UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI TECNICA E GESTIONE DEI SISTEMI INDUSTRIALI

Corso di Laurea: Ingegneria Meccatronica (L-8 D.M. 270/2004)

Tesi di Laurea triennale:

SICUREZZA FUNZIONALE NELL'INDUSTRIA DI PROCESSO: METODO HAZOP

(Functional safety in the process industry: HAZOP method)

Relatore: Ing. Diego Dainese

Laureanda: Letizia Zordan

1161967

Anno Accademico 2020/2021

Legge di Murphy: corollari

1. *Niente è facile come sembra;*
2. *Tutto richiede più tempo di quanto si pensi;*
3. *Se c'è una possibilità che varie cose vadano male, quella che causa il danno maggiore sarà la prima a farlo;*
4. *Se si prevedono quattro possibili modi in cui qualcosa può andare male e si prevengono, immediatamente se ne rivelerà un quinto;*
5. *Lasciate a sé stesse le cose vanno di male in peggio;*
6. *Non ci si può mettere a fare qualcosa senza che qualcos'altro vada fatto prima;*
7. *Ogni soluzione genera nuovi problemi;*
8. *I cretini sono sempre più ingegnosi delle precauzioni che si prendono per impedirgli di nuocere;*
9. *Per quanto nascosta sia una pecca, la natura riuscirà sempre a trovarla;*
10. *Madre Natura è una stronza.*

Indice

Sommario

Con la presente tesi si vuole eseguire una panoramica legislativa e tecnica inerente alla sicurezza funzionale applicata al settore dell'industria di processo, evidenziandone anche una correlazione con aspetti di *security*. Si pone particolare attenzione all'organizzazione di una valutazione del rischio, studio necessario al processo decisionale per la progettazione di sistemi di salvaguardia e pianificazione di sistemi di gestione di sicurezza all'interno di un impianto tecnico, focalizzandosi nello stadio di identificazione dei pericoli mediante la tecnica HAZOP. Questa metodologia nata per lo studio di deviazioni di processo, viene descritta nella sua pianificazione ed esecuzione analizzando anche varianti applicate allo studio del sistema di controllo. Nel capitolo finale si illustrano i principali aspetti, requisiti e vincoli di progettazione richiesti dalla normativa di riferimento per sistemi di sicurezza.

Capitolo 1: sicurezza ed industria

1.1 Introduzione

Alla parola sicurezza viene comunemente associato un significato "rassicurante", rappresenta una condizione (dal latino sine-cura), senza preoccupazione, condizione dalla quale non è possibile esimersi, specialmente quando sono coinvolte vite umane.

L'industria nel corso dei decenni ha subito un'enorme evoluzione, sia per quanto riguarda le conoscenze in ambito tecnico, sia per la complessità che i processi possono raggiungere, con un costante sguardo verso produttività e qualità. L'automazione ha accompagnato questo cambiamento e ora più che mai pervade qualsiasi ambito di applicazione, un'integrazione che non riguarda solo la gestione/lavorazione di flussi di materiali, ma anche una nuova e stretta collaborazione tra uomo e macchina.
A fronte di questo sviluppo si rende necessario un progresso nelle metodologie e soluzioni destinate alla *safety*, ma grazie ad una crescente interconnessione introdotta dalle tecnologie dell'IoT (*Internet of things)* della "Smart Factory", anche alla *security*, due facce della stessa medaglia[1].
In tal senso, l'Unione europea si è adoperata per agire in favore di ciò, non solo in ambito industriale, e tuttora lavora per un costante aggiornamento. Con la risoluzione del Consiglio europeo del 7 maggio 1985 (85/C 136/01), viene introdotta una nuova strategia legislativa in merito a settori di prodotti o tipologie di rischi, incentrata su un rimodellamento dell'armonizzazione tecnica, denominata di "nuovo approccio". L'importanza di questa nuova condotta è da ritrovare non solo in una maggiore apertura dei mercati e libera circolazione dei beni tra i vari Stati europei, ma anche nell'uniformazione in merito a criteri di sicurezza imposti, che devono essere rispettati e dimostrati.

Nel seguente capitolo verranno illustrati e definiti i principali concetti inerenti al seguente lavoro di tesi, con particolare riguardo verso le applicazioni nell'industria di processo.

[1] Safety e security, termini anglosassoni legati alla sicurezza. Il primo si riferisce alla tutela della salute ed incolumità delle persone da rischi ed incidenti, il secondo è rivolto alla protezione da minacce ed attacchi criminosi.

1.2 L'industria di processo

Con il termine industria di processo si intende l'insieme degli impianti industriali caratterizzati da una produzione per processo.

L'impianto industriale è l'insieme dei macchinari, attrezzature e servizi che hanno lo scopo di trasformare materie prime e semilavorati in prodotti finiti. Normalmente viene a collocarsi in una realtà più ampia, all'interno di un'azienda, cui finalità sta nell'ottenere un utile dai prodotti in uscita, aventi un valore maggiore del materiale lavorato.
La produzione per processo è una classificazione di impianti industriali riferita al modo in cui il prodotto viene realizzato: in particolare non è possibile distinguere i singoli elementi che lo compongono, in quanto durante la lavorazione i materiali in ingresso subiscono una serie di trasformazioni chimiche-fisiche. Si contrappone alla produzione per parti, in cui il prodotto finito è dato dall'assembramento di più componenti.
Viene definita a ciclo tecnologico obbligato, in quanto le diverse fasi di trasformazione e quindi la disposizione dei diversi macchinari seguono una precisa successione vincolante: osservando il layout[2] è possibile coglierne il processo produttivo.

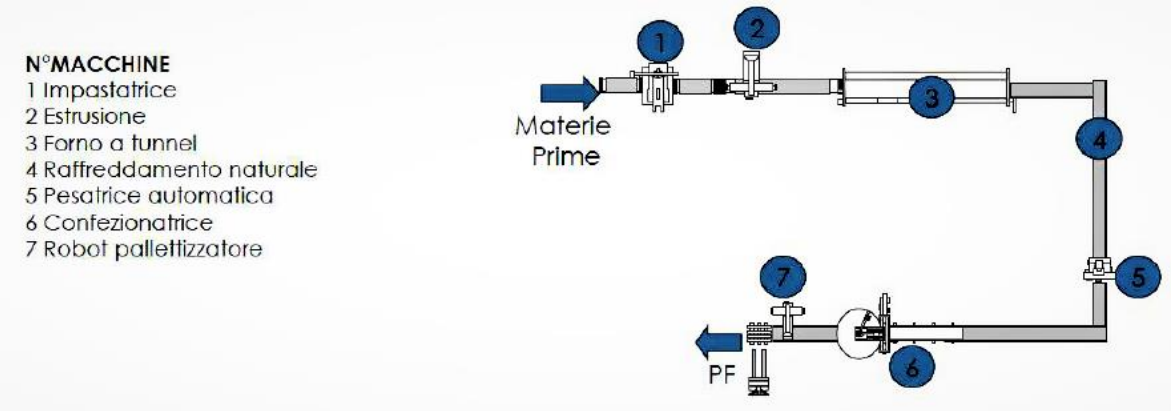

Figura n.1.1 Esempio di layout di una linea produttiva di un impianto alimentare per pasta

A queste tipologie di impianti tecnologici sono normalmente associati elevati flussi in uscita con poca varietà di prodotti e per questo rientrano in una classificazione a produzione continua. Le movimentazioni e lavorazioni di materiali sono estremamente automatizzate e

[2] Disposizione planimetrica di macchinari ed attrezzature appartenenti all'impianto tecnologico principale e agli impianti di servizio ad esso correlati.

la manodopera impiegata è generica e di bassa specializzazione, svolgendo ruolo di controllo e supervisione.
Rientrano, per esempio, in questa categoria di impianti:

- Industria cartaria
- Industria chimica
- Industria alimentare
- Industria del cemento
- Industria chimica e farmaceutica
- Industria petrolchimica e raffineria
- Industria dell'alluminio
- Industria siderurgica e metallurgica
- Industria della ceramica e laterizio
- Industria mineraria
- Industria tessile

1.3 Legislazione di riferimento

1.3.1 Direttive

La direttiva è una delle fonti derivate del diritto dell'Unione Europea ed è uno strumento che consente di armonizzare le legislazioni tra Stati membri.
A seconda che si riferisca ad una parte o a tutti gli stati, può essere classificata in direttiva individuale o generale. È un documento suddiviso in articoli ed allegati, pubblicato nella Gazzetta ufficiale dell'Unione europea ed impone determinati obiettivi da raggiungere, in merito ad un certo scopo ed applicazione, definiti negli articoli iniziali: il modo in cui vengono raggiunti compete ai singoli stati interessati, attraverso il recepimento della stessa mediante disposizioni e provvedimenti di carattere nazionale, entro date specificate, abrogando eventuali leggi nazionali in contrasto con la direttiva. Per quanto riguarda l'Italia, l'adeguamento avviene attraverso l'emanazione di decreti legislativi in Gazzetta Ufficiale affidati con Legge delega al Governo.
Le direttive possono essere suddivise in due categorie: direttive prodotto e direttive sociali.

Le direttive prodotto definiscono i requisiti essenziali che una certa categoria di prodotti deve rispettare affinché possa circolare nel mercato europeo. Possono riguardare la sicurezza verso altri prodotti, persone, ambiente o particolari caratteristiche costruttive. La responsabilità di conformazione ricade nelle figure di fabbricanti e costruttori. Queste direttive sono soggette alla risoluzione 85/C 136/01 che introduce una nuova strategia legislativa denominata di "nuovo approccio". I prodotti devono essere conformi ai requisiti

esposti nelle direttive[3] e la conformità è raggiunta attraverso specifiche procedure di certificazione che possono richiedere l'intervento di organismi terzi notificati, la redazione di una dichiarazione di conformità, l'apposizione di specifica marcatura (es. marcatura CE, marcatura ATEX) e la redazione di documentazione tecnica che illustri le soluzioni progettuali adottate e che ne dimostri la congruenza con i requisiti essenziali. Aspetto importante è che la conformità può essere ottenuta anche attraverso l'applicazione di norme tecniche armonizzate.

Tra queste vi è la direttiva 2006/42/CE "Macchine" che modifica la precedente 95/16/CE, recepita in Italia con il D. Lgs.17/2010. Definisce requisiti essenziali di sicurezza (RES), prescrizioni progettuali inderogabili, per determinate categorie di prodotti che vengono classificati in macchine[4] e quasi-macchine[5], così come la gestione delle pratiche e responsabilità ai fini dell'immissione sul mercato e della loro messa in servizio. La progettazione e costruzione di macchine e quasi-macchine segue i "principi d'integrazione di sicurezza*"* definiti al punto 1.1.2 dell'Allegato I e si basa su un'analisi di valutazione dei rischi. In particolare il fabbricante o costruttore è tenuto a progettare la macchina o quasi-macchina adottando misure che eliminino pericoli o riducano rischi durante tutta la loro esistenza (trasporto, montaggio, smantellamento, rottamazione, manutenzione) nelle condizioni di uso corretto o scorretto ragionevolmente prevedibile. La scelta delle soluzioni di sicurezza adottate segue un preciso ordine di priorità: si tenta di eliminare nella misura del possibile pericoli adottando regole di buona tecnica in fase di progettazione, si adottano ulteriori sistemi di protezione verso rischi non eliminati e se vi fossero ancora dei rischi ineliminabili non trascurabili gli utilizzatori vengono informati e se necessario viene previsto l'uso di dispositivi di protezione individuale.

In relazione alle applicazioni nell'industria di processo si evidenzia come anche un impianto tecnologico rientri nella definizione di macchina intesa come "*insiemi di macchine […] o di quasi-macchine che per raggiungere uno stesso risultato sono disposti e comandati in modo da avere un funzionamento solidale*" e pertanto soggetto alle disposizioni richieste dalla suddetta direttiva.

---

[3] Antecedentemente alla risoluzione i prodotti dovevano sottostare a norme che definivano in modo particolareggiato le caratteristiche costruttive.

[4] Insieme equipaggiato o destinato ad essere equipaggiato di un sistema di azionamento diverso dalla forza umana o animale diretta, composto di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidamente per un'applicazione ben determinata, così come quelle al quale mancano solamente elementi di collegamento al sito di impiego o di allacciamento alle fonti di energia e di movimento.

[5] Insiemi che costituiscono quasi una macchina, ma che, da soli, non sono in grado di garantire un'applicazione ben determinata.

Le direttive sociali stabiliscono, invece, requisiti di salute, igiene, condizioni lavorative, occupazione, formazione e diritto sindacale dei lavoratori sul luogo di lavoro, nonché requisiti di sicurezza sociale. In questo caso la responsabilità di conformità alle stesse ricade nel datore di lavoro.

1.3.2 Norme tecniche

Le norme tecniche sono delle pubblicazioni che definiscono le caratteristiche costruttive, progettuali, organizzative di un certo prodotto o servizio, rappresentano uno standard di riferimento. Vengono rilasciate da enti di normazione, ossia comitati tecnici, specializzati in alcuni ambiti di competenza e a seconda della loro estensione operativa, le norme possono avere valenza nazionale, europea o internazionale.
Le norme vengono nominate con una sigla, costituita da un numero identificativo e l'anno di pubblicazione, anteposto dall'acronimo dell'ente che l'ha redatta e/o recepita. Vengono riviste e aggiornate con cadenza periodica per perseguire lo sviluppo tecnico più attuale raggiunto in un certo momento (stato dell'arte in materia). Le norme internazionali vengono adottate su base volontaria dai singoli stati. Tutte le norme recepite/elaborate a livello europeo, invece, devono essere obbligatoriamente accolte da tutti gli stati membri, abrogando eventuali norme nazionali contrastanti, lo scopo: avere un comune quadro legislativo di riferimento.

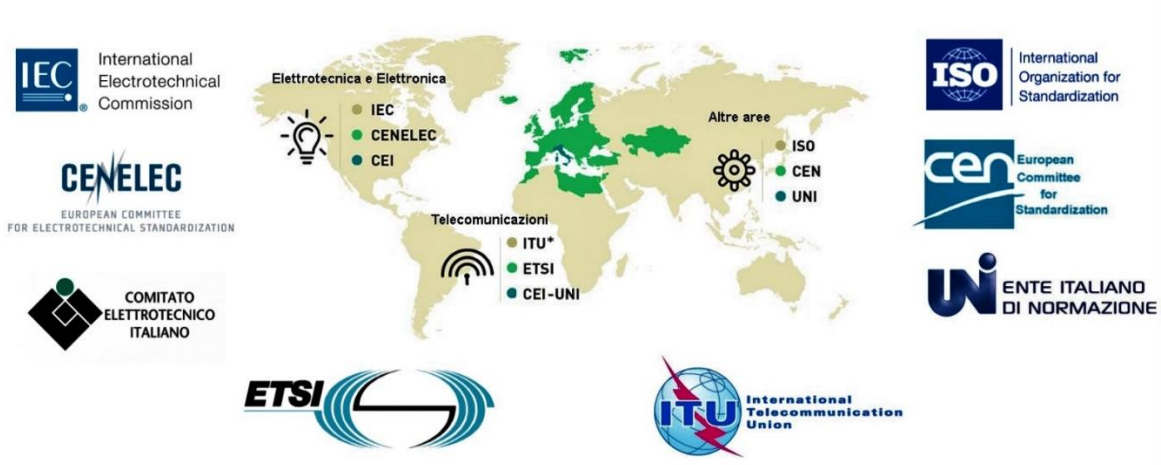

Figura n.1.2 Principali enti di normazione e rispettive aree di competenza

Le norme tecniche non hanno potere giuridico e pertanto non costituiscono un obbligo, ad eccezione di casi esplicitamente richiesti, se vengono seguite il prodotto o servizio si definisce realizzato "a regola d'arte "e in ogni caso costituiscono una garanzia di qualità.
Importante aspetto da evidenziare è che queste specifiche quando armonizzate, ossia recepite a livello europeo e pubblicate nella Gazzetta ufficiale dell'Unione europea, hanno potere di conferire "presunzione di conformità", ossia dimostrare di rispondere a certi requisiti essenziali richiesti dalle direttive prodotto definite precedentemente, diventando un potente strumento di supporto contro eventuali contenziosi legali, nonché facilitare la redazione della documentazione tecnica. La volontarietà delle stesse consente, in ogni caso, libertà progettuale eliminando qualsiasi ostacolo per innovazioni e prodotti non ancora normati.

1.4 Sicurezza: concetti e definizioni

1.4.1 Sicurezza e pericolo

Di seguito si cerca di fornire un'interpretazione più formale del concetto di sicurezza.
Al fine della comprensione è opportuno, anzitutto, definire il concetto di evento iniziatore, in riferimento ad applicazioni tecnico-industriali. Con questo termine si intende un qualunque evento che porti un sistema esaminato (es. componente, macchinario, impianto) in una condizione di possibile danno, cioè di pericolo. Il verificarsi di un guasto o un incidente rappresenta, per esempio, un evento iniziatore. Da tenere presente che la condizione di pericolo non implica necessariamente il verificarsi di un danno, ma questo possiede una certa probabilità di accadere, ossia un rischio.

Si consideri un gruppo di N oggetti di uguali caratteristiche e testati nelle medesime condizioni per un determinato intervallo di tempo T, a partire da un istante iniziale nullo. Con $n\_sani(T)$ si indichi il numero di elementi nei quali non si sono verificati eventi iniziatori nell'intervallo $t = [0; T]$, con $n\_guasti(T)$, invece, quelli in cui avviene.
È possibile definire sicurezza $S(t)$ con il seguente rapporto (1.1); rappresenta la probabilità di trovare dopo un intervallo T l'elemento ancora sano e pertanto può assumere dei valori compresi tra $[0; 1]$:

$$S(T) = \frac{n\_sani(T)}{N} \qquad (1.1)$$

Ad $S(t)$ è associata, dunque, l'affidabilità del sistema in relazione alla sicurezza nel tempo, ed è strettamente correlata al concetto di pericolo o inaffidabilità, espresso come il suo complementare:

$$F(t) = \frac{n\_guasti(t)}{N} = 1 - S(t) \qquad (1.2)$$

In particolare tenendo conto della funzione tasso di guasto[6] (1.3), definita come densità di probabilità che si verifichi un evento sfavorevole nell'intervallo t e dt in un oggetto considerato sano al tempo t e assunta costante nel tempo:

$$\lambda(t) = \frac{1}{n\_sani(t)} * \frac{dn\_guasti(t)}{dt} = -\frac{1}{S(t)} * \frac{dS(t)}{dt} \qquad (1.3)$$

è possibile rappresentare $S(t)$ come una funzione avente un andamento esponenziale:

$$S(t) = e^{-\int_0^t \lambda(\tau) * d\tau} = e^{-\lambda * t} \qquad (1.4)$$

Da notare come per $t \to \infty$, la funzione tenda asintoticamente a zero e quindi come prima o poi un qualsiasi oggetto diventi un pericolo. Essa assume valore nullo anche quando il sistema considerato rappresenta esso stesso una potenziale fonte di danno, senza che si verifichi un evento sfavorevole affinché lo diventi, è il caso in cui $\lambda \to \infty$.
Nel caso di sistemi complessi, cioè costituiti da più componenti ai quali è associato un certo tasso di guasto, è possibile definire *S(t)* relativo all'intero sistema a seconda di come questi sono interconnessi tra loro. In particolare si distinguono due tipologie di sistemi: sistemi in serie e sistemi in parallelo.

Nei sistemi in serie il funzionamento dipende dal contemporaneo funzionamento di tutti i gli elementi che lo compongono. Se questi si considerano indipendenti tra loro[7], ossia che il

[6] Funzione che rappresenta una "velocità di guasto" del sistema in considerazione. Viene dichiarata da fabbricanti e costruttori ed è espressa comunemente in guasti/h o numero di azionamenti al guasto. È stato studiato che un modello tipico di tasso di guasto per un qualsiasi componente segue l'andamento della "bathtub curve". Si può riferire a guasti pericolosi (dangerous) e non (safe). A loro volta questi possono essere classificati in guasti rilevati, ad esempio da un sistema di diagnostica o monitoraggio (detected) e non rilevati (undetected). Il tasso di guasto valutato per un certo componente si riferisce alla somma dei guasti pericolosi/non pericolosi, rilevati/non rilevati.
[7] È possibile pertanto considerare probabilità incondizionate.

verificarsi di un evento sfavorevole in uno di essi non influenzi la funzionalità degli altri, la *S(t)* si esprime come:

$$S(t) = \prod_{i=1}^{n} S(t)_i = e^{-(\sum_{i=1}^{n} \lambda_i)*t} \tag{1.5}$$

È possibile notare che in questa configurazione la *S(t)* complessiva diminuisca con il numero di componenti e sia minore del componente meno sicuro.

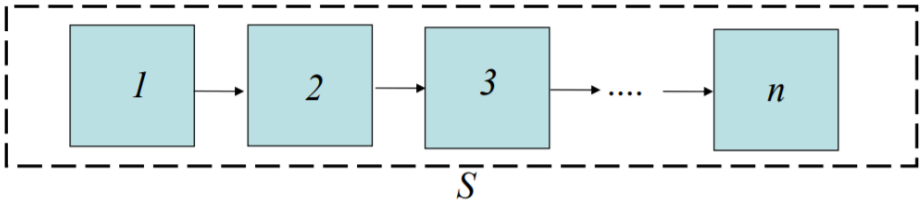

Figura n.1.3 Schema connessione in serie

Nei sistemi in parallelo la funzionalità viene persa se in tutti gli elementi che lo compongono si perde la funzione. È il caso di sistemi ridondanti. In questo caso sempre nell'ipotesi di indipendenza tra i vari componenti, *S(t)* si esprime come:

$$S(t) = 1 - \prod_{i=1}^{n}(1 - S(t)_i) = 1 - \prod_{i=1}^{n}(1 - e^{-\lambda_i * t}) \tag{1.6}$$

In questo caso l'affidabilità aumenta con il numero di componenti interconnessi ed è maggiore del componente più sicuro.

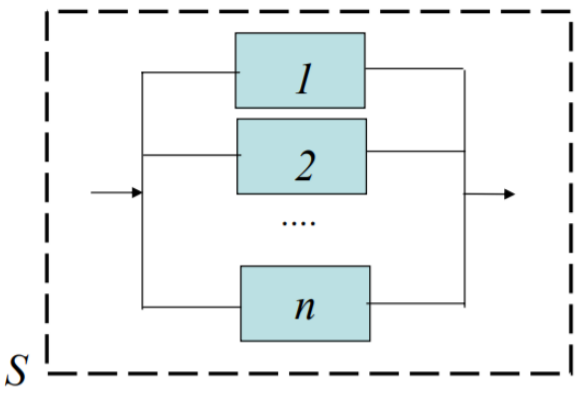

Figura n.1.4 Schema connessione in parallelo

Agire in funzione della sicurezza significa, pertanto, adottare un comportamento volto ad evitare l'insorgenza di eventi sfavorevoli, eliminare la presenza di pericoli o adottare soluzioni per mitigare le eventuali conseguenze dannose che questi possono comportare.

1.4.2 Il rischio

Come anticipato al paragrafo precedente, il rischio rappresenta la probabilità associata ad un evento dannoso, come conseguenza alla presenza di un certo pericolo. Viene definito come:

$$R(t) = [1 - S(t)] * f * d \quad (1.7)$$

Dove f rappresenta la probabilità che questo possa accadere, mentre d la magnitudo o gravità associata al danno che può verificarsi. È importante sottolineare che ha senso parlare di rischio solo in presenza di pericoli, ossia quando il termine $[1 - S(t)]$ sia diverso da zero.

1.5 Sistemi di sicurezza

I sistemi di sicurezza o *protection layer* (PL) sono i mezzi attraverso i quali è possibile garantire che una certa attività venga svolta in modo sicuro. Sono rappresentati da tutte quelle strumentazioni, sistemi, o procedure operative che svolgono la funzione di protezione e prevenzione nei confronti di pericoli.
È possibile identificare una sottocategoria di questi sistemi di sicurezza denominata *Indipendent protection layer* (IPL). È questa la tipologia di protezioni che verrà considerata durante la progettazione e l'implementazione di funzioni di sicurezza. Affinché un PL possa essere considerato tale, deve presentare determinate caratteristiche, in particolare:

- Specificità: essere progettato per svolgere una funzione per uno specifico pericolo.
- Indipendenza: non essere influenzato da altri sistemi di protezione in relazione all'accadimento del medesimo evento di pericolo.
- Affidabilità: garantire un certo fattore di sicurezza noto e quantificato secondo opportune unità di misura, così come l'inaffidabilità, intesa come probabilità di guasti casuali e sistematici.

- Verificabilità: permettere una convalida periodica attraverso test diagnostici e manutentivi.
- Garantire un PFD_{avg}[8] $\leq 10^{-1}$.

Di seguito si riporta uno schema con le categorie di PL/IPL riscontrabili in un impianto di processo.

Figura n.1.5 Organizzazione di PL/IPL in un contesto impiantistico

I sistemi di sicurezza (PL/IPL) possono essere suddivisi in ulteriori classificazioni.

- Sistemi attivi: il funzionamento dipende dalle azioni intraprese da parte di un operatore o un sistema di controllo.
- Sistemi passivi: il funzionamento non dipende dalle azioni intraprese da parte di un sistema esterno. (es. barriere fisiche)

- Sistemi proattivi: riducono la probabilità che un certo pericolo si manifesti, influiscono sulla frequenza di accadimento dello stesso (es. SIS, allarmi, sistema di controllo di processo BPCS, azione di un operatore).
- Sistemi reattivi: riducono le conseguenze che un certo pericolo può comportare, mitigano i danni probabili che questo può arrecare (es. barriere fisiche, sistema antincendio, rilevatori di fumo e gas).

[8] Average probability of failure on demand. Si riferisce solo a guasti pericolosi, cioè che impediscono l'attivazione della funzione di sicurezza.

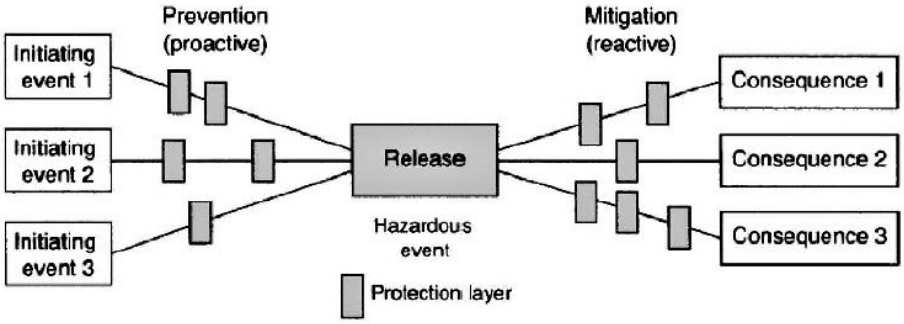

Figura n.1.6 Protezioni proattive e reattive

1.5.1 Sicurezza funzionale

Con sicurezza funzionale si intende quella categoria di soluzioni di sicurezza (*safety*) proattive o reattive che fa affidamento su circuiti di comando e controllo. Queste rientrano nella definizione di componente di sicurezza[9] oggetto della Direttiva "Macchine" ed elencate in Allegato V come "*blocchi logici per assicurare funzioni di sicurezza"*, pertanto vincolate ai RES definiti dalla direttiva. Le funzioni di sicurezza, *safety instrumented function* (SIF), richieste, vengono tipicamente implementate in sistemi elettrici/elettronici/elettronici programmabili (E/E/PE), che sono in grado di svolgere un'azione attiva a fronte di determinate circostanze. Sono in grado di intervenire riportando il sistema ad uno stato sicuro, interrompendo una situazione che può comportare un pericolo o avviando processi di salvaguardia. La sicurezza funzionale subentra quando non viene garantita una sicurezza intrinseca alla progettazione del sistema.
L'organizzazione di un circuito relativo alla sicurezza funzionale, *safety instrumented system* (SIS), può essere organizzata in tre sottosistemi interconnessi in serie:

- dispositivi di input: sono quegli elementi che compongono il circuito di comando e a seguito del verificarsi di un certo evento, generano dei segnali in ingresso al sistema di controllo, più semplicemente attivano la funzione di sicurezza. Questa funzione viene svolta tipicamente da sensori e/o switch nelle più svariate tecnologie: meccaniche, elettriche, magnetiche, oleodinamiche, pneumatiche, RFID, ottiche o

[9] Componente destinato ad espletare una funzione di sicurezza, immesso sul mercato separatamente, il cui guasto e/o malfunzionamento, mette a repentaglio la sicurezza delle persone, e che non è indispensabile per lo scopo per cui è stata progettata la macchina o che per tale funzione può essere sostituito con altri componenti. Rientra nella categoria più generica di macchina.

basate su telecamera; alcuni esempi possono essere rappresentati da sensori di flusso, pressione, temperatura, barriere fotoelettriche, switch di arresto di emergenza o contatti ad azione positiva.

Figura n.1.7 Esempio di sensori digitali di pressione e livello (da sinistra a destra)

- logica di controllo: svolge un'attività di elaborazione dei segnali ricevuti dal circuito di comando. Attraverso software caricato e i dati ricevuti predispongono comandi automatici mediante circuiti di potenza sui dispositivi in uscita. Viene gestita da controllori logico programmabili, centraline, relay, moduli e PLC di sicurezza;

Figura n.1.8 Esempio di controller di sicurezza modulare

- dispositivi di output: dispositivi che attuano la funzione di sicurezza ad esempio attraverso, teleruttori, valvole e servo-azionamenti.

Figura n.1.9 Esempio di unità controllo attuatore per funzioni di sicurezza

La progettazione di un circuito di sicurezza funzionale, implica pertanto considerare l'interconnessione di queste tre categorie di dispositivi, ed è essenziale la determinazione della SIF da implementare e l'affidabilità che questa deve essere in grado di offrire, durante la valutazione dei rischi. In particolare quest'ultima caratteristica viene quantificata mediante un parametro, che a seconda della normativa di riferimento, prende il nome di *Performance Level* (PL), o *Safety Integrity Level* (SIL). Entrambi i parametri si riferiscono alla capacità del sistema di eseguire una funzione di sicurezza in determinate condizioni. Vengono suddivisi in livelli discreti, associati ad un certo grado di affidabilità espresso in PFD_{avg} o PFHd[10]. Seguono delle procedure di calcolo differente, ma solitamente nelle norme vengono fornite tabelle in cui è possibile definire una corrispondenza tra i due: nell'ultimo capitolo questi concetti verranno ripresi con un maggiore approfondimento in relazione alla normativa internazionale *IEC 61511: Sicurezza funzionale – Sistemi strumentati di sicurezza per il settore dell'industria di processo*, che ne definisce i criteri di progetto.

[10] Probability of a dangerous failure per hour. Si riferisce a guasti pericolosi, rilevati e non.

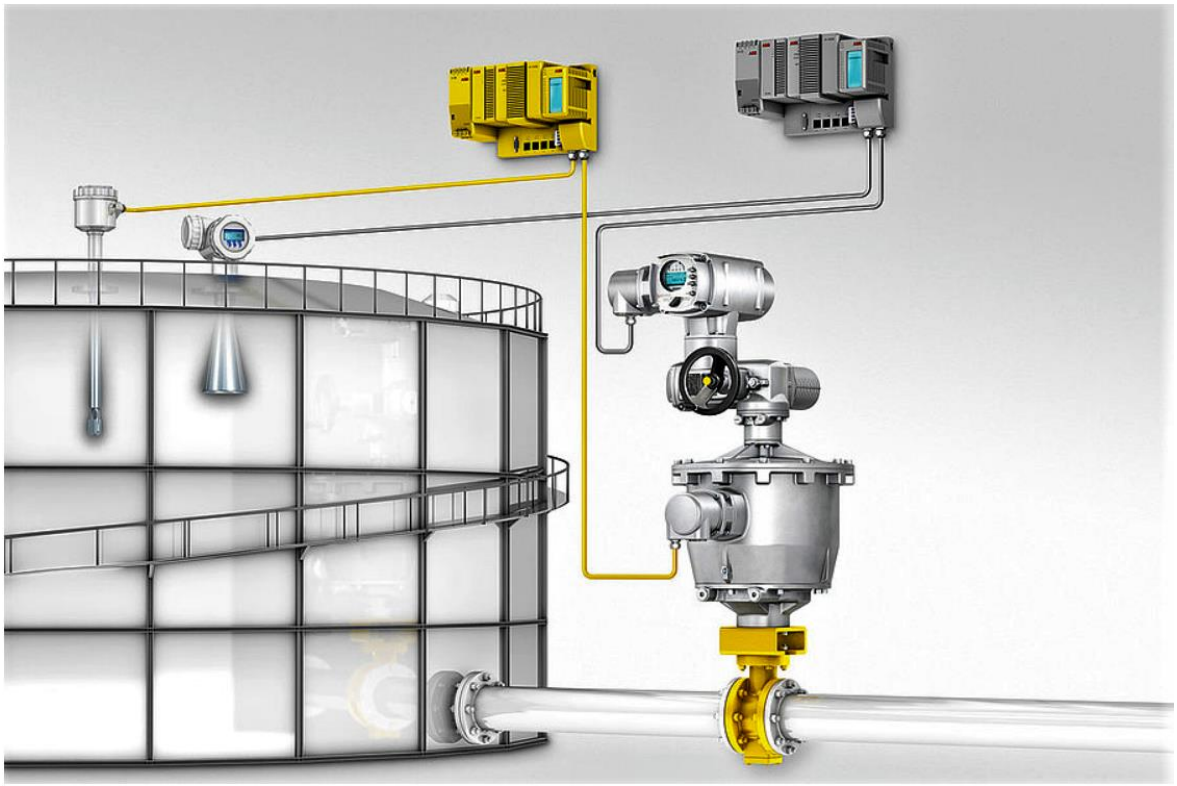

Figura n.1.10 Esempio di circuito SIS che realizza una SIF (in giallo)

1.5.2 Architettura K out of N (KooN)

KooN è una configurazione basata su sistemi ridondanti che viene applicata, tipicamente (ma non solo), agli elementi di input di un SIS. Questa architettura viene implementata non solo per soddisfare vincoli hardware progettuali normativi (Hard Fault Tolerance) per raggiungere un dato livello di sicurezza e raggiungere una maggiore tolleranza ai guasti ed affidabilità, ma anche per prevenire guasti spuri di una funzione SIF, che causano fermi macchina non necessari. Secondo questa architettura un sistema KooN è composto da N elementi ridondanti; per attivare una funzione SIF è necessario che la logica di controllo riceva un segnale da M dei suoi elementi e prima che la SIF venga perduta, il sistema è tollerante ad (N – K) guasti. È chiaro che nel caso fosse utilizzato un sistema con un unico elemento (configurazione 1oo1), è sufficiente un unico guasto per perdere la funzionalità o una falsa attivazione per un fermo macchina. Per questo evitare quest'ultima condizione si prediligono sistemi con $K \geq 2$.

Assumendo come ipotesi che gli elementi di un sistema KooN abbiano canali identici ed indipendenti, testati nel medesimo istante e con un tempo di non disponibilità trascurabile è possibile ottenere delle formule approssimate per il calcolo del PFD del sistema:

k/n	1	2	3	4
1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
2	–	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
3	–	–	$\frac{2\lambda_{DU}\tau}{2}$	$2(\lambda_{DU}\tau)^2$
4	–	–	–	$2\lambda_{DU}\tau$

Figura n.1.11 Tabella PFD sistemi KooN

1.5.3 PFD, PFH

Sono parametri associati ad un componente o ad un sistema che consentono di assegnare un certo livello di sicurezza.

Il probability of failure on demand (PFD) corrisponde alla probabilità che un certo sistema si guasti in un certo intervallo di tempo ed impedisca l'esecuzione di una certa funzione di sicurezza, apparecchiatura o causi perdite di vite. L'intervallo temporale in cui questo viene valutato è il tempo delle prove di verifica periodiche che vengono stabilite in fase di progettazione del sistema (es. 1 anno per sistemi on demand mode, 3 mesi per sistemi in continuous mode) e a seguito di ogni test di prova il sistema viene considerato "*as good as new"*. Nella valutazione si considera solo il tasso di guasti pericolosi non rilevati (dangerous undetected).

$$PFD(t) = 1 - e^{-\lambda_{DU}*t} \tag{1.8}$$

Nella normativa si fa riferimento al valore medio, considerando τ l'intervallo tra una prova periodica ed un'altra.

$$PFD_{avg} = \frac{1}{\tau} * \int_0^{\tau} \left(1 - e^{-\lambda_{DU}*t}\right) * dt \tag{1.9}$$

I guasti che coinvolgono normalmente gli elementi di un SIS sono: guasti al trasmettitore, rotture meccaniche (sensori), guasti a relay, CPU, circuiti di I/O, cortocircuiti, apertura di circuiti (logica di controllo), blocco dell'albero, otturatore, guasto del solenoide (attuatori).

Per quanto riguarda il calcolo del PFD associato all'intero sistema SIS, questo può essere approssimato al contributo dei PFD di ciascun elemento di cui è costituito ($PFD_{sensore}$ + $PFD_{logica\ di\ controllo}$ + $PFD_{attuatore}$).

Nel caso di sistemi ridondanti occorre tenere in considerazione l'effetto dei *Common Cause Failures* (CCF), secondo il modello del fattore ß[11]. Nel calcolo del PFD il λ_{DU} associato ai vari elementi del sistema è affetto dal parametro ß, e l'effetto del CCF viene considerato come un guasto indipendente dall'evento multiplo di guasti indipendenti, ponendolo in serie al sistema ridondante quanto segue:

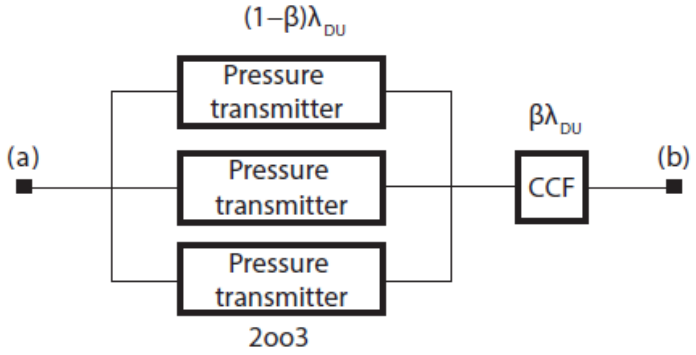

Figura n.1.12 Esempio inclusione CCF in un sistema 2003 di componenti identici

Il PFD del sistema ridondante pertanto può essere calcolato come la probabilità di guasto del sistema ridondante (con il nuovo tasso di guasto associato) e il contributo del CCF:

$$PFD_{avg} = PFD_{avg,sist} + PFD_{avg,CCF} \quad (1.10)$$

Il probability of dangerous failure per hour (PFH) viene valutato come la frequenza oraria del verificarsi di un guasto pericoloso, viene considerato normalmente per sistemi in continuous mode.

[11] Il modello del fattore ß assume che una frazione del tasso di guasto λ_{DU} sia dovuta esclusivamente ad eventi CCF, mentre la restante a guasti indipendenti. $\lambda_{DU} = (1- ß)* \lambda_{DU} + ß* \lambda_{DU}$. ß è considerata come la probabilità condizionata che un guasto in un canale sia un guasto CCF. Da normativa viene valutata attraverso un giudizio tecnico basato su punteggi assegnati su certe caratteristiche relative ad un sistema.

Capitolo 2: Seveso, l'incidente e la direttiva

2.1 Introduzione

Per certe applicazioni agire in favore della sicurezza riveste un ruolo di maggiore rilievo, in particolare quando i danni che possono verificarsi coinvolgono un contesto più ampio, non solo interno al sito di lavoro, ma anche in termini di vite civili e salvaguardia ambientale; questo fa sì che venga pubblicata specifica regolamentazione.

È il caso della direttiva sociale "Seveso", che trova vasta attuazione nell'industria di processo dove l'organizzazione delle misure di sicurezza viene affidata ad un sistema di gestione.

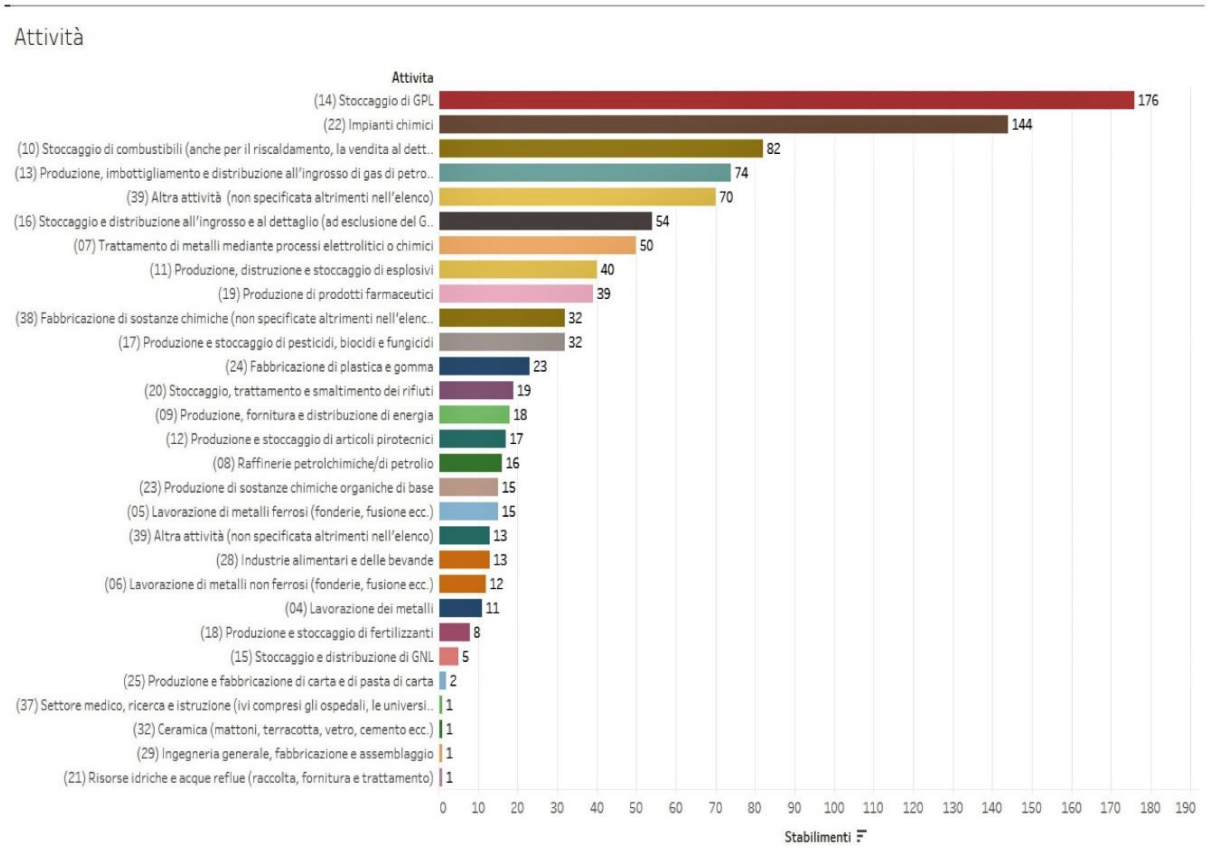

Figura n.2.1 Tipologie di stabilimenti a pericolo di incidente rilevante (dati ISPRA aggiornati al 30/06/19)

Di seguito ne verranno evidenziati gli aspetti principali nonché quelli in stretta relazione alla valutazione del rischio e sicurezza funzionale. Viene fornita anche una descrizione degli eventi che ne hanno portato la nascita, per sottolineare l'importanza che questa rappresenta non solo dal punto di vista pratico, ma anche storico.

2.2 L'incidente, 10 luglio 1976

A 26 km a nord di Milano, nel comune di Meda, da uno stabilimento chimico, vengono rilasciati nell'atmosfera circa 400Kg di sostanze chimiche tra cui TCDD (2,3,7,8-tetraclorodibenzo-p-diossina), la variante più tossica della classe di composti delle diossine e tutt'oggi classificata come agente cancerogeno per l'uomo ed animali[12].
Lo stabilimento coinvolto nell'incidente fu l'ICMESA (Industrie Chimiche Meda Società Azionaria) appartenente al gruppo Givaudan & C. di Vernier S.A, una multinazionale svizzera, stabilitosi nel 1945 a Meda come produttrice di sostanze base per l'industria chimica, cosmetici e triclorofenolo fungicida utilizzato in disinfettanti, diserbanti agricoli e defoglianti, come l'Agent Orange utilizzato dagli Stati Uniti durante la guerra in Vietnam.
Fin dai primi anni di operatività l'impianto, battezzato come "la fabbrica dei profumi", ha sollevato grandi proteste nella comunità dei paesi adiacenti, come Seveso, per gli odori nauseabondi e maleodoranti provenienti dal torrente Certesa dovuti agli scarichi dell'impianto non adeguatamente depurati o per i fumi tossici prodotti da fuochi appiccati ai materiali di scarto. Numerose furono le analisi ed ispezioni condotte dalle autorità a conferma della nocività dell'impianto, ma di fatto non vennero mai prese efficienti contromisure, da entrambe le parti.

L'incidente avvenne nel reattore appartenente alla linea di produzione del triclorofenolo.
Al termine del turno di lavoro del venerdì, come di consueto per interrompere la produzione nell'impianto, al termine della reazione venne arrestato l'agitatore del reattore. Purtroppo, non si tenne conto della temperatura delle sostanze ancora troppo elevata, al di sopra della soglia di sicurezza e in assenza di una adeguata miscelazione i prodotti aumentarono ulteriormente di temperatura, si stima oltre ai 500°C, secondo una reazione conosciuta in letteratura tecnica con il termine di "runaway", determinando la formazione di TCDD. Nella sala del reattore non vi era disponibile alcun sistema di controllo di temperatura o pressione automatico, solo di tipo manuale gestibile da personale tecnico, che al momento dell'incidente non era presente in quanto giornata di pausa. Alle 12:40 del giorno successivo la pressione dei reagenti fu così elevata che determinò l'apertura del disco di rottura a valle del reattore, collegato direttamente all'esterno dell'impianto, con conseguente fuoriuscita

[10] Classificazione IARC Gruppo 1: Agenti cancerogeni per l'uomo e gli animali.

della nube tossica, che venne trascinata dal vento nelle zone circostanti dove l'area più interessata fu Seveso.

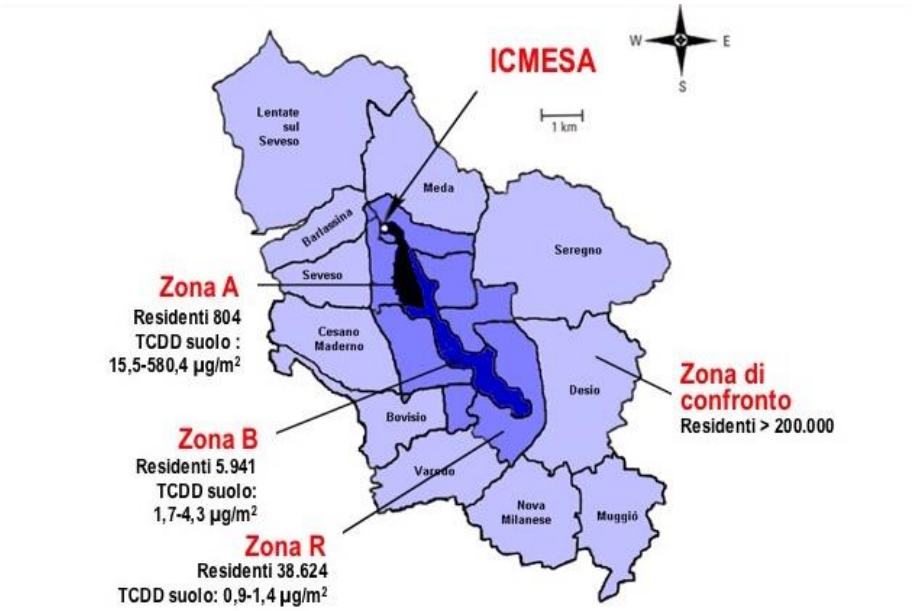

Figura n.2.2 Aree colpite dall'incidente

I primi provvedimenti a tutela della popolazione vennero intrapresi solamente cinque giorni dopo e dopo sedici iniziarono le prime evacuazioni delle zone colpite tra le proteste ed incertezze della gente. Nel frattempo vennero registrati un gran numero di casi di intossicazione e cloracne, una dermatosi provocata a seguito dall'esposizione prolungata al TCDD, inoltre, temendo malformazioni nel feto, molte furono le donne che decisero di procedere all'aborto, al tempo illegale, ma consentito da una legge deroga dal governo Andreotti. Gravi segni di bruciatura vennero lasciati su tutta la vegetazione e una moria di una grande quantità di animali ai quali si aggiunsero quelli abbattuti dalle autorità, per evitare che entrassero nella catena alimentare.

Tra il 1979 e 1986 viene condotta un'attività di rimboschimento e bonifica del terreno che portò alla trasformazione di parte della "zona A" in area verde, l'attuale Bosco delle Querce, nella quale vennero realizzate due vasche di confinamento controllato, contenenti il materiale inquinato.

Decessi	0
Animali morti + abbattuti	3300 + 76000
Intossicazioni	626

Sfollati	676
Materiale tossico	280000 m^3

Tabella n.2.1 Numeri dell'incidente

Secondo quanto emerso da successive indagini, l'incidente all'ICMESA è da attribuirsi ad un errore di comunicazione tra tecnici dell'impianto, così come da una cattiva politica aziendale. Difatti, secondo quanto riportato nell'articolo [14] nelle dichiarazioni in un libro-confessione da Jorg Sambeth, ex direttore tecnico della Givaudan, emerge l'assenza di un adeguato piano di gestione del rischio: insufficienza di strumentazioni di sicurezza o sistemi di allarme, formazione del personale, limitata conoscenza sulle inattese deviazioni dei normali processi termo-chimici.
La vera causa, però, pone radici ben più profonde. La scena industriale italiana di inizio anni '70 si presenta incentrata al profitto e alla produzione a basso costo accompagnata da un esasperato sfruttamento delle risorse ecologiche, il tutto gestito da un esile sistema di regolamentazione costituito da una manciata di norme, per di più circoscritte ad alcuni settori e da un apparato di enti e istituzioni di controllo inefficienti, sia dal punto di vista tecnologico che organizzativo.

A seguito del disastro ci si iniziò a domandare fino a che punto il benessere economico possa coincidere con il benessere del Paese e solo successivamente la Commissione europea si adoprerò verso una maggiore sensibilizzazione legislativa volta a gestire e prevenire incidenti industriali, conosciuta tutt'oggi come Direttiva "Seveso". Nei due anni antecedenti si erano già verificati una serie incidenti simili, di cui si ricordano Flixborough (1974) e Beek (1975), ma di fatto le conseguenze sono sempre rimaste circoscritte al sito di lavoro.

2.3 La direttiva "Seveso III": generalità e campo di applicazione

L'azione legislativa, "post-Seveso", viene condotta per la prima volta dalla Comunità economica europea (CEE) nel 1982, con l'adozione di misure a livello comunitario; lo scopo, condiviso da tutte le versioni successive (art.1): la "*prevenzione di incidenti rilevanti [...] così come la limitazione delle loro conseguenze per l'uomo e l'ambiente*".

Nel tempo queste hanno subito modifiche, integrazioni ed abrogazioni fino ai giorni attuali, un'evoluzione che si articola principalmente in tre fasi, coprendo un arco temporale di trent'anni.

- Direttiva 82/501/CEE, "Seveso I" recepita con D.P.R. 17 maggio 1988, n.175;
- Direttiva 96/82/CE, "Seveso II" recepita con D.lgs. 17 agosto 1999, n.334;
- Direttiva 2003/105/CE "Seveso II-bis" recepita con D.lgs. 21 settembre 2005, n.238 (aggiornamento della Seveso II);
- Direttiva 2012/18/UE "Seveso III" recepita con D.lgs. 26 giugno 2015, n.105.

Di seguito si farà riferimento alla direttiva 2012/18/UE "Seveso III", attualmente in vigore.

La direttiva generale 2012/18/UE, che va a modificare ed abrogare la precedente 96/82CE, con effetto dal 1° giugno 2015, viene recepita in Italia con il D.lgs. del 26 giugno 2015 n.105, a seguito della sua pubblicazione nella Gazzetta Ufficiale.
Di fatto questa trova applicazione negli impianti (art.3) definiti come:
"*unità tecnica all'interno di uno stabilimento e che si trovi sia a livello suolo che a livello sotterraneo, nel quale sono prodotte, utilizzate, maneggiate o immagazzinate le sostanze pericolose; esso comprende tutte le apparecchiature, le strutture, le condotte, i macchinari, gli utensili, le diramazioni ferroviarie private, le banchine, i pontili che servono all'impianto, i moli, i magazzini e le strutture analoghe, galleggianti o meno, necessari per il funzionamento di tale impianto*".
La presente direttiva lega la presenza di pericoli e rischi alla presenza di certi quantitativi di sostanze pericolose specificate nell'Allegato 1 della stessa. Questo è anche il medesimo criterio che porta alla classificazione di due tipologie di stabilimenti, per i quali sono previste procedure amministrative differenti: stabilimenti di soglia inferiore e stabilimenti di soglia superiore, dove per stabilimento (art. 3) si intende:
"*tutta l'area sottoposta al controllo di un gestore, nella quale sono presenti sostanze pericolose all'interno di uno o più impianti, comprese le infrastrutture o le attività comuni o connesse*".

Vengono esclusi dalla direttiva (art. 2), perché non contemplati o gestiti da legislazioni più specifiche:

- Stabilimenti, impianti e depositi militari
- Pericoli connessi alle radiazioni ionizzanti derivanti dalle sostanze
- Il trasporto di sostanze pericolose e al deposito temporaneo intermedio direttamente connesso su strada, per ferrovia, per idrovia interna e marittima o per via aerea, comprese le attività di carico e scarico e al trasferimento da e verso un altro modo di trasporto alle banchine, ai moli o agli scali ferroviari di smistamento, al di fuori degli stabilimenti soggetti alla presente direttiva
- Il trasporto di sostanze pericolose in condotte, comprese le stazioni di pompaggio al di fuori degli stabilimenti soggetti alla presente direttiva
- Lo sfruttamento, vale a dire l'esplorazione, l'estrazione e la preparazione di minerali in miniere e cave, anche mediante trivellazione
- L'esplorazione e allo sfruttamento offshore di minerali, compresi gli idrocarburi;
- Stoccaggio di gas in siti sotterranei offshore, compresi i siti di stoccaggio dedicati e i siti in cui si effettuano anche l'esplorazione e lo sfruttamento di minerali, tra cui idrocarburi;
- Discariche di rifiuti, compresi i siti di stoccaggio sotterraneo;
- Ad eccezione dello stoccaggio sotterraneo sulla terraferma di gas in giacimenti naturali, acquiferi, cavità saline o miniere esaurite e le operazioni di preparazione chimica o termica e il deposito a esse relativo, che comportano l'impiego di sostanze pericolose nonché gli impianti operativi di smaltimento degli sterili, compresi i bacini e le dighe di raccolta degli sterili, contenenti sostanze pericolose, che sono inclusi nell'ambito di applicazione della presente direttiva.

La direttiva mira a garantire il controllo del pericolo di incidenti rilevanti considerando non solo esclusivamente il sito di lavoro, ma inserendo lo stabilimento in un contesto urbanistico e territoriale. Questo avviene attraverso un approccio organizzativo e gestionale, applicato quindi non solo agli aspetti più tecnici della sicurezza, ma si traduce anche in una gestione dei rapporti con autorità e organismi di riferimento nazionali e regionali che svolgono ruolo nell'applicazione della stessa, in particolare per quanto concerne il controllo dell'urbanizzazione, il sistema di ispezioni e l'insieme delle procedure mitigative in caso di incidente rilevante del piano di emergenza esterno.

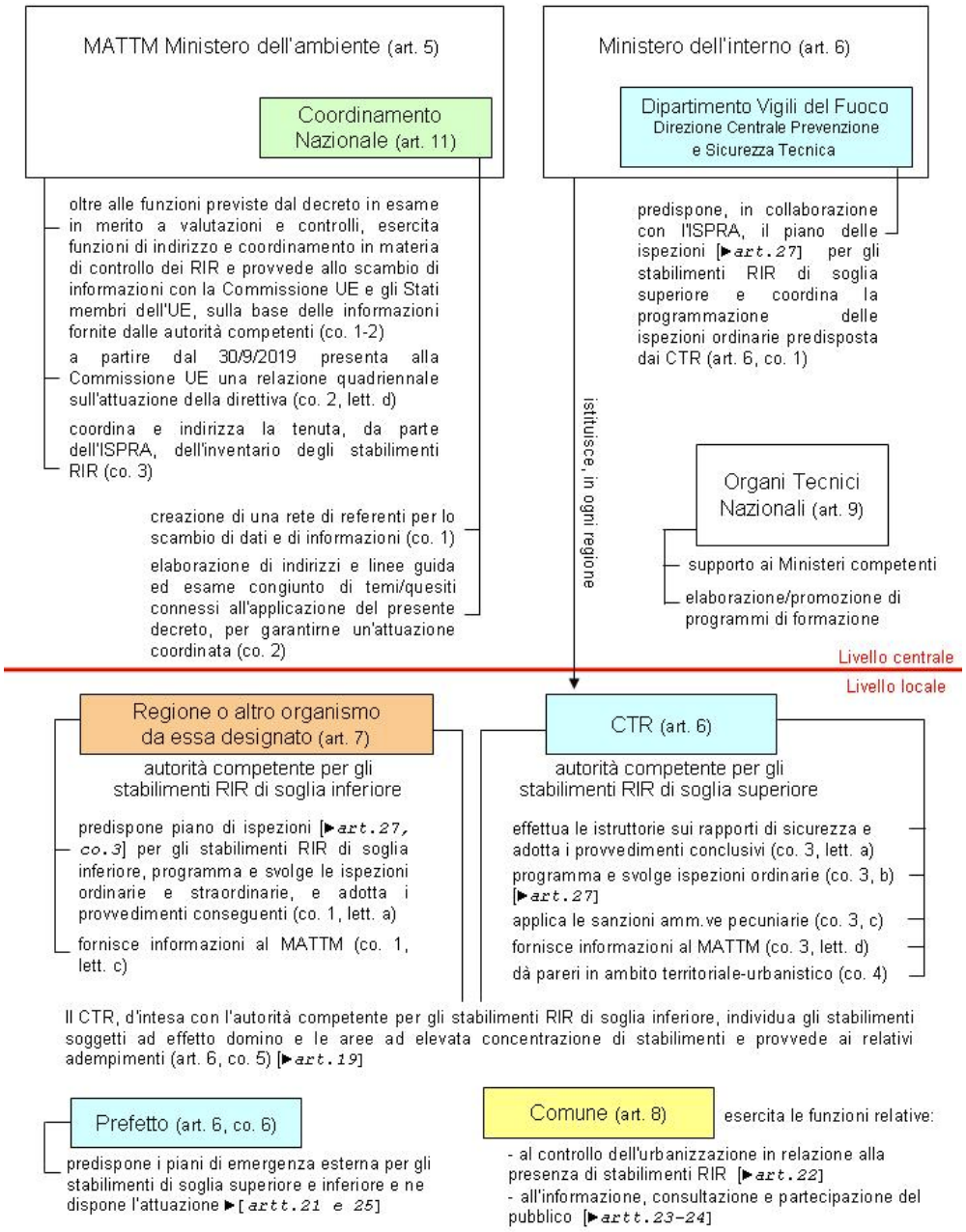

Figura n.2.3 Organizzazione e funzioni delle autorità competenti in accordo al D.lgs. 2015/15

Lo stesso vale per il pubblico interessato[13], il quale riceve informazioni in merito allo stabilimento e possiede diritto di partecipazione al processo decisionale per modifiche significative e realizzazione di nuovi stabilimenti.

[13] Pubblico che subisce o può subire gli effetti delle decisioni adottate su questioni disciplinate dall'art.15, paragrafo 1, o che ha un interesse da far valere in tali decisioni: ai fini della presente definizione le organizzazioni non governative che promuovono la protezione dell'ambiente e che soddisfano i requisiti applicabili di diritto nazionale si considerano portatrici di un siffatto interesse.

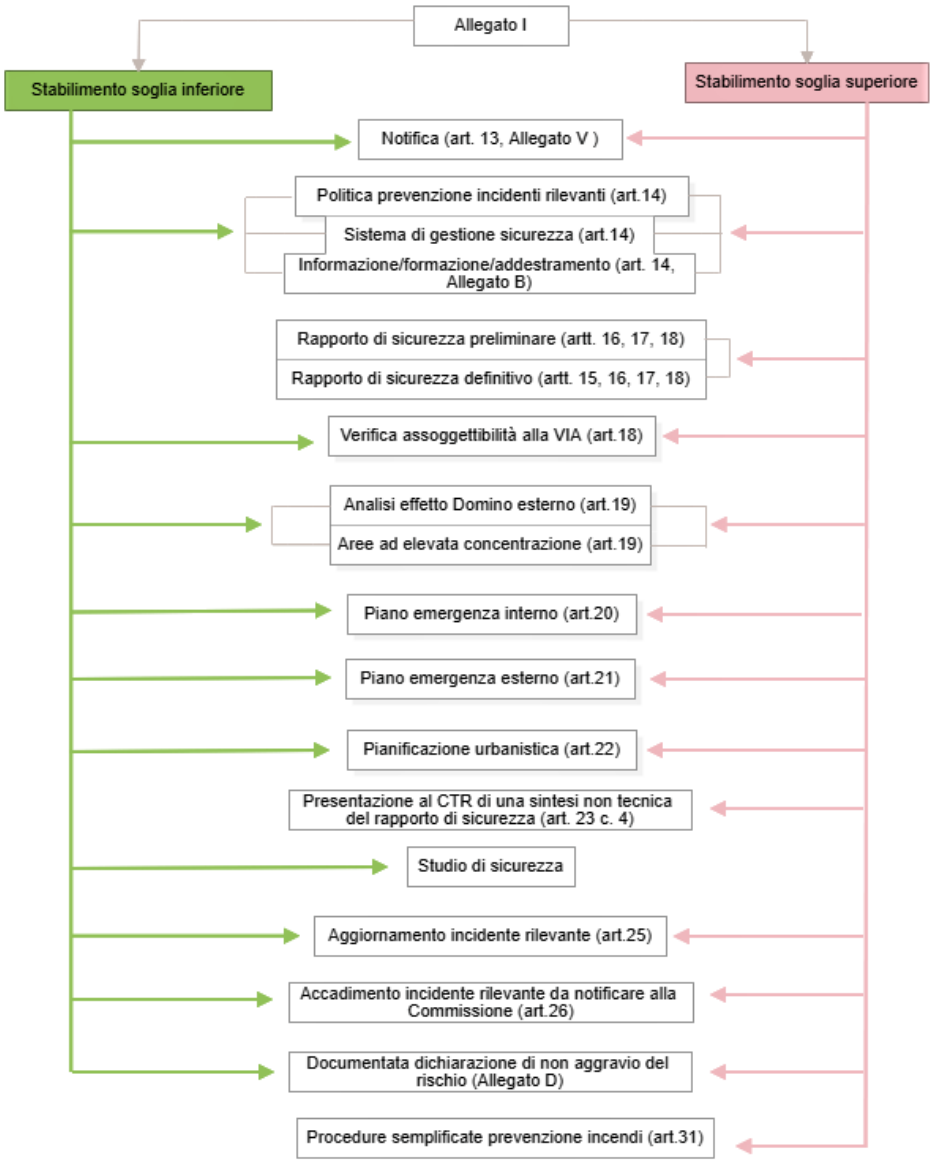

Figura n.2.4 Schema adempimenti del gestore in accordo al D.lgs. 2015/15

2.3.1 Il Sistema di gestione sicurezza

Il sistema di gestione della sicurezza (SGS), è l'elemento cardine della politica di prevenzione degli incidenti rilevanti (art.14), definita sotto diretta responsabilità del gestore per tutti gli stabilimenti oggetto dalla direttiva, e sottoposta ad ispezioni e riesami periodici. È lo strumento attraverso il quale individuare, attuare e gestire opportune soluzioni di sicurezza all'interno dello stabilimento a rischio di incidente rilevante.

Per gli stabilimenti di soglia superiore, è parte integrante del cosiddetto "Rapporto di sicurezza", mentre per quanto riguarda gli stabilimenti di soglia inferiore questo va a coprire

anche le predisposizioni richieste dal "Piano di emergenza interna". Il documento relativo alla politica di pericolo incidente rilevante deve essere redatto e depositato all'interno dello stabilimento centottanta giorni prima dell'inizio delle attività o in caso di modifiche dell'inventario delle sostanze pericolose con possibile aggravio (per gli stabilimenti di nuova realizzazione) e deve essere riesaminato e se necessario aggiornato, con cadenza biennale. Negli allegati della direttiva (Allegato III) se ne forniscono le linee guida e le indicazioni generali al fine della sua articolazione, in particolare ci si riferisce allo stato dell'arte in materia nazionale, comunitario o internazionale. Si evidenzia la norma nazionale UNI 10617: Stabilimenti con pericolo di incidente rilevante – Sistemi di gestione della sicurezza, che ne definisce i requisiti per la sua implementazione e gestione.

I sistemi di gestione sono degli efficienti strumenti manageriali, che per le loro caratteristiche di sistematicità, rigore e flessibilità di applicazione, trovano sempre più consensi nelle realtà aziendali, di qualunque settore. Consentono di raggiungere determinati obbiettivi con l'attuazione di procedure operative, applicate all'intera organizzazione o limitati per certi aspetti o funzioni.

La struttura del sistema gestionale è l'elemento che lo rende così efficace e pone fondamento nel ciclo PDCA, una variante della teoria attribuita a W.E. Deming[14]. Adottando un approccio scientifico, Deming afferma che qualsiasi azione/decisione innovativa non può essere intrapresa in assenza di predizioni e teorie. L'osservazione e lo studio di dati ci consentono di realizzare un confronto con quanto inizialmente previsto a sostegno o meno delle teorie su cui ci si basa e solo attraverso questo processo è possibile realizzare un apprendimento costruttivo.

Sulla base di questi principi, il ciclo PDCA è organizzato in quattro stadi che vengono ripetuti ciclicamente, in virtù di un miglioramento continuo.

[14] W.E.Deming (1990-1993), statista e consulente di gestione aziendale. In Giappone è riconosciuto ed onorato per aver risollevato l'economia dopo la Seconda Guerra Mondiale, attraverso sistemi di gestione qualità. Gli sono attribuiti il ciclo di Deming o PDSA e la teoria TPK (Theory of Profound Knowledge).

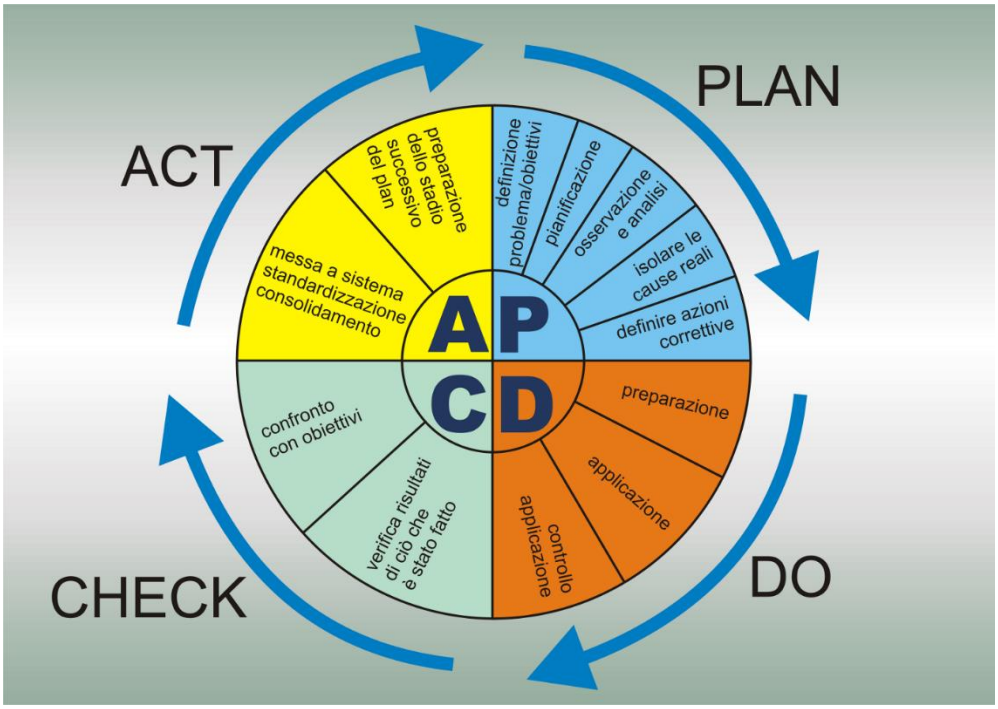

Figura n.2.5 Schema PDCA

2.3.2 La normativa *UNI 10617*: ciclo PDCA

In riferimento alla normativa *UNI 10617: Stabilimenti con pericolo di incidente rilevante – Sistemi di gestione di sicurezza* di seguito si chiariscono le diverse fasi che compongono il ciclo PDCA:

- Plan: stabilire degli obiettivi o miglioramenti, definire una politica per raggiungerli, formulare previsioni sui risultati attesi.
  Dato che gli obiettivi generali che il SGS persegue riguardano la conduzione in sicurezza dello stabilimento con pericolo di incidente rilevante, la fase di pianificazione è incentrata su un'analisi di valutazione dei rischi che consenta di individuare e attuare opportune misure di sicurezza, tenendo conto di eventuali obblighi di conformità[15] cui l'organizzazione è vincolata o aderisce. In ogni caso si richiede che la valutazione venga eseguita, documentata e aggiornata per tutte le attività, prodotti e servizi cui il SGS è applicato così come per tutte le circostanze normali o anormali di emergenza ragionevolmente prevedibili durante qualsiasi fase

[15] Legislazione nazionale, locale o internazionale, compresi statuti e regolamenti, decreti, direttive, ordinanze, permessi, licenze o altre forme di autorizzazione, trattati, convenzioni, protocolli, accordi collettivi di contrattazione, sentenze di corti o tribunali.

di vita degli impianti (dalla progettazione, costruzione, esercizio, manutenzione, dismissione e smantellamento), considerando scenari dovuti a cause interne allo stabilimento (operative, monitoraggio, invecchiamento) o fattori esterni (eventi NaTech[16], effetto domino[17] di altri impianti, attività svolta da personale o visitatori esterni e atti deliberati di matrice terroristica).

- Do: mettere in pratica quanto definito nello stadio di pianificazione.
  Per l'applicazione di quanto pianificato è necessario che vengano implementate procedure per tutte le attività svolte all'interno dello stabilimento ai fini della sicurezza e che vengano attuati controlli nei processi. Questi ultimi possono essere di carattere tecnico-ingegneristico gestiti con programmi di manutenzione ed ispezioni preventive/predittive o la misurazione dei processi. Si richiede, inoltre, che sia stato predisposto un piano di emergenza interno che gestisca le attività di risposta ad un possibile evento di incidente rilevante e la raccolta e trasmissione dei dati alle autorità competenti, così come un programma di gestione delle modifiche del SGS.

- Check: verificare la corrispondenza con quanto inizialmente previsto e studiare i risultati delle politiche attuate.
  Il gestore dello stabilimento organizza e documenta un'attività di monitoraggio, analisi e valutazione sulla politica di sicurezza implementata, attraverso un programma di audit interni pianificati. Si deve tenere conto di incidenti, quasi-incidenti, o anomalie, ispezioni sui componenti e sistemi di sicurezza, verifica sulla qualificazione professionale degli addetti, una valutazione dell'efficacia, dell'organizzazione del SGS e del corretto adempimento agli obblighi di conformità. È necessario che i risultati ottenuti siano affidabili, riproducibili e tracciabili. Segue poi il riesame di direzione con cadenza almeno annuale.

- Act: dagli studi e analisi dello stadio precedente, adottare soluzioni di miglioramento. Possono essere di carattere gestionale o tecnico-impiantistico.

[16] Natural Technological: si intendono quegli incidenti tecnologici, come incendi, esplosioni, rilasci di sostanze tossiche indotti da fenomeni naturali come terremoti, alluvioni, frane, fulminazioni, vento forte.
[17] Rischi e conseguenze subite da un incidente rilevante di uno stabilimento nelle vicinanze.

Capitolo 3: valutazione del rischio

3.1 Introduzione

Con valutazione del rischio (*risk assessment)* si intende quel processo volto ad assegnare una dimensione al concetto di rischio, in termini di frequenza e magnitudo, è uno strumento di supporto per avere maggiore chiarezza e intraprendere decisioni/azioni in merito ad essi. È una procedura che si articola in diverse fasi, di seguito se ne riporta lo schema e successivamente si approfondiranno i diversi stadi.

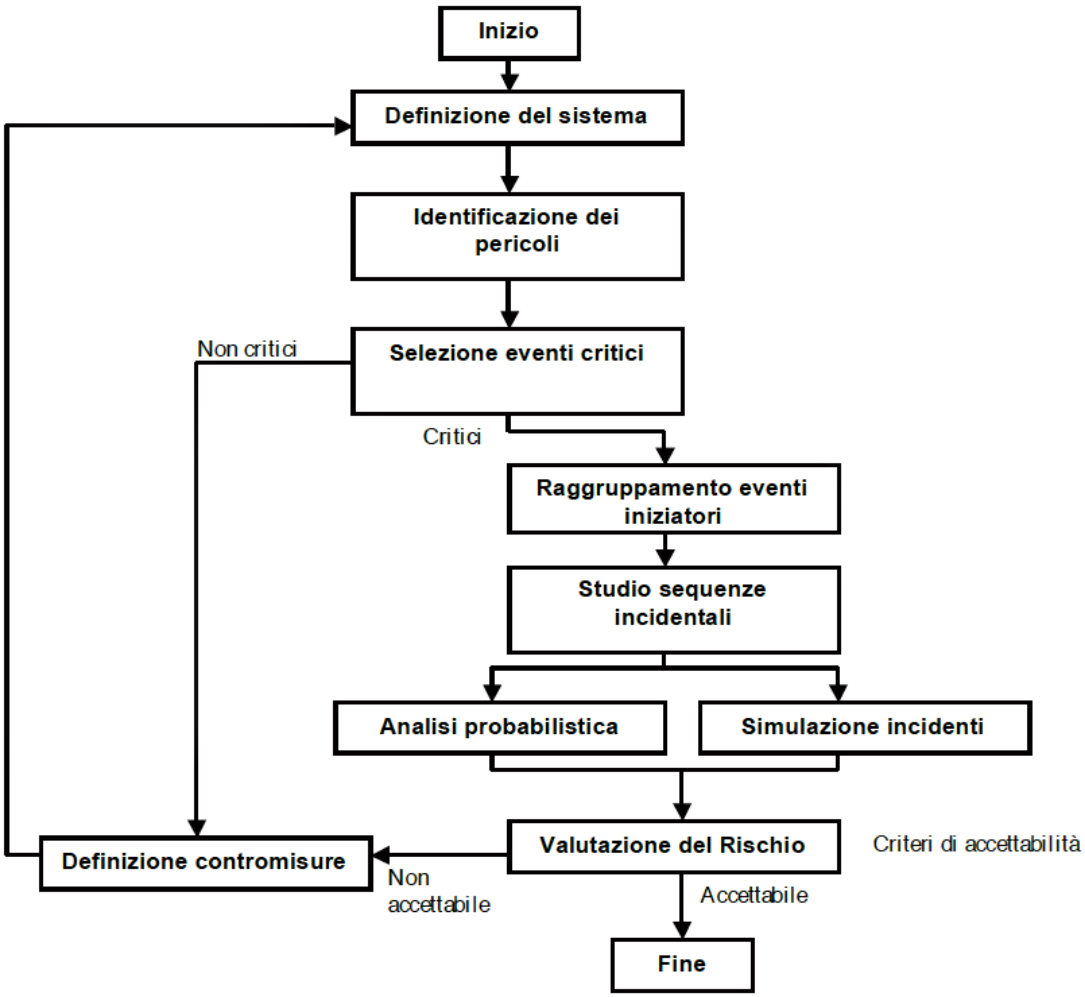

Figura n.3.1 Struttura della valutazione dei rischi (*risk assessment*)

3.2 Definizione del sistema

Questa fase viene a collocarsi in modo preliminare alla valutazione del rischio vera e propria e ha lo scopo di raccogliere tutte le informazioni necessarie al fine di organizzare la valutazione in modo efficiente e affinché venga intrepretata nel modo migliore: è da questa che dipenderanno le future decisioni.
Viene definito il sistema che sarà oggetto di studio e il contesto cui fa parte (es. nel caso di un impianto tecnologico si evidenziano gli aspetti impiantistici/di processo, informazioni sulle sostanze pericolose presenti, il layout, come si inserisce all'interno del territorio, dati ambientali-metereologici che possono influire sullo stabile) in modo da definire la complessità, il grado di approfondimento e la natura dei dati in uscita all'analisi dei rischi (*risk analysis*), così come individuare eventuali vincoli legislativi, fissare tempistiche e costi.
Importante è il confronto con gli interessi degli *stakeholder*[18] non necessariamente fisicamente presenti al momento della valutazione, ma le loro opinioni possono essere ricavate da sondaggi o interviste effettuate in precedenza, dalle quali si possono stabilire i criteri di accettabilità del rischio.

3.3 Criteri di accettabilità del rischio: principio ALARP

I criteri di accettabilità del rischio stanno alla base delle decisioni che vengono intraprese a seguito dell'analisi dei rischi, in particolare rappresentano un riferimento e vengono considerati durante lo studio di *risk evaluation*, per determinare se un rischio è accettabile o meno e in quale misura questo deve essere trattato.
La scelta del criterio dipende dall'organizzazione, il contesto e gli interessi degli *stakeholder*. Tra le applicazioni che riguardano la sicurezza particolarmente seguito è il metodo "*as low as is reasonably practicable*" (ALARP).
Seguendo questa metodologia i rischi vengono suddivisi in tre categorie:

- Accettabili: i rischi che ricadono in questa regione possono essere trascurati e non occorrono azioni da intraprendere, non destano alcuna preoccupazione.

[18] tutte le persone ed associazioni che sono coinvolte direttamente o indirettamente dalle azioni che verranno intraprese, lo sono per esempio project manager, autorità legislative locali e non, progettisti, rappresentanti sindacali rappresentanti dei lavoratori, compagnie di assicurazione.

- Tollerabili (Regione ALARP): non possono essere ignorati, vengono ridotti il più possibile fino a quando i costi delle misure per ridurli non sono sproporzionati ai benefici ottenuti, in termini di salute, sicurezza, vite umane e danni ambientali. Questa valutazione può essere effettuata sulla base del giudizio di esperti, buona pratica ed esperienza, ma in alcune circostanze si rendono necessari ulteriori approfondimenti con un'analisi di costi/benefici.

- Inaccettabili: i rischi non sono giustificati (tranne casi eccezionali) e devono essere resi accettabili o per lo meno tollerabili, qualunque sia il costo delle misure da intraprendere.

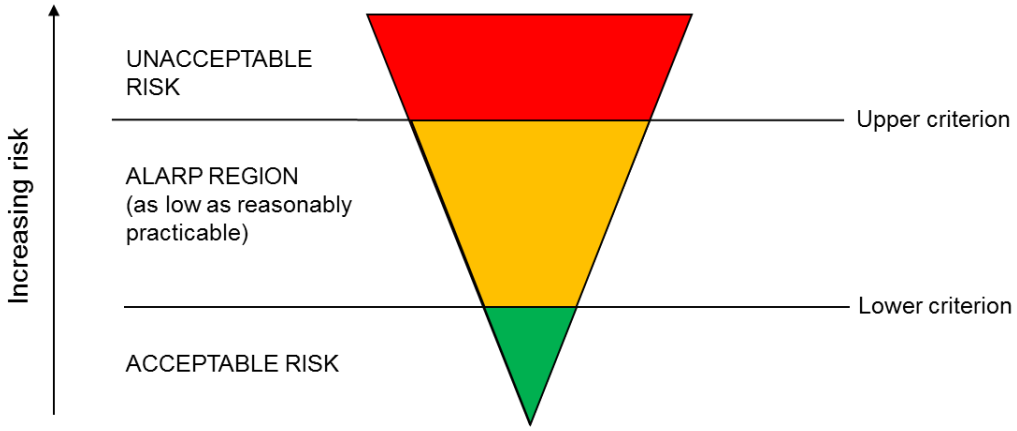

Figura n.3.2 Regioni di rischio principio ALARP

La Regione ALARP viene delimitata da livelli di tollerabilità del rischio, superiori (limite di non accettabilità) ed inferiori (limite di accettabilità). Questa zona può essere individuata nella fase preliminare in modo qualitativo rispettando le finalità e l'esperienza degli *stakeholder*, ma talvolta possono essere considerati dei valori di riferimento stabiliti dalla legislazione o dalla pratica vigente in ciascun Paese.

I parametri numerici di riferimento normalmente vengono espressi in termini di rischio individuale o rischio sociale. Il primo è da intendersi come il rischio cui un individuo è esposto quando viene a trovarsi in una certa posizione rispetto ad un certo pericolo, viene valutato come probabilità di morte annua per persona mappabile attraverso curve iso-rischio, il secondo invece, come il rischio subito da una popolazione rispetto ad un pericolo, rappresentato in curve F-N, che relazionano frequenza di eventi incidentali annui per numero di morti.

Di seguito si riportano i limiti ALARP associati al rischio sociale rappresentati in curve F-N bi-logaritmiche adottate/proposte da diversi Paesi[19].

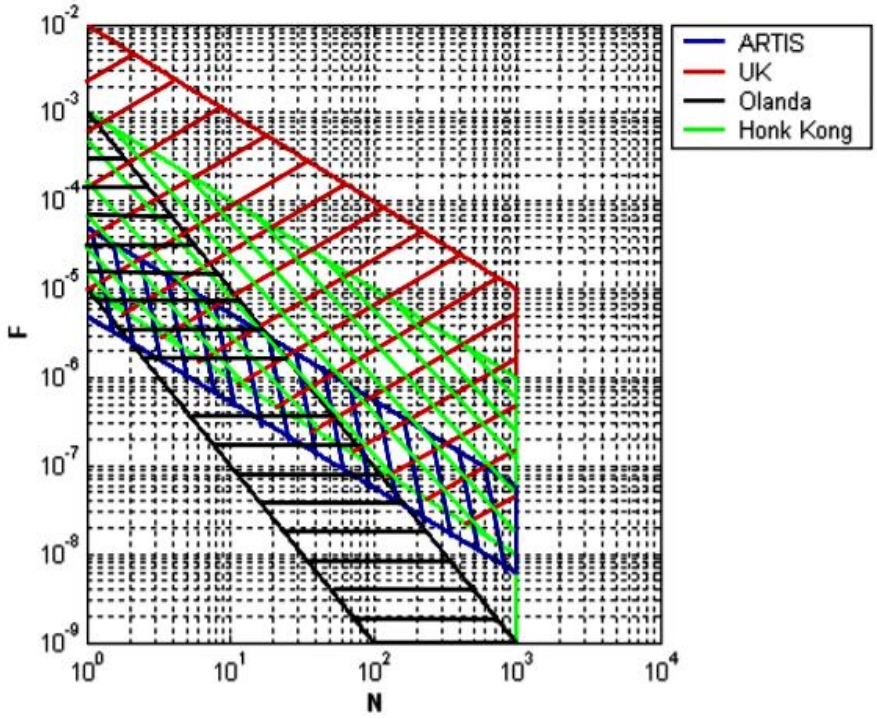

Figura n.3.3 Limiti superiori e inferiori ALARP per vari Paesi

3.4 Valutazione del rischio (*risk assessment*)

3.4.1 Identificazione dei pericoli (*risk identification*)

In questa prima fase vengono identificati tutti i potenziali pericoli, fonti di possibile danno, presenti o che possono insorgere nel sistema oggetto di studio. Se ne fornisce una descrizione completa di come, in quale parte del sistema può verificarsi, le cause, le possibili combinazioni con altri pericoli, soluzioni di protezione, tenendo conto di tutte le modalità e condizioni operative previste e non, ragionevolmente prevedibili. Si presenta come una procedura sistematica ed iterativa: se un pericolo viene trascurato, non verrà tenuto conto nella fase di stima. È possibile fare affidamento anche su analisi storiche in banche dati, dalle quali si reperiscono maggiori informazioni da incidenti passati, sulle cause che possono scatenare un certo evento pericoloso, in quale modalità, elementi che lo possono aggravare

[19] L'Italia non ha adottato dei valori di riferimento a livello nazionale, ma si evidenzia il progetto ARTIS promosso nel 1990 dalla Regione Friuli Venezia Giulia, volto a quantificare i limiti ALARP, in uno studio sui rischi per la popolazione derivanti da incendi, esplosioni e fumi tossici causati da attività industriali nell'area industriale e portuale della città di Trieste.

ed estensioni degli effetti. Per certe tipologie di pericoli, invece, è opportuno fare affidamento a studi specialistici (es. studi Natech). Relativamente agli impianti Seveso esiste la banca dati online e-MARS (*Major Accident Reporting System*) che registra le segnalazioni di incidenti rilevanti, ai sensi dell'art.18 e Allegato VI della direttiva 2012/18/UE. Di seguito si riportano alcune metodologie che meglio si adattano all'identificazione di pericoli suddivisi per categorie, sempre in riferimento ad impianti a rischio incidente rilevante. Nel capitolo 4 verrà trattato il metodo HAZOP legato a pericoli dovuti a deviazioni dal normale funzionamento del processo.

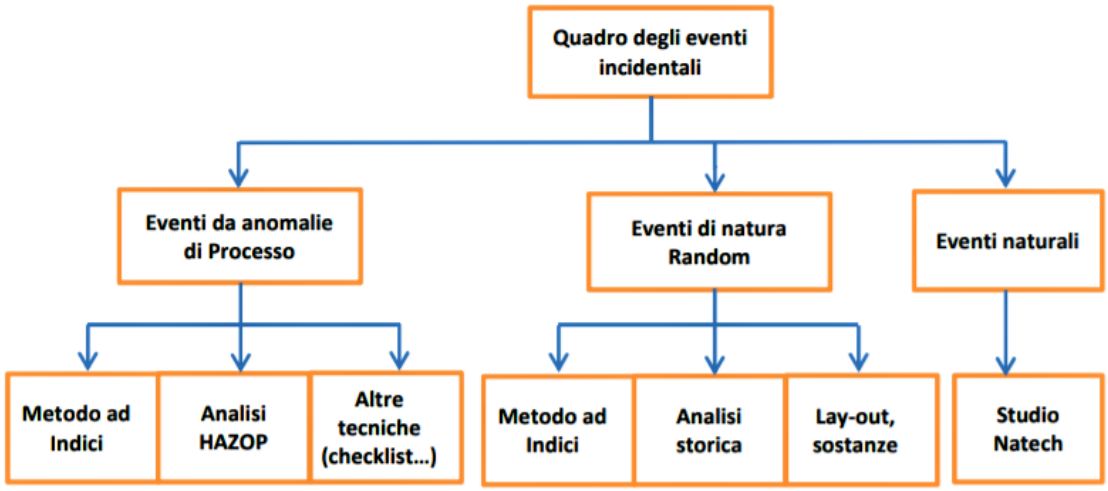

Figura n.3.4 Metodologie di identificazione pericoli in impianti Seveso

Al termine di questo studio si ottiene una lista di tutti gli eventi iniziatori[20] che possono portare ad un pericolo con la loro relativa descrizione (in termini di cause, conseguenze, ed eventuali contromisure). I risultati considerati più rilevanti, quindi i pericoli più critici vengono selezionati per ulteriori approfondimenti.

3.4.2 Analisi del rischio (*risk analysis*)

A seconda delle scelte effettuate in fase di pianificazione l'analisi di frequenze e magnitudo può essere di carattere differente, in base alla natura dei dati che vengono forniti in uscita. È possibile distinguere tre tipologie differenti:

[20] Si faccia riferimento agli *initiating events* di figura n.1.6. Più eventi iniziatori possono portare al medesimo pericolo.

- Analisi qualitativa: frequenze e magnitudo dei rischi vengono espressi con scale di valori, ciascuna delle quali viene definita in forma descrittiva. Questa tipologia di analisi si basa fortemente sull'esperienza, il giudizio e dibattito tra esperti. Mancano di rigore matematico, ma hanno il vantaggio di essere chiare, di facile comprensione ed esecuzione. Sono particolarmente utili per eseguire un'analisi generica accompagnata poi da analisi più dettagliate o quando il contesto di studio non richiede eccesivi sforzi o impiego di tempi/costi. Talvolta la soggettività insita può influire con un'esagerazione di valutazione dei risultati che si traduce in un sovradimensionamento delle misure di sicurezza.

- Analisi quantitativa: frequenza e magnitudo sono di carattere numerico, ricavati da cataloghi tecnici e banche dati, in forma di grafici o distribuzione di frequenze, espressi secondo una appropriata unità di misura, a valle di analisi probabilistiche o implementazione di modelli fisico-matematici. Il loro punto di forza risiede nel rigore e nell'accuratezza che sono in grado di dimostrare. Per contro, la bontà dei risultati dipende fortemente, in senso statistico, dalla qualità dei dati considerati. Richiedono un grande impegno in termine di costi e tempo per raccogliere informazioni e per la loro elaborazione, spesse volte attraverso l'utilizzo di software al calcolatore, ma si rendono necessari in contesti di discreta complessità. Occorre prestare particolare attenzione durante l'interpretazione dei risultati, non sempre di immediata comprensione, occorrono conoscenze matematiche.

- Analisi semi-quantitativa: si presenta come un'analisi qualitativa più dettagliata. Si può fare affidamento quando il contesto è troppo complesso per un'analisi totalmente qualitativa (non sono chiari eventi iniziatori, sequenze), ma un'analisi quantitativa sarebbe eccessiva. Tipicamente la frequenza viene espressa in scala numerica, mentre alla magnitudo viene assegnato un valore appartenente ad una certa scala di valori, cui significato viene definito qualitativamente.

Occorre precisare che la scelta del tipo di analisi deve essere compatibile con i criteri di accettabilità adottati. Le grandezze in uscita dalla *risk analysis* devono essere rappresentate in un formato tale affinché possano essere comparate adeguatamente.

In questo stadio a partire da ogni evento iniziatore è possibile delineare una o più sequenze incidentali. A partire da ciascuno di essi viene individuato uno o più percorsi/scenari di eventi che terminano in un evento finale al quale è associata una certa probabilità di danno (un rischio) valutati in relazione alle protezioni adottate secondo le regole di buona tecnica, cui il sistema è dotato. Per ciascuno scenario (delimitato da un evento iniziatore ed un evento finale) viene associata una certa frequenza di accadimento. Successivamente per ciascuno di essi viene eseguito uno studio delle conseguenze che questi comportano, associandoli ad un certo valore di danno o magnitudo.

In relazione agli impianti a rischio incidente rilevante per quanto riguarda lo studio degli effetti delle conseguenze degli scenari incidentali, tipicamente si fa affidamento su software e programmi di calcolo specialistici che realizzano simulazioni sulla base di modelli matematici. Gli scenari tipici coinvolgono rilascio di materia ed energia, che possono essere classificati in tre categorie: incendi, esplosioni e rilascio di sostanze tossiche. Le simulazioni consentono per esempio di valutare l'estensione e l'intensità dei fenomeni, sovrappressione di esplosioni, modalità, direzione e portata delle sostanze rilasciate. La legislazione italiana in accordo al D.M. 09/05/2001: "Requisiti minimi di sicurezza in materia di pianificazione urbanistica e territoriale per le zone interessate da stabilimenti a rischio di incidente rilevante", fornisce dei livelli di soglia di riferimento con i quali valutare le conseguenze.

Scenario incidentale	Elevata letalità	Inizio letalità	Lesioni irreversibili	Lesioni reversibili	Danni alle strutture / Effetti domino
	1	2	3	4	5
Incendio (radiazione termica stazionaria)	12,5 kW/m^2	7 kW/m^2	5 kW/m^2	3 kW/m^2	12,5 kW/m^2
BLEVE/Fireball (radiazione termica variabile)	Raggio fireball	350 kJ/m^2	200 kJ/m^2	125 kJ/m^2	200-800 m (*)
Flash-fire (radiazione termica istantanea)	LFL	½ LFL			
VCE (sovrapressione di picco)	0,3 bar (0,6 spazi aperti)	0,14 bar	0,07 bar	0,03 bar	0,3 bar
Rilascio tossico (dose assorbita)	LC50 (30min,hmn)		IDLH		

Tabella n.3.1 Valori di soglia D.M. 09/05/2001

3.4.3 Valutazione del rischio (risk evaluation)

La *risk evaluation* è lo stadio finale del processo di valutazione del rischio (*risk assessment*). Per ogni sequenza incidentale individuata è possibile fornire la stima dei rischi, intesi come la combinazione della frequenza di accadimento e la sua magnitudo. Vengono poi confrontati con i criteri di accettabilità per valutare la necessità o meno di azioni e misure per renderli accettabili.

3.5 Fasi di sviluppo di un progetto

I paragrafi precedenti descrivono una valutazione del rischio intendendo una generica applicazione. Di fatto la progettazione di un sistema tecnico-ingegneristico si può suddividere in 6 stadi. Nelle fasi iniziali (1-2-3) si rende necessaria una valutazione del rischio, con caratteristiche adattate agli scopi. Le fasi finali (4-5-6) consistono in una attività di validazione, collaudo e verifica a quanto definito negli stadi precedenti.
In riferimento ad un impianto di processo, di seguito se ne riporta la descrizione:

1. Fase concettuale: vengono raccolte informazioni riguardanti il progetto proposto al fine di individuare e risolvere le principali eventuali criticità o fattibilità di realizzazione in termini di sicurezza. In questa prima fase non sono ancora stati definiti aspetti tecnici.
2. Definizione del progetto: vengono eseguiti studi sul processo da implementare mediante *flowsheet* che rappresentano graficamente le operazioni e le diverse interconnessioni tra le macchine che realizzano un impianto tecnologico. Sulla base di questi viene elaborato il progetto ingegneristico, in relazione alla pratica tecnica e da eventuali obblighi legislativi. Si adottano misure di sicurezza nei confronti dei rischi individuati.
3. Esame dettagliato del progetto: si esegue una sistematica revisione del progetto prima della conferma definitiva. Vengono individuate ulteriori modifiche nei sistemi di sicurezza o a livello di operabilità, affinché il sistema possa ritenersi sicuro ed affidabile.
4. Validazione del design: si colloca al termine della costruzione del progetto e consiste nel verificare la corretta implementazione del sistema, in linea con quanto previsto

e stabilito negli stadi precedenti, così come una revisione sulle procedure operative e di emergenza.

5. Validazione operativa (pre-startup review): si verificano le funzioni del sistema e si collaudano i SIS implementati in accordo alla normativa vigente. Avviene il completamento della formazione degli operatori.
6. Post-startup review: il sistema viene studiato qualche mese dopo l'inizio della produzione. Si verificano eventuali deviazioni operative dall'intento iniziale e si raccolgono informazioni per utilizzi futuri.

3.6 Tecniche di valutazione del rischio

Ufficialmente sono riconosciute 41 tecniche per poter condurre un'analisi di valutazione del rischio[21]. Queste vengono classificate in base all'applicazione che si presta meglio all'interno del processo di valutazione, difatti alcune di esse possono essere utilizzate all'interno di più fasi, ma con gradi di applicabilità differenti. La scelta di quale o quali tecniche utilizzare ricade negli specialisti che conducono lo studio, considerando le scelte effettuate in fase di pianificazione. Fattori da considerare sono: complessità di attuazione (*low, medium, high*), tempo di esecuzione (*short, medium, long, any*) esperienza richiesta da parte degli specialisti (*low*=intuitiva*, moderate*=corso di studio*, high*=esperienza di applicazione), tipologia (*quantitative, qualitative, semi-quantitative, either*), livello di informazioni richieste inizialmente (*high, medium, low*) e stadio di studio (par. 3.5).

3.6.1 Matrice di rischio

La matrice di rischio è una tecnica utilizzata per rappresentare e categorizzare rischi attraverso una combinazione di conseguenze e probabilità e a seconda dei dati considerati può essere qualitativa, quantitativa o semi-quantitativa.
Comunemente viene impiegata nella fase di risk evaluation nel confronto con i criteri di accettabilità, oppure anche a valle della risk identification nella selezione di eventi critici.
La matrice di rischio si presenta come una griglia, dove negli assi delle ascisse ed ordinate vengono associate frequenze e magnitudo suddivisi in una scala di valori discreti, definiti in

[21] In accordo alla normativa di riferimento *IEC 31010: Tecniche di valutazione del rischio*.

modo qualitativo o quantitativo. Ad ogni cella, pertanto corrisponde un certo livello di rischio.

È particolarmente semplice da implementare, di chiara comprensione e applicabile in contesti molto differenti tra loro, per questo è una tecnica piuttosto praticata. Le principali limitazioni riguardano la definizione delle scale utilizzate, dalle quali dipende la bontà della matrice del rischio stessa. Possono assegnare a rischi quantitativamente differenti il medesimo valore nella griglia della matrice e di conseguenza questo influisce sulla scelta delle misure da intraprendere, risulta difficile comparare rischi con tipologie di conseguenze molto differenti tra loro.

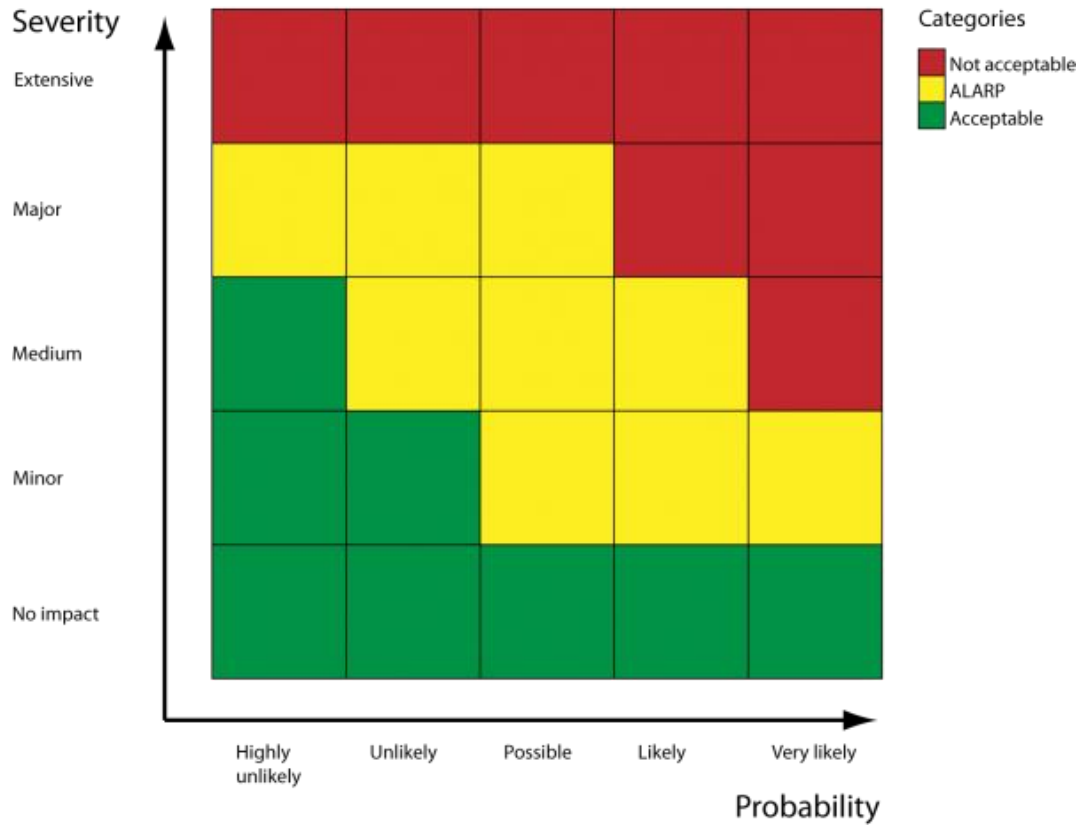

Figura n.3.5 Esempio di matrice di rischio 5x5 qualitativa con zona ALARP

3.6.2 *Layer of protection analysis* (LOPA)

LOPA è una tecnica semi-quantitativa che viene riconosciuta principalmente per individuare e valutare se i sistemi di protezione adottati secondo le norme di buona tecnica sono adeguati al fine della tollerabilità dei rischi individuati, stabilendo se sono necessarie modifiche di progetto o l'implementazione di funzioni di sicurezza calcolandone il relativo livello SIL richiesto.

Dal punto di vista pratico questa tecnica è in grado di coprire entrambe le fasi della valutazione del rischio (identificazione di pericoli e analisi dei rischi), ma molto più comunemente viene utilizzata a seguito di una analisi HAZOP, una combinazione vantaggiosa in quanto questa fornisce tutte le informazioni necessarie allo sviluppo della LOPA e per il fatto che il team di studio è più famigliare con il sistema in esame.
Di seguito si illustrano brevemente le principali fasi in cui si articola la tecnica:

1. Per ogni evento iniziatore individuato dallo studio HAZOP viene delineata la sequenza degli eventi incidentali, individuando i sistemi di protezioni che possono essere coinvolti. Verranno considerati solo i sistemi IPL. Per ogni evento viene realizzato in forma grafica un albero di sequenze di eventi che possono verificarsi nel caso le protezioni installate abbiano successo o meno (in figura n.3.6 "true" o "false"). Questa procedura porta a delineare una lista di eventi finali cui è associato un danno probabile. Per ciascun IPL viene assegnato un certo valore PFD e per ogni evento finale si assegna un certo valore di magnitudo che viene definito qualitativamente.

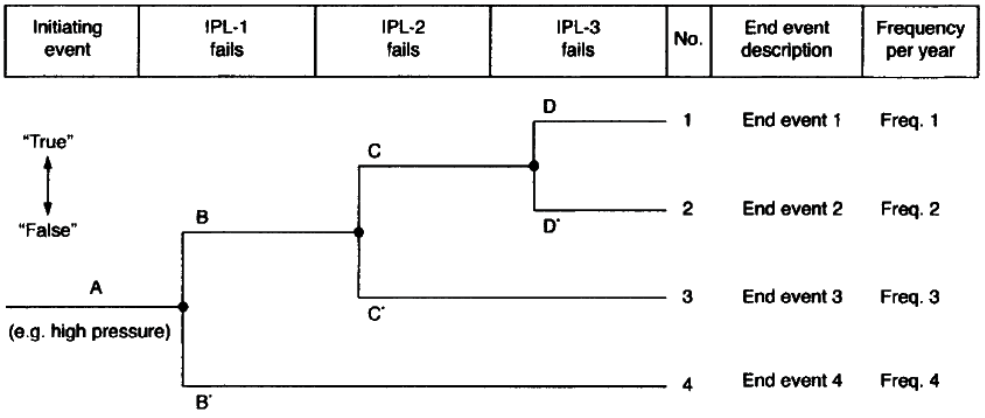

Figura n.3.6 Albero delle sequenze incidentali

2. Si stima una frequenza di accadimento per ciascun evento iniziatore in termini di eventi/annui. È possibile pensare di applicare modifiche al progetto per eliminare questi pericoli e pertanto escluderli a priori dallo studio.
3. Si stima il rischio associato ad ogni scenario incidentale. La frequenza attribuita ad ogni scenario corrisponde al prodotto della frequenza di accadimento dell'evento

iniziatore e del PFD di ciascun IPL coinvolto nella sequenza di eventi. (sono eventi indipendenti, probabilità incondizionate).

4. I rischi individuati vengono confrontati con i criteri di accettazione. Quelli che necessitano una riduzione, vengono inizialmente trattati modificando il design di progetto. Nel caso questo non fosse sufficiente, occorre implementare funzioni di sicurezza strumentate (SIF).
5. Si stima il PFD richiesto dalla SIF per ridurre il rischio, e pertanto il relativo livello SIL. Questo viene calcolato come rapporto tra il valore del rischio ritenuto tollerabile (in frequenza annua) e la frequenza del rischio associata allo scenario calcolata nello stadio 3.

Questa tecnica presenta i vantaggi delle tecniche semi-quantitative e pertanto è più rigorosa di un approccio totalmente qualitativo, e richiede meno sforzi rispetto ad una tecnica quantitativa. Risulta difficilmente applicabile in contesti molto complessi dove si verificano interazioni tra rischi o tra i sistemi di protezione.

Capitolo 4: Hazard and Operability studies (HAZOP)

4.1 Introduzione

In Inghilterra tra gli anni ’50 e ‘60 lo sviluppo di nuovi impianti chimici, più grandi e con processi più complessi da gestire e rispetto a quanto fino ad allora, si tradusse in un incremento delle morti dovuti ad incidenti industriali. Ci si rese pertanto conto della necessità di un nuovo atteggiamento nei confronti della sicurezza, denominato come “*loss prevention*”, portando al compimento i primi studi sull’identificazione dei pericoli, analisi del rischio, riesame degli incidenti e sulla realizzazione sicura del design, tutti aspetti già definiti nei capitoli precedenti che pongono le basi per gli studi sulla sicurezza attuali.

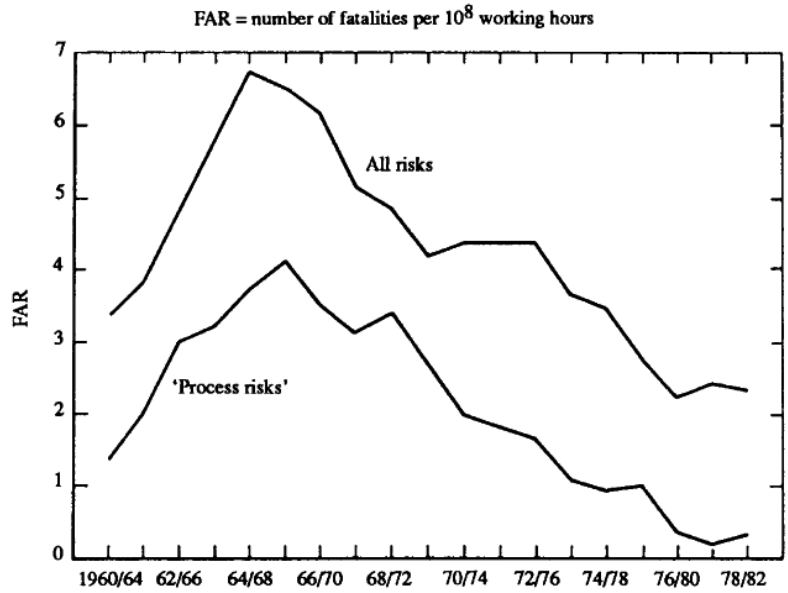

Figura n.4.1 Andamento tasso di incidenti mortali tra il periodo 1960 /1982

La tecnica HAZOP viene presentata per la prima volta in una linea guida nel 1977, con la pubblicazione degli “Hazard and operability Studies” da parte della Chemical Industries Association (CIA) e dato il successo raggiunto poi è stata formalizzata ufficialmente nella normativa *IEC 61882: Studi di pericolo ed operabilità (HAZOP)*.

HAZOP è una tecnica qualitativa di identificazione dei pericoli, è un’indagine condotta da un team di lavoro, sulle deviazioni operative dagli intenti progettuali, consente di valutare pericoli, eventi iniziatori e conseguenze. In relazione alle fasi di vita di un progetto, questo

ricade nell'esame dettagliato di progetto (stadio 3 par. 3.5) e pertanto viene condotto su uno schema proposto (non necessariamente completo e definitivo) o in un riesame di uno già esistente.
Ciò che rende questa tecnica così efficace, oltre alla sistematicità di indagine, è il fatto che non si incentra sui singoli componenti che realizzano un sistema, ma bensì sulla funzionalità di un certo elemento. Questo rende la sua applicazione indipendente dal sistema considerato e può essere utilizzata in progetti in fase molto preliminare alla loro definizione e su tecnologie di nuova generazione. In conseguenza a ciò, nonostante sia stata definita inizialmente per l'industria chimica e di processo dove vengono gestiti flussi di materiali in impianti tecnologici, soprattutto negli ultimi anni, sono state avanzate varianti di questa tecnica che la portano ad essere applicata in altri ambiti che coinvolgono ad esempio flussi di informazioni (software HAZOP), sistemi di controllo elettrici ed elettronici (CHAZOP), gestione degli errori operativi e manutentivi (human HAZOP) o procedure operative (procedure HAZOP).

4.2 Organizzazione studio Hazop

Analogamente a quanto visto al paragrafo 3.2 nella valutazione del rischio, prima dell'esecuzione dello studio vera e propria si rende necessaria una fase di pianificazione. Normalmente viene condotta da chi ha responsabilità in merito al progetto: il project manager e il rappresentante del gruppo di studio, il team leader. Vengono definiti i dettagli del sistema in esame così come obiettivi, scopi ed aspetti cui il gruppo di lavoro dovrà focalizzarsi e come dovrà essere articolata l'analisi.

4.2.1 Team HAZOP

L'analisi condotta in uno studio HAZOP dipende essenzialmente dal lavoro svolto da parte di un gruppo. È una tecnica di tipo qualitativa, quindi l'analisi si basa in uno scambio di idee e discussioni seguendo un approccio creativo-induttivo; la bontà dei risultati pertanto dipende fortemente dal giudizio, e dall'esperienza dei membri del gruppo, ma anche dalla capacità di creare un ambiente costruttivo, aperto positivamente al dibattito, aspetti che in questa tipologia di tecniche assumono un peso e responsabilità maggiore.

La formazione del team HAZOP viene definita dal project manager, concordata poi con il team leader. Quest'ultima figura deve possedere esperienza pregressa in leadership di studi HAZOP oltre che esperienza nella progettazione, mentre per gli altri membri è richiesto almeno la frequentazione di un corso di formazione e maturata esperienza nel settore di professione: la scelta di queste figure deve coprire tutti gli aspetti del progetto. Al fine di un'analisi efficace sia in termini operativi che di tempistiche si prediligono gruppi di piccole dimensioni (tipicamente 5-7 professionisti) in relazione alla complessità del sistema e che la formazione del team rimanga più stabile possibile nel tempo. Si individuano alcune figure ricorrenti:

- Team leader: è la figura che possiede responsabilità nella pianificazione e nella conduzione dello studio HAZOP, gestisce i rapporti con il project manager e con i membri del team al fine di rendere lo studio produttivo, non necessariamente deve essere un professionista interno al progetto. I compiti principali riguardano la raccolta e riorganizzazione dei dati utili allo studio come la documentazione tecnica che ne descriva quantitativamente o qualitativamente la struttura fisica e la logica di funzionamento del progetto (per un impianto di processo per esempio P&ID, layout, bilanci energetici/di materiali, data sheet, modelli 3D, data flow diagram, proprietà dei materiali, diagrammi di stato, istruzioni operative e manutenzione), documenti legislativi e ricerche in banche dati di incidenti pregressi. Si occupa di suddividere il sistema in sezioni (nodi), che andranno analizzate singolarmente. Definisce proprietà e parole guida necessarie allo svolgimento dello studio. Pianifica ed organizza le sessioni di incontro[22].

- Recorder: figura con buone conoscenze tecniche, che assiste il team leader nelle pratiche amministrative, definizione di proprietà e parole guida, documenta le conclusioni e risultati di ogni sessione di incontro nei worksheets. A volte questo ruolo viene ricoperto dal team leader stesso.

- Progettisti: figure che chiariscono il funzionamento degli schemi tecnici di riferimento (es. ingegnere di processo/controllo/meccanico/chimico), propongono

[22] Tipicamente ogni sessione ha una durata massima di 3h, intervallata da una pausa, per mantenere alta la concentrazione del team. In genere uno studio HAZOP si completa in 5-10 sessioni, ma per i sistemi più complessi possono essere richiesti anche mesi.

come il sistema potrebbe rispondere al verificarsi di una certa deviazione. È preferibile che abbiano conoscenza del progetto, ma non strettamente necessario.

- Specialisti: figure che possono partecipare, anche per un periodo limitato, offrendo la loro esperienza in un particolare settore. (es. ricercatori)

- User: figura che spiega il contesto cui il sistema verrà ad operare, consente di valutare gli effetti e conseguenze operative che una deviazione può comportare.

- Manutentori/operatore esperto: figure richieste soprattutto nel il riesame di strutture già esistenti.

4.2.2 Nodi

I nodi sono le parti in cui sistema viene suddiviso dal team leader, affinché ciascuna di esse possa essere esaminata sistematicamente. I nodi possono essere di natura fisica (es. parti di un impianto, macchinario, circuito di controllo), ma anche logica (es. parte di una procedura). La scelta accurata dei nodi è importante, perché da questa dipenderà lo sviluppo dello studio. Nodi troppo piccoli rendono lo studio lungo e ripetitivo, nodi grandi facilitano l'analisi, ma c'è il rischio di perdere qualche deviazione. In ogni caso ad ogni nodo deve essere associata una funzione ben definita, che siano chiare le intenzioni di progetto (es. parametri e range di operatività) e che ogni elemento sia identificato univocamente, nel caso dell'industria di processo questi vengono evidenziati in schemi P&ID, accompagnati da una descrizione qualitativa del funzionamento richiesto.
Non esiste un criterio generale di selezione data la variabilità dei sistemi in analisi, pertanto questo dipende essenzialmente dall'esperienza del team leader. È possibile però prendere come riferimento i *change paths*.
I *change paths* sono delle sezioni dove è possibile individuare un cambiamento/trasformazione tra uno stato iniziale ed uno stato finale. In particolare possono essere individuati per:

- Materiale (es. sostanze, energia, dati, software) in input da una sorgente;
- Attività di elaborazione o trasformazione sul materiale (es. reazione chimica, trasferimento, esecuzione di una procedura);

- Materiale in output in una destinazione.

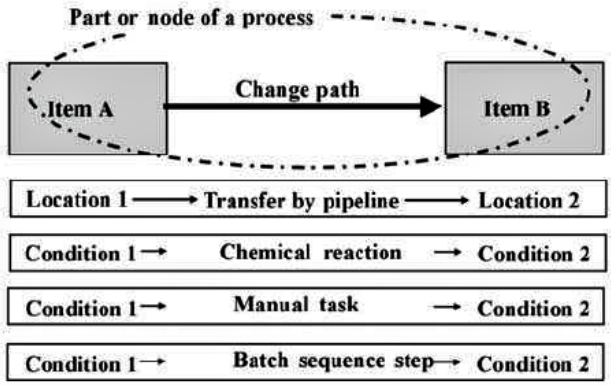

Figura n.4.2 Schema/esempi di change paths

4.2.3 Proprietà

Le proprietà sono degli elementi associati ad un determinato nodo che descrivono le sue caratteristiche essenziali, esprimono in modo sintetico gli aspetti progettuali che possono influenzare una certa attività e rappresentare fonti di possibili deviazioni dagli intenti operativi e di sicurezza. Possono riguardare il materiale coinvolto (input/output), la funzione operativa eseguita nel nodo o le attrezzature impiegate (es. punto di partenza/destinazione, elementi di controllo). A sua volta ogni proprietà può essere descritta mediante caratteristiche o parametri.

Al fine di maggior chiarezza si consideri il semplice esempio di figura sottostante. Rappresenta un nodo individuato all'interno di un impianto tecnico di processo, dove il materiale contenuto nel serbatoio A, una sostanza acida, deve essere trasferito in modo continuo nel reattore B. Si noti come la scelta del nodo segua la definizione dei *change paths*. Le proprietà associate al nodo possono essere individuate: nel serbatoio in A, nel reattore in B e il trasferimento di materiale, gestito da una pompa e da una valvola di controllo. Queste possono essere descritte ulteriormente attribuendo delle particolari caratteristiche (es. flusso, pressione, temperatura), come quelle riportate nell'esempio.

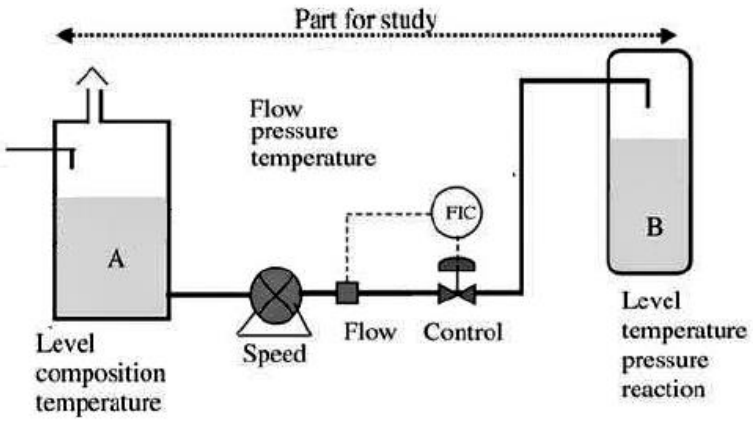

Figura n.4.3 Proprietà e caratteristiche

4.2.4 Parole guida e deviazioni

Le parole guida sono lo strumento per condurre lo studio, consentono di individuare possibili deviazioni. Si presentano come una lista di parole a ciascuna delle quali è associata una particolare condizione. Il team leader prima dell'analisi fornisce la lista delle parole guida necessarie allo studio del sistema. Possono essere scelte sulla base di una lista predefinita per un particolare settore o possono esserne create di nuove, importante che queste non siano troppo specifiche limitando il pensiero creativo, ma neanche troppo generiche rendendo lo studio poco efficiente. Di seguito si fornisce una lista non esaustiva delle parole guida utilizzate comunemente nell'industria di processo.

Tipo	Parola guida	Significato
Negazione	NO/NONE/NOT	Intento progettuale non raggiunto, completa negazione, ma nient'altro accade
Quantitativa	MORE	Incremento quantitativo
Quantitativo	LESS	Decremento quantitativo
Qualitativo	PART OF	Intento progettuale parzialmente raggiunto
Qualitativo	AS WELL AS	Modifica qualitativa
Sostituzione	REVERSE	Logica opposta all'intento di progetto
Sostituzione	OTHER THAN	Completa sostituzione, l'intento progettuale viene sostituito con qualcosa o attività differente (es. startup, shutdown, operazione alternativa, manutenzione)
Temporale	EARLY/LATE	Temporizzazione diversa da progetto
Temporale	BEFORE/AFTER	Sequenza diversa da progetto
Locazione	WHERE ELSE	Locazione aggiuntiva o differente

Tabella n.4.1 Parole guida

Ciascuna di queste verrà poi applicata per ogni proprietà (o caratteristica) per ciascun nodo individuato. La combinazione di parole guida e proprietà origina una deviazione, ossia possibili variazioni dal progetto iniziale (es. NO + Flow in pipe = assenza di flusso nella tubazione; MORE + temperature in pipe = innalzamento della temperatura nella tubazione oltre ai requisiti di progetto). Non tutte le parole guida si adattano alle proprietà del sistema individuate, spetta al team valutare quelle applicabili (es. NO + temperatura = assenza di temperatura, è priva di significato). Tipicamente queste vengono riportate in forma matriciale, in relazione all'esempio di figura n.4.5:

Element (parameter)	Guidewords								
	NO	MORE	LESS	REVERSE	PART OF	AS WELL AS	WHERE ELSE	EARLY/ LATE	OTHER
Tank A level	X	X	X						
Tank A composition		X	X			X			
Flow in pipe	X	X	X	X		X			
Temperature in pipe		X	X						
Pressure in pipe	X	X	X						X
Speed of pump	X	X	X	X					
Control valve opening	X	X	X						
Tank B level	X	X	X						
Tank B composition		X	X		X	X			X
Tank B pressure	X	X	X	X					
Tank B reaction	X	X	X		X	X			

Tabella n.4.2 Matrice proprietà-caratteristiche (element) / parole guida

4.3 Metodologia operativa

L'analisi HAZOP consiste in un esame sistematico basata sulla combinazione di proprietà/caratteristiche e parole guida per ogni nodo del sistema, individuando tutte le possibili deviazioni dalle condizioni operative previste, che possono influire sulla sicurezza e sull'operabilità. Durante lo studio è preferibile seguire la sequenza logica imposta dal sistema. Di seguito se ne riporta lo schema operativo[23]:

[23] Sono possibili due procedure operative: per proprietà e per parole guida. Nella prima si ricercano deviazioni a partire dalle proprietà individuate in un nodo, la seconda avviene vagliando ogni parola guida scelta applicata a ciascuna proprietà del nodo. Lo schema logico si riferisce alla procedura per proprietà.

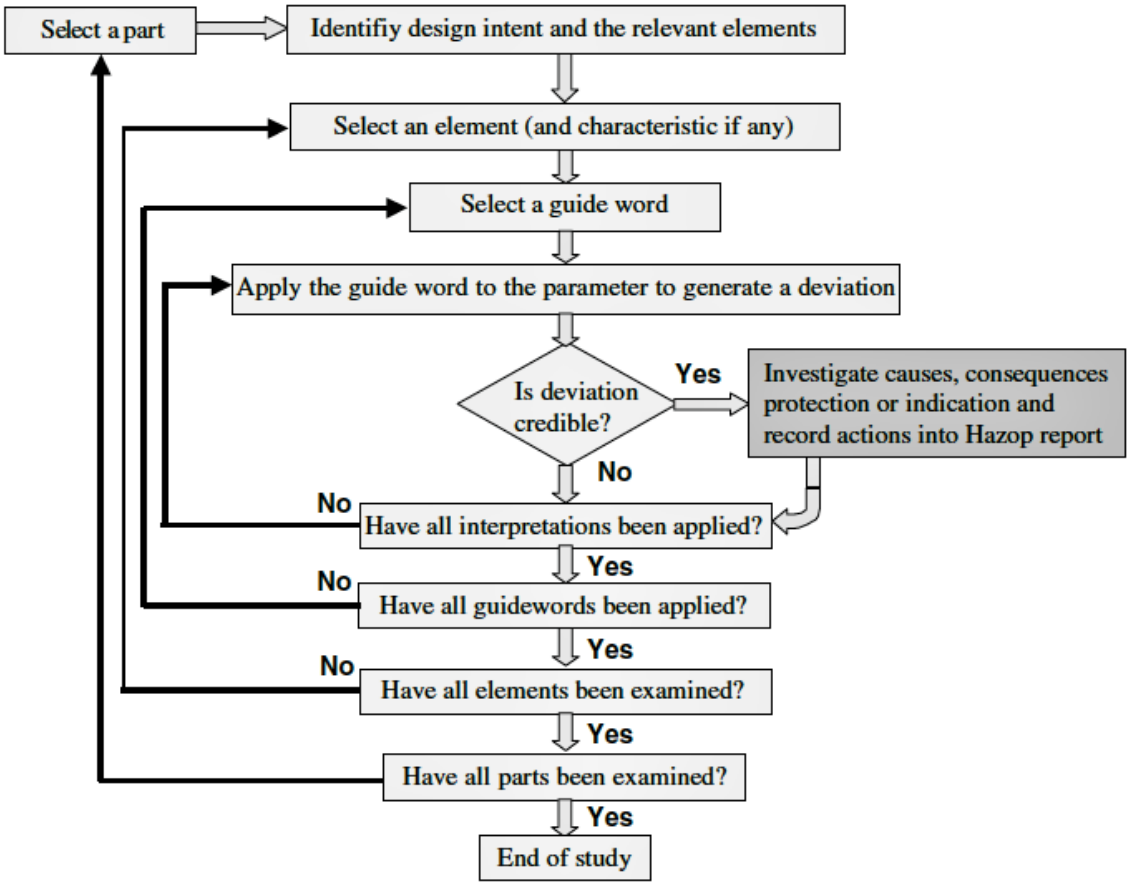

Figura n.4.4 Schema logico HAZOP per proprietà

Sulla base dell'esperienza del team, brainstorming e dei dati raccolti da banche dati, per ogni deviazione vengono analizzate in modo qualitativo le possibili cause. Tra i principali fattori nell'industria di processo sono comuni malfunzionamenti nel sistema di controllo, ostruzioni, guasti di componenti o attrezzature, errori umani da parte degli operatori sia manutentivi che operativi, o fattori esterni come interruzioni negli impianti di servizio di alimentazione elettrica o impianti di raffreddamento. Nel caso non dovessero essere individuate cause realistiche, la deviazione viene definita irrealizzabile. Successivamente si valutano, qualitativamente, le conseguenze (anche multiple) escludendo inizialmente la presenza di eventuali sistemi di protezione. È importante considerare non solo le cause immediate alla deviazione, ma anche prolungate nel tempo. Se in fase di pianificazione è stato previsto, è possibile esprimere raccomandazioni, commenti o azioni (puramente qualitative e non progettuali) da intraprendere in merito ad una certa deviazione/conseguenza. Si valuta se i sistemi di protezione (mitigativi, preventivi, allarmi, procedure amministrative) presenti siano adeguati e nel caso fornire suggerimenti. Le modifiche richieste possono riguardare l'equipaggiamento, il design, il layout del sistema,

richiedere un'aggiunta di strumentazione di salvaguardia come SIS o un cambio di procedure operative, riportandone il soggetto o la società incaricata. Se un problema, argomento di discussione, si prolunga eccessivamente è necessario riprenderlo al di fuori della sessione.

Part: Transfer of Acid from A to B	**Element: Contents of Tank A**	**Parameter: Temperature**	
Deviation	**MORE**	**Meaning/Effect**	**Material Hotter than Intended**
Is it possible	YES		
Causes	1: Temperature control fault on steam jacket controls		
How often?	Possible		
Consequences	1: Excessive vapor from the acid. Enviro. pollution	2: Acute toxic risk to persons	3: High rate of corrosion
Severity	Moderate	Serious	Minor
Safeguards	High temperature alarm	Extended vent stack	Rubber-lined tanks and vent stack
Acceptable risk	No	No	Yes
What should be done	1: Consider design change to hot water jacket instead of steam or see 2	2: Provide high temperature trip on heating	
Action	Process to review design and decide on cost of design change vs cost of trips. Instruments to estimate cost of trips		

Figura n.4.5 Esempio di analisi proprietà

I risultati dello studio vengono registrati da parte del recorder nei worksheets. I metodi di registrazione vengono stabiliti in fase di preparazione dello studio. Comunemente vengono utilizzati word-processing o spread-sheet software, ma sono consentiti anche programmi più specifici. Al termine dello studio viene realizzato il report HAZOP dove vengono riassunti: scopi, obiettivi, conclusioni, HAZOP worksheets, schemi e documentazione tecnica di riferimento che dovrà essere approvato da tutto il team e il project manager.

HAZOP si presenta come una metodologia di revisione progettuale di grande successo, in modo particolare nell'industria di processo, ne rappresenta lo studio più importante. I principali punti di forza risiedono nella sistematicità e flessibilità di applicazione da parte di un team multidisciplinare, nonché un guadagno dei costi sulle modifiche individuate e attuate in questa fase, anziché a progetto avvenuto. Per contro questa tecnica può risultare molto dispendiosa in termini di sforzi. Dipende fortemente sull'esperienza e la creatività di un team di lavoro ai quali si richiede una grande concentrazione. Inoltre si basa fortemente

sui progetti e informazioni a disposizione, se qualche particolare non viene riportato di questo non se ne terrà conto.

4.4 CHAZOP (Control system HAZOP)

Nell'industria di processo HAZOP si presenta come una tecnica ben consolidata e attuata nella pratica comune, tuttavia pone la sua attenzione principalmente agli aspetti direttamente correlati ai processi dell'impianto tecnologico. Ora più che mai, data la crescente integrazione dei sistemi di automazione e controllo sempre più complessi e con una funzione sempre più da protagonista all'interno dell'impianto, si rende necessario un aggiornamento delle pratiche inerenti alla sicurezza, che tengano conto di questi fattori, non più trascurabili. Durante uno studio HAZOP il sistema di controllo viene considerato, ma di fatto mai in modo approfondito, limitato solitamente alle attrezzature di campo. Questo limita lo studio sulla sicurezza dato che molteplici cause possono comunque innescare errori nel sistema di controllo, inducendo fermate non necessarie, che compromettono la qualità di produzione e disponibilità di impianto, ma anche possibili deviazioni pericolose nel processo impiantistico.

CHAZOP è una tecnica che consente di analizzare le debolezze di un sistema di controllo in un impianto di processo, è una variante che discende direttamente dalla metodologia HAZOP e pertanto presenta i medesimi obiettivi ed approccio. È facilmente implementabile a seguito di uno studio HAZOP, ma di fatto non è ancora prassi comune. Uno studio CHAZOP è pianificato sostanzialmente come la versione tradizionale della tecnica, già discusso nei paragrafi precedenti. In questo caso il team di lavoro sarà composto da figure professionali più orientate all'ambito dell'informazione come ingegneri elettrici/elettronici/di sistemi di controllo/automazione. I documenti richiesti allo studio saranno: schemi elettrici, schemi elettrici dell'alimentazione, architettura rete di controllo, data sheet, guide dei fornitori dei vari componenti, diagramma a stati, modalità di errori e il report HAZOP dell'impianto di processo gestito dal sistema di controllo. Con questo sarà possibile valutare le conseguenze indotte nel processo.

Per quanto riguarda la metodologia operativa si possono individuare due varianti: la prima strettamente correlata al metodo tradizionale, ne rappresenta la diretta evoluzione logica in termini di applicazione sfruttando quindi nodi, parole guida e proprietà. Esempi di proprietà possono essere: segnale, informazioni, flusso dati, velocità dati, valore dati, azione, tempo di risposta, codifica. La seconda, invece, considerando aree funzionali. Più precisamente

quest'ultima considera il sistema di controllo come un insieme di componenti, differenti per funzione ed architettura, che scambiano dati attraverso una rete di comunicazione (es. BPCS[24], SIS, pannelli nell'area di controllo, workstation, PLC singoli, strumentazione di rete come switches, gateway, firewall, sistemi di alimentazione). L'analisi avviene sistematicamente per ogni elemento, valutando tutte le possibili modalità in cui quell'elemento può generare un errore a partire da una serie di classi:

- Alimentazione elettrica (es. guasti, interruzioni ripetute, perdita di alimentazione);
- Guasti hardware (es. schede, connettori, moduli, tastiere);
- Software si considerano i peggiori casi cui l'output di un programma può assumere (es. dati congelati, alti, bassi, senza significato e nessun valore);
- Comunicazione (es. errori di rete, compatibilità con apparecchiature);
- Fattori umani (es. inserimento di dati e comandi scorretti, sovraccarico di comandi);
- Manutenzione
- Diagnostica (es. falsi allarmi dovuti alla diagnostica interna al sistema);
- Security (es. violazioni intenzionali: cyber/physical security);
- Condizioni ambientali (es. polvere, temperatura, fluidi, guasti nella ventilazione);
- Perdita di dati in memoria
- Modalità operative specifiche: (es. accensione, spegnimento, condizione di emergenza);

4.5 *Security risk assessment*

Come già anticipato precedentemente la tendenza e l'obiettivo perseguito a livello industriale è la realizzazione della "fabbrica automatica", ossia gestire processi, realizzare prodotti di qualità in modo efficiente senza l'intervento diretto dell'uomo, che svolge solo ruoli di controllo e supervisione, il modello CIM (Computer Integrated Manufacturing) ne rappresenta la struttura di riferimento.

[24] BPCS (Basic Process Control system), si intende quel sistema costituito dall'interconnessione di sensori, logica e attuatori, che esegue funzioni di processo e monitoraggio (figura 1.10 in grigio). Lavora in parallelo ai SIS.

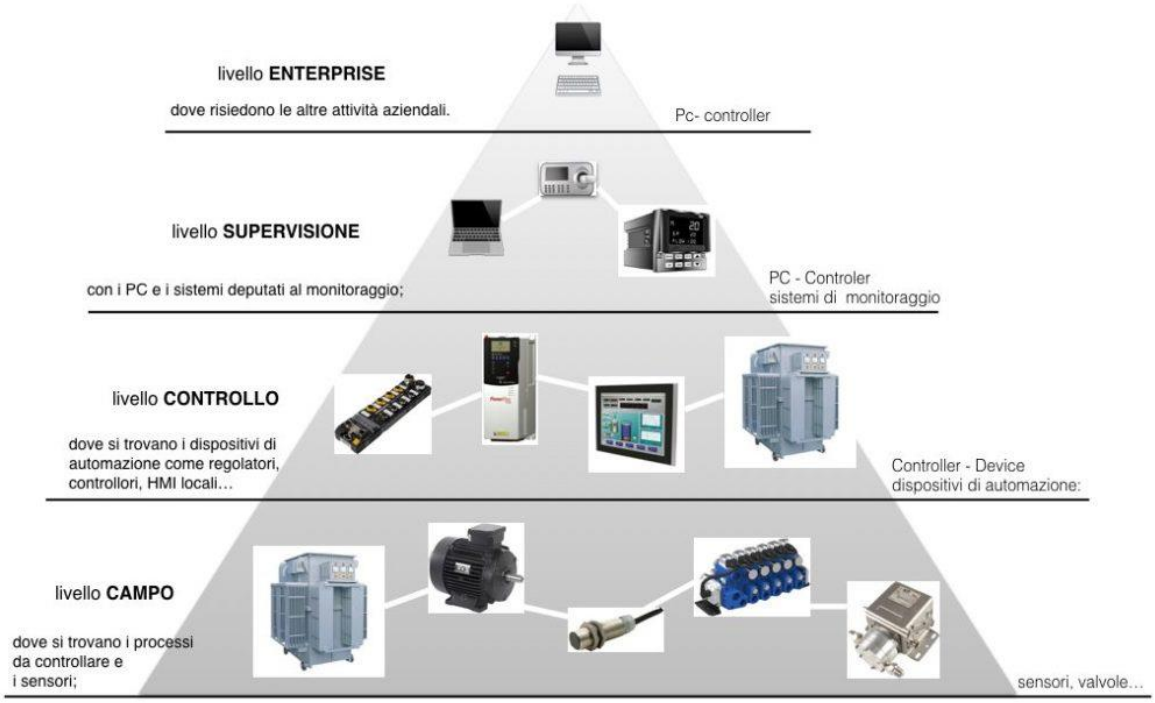

Figura n.4.6 Struttura del modello CIM

Il principio alla base sta nell'integrazione dei diversi livelli del processo produttivo/azienda in un'unica infrastruttura informatica che è in grado di gestire diverse tipologie di dati con caratteristiche ed esigenze differenti, realizzando una comunicazione verticale ed orizzontale di informazioni[25]. I vantaggi del modello CIM tra cui una maggiore efficienza dei processi produttivi, sono innumerevoli, ma l'integrazione di reti differenti può introdurre, vulnerabilità nel sistema, da intendersi non solo come minacce da parte del personale interno al sito di lavoro, ma anche nei confronti di minacce intenzionali esterne fisiche o virtuali.

Nel settore industriale una valutazione del rischio associata alla *security* si rende sempre più necessaria, al fine di garantire disponibilità, integrità, riservatezza di processi ed informazioni. Per quanto riguarda un impianto tecnico di produzione gli aspetti di sicurezza più importanti riguardano la disponibilità ed integrità: è essenziale evitare perdite di continuità non necessarie dei servizi della produzione e danneggiamenti fisici dei sistemi. La riservatezza dei dati non è una priorità a questo livello, la maggior parte di essi sono dati grezzi e senza contesto non hanno alcun valore. Per un'azienda una violazione criminosa può rappresentare oltre che una grave perdita dal punto di vista monetario, anche un danno all'immagine ed affidabilità dell'azienda stessa, incrinando rapporti con clienti e fornitori.

[25] Si pensi all'implementazione dei protocolli di comunicazione industriali Real time Ethernet (RTE).

A partire dalla seconda edizione dello standard internazionale *IEC 61511* (2016, attualmente in vigore) è stato introdotto (comma 8.4.2) la conduzione di una *security risk assessment* e che SIS e tutti i dispositivi associati ad esso siano progettati affinché garantiscano resilienza a rischi di questo genere. Nella maggior parte dei casi se un attacco criminoso è rivolto verso il sistema di controllo di processo (BPCS) le conseguenze che si verificano sono comparabili a quelle di un errore operativo o di un danneggiamento di una attrezzatura innescando la funzione di un SIS e riportando l'impianto ad uno stato sicuro. Ma se l'obiettivo della minaccia è un SIS la funzione di sicurezza associata può essere perduta, possono innescarsi errori nel sistema, comportamenti imprevedibili e rappresentare pertanto possibili fonti di danno. Violazioni di *security* nel sistema possono comprometterne la sicurezza funzionale[26].

Una valutazione dei rischi inerenti alla *security* può essere condotta a partire da un'analisi CHAZOP, dove vengono analizzate tutte le vulnerabilità di ciascun dispositivo collegato al sistema di controllo, considerando violazioni sia dal punto di vista hardware che dal punto di vista software che possono comportare conseguenze dannose. È importante, durante la valutazione, considerare tutti i possibili vettori della minaccia: percorsi, particolari condizioni o interconnessioni con sistemi interni ed esterni al sistema di controllo che possono favorire una violazione sia a livello fisico che a livello di rete. I principali punti di vulnerabilità di quest'ultima sono ad esempio: collegamenti non sicuri ad Internet, Firewall non adeguatamente configurati, collegamenti wireless e Modem non sicuri, stazioni PC/chiavette USB/programmi PLC infetti, collegamenti seriali RS-232 non sicuri. Le più comuni modalità di violazione virtuale sono: attraverso malware, malavertising, phishing email contenenti link verso siti/programmi infetti, Man in the Middle (MITM) che accede alla rete attraverso collegamenti wireless non protetti, rogue software ossia malware

[26] Nel 2017 si registra il primo caso di violazione di un SIS in un impianto petrolchimico in Arabia Saudita, a seguito di un attacco malware denominato come TRITON, riprogrammato attraverso software malevolo determinando uno stato d'errore nel sistema e causando l'arresto automatico in sicurezza del processo. L'obiettivo della minaccia è stato un controller Triconex della Schneider Electric. Secondo i ricercatori che hanno studiato l'incidente, gli autori dell'attacco hanno sfruttato metodi comuni come backdoor, programmi Mimikatz, e sessioni desktop remote per passare alla rete del sistema di controllo ed introdurre all'interno di una workstation il malware TRITON mascherato come software legittimo, necessario a gestire i log del controller. A seguito dell'esecuzione del programma, l'effettivo malware payload viene caricato nella memoria del controller cedendo il controllo remoto ad utenti esterni. A differenza di tecniche comuni utilizzate durante l'intrusione, per quanto riguarda lo sviluppo del software malevolo, i fautori dell'attacco hanno investito un discreto sforzo nella sua realizzazione violando il protocollo di comunicazione proprietario del controller, dimostrando una certa intenzionalità, probabilmente con lo scopo di creare ripercussioni fisiche.

mascherati come programmi di sicurezza necessari e drive by download ossia malware scaricati in un PC utente da un sito legittimo.

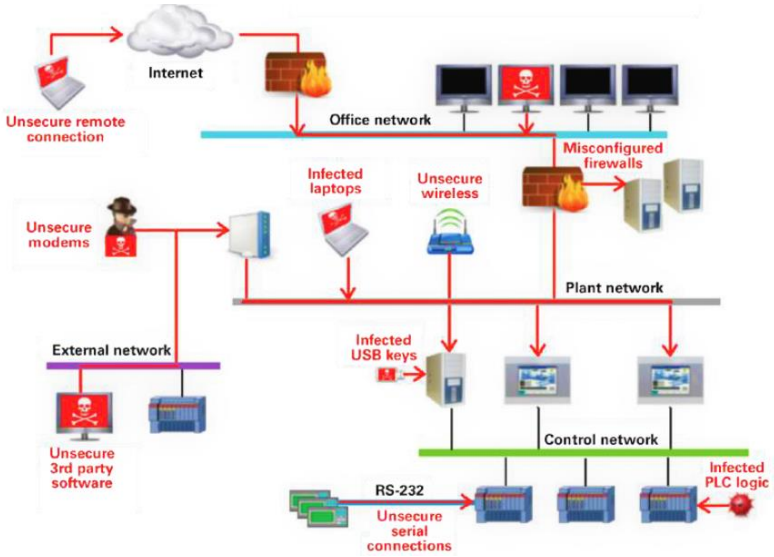

Figura n.4.7 Percorsi vulnerabili architettura di rete di controllo

Un criterio per procedere alla valutazione in particolare per individuare le aree di studio, viene illustrato nello standard *IEC 62443* e consiste nel suddividere l'architettura del sistema in zone e condotti. Le prime sono insiemi fisici o logici di elementi che condividono i medesimi requisiti di sicurezza o che isolano sistemi di controllo critici. I condotti sono raggruppamenti di comunicazioni che scambiano informazioni da e per una zona.

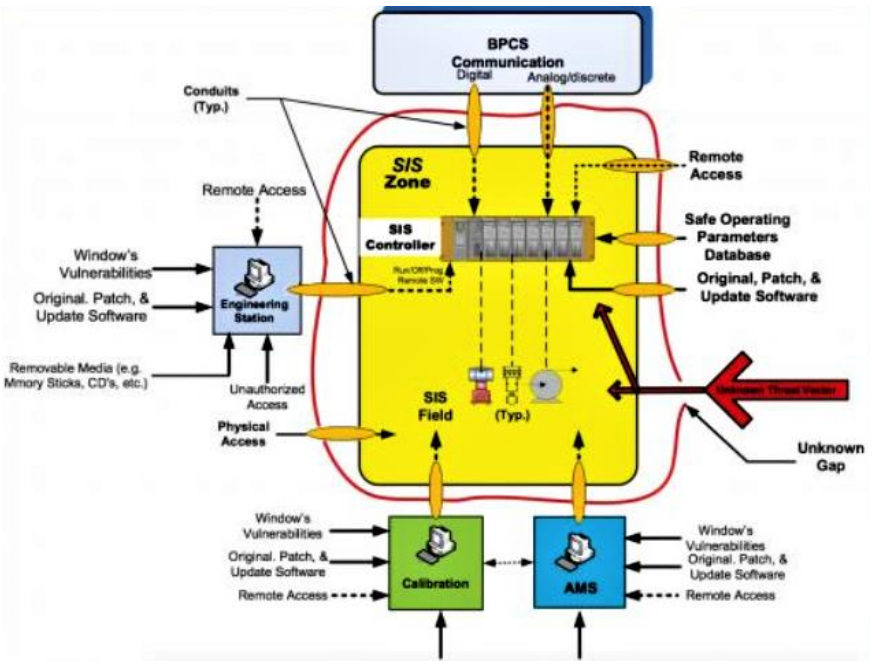

Figura n.4.8 Esempio di zona/condotti associata ad un sistema SIS

Capitolo 5: Design SIS

5.1 Introduzione

Il riferimento normativo inerente alla sicurezza funzionale è rappresentato dallo standard internazionale *IEC 61508: Sicurezza funzionale dei sistemi elettrici/elettronici/elettronici programmabili relativi alla sicurezza* che definisce linee guida in merito ai sistemi strumentati legati alla sicurezza, applicabili in qualsiasi settore industriale. A partire da questa sono stati adattati poi altri riferimenti normativi per settori più specifici e per quanto riguarda l'industria di processo lo standard è *IEC 61511*. Nel seguente capitolo ci si riferirà direttamente a quest'ultimo.
Per quanto riguarda la security industriale, invece, la norma guida è l'internazionale *IEC 62443: Sicurezza per l'automazione industriale e sistemi di controllo,* citata anche negli standard precedenti che definisce ed implementa i requisiti di *security* inerenti a sistemi di controllo legati all'automazione industriale (IACS).

Entrambi i riferimenti normativi fondano l'implementazione e il raggiungimento di un certo grado di sicurezza non solo a livello tecnologico, ma anche attraverso un approccio di ottimizzazione gestionale, durante l'intero ciclo di vita dei componenti, secondo un modello PDCA. Dalla fase di analisi di rischio, pianificazione, design, installazione e messa in servizio (pianificazione di procedure, organizzazione del personale, reparti), validazione (verifica del raggiungimento degli obiettivi preposti durante tutte le modalità di funzionamento: avviamento, spegnimento, manutenzione e attività anomale), manutenzione (gestione di programmi di manutenzione ordinaria e straordinaria, prove funzionali, audit), modifiche del sistema e dismissione.

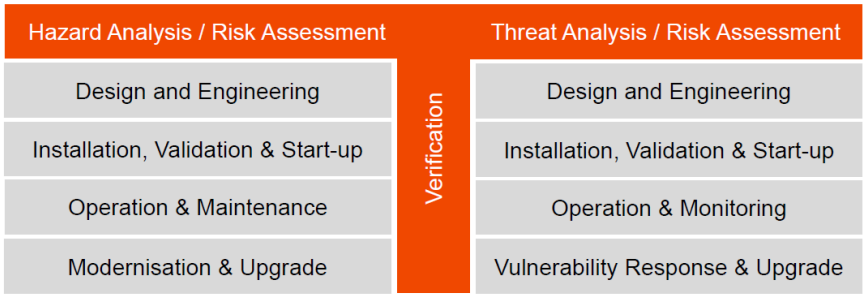

Figura n.5.1 Safety/security life cycle

Di seguito ci si focalizzerà principalmente sulle linee guida inerenti agli aspetti progettuali.

5.2 Livelli di sicurezza

5.2.1 *Safety Integrity Level* (SIL)

Il *Safety Integrity Level* (SIL) rappresenta un livello discreto legato ad un certo fattore di sicurezza che un SIS deve garantire, per svolgere una determinata funzione di sicurezza. La *IEC 61511* prevede 4 livelli discreti (SIL 1 – 4) in ordine di affidabilità crescente e a ciascuno di essi viene assegnato un determinato intervallo di valori in termini di PFD_{avg} o PFH, determinati quantitativamente in riferimento ai componenti di un certo sistema. Lo standard prevede due tabelle di riferimento SIL sulla base della modalità di funzionamento di una SIF valutata sul tasso di domanda[27] della stessa:

- Low demand mode: il tasso di domanda di una SIF è minore di 1 volta all'anno;
- High demand mode: il tasso di domanda di una SIF è maggiore di 1 volta all'anno;
- Continuous mode: la SIF riporta il sistema in uno stato sicuro come parte di una normale operazione.

Una volta individuata la modalità di funzionamento occorre stabilire il fattore di protezione o sicurezza richiesto da una certa funzione, individuata sulla base di un'analisi di valutazione dei rischi e stimata successivamente ad esempio attraverso un'analisi LOPA (vedi par. 3.6.2). Per la modalità high demand e continuous vengono utilizzati i medesimi riferimenti.

Quando un fabbricante/costruttore attesta la certificazione SIL per un dato dispositivo significa che questo può essere utilizzato per realizzare un SIS che richiede un certo livello di sicurezza. Utilizzare tutti dispositivi conformi non ne determina automaticamente la conformità, che deve essere dimostrata per l'intera funzione di sicurezza.
In ogni caso il livello SIL raggiunto da un SIS è sempre limitato dal dispositivo avente il livello di sicurezza minore.

[27] È determinato dalla frequenza degli eventi intermedi associato ad un certo scenario incidentale (es. vedi punto 3 par. 3.6.2).

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**PFD_{avg}**	**Required risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	**Average frequency of dangerous failures (failures per hour)**
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Tabella 5.1 Valori SIL

5.2.2 *Security Level* (SL)

I SL sono i livelli di riferimento forniti dalla *IEC 62443* che definiscono le capacità intrinseche di sicurezza che i sistemi di protezione (dispositivi di rete, software, integrati o altre particolari contromisure) devono garantire. A differenza dei livelli SIL che vengono assegnati sulla base di valori quantitativi associati alle probabilità di guasto dei componenti, i livelli SL vengono assegnati solo qualitativamente. Infatti, le cause associate a violazioni di security sono dovute ad attacchi intenzionali così come si considerano errori da parte di operatori, molto complesso da definire attraverso un approccio matematico. I SL si suddividono in quattro livelli (SL 1 – 4) in ordine di sicurezza crescente.

Sulla base di una valutazione del rischio che prevede la suddivisione del sistema di controllo in aree di analisi, per ciascuna di esse viene assegnato un determinato livello SL.

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No ojective
SL2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violations using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL4	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical Damage	High sophisticated	High	Aggressive

Figura n.5.2 Security level (SL)

5.3 Requisiti di progettazione *IEC 61511*

5.3.1 Specifica Requisiti di Sicurezza (SRS)

La specifica SRS è un insieme di uno o più documenti necessari alla redazione della specifica di progetto e validazione del sistema strumentato di sicurezza, descrive i requisiti a livello di architettura e programma applicativo installato che la funzione di sicurezza deve possedere, ricavati sulla base di osservazioni dal team di lavoro o individuate durante l'analisi di valutazione del rischio. In sostanza si descrive la SIF dal punto di vista funzionale. Secondo lo standard la specifica SRS dovrebbe contenere informazioni che riguardano:

- Una descrizione qualitativa/schematica della funzione di sicurezza da implementare (es. diagrammi causa-effetto), modalità di funzionamento e livello SIL associato. Si richiedono anche informazioni a riguardo dei parametri monitorati dalla funzione (es. range opearativi, accuratezza) e relazioni tra ingressi ed uscite (es. funzioni matematiche, logiche);
- Informazioni relative ai guasti di modo comune;
- Una descrizione dello stato sicuro attuato dalla SIF, in termini di elementi dell'impianto coinvolti (es. sensori, attuatori) e in quale sequenza questi operano;
- Informazioni sull'intervallo di test funzionali e sulla loro conduzione potrebbe influire sulla realizzazione del sistema (es. documenti, durante del test, stato dei device);
- Tempo di intervento da parte di un SIS per riportare il processo ad uno stato sicuro;
- Modalità di rilevamento (es. allarmi) e risposta di un SIS (es. vicino alle condizioni limite o lontano);
- Informazioni a riguardo di un eventuale restart del processo dopo l'attuazione di una SIF (es. manuale, semi-automatico, automatico);
- Requisiti per bypassare SIS durante attività di manutenzione o test mentre i processi sono in corso (es. device, chiavi di accesso, password);
- Interfaccia tra il SIS ed altri sistemi (es. BPCS, operatori);
- Requisiti sul programma applicativo implementato;
- Identificazioni di condizioni ambientali estreme cui il SIS potrebbe essere esposto durante la sua vita operativa (es. temperatura, umidità, vibrazioni, agenti

contaminanti, interferenze elettromagnetiche/onde radio EMI/RFI, accumulo di cariche, allagamento, fulminazione);

5.3.2 Progettazione e sviluppo SIS

Sulla base dei requisiti espressi nella specifica SRS, vengono redatti i documenti tecnici di progetto per la realizzazione della SIF che consentano poi di verificare il raggiungimento del livello SIL necessario. Le specifiche di progetto dovrebbero rispettare almeno i seguenti requisiti:

Requisito	Descrizione
Comportamento del sistema al rilevamento di un guasto	Al rilevamento di un guasto da parte di un sistema diagnostica, test di prova o altro, la sicurezza del sistema dovrebbe essere garantita, in caso contrario dovrebbe essere adottata un'azione per ottenerla. Se queste azioni dipendono da un'azione manuale da parte di un operatore in seguito ad un allarme, quest'ultimo viene considerato come parte integrante del SIS;
Tolleranza guasti hardware	Vincoli hardware del sistema in relazione al SIL;
Selezione dei componenti	La scelta dei dispostivi utilizzati per un SIS dovrebbe essere supportata da appropriata documentazione che riporta informazioni riguardanti specifiche tecniche, considerazioni di qualità dal fabbricante, performance del dispositivo in certi ambienti operativi, esperienza operativa;
Dispositivi di campo	Dovrebbero essere selezionati ed installati in modo da ridurre guasti dovuti all'ambiente operativo, dovrebbero essere considerate condizioni come: corrosione, congelamento di materiale nelle condutture, polimerizzazione, temperature e pressioni estreme, dovrebbero essere garantite misure per garantire l'integrità del circuito di alimentazione;
Interfacce operatore/manutentore/comunicazione	Il progetto del SIS dovrebbe richiedere la minor richiesta da parte dell'operatore di selezionare opzioni o bypassare il sistema. L'interfaccia operatore dovrebbe contenere informazioni

	riguardanti: la sequenza in corso del processo, se la funzione SIF è stata attivata, presenza di bypass, stato di sensori e attuatori, risultato della diagnostica. L'interfaccia manutentore dovrebbe consentire funzioni protette come: modalità operativa, diagnostica SIS, modifica del programma applicativo. Dovrebbe essere separata dall'interfaccia operatore e qualsiasi guasto nell'interfaccia non dovrebbe interferire nella funzione del SIS. Nell'interfaccia di comunicazione del SIS un guasto non deve pregiudicare la SIF o il mantenimento dello stato sicuro.
Manutenzione e collaudo	Il design dovrebbe permettere di testare il SIS nel suo completo che per segmenti. Qualora il tempo di downtime del sistema fosse più grande dell'intervallo di prova sono richiesti test online (che entrano a far parte del SIS). Durante il bypass di un SIS l'operatore dovrebbe essere avvisato mediante allarmi o procedure, la sicurezza deve essere sempre garantita. La forzatura di input o output del sistema non dovrebbe essere permessa senza la messa offline del SIS a meno di procedure e protezioni adeguate.
Probabilità di guasto SIF	Si richiede il calcolo della probabilità di guasto per ogni SIF;
Software applicativo	Si richiede l'utilizzo di linguaggi di programmazione LVL e FVL. Qualora il software implementi funzioni di sicurezza e non, occorre dimostrare che queste non interferiscano tra loro e viene considerato parte del SIS. Il programma dovrebbe essere progettato in modo che una volta portato il sistema in uno stato sicuro questo venga mantenuto fino ad un comando di reset, anche in condizioni di perdita di alimentazione.

Tabella n.5.1 Requisiti progettuali SIS

- Requisiti di tolleranza ai guasti hardware: gli elementi che costituiscono un SIS sono vincolati ad un certo valore di Hard Fault Tolerance (HFT)[28] che determina un livello minimo di ridondanza nell'architettura, sulla base del livello SIL di riferimento. Gli standard indicano due possibili strade: una metodologia quantitativa (1H) ed una metodologia più qualitativa applicabile quando si dispongono di una grande quantità di dati relativi ai componenti (2H). Di seguito si farà riferimento alla 1H. Sulla base delle loro caratteristiche i componenti vengono suddivisi in due categorie: tipologia A e B ai quali corrispondono requisiti hardware differenti. Nella classificazione di tipo A tipicamente rientrano i sistemi più semplici, che al loro interno non incorporano microprocessori (es. valvole meccaniche) e in cui si ha una completa definizione di tutte le modalità di guasto di tutti i gli elementi che lo compongono e sufficiente documentazione di dati storici a supporto dei valori di tasso di guasti pericolosi (rilevati e non); nella classificazione di tipo B rientrano sistemi che non riescono a garantire quanto detto precedentemente, normalmente ne fanno parte sistemi complessi a microprocessore e software (es. PLC). Per ogni elemento viene assegnato un certo valore di *Safe Failure Fraction* (SFF) valutato quanto segue:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \qquad (5.1)$$

Sulla base dei valori delle tabelle di riferimento incrociando i valori SFF e il valore di HFT ricavato dalla architettura prevista inizialmente è possibile stabilire il SIL raggiunto da un dato elemento che dovrà essere conforme al minimo con quanto previsto (ci possono essere condizioni da considerare che possono indurre a scelte più restrittive).

SFF	TYPE A Minimum Hardware Fault Tolerance			TYPE B Minimum Hardware Fault Tolerance		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	Not allowed	SIL 1	SIL 2
60% < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Tabella 5.2 Vincoli HFT

[28] È associato al valore N - K di un sistema KooN.

5.4 Misure di protezione (*security*)

Analogamente con quanto avviene in un sistema impiantistico (Fig. 1.5) i sistemi di protezione relativi alla security di uno IACS sono implementati in livelli e con metodologie differenti, per ridurre la probabilità che una violazione venga fermata prima che raggiunga l'obiettivo target. La sicurezza ottenuta attraverso questa strategia denominata *defense in depth* si basa sull'integrazione di sistemi di protezione (*layer of defense*) appartenenti a tre categorie: tecnologie, processi e persone rappresentati da tre figure differenti: *product supplier* responsabile dello sviluppo e commercializzazione dei componenti utilizzati nel sistema di automazione, il *system integrator* che ha il ruolo di implementare i diversi prodotti e tecnologie nel sistema di automazione configurandoli in modo da raggiungere i requisiti previsti e *l'asset owner* responsabile della definizione di requisiti, operazioni, manutenzione e dismissione dello IACS. In sostanza la sicurezza di un sistema viene raggiunta convergendo tecnologia e misure organizzative con la collaborazione di più figure di ruolo.

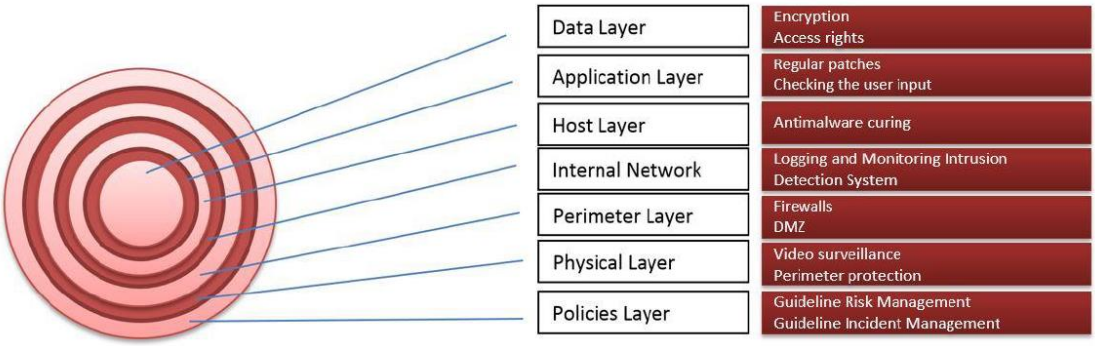

Figura n.5.3 Defense in depth

Non esistono soluzioni di sicurezza standard, dato che ogni stabilimento possiede vincoli ed obiettivi differenti, ma possono essere individuati tre fattori chiave per la sicurezza: *plant security*, *network security* e *system integrity*.

5.4.1 *Plant security*

Ci si focalizza sulla protezione da violazioni fisiche dello stabilimento. Si adottano misure e procedure quali barriere, tornelli, videocamere, e lettori badge per limitare gli accessi a personale non autorizzato in determinate zone dell'impianto. È possibile adottare una separazione fisica delle diverse aree della produzione con accessi differenziati o adottare una

protezione fisica (es. contenitori bloccati) per determinati componenti dello IACS. Le misure fisiche dello stabilimento influiscono sulla sicurezza di rete: se un'area è stata fisicamente protetta le misure di rete possono essere meno stringenti.

5.4.2 *Network security*

Lo scopo è quello di controllare e limitare gli accessi non autorizzati tra interfacce delle varie reti dello IACS (es. reti di ufficio, rete di sistema di controllo), intercettazioni e manipolazioni delle informazioni trasmesse all'interno della stessa.

Questo può essere ottenuto implementando firewall o una zona demilitarizzata (DMZ). La DMZ è una porzione di rete pubblica accessibile dall'esterno che funge da cuscinetto tra la rete esterna (es. WAN, Internet) e la rete interna (es. rete del sistema di automazione) le quali non possono comunicare direttamente. Gli accessi verso dati, dispostivi, server e servizi vengono protetti e gestiti dalla DMZ.

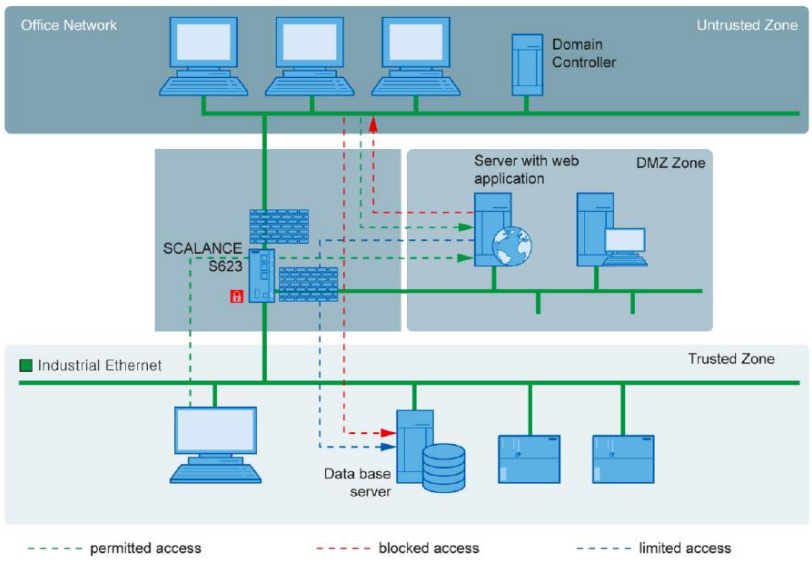

Figura n.5.4 DMZ tra rete office e rete di impianto

Un altro aspetto importante che contribuisce all'incremento della sicurezza è la segmentazione della rete in sotto-reti a ciascuna delle quali è associata una cella automatica. Questa separazione viene raggiunta adottando componenti di rete con capacità di sicurezza

integrata[29] che gestiscono la comunicazione tra la rete della cella e la rete esterna senza comprometterne la funzionalità. Queste possono stabilire con quali nodi della rete possono comunicare e attraverso quali protocolli, è possibile inoltre adottare tecniche di comunicazione crittografate.

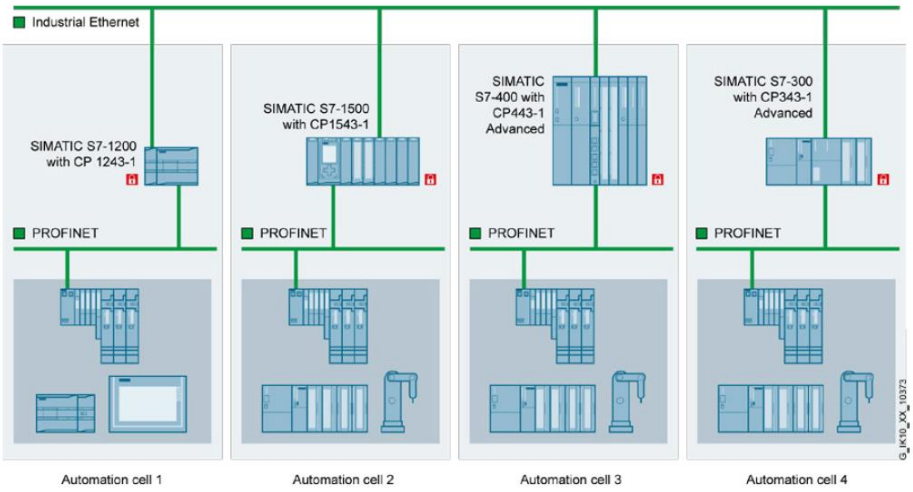

Figura n.5.5 Segmentazione rete con device dotati di sicurezza integrata

Per quanto riguarda la comunicazione remota (GPRS, UMTS, LTE) collegata direttamente ad Internet, utilizzata particolarmente per il monitoraggio e manutenzione a distanza, vengono utilizzati meccanismi di comunicazione VPN per garantire autenticazione, crittografia ed integrità dei dati trasmessi proteggendo la rete da accessi non autorizzati.

5.4.3 *System integrity*

L'obiettivo è quello di garantire l'integrità di sistemi di controllo e automazione, controllori e stazioni di PC industriali, da accessi non autorizzati, malware o altri specifici requisiti.

Per quanti riguarda le stazioni di PC industriali si ricerca la protezione attraverso software antivirus purché questi non influenzino l'attività di automazione o in aggiunta attraverso whitelisting, ossia la creazione di elenchi approvati dall'utente in cui vengono specificati i programmi che possono essere installati in un determinato PC.

[29] Tecniche di sicurezza integrata possono essere: whitelist del codice eseguibile, in cui solo i programmi autorizzati possono essere eseguiti nel device sulle quali sono permesse solo modifiche autorizzate e registrate, controllo della memoria durante l'esecuzione dei processi, sistema di audit integrati.

Per quanto riguarda i controllori la sicurezza viene raggiunta attraverso protezione multi-accesso con diritti di accesso differenziati e attraverso specifici protocolli di comunicazione con sicurezza integrata. Talvolta questi possono implementare interfacce sicure con il resto della rete attraverso firewall integrati o connessioni VPN.

Conclusioni

L'identificazione dei pericoli si presenta come uno studio fondamentale all'interno di una valutazione dei rischi perché è sulla base dei risultati in uscita che verrà eseguita l'analisi e per quanto questa possa essere accurata se i pericoli, fonte di possibile danno, non sono stati esaminati in modo sistematico, in conclusione lo studio sulla sicurezza presenta gravi lacune. Per l'industria di processo HAZOP nonostante sia una tecnica che richiede un discreto sforzo esecutivo, è una metodologia potente e flessibile per questa tipologia di studi e difatti è ampliamente applicata e accettata.

Alla luce delle problematiche evidenziate in merito all'integrazione di tecnologie di automazione e interconnessione di reti differenti, si rende necessario uno studio sul sistema di controllo associato ai processi di un impianto tecnologico così come una valutazione sulla *security* del sistema che talvolta può sfociare in una questione di sicurezza funzionale. Quest'ultimo aspetto recentemente sta acquistando sempre più spessore, viene richiesta un'analisi di *security* anche nelle norme di riferimento per i SIS di processo, *IEC 61511*, così come in fase di pianificazione del sistema di gestione di sicurezza per impianti "Seveso", nella *UNI 10617*.

Grazie all'adattabilità della tecnica HAZOP è possibile realizzare uno studio sulle deviazioni nel sistema di controllo che influiscono sulla disponibilità dell'impianto di processo o degenerare in conseguenze dannose, così come lo studio sulla *security*, attraverso l'esecuzione della variante denominata CHAZOP. Questa è facilmente implementabile a seguito dello studio "tradizionale", ma non è ancora una prassi comune. Sulla base di queste considerazioni si può pensare di organizzare lo studio di identificazione dei pericoli per un impianto di processo combinando in modo efficace entrambe le metodologie, per risolvere le esigenze di sicurezza richieste.

Bibliografia

[1] Dave McDonald, Hazop, Trips and Alarms;

[2] David J. Smith, Kenneth G. L. Simpson, The Safety Critical Systems Handbook;

[3] Department of Mechanical and Industrial Engineering – NTNU, Mary Ann Lundteigen, Marvin Rausand, Calculation of PFD using RBD;

[4] Dipartimento di Energetica – Politecnico di Torino, Andrea Carpignano, Sara Tuninetti, Analisi comparativa dei criteri di accettabilità del rischio e considerazioni sul D.M. maggio 2001;

[5] Dipartimento di Scienze politiche e sociali – Università di Pavia, Bruno Ziglioli, "Un groviglio di problemi": le conseguenze politiche, istituzionali e amministrative di un disastro industriale;

[6] Direttiva 2006/42/CE, "Macchine";

[7] Direttiva 2012/18/UE, "Seveso III";

[8] D.lgs. 26 giugno 2015, n.105, attuazione della direttiva 2012/18/UE relativa al controllo del pericolo di incidenti rilevanti connessi con sostanze pericolose;

[9] D.M. 09/05/2001, Requisiti minimi di sicurezza in materia di pianificazione urbanistica e territoriale per le zone interessate da stabilimenti a rischio di incidente rilevante;

[10] Edoardo Galatola, Corrado Clini, Giorgio Macchi, Rita Caroselli, Le analisi di rischio d'area, stato dell'arte, diffusione ed utilità;

[11] Frank Crawley, Hazop: Guide to Best Practise;

[12] ICARO s.r.l., Metodologie per l'elaborazione dell'analisi dei rischi di incidente rilevante;

[13] Inail, Paolo Pittiglio, Paolo Bragatto, Gestire la sicurezza negli stabilimenti industriali;

[14] La Chimica e l'industria, Quali lezioni dall'incidente di Seveso?, Settembre 2004, Anno 86 n.7;

[15] La Stampa, Seveso: non fatalità ma una scelta, lunedì 9 Agosto 1976, Anno 108 – Numero 167;

[16] Marvin Rausand, Risk Assessment – Theory, Methods and Applications;

[17] Mino Carrara, Giampiero Valsecchi, Un racconto dell'emergenza e della bonifica;

[18] Normativa *UNI 10617;*

[19] Normativa *IEC EN CEI 31010;*

[20] Normativa *IEC EN CEI 61511;*

[21] Normativa *IEC EN CEI 61882;*

[22] Normativa *IEC EN CEI 62443;*

[23] Paolo Senni, La filosofia di Deming e il ciclo PDCA;

[24] Peter Clarke, Introduction to CHAZOP: Introduction to chazop: assessing the risks of control system failure, whitepaper;

[25] Risoluzione del Consiglio, 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione;

[26] Siemens, Security concept for process and discrete industries, whitepaper;

[27] T.A. Kletz, The Origins and History of Lost Prevention;

[28] TUV Nord Group, Industrial security based on IEC 62443, whitepaper;

[29] Vito Carrescia, Fondamenti di Sicurezza Elettrica;

Sitografia

[30] www.boscodellequerce.it;

[31] www.europa.eu;

[32] www.fireeye.com

[33] www.isprambiente.it;