ANALISI DI RISCHIO

dell'industria e dell'impiantistica di processo e produttiva

- **HAZOP**: QUESTO (S)CONOSCIUTO

Michelangelo Costa

ANALISI DI RISCHIO

L'analisi di rischio ha radici lontane nel tempo. Fu il metodo per eccellenza utilizzato negli ambienti scientifici internazionali sin dagli anni '50 – '60 per stimare prima e quantificare poi il rischio effettivo associabile ad impianti complessi, spesso definibili ad alto rischio, cioè impianti o stabilimenti in cui si potevano immaginare o prevedere accadimenti con conseguenze e percoli anche gravi per i lavoratori e la popolazione.

I settori in cui si svilupparono le prime metodologie "strutturate" e guidate da standard sempre più evoluti e definiti per le applicazioni degli analisti di scurezza e quindi anche per la verifica da parte delle Autorities furono: il settore nucleare (uso pacifico dell'energia nucleare) e quello aeronautico.

Iniziarono così a prendere corpo le definizioni di affidabilità, disponibilità frequenza di accadimento e quindi fu definito il concetto vero e proprio di rischio, inteso come combinazione di frequenze (probabilità) e conseguenze (danni).

I primi a formulare in modo organico e ragionato standards e tecniche di analisi di rischio furono senza dubbio gli americani. Il metodo di analisi di rischio quantitativo chiamato inizialmente con il nome di PSA (Probabilistic Safety Assessment) costituì la rampa di lancio per il successivo sviluppo e la conseguente diversificazione di tutte quelle tecniche oggi così tanto affermate ed applicate nel mondo, nei più svariati settori dell'industria ad alto-medio rischio o agli impianti pericolosi o ai prototipi di impianti o sistemi innovativi ad alto rischio atteso.

A ben pensarci, la storia di questo sviluppo è comunque stata alquanto breve.

Si tratta infatti di circa poco più che un mezzo secolo, e ciò rappresenta in effetti un breve lasso di tempo rispetto all'intera storia dello sviluppo industriale mondiale.

E' necessario subito affermare un concetto basilare, anche se apparentemente ovvio, ma che ritengo personalmente invece molto interessante anche se crudo.

Ovvero il fatto che quando l'uomo si trova ad affrontare e gestire tecnologie o sistemi complessi nuovi, nonostante la sua enorme potenzialità conoscitiva, devono accadere eventi disastrosi perché riesca a "soppesare" e prendere la giusta coscienza dell'adeguatezza delle analisi di sicurezza da lui prima adottate. Cioè, con altre parole, deve potere essere in grado di testarne l'idoneità, facendo esperienza diretta di una vasta gamma di eventi incidentali ad ampio spettro. Certo ciò può determinare spesso la gravissima perdita di vite umane e di impatti ambientali globali a volte anche difficilmente recuperabili, ma questa è la natura della dinamica del consolidamento dell'affidabilità stessa delle tecniche di valutazione del rischio.

Questo vale per tutte le discipline in cui sono presenti tecnologie cosiddette "pericolose" ed è sotto gli occhi di tutti, ma spesso siamo portati a dimenticare.

Non è forse questo quello che accade quando avviene un grave e rarissimo sisma di elevata intensità? Dopo (ma solo dopo) si inaspriscono le previgenti normative sulle costruzioni antisismiche e si aggiorna la mappature delle zone classificate sismicamente.

Dopo (ma solo dopo) il grave incidente di Seveso partì una specifica normazione di regolamentazione dei siti industriali classificati a incidente di rischio rilevante. Dopo (ma solo dopo) il disastro di Fukushima si iniziò (per la prima volta) a livello internazionale a mettere in discussione l'accettabilità del concetto di frequenza di accadimento per le analisi di rischio in campo nucleare, ecc. ecc.

Questa analisi porta a meglio comprendere che nel tempo (lungo i decenni) è naturale che vi sia una sempre maggiore attenzione e consapevolezza al rischio a cui siamo soggetti e quindi che ciò ci insegni a modificare di conseguenza il nostro atteggiamento umano e professionale.

AMBITO NORMATIVO DI RIFERIMENTO

Se restringiamo ora il nostro campo di indagine, almeno per gli scopi di questo articolo, al settore industriale o di processo o di impianti ad alto rischio, dobbiamo subito prendere visione del contesto normativo in cui stiamo agendo nel parlare di analisi di rischio.

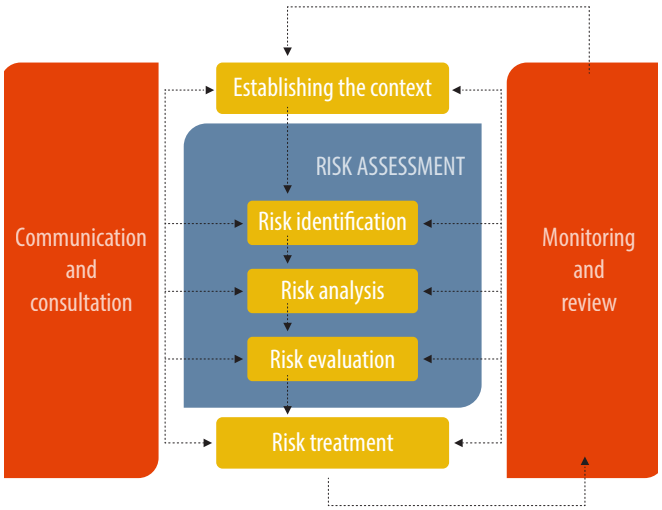
Solo recentemente sono stati emessi, finalmente, alcuni standard internazionali che delimitano il campo in cui l'analisi di rischio (anche industriale o di impianto-sistema) si colloca. In particolare il grande ampio ambiente è delineato dalla:

ISO 31000 : 2009 "Gestione del Rischio – Principi e linee guida"

che ne definisce l'ambito in senso del tutto generale, nel senso che qui si tratta di qualsiasi rischio, da quello di perdita di vita umane a quelli finanziario.

Pertanto, dentro quest'ambito il tema qui trattato trova una collocazione di sottoinsieme in termini di analisi di rischio inteso come sicurezza industriale e quindi ne costituisce un approfondimento di tipo verticale.

CONTRIBUTION OF RISK ASSESSMENT TO THE RISK MANAGMENT PROCESS



Una sotto-norma correlata alla ISO 31000 è la:

IEC 31010 : 2009 "Gestione del Rischio – Tecniche di valutazione del rischio"

In cui vengono presentate le tecniche oggi più utilizzate descrivendone: le caratteristiche, i vantaggi e gli svantaggi.

Oltre alla IEC 31010, vi sono poi una serie di normative molto dettagliate in materia di affidabilità e disponibilità che fanno capo al grande ambito dei cosiddetti "International standards on Dependability" emessi dalla IEC (International Electrotechnical Commission) e che sono strettamente correlati alla famiglia di standard sempre di IEC sulla sicurezza funzionale: le IEC 61508:2010 e le IEC 61511:2003.

Per chiudere questo breve inquadramento normativo di riferimento, dobbiamo anche citare lo standard, apparentemente isolato, ma in realtà strettamente connesso alle norme più sopra citate, ovvero la norma ISO inerente alla BUSINESS CONTINUITY, oggi alquanto di moda.

IEC 22301 : 2009 "Societal Security – Business continuity management systems – requirements"

LE TECNICHE UTILIZZATE

Tra le 31 tecniche di valutazione del rischio presentate nello standard IEC 31010, quelle più adatte al tema trattato sono le seguenti:

- ***HAZOP (Hazard and Operability studies)***
- ***FMEA (Failure Mode and Effect Analysis)***
- ***ETA (Event Tree Analysis)***
- ***FTA (Fault Tree Analysis)***
- ***LOPA (Layer of Protection Analysis)***
- ***Couse and Consequences Analysis***
- ***Couse and Effect Analysis***
- ***Risk Indices***
- ***Ecc.***

Si deve comunque dire che entro l'elenco della IEC 31010 vi sono anche tecniche come la "chck-list" o il "brainstorming", e quindi in effetti tra le 31 tecniche presentate ve ne sono parecchie di tipo molto limitato.

Queste tecniche hanno spesso applicazioni molto diversificate e raramente sono alternative o interscambiabili. L'analista di rischio esperto non trova molta difficoltà, quando il cliente gli sottopone i sui desiderata in termini di analisi di rischio o di ottimizzazione dell'affidabilità, ad individuare quale tecnica sia più adatta al caso in esame.

Comunque sono classificate in relazione alla loro capacità di ottenere:

1. ***Identificazione dei rischi (Risk identification);***
2. ***Analisi di Rischio (conseguenze, probabilità, livello di rischio)***
3. ***Quantificazione del rischio (Risk evaluation)***

Le tecniche che sono in grado di determinare tutte e tre i livelli di *Risk assessment process* qui sopra elencati sono però solo 13 su 31.

IL METODO "HAZOP"

Il metodo di analisi di rischio HAZOP, definito in modo preciso dallo standard:

IEC 61882 : 2001 – "Hazard and Operability studies (HAZOP studies) – Application guide"

è una delle più note tecniche a livello internazionale, adottato per lo sviluppo di analisi di sicurezza, impatto ambientale e operabilità di impianto, applicata in ambito medio-alto rischio.

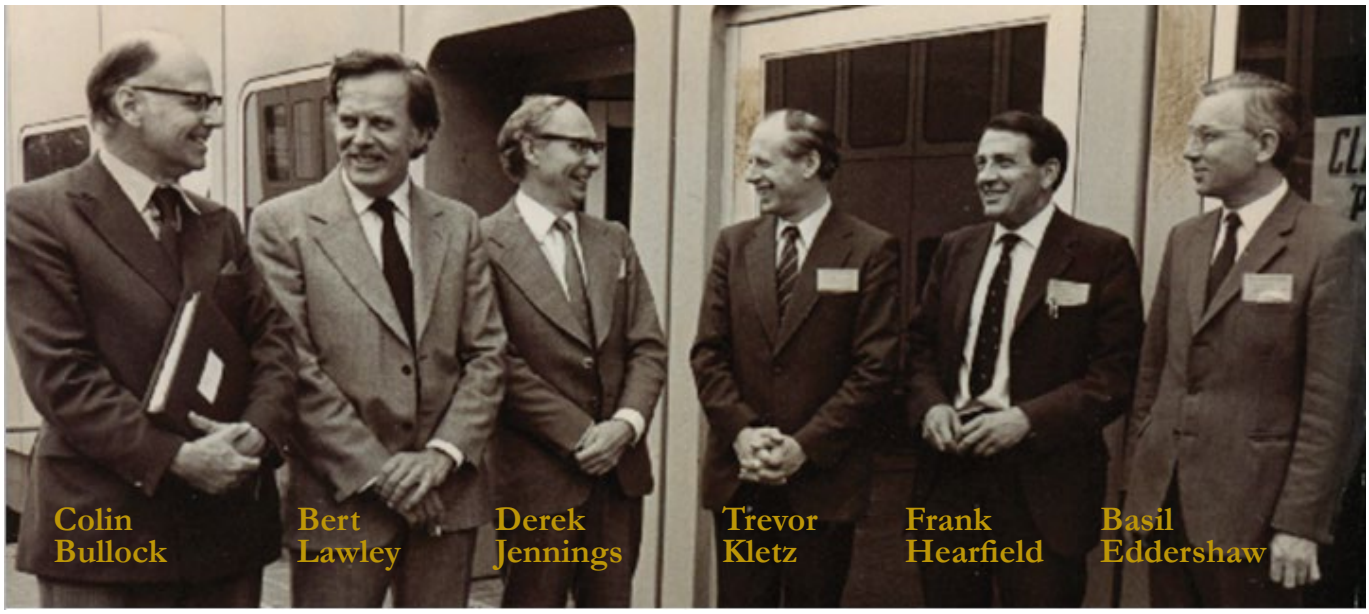
Si utilizza per effettuare una corretta e completa ANALISI DI SISTEMA nella sua interezza e determinare, mediante diverse sessioni di studio che si svolgono come "brainstorming" coinvolgendo diverse figure del processo, del progetto e della manutenzione, tutte le possibili azioni correttive / migliorative sul progetto lungo il suo iter di sviluppo sino alla approvazione e alla costruzione.

UN PO' DI STORIA

Il metodo HAZOP nacque in UK negli anni sessanta.
Avvennero in alcuni impianti chimici inglesi degli incidenti "anomali" e di cui non si riusciva ad identificare le cause scatenanti, diciamo che si poteva trattare in un certo sensi di "eventi misteriosi".

Allora le Autorità Britanniche decisero subito di costituire una sorta di gruppo di esperti di sicurezza industriale per mettere a punto un nuovo metodo di analisi di scurezza applicabile ai casi accaduti.
Nacque così un team di esperti che fondarono il METODO HAZOP.

La culla dell'HAZOP fu Manchester dove allora era attivo un dei poli industriali più forti d'Europa.



LE POTENZIALITÀ DEL METODO HAZOP

Il metodo HAZOP ha elevatissime potenzialità di analisi.
Ciò è dovuto essenzialmente al fatto che si tratta di un'analisi di rischio di tipo FUNZIONALE e non di sistema e quindi può essere applicato in modo molto efficace anche in fase molto preliminare del progetto (fase concettuale) e può adattarsi lungo lo sviluppo o l'evoluzione del progetto, guidando le scelte progettuali in termini di sicurezza e affidabilità oltre che di operabilità di impianto o di processo.
Questa sua versatilità risulta inoltre particolarmente vantaggiosa quando si debba analizzare prototipi o esemplari unici e quindi dove non si disponga di alcun dato di esperienza pregressa.

Contrariamente a quanto si pensi, inoltre, il metodo HAZOP è utilissimo anche su impianti o sistemi esistenti. Infatti esso è in grado, partendo dai disegni del processo o del sistema (PFD o P&ID) qualunque sia il loro livello di dettaglio o di complicatezza, di analizzare in modo sistematico ed esaustivo le eventuali lacune in termini di sicurezza e affidabilità.

Queste potenzialità, che saranno dimostrate tanto più importanti quanto più esperto sarà l'HAZOP Leader che il Cliente incaricherà per la gestione dell'analisi, sono molto bene espresse dalla definizione stessa di HAZOP, riportata qui di seguito secondo la formulazione storica ufficiale dei Padri Fondatori.

WHAT IS HAZOP?

Hazard and operability study (HAZOP) is a ***formal, qualitative, systematic*** *and* ***rigorous*** *examination of a plant, process or operation to identify credible* ***deviations*** *from the design intent in the context of the* ***complete system*** *that can contribute to hazards or operability problems, by applying the* ***experience, judgement*** *and* ***imagination,*** *stimulated by key words, of a* ***team.***

L'APPLICAZIONE DEL METODO

1 Sul Process Flow Diagram (PFD) generale di impianto si definiscono le sottosezioni di impianto da sottoporre ad analisi (chiamati "segmenti" o "nodi")

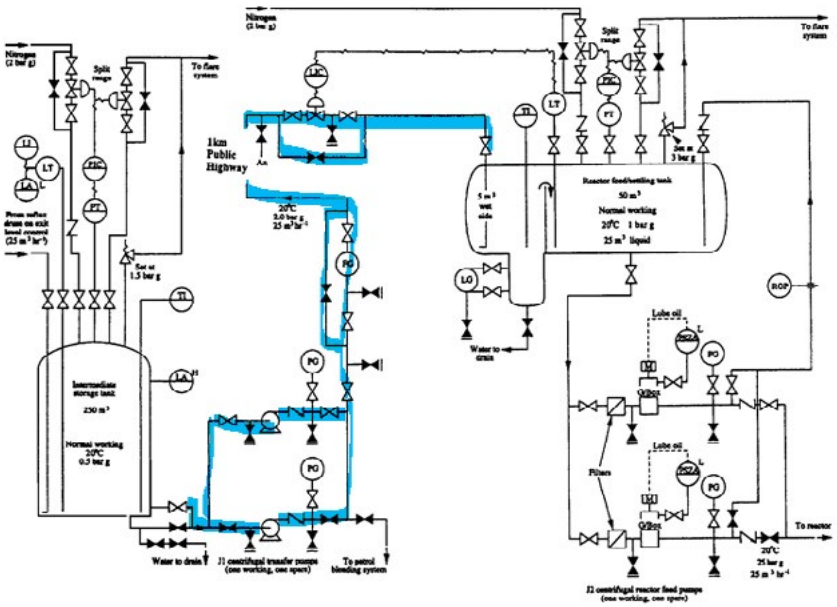
2 Si definiscono i PARAMETRI FISICI da analizzare

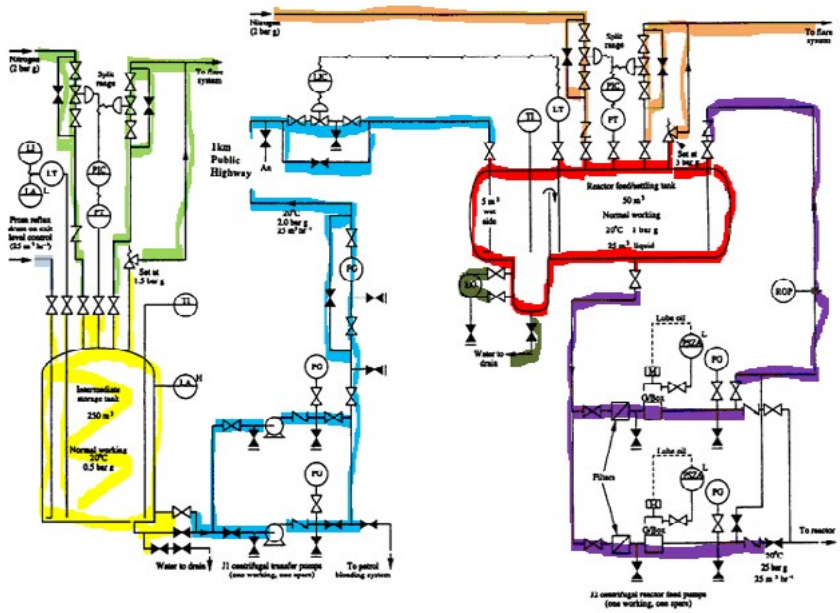
PROCESS

- *Flow*
- *Temperature*
- *Pressure*
- *Level*
- *Separation (settle, filter, centrifuge)*
- *Composition*
- *Reduction*
- *Mixing*
- *Absorb*
- *Corrode*
- *Erode*

OPERABILITY

- *Isolate*
- *Vent*
- *Drain*
- *Purge*
- *Insperct*
- *Maintain*
- *Start-up*
- *Shutdown*





3 Si definisce con il Cliente l'INTENTO o lo SCOPO PRIMARIO dell'impianto

4 Si definiscono le PAROLE GUIDA

WORD	MEANING
No *not, none*	The design intent does not occur, or the operational aspect is not achievable
Less *less of, lower*	A quantitative decrease in the design intent occurs
More *more of, higher*	A quantitative increase in the design intent occurs
Reverse	The opposite of the deign intent occurs
Also *as well as, more than*	The design intent is completely fulfilled, but in addiction some other related activity occurs
Other *other than*	The activity occurs, but not in the way intended
Fluctuation	The design intention is achieved only part of the time
Before/After	Usually used when studying sequential operations, this would indicate that a step is done out of sequence
Early/Late	Usually used when studying sequential operations, this would indicate that a step is started at the wrong time
Fast/Slower	The step is done/not done whit the right timing

5 Si definiscono le DEVIAZIONI
combinazioni PARAMETRI + PAROLE GUIDA

EXAMPLES OF DEVIATION

Process variables	NO, NOT, NONE	LESS, LOW, SHORT	MORE, HIGH, LONG	PART OF	AS WELL AS, ALSO	OTHER THAN	REVERSE
	GUIDE WORDS						
Flow	*No flow*	*Low rate*	*High rate*	*Missing feed*	*Additional feed*	*Wrog material*	*Backflow*
Pressure		*Low pressure*	*High pressure*				
Temperature		*Low temperature*	*High temperature*			*Phase change*	
Confinement	*Rupture*	*Leaks*		*Single barrier*	*Tritium diffusion*	*Relief path*	*In-leakage*
Level/ Capacity	*Empty*	*Low level*	*High level*				
Composition *Tritium*	*No tritium*	*Low tritium concentration*	*High tritium concentration*				
Reaction	*No reaction*			*Partial reaction*			
Power	*Low power failure*	*Short power failiure*					*Reverse polarity*

6 Si definisce col Cliente (e talvolta anche con l'Autorità di controllo) la composizione del TEAM (persone da invitare alle sessioni di lavoro).

7 Si definisce la matrice di rischio (frequenze - danni) di riferimento.

HAZOP TEAM

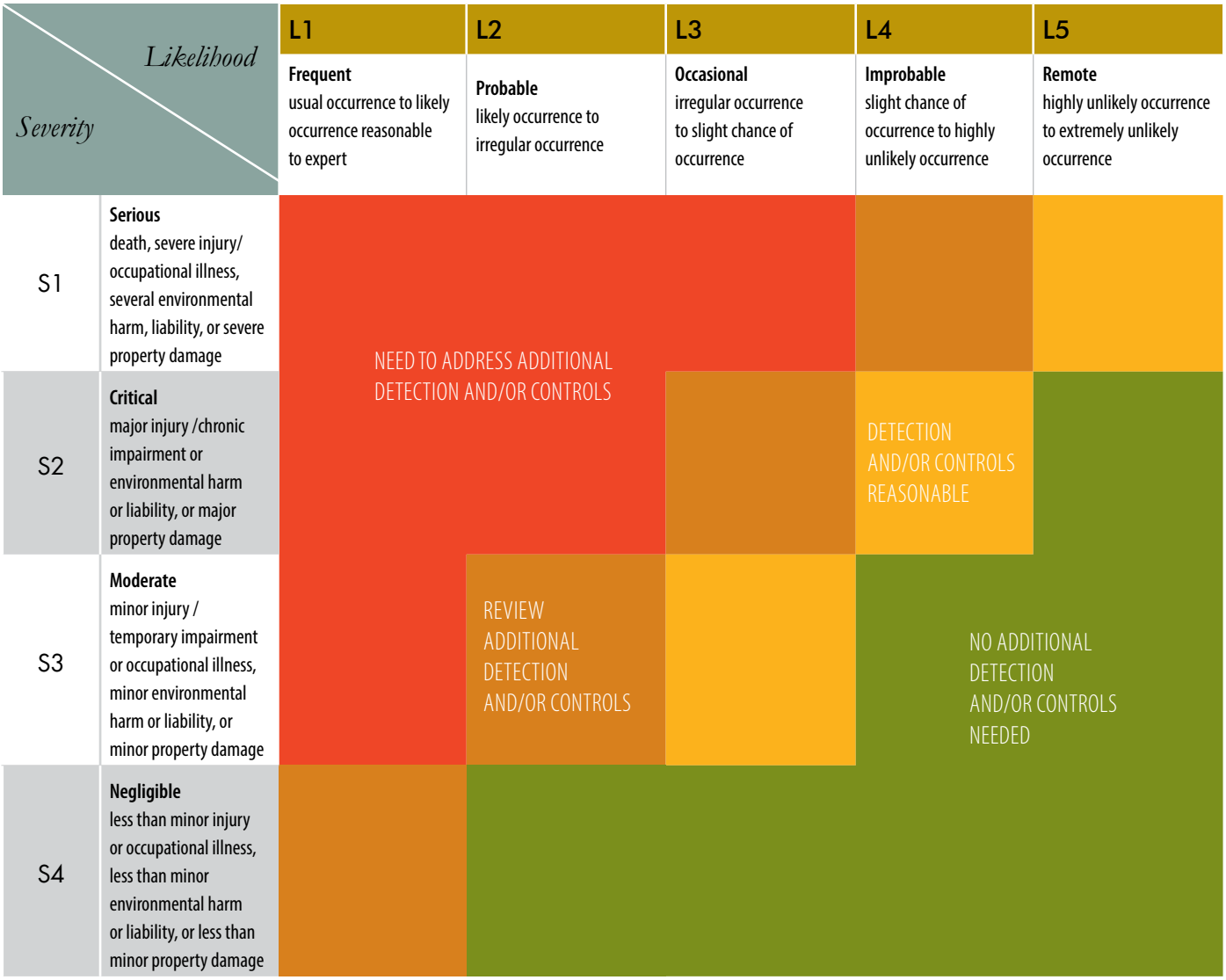
CORE MEMBERS

- *Team leader*
- *Secretary/ scribe*
- *Process design engineer*
- *Control/ electrical engineer*
- *Operators*
  **boiler suit not 3-piece suit **
  **most important! **
- *Project specialist*
  **not the project manager **
- *Mixing*
- *Absorb*
- *Corrode*
- *Erode*

CONSULTATION

- *Chemist*
- *Piping engineer*
- *Civil engineer*
- *Others*

	CONSEQUENCE				INCREASING PROBABILITY				
Severity	PEOPLE	ASSETS	ENVIRON-MENT	REPUTA-TION	A	B	C	D	E
					never heard of in EP industry	has occurred in EP industry	incident has occurred in Opco	happens several times per year in Opco	happens several times per year in location
0	*No injury*	*No damage*	*No effect*	*No impact*					
1	*Slight injury*	*Slight damage*	*Slight effect*	*Slight impact*					
2	*Minor injury*	*Minor damage temperature*	*Minor effect*	*Limited impact*					
3	*Major injury*	*Localised damage*	*Localised effect*	*Considerable*					
4	*Single fatality*	*Major damage*	*Major effect*	*National impact*					
5	*Multiple fatalities*	*Extensive damage concentration*	*Massive effect*	*International impact*					



8 I professionisti specialisti HAZOP guidano le analisi con il TEAM e registrano i risultati dell'analisi passo-passo e poi producono un "HAZOP Final Report" che ha come risultato principale un elenco dettagliato delle azioni di miglioramento dell'impianto. Una volta recepite queste azioni correttive, il progetto quindi lo si ritiene SICURO e AFFIDABILE (ovviamente con un rischio residuo ritenuto accettabile).

Il metodo HAZOP può essere utilizzato mediante ausilio di semplici spreadsheets tipo EXCEL oppure anche con software dedicati più o meno complessi. Gli esperti HAZOP non prediligono molto i software perché inevitabilmente inseriscono nell'analisi un fattore di rigidezza che limita il grado di libertà che può emergere delle discussioni dell'HAZOP Team.

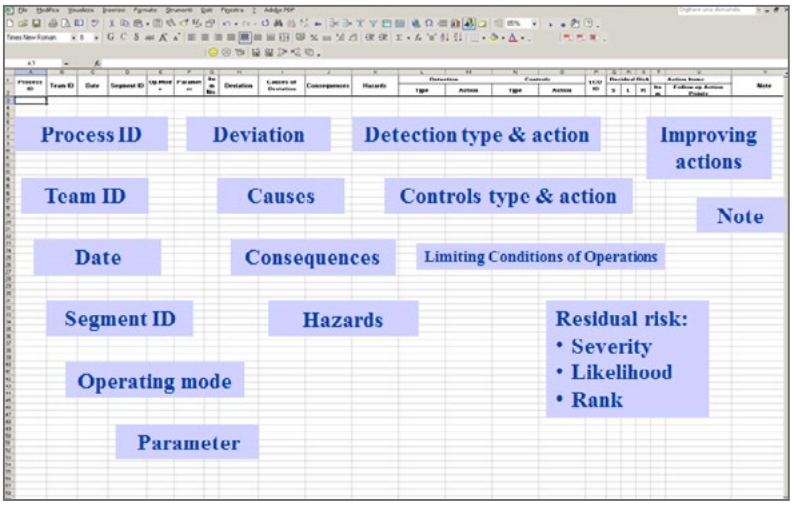
I CAMPI DI IMPIEGO

Il metodo HAZOP oggi è utilizzato come una procedura consueta per le valutazioni di sicurezza e operabilità in impianti o processi di medio-alto rischio, come:

- ***Nucleare (fissione e fusione, impianti prototipo e sperimentali)***
- ***Settore Oil & Gas (offshore e onshore) e petrolifero in genere***
- ***Impianti di processo e industriali di grandi dimensioni ad alto rischio (anche in regime Seveso)***
- ***Farmaceutico***
- ***Agroalimentare e agrochimico***
- ***Power plants (tradizionali e innovativi o energie alternative: eolico, idroelettrico, biomasse, ecc.)***
- ***Navale***
- ***Aeronautico ed elicotteristico***

HAZOP AUXILIARY SHEETS

HAZOP MAIN SHEET



Esempi di fogli di un software dedicato e nato specificatamente per analisi HAZOP

CONCLUSIONE

All'interno dell'ampio dominio dell'analisi di rischio industriale, senza dubbio il metodo HAZOP oltre che il più noto e applicato è anche quello più versatile e interessante in termini di identificazione delle possibili azioni migliorative e spesso anche portando a notevoli benefici economici, a causa dell'incrementata affidabilità e operabilità di impianto.

Ad oggi questa tecnica, nata negli anni '60 in Inghilterra e da sempre applicata come un MUST nei settore nucleare e Oil&Gas sta divenendo nota e sempre più apprezzata anche nei settori a minor rischio, specialmente negli impianti di produzione di energia perché permette di ottimizzare la Business Continuity e di minimizzare i fermi impianto non programmati.

> **Risulta molto ben applicabile alle più svariate tecnologie anche innovative o pionieristiche.**

MICHELANGELO COSTA

Ingegnere nucleare, si è occupato per oltre 10 anni di valutazioni di rischio in campo fusione nucleare in ambito internazionale. Ha svolto poi un'importante esperienza nel settore impiantistico dell'ingegneria civile ed attualmente riveste il ruolo di responsabile di tutte le attività di Fire Engineering e Risk Analysis di Techno srl.