e Decisione**

Confrontiamo la frequenza residua con i criteri di rischio accettabili definiti dall'azienda. Se il rischio risultante è inferiore al livello di rischio tollerabile, possiamo considerare le misure di sicurezza adeguate. In caso contrario, dovremmo implementare ulteriori strati di protezione.

In questo esempio, la frequenza residua di **0,00001 volte all'anno** è molto bassa e potrebbe essere considerata accettabile per la maggior parte delle aziende, indicando che le misure di protezione attualmente implementate sono sufficienti per mitigare il rischio.

**Conclusioni sull'Esempio**

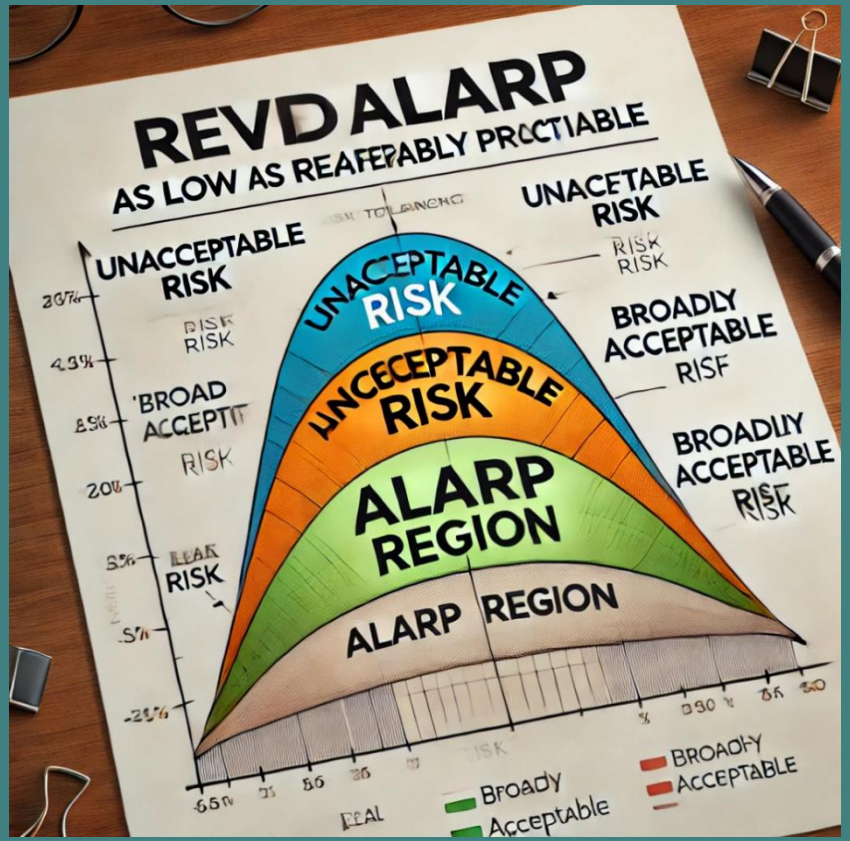
Il metodo LOPA permette di valutare, in modo sistematico, la sufficienza degli strati di protezione indipendenti nel ridurre il rischio associato a uno scenario specifico. In questo esempio, l'analisi mostra che i tre strati di protezione riducono il rischio a un livello molto basso, garantendo la sicurezza del processo e dei lavoratori.

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



# ALARP

*as low as reasonably practicable*



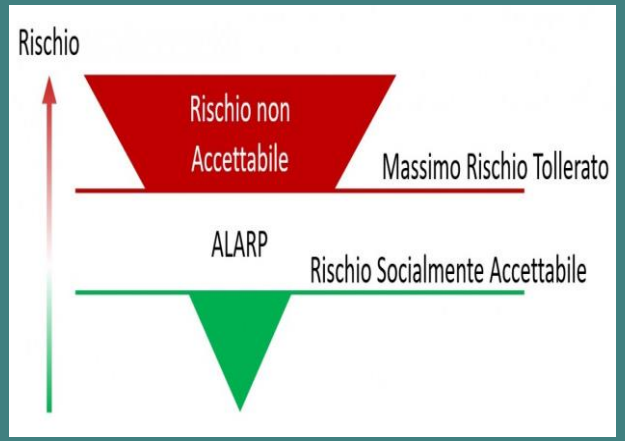
# DIRETTIVA MACCHINE: IL PRINCIPIO ALARP - *as low as reasonably practicable*
## Rischio Trascurabile, Rischio Tollerabile, Rischio Non Accettabile

Il Principio Alarp riconosce tre grandi categorie di rischi:

**1.Rischio trascurabile:** Largamente accettato dalla maggior parte delle persone in quanto vi si incorre normalmente nella vita di tutti i giorni. Questa categoria di rischi include la possibilità di essere colpiti da un fulmine o avere un guasto ai freni dell'automobile.

**2. Rischio Tollerabile:** Si preferirebbe non avere questo rischio, ma lo si tollera in vista dei benefici che si possono ottenere accettandolo. Il costo in termini di denaro è bilanciato dalla scala del rischio e si accetta un compromesso. Questa categoria di rischio si può applicare ad esempio al viaggio in auto, accettiamo che possano accadere incidenti ma facciamo del nostro meglio per minimizzare le probabilità che avvenga un disastro. Si può fare la stessa considerazione per il bungee jumping ?

**3. Rischio Non Accettabile:** Il rischio è talmente alto che non si è disposti a correrlo. Le perdite superano di gran lunga i benefici che si avrebbero dall'accettare tale rischio. Uno degli aspetti più difficili nell'applicare il Principio ALARP è di definire i 3 livelli di rischio.



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

# ALARP

DIPARTIMENTO
DI INGEGNERIA
E ARCHITETTURA

*Tradotto da "Reducing risk, protecting people" di HSE:*

*Qui di seguito, l'approccio dell'HSE (Health and Safety Executive, in UK).*

*L'HSE ritiene che un rischio individuale di morte di uno su un milione all'anno per i lavoratori o terzi (ospiti o pubblico), corrisponde ad un bassissimo livello di rischio e deve essere utilizzato come linea guida per il confine tra la regione "ampiamente accettabile" e quella "tollerabile". [...]*
*[...] Tuttavia, nel nostro documento sulla tollerabilità dei rischi nelle centrali nucleari, abbiamo suggerito che un rischio individuale di morte di uno su mille annuo dovrebbe rappresentare la linea di demarcazione tra ciò che può essere appena tollerabile per qualunque categoria di lavoratori e ciò che è inaccettabile per chiunque eccetto particolari categorie. Per i membri del pubblico, il cui rischio imposto su di essi è 'nel più ampio interesse dell'azienda', si considera tale limite di un ordine di grandezza inferiore, 1:10.000 all'anno. [...]*

Essenzialmente, questo principio, guida i progettisti e gli specialisti della sicurezza nello stabilire un target in termini di rischio tollerabile per una determinata situazione pericolosa. Questo è il primo passo nella determinazione del livello di prestazione per qualsiasi sistema di sicurezza.

**Qui un esempio di applicazione del principio ALARP.**

In una specifica azienda, si fissa una spesa target di £ 1.000.000 per ogni vita salvata. Viene stabilito come obiettivo, un rischio tollerabile massimo di $10^{-4}$ pa* per uno specifico rischio, il quale può arrivare a provocare 2 morti.
Il sistema proposto viene valutato e si ottiene un rischio predetto di $8\times10^{-5}$ pa.
Poiché come rischio trascurabile si considera $10^{-6}$pa allora è necessaria l'applicazione del Principio ALARP.
Per un costo di £3.000, con strumentazione addizionale e ridondanza si può ridurre il rischio fin poco al di sopra della regione di rischio trascurabile ($2\times10^{-6}$ pa). La vita dell'impianto è di 30 anni.

**Soluzione:**

$1.000.000 \times (8\times10^{-5} - 2\times10^{-6}) \times 2 \times 30 = £4.680 > £3.000$. Pertanto, la proposta dovrebbe essere adottata.

*pa=personal accident

Prof. Claudio Pantanali, PhD cpantanali@units.it


**“Esiste un solo bene, la conoscenza, ed un solo male, l'ignoranza.”**

**“La pena che i buoni devono scontare per l'indifferenza alla cosa pubblica è quella di essere governati da uomini malvagi.”**

**SOCRATE**