Università degli Studi di Napoli Federico II

SCUOLA DI DOTTORATO

in

TECNOLOGIE E SISTEMI DI PRODUZIONE

Ciclo XXVII – triennio accademico 2012/2015

Dipartimento di Ingegneria Chimica dei Materiali e della Produzione Industriale

Tesi Di Dottorato

Dal Rischio alla Resilienza degli impianti industriali

applicati alla gestione dei sistemi socio - tecnologici

COORDINATORE

Ch.mo prof. ing. L. Carrino

TUTOR

Ch.ma Prof.ssa Ing. L.C. Santillo

CANDIDATO

ing. Mario Di Nardo

ANNO ACCADEMICO 2013 – 2014

Indice dei contenuti

Introduzione **7**

CAPITOLO I : DALLA SAFETY CULTURE AL RISK MANAGEMENT ... **14**

1.1 La Safety Culture *14*

1.2 Il Quantitative Risk Assessment *17*

1.3 Il Rischio nell'ottica della sicurezza industriale *18*

1.4 Il Risk Management in ambito Safety *19*

1.5 Gli approcci alla sicurezza *25*

1.5.1 L'approccio tradizionale 25
1.5.2 L'approccio moderno 26
1.5.3 Dynamic Sequential Accident Models 31
1.5.4 Process Hazard Prevention Accident Models (PHPAMs) 33

1.6 Il comportamento umano *35*

1.7 La sicurezza sui luoghi di lavoro e i riferimenti normativi in Italia *36*

1.7.1 Il D.P.R n.151 del 2011 37
1.7.2 Protezione da atmosfere esplosive: il rischio ATEX 37

CAPITOLO II : LA RESILIENZA **39**

2.1 La Resilienza: definizioni *39*

2.2 Applicazione del concetto di Resilienza nelle diverse discipline *42*

2.2.1 La Resilienza nei sistemi ecologici 42
2.2.2 La Resilienza negli ecosistemi industriali 42
2.2.3 La Resilienza applicata alle reti ed alla Supply Chain 43
2.2.4 La Resilienza applicata alla sicurezza 45

2.3 Principi e fattori contributivi della Resilience Engineering *48*

2.4 Approcci qualitativi e quantitativi della Resilienza *54*

2.5 Utilizzo dei modelli simulativi per la sicurezza degli impianti industriali e la RE *67*

2.5.1 La System Dynamics 69

CAPITOLO III: L' APPROCCIO SIMULATIVO PER SUPPORTARE LA VALUTAZIONE DEL RISCHIO **77**

3.1 Cenni sulle metodologie di risk assessment maggiormente utilizzate *77*

3.2 La metodologia LOPA *79*

3.3 Approccio metodologico 82

3.4 Costruzione della CLD 83

3.5 L'azienda ed il processo produttivo dello stampaggio plastico 87

3.6 Applicazione della tecnica HazOp 88

3.7 GLI SCENARI INCIDENTALI 95

3.7.1 Primo scenario incidentale 95

Rottura del circuito oleodinamico per raggiungimento della pressione limite e fuoriuscita olio a elevata pressione e temperatura 95

3.7.2 Secondo scenario incidentale 100

Rottura del sistema di raffreddamento stampo e fuoriuscita di materiale ad elevata temperatura 100

3.7.3 Terzo scenario incidentale 101

Esplosione nel sistema di alimentazione 101

3.8 Commento all'applicazione della tecnica LOPA 105

3.9 Costruzione del modello simulativo 108

3.10 Considerazioni analitiche sul modello simulativo 118

3.11 Conclusioni 119

CAPITOLO IV 121

LA RESILIENZA NEGLI IMPIANTI INDUSTRIALI MEDIANTE IL SUPPORTO DELLA SYSTEM DYNAMICS 121

4.1 Dal rischio alla Resilienza 121

4.2 Il nuovo modello "RESILIENTE" 125

4.3 La scelta del Caso studio 127

4.4 Breve descrizione del processo produttivo 128

4.5 Il modello in Powersim e i risultati delle simulazioni 129

4.6 Ulteriori contributi alla sicurezza ed alla Resilienza : il fattore umano 132

4.7 Risultati preliminari 133

4.8 Framework dell'analisi della human reliability 134

4.8.1 Modello cognitivo e tassonomia 135

4.9 Metodologie e raccolta dati 137

4.10 Human Performance: fattori di forma /SHAPING FACTORS 138

4.11 Applicazione della System Dynamics all' HRA 139

4.12 Causal Loop Diagrams (CLD) dell'errore umano 140

4.13 Implementazione della Causal Loop Diagram 145

4.14 Possibili scenari futuri 147

Conclusioni 148

BIBLIOGRAFIA 150

Indice delle figure

Figura 1 ISO 31000: Risk Management overview [16]. **20**
Figura 2 Swiss Cheese Model of Defences **22**
Figura 3 Visione gerarchica di un modello socio tecncico [24]. **27**
Figura 4 Off-shore oil and gas prevention accident [2]. **34**
Figura 5 Fault Tree nel modello Off-shore oil and gas prevention [2]. **34**
Figura 6 Event Tree nel modello Off-shore oil and gas prevention [43]. **35**
Figura 7 Transizione dello stato nel sistema della Resilienza **60**
Figura 8 Evoluzione dello stato di un sistema resiliente in seguito ad una perturbazione [66]. **61**
Figura 9 Resilience triangle [70]. **64**
Figura 10 Resilience principles [73]. **65**
Figura 11 Esempio di Causal Loop Diagram relativo all'adozione di un nuovo prodotto **71**
Figura 12 Esempio di Balancing Loop (regolazione della temperatura) e rappresentazione della corrispondente evoluzione del sistema [79]. **72**
Figura 13 Esempio di Reinforcing Loop (crescita del conto bancario) e rappresentazione della corrispondente evoluzione del sistema [79]. **73**
Figura 14 Esempio di Reinforcing and Balancing Loop con delay. **74**
Figura 15 Un esempio di System Archetype: "Limits to growth" [80]. **74**
Figura 16 Esempio di rappresentazione delle variabili in uno Stock and Flow Diagram. **76**
Figura 17 Costruzione della CLD **84**
Figura 18 Interpretazione grafica della tecnica LOPA [19] **86**
Figura 19 Il modello simulativo mediante il software Powersim **109**
Figura 20 Modello simulativo **110**
Figura 21 Interfaccia utente del modello simulativo, configurazione 1 ..... **111**
Figura 22 Interfaccia utente del modello simulativo, configurazione 2 ..... **112**
Figura 23 Confronto tra modelli con PFD constante e PFD funzione del tempo **115**
Figura 24 Interfaccia utente, ipotesi di ageing delle valvole **116**
Figura 25 La Resilienza : il Modello organizzativo **125**
Figura 26 Casual Loop Diagram: Modello Proposto **126**
Figura 27 Mappa del rischio **127**
Figura 28 Schema di impianto **129**
Figura 29 Modello simulativo **130**
Figura 30 Modello di Rasmussen's skill-rule-knowledge [108] **136**
Figura 31 Casual Loop Diagram **140**
Figura 32 Casual effect diagram for human performance model **143**
Figura 33 Causal Loop Diagram applied to Case Study **144**
Figura 34 CLD implementata **146**

Indice delle tabelle

Tabella 1 Safety Integrity Levels 80
Tabella 2 Nodi e parametri dell'analisi HazOp 89
Tabella 3 Analisi HazOp, tabella riassuntiva 94
Tabella 4 Tecnica LOPA, probabilità scenario incidentale 98
Tabella 5 Event severity, LOPA 98
Tabella 6 Decision Table, LOPA 99
Tabella 7 Typical Protection Layer (Prevention & Mitigation) PFDs 103
Tabella 8 Tabella riassuntiva LOPA 104
Tabella 9 Confronto frequenze di accadimento, prima e dopo la simulazione 113
Tabella 10 Frequenze dei top events e variazioni percentuali, improved model e ageing model 117
Tabella 11 Failure Rate used for the SD reported in Figure 5. SIS = Safety Instrumented System 131
Tabella 12 Resiliens Indicator results 132

Introduzione

L'evoluzione tecnologica, l'analisi degli ambienti di lavoro e la presa di coscienza da parte dei lavoratori del diritto a vivere una situazione lavorativa "sicura" hanno portato, negli ultimi decenni, ad un decremento di incidenti dovuti a guasti di natura tecnica grazie a ridondanze e protezioni, che hanno reso i sistemi sempre più affidabili. Tuttavia non è possibile parlare di affidabilità di un sistema senza portare in conto il tasso di guasto di tutti i suoi componenti, in particolare il componente "uomo", il cui tasso di guasto/errore va a influire in maniera significativa su quello complessivo del sistema in cui è inserito. Questo ha reso evidente, sia a livello statistico sia in termini di gravità delle conseguenze, la necessità di considerare il contributo del fattore umano nelle dinamiche degli incidenti.

Tale necessità è avvalorata dai dati che si riscontrano dalla realtà odierna.

Le stime concordano nell'attribuire agli errori commessi dall'uomo la responsabilità nel 60-80% degli incidenti mentre solo per la restante parte le cause sono imputabili a carenze tecniche. Pertanto, al fine di assicurare un'efficace prevenzione degli eventi dannosi, il processo di valutazione dei rischi non può ignorare il ruolo dell'uomo nella dinamica degli eventi incidentali e quindi la gravità delle conseguenze derivabili.

Data l'importanza sociale ed economica che riveste la sicurezza nel contesto attuale, si è deciso di effettuare un percorso di ricerca quanto più completo, approfondendo tutti gli aspetti che si è ritenuto opportuno, in modo da presentare dei risultati non solo originali, ma che potessero avere fondamenta teoriche solide. Per tale motivo, il lavoro di ricerca proposto ha preso origine dall'analisi dell'evoluzione della sicurezza degli impianti industriali negli ultimi anni (Capitolo I), partendo dal concetto di Safety Culture.

La complessità degli incidenti industriali che riflette le criticità dei moderni sistemi tecnologico-produttivi, le nuove interazioni stabilite tra uomo-macchina-ambiente e la mancata percezione dell'importanza di una cultura della sicurezza costantemente alimentata e arricchita, hanno reso evidenti i limiti dell'approccio alla gestione della sicurezza (Safety Management) comunemente intesa ed applicata.

Tale gestione applicata agli impianti di processo (Process Safety Management) è definita come "l'applicazione dei sistemi di gestione per l'identificazione, la comprensione e il controllo dei pericoli di un processo al fine di evitare infortuni e incidenti ad esso correlati"; alternativamente, esso può essere definita come un processo continuo, che coinvolge ciascun manager, dipendente e lavoratore a contratto, orientato a minimizzare le deviazioni progettuali ed operative e a mantenere il processo entro limiti di sicurezza prestabiliti [1].

Il Safety Management è, quindi, l'insieme dei processi finalizzati ad individuare, valutare e classificare i rischi per la sicurezza in base alle loro priorità, a cui si affianca, parallelamente, l'impiego di risorse – coordinato ed economico - avente, da un lato, lo scopo di minimizzare e monitorare la frequenza e le possibili conseguenze di eventi indesiderati e, dall'altro, quello di massimizzare la realizzazione delle opportunità.

L'evoluzione delle variabili che figurano nei processi d'identificazione, valutazione, pianificazione/implementazione di misure correttive e controllo, quali, ad esempio, lo sviluppo di nuovi fattori di rischio, gli aggiornamenti delle loro definizioni e del loro livello di accettabilità, contrasta con la loro caratteristica di staticità, la quale è stata considerata, negli approcci tradizionali alla sicurezza e nella rappresentazione dei fattori di rischio, come ipotesi alla base, per una più agevole gestione delle informazioni da trattare.

Di conseguenza, al fine di migliorare l'efficienza e l'efficacia dell'intero processo di gestione, nasce l'esigenza di adottare innanzitutto una metodologia in grado di risolvere le criticità introdotte, estendendo l'approccio "classico" e proponendo, di fatto, una nuova visione della gestione del rischio. Constatata la complessità dei moderni sistemi socio-tecnici, in particolare degli impianti di processo, è necessario utilizzare un approccio sistemico che permetta di controllarne lo stato in qualsiasi momento, attraverso la predisposizione di strumenti che consentano l'aggiornamento delle variabili del processo, qualora queste subiscano variazioni.

Partendo perciò da tale necessità, si indaga come, attraverso successive evoluzioni, si è giunti al concetto di Resilience Engineering (RE) applicato alla sicurezza degli impianti industriali.

Tale analisi è illustrata nel Capitolo II, nel quale si descriverà, inoltre, il concetto di "Resilienza".

L'applicazione di tale concetto ai sistemi industriali, in ambito della sicurezza, risulta essere un nodo centrale del lavoro di ricerca. Pertanto si è ritenuto necessario effettuare una sua descrizione esaustiva, in modo da avere le necessarie basi al fine di conseguire dei risultati utili e innovativi.

La Resilienza si può definire come una caratteristica intrinseca di un materiale, corpo, individuo o sistema che ne misura la sua capacità a resistere e a riprendersi in seguito ad un evento avverso. Ai fini di tale lavoro, partendo da tale definizione, la Resilienza può essere definita come, nell'ambito della sicurezza degli impianti industriali [2] l'attitudine del sistema a ripristinare una configurazione operativa sicura, in seguito ad un malfunzionamento o ad una perturbazione delle sue condizioni di funzionamento nominali, come può accadere nel caso di un evento incidentale.

Il percorso che viene sviluppato nel presente elaborato permetterà, quindi di applicare la RE (Resilience Engineering) alla gestione della sicurezza in ambienti socio-tecnici e pericolosi connettendola direttamente al concetto di Rischio. La gestione del rischio, in particolare, ha il suo fulcro nell'identificazione e nella riduzione dei fattori di rischio; in tale senso, la RE si pone l'obiettivo di aumentare la capacità del sistema di reagire al fine di essere intrinsecamente sicuro, compensando anche le carenze di un sistema, che possono derivare da una cattiva progettazione dei processi o da una scarsa capacità di gestione.

Nell'ottica della RE, il concetto di sicurezza intesa come semplice assenza di rischi viene esteso: *Safety as the ability to succeed under varying conditions*. Emerge quindi l'idea che la sicurezza non sia più un'entità statica, caratteristica del sistema in esame, ma sia il frutto di un processo dinamico a cui prende parte il sistema stesso. Di conseguenza, non ci si limita più ad analizzare soltanto ciò che può "andare male":

la comprensione di come funziona un sistema socio-tecnico diventa condizione necessaria per capire come esso possa fallire, dal momento che successi e insuccessi sono conseguenze possibili dello stesso processo.

L'approccio sistemico diventa utile per gestire la complessità degli impianti industriali. In particolare un'analisi dettagliata degli eventi incidentali e delle componenti che aumentano il rischio ha necessitato di strumenti di supporto alle decisioni per analizzare l'evoluzione nel tempo del fattore di Rischio prima e della misura della Resilienza dopo.

A tal fine possibile, la metodologia richiesta deve permettere uno screening olistico del sistema in esame: nel ricercare le cause di un generico evento incidentale, non è sufficiente limitarsi a considerare soltanto ciò che è strettamente correlato ad esso, e quindi tangibile e facilmente intuibile, bensì il campo di indagine deve essere ampliato fino a comprendere l'insieme dei fattori, sia interni che esterni, con cui il sistema si trova ad interagire nel corso del suo normale funzionamento. Attraverso gli strumenti della System Dynamics, SD, (Causal Loop Diagram – Stock and Flow Diagram), che, implementando i principi di funzionamento dei sistemi dinamici, ne consentono la rappresentazione e la simulazione, è possibile evidenziare il tipo di relazione e le influenze reciproche esistenti tra gli elementi di una specifica realtà di interesse.

Si presenteranno quindi, brevemente, la filosofia della System Dynamics e gli strumenti metodologi su cui si fonda (Causal Loop Diagram – Stock and flow diagram). In particolare si procede all'analisi delle principali nozioni che permetteranno, in seguito, la descrizione dei diagrammi causali sviluppati per realizzare un modello rappresentativo dell'industria di processo.

L'analisi di studio teorico preliminare troverà una sua applicazione nel Terzo Capitolo attraverso l'impiego degli strumenti offerti dalla metodologia della System Dynamics; inoltre il nuovo approccio sistemico sarà applicato come strumento di supporto alle decisioni al Quantitative Risk Assessment (QRA) introdotto nel primo capitolo.

Il Quantitative Risk Assessment è stato svolto in modo tale da valutare l'evoluzione del rischio (e della sua gestione al fine di attuare le corrette misure di prevenzione) nel tempo in un'azienda di stampaggio plastico, considerando i possibili scenari incidentali che caratterizzano tale realtà produttiva. I risultati di tale studio sono stati oggetto di pubblicazione nel lavoro [80].

In questa sede, l'applicazione al caso reale verrà sinteticamente descritta, focalizzandosi principalmente sull'evoluzione che il processo di analisi del rischio dovrebbe avere in tutte le realtà produttive, illustrando le varie metodologie e i vari strumenti impiegati, descrivendo, per ognuno di essi, pregi e difetti, e l'utilità di impiegare tali strumenti in un processo sistematico di analisi del rischio.

Argomento del Quarto Capitolo è la presentazione di un modello organizzativo generale della Resilienza. Nel modello presentato, la Resilienza diventa fulcro e misura della sicurezza di un sistema [93].

Approfondendo l'analisi della Resilienza, si è potuto constatare come essa sia fortemente legata ai fattori umani, alla teoria del controllo ed all'ingegneria della sicurezza. Proprio da tale considerazione nasce la necessità di comprendere come le persone riescano ad adattarsi ad un ambiente ricco di pericoli ed insidie, e, in altre parole, in che modo le persone facenti parte di un sistema, siano in grado di presentare delle caratteristiche "resilienti", tali da modificare la Resilienza stessa del sistema.

Il risultato che verrà presentato descriverà come il fattore umano incida sul Rischio il quale è connesso alla Resilienza, sulla base del modello che verrà, per l'appunto, descritto nel quarto Capitolo. Anche tale modello verrà presentato in maniera sintetica, focalizzandosi sugli aspetti utili per descrivere le sue evoluzioni nonchè i contributi che esso può apportare all'analisi della Resilience Egineering nell'ambito dello studio della sicurezza all'interno degli impianti industriali [94].

Al termine del capitolo si è proposto quindi un'implementazione dell'analisi effettuata, ponendo le basi per ulteriori e futuri lavori di ricerca.

L'obiettivo futuro che ci si vuole prefiggere è quello di realizzare un modello completo che simuli l'evoluzione di un impianto di processo attraverso cui sia

possibile evidenziare la rete di interazioni causali che determina la probabilità di un evento incidentale e quindi i suoi possibili scenari, dalla cui analisi ricavare la Resilienza del sistema.

RINGRAZIAMENTI

Il percorso di formazione del dottorato di ricerca risulta, ad oggi, il più importante e riconosciuto in tutta la UE. Durante questo percorso ho avuto modo di conoscere persone eccezionali, in primis la prof.ssa ing. L.C. Santillo, che mi ha dato la possibilità ed il tempo di formarmi, incoraggiandomi sempre e che ha permesso, grazie alla sua lungimiranza, la mia affermazione professionale. A lei va il mio più grande grazie. Ringrazio l'ing. Mosè Gallo che non mi ha mai fatto mancare la sua amicizia, sempre pungolo per un miglioramento continuo. Ringrazio inoltre la cara amica ing. Marianna Madonna per il supporto ed il contributo datomi nella stesura di questo lavoro.

Un grazie alla mia famiglia, ai miei genitori, che da sempre ed in particolare, nel mio "Annus Horribilis", mi hanno sempre sostenuto ed incoraggiato nelle difficoltà.

Un particolare grazie a mia sorella Rosaria, vera guida e consigliera in ogni momento, una vera milestone della mia vita.

Infine un grazie a chi è entrato nella mia vita e ha creduto in me giorno dopo giorno, non "contando", diventando oggi giorno sempre più importante.

CAPITOLO I: DALLA SAFETY CULTURE AL RISK MANAGEMENT

Negli ultimi anni, è stato possibile riscontrare, sia nella società comune che nel mondo specifico della ricerca, come si sia sviluppato ed evoluto il concetto di "cultura della sicurezza" negli ambienti lavorativi e non. Tale sviluppo può essere inteso sia come risposta alle esigenze dei lavoratori, sia come risposta a grandi eventi che hanno interessato la storia contemporanea, come ad esempio il disastro di Chernobyl.

Nella trattazione che segue si effettua un excursus sulla cultura della sicurezza. Tale trattazione diventa propedeutica e necessaria nell'analisi e nella gestione dei rischi in contesti organizzativi.

L'individuazione dei fattori di rischio, la valutazione della probabilità di accadimento e le possibili conseguenze risultano cruciali per la corretta gestione dello stesso. In particolare il ruolo della gestione del rischio diventa delicato per ogni evento singolo o successione di eventi imprevisti che può arrecare danno a persone, a beni materiali o all'ambiente circostante. Diventa quindi importante la tipologia di approccio alla sicurezza che negli ultimi anni è divenuta sempre più dinamica ai fini della valutazione del fenomeno incidentale e quindi della gestione della sicurezza industriale.

1.1 La Safety Culture

Il concetto di Safety Culture spesso viene presentato separatamente dalle altre caratteristiche di un'organizzazione aziendale, quali uno scheduling del lavoro, la tecnologia da utilizzare, una strategia di business oppure una decisione finanziaria.
Reiman e Oedewald [3] affermano che questa separazione concettuale della Safety Culture consente di riferirsi solo a fattori che sono chiaramente connessi alla Safety,

quali le sue attitudini e la sua valutazione. Sebbene sia stato utilizzato ampiamente per molti anni, il concetto di Safety Culture non è ancora molto chiaro.

Negli ultimi quindici anni sono stati presentati numerosi studi a riguardo ed in letteratura esistono molte sue definizioni con relativi esempi e campi di applicazione. A riguardo, studi pionieristici, come quello dell' International Atomic Energy Agency per ciò che riguardava un report sull'International Nuclear Safety Advisory Group (INSAG-4) [4], hanno sviluppato, nel dettaglio, il concetto di Safety Culture definendola come quell'insieme di caratteristiche ed attitudini insite in un'organizzazione e negli individui che la compongono, in grado di stabilire che i problemi di sicurezza degli impianti nucleari ricevano un livello di attenzione direttamente proporzionale al loro grado di pericolosità.

Tale definizione mette in evidenza due punti cruciali:

- La Safety Culture non è solo una buona attitudine ma è anche un vero e proprio "diktat" imposto dal management aziendale;
- Una buona politica di Safety Culture significa assicurare la massima priorità alla sicurezza.

Nonostante tale report metta in evidenza i problemi di sicurezza, nell'ambito degli impianti nucleari, e le relative azioni preventive da intraprendere, sia a livello organizzativo che individuale, esso omette il collegamento tra la Safety Culture e gli indicatori di Safety Performance.

Secondo l'Advisory Committee on the Safety of Nuclear Installations (ACSNI) [5], la Safety Culture di un'organizzazione è il prodotto di valori di gruppo e di valori individuali, attitudini, competenze e modelli di comportamento che determinano il conseguimento di un soddisfacente livello di sicurezza per l'organizzazione stessa.

Il principale difetto mostrato in molti dei modelli di Safety Culture, proposti in letteratura, è stato quello di valutare gli stessi al di fuori dell'organizzazione culturale. Secondo Schein [6], l'organizzazione culturale è strettamente radicata alle attività dei singoli individui che la compongono ed alle loro relazioni. Per questo motivo anche i modelli di Safety Culture devono essere visti come dei sistemi socio-tecnici. Sulla scia di quanto detto, gli studiosi Grote e Kunzler [7] inseriscono la Safety Culture nella struttura generale di un'organizzazione.

Geller [8], invece, ha presentato un modello che annoverava al suo interno i fattori dinamici ed interattivi costituiti dalle persone, dai loro comportamenti e dal contesto ambientale. In questo studio viene proposto un modello con dieci principi che avrebbero garantito il raggiungimento di una "total safety culture". Cooper [9] delinea la cultura organizzativa come prodotto delle interazioni tra persone (psicologico), lavoro (comportamentale) ed organizzazione (situazionale).

Egli propone un modello di Safety Culture nel quale le attitudini e le percezioni possono essere valutate attraverso questionari di "Safety Climate" ed inoltre, sia i comportamenti presenti che le azioni future, possono essere valutati con sistemi di audit ed ispezioni, che siano in grado di attestare l'effettivo livello di sicurezza di un determinato sistema organizzativo. Glendon, Litherland [10] e Neal [11] hanno esaminato la relazione tra Safety Culture, Safety Climate e Safety Performance. Gli aspetti situazionali della Safety culture possono essere visti, nella struttura organizzativa, attraverso le politiche, le procedure di lavoro ed i sistemi di gestione.

Gli aspetti comportamentali della Safety Culture, invece, possono essere misurati con delle osservazioni, dei report e con la valutazione dei risultati ottenuti.

A conferma di quanto affermato, Kennedy e Kirwan [12] hanno sviluppato il Safety Culture and Operability (SCHAZOP), approccio che si focalizza su molteplici aspetti di pratiche riguardanti il safety management, includendo le differenti aree aziendali e proponendo un approccio di tipo olistico alla Safety. Richter e Koch [13] sostengono che la Safety Culture è in continua fase di sviluppo e soprattutto si deve confrontare sia con gli aspetti interni che con quelli esterni che gravitano intorno ad una determinata realtà organizzativa. Secondo Mohamed [14] un soddisfacente livello di sicurezza è direttamente proporzionale alle capacità del top management, che quindi, oltre a considerare la Safety Culture una priorità, deve trasmettere la stessa filosofia ai dipendenti con un approccio top-down.

In quanto sopra argomentato, il concetto di *Safety Culture* diventa sintesi di comportamenti ed attitudini per una corretta gestione proattiva della sicurezza e non può che implicare tutti gli aspetti aziendali.

1.2 Il Quantitative Risk Assessment

Un ruolo cruciale nel gestire la sicurezza di un impianto di processo è svolto dal Quantitative Risk Assessment (QRA), procedura sistemica che permette l'individuazione dei fattori di rischio (*Hazards Identification*), la valutazione della probabilità di accadimento (*Hazards Assessment*) e le possibili conseguenze implicate (*Risk Estimation*). Originariamente sviluppato per applicazioni specifiche nel settore nucleare, il suo utilizzo è stato successivamente esteso all'industria di processo con risultati soddisfacenti.

Nonostante le principali tecniche di assessment costituiscano un valido strumento per l'analisi degli incidenti, in special modo i rilevanti, il QRA non è in grado di esprimere la dipendenza del rischio dal tempo, restituendo un risultato statico: la procedura non è quindi in grado di apprendere dalla storia del processo. Oggigiorno, la soluzione a tale limite è ricercata in un approccio dinamico al Risk Management che permetta di aggiornare sistematicamente le informazioni sul rischio, tenendo conto delle nuove conoscenze e costituendo un valido strumento di supporto alle decisioni.

Si vuole qui realizzare una panoramica sullo stato dell'arte dei principali approcci al Risk Management nell'ambito della sicurezza degli impianti industriali, attraverso lo sviluppo dei seguenti punti:

- Introduzione al Safety Management;
- Processi e attività fondamentali in cui esso è articolato;
- Approcci e principali tecniche impiegate nell'Accident Analysis e nel Risk Assessment;
- Individuazione di punti di forza e limiti per ciascuna delle metodologie proposte.

1.3 Il Rischio nell'ottica della sicurezza industriale

Nel linguaggio comune, la distinzione tra "rischio" e "pericolo" (hazard) non è così netta, a tal punto che essi sono spesso considerati sinonimi: in realtà, vi è una sostanziale differenza di tipo concettuale tra i due termini.

In particolare, il pericolo designa il potenziale "danno" che può derivare dalle proprietà (chimiche, fisiche, biologiche, ecc.) o dalle caratteristiche possedute da una particolare sostanza, sistema, componente (ad es. un investimento) o processo. Per tali ragioni esso viene spesso indicato come fonte di rischio: d'altra parte quest'ultimo, invece, si configura come la possibilità che qualcuno o qualcosa possa subire un'alterazione in virtù dell'esistenza di un certo pericolo.

Essendo il Rischio un argomento dalla portata molto vasta che investe diversi ambiti culturali, è possibile riscontrare, nella letteratura scientifica e nei vari standard proposti sui sistemi di gestione, diverse definizioni, tutte accomunate dalla presenza di tre elementi:

1. Fattori di rischio (*Hazards*);
2. Entità delle conseguenze (*Consequence Seriousness*);
3. Frequenza di uno specifico scenario (*Frequency of a specific scenario*).

Quindi, affinché sussista un rischio è necessario che si manifesti un certo evento, a seconda del cui impatto ci si riferisce ad un'opportunità, ad una perdita o alla presenza di incertezza: gli eventi con sole conseguenze negative vengono indicati come *pure risks*: in genere per essi viene fissata una soglia di tollerabilità e li si gestisce in modo tale che rientrino in tale soglia; l'incertezza in genere si riferisce al tipo di output: situazioni tipiche del project management sono delivery on time oppure degli investimenti in cui l'azione è rischiosa ma viene compiuta nella speranza di un ottenere un ritorno (*risk opportunity*). Kaplan [15] associa al rischio tre aspetti (*Risk Triplet*):

1. *Hazard (disruption)*: evento o insieme di eventi, il cui verificarsi è in grado di alterare il normale funzionamento del sistema;

2. *Exposure*: dipende sia dalle proprietà del processo che scatenano l'evento di danno (descritte in termini probabilistici) sia dal comportamento del sistema che vi è soggetto (descritto in termini deterministici o probabilistici).
3. *Vulnerability*: è funzione della probabilità del guasto del sistema (condizionata) e delle conseguenze dell'evento che si è verificato; in altri termini, tale grandezza non dipende solo dall'esposizione del sistema al particolare evento di rischio ma anche da quanto il suo funzionamento sia stato compromesso.

1.4 Il Risk Management in ambito Safety

Ogni evento singolo o successione di eventi imprevisti può arrecare danno a persone, a beni materiali o all'ambiente circostante: ne risulta che, qualunque sia il contesto a cui ci riferisce, il rischio rappresenta una componente che è sempre presente.

Di conseguenza, si rende necessario, a livello organizzativo:

1. individuare i fattori di rischio attraverso delle procedure sistemiche;
2. valutarli attraverso metodi quantitativi;
3. pianificare e implementare un insieme di misure preventive e protettive, volte a garantire l'incolumità di persone, beni ed ambiente, nonché evitare di incorrere in perdite economico-produttive qualora si verificasse l'evento indesiderato.

L'ISO 31000:2009 è uno standard internazionale che fornisce le linee guida e i principi per una gestione del rischio efficace e sistemica, indipendentemente dal settore, dal tipo di industria e dalla categoria di rischio. Precedentemente, Australia e Nuova Zelanda avevano sviluppato lo standard AS/NZS 4360:1999 – rivisto e modificato nel 4360:2004 primo tentativo al mondo di formalizzare i processi e gli scopi del Risk Management attraverso uno standard: nel 2005, la ISO cominciò a lavorare alla stesura dello standard 31000, partendo da quello australiano come riferimento, pubblicato poi nel 2009. Integrano la ISO 31000 gli standard ISO/IEC

31010:2009 (Risk Assessment techniques) e ISO guide 73:2009 (Risk Mangement vocabulary).

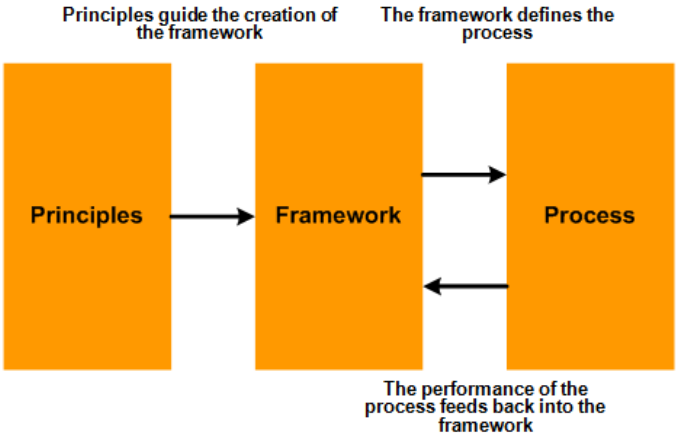

Figura 1 ISO 31000: Risk Management overview [16].

Configurandosi come strumento in grado di sopperire alle necessità introdotte, il Risk Management costituisce un approccio integrato alla valutazione, al controllo e al monitoraggio di eventi che possono impedire il raggiungimento di obiettivi prefissati, alterandone il risultato o incrementandone l'incertezza; in casi rari, tali eventi configurano delle opportunità [19]. Esso risulta, quindi, essere l'insieme di attività che un'organizzazione intraprende volontariamente per comprendere e ridurre tali effetti: in particolare, una gestione efficace consente di realizzare tali processi in maniera efficiente e tale da dimostrare i miglioramenti conseguiti dall'organizzazione, così da poter essere ripetuti [15].

Tale approccio non è isolato ma si colloca all'interno di un framework, ovvero un insieme di componenti che costituiscono le fondamenta (politiche, obiettivi, commitment) e le disposizioni organizzative (piani, relazioni, responsabilità, risorse, processi e attività) per la progettazione, l'implementazione, il monitoraggio, il controllo e il miglioramento continuo dei processi di Risk Management all'interno dell'organizzazione.

I processi di Risk Management costituiscono la sistematica applicazione delle politiche di gestione, delle procedure e delle pratiche alle attività di comunicazione, consultazione, identificazione, analisi, valutazione, trattamento, monitoraggio e controllo del rischio. In particolare, si hanno [17]:

1) *Identification*: Consiste nell'individuazione dei pericoli e dei fattori di rischio, che, potenzialmente, possono contribuire al *Top Event*, evento dalle conseguenze gravi - o gravissime – da scongiurare ad ogni costo. Tale fase costituisce, quindi, il presupposto per l'effettiva gestione del rischio: una volta che i rischi sono stati correttamente identificati, conformemente a quanto stabilito dalle disposizioni di legge, dalla regolamentazione e dagli standard, si procede alla loro quantificazione.

2) *Assessment and Evaluation*: In tale fase, è necessaria la conoscenza di due fattori: la probabilità che l'evento indesiderato si verifichi e le sue conseguenze in tal caso; condizionatamente al verificarsi del pericolo, tali conseguenze possono essere caratterizzate da una distribuzione di probabilità circa la loro gravità. Per ogni fattore di rischio precedentemente individuato si va quindi a determinare la potenziale pericolosità e si associa un indice di priorità.

3) *Control*: La classificazione dei rischi in base alle priorità consente di pianificare insiemi di misure atte ad eliminarli, ridurli o semplicemente monitorarli. E' bene specificare che quest'ultima fase non si esaurisce con la programmazione delle azioni correttive, ma comprende anche la loro implementazione, da realizzarsi attraverso l'aggiornamento periodico, la regolamentazione, il monitoraggio, il controllo e la supervisione.

Reason [17] illustra le condizioni in cui si viene a determinare un incidente all'interno di sistemi tecnologici complessi, partendo dal presupposto secondo cui non esiste un'unica causa bensì un'interconnessione tra più fattori, ciascuno dei quali afferisce a uno specifico livello del sistema. Per la prima volta, vengono introdotti nell'analisi

gli aspetti organizzativi (procedure, decisioni manageriali) e le misure di sicurezza (barriere protettive), mostrando come essi possano fallire.

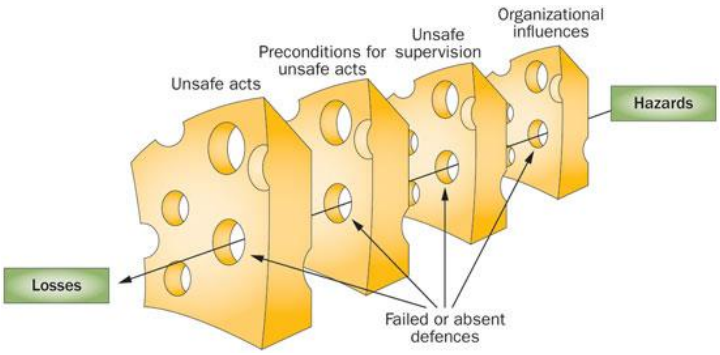

Figura 2 Swiss Cheese Model of Defences

In un sistema tecnologico è possibile individuare una serie di strati protettivi (*layers of defence*) raggruppabili in tre categorie: i sistemi ingegnerizzati (dispositivi di controllo automatico, sistemi di blocco, misure di spegnimento, barriere automatiche, ecc.), le misure dipendenti dall'intervento umano (ad es, sistemi di controllo manuale) e, infine, le procedure e i controlli organizzativi.

Come si può osservare in figura, Reason descrive la dinamica di un incidente come propagazione di un insieme di falle che coinvolgono i vari strati difensivi all'interno del sistema. La formazione di tali brecce può essere riconducibile a diversi fattori:

1. Usura e deterioramento delle barriere fisiche;
2. Modifiche o riprogettazioni del sistema;
3. Violazioni procedurali;
4. Errori;
5. Rimozione delle barriere in fase di test o di manutenzione.

La presenza di falle all'interno di un singolo strato non è sufficiente a configurare una condizione di rischio: il problema si pone quando l'insieme di più fori, relativi a diversi livelli, delinea una traiettoria che rende possibile la transizione Hazards - Losses.

In particolare, nel modello di Reason viene posto l'accento sui concetti di *Active Failures* e *Latent Conditions*.

Gli Active Failures sono errori che riguardano persone a contatto diretto con il sistema: si definisce errore quel fattore, non imputabile al caso, che determina il fallimento di una sequenza pianificata di attività - fisiche o mentali - impedendo il raggiungimento degli obiettivi previsti. In generale, si è soliti distinguere tra le seguenti tipologie di errori:

- **Skill based errors**: si verificano quando l'azione non viene eseguita come pianificato. In particolare, possono verificarsi: 1) omissioni involontarie (Slips) quando l'errore si manifesta nello svolgimento di un task abitudinario a causa di un imprevisto o di un'interferenza esterna; 2) distrazioni e interruzioni (Lapse).

- **Errori procedurali (Rule based mistakes)**: L'errore può scaturire da una percezione sbagliata del problema che determina l'adozione di una procedura non adeguata oppure dall'errata esecuzione della procedura scelta.

- **Errori di giudizio (Knowledge based mistakes)**: L'errore è frutto della mancanza di conoscenze o della loro mancata applicazione.

Le Latent Conditions sono condizioni instauratesi nelle fasi di progettazione e di realizzazione del sistema, dovute al tipo di procedure implementate e al tipo di decisioni prese. Essendo latenti, possono celarsi per lungo tempo senza essere rilevate, fino a che la loro combinazione con gli active failures non determina una situazione favorevole all'occorrenza di un incidente: comprendere la genesi di tali dinamiche permette di distinguere tra Proactive e Reactive Risk Management.

Concludendo, Reason, per la prima volta, nel ricercare le cause di un incidente, non si limita all'evento più prossimo, aprendo, di fatto, la strada per l'analisi dei sistemi complessi. Tuttavia, all'interno del suo modello sono riscontrabili i seguenti limiti:

- Linearità del rapporto causa-effetto;

- Visione statica del sistema;
- Descrizione puramente qualitativa: non viene illustrato come i fattori causali si combinino tra loro.

Dall'impostazione logica del modello proposto da Reason deriva la LOPA, *Layers of Protection Analysis*, tecnica comunemente utilizzata nell'industria di processo chimico, in grado di individuare eventuali criticità nell'insieme di misure di sicurezza: essa permette, infatti, di quantificare l'impatto che avrebbe una deviazione di processo qualora non venisse interrotta dagli Independent Protective Layers (IPLs), dispositivi di sicurezza in grado di impedire la propagazione di un particolare scenario di rischio, il cui funzionamento non risente né dell'evento specifico, né dell'attivazione (o mancata attivazione) di altri IPL [19].

Besnard e Baxter [20] comparando il modello di Reason con la LOPA individuano delle similitudini e ne propongono un'alternativa in grado di considerare contemporaneamente gli aspetti tecnici e organizzativi nell'analisi di un incidente. E' possibile infatti rinvenire i seguenti concetti comuni:

- La possibilità di scomporre un sistema in un insieme di sottosistemi o di individui in grado di modificarne il suo funzionamento;

- L'esistenza di condizioni di instabilità che non hanno un effetto immediato sul sistema e sul suo funzionamento;

- La possibilità di rintracciare le cause in errori di progettazione iniziale che, sotto opportune condizioni, possono "attivare" un evento indesiderato;

- Il collasso dell'intero sistema è dovuto all'interazione fra più guasti.

L'idea di Besnard e Baxter è che i fori presenti nei layer del modello di Reason siano associati ad una sequenza {fault – error – failure}, originatasi in fase di creazione del sistema o durante il suo funzionamento. Combinando la prospettiva tecnica

dell'approccio sequenziale con quella organizzativa di Reason, è possibile realizzare una descrizione più dettagliata e, quantomeno, più realistica delle modalità di failure nei sistemi socio-tecnici. In pratica lo studio di Besnard e Baxter effettua un'analisi di tipo qualitativo a cui si sovrappone l'utilizzo della tecnica LOPA. Per ulteriori aspetti si rimanda al capitolo 3, dove è stata effettuata una più ampia trattazione delle tecniche di valutazione del rischio.

1.5 Gli approcci alla sicurezza

L'industria è un sistema complesso dove l'interazione tra fattori eterogenei (sostanze pericolose, fattore umano, aspetti manageriali e organizzativi) può dare luogo a deviazioni di processo che, se non gestite in maniera opportuna, possono risultare in guasti del sistema con conseguenze più o meno gravi [20]: pertanto è opportuno individuare preventivamente come suddette deviazioni possano manifestarsi affinché il sistema possa sopravvivere.

L'utilizzo di modelli incidentali ha un duplice scopo: rende possibile la comprensione di incidenti che si sono già verificati e permette di evitare che essi si presentino nuovamente in futuro, attraverso la predisposizione di apposite misure aventi l'obiettivo di incrementare il livello di sicurezza del sistema considerato.

Quereshi [28] individua due tipologie di approcci, *tradizionale* e *moderno*: appartengono alla prima categoria i modelli di tipo *sequenziale* ed *epidemiologico* mentre alla seconda appartengono i modelli *sistemici* e *formali*. Tale classificazione può essere ampliata introducendo una terza categoria all'interno dell'approccio moderno [29], denominata *Dynamic Sequential Accidental Models*.

1.5.1 L'approccio tradizionale

L'approccio tradizionale, con i metodi sequenziali ed epidemiologici, consente una rappresentazione semplice, intuitiva e lineare della sequenza cronologica di eventi

che si conclude col Top Event. Tale semplicità li rende particolarmente utili nella fase di progettazione e sviluppo di sistemi critici per la sicurezza. Tuttavia, tale ottica non è in grado di cogliere la complessità e di rappresentare la dinamicità dei moderni sistemi socio-tecnici che derivano dalle particolari interazioni – generalmente non lineari – tra le componenti umane - tecniche - organizzative. Inoltre, nel processo di analisi, non tutti gli elementi del sistema sono presi in considerazione. Ne consegue quindi un'analisi statica, a cui molto spesso si aggiungono difficoltà legate alla scarsità di dati e di incertezza ad essi associata.

1.5.2 L'approccio moderno

La teoria dei sistemi definisce l'insieme di leggi, principi e schemi che permettono la rappresentazione e la comprensione dei legami e delle dipendenze esistenti tra gli elementi di un sistema complesso.

1.5.2.1 L'approccio moderno: i modelli sistemici

Gli approcci sistemici sono così definiti in quanto adottano una visione sistemica della realtà d'interesse, nella quale il tipo di interazioni può essere responsabile di un peggioramento della performance globale o della probabilità di un incidente. Elementi caratteristici di tale rappresentazione sono i cicli di feedback (di flussi informativi o di controllo): i processi non sono statici ma evolvono e mutano di continuo affinché sia possibile raggiungere gli obiettivi prefissati (performance, sicurezza, economici, produttivi, ecc) e sia possibile adattarsi alle condizioni a contorno. Adottando, pertanto, una prospettiva sistemica, Rasmussen propone un modello che delinea le varie strutture (tecniche, manageriali, organizzative) presenti all'interno di un'organizzazione, ciascuna delle quali può determinare una o più precondizioni favorevoli ad un incidente industriale.

In tale ottica, la gestione del rischio è equiparabile a un problema di controllo, in cui un infortunio o altre conseguenze pericolose sono causate dalla mancanza/perdita di

controllo sui processi fisici, a seguito di violazioni dei margini operativi definiti attraverso limiti funzionali, amministrativi e di sicurezza [23].

Rasmussen schematizza un sistema socio-tecnico come una struttura gerarchica, in cui il numero e il tipo di livelli possono variare a seconda del contesto organizzativo considerato.

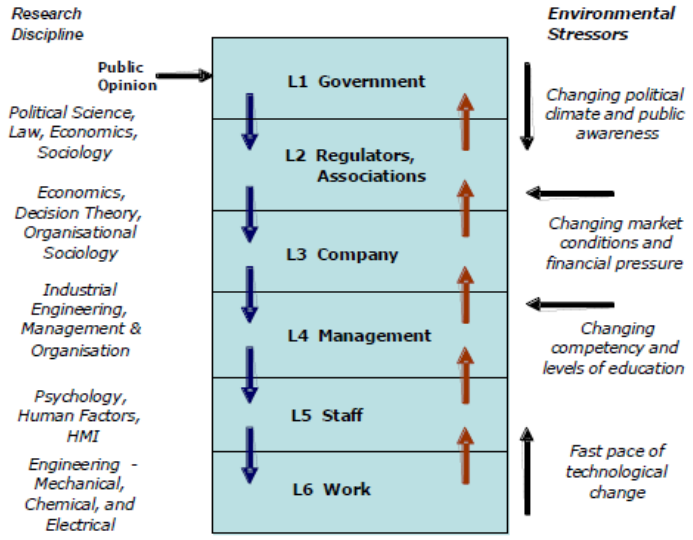

Figura 3 Visione gerarchica di un modello socio tecncico [24].

Partendo dall'alto, si individuano:

1. Le disposizioni legislative che decretano il modo in cui deve essere gestita e amministrata la sicurezza;
2. Le associazioni e le unioni industriali (ad es. le unioni di ingegneri) che percepiscono tali disposizioni e le introducono nei rispettivi settori di appartenenza;
3. L'organizzazione;
4. Il Management, che ha lo scopo di indirizzare, gestire e controllare il lavoro dei propri dipendenti;
5. Gli organi di staff, che si trovano a contatto diretto con i processi operativi;
6. La progettazione del sistema e delle operations.

Come mostrato in figura, il funzionamento del sistema è schematizzabile come un ciclo di feedback, in cui le decisioni prese ai livelli superiori sono trasmesse e recepite a quelli più bassi della gerarchia; parimenti, le informazioni riguardanti i processi operativi devono risalire lungo di essa. Il corretto funzionamento di tale ciclo garantisce la sicurezza dell'intero sistema socio-tecnico, che risulta essere frutto di decisioni e azioni intraprese a vari livelli della gerarchia e non esclusivamente a quello tecnico.

Mentre nella parte laterale di sinistra sono indicate le competenze richieste per comprendere il funzionamento di un particolare livello, in quella di destra sono indicati i fattori esterni a cui ciascun livello è suscettibile di variazione: tali elementi presentano caratteristiche di imprevedibilità, evolvono continuamente e sono tali da modificare il comportamento di ogni singolo livello.

Per analizzare la sicurezza di un sistema socio-tecnico è necessario individuare i confini che delimitano il passaggio da una condizione operativa sicura a una che non lo è. Rasmussen [25] paragona un'organizzazione ad una nave la cui traiettoria è influenzata da fattori esterni in grado di alterarla: ad esempio, pressioni economico-finanziarie o carichi lavorativi eccessivi possono essere responsabili di variazioni comportamentali nell'uomo – nel tentativo di adattarsi ad essi - che possono avere ripercussioni serie per la sicurezza, in un'ottica di lungo periodo. Quindi un incidente industriale in un sistema socio-tecnico non è imputabile a singoli fattori indipendenti (guasto tecnico, negligenza umana) ma è il risultato di un cambiamento di stato che coinvolge l'intera struttura e che ha origine da una piccola variazione - di processo o comportamentale – all'interno di un contesto fortemente dinamico e competitivo.

Il modello STAMP (Systems Theoretic Accident Model and Processes) - elaborato da Leveson e applicato allo studio degli incidenti relativi allo Space Shuttle Challenger e Mars Polar Lander - individua le cause, non nell'occorrenza di failure indipendenti, ma nelle perturbazioni esterne o nelle interazioni anomale fra le componenti del sistema che non sono opportunamente gestite: in tal senso, viene ripresa la concezione di Rasmussen, secondo cui vi è un problema di controllo inadeguato/mancante o di errata progettazione della sicurezza [26].

Un sistema complesso, infatti, possiede un comportamento dinamico che lo porta ad adattarsi continuamente ai cambiamenti interni e alle sollecitazioni esterne cui è soggetto durante il suo normale funzionamento: perché non sia compromessa la sua stabilità, esso deve essere progettato in modo da poter rafforzare i vincoli imposti sulla sicurezza e la suddetta capacità adattativa.

L'innovazione apportata da Leveson sta nell'aver posto l'attenzione sulla mancanza di vincoli imposti al sistema, in fase progettuale e operativa. Partendo da tale posizione, un comportamento non sicuro rappresenta la violazione di un vincolo, che può scaturire dalla sua assenza, dalla sua inadeguatezza o dalla sua mancata applicazione.

Infatti, relativamente all'incidente della navetta spaziale Challenger, Leveson individua la causa nel difetto delle guarnizioni meccaniche, colpevoli di non essere state in grado di controllare il rilascio di gas propellente per sigillare una piccola apertura nella giunzione inferiore; analogamente, nel caso della perdita del Mars Polar Lander, il problema riguardava il software, non in grado di controllare adeguatamente la velocità di discesa della sonda, avendo interpretato erroneamente il rumore di un sensore come segnale del fatto che essa avesse finalmente raggiunto la superficie del pianeta.

Concludendo, l'applicazione del modello STAMP prevede una prima fase in cui viene sviluppata la struttura di controllo gerarchico e in cui vengono individuate le interazioni fra le componenti sistemiche, i requisiti di sicurezza e i vincoli; successivamente, si procede a classificare e ad analizzare i difetti insiti nei cicli di controllo, indicati come *Contraint Failures*. Una gestione della sicurezza efficiente richiede l'individuazione dei vincoli che regolano il comportamento di un processo, e l'imposizione di quest'ultimi, durante l'intero ciclo di vita dello stesso, affinché non ci siano variazioni del livello di sicurezza quando il sistema intraprende cambiamenti: dunque l'enfasi non è posta sul tentativo di prevenire i possibili guasti dei componenti, bensì sui processi di controllo volti a verificare che i vincoli siano implementati correttamente e rispettati.

1.5.2.2 L'approccio moderno: la modellizzazione formale e probabilistica

La Modellizzazione formale si basa sul linguaggio matematico, utilizzato per definire, progettare e verificare, attraverso un procedimento rigoroso, architetture hardware e software molto complesse: in particolare, tali approcci consentono di modellarne il comportamento e di verificare formalmente il rispetto dei requisiti stabiliti in fase di design e di implementazione. Il loro impiego consente quindi di rilevare possibili errori di fondo, che in fase avanzata possono determinare costi di riparazione eccessivi.

Il vantaggio conseguito attraverso l'utilizzo di uno linguaggio formale deriva da tre fattori [30]:

- la *sintassi*, insieme di regole che permette la corretta formulazione di un'espressione;
- la *semantica*, insieme di regole definite su uno specifico dominio, attraverso cui è possibile attribuire il significato esatto a un dato concetto;
- la *proof theory*, procedimento induttivo che permette di desumere informazioni generali da casi particolari.

Si ottengono quindi una descrizione e una valutazione corrette, consistenti e complete. La modellizzazione matematica fornisce un'interpretazione del legame causa-effetto di tipo deterministico, ovvero se A implica B, ogniqualvolta A si verificherà, sarà automaticamente presente anche B: tuttavia, non è detto che il verificarsi di particolari condizioni garantisca sempre la riproduzione dei medesimi effetti. Di conseguenza, si fa strada l'esigenza di supportare l'analisi di un incidente mediante l'impiego di modelli probabilistici (*Probabilistic Models of Causality*).

L'idea di base è quella secondo cui l'occorrenza di uno specifico fattore causale aumenti la probabilità che quel particolare effetto ad esso associato si realizzi.

1.5.3 Dynamic Sequential Accident Models

Inizialmente sviluppati per il settore finanziario, i Dynamic Sequential Accident Models (DSAMs) sono stati successivamente estesi ad applicazioni nel campo nucleare e nell'industria di processo in generale. Tali metodi combinano la semplicità che deriva dalla struttura sequenziale – di un Fault Tree o di un Event Tree – per la rappresentazione dello scenario incidentale con l'utilizzo di altre tecniche in grado di rappresentare relazioni complesse e non lineari.

Il loro funzionamento si basa su dati precursori, ovvero quegli eventi spesso indicati come incidenti sfiorati o infortuni minori (near-misses and mishaps) che costituiscono il preludio ad un incidente vero e proprio e che possono essere impiegati per aggiornare le valutazioni sul rischio in tempo reale: in questo modo, è possibile tener conto della presenza di nuovi fattori di rischio, migliorarne le definizioni e i loro criteri e livelli di accettabilità.

Tali modelli sono classificabili in due categorie:

1. Dynamic Risk Assessment (DRA);
2. Process Hazard Prevention Accident Models (PHPAMs).

Nel dettaglio le fasi del Dynamic Risk Assessment sono [43]:

1. Identificazione degli scenari incidentali più plausibili, specificando per ciascuno di essi i tipi di failure implicati e i possibili stati finali. L'output di tale fase è la realizzazione di una Bow-Tie per avere una rappresentazione grafica degli eventi critici (CE) selezionati (nodi del diagramma), in cui vengono indicate le relative cause (Initiating Events, IEs), le possibili conseguenze (Outcome Events, OEs, o End-states) e le barriere di sicurezza predisposte al controllo/mitigazione del rischio: il nodo centrale rappresenta l'evento critico (Critical Event (CE)).

2. Determinazione delle probabilità a priori, utilizzando dati tratti dalla letteratura o presenti nei manuali scientifici. La probabilità che

caratterizza ciascuno stato finale viene calcolata moltiplicando i valori presenti lungo il ramo che collega l'evento iniziale allo stato in esame:

a) Fr{CE}= frequenza di CE;
b) Pr{OE}= probabilità che si verifichi OE a causa di CE;
c) Pr{SB_{OE}}= probabilità di guasto della barriera relativa ad OE;

$$Freq\{OE\} = Freq\{CE\}*Prob\{OE\}*Prob\{SB_{OE}\}$$

Tali grandezze, deterministiche, rappresentano la conoscenza che si ha del sistema prima che venga avviato il suo funzionamento. Nella realtà però la probabilità di failure di un sistema di sicurezza tende a seguire una distribuzione: l'approccio probabilistico esprime quindi la probabilità degli end-states moltiplicando la funzione di densità di probabilità di ciascun sistema, come nel caso deterministico. La distribuzione utilizzata, in genere, è quella Beta, di parametri ($\alpha, \beta > 0$), definita sull'intervallo [0,1] avente pdf:

$$f(x)= \frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha,\beta)}.$$

Per ciascun sistema di sicurezza vengono quindi specificati i parametri α e β.

3. Creazione della funzione di verosimiglianza, utilizzando i dati ASP (near-misses and incidents), registrati durante il periodo di osservazione: è lo step che determina il passaggio dal QRA al DRA. Tra i vari approcci per la costruzione di tale funzione, quello più conveniente consiste nello scegliere una funzione coniugata di quella a priori. Si utilizza pertanto una distribuzione binomiale, coniugata della funzione beta:

$$g(data|x)= \frac{n}{s} x^s (1-x)^f,$$

- n= numero di osservazioni;
- s=numero di successi;
- f=n-s=numero di failures;

4. Costruzione funzione probabilità di guasto a posteriori mediante l'inferenza bayesiana: tale passaggio permette di migliorare la stima del parametro, convogliando nuove informazioni ricavate dal processo e simulando pertanto il meccanismo di apprendimento. Indicando con:

   - x = la probabilità di guasto;
   - data = ASP;
   - f(x) = la distribuzione di probabilità di guasto a priori;
   - g(data|x) = la funzione di verosimiglianza;
   - f(x|data) = la distribuzione di probabilità di guasto a posteriori;

   il risultato del processo di inferenza è $f(x|data) \propto g(data|x)*f(x)$.

5. Valutazione delle conseguenze: disponendo delle probabilità a posteriori ed esprimendo le conseguenze, ad esempio, in termini di costi, il rischio associato a un particolare end-state è dato dal prodotto della sua probabilità a posteriori e della sua entità.

Molto spesso il Dynamic Risk Assessment viene combinato con altre tecniche, come nel caso di Paltrinieri et al. [44], che vi associano una tecnica di hazard identification (Dynamic Procedure for Atypical scenarios Identification – DyPASI), con l'obiettivo di soddisfare i requisiti di dinamicità e di poter apportare miglioramenti continui alla valutazione del rischio, attraverso processi iterativi.

La DyPASI rappresenta, di fatto, un'estensione della tradizionale bow-tie, che consente la sistematizzazione delle informazioni provenienti dai segnali precursori e che implica uno screening completo del sistema volto ad individuare i possibili scenari incidentali atipici.

1.5.4 Process Hazard Prevention Accident Models (PHPAMs)

Si tratta di modelli introdotti da F. Khan e da suoi collaboratori ([2] e [45]), relativamente ad applicazioni nell'industria di processo chimico: in particolare, sono stati proposti due modelli, uno relativo ad un'industria off-shore di petrolio e gas e

uno per l'identificazione, la predizione e la prevenzione dei pericoli di un sistema (SHIPP).

Figura 4 Off - shore oil and gas prevention accident [2].

Il primo parte dal presupposto secondo cui, in un'industria di trattamento di petrolio e gas, un qualsiasi incidente scaturisce da una perdita di idrocarburi: sono, quindi, predisposte cinque barriere di sicurezza, il cui malfunzionamento consente all'evento iniziale di propagarsi lungo la sequenza rappresentata in figura (la situazione in cui tutte le misure falliscono configura il worst-case). La probabilità di guasto di ciascun layer è calcolata attraverso l'utilizzo di un Fault Tree mentre le conseguenze implicate come Event Tree.

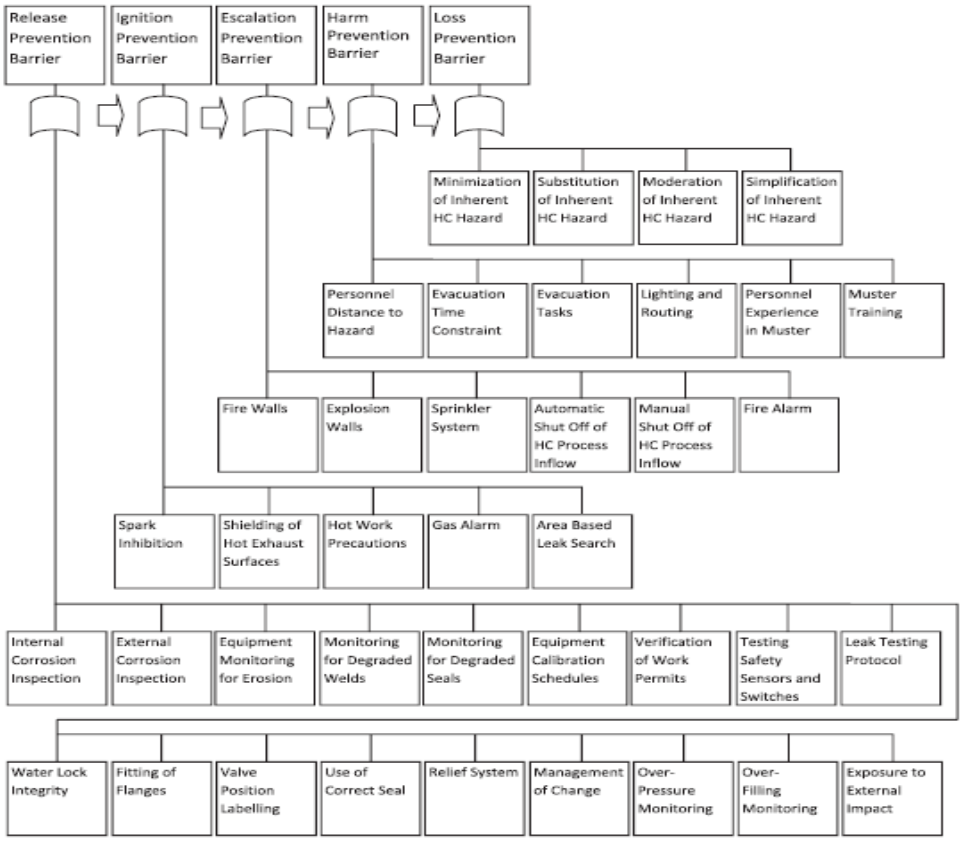

Figura 5 Fault Tree nel modello Off-shore oil and gas prevention [2].

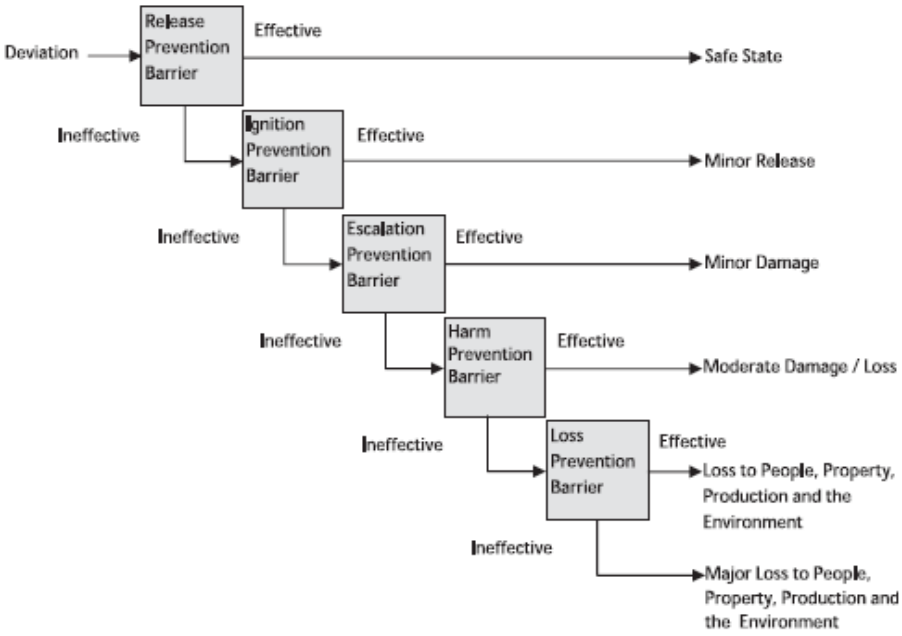

Figura 6 Event Tree nel modello Off - shore oil and gas prevention [43].

L'aggiornamento dei valori probabilistici viene effettuato attraverso un meccanismo bayesiano che si basa sull'utilizzo dei dati precursori ricavabili dall'Event Tree.

Tale modello possiede le seguenti limitazioni:

1. Le cause di un incidente sono solo di tipo tecnico-operativo: il fattore umano e il contesto organizzativo non rientrano nel processo di analisi;
2. Il modello è impostato soltanto sulla possibilità di ignizione: altri eventi iniziali, come ad esempio il rischio di esplosione, non vengono contemplati.

1.6 Il comportamento umano

Se da un lato, il progresso tecnologico ha aumentato l'affidabilità dei sistemi, riducendo significativamente il numero di incidenti di natura tecnica, dall'altro bisogna tener presente che la componente umana risulta essere responsabile del 60 - 80% degli incidenti sul luogo di lavoro.

Si rende quindi necessario quantificare il contributo che il fattore umano apporta all'affidabilità del sistema: l'Human Reliability è lo studio dei fattori esterni all'uomo

– ovvero dipendenti dal luogo di lavoro (attrezzature adottate, materiali utilizzati, predisposizione ed ergonomia dei luoghi di lavoro, organizzazione delle attività lavorative) - ed interni - condizioni psico-fisiche dell'operatore – in grado di condizionarne la performance lavorativa.

Un primo approccio alla valutazione del comportamento umano è quello fondato sui principi psicologici che individuano nel processo cognitivo la causa degli errori umani. Il paradigma di riferimento è l'IPS - Information Processing System - che si riferisce alle funzioni cognitive e comportamentali principali: percezione, interpretazione, pianificazione e azione [22]. Una trattazione più esaustiva è presente nel IV capitolo.

1.7 La sicurezza sui luoghi di lavoro e i riferimenti normativi in Italia

Il tema della sicurezza sul lavoro vede una grande sinergia di intenti dal punto di vista della ricerca scientifica e rappresenta un ambito privilegiato di competenza istituzionale, oggetto di un impegno costante per una piena tutela della salute, dell'integrità e della dignità della persona in ogni ambiente di lavoro.

La promozione di un contesto lavorativo sicuro passa attraverso la preparazione e l'attuazione di adeguate misure, volte a garantire a ciascun individuo la possibilità di esercitare il proprio diritto al lavoro.

In Italia il riferimento normativo in materia di sicurezza e salute sui luoghi di lavoro è il decreto legislativo n.81 del 9 aprile 2008 (noto anche come "Testo Unico di salute e sicurezza sul lavoro") che ha unificato, riformato e armonizzato tutte le disposizioni previste dalle precedenti normative in materia di sicurezza, abrogandole.

L'obiettivo è costruire e diffondere la cultura della sicurezza e della prevenzione, privilegiando tutte quelle attività e iniziative volte a promuovere comportamenti responsabili, improntati alla tutela dell'incolumità propria e altrui e alla individuazione di strategie in grado di contrastare efficacemente il fenomeno degli infortuni sul lavoro: a tal riguardo il Ministero svolge un'azione di monitoraggio dello

stato di attuazione delle vigenti disposizioni, finalizzata ad individuarne i problemi applicativi e ad elaborare interventi migliorativi.

1.7.1 Il D.P.R n.151 del 2011

Il provvedimento n.151 del 1 agosto del 2011 contiene il nuovo regolamento per la disciplina dei procedimenti relativi alla prevenzione incendi, che va a sostituire il decreto del Ministro dell'Interno del 4 maggio 1998, recante "Disposizioni relative alle modalità di presentazione ed al contenuto delle domande per l'avvio di procedimenti di prevenzione incendi, nonché all'uniformità dei connessi servizi resi dai Comandi provinciali dei vigili del fuoco", adottato ai sensi del precedente regolamento di prevenzione incendi di cui al D.P.R. n. 37 del 1998: vengono individuate le attività soggette ai controlli di prevenzione incendi e fornite le indicazioni per la verifica delle condizioni di sicurezza antincendio (deposito ed esame dei progetti, visite tecniche, approvazione di deroghe a specifiche normative) di competenza del Corpo nazionale dei vigili del fuoco [6].

Il nuovo regolamento, recependo i contenuti dalla legge n.122 del 30 luglio 2010 circa lo snellimento dell'attività amministrativa, opera una sostanziale semplificazione riguardo gli adempimenti da parte dei soggetti interessati: sono escluse dalla sua applicazione le attività industriali a rischio di incidente rilevante, per le quali continua a vigere l'obbligo di redazione del "rapporto di sicurezza" previsto dall'art. 8 del d.lgs. 334/99.

1.7.2 Protezione da atmosfere esplosive: il rischio ATEX

Il titolo XI del Testo Unico prescrive le misure per la tutela della sicurezza e della salute dei lavoratori esposti al rischio di atmosfere esplosive, ovvero miscele composte da aria, a condizioni atmosferiche (concentrazione di ossigeno del 21%, temperatura di 25°C, pressione di 1 atm), e da sostanze infiammabili allo stato di gas, vapore, nebbie o polveri, in cui, una volta innescata, la combustione si propaga

all’interno della miscela incombusta (art.288) [6] (si rimanda al capitolo 4 la descrizione del fenomeno fisico, limitandosi qui a considerare soltanto gli aspetti normativi).

Esistono due direttive riguardo tale tema:

1. **Direttiva 94/9/CE**, recepita con il regolamento di attuazione D.P.R. n.126 del 23 marzo del 1998 (allegato L parte B del D.Lgs. 81/08), che stabilisce i requisiti di sicurezza per gli apparecchi e i sistemi di protezione destinati ad essere utilizzati in ambienti potenzialmente esplosivi;
2. **Direttiva 99/92/CE**, recepita tramite D.Lgs. n.233 del 12 giugno 2003 (inserita nel titolo XI del D.Lgs. 81/08), che prescrive le misure per la tutela della sicurezza e della salute dei lavoratori che possono essere esposti al rischio di atmosfere esplosive.

In base alla valutazione dei rischi, il datore di lavoro deve prevenire la formazione di atmosfere esplosive o, qualora l’attività in esame non lo renda possibile, evitare che esse vengano innescate e attenuare gli effetti pregiudizievoli di esplosione in modo da garantire la salute e la sicurezza dei lavoratori: è necessario determinare la probabilità di formazione di un’atmosfera esplosiva, analizzando la presenza e la quantità di sostanze suscettibili di esplosione, individuare la possibile presenza di fonti di innesco della miscela e cercare di stimare le conseguenze.

CAPITOLO II: LA RESILIENZA

In un mondo sempre più interconnesso (sia sotto un punto di vista sociale, che tecnologico ma anche ambientale), nessuna organizzazione o nessun sistema complesso può essere in grado di conservare una posizione competitiva o addirittura sopravvivere a eventuali interruzioni o all'attacco di eventi imprevisti. Le minacce che incombono su una qualsiasi entità organizzativa possono essere distinte in base alla gravità e alla frequenza, e soprattutto possono derivare tanto dall'interno quanto dall'esterno del sistema stesso.

Un evento che si origina in un settore, spesso, genera effetti (sia positivi che negativi) anche negli altri settori ad esso connesso. I sistemi complessi non sono in grado di resistere a queste sfide, perciò è essenziale e necessario che tutti gli sforzi siano incanalati nel rendere le imprese robuste e resilienti al verificarsi di eventi incerti ed inaspettati. Il concetto di Resilienza è utilizzato in una vasta area di discipline e in questo lavoro verrà trattato soprattutto nell'ambito dell'ingegneria della sicurezza.

La parola "Resilienza" ha le sue origini nella parola latina "*resiliere*", che significa "riprendersi" . L'uso comune del termine Resilienza in forma scritta e orale si riferisce soprattutto alla capacità di un'entità di riprendersi. Tale entità può essere rappresentata, per esempio, da un certo numero di individui (o famiglie) che superano una scossa personale o grandi difficoltà e sono pertanto considerati resilienti.

2.1 La Resilienza: definizioni

La valutazione del rischio effettuata grazie al Quantitative Risk Assessment non riesce a tenere conto di tutti gli aspetti relativi alla sicurezza di un impianto, in quanto ci si concentra sui singoli eventi incidentali, senza guardare la "robustezza" dello stesso, in quanto costituto da uomini e macchine che interagiscono sistemicamente in un'organizzazione complessa. Per superare questa "visione" parziale si introduce il concetto di Resilienza. Esso è stato introdotto nei primi decenni del XX secolo in una

varietà di settori scientifici, come la fisica, la psicologia e la psichiatria, l'ecologia, le imprese, la sicurezza industriale e delle telecomunicazioni.

Il concetto di Resilienza, ovvero "la capacità di un corpo teso di recuperare dimensione e forma in seguito ad una deformazione causata soprattutto da sollecitazioni di compressione", si riferisce ad un materiale con proprietà simili all'elasticità. Nella disciplina della scienza dei materiali è anche definito un modulo di elasticità utilizzato per rappresentare l'energia assorbita per unità di volume di materiale quando viene stressato al limite (cioè senza creare una deformazione permanente). In riferimento a tale definizione, è possibile rappresentarla come il limite di energia di un disturbo che un sistema può assorbire prima di diventare instabile. In analogia con queste definizioni, Steen e Aven [33] hanno definito il concetto di Resilienza come la probabilità di un sistema di soccombere ad eventi negativi e l'hanno formalizzata come una funzione dipendente da differenti parametri, come ad esempio: barriere di sicurezza, conseguenze, incertezza ed eventi incidentali. La seconda definizione, "la capacità di recuperare a causa di un evento o cambiamento imprevisto", si riferisce ad un tratto personale nelle persone [34].

Sulla base di quanto si è detto in precedenza, è necessario fornire una serie di definizioni che si sono succedute nel corso degli anni, delineando di fatto un'evoluzione temporale e cognitiva del concetto stesso di Resilienza. Facendo riferimento ai sistemi socio - ecologici, si può definire la Resilienza come la grandezza di disturbo che può essere tollerata prima che il sistema si sposti in una diversa regione dello spazio di stato controllato da un diverso insieme di processi [35]. Questa definizione è basata sul concetto di Resilienza ecologica, che secondo Holling [36], può essere misurata come la grandezza di disturbo che può essere assorbita prima che il sistema cambi la sua struttura insieme al cambiamento delle variabili e dei processi che ne controllano il comportamento. Secondo Fiksel, la Resilienza può essere definita come la capacità di un sistema di tollerare i disturbi pur mantenendo inalterate la struttura e la funzione. Hoffman, invece, definisce la Resilienza in termini di business, come la capacità di un'organizzazione, di una risorsa o di una struttura di sostenere l'impatto di un'interruzione, di recuperare e di riprendere le sue operazioni per continuare a fornire servizi minimi. Secondo

Hoffman, un’organizzazione risulta essere resiliente se e solo se raggiunge i livelli di servizio minimi in seguito al verificarsi di un’interruzione. Wreathall aggiunge l'elemento di rapidità alle operazioni svolte durante un’interruzione e definisce la Resilienza come la capacità di un’organizzazione (o di un sistema) di mantenere o di recuperare in fretta uno stato stabile, garantendo lo svolgimento continuo delle operazioni durante e dopo il verificarsi di un grave incidente, o in presenza di continue sollecitazioni significative. Vogus e Sutcliffe, invece, definiscono la Resilienza organizzativa come il mantenimento dell’assestamento positivo sotto difficili condizioni, in modo che l'organizzazione sia in grado di emergere da tali condizioni rafforzata e più intraprendente. Imprese resilienti crescono, prosperano e diventano migliori in parte perché hanno affrontato e superato grandi sfide. Simile agli sforzi dell'azienda per sviluppare la capacità di cambiare direzione con breve preavviso e a basso costo, gli sforzi per costruire una capacità di Resilienza presumono che il cambiamento e la sorpresa possano essere fonte di opportunità, così come segni di potenziale minaccia, ma che, per capitalizzare queste opportunità, è spesso necessaria una trasformazione a livello organizzativo. Pertanto in base alle differenti definizioni date nel corso degli anni al concetto di Resilienza organizzativa, la letteratura ne offre due differenti punti di vista. Alcuni vedono la Resilienza organizzativa semplicemente come la capacità di rimbalzare da stressanti, avverse e inattese situazioni e di ritornare alla condizione iniziale [37]. Questo punto di vista prende forma dalla definizione, prima fornita, di Resilienza nel campo delle scienze fisiche in cui un materiale è resiliente se è in grado di riconquistare la sua forma e le caratteristiche originali dopo esser stato allungato. Pertanto da queste prime definizioni risulta chiaro che il concetto di Resilienza risulta applicato ai vari ambiti scientifici e a seconda del campo di applicazione, il concetto di Resilienza può assumere svariati significati e soprattutto si possono evidenziare diversi fattori e principi contributivi.

2.2 Applicazione del concetto di Resilienza nelle diverse discipline

2.2.1 La Resilienza nei sistemi ecologici

La Resilienza, valutata da Holling [36] in riferimento ai sistemi ecologici, è stata definita come la capacità di un qualsiasi sistema di assorbire i cambiamenti, di sopravvivere alle perturbazioni sia esterne che interne e di riportarsi ad uno stato di equilibrio. Alcuni altri autori in seguito hanno definito la Resilienza nei sistemi ecologici come il tempo necessario per un sistema di ritornare ad uno stato stazionario o di equilibrio in seguito ad una perturbazione (Pimm, 1984). L'esistenza di stati stabili alternativi che sono soggetti a modifiche innescate da fattori esogeni (Beisner, 2003) suggerisce una comprensione dinamica e globale della Resilienza rispetto alla definizione che è stata fornita da Holling, intendendo la Resilienza come la capacità di un sistema di assorbire le perturbazioni e di riorganizzarsi durante la fase di cambiamento, in modo da svolgere essenzialmente la sua funzione, mantenendo di fatto inalterata la propria struttura (Walker, 2004) [35].

2.2.2 La Resilienza negli ecosistemi industriali

Poiché gli ecosistemi industriali, così come le supply chain, si basano sulle relazioni di domanda e di offerta di prodotti e servizi, alcuni spunti dalla letteratura della supply chain possono far luce sulla discussione della Resilienza degli ecosistemi industriali. Tuttavia, gli ecosistemi industriali differiscono dalle catene di approvvigionamento in almeno due aspetti. In primo luogo, mentre la gestione della supply chain riguarda la prestazione operativa e finanziaria delle imprese, la gestione degli ecosistemi industriali comprende anche la mitigazione della velocità del materiale e dell'energia, e gli impatti ambientali. È quest'ultimo che definisce un sistema industriale regolare come un ecosistema industriale. In secondo luogo, un elemento importante per la costruzione e la gestione degli ecosistemi industriali, tecnologicamente fattibili ed economicamente interessanti, è l'eco – efficienza. L'eco - efficienza si raggiunge attraverso la riduzione di materia ed energia senza però influenzare i beni e i servizi forniti, e ottimizzando le linee di produzione. Tuttavia, se l'eco - efficienza è intesa

come l'unico obiettivo da perseguire, si può assistere ad una diminuzione della Resilienza di un sistema industriale e della sua capacità di sopravvivere in un contesto di mercato variabile. Inoltre, si può assistere ad una struttura di rete più complessa negli ecosistemi industriali, rispetto a quelle presenti nelle supply chain. Le caratteristiche degli ecosistemi industriali, la realizzazione di obiettivi ambientali più ampi e la nascita di strutture sempre più complesse portano i sistemi industriali in un nuovo bacino di attrazione, modificando l'intero panorama di stabilità e la loro posizione al suo interno. Pertanto, la Resilienza degli ecosistemi industriali tende ad incrementarsi, se si intende aumentare il livello di eco – efficienza e mitigare l'impatto ambientale attraverso un maggior utilizzo di risorse e una considerazione sistematica dell'impatto dei processi di produzione [42].

2.2.3 La Resilienza applicata alle reti ed alla Supply Chain

La Resilienza della rete è stata valutata come la proprietà che ha una rete di sostenere le sue operazioni di routine e le prestazioni desiderate nel momento in cui ci si trova di fronte ad una serie di situazioni prevedibili o imprevedibili, come minacce e modifiche. È possibile, inoltre, affermare che il concetto di Resilienza evolve in parallelo con lo sviluppo di una rete, e con le esigenze e le sfide di carattere operativo [40]. La Resilienza si può definire attraverso le relazioni che intraprende con determinati "enti". Tali "enti" sono: agenti di minaccia, dominio, proprietà, minacce e mezzi. Questi enti, però, possono essere in conflitto, evidenziando in tal modo la necessità di compromessi al fine di trovare l'equilibrio ideale delle contromisure contro le minacce [41].

La robustezza della supply chain può essere definita come la capacità di gestire la variabilità dei fattori di input mantenendo a bassi livelli, o comunque sotto controllo, la variabilità degli output (performance, costi e livelli di servizio). Tale capacità può essere interpretata in termini di Resilienza. Il concetto di Resilienza applicato alla supply chain, inoltre, affronta la prestazione operativa e finanziaria in un mondo dinamico come quello degli affari, il quale è soggetto a cambiamenti rapidi e significativi. Il concetto di Resilienza è strettamente legato a concetti come la vulnerabilità e la gestione del rischio (Jüttner, 2003; Wagner e Bode, 2006), la

velocità, l'agilità e la flessibilità (Duclos, 2003; Prater, 2001). Un altro concetto importante, connesso a quello di Resilienza, è rappresentato dalla capacità di adattamento: la gravità delle interruzioni nella supply chain dipende sia dalle caratteristiche di progettazione (Resilienza), sia dalla capacità di mitigazione (adattabilità) (Craighead, 2007) [38]. Nonostante non ci sia una definizione generale di Resilienza nelle supply chain, il concetto funge da base per l'attività di gestione del rischio per trattare la vulnerabilità della supply chain, sulla base di una conoscenza avanzata della supply chain stessa e del giusto compromesso tra l'esposizione al rischio e la perdita di profitto [39]. Nel contesto delle attività, una supply chain resiliente deve essere anche adattabile, in quanto lo stato desiderato può essere differente dai processi originali. Una supply chain robusta, invece, può essere forte ma non adattabile, per cui una filiera di processi robusti non è necessariamente resiliente: dunque la differenza fondamentale tra i due sinonimi sta nella capacità di risposta alle variazioni in ingresso. Una catena di fornitura robusta è in grado di affrontare la variabilità in ingresso, mantenendo un buon controllo; una catena di fornitura resiliente è molto più sensibile alla variabilità in ingresso ed inoltre è in grado di rispondere ad un improvviso ed inaspettato spostamento nel livello di input. La Resilienza di una catena può essere realizzata attraverso i seguenti quattro principi (Christopher e Peck, 2004):

- la Resilienza può essere costruita in un sistema in anticipo (re - engineering);
- la collaborazione è necessaria per identificare e gestire i rischi;
- l'agilità è indispensabile per reagire rapidamente a eventi imprevisti;
- la cultura della gestione del rischio è una necessità.

Il grado di Resilienza di una supply chain è valutato in funzione di due dimensioni: la vulnerabilità e la capacità. Essa aumenta all'aumentare della capacità e al diminuire della vulnerabilità. Pertanto la Resilienza equilibrata sarà il giusto compromesso tra fattori di vulnerabilità e di capacità.

2.2.4 La Resilienza applicata alla sicurezza

Avendo definito e analizzato nel dettaglio l'evoluzione storica e concettuale della Resilienza, è possibile applicare tale concetto nel campo specifico della sicurezza. Negli anni, errori umani e guasti di singoli componenti sono stati considerati la causa principale del verificarsi della maggior parte degli incidenti. Tuttavia, oggi, è ben noto che le principali cause di incidenti possono essere rintracciate nei fattori organizzativi, nelle variabilità funzionali delle prestazioni e nella presenza di combinazioni inaspettate [43]. È possibile affermare che le attività fortemente interattive e multidimensionali non possono essere controllate da un metodo tradizionale puro, che mira semplicemente a limitare gli errori (Heikkila, 2010). Sistemi di sicurezza tradizionali, infatti, si basano sulle analisi di eventi e di incidenti; tali analisi possono aiutare le organizzazioni e i sistemi ad ottenere una panoramica degli incidenti, limitandosi però a contare gli eventi negativi (errori, violazioni e incidenti), non riducendo di fatto i potenziali rischi. In altre parole, la segnalazione di inconvenienti, incidenti ed errori e la conseguente analisi, non possono incrementare il livello di sicurezza di sistemi ed ambienti pericolosi (Huber, 2009): da qui l'introduzione del concetto di Resilienza ingegneristica (RE). In passato, gli approcci di gestione della sicurezza presentavano una natura reattiva, mentre l'approccio della RE segna la maturazione e la presentazione di un nuovo e propositivo approccio alla gestione della sicurezza [44]. In un mondo di risorse limitate, di incertezza irriducibile e di molteplici obiettivi contrastanti, si crea sicurezza attraverso l'implementazione di processi resilienti proattivi piuttosto che reattivi. La RE è la capacità dei sistemi e delle organizzazioni di anticipare e di adattarsi al potenziale di sorpresa e di fallimento (Woods e Hollnagel, 2006) [2]. Si tratta di un approccio proattivo che permette di rimuovere i vincoli precedenti. Inoltre, è un paradigma per la gestione della sicurezza che si concentra su come aiutare le persone ad anticipare le diverse forme di rischio, al fine di far fronte in maniera efficiente ed efficace alle difficoltà e ad orientarsi verso il successo (Haimes, 2009). La RE, pertanto, considera il fallimento e il successo come fenomeni strettamente connessi tra loro. Essendo la Resilienza la generica abilità di far fronte alle sfide impreviste, sfruttando la propria flessibilità per riuscire a soddisfarle

(Hollnagel, 2008), essa va intesa necessariamente come una misura di sicurezza aggiuntiva (Dinh, 2012) [45]. La RE sottolinea il modo in cui si ottiene il successo, come le persone, i sistemi e le organizzazioni imparano e si adattano, e crea così la sicurezza in un ambiente caratterizzato da rischi, compromessi e molteplici obiettivi (Hollnagel, 2006). La capacità di un sistema di regolare un ambiente in costante evoluzione potrebbe essere il fattore predittivo più importante del futuro della sicurezza (Dekker, 2006; Dekker e Laursen, 2007). La volontà degli imprenditori di investire nel settore della sicurezza e di assegnare risorse con un metodo puntuale e proattivo, è un elemento imprescindibile per poter garantire l'esistenza di un'organizzazione o di un sistema resiliente (Gilmour, 2006). L'idea alla base della RE consiste nella creazione di processi di gestione del rischio che sono robusti, conservando però, al tempo stesso, una grande flessibilità (Gilmour, 2006). Sono stati condotti alcuni studi nel contesto della RE, il cui scopo era spesso il miglioramento del sistema di sicurezza di impianti di distribuzione dell'olio (Abech, 2006), impianti di raffinazione (Tazi e Amalberti, 2006), aviazione (Zimmermann, 2011; Dekker, 2008), sistemi di gestione della salute e della sicurezza [46], ambienti di processo ad alto rischio (Huber, 2009), distributori di energia elettrica (Saurin e Carim Junior, 2011), impianti chimici (Shirali, 2012), processi industriali (Dinh, 2012). Pertanto, oggi la Resilienza deve essere intesa come un concetto strategico che interessa fortemente il miglioramento della sicurezza nei sistemi complessi, dal momento che potrebbe conciliare prestazioni e sicurezza, piuttosto che opporsi sistematicamente (Morel, 2009). La valutazione delle prestazioni dei servizi nella maggior parte delle imprese, è un tema importante per dirigenti, decisori e ricercatori [47].

2.2.4.1 Binomio sicurezza – Resilienza applicato ai processi industriali

È necessario, arrivati a questo punto, analizzare il funzionamento di una qualsiasi organizzazione industriale e valutare come il binomio sicurezza - Resilienza risulti essere indispensabile per la sopravvivenza della stessa organizzazione.

Mentre un sistema resiliente è nello stesso tempo anche sicuro, dire che il sistema di sicurezza di un'organizzazione è efficiente e a norma non implica che essa sia resiliente: è infatti necessaria, in primo luogo, una capacità di gestione che trascende

la semplice conformità a disposizioni normative. La sicurezza, inoltre, può essere ottenuta a scapito di altri obiettivi, ad esempio mantenendo l'operatività del sistema al di sotto della performance ottimale. In riferimento a ciò, uno studio sulla rete ferroviaria olandese, presentato nel testo di Hollnagel, Woods e Leveson [48], ha dimostrato come la sicurezza dei passeggeri veniva ottenuta sacrificando altri fattori, come la puntualità del servizio. Il sistema era organizzato in una serie di zone di sicurezza predefinite: nel momento in cui un treno usciva al di fuori di esse, l'intero sistema veniva bloccato, riorganizzato e, solo dopo aver ripristinato la configurazione di sicurezza, riprendeva il suo normale funzionamento. Tale esempio mostra come, da un lato, la rete garantiva un livello di sicurezza elevato ma, dall'altro, aveva una capacità di adattamento alle condizioni a contorno inesistente: pertanto, essa non era affatto resiliente.

Nel funzionamento di un processo industriale, si possono distinguere tre stati del sistema: normale, sconvolto e catastrofico. I sistemi di processo devono essere mantenuti nella regione di stato normale. Tuttavia, i disturbi esistono in qualsiasi realtà e tendono a forzare lo stato del sistema dalla regione di stato normale. Se il sistema ha la capacità di rilevare disturbi e manipolare le variabili di funzionamento effettivo (in funzione di un sistema di controllo di processo), allora è possibile rimanere nello stato normale. Ma la rilevazione può non riuscire, alcune azioni possono essere trascurate e anche la manipolazione può non essere in grado di mantenere lo stato normale del sistema. Tutto questo potrebbe causare incidenti più o meno gravi; di conseguenza, lo stato del sistema può cambiare e divenire in tal modo sconvolto. Il sistema può essere recuperato e riportato ad uno stato normale attraverso metodi efficaci di recupero. Se un sistema sconvolto non è gestito correttamente e non è in grado di riportarsi al suo stato normale, allora possono seguire grandi eventi e il sistema può transitare in uno stato catastrofico. Questo stato può ancora essere recuperato e portato alla normalità, se e solo se l'azione viene svolta entro un certo lasso di tempo. Quanto veloce ed efficace sia questo recupero, dipenderà non solo dai piani di recupero, ma anche e soprattutto dalla progettazione del sistema. Gran parte della ricerca nel settore della sicurezza di processo mira a prevenire ed evitare la transizione dello stato del sistema all'interno della zona catastrofica. Nonostante i continui sforzi, rivolti ad incrementare il livello di sicurezza

dei processi, gli incidenti purtroppo ancora si verificano. Tali incidenti possono essere causati da guasti tecnici e umani, a cause naturali (ad esempio uragani) o ad azioni umane intenzionali (ad esempio il terrorismo e il sabotaggio). Nei sistemi complessi e di grandi dimensioni, si possono verificare queste situazioni inaspettate, nonostante la corretta e completa esecuzioni di tutte le fasi di gestione del rischio. Nel momento in cui si verificano queste situazioni, le priorità per gli operatori consistono nel ridurre al minimo i danni e intraprendere operazioni per tentare di ripristinare le normali condizioni: questa è l'idea del concetto di Resilienza nei processi industriali. La RE pertanto aiuta a recuperare in seguito al verificarsi di incidenti, piuttosto che impedire agli incidenti stessi di verificarsi. La prevenzione degli incidenti diviene in questo modo essenziale, anche se è impossibile prevedere tutti i possibili scenari ed evitare tutte le minacce. Di conseguenza, la Resilienza è necessaria come misura di sicurezza aggiuntiva [49]. Le applicazioni della RE sono particolarmente adatte per sistemi ad alto rischio con caratteristiche complesse, come (Christoffersen e Woods, 1999):

- l'elevato grado di interconnessione tra i diversi componenti del sistema, la cui conseguenza è la grandissima difficoltà dell'operatore di riuscire a prevedere gli effetti delle sue azioni e soprattutto la rapida propagazione degli errori;
- l’incertezza e la variabilità.

2.3 Principi e fattori contributivi della Resilience Engineering

Considerando che non vi è un insieme di principi della RE che è ampiamente accettato nei circoli accademici e che ci sono differenze nella terminologia adottata dai diversi autori, ai fini del presente lavoro, vi è la necessità di cercare di compilare una serie di principi che funga da riferimento. Vale la pena sottolineare che i principi della RE possono essere utilizzati a qualsiasi livello di aggregazione del sistema cognitivo, che vanno dalla messa a fuoco di un singolo lavoratore sul posto di lavoro alla messa a fuoco dell'intera organizzazione nel suo complesso. Pertanto, sulla base dei diversi studi (Rasmussen, 1997; Hollnagel e Woods, 2005; Hale e Heijer, 2006; Wreathall, 2006; Saurin, 2008), sono stati identificati i seguenti principi, i quali non possiedono limiti strettamente definiti:

- L’impegno del top management: il top management riconosce le preoccupazioni e i problemi connessi alle prestazioni umane e cerca di risolverli (Wreathall, 2006). Pertanto si evince che la sicurezza diventa un valore organizzativo fondamentale, più che una priorità momentanea (Costella, 2009);
- Aumentare la flessibilità: un assunto di base della RE è che gli errori umani sono inevitabili a causa delle pressioni individuali e organizzative (ad esempio, carico di lavoro e costi) (Rasmussen, 1994). Pertanto la progettazione del sistema di lavoro deve essere flessibile, riconoscendo che la gestione della variabilità è importante quanto la riduzione della variabilità stessa. In realtà, la progettazione dovrebbe sostenere le naturali strategie umane per affrontare nel modo migliore i pericoli, piuttosto che imporre una particolare strategia. Questo significa che nella progettazione dei posti di lavoro dovrebbe essere specificato solo quello che è assolutamente essenziale (Clegg, 2000). Ciò implica di studiare ciò che le persone effettivamente fanno e poi valutare se è possibile sostenere le loro azioni attraverso la progettazione (Hollnagel e Woods, 2005). Wreathall (2006) sottolinea, inoltre, che la flessibilità richiede che le persone a livello operativo (in particolare le autorità di vigilanza di primo livello) debbano essere in grado di prendere decisioni importanti, senza dover attendere inutilmente per le istruzioni di gestione [48];
- Imparare sia dagli incidenti che dal lavoro normale (apprendimento): la RE sottolinea la necessità di comprendere dal lavoro normale piuttosto che imparare dagli incidenti, al fine di apprendere e diffondere le strategie di lavoro di successo. Tuttavia, l'apprendimento richiede un ambiente organizzativo che sia in grado di incoraggiare la comunicazione degli incidenti e riconoscere le strategie di adattamento, anche se non tollererà i comportamenti colposi (Wreathall, 2006). Inoltre, l'apprendimento deve prendere in considerazione il modo in cui le procedure vengono implementate. In realtà, monitorare l'attuazione delle procedure dovrebbe essere considerata importante quanto l’elaborazione delle procedure stesse, in quanto ciò può contribuire a ridurre il divario tra il lavoro come

immaginato dai manager e il lavoro come interpretato dagli operatori. Quanto più piccolo risulterà questo divario, tanto maggiore sarà la prova che l'apprendimento sta avvenendo (Wreathall, 2006; Hale e Heijer, 2006);

- Essere consapevoli dello stato del sistema (consapevolezza): questo principio implica che gli attori devono essere consapevoli sia del loro stato attuale che dello stato delle difese del sistema. Questo è fondamentale per anticipare i futuri cambiamenti ambientali che possono influenzare la capacità di funzionamento del sistema (Resilience Network Engineering, 2008). La consapevolezza è importante anche per la valutazione dei trade - off tra la produzione e la sicurezza (Hale e Heijer, 2006; Hollnagel e Woods, 2005). Rasmussen (1994) suggerisce due grandi approcci per l'attuazione di questo principio: la misurazione delle performance basata su indicatori proattivi e il disegno dei confini visibili della performance;
- La cultura della segnalazione: supporta la segnalazione di problemi e di questioni attraverso l'organizzazione o il sistema, ma non tollera i comportamenti colposi. Senza una cultura della segnalazione, la disponibilità del personale a segnalare i problemi sarebbe piuttosto bassa;
- La preparazione: l'organizzazione e il sistema prevedono attivamente i problemi dell'azione umana nei sistemi uomo - macchina e si preparano ad affrontarli;
- La minimizzazione del fallimento: il fallimento è uno stato che non soddisfa un obiettivo desiderato o previsto, o che potenzialmente crea una situazione di pericolo per le persone (ad esempio, rilascio di gas tossici) e danni alle apparecchiature (ad esempio, perdite e rotture). Pertanto tale principio consiste nell'evitare che qualcosa di brutto possa verificarsi, mediante l'impiego di misure preventive, l'utilizzo corretto dei dispositivi di protezione ed una adeguata gestione della sicurezza;
- La diagnosi precoce: quando le misure preventive non possono impedire che un guasto si verifichi, entra in gioco il principio della diagnosi precoce. La più dannosa interruzione e la più difficile situazione che si può verificare è quando un disturbo non viene rilevato in tempo, in quanto nessuna azione correttiva verrà intrapresa per tutti gli errori che rimangono inosservati (Van

Der Schaaf e Kanse, 2000). Pertanto la diagnosi precoce diviene fondamentale per ogni forma di disturbo e soprattutto rappresenta un fattore determinante della Resilienza (Sheffi, 2005 e 2007) [50];

- La controllabilità: è la capacità del sistema di raggiungere un target specifico (Rosenbrock, 1970). Essa è determinata da quanto efficacemente il sistema possa essere controllato. Un processo è definito controllabile se i parametri di uscita da controllare possono essere portati al valore target in un lasso di tempo accettabile in seguito alla deviazione di un ingresso inaspettato. Pertanto esiste una differenza sostanziale tra flessibilità e controllabilità: la flessibilità corrisponde a stati stazionari, mentre la controllabilità si riferisce a stati dinamici. L'obiettivo di tale principio è quello di progettare un processo più controllabile. Mentre il principio di flessibilità consente ai processi di operare in varie condizioni, quello di controllabilità permette di cambiare il funzionamento da una condizione all'altra: quindi sia la flessibilità che la controllabilità sono necessari per poter realizzare la strategia di Resilienza;
- La limitazione degli effetti: nonostante la probabilità di guasto sia piuttosto bassa, il momento preciso in cui un guasto può verificarsi non può essere conosciuto o previsto. Se non è possibile escludere i guasti o evitare gli incidenti, è importante limitarne gli effetti. Infatti più gravi sono le conseguenze, tanto più tempo sarà richiesto per implementare le azioni di recupero. Tale principio, pertanto, consiste nell'utilizzare le corrette misure di salvaguardia al fine di limitare le conseguenze di un evento minaccioso;
- I controlli e le procedure amministrative: lo stato sconvolto derivante da un evento imprevisto può essere minimizzato grazie all'attuazione di aspetti progettuali quali la flessibilità e la controllabilità. Tuttavia, per alcuni disturbi imprevisti, una soluzione sotto forma di un disegno resiliente può essere impraticabile; inoltre, non tutti i rischi possono essere previsti. Pertanto, il principio di Resilienza dovrebbe coinvolgere i sistemi di gestione attraverso controlli e procedure amministrativi. I controlli amministrativi, quali ad esempio la formazione e le procedure operative standard, rappresentano un

valido strumento per prevenire e recuperare da deviazioni di processo e di rilascio accidentale.

Oltre a questi principi, un altro concetto merita di essere evidenziato: la proattività. La proattività consiste nell'anticipare i problemi, i bisogni o i cambiamenti, e conduce ad azioni che alterano direttamente l'ambiente circostante. In termini di sicurezza, la proattività si riferisce ad anticipare i rischi e le misure di controllo, in modo da interrompere l'evoluzione degli incidenti. Naturalmente, i principi della RE presentati si sovrappongono in alcuni casi con i principi di altri paradigmi di gestione della sicurezza e sono pienamente in linea con i principi generali per la progettazione dei sistemi socio - tecnici stabiliti da studi precedenti, come quello di Clegg (2000). Ad esempio, vi è una sovrapposizione con la prospettiva di cultura della sicurezza espressa da Reason (1997), dal momento che è d'accordo con la posizione che la cultura della sicurezza possa essere progettata e gestita e dovrebbe comprendere quattro sottocomponenti: una cultura di riferimento, una cultura just, una cultura flessibile e una cultura dell'apprendimento. Sulla base di quanto è stato detto finora, si intuisce che la RE è diventato un campo importante per la gestione della sicurezza tanto nei sistemi socio - tecnici quanto in quelli complessi. Notevoli sforzi sono stati fatti negli ultimi anni per specificare le caratteristiche di base delle organizzazioni o dei sistemi resilienti. Oltre ai principi della RE, è possibile elencare una serie di elementi che servono a migliorare il livello di sicurezza nei sistemi:

- L'auto - organizzazione: le applicazioni di più entità indipendenti tra loro che sono generalmente fatte con una conoscenza limitata del loro ambiente e che localmente interagiscono (direttamente o indirettamente) per generare un risultato. Entità indipendenti, di solito, lavorano in modo decentrato (Serugendo, 2009). Nei sistemi di auto - organizzazione, l'ordine deriva dalle azioni di agenti interdipendenti che si scambiano informazioni, che intraprendono azioni e che continuamente si adeguano alle azioni degli altri, piuttosto che dall'imposizione di un piano generale di un'autorità centrale (Plowman, 2007). I sistemi di auto - organizzazione di solito superano un ampio range di modifiche e di guasti (Serugendo, 2009);

- Il lavoro di squadra: è uno dei più importanti fattori per il raggiungimento di risultati positivi nei diversi contesti organizzativi. Comporta anche una maggiore adattabilità e produttività, più alta di quella che potrebbe essere offerta da qualsiasi individuo, aumentando nel contempo la soddisfazione sul luogo di lavoro e il mantenimento del personale (Xyrichis e Ream, 2008). Recenti indagini hanno evidenziato il ruolo del lavoro di squadra nelle diverse aree della sanità. Le industrie ad alto rischio, come l'aviazione e l'industria nucleare, hanno da tempo riconosciuto l'importanza del lavoro di squadra per migliorarne il livello di sicurezza (Burtscher and Manser, 2012). Un assunto di base della RE è che gli errori umani sono inevitabili, a causa delle pressioni individuali ed organizzative (Rasmussen, 1994). I componenti che hanno un'influenza rilevante sul lavoro di squadra sono la leadership, la comunicazione, il sostegno reciproco e il monitoraggio della situazione (Battles e King, 2010). Quando il carico di lavoro del sistema è elevato, il lavoro di squadra è in grado di diminuire le pressioni individuali ed organizzative, mediante il sostegno e l'assistenza reciproci: in questo modo gli errori umani diminuiscono e l'affidabilità del sistema aumenta. Di conseguenza, il lavoro di squadra comporta un incremento del livello di sicurezza;
- La ridondanza: viene generalmente definita come l'assenza di componenti critici, il cui guasto causerebbe il collasso dell'intera struttura (Frangopol e Curley, 1987). Inoltre, la ridondanza è l'esistenza di vie alternative o la capacità in eccesso in condizioni normali, da utilizzare nel momento in cui i componenti non sono più disponibili (Kalungi e Tanyimboh, 2003). Essa esiste in un sistema uomo - macchina nel momento in cui due o più operatori (persone) sono preoccupati per il completamento di una specifica funzione richiesta e hanno accesso a informazioni relative a tale funzione. La ridondanza umana è una caratteristica chiave della progettazione delle organizzazioni o dei sistemi che presentano standard piuttosto elevati in termini di prestazioni nell'ambito della sicurezza (Clarke, 2005). La misura degli elementi, sistemi e altre unità di analisi, che soddisfano i requisiti funzionali in seguito al verificarsi di perturbazioni, il degrado o perdita di

funzionalità, le risorse umane e la ridondanza organizzativa rientrano in questa categoria (Storseth, 2009) [51];

- Fault - tolerant: un sistema fault - tolerant è uno dei metodi che permette di aumentare la sicurezza e l'affidabilità del sistema. Lo scopo principale di un sistema fault - tolerant è mantenere la prestazione specifica di un sistema in presenza di errori (Ling e Duan, 2010). I sistemi critici per la sicurezza, che ad esempio vengono impiegati in aeronautica e nello spazio, vengono progettati in modo da poter funzionare anche in presenza di guasti di uno o più componenti. Così, tali sistemi devono avere la capacità di adattarsi a situazioni estreme. Questi tipi di sistemi adattabili sono noti come sistemi fault - tolerant (Dominguez e Garcia, 2008): pertanto, l'elemento di fault - tolerance può risultare fondamentale per i sistemi resilienti.

2.4 Approcci qualitativi e quantitativi della Resilienza

Si cercherà a questo punto di comprendere come il processo di Resilienza ingegneristica possa contribuire all'incremento della sicurezza in un'organizzazione qualsiasi. La premessa fondamentale è che i metodi di valutazione del rischio di un processo sono importanti e pensare in termini di scenari avviati da un disturbo è indispensabile. Vari strumenti sono stati sviluppati a riguardo; gli strumenti di maggior successo sono stati: Hazard and Operability study (HazOp) e Failure Mode and Effect Analysis (FMEA) [53]. L'HazOp ha lo scopo di esaminare gli ambienti di lavoro e identificare i pericoli a cui tali ambienti espongano i lavoratori; FMEA invece è una metodologia che viene utilizzata principalmente per analizzare le modalità di guasto di un processo, di un prodotto o di un sistema. Applicati per molti anni per descrivere e analizzare gli scenari sono stati gli alberi degli errori e degli eventi, che hanno mostrato anche il ruolo funzionale delle barriere di prevenzione e protezione. Un'analisi completa del rischio è piuttosto complessa, a causa della grande incertezza non solo dovuta alla mancanza di dati sufficienti, ma anche per la grande variabilità nel comportamento umano. L'analisi dei rischi risulta ancora più difficile se si vuole includere gli stati anomali e gli stati non stazionari, come le partenze e le fermate, e gli effetti di decisioni operative errate. Infine, le analisi di

rischio standard non tengono conto delle dinamiche delle variazioni di rischio dalla presenza di stati anomali o modifiche nell'esposizione del numero di persone alle attività pericolose. Così, da un lato, date le rimanenze di materiali pericolosi, le conseguenze fisiche di perdita di contenimento e le conseguenti esplosioni, incendi o dispersioni tossiche possono essere determinate per la maggior parte dei casi. Dall'altro lato però, a causa dell'identificazione dei tanti scenari possibili che possono portare ad una perdita di contenimento e la loro probabilità, in particolare quando includono le influenze di fattori umani, l'incertezza oscura il piano. A tal proposito Hollnagel pone la base fondamentale di un tale approccio per le organizzazioni, riferendosi in particolar modo ai sistemi socio – tecnici [54]. Dapprima considera la combinazione lineare di guasto di un componente in un sistema scomponibile, consentendo la stima della probabilità di incidente; poi, al contrario, osserva che nei sistemi socio - tecnici tale decomposizione non funziona, perché i rischi possono emergere, compresi quelli intrattabili. La variabilità delle prestazioni umane provoca un incidente per caso; quest'ultima è una forma di non linearità casuale. Non esiste una soluzione pratica e, pertanto, bisogna fare i conti con disturbi imprevisti, deviazioni ed errori derivanti dalle azioni umane. Alcuni cercano una soluzione in un approccio di sistema. Venkatasubramanian ha sottolineato un approccio di sistema nel contesto delle operazioni dell'industria di processo. Più in generale, Leveson ha aggiornato i contenuti dei suoi precedenti lavori nel testo "Engineering a Safer World, Systems Thinking Applied to Safety". L'attuale complessità del sistema quotidiano, i ruoli dei computer e dei software, il modo in cui le organizzazioni funzionano, richiedono un approccio più globale alla sicurezza. Si deve pertanto necessariamente sviluppare una visione integrale che coinvolga la progettazione, l'operatività e le singole fasi dei processi di manutenzione tenendo conto del pilastro gerarchico delle funzioni e delle responsabilità attraverso i vari livelli di gestione. Successivamente, si devono definire i rischi del sistema, i vincoli di sicurezza e la struttura di controllo. A tal proposito sono stati sviluppati nuovi strumenti quali: System - Theoretic Accident Model and Processes (STAMP), Causal Analysis using System Theory (CAST) basato su STAMP and System - Theoretic Process Analysis (STPA). Steen e Aven, invece, forniscono un resoconto chiaro di conformità e sottolineano la differenza tra analisi di Resilienza e valutazione del rischio [55].

Mentre in ottica tradizionale al rischio viene sempre attribuita una distribuzione di probabilità, esso può essere anche espresso come funzione dell'incertezza associata alla possibilità che un certo evento A si verifichi e alle sue possibili implicazioni C: tale caratterizzazione del rischio viene indicata come (A, C, U) perspective [53].

Riferendosi a quest'ultima, s'introducono i seguenti fattori:

I. A = initiating event;
II. P = occurrence probability of A;
III. C = possible consequences of A;
IV. U = uncertainty about and severity of C, given the occurrence of A;
V. K = assumptions.

La vulnerabilità di un sistema (contrario di robustezza) può essere espressa come funzione di tali parametri:

$$V = f (C, P, U, K \mid A).$$

Adottando la stessa notazione, la Resilienza è esprimibile come:

$$R = f (C, P, U, K \mid \text{any A, including new types of A})$$

Tale tipo di scrittura evidenzia la differenza che intercorre tra i due modi di concepire la sicurezza, racchiusa nell'evento iniziale: mentre la vulnerabilità e la robustezza sono collegate alle conseguenze incerte di un particolare evento, la Resilienza è funzione di un qualsiasi tipo evento, anche completamente imprevisto.

Per chiarire tale aspetto, si consideri la vulnerabilità di un individuo nei confronti di un particolare tipo di virus (l'evento A è fissato) [56]: essa rappresenta le possibili conseguenze, incerte, derivanti da tale esposizione, esprimibili in termini probabilistici; da sottolineare che la vulnerabilità è funzione delle condizioni dell'entità a cui si riferisce. Diversamente, la Resilienza è una proprietà assoluta, ovvero indipendente dalle conseguenze di un particolare evento.

Si tenga presente però che è necessario, ai fini della completezza della trattazione, fissare dei vincoli (K) sull'evento A, rispetto al quale viene valutata la Resilienza di un sistema.

L'analisi di Resilienza sarà quindi molto impegnativa. Il grado in cui un processo è reso resiliente, dipende non solo dalla grandezza delle possibili minacce e dalla propensione di entrare in uno stato sconvolto data una minaccia, ma anche dalla capacità di evitare un tale stato e di correggere il suo decorso o guidarlo fuori da esso.

È stato sviluppato in seguito un metodo per valutare i sistemi di gestione della salute e della sicurezza (MAHS), introducendo due caratteristiche innovative:

- Considerare i tre principali metodi di controllo di sicurezza e salute (HS): approccio strutturale, operazionale e prestazionale;
- Enfatizzare la prospettiva della Resilienza ingegneristica su HS, prendendo in considerazione i seguenti quattro principi: la flessibilità, l'apprendimento, la consapevolezza e l'impegno del top management. Tali principi sono alla base di sette criteri di valutazione, che a loro volta sono divisi in articoli. Gli articoli sono suddivisi in dichiarazioni che identificano i requisiti che dovrebbero essere valutati sulla base di interviste, analisi di documenti ed osservazioni dirette. All'interno dei 112 requisiti proposti, 38 hanno chiari legami con almeno uno dei quattro principi della Resilienza adottati. I requisiti rimanenti si basano su ipotesi tradizionali alla base delle cosiddette migliori pratiche di gestione HS. I risultati della valutazione per ciascun elemento sono espressi con un punteggio su una scala costruita in base ai requisiti stabiliti, compresa tra 0% e 100 %. Il punteggio specifico all'interno di tale scala è ottenuto utilizzando specifiche tabelle [57].

Essendo l'improvvisazione un elemento molto importante dei sistemi resilienti, sono state proposte le seguenti metodologie: Rasmussen's Risk Management Framework e Accimap Methodology. Esse vengono impiegate per esaminare i fattori che influenzano l'improvvisazione in situazioni critiche per la sicurezza. Le Impromaps (ossia le Accimaps dell'improvvisazione) sono state utilizzate per determinare se i

fattori, identificati come elementi che influenzano l'improvvisazione in determinate circostanze, rispettano o meno le previsioni fatte dal Rasmussen's Risk Management Framework. I risultati indicano che l'improvvisazione è un fenomeno dei sistemi e supportano l'utilizzo del Framework e di Impromaps come una metodologia di analisi per l'esame degli incidenti di improvvisazione. La metodologia ha permesso l'identificazione di fattori di tutti i livelli dei diversi sistemi ed è stata in grado di descrivere le relazioni tra fattori interni ed esterni del sistema [58], [59].

È stata anche proposta una nuova versione della RE definita RE integrata (IRE). La IRE considera oltre all'apprendimento, alla consapevolezza, alla preparazione e alla flessibilità, che sono i fattori valutati dalla RE, anche il lavoro di squadra, l'auto - organizzazione, la ridondanza e il fault - tolerant [60]. Questo metodo valuta la performance della IRE in un generico impianto con i dati ottenuti da questionari e l'approccio "data envelopment analysis" (DEA). Inoltre, i risultati della RE e della IRE vengono confrontati e discussi. Tali risultati mostrano che, anche se vi è una forte correlazione tra i risultati dell'analisi DEA nei due quadri, i punteggi medi di efficienza nella IRE sono leggermente superiori a quelli in RE [61], [47].

Sono state proposte anche numerose metriche che specificamente valutano la Resilienza nell'ambito della psicologia. Il Baruth Protective Factors Inventory (BPFI) si basa sulla teoria che ci sono quattro fattori che contribuiscono alla Resilienza: la personalità adattabile, l'ambiente favorevole, meno stress e le esperienze di compensazione. Quattro elementi rappresentativi di ciascuno di questi fattori sono ulteriormente identificati e una tabella di 16 elementi è valutata con una scala di tipo Likert (1-5), la quale viene usata per produrre un punteggio complessivo della Resilienza compreso tra 16 e 80 [62]. La scala Connor - Davidson Resilience (CD - RISC) segue un approccio simile, in cui sono elencati 25 elementi, ciascuno valutato su una scala a 5 punti (0-4) con punteggi totali che vanno da 0 a 100 [63]. La scala Brief Resilience (BRS), invece, fornisce una scala affidabile per il concetto unitario fondamentale di Resilienza. BRS comprende sei elementi per valutare la capacità di riprendersi e recuperare dallo stress, e ogni valutazione viene fatta su una scala a 5 punti (1-5). Attoh e Okine hanno, a loro volta, proposto un indice di Resilienza per l'infrastruttura urbana utilizzando una struttura di funzione di opinione; Li e Lence

hanno proposto una formula dell'indice di Resilienza, come rapporto tra la probabilità di guasto e il ripristino del sistema. Omer ha proposto un approccio quantitativo per definire e misurare la Resilienza di un sistema di cavi di telecomunicazione, definendo la Resilienza di base come il rapporto tra la distribuzione del valore della rete dopo un'interruzione e la distribuzione del valore della rete prima dell'interruzione, dove la distribuzione del valore è la quantità di informazioni che deve essere trasmessa dalla rete. Reed delinea una metodologia per valutare la Resilienza ingegneristica e l'interdipendenza per i sottosistemi di un'infrastruttura di rete multi - sistema per gli eventi naturali pericolosi. La Resilienza è misurata come l'area sotto la curva qualità Q(t), che assume un valore di 1 quando è completamente funzionante e un valore nullo quando risulta inutilizzabile [64]. Tierney e Bruneau definiscono la Resilienza delle catastrofi come la capacità delle unità sociali di attenuare i rischi, di contenere l'effetto dei disastri quando si verificano e di svolgere le attività di recupero in modo che minimizzino la disgregazione sociale e attenuino gli effetti dei disastri futuri.
Altri autori hanno invece delineato una serie di metriche della Resilienza, applicabili nell'ambito delle reti. A riguardo, Najjar e Gaudiot hanno proposto la Resilienza di rete e la Resilienza di rete relativa come due misure della tolleranza dell'errore di rete in un sistema multi - computer. La tolleranza dell'errore di rete è tradizionalmente espressa come il livello di rete e non considera il numero totale di nodi nel sistema e la probabilità di una disconnessione. La Resilienza di rete NR(p) è una misura che fornisce il limite superiore al numero di errori possibili del nodo ed è definito come il numero massimo di errori del nodo che può essere accettato, mentre la rete rimane connessa con una probabilità pari a (1-p). La misura della Resilienza della rete relativa RNR(p) viene definita come NR(p)/N, dove N è il numero di nodi nella rete. Whitson e Ramirez - Marquez propongono un approccio basato sulla simulazione Monte - Carlo per calcolare la Resilienza di una rete, che è un composto della sua capacità di fornire il servizio nonostante il guasto esterno e il tempo per poter ripristinare il servizio [65].

Dalziell e McManus propongono un approccio che richiede l'identificazione dei "Key Performance Indicators" (KPI). Tali indicatori sono le misure concrete con cui l'organizzazione può monitorare le prestazioni rispetto agli obiettivi dichiarati, al fine

di fornire una misura della Resilienza organizzativa. La variazione nei KPI selezionati viene tracciata rispetto al tempo, dall'inizio dell'impatto fino a che il cambiamento diviene nullo. La gravità delle conseguenze (o variazione massima nei KPI) indica la vulnerabilità del sistema, mentre il tempo di recupero denota la capacità di adattamento del sistema.

Henry e Ramirez-Marquez [66] forniscono una formulazione matematica per calcolare la Resilienza di un sistema, partendo da una rappresentazione grafica. Siano:

a) S0: stato iniziale del sistema;
b) Sd: stato conseguente l'evento indesiderato (di natura interna o esterna);
c) Sf: stato conseguente il ripristino del sistema.

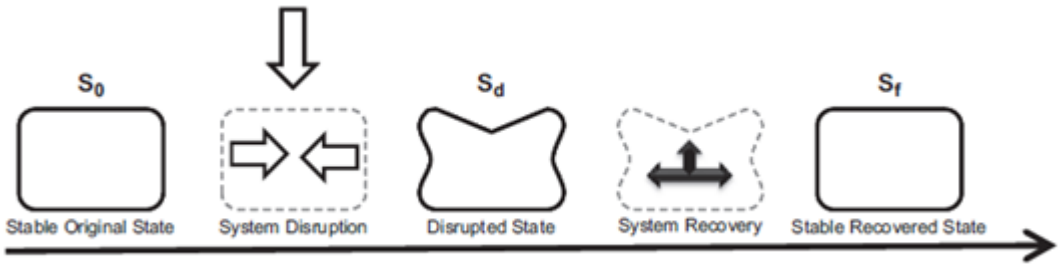

Figura 7 Transizione dello stato nel sistema della Resilienza

E' possibile schematizzare l'evoluzione del sistema attraverso il seguente grafico, che mostra un ipotetico andamento (ad esempio, lineare) della funzione F(t) rappresentante la performance del sistema, una grandezza caratteristica (ad esempio, l'affidabilità) o un insieme di queste, essendo la Resilienza frutto di molteplici fattori: F(t) deve poter essere misurata.

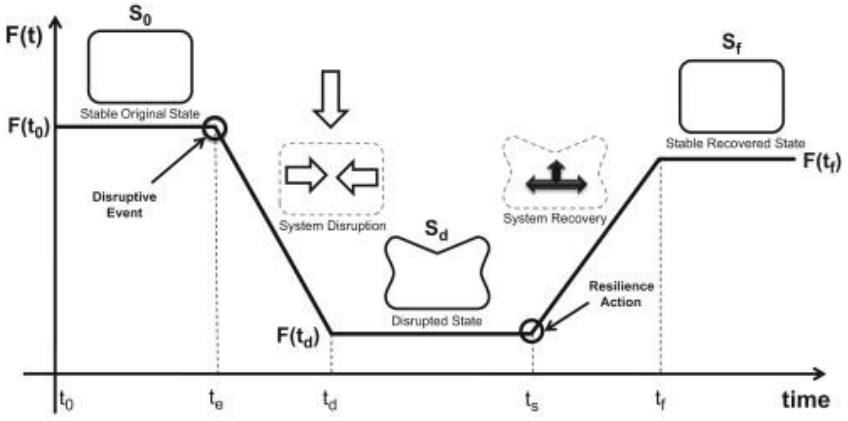

Figura 8 Evoluzione dello stato di un sistema resiliente in seguito ad una perturbazione [66].

Il sistema permane nello stato iniziale $\mathbf{S_0}$, caratterizzato da un livello di performance costante e pari a $\mathbf{F(t_0)}$, fino a quando viene perturbato all'istante $\mathbf{t_e}$: la sua configurazione si modifica progressivamente, culminando nello stato $\mathbf{S_d}$ all'istante $\mathbf{t_d}$, a cui corrisponde un valore rappresentativo pari a $\mathbf{F(t_d)}$. Attraverso specifiche azioni - che dipendono da quanto il sistema è resiliente - ha luogo la fase di ripristino/recupero all'istante $\mathbf{t_s}$ che termina una volta che il sistema ha raggiunto lo stato $\mathbf{S_f}$ (all'istante a $\mathbf{t_f}$), caratterizzato da un valore di performance $\mathbf{F(t_f)}$, che viene mantenuto tale. Da notare che quest'ultimo stato non necessariamente corrisponde a quello iniziale (ad esempio come riportato in figura, esso può essere inferiore a S_0).

Perché abbia luogo un cambiamento di stato, l'evento che lo innesca deve essere tale da modificare la cifra di merito F(t): per cui, detto $E=\{e_1,..e_n\}$ l'insieme di tutti gli eventi possibili, il sottoinsieme di eventi che determinano la transizione di stato sopra descritta è $D=\{e_j \in E \mid F(t_d|e_j) < F(t_0)\}$. L'azione di recupero (resilience action) deve essere tale da incrementare il valore di F(t) nell'intervallo compreso tra t_s e t_f .

La Resilienza del sistema Я(t) viene espressa come rapporto tra il recupero conseguito all'istante t e le perdite subite ad un istante precedente(t_d):

$$Я(t) = \text{Recovery}(t) / \text{Loss}(t_d)$$

che, in termini di F(t), diventa:

$$Я_F(t_r|e_j) = \frac{F(t_r|e_j) - F(t_d|e_j)}{F(t_0) - F(t_d|e_j)} \quad \forall e_j \in D$$

dove t_r è un istante di tempo appartenente all'intervallo (t_d, t_f).

Tale formulazione rispecchia perfettamente il significato basilare del concetto di Resilienza ("rimbalzare indietro"):

- se $F(t_r|e_j)=F(t_d|e_j)$, che corrisponde al caso in cui il sistema non è stato ripristinato, $Я(t) = 0$ e ciò è riconducibile all'assenza o all'inefficacia dell'azione di recupero;

- se invece $F(t_r|e_j) =F(t_0)$, il sistema è pienamente resiliente ($Я(t) = 1$) in quanto si è riportato allo stato iniziale. Da sottolineare, come già fatto in precedenza, che $F(t_0)$ non rappresenta un limite superiore per $F(t_r|e_j)$: può infatti verificarsi $F(t_r|e_j)>F(t_0)$ che corrisponde alla situazione in cui il sistema ha raggiunto una configurazione migliore del suo stato iniziale;

- per $F(t_d|e_j)=F(t_0)$, la funzione non è definita: tuttavia per le ipotesi fatte circa gli eventi considerati (sottoinsieme D), tale condizione non si verifica mai.

L'evoluzione di stato rappresentata in grafico è scandita da quattro fasi, che rappresentano grandezze caratteristiche del sistema in esame e della Resilienza stessa [67]:

1. In assenza di eventi indesiderati (intervallo $[t_0; t_e]$), il funzionamento del sistema dipende dal suo grado di affidabilità (***Reliability***);

2. L'impatto che l'evento e_j ha sul sistema dipende da quanto questo sia vulnerabile (***Vulnerability***);

3. L’attuazione di misure mitigative, mirate cioè a ridurre gli effetti dell’evento indesiderato, garantisce un certo margine di “sopravvivenza” al sistema (***Survivability***);

4. La ***Recoverability*** esprime la rapidità con cui il sistema, a seguito della perturbazione, riesce a recuperare una configurazione di stabilità.

Alcuni autori, tra i quali Shirali et al. [68], propongono un set di indicatori per stimare il potenziale della Resilienza in un dato sistema in maniera qualitativa:

1. ***Top Management Commitment*****:** la sicurezza è il valore assoluto e riveste un’importanza superiore o pari a quella degli altri obiettivi dell'organizzazione;

2. ***Just Culture*****:** creazione di un clima che incoraggia i dipendenti a segnalare questioni legate alla sicurezza;

3. ***Learning Culture*****:** delinea la capacità di apprendimento dalla pratica quotidiana, non solo dagli eventi passati;

4. ***Awareness and Opacity*****:** ciascun dipendente deve conoscere lo stato attuale del sistema e delle misure predisposte a difesa dell’impianto;

5. ***Preparedness*****:** il sistema ha un’impostazione proattiva, essendo in grado di anticipare le possibili minacce e prepararsi ad affrontarle;

6. ***Flexibility*****:** denota la capacità del sistema a ristrutturarsi per accompagnare il cambiamento e adattarsi alla variabilità.

È importante precisare che tale valutazione avviene utilizzando PCA e l’approccio tassonomico numerico (NT). A tal proposito è stato progettato un questionario per misurare questi sei indicatori; tale questionario è stato successivamente consegnato ai dipendenti, ciascuno dei quali ha fornito una valutazione di tipo numerico. I risultati rappresentano, pertanto, un supporto per la valutazione quantitativa di RE ad opera dei responsabili dell’impianto [68].

Bruneau invece fornisce una base forte per lo sviluppo di misure quantitative, le quali possono essere applicate alla Resilienza in un contesto più generale: tale base è rappresentata dal cosiddetto "resilience triangle". Alla base di questo nuovo strumento vi è il concetto di Resilienza connessa a eventi disastrosi, il quale è caratterizzato dai seguenti fattori: robustezza, rapidità, intraprendenza e ridondanza. In base a tali elementi, matematicamente la Resilienza viene valutata in funzione della qualità dell'infrastruttura del sistema in un certo arco temporale [69].

Anche Francis e Bekera [70] propongono il cosiddetto "triangolo della Resilienza" come riferimento per valutare la Resilienza di un sistema:

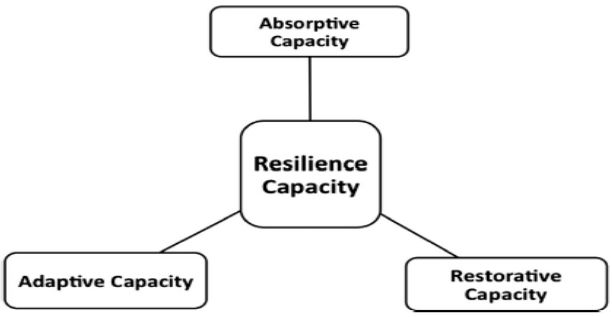

Figura 9 Resilience triangle [70].

a) Absorptive Capacity

Esprime la misura in cui il sistema è in grado di assorbire l'impatto di una perturbazioni esterna e di minimizzarlo, con uno sforzo contenuto [70]. Si capisce che tale abilità dipende da come esso è configurato e gestito a livello organizzativo, procedurale e operativo: robustezza e ridondanza possono essere considerate grandezze indicative di tale capacità. Un esempio in cui si concretizza tale proprietà sistemica potrebbe essere la dotazione, in un sistema produttivo, di una capacità di buffer che permetta di rimediare ad eventuali blocchi della linea produttiva.

b) Adaptive Capacity

Data la natura dinamica dei sistemi complessi, tale abilità indica fino a che punto il sistema è in grado di modificare la propria configurazione in risposta ad un evento imprevisto, adattandosi ad esso in maniera graduale e flessibile, senza che ne consegua un calo di performance o un declino delle sue funzionalità. E' una proprietà strettamente legata all'evento in questione. In tale ottica, notevole importanza assume la capacità di previsione (*Anticipation*) di ciò che Kaplan [72] definisce *"risk triplet"* (hazard, exposure, vulnerability) in modo che il sistema possa prepararsi ad esso in maniera adeguata e contrastarlo efficacemente.

c) Recovery/Restorative Capacity

Tale proprietà è generalmente espressa come la velocità con cui il sistema è in grado di ripristinare il normale funzionamento e di riportarsi alla sua configurazione iniziale, successivamente all'evento di danno: pertanto, essa va valutata rispetto ad un predeterminato livello di servizio.

Pasman et al. [73] conseguono un livello di dettaglio maggiore, esplicitando i principi che rivestono un ruolo cruciale nel determinare il livello di Resilienza di un sistema.

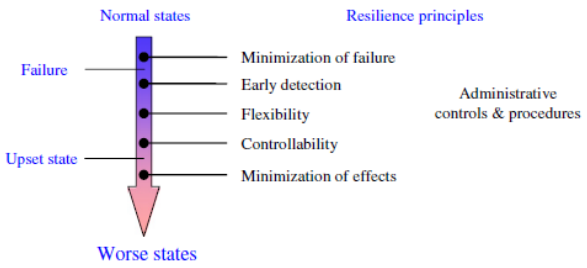

Figura 10 Resilience principles [73].

1. *Minimization of failure* Dal momento che un guasto configura una condizione di potenziale pericolo sia per le persone (ad esempio, il rilascio di sostanze tossiche) sia per le attrezzature (ad esempio, la rottura di un

dispositivo), il principio di minimizzazione ha l'obiettivo di prevenire l'occorrenza di tale situazione attraverso l'adozione di misure preventive, quali ad esempio una progettazione sicura dei processi, un utilizzo adeguato dei dispositivi di protezione e una corretta gestione della sicurezza.

2. *Early detection* Qualora le misure preventive, designate in base al principio precedente, non risultassero sufficienti per impedire l'occorrenza del guasto, risulta fondamentale essere in grado di individuarlo prima che sia troppo tardi, così da avviare efficacemente la fase di ripristino del sistema.

3. *Flexibility* Un processo è flessibile quando, al variare degli input all'interno di un intervallo di accettabilità predefinito, l'output risponde alle specifiche inizialmente stabilite: ad esempio, un impianto flessibile è quello progettato in modo da poter realizzare lo stesso output a partire da diversi tipi di materie prime. Nell'ottica della RE, aumentare la flessibilità di un processo permette sia di assecondarne le fluttuazioni in ingresso, sia di tollerarne interruzioni significative, senza mai violare i requisiti specificati.
4. *Controllability* E' la capacità di un sistema a raggiungere uno specifico stato e dipende da come esso possa essere controllato, attraverso meccanismi di feedback o di feed-forward: un processo si dice controllabile se i parametri di output, deviati a seguito di un ingresso imprevisto, possono essere regolati in un tempo accettabile. Mentre la flessibilità si riferisce a stati stazionari, la controllabilità riguarda stati dinamici: la prima consente ai processi di operare sotto varie condizioni, la seconda permette di cambiare il funzionamento nel passaggio da una condizione all'altra.

5. *Limitation of effects* Nel momento in cui il guasto non può essere evitato e non è possibile scongiurare l'incidente, si rende necessario l'impiego di dispositivi di protezione o l'attuazione di misure mitigative per limitarne le conseguenze.

6. *Administrative controls and procedures* Talvolta i principi appena visti non sono sufficienti a identificare eventi inattesi: pertanto la RE deve coinvolgere

anche il management attraverso controlli e procedure amministrative (ACP). La formazione e la conformità a standard operativi rappresentano uno strumento di salvaguardia per prevenire o affrontare le deviazioni di un processo dalla normalità.

L'analisi fin qui svolta effettuata, dalla Sicurezza (Capitolo I) alla Resilienza, nonché il loro punto di contatto, ha come fine migliorare l'intero processo di gestione, efficienza di un sistema complesso quale quello industriale. Si sono visti gli approcci alla sicurezza *tradizionali e moderni*, quest'ultimi in grado di superare la staticità della sequenza "identificazione – valutazione – azione – controllo".

Nel ricercare le cause di un generico evento non è sufficiente limitarsi a considerare soltanto ciò che è strettamente correlato - e quindi "tangibile" e facilmente intuibile - ad esso, bensì il campo di indagine deve essere ampliato fino ad includere la totalità dei fattori, sia interni che esterni, con cui il sistema si trova ad interagire nel corso del suo normale funzionamento, al fine di coglierne gli aspetti dinamici e complessi.

"It is proposed that the usual causal analysis tools should be used to analyse the incident sequence and causal factors that are more immediate to the incident. Key causal factors can then be further analysed using tools designed to model dynamic complexity" [75].

Bisogna quindi adottare una metodologia che consenta uno screening olistico e minuzioso del sistema in esame: nel presente lavoro, sono stati utilizzati i concetti tipici della System Dynamics per i quali si rimandi al prossimo paragrafo.

2.5 Utilizzo dei modelli simulativi per la sicurezza degli impianti industriali e la RE

La gestione, lo stoccaggio, l'utilizzo di sostanze potenzialmente pericolose, così come l'esecuzione di procedure particolarmente rischiose, richiedono l'adempimento ad elevati standard di sicurezza, conseguibili mediante una adeguata progettazione

dei luoghi e dei processi, un'efficiente gestione e controllo dell'impianto, affinché siano scongiurati conseguenze quali fatalità o infortuni, rilascio di sostanze tossiche, perdite economiche e produttive, ecc.

Non essendo possibile eliminare la pericolosità intrinseca di tali elementi, le strategie organizzative e gli studi di ricerca devono puntare a ridurre l'occorrenza e l'impatto di tali eventi fino a raggiungere un valore accettabile: identificati i top event.

L'utilizzo di software simulativi per l'analisi e la valutazione degli scenari incidentali può fungere da supporto per decidere quali azioni intraprendere al fine di scongiurarne le conseguenze (riprogettare l'impianto in fase di pianificazione, scegliere i sistemi di mitigazione più adatti, definire procedure di sicurezza, ecc) [76]; ovviamente, tali strumenti non possono sostituirsi all'esperienza maturata nel corso degli anni ma ne costituiscono un completamento.

La simulazione è quel processo che consente di riprodurre artificialmente un dato fenomeno o sistema reale ed evidenziarne taluni aspetti ritenuti rilevanti, al fine di trarre indicazioni utili a modificarne il comportamento nella realtà o a verificare l'effetto di condizioni e/o controlli imposti dall'analista: ad esempio, in campo aeronautico l'utilizzo di un simulatore di volo risponde alla necessità di dover prevedere il comportamento del veicolo e a testare la capacità di volo del pilota in situazioni particolari.

Si capisce quindi il potenziale e l'importanza che un simile strumento di analisi possiede, soprattutto in contesti strategici e tecnologici, come i sistemi produttivi, o in ambito scientifico, a fronte dell'impossibilità e delle difficoltà economiche derivanti dal dover riprodurre in laboratorio le effettive condizioni che si vogliono studiare: avvalendosi al giorno d'oggi dei mezzi messi a disposizione dalle tecnologie informatiche, è possibile paragonare tale processo ad una sorta di laboratorio "virtuale", in cui osservare cosa implica il cambiamento di alcuni parametri.
Esistono però anche riproduzioni fisiche, in scala geometrica: in tal caso si parla di prototipazione, ovvero un processo risultante nella realizzazione di un manufatto o di un dispositivo da testare, sul quale apportare eventuali modifiche e correzioni al fine di ottimizzare le prestazioni e i risultati dello stesso. La classificazione dei modelli

può avvenire in base a diversi fattori. Generalmente, si è soliti distinguere fra modelli statici e modelli dinamici: i primi non forniscono una rappresentazione dell'evoluzione del un sistema nel tempo ma si limitano a descriverne il comportamento relativo ad uno specifico istante di tempo t; pertanto essi sono espressi attraverso sistemi di equazioni matematiche di grado n (generico). Invece, i modelli dinamici, descritti attraverso sistemi di equazioni differenziali o alle differenze, rappresentano come sistema si modifica nel corso del tempo.

2.5.1 La System Dynamics

Sviluppata negli anni '50 come strumento di supporto ai manager aziendali, la System Dynamics è una tecnica di modellazione e simulazione al computer che permette di comprendere la struttura di sistemi complessi e di analizzare come varia il loro comportamento nel corso del tempo:

"It is a modeling methodology for understanding and representing complex systems and analyzing their dynamic behavior" [77].

La System Dynamics si focalizza, in particolare, sull'individuazione delle relazioni causali tra gli elementi di un sistema, che determinano come esso sia strutturato. Tale filosofia porta a pensare e a concepire le cose in un modo completamente diverso da quello al quale si è abituati. Nell'analisi di un particolare elemento - ad esempio, nel ricercare le cause che hanno portato al verificarsi di un determinato fenomeno - non si può considerare quest'ultimo in maniera asettica, ovvero distaccandosi dal contesto a cui esso appartiene ma bisogna adottare un'ottica di sistema: è necessario ragionare in termini di combinazione di elementi interagenti e interdipendenti che, insieme, costituiscono un'unica entità e agiscono come tale.

In tal senso, la complessità di un sistema risiede nell'impossibilità di prevederne il comportamento, che è la diretta conseguenza delle interazioni esistenti fra le sue parti: pertanto, essa cresce all'aumentare del numero e del tipo di interdipendenze che si instaurano fra le variabili che lo costituiscono.

Riprendendo quanto descritto da Forrester [77], l'applicazione della System Dynamics per modellare un processo di business si articola in quattro step:

1. Definizione dello scopo e dei confini della realtà di studio (*system boundaries*), identificandone le entità coinvolte, le correlazioni e l'insieme dei comportamenti che si vuole evidenziare;

2. Costruzione di un *Influence Diagram* per la rappresentazione dei rapporti causa-effetto tra gli elementi del sistema: l'elaborazione di una mappa delle relazioni causali - *Causal Loop Diagram* (CLD) - permette una prima valutazione, di tipo qualitativo, della particolare realtà d'interesse;

3. Costruzione di un modello quantitativo che tiene conto della dimensione temporale;

4. Caratterizzazione di tale modello attraverso la definizione delle leggi che governano e regolano il comportamento del sistema e l'inizializzazione delle variabili in gioco. Tale fase permette la realizzazione di un modello dinamico - *Stock and Flow Diagram* (SFD) – ottenuto a partire dalla CLD precedentemente costruita, attraverso cui è possibile valutare quantitativamente l'evoluzione del sistema nel lungo periodo.

2.5.1.1 Causal Loop Diagram

Le Causal loop diagram (CLD) sono utilizzate nella fase iniziale della simulazione dei processi di business, per visualizzare graficamente i meccanismi causali intercorrenti tra le componenti del processo/sistema in esame, che lo caratterizzano e ne determinano il comportamento.

Tali variabili (o nodi) possono rappresentare grandezze di tipo quantitativo, ovvero misurabili (ad esempio, reddito, profitto, produttività) oppure di tipo qualitativo (ad esempio, motivazione, fiducia, reputazione). A ciascun legame - rappresentato

graficamente come una freccia orientata che collega l'elemento "causa" all'elemento "effetto" - viene associata una polarità:

1. una polarità positiva (+) indica che le due variabili sono suscettibili della stessa variazione (se la causa aumenta/diminuisce, parimenti l'effetto aumenta/diminuisce);
2. una polarità negativa (-) indica che le due variabili variano lungo direzioni diametralmente opposte (se la causa aumenta/diminuisce, l'effetto diminuisce/aumenta).

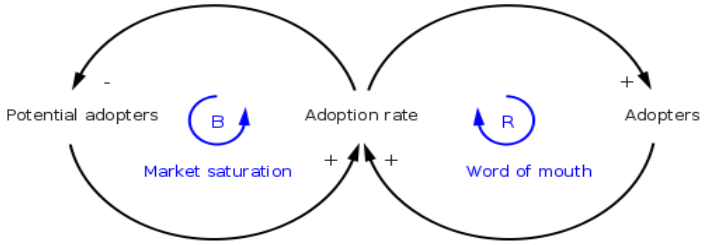

Figura 11 Esempio di Causal Loop Diagram relativo all'adozione di un nuovo prodotto

La caratteristica principale di tale rappresentazione grafica – e in generale della System Dynamics - è la presenza di cicli di feedback (*feedback loops*) [78].

Il feedback è definito come il processo di trasmissione e ritorno dell'informazione: nel linguaggio scientifico, esso è l'effetto di controreazione di un'azione che si riflette sul sistema stesso e che permette di controllarne, correggerne o modificarne il comportamento; in altri termini, un ciclo di feedback è una sequenza chiusa causa-effetto [48].

Esistono due tipologie di cicli in una Causal Loop Diagram: i meccanismi di feedback positivi (*Reinforcing Loop*), che rafforzano la variazione di una determinata variabile del sistema, e i meccanismi di feedback negativi (*Balancing Loop*) che, invece, la bilanciano.

Oltre alla polarità di legame precedentemente descritta, è possibile associarne una anche ai loop, in modo da identificarli facilmente. Quest'ultima è determinata dal numero di segni negativi associati ai collegamenti che compongono il ciclo: in particolare, un feedback loop è "positivo", indicato con (+), quando contiene un

numero pari di collegamenti negativi, "negativo", indicato con (-), quando ne contiene un numero dispari.

Un Balancing Loop è tipico di situazioni in cui si vuole portare lo stato attuale del sistema verso un particolare stato desiderato (obiettivo), intraprendendo una specifica azione: in tal caso si parla di problema di regolazione. La "distanza" tra i due determina un gap (esprimibile come differenza tra stato desiderato e stato attuale) che innesca l'azione, o l'insieme di azioni, volta a ridurre tale quantità: maggiore è il divario, maggiore sarà la necessità e la tendenza ad agire; raggiunto l'obiettivo (gap nullo), l'azione cessa.

Esempi di situazioni in cui si viene a determinare tale struttura sono, ad esempio, il tentativo di incrementare le vendite di un prodotto o lo sviluppo di un nuovo prodotto.

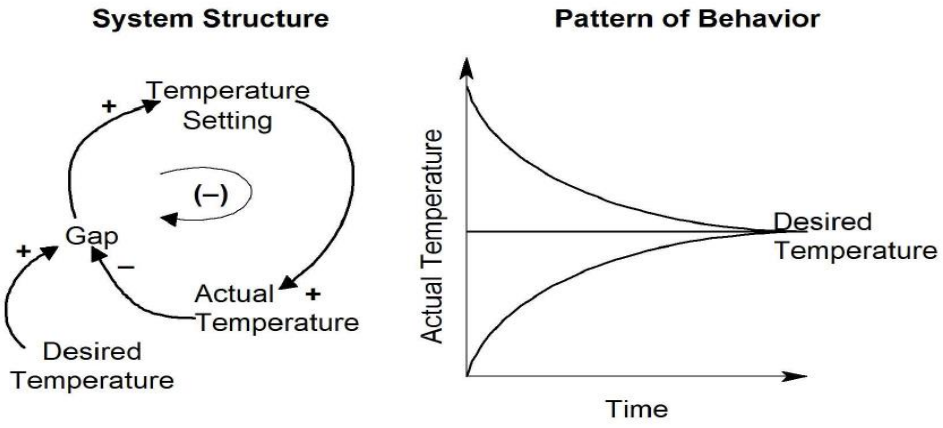

Figura 12 Esempio di Balancing Loop (regolazione della temperatura) e rappresentazione della corrispondente evoluzione del sistema [79].

Affinché la strategia intrapresa sia efficace, è necessario:

- Individuare correttamente l'obiettivo che si intende perseguire e definire in maniera obiettiva lo stato corrente del sistema: essendo il gap ad innescare la pianificazione e la successiva azione, se lo stato non è correttamente definito, l'azione potrebbe risultare inadeguata;

- Tener presente che l'azione, essendo "proporzionale" all'entità del gap, tende a ridursi man mano che ci si avvicina all'obiettivo: infatti, più si è prossimi alla conclusione del processo, più è difficile - anche da un punto di vista

economico - conseguire ulteriori miglioramenti. Ne risulta quindi che non può essere soltanto il gap ad "attivare" l'azione (ad esempio, si potrebbe innescare un meccanismo a livello organizzativo in cui vi è la motivazione a concludere rapidamente un progetto per poterne iniziare subito un altro).

Un Reinforcing Loop, invece, rafforzando la variazione di una certa variabile, è una struttura in grado di determinare una crescita esponenziale o un rapido declino nel suo comportamento.

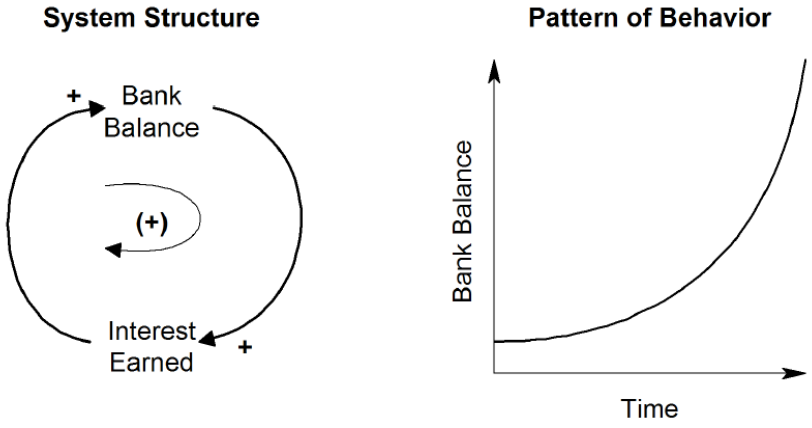

Figura 13 Esempio di Reinforcing Loop (crescita del conto bancario) e rappresentazione della corrispondente evoluzione del sistema [79].

E' bene tener presente che:

1. Quando viene prodotto un risultato desiderabile, tale struttura viene indicata come "circolo virtuoso" e si tende a lasciare le cose come stanno: dal momento che nulla cresce per sempre, quando si innesca tale ciclo è necessario capire come assicurarsi che esso continui a sostenersi.

2. Quando tale struttura produce un risultato non desiderabile, essa viene indicata come "circolo viscoso" (viscous cycle): in tal caso, l'unica soluzione possibile è interrompere il ciclo, spezzando i legami che lo compongono, di modo che la struttura non possa rinforzarsi ulteriormente.

Resta infine da introdurre un ultimo elemento, l'operatore di *delay*, fondamentale nella simulazione di processi dinamici: tale costrutto, infatti, è in grado di rappresentare lo sfasamento temporale tra causa ed effetto, come possono essere, ad esempio, i risultati di una determinata politica di gestione [78].

Come si può notare nell'esempio riportato di seguito circa il fenomeno di crescita/decrescita della popolazione, il delay viene rappresentato graficamente mediante due segmenti (||) posti sulla relazione causale di cui si vuole rappresentare l'effetto ritardato.

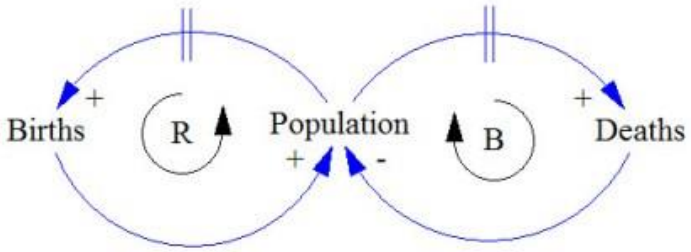

Figura 14 Esempio di Reinforcing and Balancing Loop con delay.

Vi sono poi i System Archetypes, schemi generali che rappresentano il comportamento di sistemi di qualsiasi tipo attraverso la combinazione di cicli di feedback positivi e negativi: ciò consente la comprensione del sistema nella sua interezza, nonché di predirne il comportamento, scegliendo il modello che meglio rappresenta il sistema in esame.

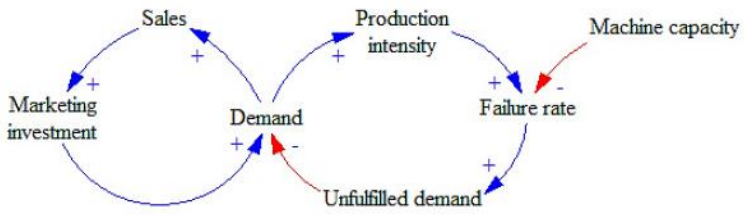

Figura 15 Un esempio di System Archetype: "Limits to growth" [80].

In figura è riportato uno degli archetipi più semplici ("Limits to growth"), costituito da un ciclo di rinforzo, che regola la crescita di una certa variabile, e da uno di

bilanciamento, che agisce come fattore limitante: generalmente, il primo opera per un certo tempo fino quando non subentra il secondo che rallenta la crescita fino a bloccarla del tutto.

Nell'esempio riportato, il limite è la capacità di un sistema produttivo costituito da una singola macchina [80]. L'azienda genera la domanda dei suoi prodotti attraverso varie strategie di marketing: da un lato, crescendo la domanda, aumenteranno le vendite e quindi gli investimenti nel marketing che, a loro volta, andranno ad incrementare le richieste (ciclo di rinforzo); nello stesso tempo, però, bisogna aumentare la produzione, ovvero sovraccaricare la macchina, con un innalzamento del tasso di guasto e dei costi di riparazione, che impedirà il soddisfacimento della domanda al 100%.

Concludendo, ci si rende conto che, attraverso la costruzione di una CLD, è possibile ottenere una descrizione qualitativa, olistica e minuziosa, basata su una struttura con cicli di feedback e delay, che ben si presta ad un'analisi sistemica: in virtù di tale caratteristica, le CLD costituiscono uno strumento in grado di catturare la natura circolare e dinamica del rapporto causa-effetto.

2.5.1.2 Stock and Flow Diagram

Differentemente dalla CLD, lo Stock and Flow Diagram aggiunge la dimensione temporale alle relazioni causali intercorrenti tra le variabili del sistema/processo di business, mostrando quantitativamente come esse variano.

Gli elementi che figurano in uno SFD sono [81]:

1. Le variabili di *stock* - indicate anche come *level* o *accumulation* - sono variabili il cui valore può accumularsi o decrescere nel tempo: pertanto, sono da considerarsi come variabili di stato in quanto rappresentative dello stato del sistema (ad esempio, il livello di riempimento di un magazzino). Graficamente esse vengono rappresentate come rettangoli recanti il nome della variabile stessa.

2. Le variabili di flusso - *flow* o anche *rate* - sono variabili espresse in funzione del tempo, in grado di modificare le variabili di stock. Graficamente, sono rappresentate da valvole a farfalla che regolano il flusso in ingresso o in uscita ad un livello (ad esempio, il tasso di produzione o gli ordini che determinano il livello di riempimento di un magazzino).

3. Le variabili ausiliari - *auxiliaries* - vengono utilizzate per combinare o riformulare informazioni contenute in altre variabili: rappresentano, infatti, calcoli algebrici che coinvolgono livelli, flussi o altre variabili ausiliarie.

4. Le costanti - *constants* - sono grandezze che, una volta inizializzate, rimangono tali. Graficamente, sono rappresentate da rombi.

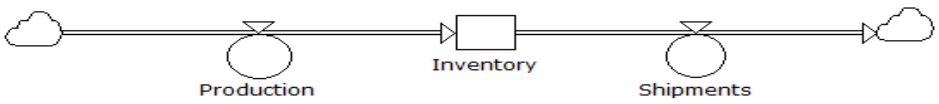

Figura 16 Esempio di rappresentazione delle variabili in uno Stock and Flow Diagram.

I confini del sistema sono modellati come particolari variabili di stock - a forma di nuvola – in quanto rappresentano una fonte non definita, al di fuori del contesto che si intende analizzare.

Il passaggio dalla CLD allo SFD non è immediato: ricavare flussi, stock e variabili ausiliari dalla prima richiede un'analisi approfondita e una perfetta conoscenza del processo/sistema che si vuole simulare.

CAPITOLO III: L' APPROCCIO SIMULATIVO PER SUPPORTARE LA VALUTAZIONE DEL RISCHIO

La sicurezza industriale, storicamente trattata in maniera superficiale o solo con l'impiego del "buon-senso", è stata oggetto negli ultimi decenni di molti studi e di particolari attenzioni da parte del Legislatore. Tale interesse ha generato sia conseguenze etiche-morali, sia benefici che una corretta gestione della sicurezza industriale può condurre alla vita dei lavoratori e della comunità.

La problematica della sicurezza industriale necessita, perciò, di un approccio di tipo scientifico. Le tecniche di valutazione del rischio da sole non permettono una corretta valutazione delle probabilità del fenomeno accidentale. In particolare sia le tecniche quantitative sia qualitative presentano dei limiti che vengono superati grazie all'impiego della System Dynamics. Il Quantitative Risk Assessment è stato affrontato in modo tale da valutare l'evoluzione del rischio (e della sua gestione al fine di attuare le corrette misure di prevenzione) nel tempo in un'azienda di stampaggio plastico, considerando i possibili scenari incidentali che caratterizzavano tale realtà produttiva. I risultati di tale studio sono stati oggetto di pubblicazione nel lavoro [80]

3.1 Cenni sulle metodologie di risk assessment maggiormente utilizzate

La valutazione del rischio è un aspetto critico e non sempre facile da affrontare. In particolare, l'assenza di sicurezza e i rischi corrispondenti nell'ambiente di lavoro possono portare ad incidenti che spesso mettono in pericolo la vita dei lavoratori e l'ambiente circostante. Nel corso degli anni sono state proposte diverse tecniche ed approcci per effettuare un'attenta analisi dei rischi della sicurezza industriale. Tali metodologie e approcci possono essere classificate in qualitative e quantitative. Le prime si basano sulla "sensibilità", cioè l'esperienza del valutatore, mentre le seconde si basano su parametri oggettivi. Le tecniche più note sono [82]: Preliminary Hazard

Analysis (PHA), HAZard and Operability (Hazop), What if analysis, Failure Modes and Effects Analysis (FMEA), Failure Mode, Effects and Criticality Analysis (FMECA), Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Bow Tie, Layer of protection analysis (LOPA).

La **PHA** è una metodologia semplice e induttiva, qualitativa, che ha come principale scopo quello di individuare tutti i possibili pericoli che potrebbero essere causa e/o nuocere ad una certa attività, struttura o sistema. È utilizzato nelle fasi di sviluppo, quando non ci sono informazioni precise sulle modalità di funzionamento. Anche l'**HazOp** è una tecnica qualitativa che si propone di identificare potenziali deviazioni dalle condizioni nominali degli impianti e di analizzare le possibili cause e le conseguenze con il metodo delle "parole guida"; il punto di partenza è una schematizzazione del sistema tramite un grafo ovvero una serie di elementi, detti nodi, collegati tra loro da linee di collegamento. Pertanto, a questo scopo, si richiede un'analisi dettagliata ad un gruppo di esperti su ciascun dispositivo, al fine di individuare le condizioni operative e le procedure di funzionamento e di manutenzione.

Estremamente semplice, ma al tempo stesso impegnativo per il team che si impegna a effettuare l'analisi dei processi in una prospettiva di sicurezza, è la "**What If Analysis**". Essa fornisce una valutazione schematica del processo di produzione valutata attraverso una sessione di brainstorming in cui un gruppo di esperti nel processo pone domande del tipo "what if?" (a proposito di possibili eventi avversi). Tuttavia, questa tecnica ha un limite: si basa fortemente sulla capacità dei partecipanti nel determinare i potenziali problemi e di riuscire ad "effettuare " le domande giuste. Un altro approccio è la FMEA, una tecnica qualitativa usata per identificare i modi in cui i componenti, sistemi o interi processi possono fallire [83]. Questa consente l'identificazione, l'analisi e la valutazione degli effetti di tutti i possibili guasti relativi a un dato sistema, nonché l'identificazione delle azioni da effettuare per eliminare o ridurre, per quanto possibile, gli errori nel sistema e le loro conseguenze. L'analisi quantitativa del rischio è, infine, fornito dalla **FMECA**. Questa tecnica esegue una valutazione di ciascun difetto critico o malfunzionamenti attraverso l'introduzione di indici di priorità (Risk Index Priority). La **ETA** (Event Tree Analysis), è basata su un approccio di tipo induttivo ed è utilizzato all'interno dei contesti industriali specifici

per l'individuazione di tutte le possibili sequenze di eventi conseguenti a un determinato evento di partenza.

Estremamente adatto per l'identificazione e l'analisi dei fattori è la **Fault Tree Analysis** ed è, allo stesso tempo, una metodologia qualitativa e quantitativa, che permette di valutare la probabilità di accadimento di un evento superiore partendo dalla valutazione delle probabilità dei singoli eventi ad essa collegati. Infine, il **BOW TIE** è una tecnica che combina sapientemente i risultati ottenuti dall'analisi FTA con quelli di un ETA. Essa determina in maniera esplicita i rapporti di causa-effetto correlate a un evento avverso. Tutte le tecniche qualitative illustrate presentano una criticità comune ovvero non considerano le protezioni esistenti organizzate in strati successivi. La **LOPA** meglio illustrata in seguito, supera tale criticità essendo una tecnica di valutazione del rischio di tipo semi quantitativa che analizza differenti livelli di protezione e le probabilità di failure di ciascun livello di protezione.

3.2 La metodologia LOPA

La LOPA (*Layers of Protection Analysis*) costituisce un utile strumento di analisi che, tipicamente, si basa sulle informazioni a carattere prettamente qualitativo analizzate in precedenza, come ad esempio la HazOp. In particolare, l'obiettivo principale della tecnica in esame è quello di capire se, all'interno di uno stabilimento, sussistono sufficienti protezioni (*Prevention and Mitigation Layers*) tali da contrastare l'insorgenza di un tipico scenario incidentale.

Ovviamente all'interno di una specifica realtà produttiva possono coesistere più tipologie di "*strati protettivi*" implementati in ridondanza. Tale aspetto è di notevole importanza poiché, sebbene ai fini della prevenzione o mitigazione delle conseguenze di un incidente sia sufficiente che anche solo uno "*strato*" intervenga in maniera idonea, è evidente che nella realtà non vi è assoluta certezza sulla effettiva buona riuscita dell'intervento da parte della misura di salvaguardia presa in considerazione, per cui è necessario prevedere la presenza di "*n layers"* in maniera tale da accrescere l'affidabilità totale del sistema.

Solitamente questi strati protettivi, anche indicati con l'acronimo IPL (*Livelli di Protezione Indipendenti*), sono misure di salvaguardia che spaziano dai dispositivi in grado di prevenire l'insorgenza di uno scenario incidentale, alle specifiche caratteristiche di progetto, ai dispositivi fisici di protezione, fino ad arrivare ai sistemi di arresto di emergenza, allarmi, protezioni fisiche *post event.*

Per le funzioni di sicurezza (*safety functions - SF*) che si attivano esclusivamente quando richiesto dalla specifica condizione operativa (*on demand mode*) la probabilità di *failure* si concretizza in un valore, di solito medio, indicato con l'acronimo PFD_{avg} (*Average Probability of Failure on Demand*) o più semplicemente PFD; per le funzioni di sicurezza, invece, che risultano continuamente in funzione la probabilità di un eventuale guasto con conseguente mancato intervento/protezione è espressa in termini frequenziali (caso *continue mode*).

Nella tabella seguente sono riportati i livelli di sicurezza (*Safety Integrity Level - SIL*[1]) in funzione della PFD o, alternativamente, del tasso di guasto λ (o f_i).

Safety Integrity Level (SIL)	***Mode of operation – on demand*** (average probability of failure to perform its design function upon demand)	***Mode of operation – continous*** (probability of dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Tabella 1 Safety Integrity Levels

[1] La norma IEC 61508, recepita in Italia come CEI EN 61508, definisce quattro *Safety Integrity Level* (da SIL1 a SIL4), ciascuno dei quali conferisce una misura quantitativa della necessaria riduzione del rischio e quindi il grado di affidabilità che uno specifico sistema di sicurezza deve raggiungere per poter garantire tale riduzione [27].

In letteratura esistono molte applicazioni della tecnica LOPA. Questa è stata sviluppata nel 2001 dal Center for Chemical Process Safety (CCP), e immediatamente attuata in tutte le principali multinazionali del settore chimico che, nel corso degli anni, hanno sviluppato la tecnica rendendola un punto di riferimento nel programma per la sicurezza di processo. Un approccio metodologico è stato definito grazie al progetto europeo ARAMIS [84]. In tale progetto è stata applicata la tecnica LOPA per migliorare la sicurezza in diversi settori, in special modo negli impianti di processo [85], al fine di proteggere i lavoratori ma anche i consumatori, come nel caso degli operatori del sistema dell'acqua [86]. Per implementare questa tecnica è necessario disporre di dati di guasto di attrezzature e impianti, ma a volte questi dati sono spesso insufficienti. L'attuazione della tecnica LOPA, in società strutturate, può aiutare ad affrontare un rischio rilevante, e può incidere direttamente sull'organizzazione. Un impianto industriale, infatti, si compone di uomini, macchine, fattori esterni, che interagendo uno con l'altro, costituiscono un sistema complesso, difficile da gestire [87]. In particolare, il ruolo del fattore umano in un potenziale evento pericoloso è importante, anzi fondamentale e richiede perciò anche la sua inclusione e la quantificazione delle azioni umane nella gestione di diversi livelli di protezione del LOPA [88]. Inoltre, le carenze gestionali e di misure organizzative possono essere la principale fonte di incidenti industriali. Approfondendo, si può dire che i principali fattori di impatto sulla gestione della sicurezza sono spesso legati ai meccanismi di gestione, alla cultura della sicurezza, delle risorse umane e alla formazione sulla sicurezza [89]. A questo scopo, l'uso di un software di simulazione, basata su un approccio di Sistems Dynamics (SD), può aiutare a gestire le complesse interazioni tra le diverse variabili coinvolte. Attualmente l'applicazione della SD alla gestione di OHS (Occupational Health and Safety) passa attraverso una fase di attenzione da parte dei ricercatori e professionisti del settore in questione. Attualmente, infatti, molte organizzazioni promuovono l'attuazione di un sistema di gestione della sicurezza in settori diversi, che tuttavia presenta problemi complessi spesso difficili da risolvere [90]. A questo proposito, la SD può essere utilizzata, per esempio, per illustrare la relazione tra la sicurezza e lavoratori nelle imprese [91] per analizzare la prevenzione degli incidenti, attraverso la costruzione di un modello di simulazione che copra i principali fattori che influenzano le prestazioni di la sicurezza

sul lavoro in sé. In realtà, l'utilizzo della System Dynamics permette di sottolineare la importanza dei loop di feedback [92] in un modello più vicino alla realtà [93] e di avere una prospettiva sistemica del problema.
Anche la tecnica LOPA ha un limite ovvero la staticità delle valutazioni di scenari di incidente credibili: essa, infatti, non tiene conto delle interazioni tra i diversi possibili scenari incidentali che possono verificarsi. Per superare questa debolezza, si presenterà un approccio integrato attraverso l'uso della System Dynamics (SD).

3.3 Approccio metodologico

Si propone un approccio metodologico che integri la tecnica di valutazione del rischio strutturata, LOPA, con un approccio di tipo Dinamico, mediante la System Dynamics (SD), permettendo di valutare le possibili interferenze di differenti scenari incidentali.
Il processo, che porta alla manifestazione incidentale, è stato analizzato e, attraverso lo sviluppo di relazioni causa-effetto, è stata aggiornata la valutazione del rischio. In particolare, l'approccio proposto prevede le seguenti fasi:

- Analisi preliminare del processo produttivo: in questa analisi tali criticità, dal punto di vista della sicurezza, devono essere evidenziate, individuando attraverso una tecnica quantitativa i diversi scenari incidentali.
- Realizzazione del processo di failure: utilizzando un Causal Loop Diagram (CLD) è possibile rappresentare in modo semplice ed immediato la struttura causale del sistema che porta all'incidente. In dettaglio, si formalizzano le relazioni causali, collegando un insieme di variabili appartenenti allo stesso sistema di riferimento ed individuando i meccanismi di feedback attivi all'interno del sistema in esame e la loro dinamica.
- Sviluppo del modello di simulazione sulla base della logica della System Dynamics che permette di quantificare gli effetti di interazione dei diversi scenari. Inoltre permette di effettuare un rapido aggiornamento della probabilità di accadimento correlate agli scenari di incidente dello specifico riferimento, sulla base della conoscenza della singola probabilità di

accadimento di ogni evento di base e delle relazioni che sussistono tra gli scenari di interesse.

3.4 Costruzione della CLD

L'approccio metodologico proposto è stato applicato ad un’azienda dello stampaggio plastico con basso rischio incendio, ma che per l’attività produttiva potrebbe avere la generazione di atmosfere esplosive (ATEX) dovuta alla presenza di polveri di propilene. Il modello della CLD che si propone considera i seguenti scenari incidentali:

1) rottura del circuito oleodinamico per raggiungimento della pressione limite e fuoriuscita olio a elevata pressione e temperatura;
2) rottura del sistema di raffreddamento stampo e fuoriuscita di materiale ad elevata temperatura;
3) esplosione nel sistema di alimentazione.

Questi interagiscono tra loro, influenzando reciprocamente le frequenze di accadimento relative a ciascun *top event*.

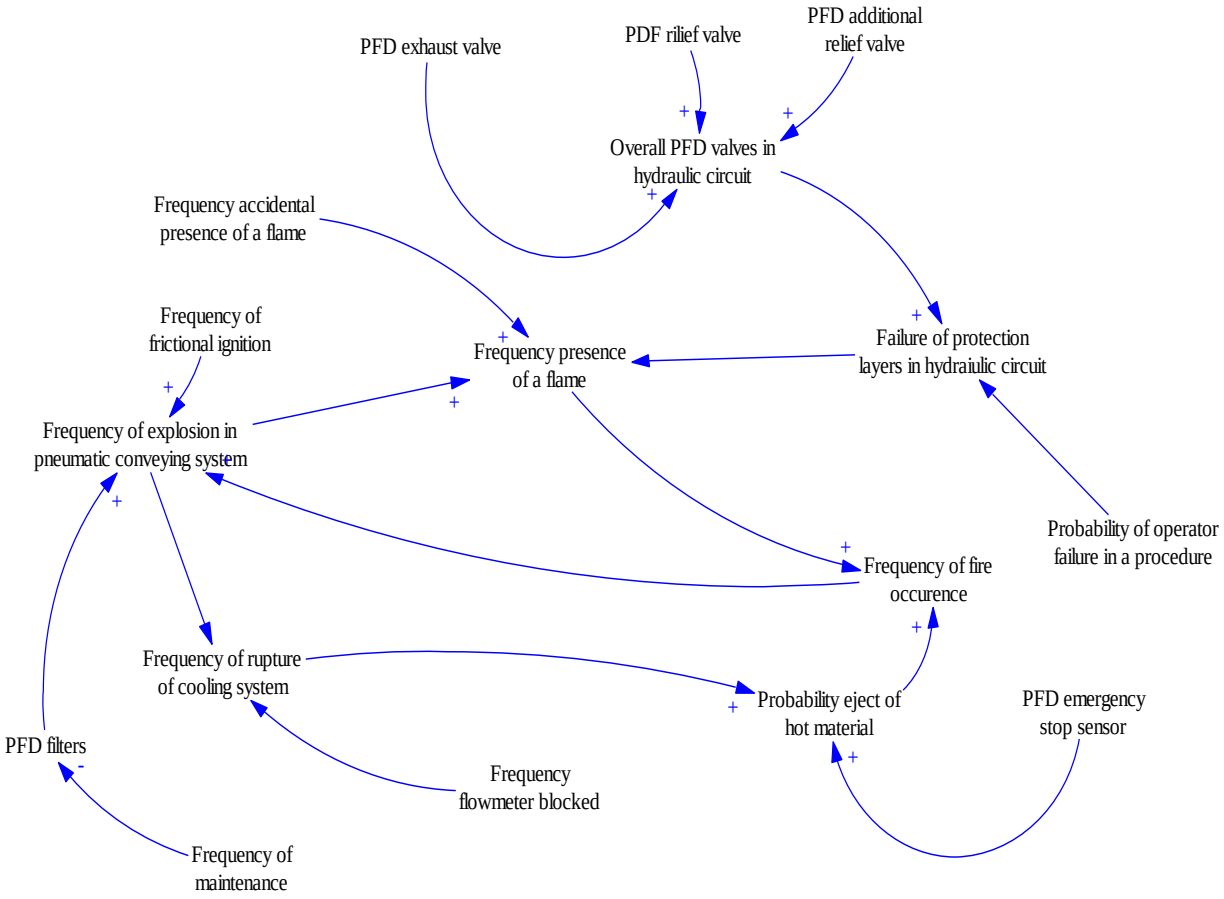

Figura 17 Costruzione della CLD

Risulta evidente come i tre scenari incidentali siano fortemente correlati. D'altronde, è facilmente intuibile come il configurarsi di un incendio possa determinare un'esplosione nel sistema di alimentazione così come un'esplosione può verosimilmente condurre ad una rottura dell'impianto di raffreddamento della pressa e quindi rappresentare un possibile evento iniziatore per lo sviluppo dell'incendio di cui prima.

Nel dettaglio, nel *Causal Loop Diagram* è possibile individuare il primo scenario relativo ad un'eventuale rottura del circuito oleodinamico per raggiungimento della pressione limite, il quale presenta il *basic events* relativo principalmente a blocchi valvola cui sono associate le rispettive PFD; essi, combinandosi con la probabilità di mancato o errato intervento dell'operatore e con la probabilità relativa all'eventuale presenza di fiamme libere in prossimità della pressa, danno luogo ad un possibile *fire*

occurrence o incendio di dimensioni più o meno ampie. Per quel che riguarda il secondo scenario, poi, quello cioè relativo alla proiezione di materiale a elevata temperatura per effetto della rottura del sistema di raffreddamento, è evidente come anch'esso basandosi sull'eventuale configurazione di eventi base, come ad esempio il mancato intervento del sensore di arresto, contribuisce ad accrescere la probabilità di un possibile incendio interno allo stabilimento originatosi da guasti a bordo macchina.

Infine vi è la probabilità di esplosione interna al sistema di alimentazione la quale, oltre a poter essere originata, ad esempio, da un'eventuale rottura del sistema filtrante, può anche trovar luogo a seguito di un incendio sviluppatosi per altre cause, a conferma della già accennata forte correlazione sussistente tra le diverse configurazioni incidentali.

Si fa notare, comunque, con riferimento all'ultimo scenario ipotizzato, come la frequenza delle operazioni manutentive possa giocare un ruolo di primo piano nella possibile riduzione della rottura del sistema filtrante costituendo, di fatto, un fattore di controllo con il quale poter implementare all'interno dello stabilimento una riduzione delle grandezze considerate nell'ottica di miglioramento continuo dei livelli di sicurezza tramite l'ausilio di misure d'intervento anche meramente organizzative. L'aspetto invece relativo al fattore umano ha necessitato un approfondimento "ad hoc" che si svilupperà nel prossimo capitolo.

Chiariti, dunque, gli scenari di interesse ai fini applicativi è possibile procedere con la definizione del cosiddetto evento iniziatore relativo a ciascun singolo scenario incidentale ipotizzato. In particolare, nel caso dell'esplosione (3), esso è verosimilmente configurabile come introduzione involontaria di un elemento metallico nel sistema di alimentazione atto a generare attriti di natura meccanica; nel caso della rottura del circuito oleodinamico (1) può intendersi come presenza di fiamme libere in prossimità della macchina; nel caso, infine, dello scenario incidentale (2) può caratterizzarsi nella rottura, o più in generale *failure*, del sistema di raffreddamento dello stampo.

Definiti gli *initialing events*, cui è possibile associare una certa frequenza f_i, sarà poi possibile procedere con l'individuazione dei *prevention and mitigation layers* nonché con la particolarizzazione delle probabilità di *failure on demand* connesse ad essi. Infatti, l'obiettivo ultimo è quello di giungere alla determinazione della frequenza di accadimento dello specifico scenario incidentale considerato mediante la semplice formula:

$$f_i^C = f_i * \prod_1^J PFD_j.$$

Tale formula, come già accennato in precedenza, contempla indirettamente una indipendenza stocastica dei vari *layers*, poiché calcola la probabilità congiunta di mancato intervento come prodotto delle singole probabilità. L'interpretazione grafica della metodologia in questione è riportata di seguito dove è possibile vedere come l'insorgenza di uno scenario incidentale qualsiasi sia la diretta conseguenza del "superamento" di una serie di barriere atte a scongiurare il rischio connesso.

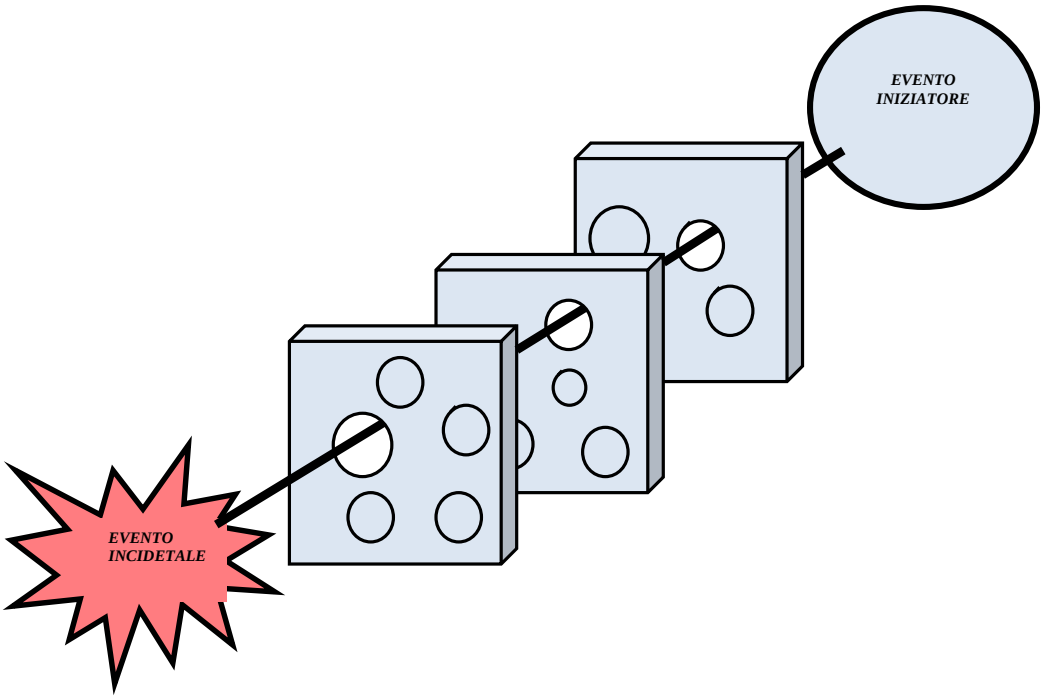

Figura 18 Interpretazione grafica della tecnica LOPA [19]

3.5 L’azienda ed il processo produttivo dello stampaggio plastico

Un’azienda di stampaggio plastico ha permesso di sviluppare il modello proposto per questa particolare realtà.

L’impianto all’interno del quale è stato condotto lo studio relativo all’applicazione di alcune delle tecniche strutturate di analisi e valutazione del rischio si occupa prevalentemente della produzione di “casse in polipropilene”.

Le fasi del processo produttivo preso in esame constano di una serie di fasi successive, di solito completamente automatizzate o semi-automatizzate. Attraverso di esse, a partire dalla materia plastica in input al processo produttivo è possibile realizzare prodotti finali dalle forme più svariate. La produzione è in gran parte alimentata da materia prima rigenerata. Infatti, in buona parte dei casi, il polipropilene utilizzato è un cumulo di residui a ridotta granulometria di cassette per l’ortofrutta precedentemente immesse sul mercato e successivamente raccolte, macinate e reinserite nel processo produttivo, realizzando di fatto un ciclo chiuso nel quale la logistica inversa costituisce una fondamentale componente gestionale.

Il ciclo lavorativo ha inizio con l’arrivo della materia prima; in alcuni casi le cassette giungono alla sede già macinate, in altri vengono sminuzzate e ridotte in granuli con la corrispondente produzione di quantitativi modesti di polvere di propilene, aspetto che, unitamente alla presenza di elementi estranei all’interno dei granuli, è di non poca importanza ai fini della sicurezza. Una volta prodotta la materia prima essa viene trasportata, tramite carrelli elevatori, ai silos e stoccata al loro interno. I granuli di polipropilene stoccati nei silos, una volta miscelati, vengono prelevati da un sistema di aspirazione pneumatico e condotti, al momento dell’alimentazione, direttamente nella tramoggia della macchina che opera lo stampaggio.

Una volta che il materiale ha raggiunto la macchina per lo stampaggio, si avvia un ciclo che si articola secondo le fasi di iniezione, impaccamento, raffreddamento ed iniezione.

Le casse in polipropilene, una volta realizzate (il tempo medio di produzione di una singola cassa è all’incirca 10 secondi), vengono impilate l’una sull’altra e successivamente trasferite automaticamente, tramite guide scorrevoli, su un nastro

trasportatore il quale provvede a traslare il carico in questione verso una macchina avvolgitrice (fasciatrice).
La fase successiva consiste nel trasferimento in opportune zone di stoccaggio dei carichi realizzati.

3.6 Applicazione della tecnica HazOp

Conclusa la presentazione del ciclo lavorativo è possibile effettuare l'applicazione della tecnica HazOp con la quale è possibile procedere all'identificazione delle potenziali "deviazioni" dell'impianto dalle condizioni nominali, di esaminarne le possibili cause e di valutarne le conseguenze. L'applicazione della tecnica in questione parte dalla suddivisione dell'impianto in una serie di elementi detti "nodi", connessi tra loro da linee di collegamento, a ciascuno dei quali sono associabili dei parametri nominali di processo.

Ovviamente tali nodi possono essere connessi più o meno fisicamente fra loro; queste connessioni, all'interno di un'analisi HazOp, degenerano in semplici linee di collegamento atte a fornire una immediata indicazione della sequenzialità del processo.

I nodi e i parametri di processo relativi a ciascun nodo, per i quali sono prese in considerazione delle caratteristiche tipiche, sono riportati nella seguente tabella:

Nodo	***Parametri considerati***
Granulatore	Polvere di polipropilene (Quantità)
Silos di stoccaggio e miscelazione	Polvere di polipropilene (Quantità)
Sistema di alimentazione	Polvere di polipropilene (Quantità)

Nodo	*Parametri considerati*
Unità di iniezione	Velocità di iniezione Pressione di iniezione Temperatura nel cilindro di plastificazione Temperatura dell'olio nel circuito oleodinamico Pressione dell'olio nel circuito oleodinamico
Unità di chiusura	Forza di chiusura Temperatura dello stampo

Tabella 2 Nodi e parametri dell'analisi HazOp

Una volta individuati i nodi e i singoli parametri sui quali concentrare l'attenzione, è possibile procedere con l'applicazione del metodo delle "parole guida".

Partendo dal presupposto che gli incidenti costituiscono una diretta conseguenza dell'allontanamento o deviazione di uno o più parametri di processo dai valori nominali, si identificano i suddetti scostamenti mediante l'ausilio di un elenco di parole guida, come ad esempio "no", "di più", "di meno", etc.

Pertanto, per procedere con la compilazione della tabella HazOp, è necessario seguire le seguenti procedure: scegliendo il primo nodo che verrà preso in analisi che, nel caso specifico in esame, è rappresentato dal granulatore, si prende in considerazione la grandezza corrispondente, la quantità di polvere polipropilene presente al suo interno. La parola guida associabile al parametro in questione è sicuramente "più di", in riferimento all'eventuale eccessiva presenza di quest'ultima nella macchina.

La causa imputabile a tale scostamento o deviazione è da ricercarsi sicuramente nelle modalità di macinazione, intese in termini di regolazione di specifici parametri operativi (ad esempio distanza tra lame fisse e lame rotanti, diametro dei fori della griglia che permette l'uscita del materiale tritato), con cui le casse per l'ortofrutta

vengono sminuzzate prima di ritornare a costituire l'*input* al processo produttivo in esame. Le conseguenze, invece, sono da individuarsi nella potenziale formazione di atmosfera esplosiva che, in presenza di un innesco qualsiasi, potrebbe dar luogo ad un'esplosione, appunto, interna al granulatore stesso. Ovviamente è bene chiarire che, ai fini di un'eventuale esplosione, è necessario che si configurino tutta una serie di condizioni atte a dar luogo allo scenario ipotizzato. In tal senso, l'innesco costituisce solo una delle suddette condizioni "necessarie" precedentemente illustrate, la quale potrebbe concretizzarsi nella possibile generazione di elettricità statica o piuttosto essere rappresentata da altri fenomeni che non siano necessariamente imputabili alla presenza di fiamme libere.

Nodo	*Parametro*	*Parola guida*	*Interpretazione Parametro + Parola Guida*	*Causa dello scostamento*	*Conseguenze dello scostamento*	*Protezioni esistenti*	*Ulteriori interventi/raccomandazioni*
Granulatore	Polvere di polipropilene (Quantità)	Più di	Eccessiva presenza di polvere di polipropilene	Errata regolazione dei parametri operativi (eccessiva macinazione)	Potenziale formazione di atmosfera esplosiva	Messa a terra	Rispetto delle istruzioni contenute nel manuale tecnico relativamente alla regolazione, messa in moto ed utilizzo della macchina.
Silos di stoccaggio e miscelazione	Polvere di polipropilene (Quantità)	Più di	Eccessiva presenza di polvere di polipropilene	Errato settaggio dei parametri di macinazione	Potenziale formazione di atmosfera esplosiva	Messa a terra	Ispezione visiva dell'integrità funzionale del silos/miscelatore
Sistema di alimentazione	Polvere di polipropilene (Quantità)	Più di	Eccessiva presenza di polvere di polipropilene	Filtri non adeguatamente manutenuti	Potenziale formazione di atmosfera esplosiva	Messa a terra dei giunti per scaricare eventuali correnti elettrostatiche Presenza di filtri per il convogliamento delle polveri	Controllo, a cadenza periodica, degli elementi che compongono il sistema filtrante Ispezione visiva dell'integrità del sistema di alimentazione
Unità di iniezione	Velocità di iniezione	Più di	Velocità di iniezione alta	Errato settaggio della velocità di iniezione	Presenza di sbavature nel prodotto	Controllo digitale della velocità di iniezione	Verifica dei settaggi
		Meno di	Velocità di iniezione bassa	Errato settaggio della velocità di iniezione	Deformazione del pezzo	Controllo digitale della velocità di iniezione	Verifica dei settaggi

Nodo	*Parametro*	*Parola guida*	*Interpretazione Parametro + Parola Guida*	*Causa dello scostamento*	*Conseguenze dello scostamento*	*Protezioni esistenti*	*Ulteriori interventi/raccomandazioni*
Unità di iniezione	Pressione di iniezione	Più di	Pressione di iniezione elevata	Errato settaggio della pressione di iniezione	Presenza di sbavature nel prodotto	Controllo digitale della pressione di iniezione	Verifica dei settaggi
		Meno di	Pressione di iniezione bassa	Errato settaggio della pressione di iniezione	Mancato completamento del pezzo	Controllo digitale della pressione di iniezione	Verifica dei settaggi
	Temperatura nel cilindro di plastificazione	Più di	Eccessiva temperatura nel cilindro di plastificazione	Termostato bloccato	Presenza di sbavature nel prodotto	Segnale di allarme della macchina	Attenta verifica dei segnali macchina
		Meno di	Bassa temperatura nel cilindro di plastificazione	Rottura di una o più resistenze del cilindro di plastificazione	Deformazione del pezzo	Segnale di allarme della macchina	Attenta verifica dei segnali macchina

Nodo	*Parametro*	*Parola guida*	*Interpretazione Parametro + Parola Guida*	*Causa dello scostamento*	*Conseguenze dello scostamento*	*Protezioni esistenti*	*Ulteriori interventi/raccomandazioni*
Unità di iniezione	Temperatura dell'olio nel circuito oleodinamico	Più di	Eccessiva temperatura dell'olio	Rottura del sistema di raffreddamento	Presenza di olio ad elevata pressione e temperatura nel circuito oleodinamico Potenziale rottura del circuito	Segnale di allarme della macchina Blocco automatico dei circuiti elettrici e idraulici in caso di *failure* del sistema di raffreddamento	Attenta verifica dei segnali macchina Manutenzione dell'impianto di raffreddamento
	Pressione dell'olio nel circuito oleodinamico	Più di	Eccessiva pressione nel circuito oleodinamico	Blocco valvole di scarico	Fuoriuscita di olio ad elevata pressione e temperatura dal circuito oleodinamico Potenziale fonte d'incendio in presenza di innesco	Valvole di sicurezza per lo scarico del circuito Canaline di convogliamento dell'olio	Attenta verifica dei segnali macchina Manutenzione regolare dell'impianto
Unità di chiusura	Forza di chiusura	Meno di	Forza di chiusura insufficiente	Alterazione nel normale funzionamento del circuito idraulico	Presenza di sbavature nel prodotto	Segnale di allarme della macchina	Manutenzione regolare dell'impianto

Nodo	*Parametro*	*Parola guida*	*Interpretazione Parametro + Parola Guida*	*Causa dello scostamento*	*Conseguenze dello scostamento*	*Protezioni esistenti*	*Ulteriori interventi/raccomandazioni*
Unità di chiusura	Temperatura dello stampo	Più di	Assenza di raffreddamento del pezzo	Rottura del sistema di raffreddamento	Fuoriuscita di materiale ad elevata temperatura	Presenza di protezioni fisse e mobili Blocco automatico della macchina	Attenta verifica del funzionamento del circuito di raffreddamento

Tabella 3 Analisi HazOp, tabella riassuntiva

Dall'analisi appena condotta è possibile trarre due conclusioni in merito al caso in esame: innanzitutto, come emerge chiaramente dalla tabella, vi sono parametri di processo che influenzano per lo più le caratteristiche qualitative dell'output prodotto ma anche parametri che hanno ricadute dirette sugli aspetti di sicurezza industriale.

Per tal motivo, a seguito di questa prima analisi qualitativa, è possibile decidere di focalizzarsi, nelle fasi successive, sugli aspetti appena citati ossia alla probabile formazione di un'atmosfera esplosiva nel sottosistema di alimentazione piuttosto che alla possibile fuoriuscita di fluido ad elevata temperatura e pressione dal circuito oleodinamico.

Altro elemento che può risultare interessante ai fini di un'adeguata valutazione dei rischi è l'eventuale rottura del sistema di raffreddamento dello stampo. Tale scenario incidentale infatti potrebbe determinare la fuoriuscita di materiale ad elevata temperatura costituendo di fatto una minaccia sempre connessa alla tipologia di rischi presi in esame, come ad esempio in termini di potenziale sviluppo di un incendio traente origine dalla combustione di determinati quantitativi di polipropilene fuso.

3.7 GLI SCENARI INCIDENTALI

3.7.1 Primo scenario incidentale

Rottura del circuito oleodinamico per raggiungimento della pressione limite e fuoriuscita olio a elevata pressione e temperatura

Innanzitutto, al fine di individuare i differenti *layers*, è necessario richiamare le modalità di funzionamento del circuito in questione. Durante il normale funzionamento della pressa, la pressione dell'olio nel circuito è misurata da appositi trasduttori di pressione che, raggiunto il valore di 175 bar (valore della pressione di linea), ne limitano l'incremento ulteriore comandando a tal fine una elettrovalvola che manda a scarico l'olio pompato. Qualora si verifichi il mancato funzionamento del dispositivo di controllo della pressione sono presenti "*valvole di massima*" che, a loro volta, impediscono il superamento di un certo valore prefissato (200 bar). Se anche queste valvole non si aprono, entrano in funzione una o più "*valvole di*

sicurezza" posizionate all'ingresso dell'imbocco del condotto di alimentazione degli accumulatori, impedendo il superamento della pressione di 250 bar. Gli accumulatori sono provvisti, poi, di una ulteriore "*valvola di massima supplementare*" tarata a 300 bar che provoca lo scarico in caso di raggiungimento di 330 bar.

Pertanto la rottura del circuito oleodinamico per effetto del raggiungimento di una pressione limite scaturisce dal "fallimento" in termini di intervento *on demand* di una serie di valvole poste in ridondanza.

Inoltre, come misure di salvaguardia relative allo scenario in esame, occorre contemplare anche il mancato intervento di un operatore all'atto della segnalazione di allarme macchina e, ad esempio, il mancato intervento dell'impianto di rivelazione di fumo (qualora venisse completata l'installazione dell'impianto) deputato all'individuazione, nello stabilimento, dell'eventuale presenza dell'innesco.

Per quel che riguarda gli aspetti quantitativi connessi allo scenario si è fatto riferimento alla consultazione della copiosa letteratura scientifica relativa alle modalità di implementazione di *safety functions* mediante l'ausilio di *Safety Instrumented Systems* (SIS). Questi ultimi nient'altro sono che un aggregato di *n Safety Instrumented Function* (SIF) presenti all'interno dell'impianto ed atti a realizzare una certa funzione di sicurezza.

Un SIF, ad esempio, è l'insieme di sensore, *logic solver* ed elemento finale (ad es. una valvola di sicurezza) che permettono in un circuito in pressione l'interruzione di un'eventuale crescita anomala dei valori operativi. Di solito, analizzando i vari dati disponibili è possibile anche conoscere l'influenza percentuale dei diversi componenti in questione (e particolarizzare lo studio, dunque, constatando che ad esempio in un SIF la probabilità di *failure* di un sensore costituisce circa il 35% della PFD totale del sistema).

Tuttavia, ai fini del presente elaborato si è ritenuto più conveniente far riferimento alla probabilità complessiva di *failure on demand*; in tal caso è sufficiente sottolineare che la probabilità di mancato intervento di una valvola nel circuito oleodinamico, per effetto ad esempio, di un blocco è pari a 10^{-2}. Per quel che riguarda, invece, il mancato

intervento da parte di un operatore all'atto di una segnalazione di allarme a bordo macchina, è stato cautelativamente utilizzato un valore pari a 10^{-1}.

In definitiva, dunque, la probabilità di *failure* complessiva delle misure di salvaguardia del circuito oleodinamico è ricavabile dal semplice prodotto delle PFD poc'anzi riportate ossia:

$$\prod_1^J PFD_j = 10^{-2^4} * 10^{-1} = 10^{-9}.$$

Di conseguenza, la frequenza dello scenario incidentale preso in considerazione (*fire occurrence*) risulta essere banalmente:

$$f_i^C = f_{innesco} * 10^{-2^4} * 10^{-1} = f_{innesco} * 10^{-9}.$$

Ipotizzando una frequenza 10^{-2} $years^{-1}$ per quel che riguarda la presenza accidentale di fiamme libere in prossimità della pressa, si ottiene il seguente valore di frequenza relativo al primo scenario d'incendio:

$$f_i^C = 10^{-2} * 10^{-9}\ years^{-1} = 10^{-11}\ years^{-1}.$$

Quest'ultimo, dunque, risulta evidentemente categorizzabile come evento raro, come emerge chiaramente dal confronto con la tabella di riferimento riportata di seguito:

Event likelihood	***Definition***
Low	A failure or a series of failure with a very low probability of occurrence within the expected lifetime of the plant (<10^{-4} failure/year)
Moderate	A failure or a series of failure with a very low probability of occurrence within the expected lifetime of the plant (10^{-4} to 10^{-2} failure/year)

Event likelihood	*Definition*
High	A failure can reasonably be expected to occur within the expected lifetime of the plant ($>10^{-2}$ failure/year)

Tabella 4 Tecnica LOPA, probabilità scenario incidentale

Definita la frequenza di insorgenza dello scenario incidentale, il passo successivo consiste nel comprendere la "*Severità*" dello stesso tramite l'ausilio di un'altra tabella di riferimento, di seguito riportata, grazie alla quale è possibile supporre verosimilmente un livello medio (*"Serious"*) di tale grandezza.

Event Severity	
Minor	Impact initially limited to local area of the event with potential for broader consequences if corrective action is not taken
Serious	One that could cause: any serious injury or fatality on-site or off-site property damage of $1million or $5million on-site
Extensive	One that is five more time worse than a serious incident

Tabella 5 Event severity, LOPA

In definitiva, nota la severità dell'evento e la corrispondente probabilità, si è in grado di valutare l'adeguatezza delle misure di salvaguardia implementate all'interno dello stabilimento; adeguatezza che, si ricorda, crescerebbe ulteriormente se si tenesse in considerazione anche la prevista predisposizione di rivelatori di fumo atti a scongiurare la presenza di eventuali fiamme libere non individuate dagli addetti al processo produttivo.

		Event Severity								
		Minor			***Serious***			***Extensive***		
Event likelihood		***Low***	***Moderate***	***High***	***Low***	***Moderate***	***High***	***Low***	***Moderate***	***High***
Number of IPLs	***3***	(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)	1
	2	(3)	(3)	1	(3)	1	2	1	2	3 (2)
	1	1	1	3	1	2	3 (2)	3 (2)	3 (2)	3 (1)

Notes	
1	One Level 3 safety interlock does not provide sufficient risk reduction at this level
2	One Level 3 safety interlock may not provide sufficient risk reduction at this level
3	SIF IPL is probably not needed
*	The values in the table without brackets refer to the integrity level (IL) required; the values in brackets refer to the number of the note given below.

Tabella 6 Decision Table, LOPA

Dalla lettura della tabella appena riportata è facilmente individuabile in taluni casi, noto tra l'altro il numero di IPLs implementati nel contesto in esame, l'*Integrity Level* (IL) richiesto. In alternativa, qualora la casella corrispondente sia identificata dal punto 3, è possibile concludere lo studio asserendo che le misure di salvaguardia adottate sono già pienamente sufficienti a mitigare lo scenario ipotizzato.

3.7.2 Secondo scenario incidentale

Rottura del sistema di raffreddamento stampo e fuoriuscita di materiale ad elevata temperatura

Anche in questo secondo caso applicativo, al fine di individuare i differenti *layers*, è necessario richiamare le modalità di funzionamento nonché la componentistica della pressa per lo stampaggio. Nel momento in cui si verifica un *failure* del sistema di raffreddamento, un allarme a bordo macchina provvede ad informare l'operatore dell'anomalia di funzionamento; inoltre, se la temperatura raggiunge un valore eccessivo, è previsto un blocco automatico della pressa. Pertanto affinché si possa configurare uno scenario incidentale come quello ipotizzato, deve innanzitutto verificarsi un guasto del sistema deputato al raffreddamento dello stampo. Tale evento, dunque, verrà utilizzato come *initialing event* del caso in esame.

Occorre poi considerare che la pressa per iniezione, qualora verifichi, mediante l'ausilio di un sensore, un problema a livello di formatura del prodotto, interviene bloccando la macchina.

Altro aspetto, poi, da contemplare tra le misure di salvaguardia riguarda, in analogia col caso precedente, l'eventuale mancato intervento di un operatore all'atto della segnalazione di allarme macchina. Per quel che riguarda l'aspetto quantitativo connesso a tale secondo scenario incidentale, valgono analoghe considerazioni espresse in precedenza circa le fonti consultabili e l'approccio adoperato (*generic data*). In tal senso, la probabilità di *failure on demand* del sensore deputato all'arresto della macchina è stimabile in 10^{-2}, mentre per il mancato intervento dell'operatore è possibile utilizzare, come in precedenza, il valore cautelativo di 10^{-1}. In definitiva, dunque, la frequenza del *top event* "*fuoriuscita di materiale ad elevata temperatura*" per effetto della rottura del sistema di raffreddamento e del mancato intervento delle misure di salvaguardia preposte è pari a:

$$f_i^C = f_{evento\ iniziatore} * 10^{-2} * 10^{-1} = f_{evento\ iniziatore} * 10^{-3}.$$

Dovendo particolarizzare ulteriormente *l'initialing event,* è possibile supporre che l'assenza di raffreddamento scaturisca da un blocco dell'elettrovalvola che regola il flusso d'acqua del flussimetro deputato, appunto, al raffreddamento dello stampo.

In questo caso, come *failure rate* del componente in esame è utilizzabile un valore di 10^{-2} $years^{-1}$, per cui la frequenza di insorgenza dello scenario analizzato risulta essere pari a:

$$f_i^C = 10^{-2} years^{-1} * 10^{-3} = 10^{-5}\ years^{-1}.$$

Tale scenario, similmente a quanto accaduto prima, risulta categorizzabile come evento raro (*Low probability*) poiché il valore risultante è inferiore a 10^{-4} $years^{-1}$ ossia quel limite al di sotto del quale l'evento è sicuramente definibile come "remoto" in termini probabilistici.

3.7.3 Terzo scenario incidentale

Esplosione nel sistema di alimentazione

Anche in questo terzo caso, in linea con quanto realizzato precedentemente, occorre richiamare le modalità di funzionamento nonché la componentistica del sistema oggetto di analisi.

Il sistema di alimentazione, a differenza di ciò che accade per la pressa per l'iniezione, non è dotato di alcun sensore che permetti il rivelamento di un'anomalia nei parametri di funzionamento o la presenza, involontaria, di un elemento estraneo nel materiale caricato nel sistema di trasporto pneumatico. D'altronde la presenza di polveri di polipropilene non è tanto legata al malfunzionamento o meno di qualche componente in particolare, bensì alla fase di macinazione che comporta la riduzione in granuli di diametro variabile della materia prima. Ciò che però è possibile affermare è che l'eventuale intasamento delle maniche del sistema filtrante dovuto ad esempio ad una rottura del sistema di scuotimento delle medesime, o la rottura stessa delle maniche potrebbe comportare una maggiore presenza di polveri potenzialmente esplosive.

Da un punto di vista quantitativo ed affidabilistico, occorre dunque individuare quale sia, ad esempio, la probabilità di rottura del sistema a scuotimento del filtro; scuotimento che, si precisa, è di tipo pneumatico, operato cioè da una valvola azionata in modo sequenziale e temporizzato da una unità di comando. Dalla consultazione della letteratura scientifica relativa a tale tipologia di *equipment* è possibile ricavare una stima della probabilità di *failure* pari a 10^{-3} (valore derivante dal rapporto fra un tasso di guasto pari a 10^{-2} hours^{-1} e un tasso di azionamento pari a 10 hours^{-1}). Pertanto applicando la formula già ampiamente commentata in precedenza si ha che la frequenza di insorgenza dello scenario incidentale ipotizzato è pari a:

$$f_i^C = f_{evento\ iniziatore} * 10^{-3}\ .$$

Ovviamente anche in questo terzo caso non è possibile concludere direttamente il ragionamento categorizzando lo scenario in uno dei possibili livelli, ma è necessario particolarizzare la frequenza di innesco non ancora esplicitata. In tal caso, si ricorda che l'evento iniziatore ipotizzato attiene all'introduzione involontaria di un elemento metallico nel sistema di alimentazione il quale potrebbe verosimilmente generare attriti di origine meccanica.

La probabilità connessa a tale evento è stimabile in $5*10^{-1}$ years^{-1} per cui, sostituendo tale valore nella formula precedente si ottiene:

$$f_i^C = f_{evento\ iniziatore} * 10^{-3} = 5 * 10^{-1} years^{-1} * 10^{-3}$$

$$= 5 * 10^{-4}\ years^{-1}.$$

A tale scenario, dunque, corrisponde una probabilità piuttosto bassa (*"Moderate probability"*) in coerenza con quanto precedentemente affermato.

Per quel che riguarda, invece, la "*Severità*" di questo terzo scenario incidentale, è bene sottolineare che la probabilità appena calcolata non fa riferimento ad una "sicura" esplosione interna al sistema di alimentazione ma piuttosto al configurarsi di una situazione di criticità che potrebbe verosimilmente fungerne da presupposto e condurre alla stessa. In altre parole, è evidente che la rottura del sistema filtrante non costituisce una condizione sufficiente per il verificarsi di un'esplosione interna al

sistema di alimentazione; infatti, affinché ciò accada deve comunque accadere che la concentrazione di polveri di polipropilene all'interno del sistema sia tale da rientrare nel range di esplodibilità.

Pertanto il secondo parametro di riferimento ai fini della valutazione dell'evento analizzato, è categorizzabile come *"Minor"* (livello più basso fra quelli proposti); tale grandezza, unita alla conoscenza del numero di *layers* implementati (1 nel caso in esame), permette di individuare l'*Integrity Level* richiesto, confermando al valutatore l'ipotesi che in corrispondenza di questo terzo scenario incidentale, in realtà, le misure di salvaguardia sono presenti ma non eccessivamente soddisfacenti. Tuttavia quanto precedentemente asserito circa la non diretta sequenzialità guasto-esplosione fa verosimilmente ritenere che, in realtà, non sussistano particolari criticità a livello di gestione della sicurezza.

Conclusa, dunque, anche questa terza implementazione, si allegano di seguito due tabelle altamente informative: nella prima si riportano le PFD, reperite in letteratura [94], relative a diversi *layers*; la seconda tabella, invece, riassume il lavoro appena svolto, con l'indicazione minuziosa di tutte le grandezze considerate.

INDEPENDENT PROTECTION LAYER	***PFD***
Control loop	1.0×10^{-1}
Relief valve	1.0×10^{-2}
Human performance (trained, no stress)	1.0×10^{-2}
Human performance (under stress)	0.5 to 1.0
Operator Response to Alarms	1.0×10^{-1}

Tabella 7 Typical Protection Layer (Prevention & Mitigation) PFDs

Number	***Impact Event & Severity***	***Initialing Cause***	***Challenge likelihood [years^{-1}]***	***Independent Protection Layers (IPLs)***				***Additional Mitigation***	***IPLs***	***Mitigated Event Likelihood [years^{-1}]***
				Process Design	***BPCS***	***Alarms, Procedures***	***SIS***			
1	Serious	Presence of a flame	10^{-2}	Exhaust valve 10^{-2}		Manual operator intervention 10^{-1}		Three relief valves 10^{-6}	5	10^{-11}
2	Serious	Rupture cooling system	10^{-2}			Manual operator intervention 10^{-1}	Emergency stop sensor 10^{-2}		2	10^{-5}
3	Minor	Frictional ignition	$5*10^{-1}$	Filter 10^{-3}					1	$5*10^{-4}$

Tabella 8 Tabella riassuntiva LOPA

3.8 Commento all'applicazione della tecnica LOPA

Realizzate le singole applicazioni relative ai tre scenari incidentali selezionati, è possibile procedere con una rapida discussione a riguardo dei risultati ottenuti al fine di trarre utili considerazioni in merito all'efficacia o meno della metodologia adoperata.

Come già osservato, ciascuna tecnica non è mai esente da limiti o comunque criticità proprie, poiché è sempre il frutto di una semplificazione concettuale di principi sicuramente più complessi e per questo di difficile applicabilità. Per quel che riguarda la tecnica LOPA, si sottolinea ancora una volta che uno dei suoi limiti principali risiede nell'incapacità, da un punto di vista strutturale, di analizzare relazioni di tipo multiplo; in altre parole, nell'analisi di uno scenario dovuto a più cause concomitanti e avente diversi tipi di conseguenze, la tecnica in questione impone di analizzare singolarmente ciascuna relazione causa-effetto di cui prima.

Inoltre, un altro aspetto che si ritiene utile richiamare è che gli scenari individuati sono solo una parte (quelli ritenuti più significativi e maggiormente complessi in termini di prevedibilità) dell'insieme di possibili eventi che potrebbero configurarsi all'interno dell'impianto industriale considerato. Ad esempio, in riferimento al primo caso applicativo, si fa notare che anche qualora non si verificasse il blocco contemporaneo di tutte le valvole di scarico, si potrebbe realizzare per effetto dell'usura comunque una rottura del circuito che, in presenza di innesco, riuscirebbe a dar vita a scenari incidentali di rilievo. In questo caso, in base alle considerazioni precedenti circa la contemporanea gestione di plurimi percorsi incidentali, la differente configurazione andrebbe analizzata singolarmente nell'ottica di determinare l'adeguatezza delle misure di salvaguardia "solo" per quello specifico scenario preso in considerazione.

Accanto a tali limiti, però, la tecnica LOPA offre anche dei vantaggi innegabili; innanzitutto va sottolineata la estrema semplicità con la quale è stata resa possibile la conduzione dello studio oggetto di discussione. Infatti una volta acquisita una minima conoscenza del processo produttivo, attraverso la consultazione del materiale tecnico

a disposizione dell'azienda nonché mediante sessioni di *brainstorming* con i responsabili del processo medesimo, è stato possibile implementare la suddetta tecnica senza particolari oneri o sforzi computazionali. D'altronde, come è stato più volte evidenziato, l'applicazione della LOPA da un punto di vista meramente analitico si riduce ad un semplice prodotto di probabilità nell'ottica di determinare la frequenza di un certo *top event* di interesse.

A tal proposito va aggiunto che la struttura intrinseca della tecnica, come si è avuto modo di constatare, è caratterizzata da un'ampia visibilità del processo in esame poiché interpreta l'insorgenza di uno specifico scenario incidentale come un susseguirsi non solo di guasti/malfunzionamenti relativi alla singola macchina/sottosistema, ma coinvolge anche altri aspetti a carattere prettamente organizzativo, che vanno dal mancato intervento di un operatore al segnale di allarme macchina, fino ad arrivare, ad esempio, al mancato intervento tempestivo delle squadre di soccorso. Tale panoramica a trecentosessanta gradi costituisce anch'essa un punto di forza della tecnica in discussione poiché si concretizza in una maggiore flessibilità, intesa come capacità di adattarsi ai contesti produttivi più disparati, nonché nel conferimento al soggetto valutatore di visione completa delle criticità connesse ai singoli eventi.

In definitiva, dunque, l'applicazione della tecnica LOPA, attraverso un minimo incremento della complessità relativa al processo di analisi e valutazione del rischio, ha consentito l'attribuzione di una maggiore solidità e credibilità di risultati che altrimenti sarebbero stato il semplice frutto di considerazioni sparse basate sull'esperienza e quindi di poca argomentazione.

Chiarite, dunque, le potenzialità della *Layers of Protection Analysis*, si vuole concludere evidenziando quali possano essere gli sviluppi ulteriori atti a conferire all'intero processo valutativo un valore aggiunto che funga da supporto e da stimolo per un miglioramento continuo della sicurezza industriale. In tal senso, sicuramente uno strumento simulativo basato sulla *System Dynamics* può rappresentare un valido riferimento attraverso il quale cercare di conferire maggiore solidità ai risultati prodotti, mediante la creazione di un modello che riproduca la complessità dei sistemi produttivi reali. Infatti determinate grandezze, che nell'analisi precedente sono state

interpretate come semplici costanti, in realtà potrebbero essere particolarizzate in funzione della variabile temporale cercando, ad esempio, di riprodurre in ambiente virtuale le dinamiche di *ageing* o invecchiamento che inevitabilmente interessano la componentistica e, in generale, le macchine industriali oggetto di analisi.

3.9 Costruzione del modello simulativo

In questo paragrafo si procederà a illustrare il processo che ha portato a costruire il modello, che è stato formulato in due versioni: la prima verrà denominata "basic model", la seconda, che verrà chiamata "improved". Di entrambe le versioni si vedranno le caratteristiche, i pregi e i difetti, e in particolare, si esaminerà il processo logico che partendo dal primo, ha permesso di formulare la versione "improved". Il software utilizzato è il "*Powersim Studio*".

Il primo modello sviluppato (definito basic model) permette, innanzitutto, una rapida determinazione delle frequenze di accadimento connesse agli specifici scenari incidentali di riferimento sulla base della conoscenza, più o meno approfondita, dei valori di PFD relativi a ciascun basic event nonché sulla base delle interrelazioni esistenti. Tale modello prevede la predisposizione di due loop che realizzano di fatto l'interconnessione tra gli scenari oggetto di approfondimento e mostrano, in tal modo, come è possibile assistere ad un mutamento (nel caso specifico si tratta di incremento) delle frequenze di accadimento ricavate dall'analisi LOPA.

Le PFD relative a ciascun Independent Protection Layer sono state, in questa prima fase, modellate mediante "Costanti", utilizzando valori di riferimento reperiti in letteratura. Altre grandezze, invece, come ad esempio la frequenza relativa alla proiezione di materiale ad alta temperatura o la frequenza di guasto del sistema di raffreddamento sono state rappresentate mediante l'utilizzo di "Variabili ausiliarie" che derivano direttamente da una combinazione analitica di altri parametri adoperati. Infine la frequenza relativa all'evento definito Fire occurrence è stata implementata con il ricorso ad un "Livello", con flussi in ingresso e flussi in uscita, in maniera tale da permettere una modifica ricorsiva dei valori adoperati. Nelle figure sottostanti si riportano le immagini tratte dalla piattaforma software e relative al modello discusso.

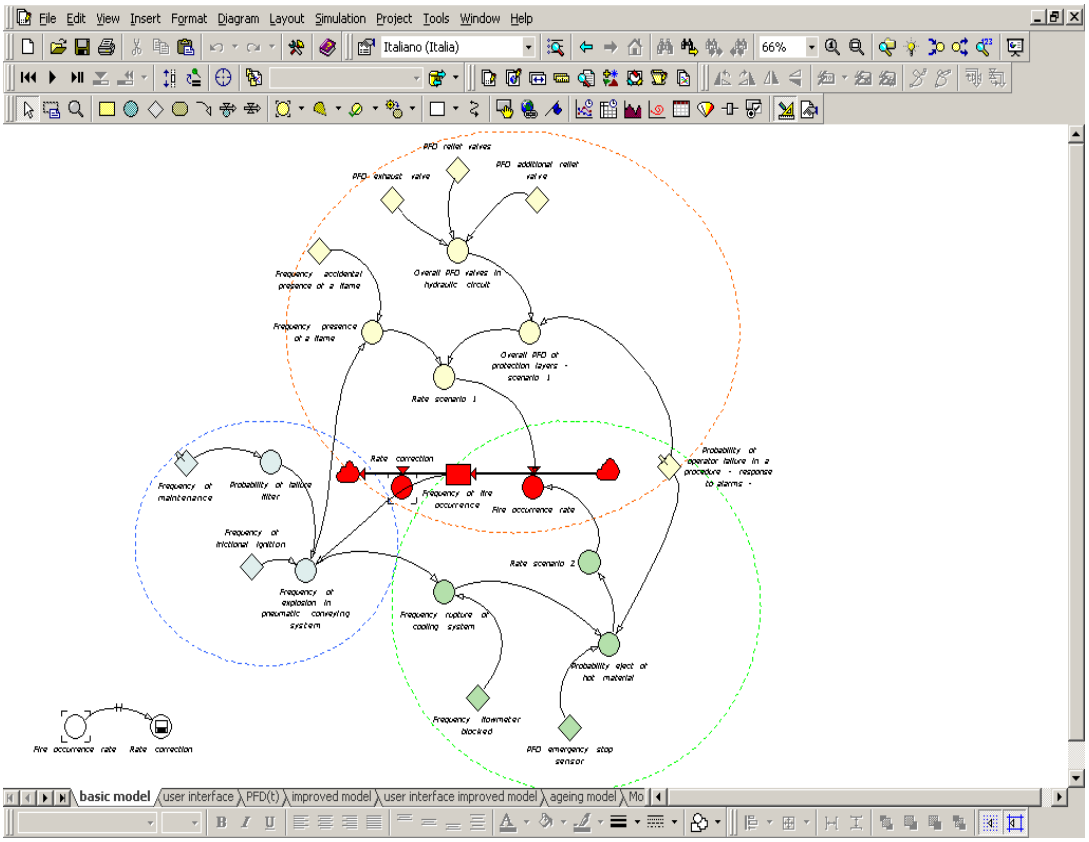

Figura 19 Il modello simulativo mediante il software Powersim

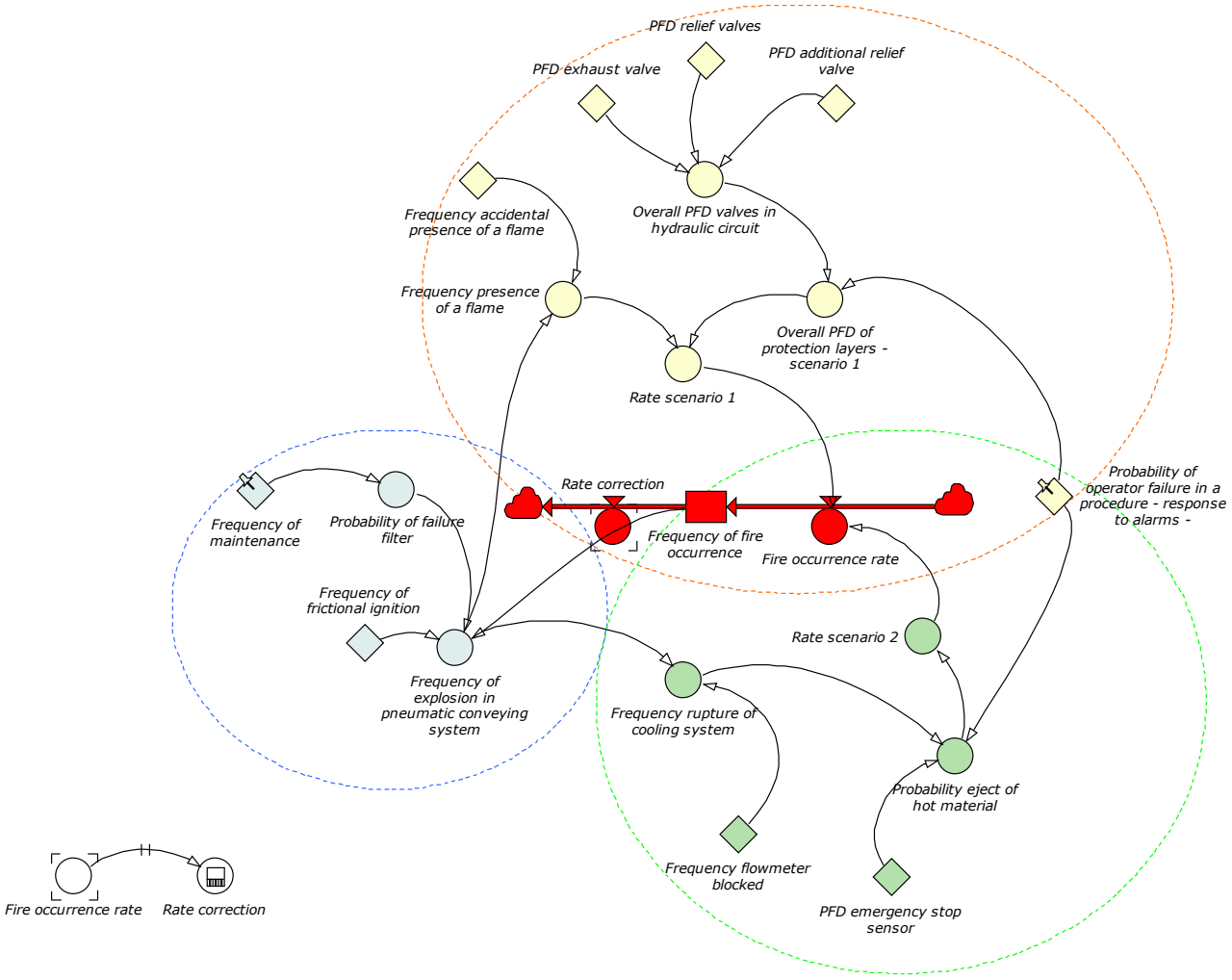

Figura 20 Modello simulativo

Costruito il modello, è stato anche possibile ricreare, al fine di una migliore comprensione e gestibilità dello stesso, una semplice ed intuitiva interfaccia utente in grado di far variare i valori delle cosiddette variabili di controllo, in maniera tale da evidenziare l'effetto che queste ultime hanno sulla dinamica dell'intero sistema. Nel caso specifico, le variabili selezionate sono state la "probabilità di mancato intervento dell'operatore" (*Probability of operator failure in a procedure*) e la "frequenza dei controlli manutentivi" (*Frequency of maintenance*). Nelle figure seguenti sono riportati i valori di frequenza di accadimento degli scenari incidentali oggetto dello studio (ossia la frequenza di accadimento di un'eventuale esplosione e quella connessa ad un'eventuale incendio diffuso) in funzione di due specifiche configurazioni delle variabili di controllo individuate.

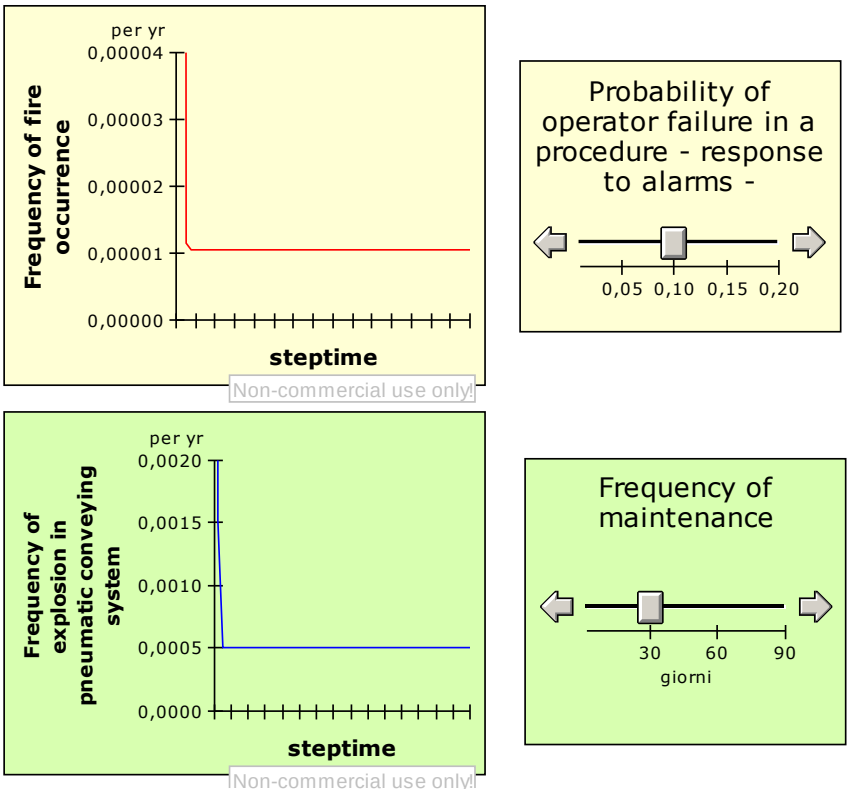

Figura 21 Interfaccia utente del modello simulativo, configurazione 1

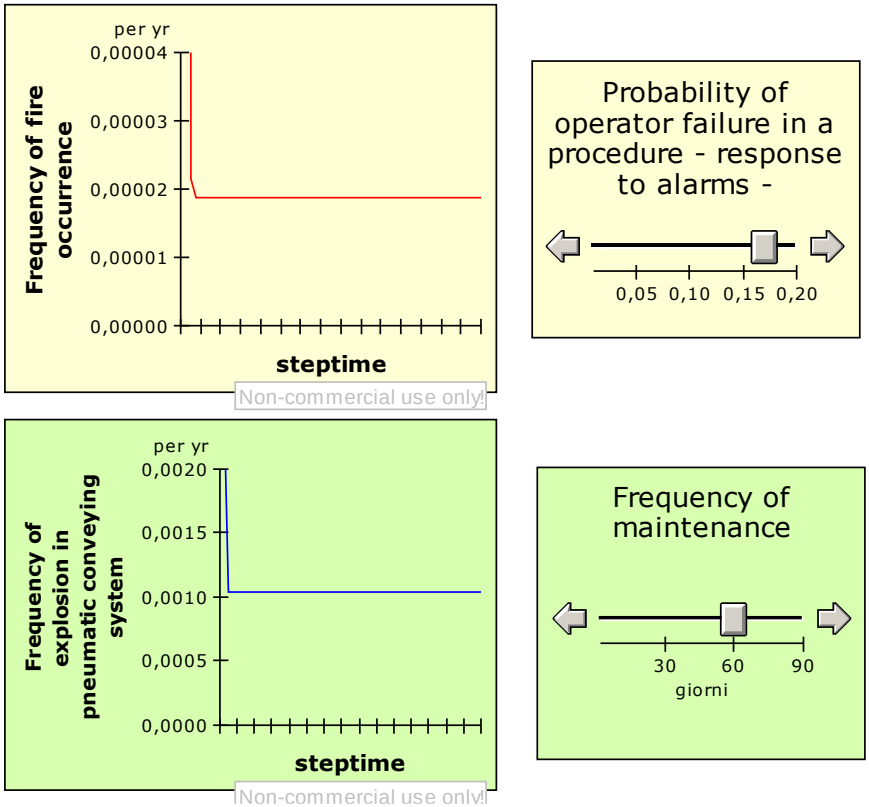

Figura 22 Interfaccia utente del modello simulativo, configurazione 2

Nella tabella seguente, invece, al fine di offrire una chiara comprensione dei vantaggi connessi con l'adozione dello strumento simulativo a supporto del processo di *risk analysis and evaluation*, si riporta un confronto tra i valori di frequenza di accadimento degli specifici scenari incidentali, prima e dopo la simulazione, nonché le variazioni (incrementi nel caso specifico) percentuali dei suddetti valori.

	Before simulation ***[1/y]***	***After simulation*** ***[1/y]***	***Percentage change*** ***[1/y]***
Scenario 1	10^{-11}	$1{,}0510747 * 10^{-11}$	*5,11%*
Scenario 2	10^{-5}	$1{,}0510747 * 10^{-5}$	*5,11%*
Scenario 3	$5*10^{-4}$	$5{,}1076074 * 10^{-4}$	*2,15%*

	Before simulation ***[1/y]***	***After simulation*** ***[1/y]***	***Percentage change*** ***[1/y]***
Fire occurrence ***(top event scenarios 1 e 2)***	*1,000001*10^{-5}*	*1,0510757 * 10^{-5}*	*5,11%*
Explosion ***(top event scenario 3)***	*5*10^{-4}*	*5,1076074 * 10^{-4}*	*2,15%*

Tabella 9 Confronto frequenze di accadimento, prima e dopo la simulazione

Dalla tabella appena riportata è possibile trarre due utili conclusioni. Innanzitutto è fondamentale sottolineare che, sebbene i valori di frequenza connessi agli specifici scenari siano estremamente contenuti anche a valle del processo simulativo, in termini percentuali è possibile evidenziare una crescita non indifferente (di poco più del 5%) per quelle configurazioni incidentali aventi come *top event* ciò che è stato definito *"fire occurrence"* ossia un incendio interno allo stabilimento, derivante da una serie di *failure* concomitanti dei sistemi di prevenzione e mitigazione.

D'altro canto, anche lo scenario relativo ad una possibile esplosione interna al sistema di alimentazione vede un incremento, questa volta però percentualmente minore (di circa il 2%), del valore di frequenza di accadimento. Questi dati sono facilmente confermabili se confrontati con il *Causal Loop Diagram* corrispondente poiché dal grafico causale sono rapidamente individuabili le diverse relazioni logiche costituenti la base di tutte le considerazioni a carattere analitico.

Ad esempio nel *Causal Loop Diagram* è evidente come il *top event* "esplosione nel sistema di alimentazione" abbia un'influenza marginale sulla determinazione della frequenza di *fire occurrence* poiché non influenza direttamente l'evento in questione ma piuttosto contribuisce ad accrescere le probabilità dei singoli eventi base, i quali costituiscono soltanto il presupposto per l'eventuale propagazione di un incendio interno allo stabilimento.

Ovviamente, il modello simulativo appena descritto può essere particolarizzato ulteriormente in funzione del livello di dettaglio e del grado di aderenza allo specifico contesto produttivo che si intende raggiungere.

Come visto, il passo successivo alla costituzione del modello si concretizza, in un approfondimento di quanto appena esaminato, in modo da verificarne aderenza alla realtà e per analizzare in che modo tale modello possa eventualmente diventare ancora più rappresentativo della realtà in essere, oggetto di studio. In particolare, per voler condurre un esempio, le probabilità di *failure* delle valvole di scarico del circuito oleodinamico non sono state più implementate come semplici costanti bensì si è provveduto alla costruzione di una funzione dipendente dalla variabile temporale di riferimento. Infatti, è sicuramente verosimile l'ipotesi secondo la quale maggiore è l'arco temporale di riferimento, maggiore è la probabilità che il componente in esame manifesti un guasto, non adempiendo dunque alla propria funzione di sicurezza. Inoltre, considerando in un primo momento costante l'eventuale tasso di guasto delle valvole oggetto di discussione (ciò equivale a ritenere che i guasti si verifichino in maniera del tutto accidentale), è stato possibile riferirsi ad un modello di distribuzione Esponenziale.

Con l'introduzione di questa ipotesi si è passati a un modello differente, che presenta un livello di complessità maggiore in quanto delle costanti sono state rappresentate ora con delle distribuzioni statistiche. Al termine dell'introduzione dell'ipotesi vagliata, e quindi della creazione del nuovo modello, è stata prodotta una interfaccia grafica di riferimento in modo tale da permettere un confronto fra i due modelli implementati. Di seguito se ne riporta un'immagine tratta dalla piattaforma *software*.

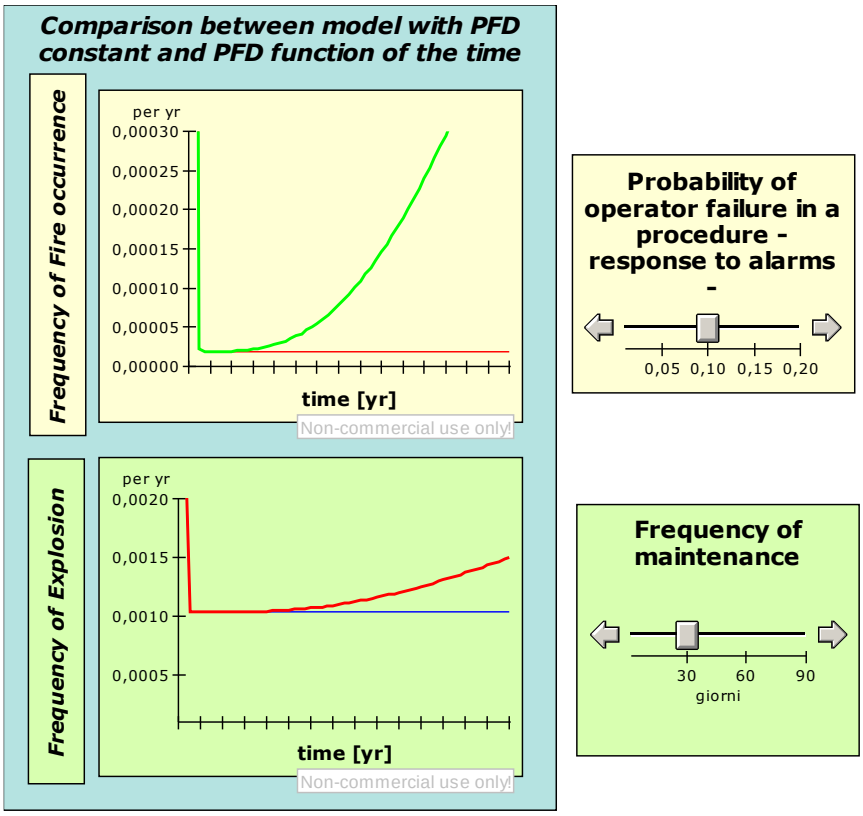

Figura 23 Confronto tra modelli con PFD constante e PFD funzione del tempo

Dalla Figura 23 si può notare come l'andamento, in funzione dell'arco temporale di riferimento, della probabilità di *failure* delle valvole di scarico si rifletta nell'andamento delle frequenze di accadimento dei *top events* di interesse, influenzando in particolar modo il primo dei due scenari incidentali complessivi ovvero ciò che è stato indicato come *fire occurrence*.

Per modellare in modo più completo questa rappresentazione della realtà, si è introdotto una nuova ipotesi, in modo tale da prendere in considerazione il cosiddetto fenomeno di *ageing*, ossia l'invecchiamento degli specifici componenti esaminati. Infatti, un'altra ipotesi piuttosto verosimile è quella secondo cui il tasso di guasto di un eventuale elemento elettromeccanico non è sempre costante durante l'intera vita fisica del componente medesimo bensì presenta un tratto costante nella fase di "vita utile" ed un tratto crescente nella fase di "usura".

Sulla base di tale considerazione è stata realizzata una terza interfaccia utente con la quale promuovere un confronto diretto fra i valori di frequenza di accadimento

estrapolati in assenza dell'ipotesi di *ageing* ed i valori ricavati a valle dell'introduzione della stessa. La figura seguente riassume in sé tale confronto.

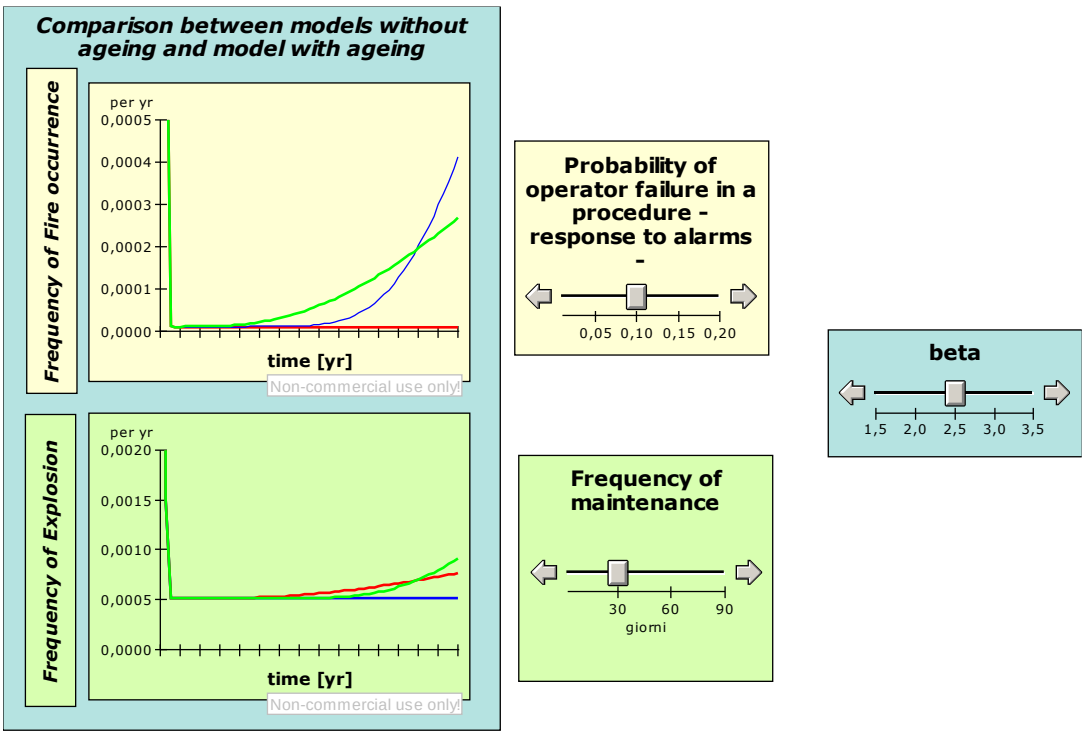

Figura 24 Interfaccia utente, ipotesi di ageing delle valvole

È quasi superfluo sottolineare che l'introduzione dell'ipotesi di *ageing* della componentistica in esame ha comportato una crescita più che proporzionale delle frequenze di accadimento oggetto dello studio. Ovviamente, in termini assoluti, le variazioni sono risultate piuttosto irrilevanti; tuttavia, analizzando nel dettaglio le curve medesime, è identificabile il tratto crescente relativo alla fase di usura del sistema di valvole (tratto blu della Figura 24). Nella tabella successiva si evidenziano, anno per anno, le variazioni percentuali relative ai due modelli appena presentati.

Frequencies of top events and percentage changes						
Time	*Frequency of fire occurrence - improved model*	*Frequency of fire occurrence - ageing model*	*Δ*	*Frequency of explosion in pneumatic conveying system - improved model -*	*Frequency of explosion in pneumatic conveying system - ageing model -*	*Δ*
01/01/2016	0,00001051	0,00001051	0,00%	0,00051076	0,00051076	0,00%
01/01/2017	0,00001052	0,00001051	-0,10%	0,00051077	0,00051076	0,00%
01/01/2018	0,00001055	0,00001051	-0,38%	0,00051080	0,00051076	-0,01%
01/01/2019	0,00001060	0,00001051	-0,85%	0,00051085	0,00051076	-0,02%
01/01/2020	0,00001069	0,00001051	-1,68%	0,00051094	0,00051076	-0,04%
01/01/2021	0,00001083	0,00001051	-2,95%	0,00051108	0,00051076	-0,06%
01/01/2022	0,00001103	0,00001051	-4,71%	0,00051128	0,00051076	-0,10%
01/01/2023	0,00001132	0,00001051	-7,16%	0,00051157	0,00051076	-0,16%
01/01/2024	0,00001169	0,00001051	-10,09%	0,00051194	0,00051076	-0,23%
01/01/2025	0,00001218	0,00001051	-13,71%	0,00051243	0,00051076	-0,33%
01/01/2026	0,00001278	0,00001051	-17,76%	0,00051303	0,00051076	-0,44%
01/01/2027	0,00001352	0,00001051	-22,26%	0,00051377	0,00051076	-0,59%
01/01/2028	0,00001441	0,00001051	-27,06%	0,00051466	0,00051076	-0,76%
01/01/2029	0,00001545	0,00001052	-31,91%	0,00051570	0,00051077	-0,96%
01/01/2030	0,00001667	0,00001052	-36,89%	0,00051692	0,00051077	-1,19%
01/01/2031	0,00001807	0,00001053	-41,73%	0,00051832	0,00051078	-1,45%
01/01/2032	0,00001966	0,00001054	-46,39%	0,00051991	0,00051079	-1,75%
01/01/2033	0,00002146	0,00001057	-50,75%	0,00052171	0,00051082	-2,09%
01/01/2034	0,00002346	0,00001060	-54,82%	0,00052371	0,00051085	-2,46%
01/01/2035	0,00002568	0,00001065	-58,53%	0,00052592	0,00051090	-2,86%
01/01/2036	0,00002811	0,00001073	-61,83%	0,00052836	0,00051098	-3,29%
01/01/2037	0,00003078	0,00001085	-64,75%	0,00053103	0,00051110	-3,75%
01/01/2038	0,00003368	0,00001101	-67,31%	0,00053393	0,00051126	-4,25%
01/01/2039	0,00003681	0,00001124	-69,46%	0,00053706	0,00051149	-4,76%
01/01/2040	0,00004018	0,00001155	-71,25%	0,00054043	0,00051180	-5,30%
01/01/2041	0,00004379	0,00001195	-72,71%	0,00054404	0,00051222	-5,85%
01/01/2042	0,00004764	0,00001252	-73,72%	0,00054789	0,00051277	-6,41%
01/01/2043	0,00005173	0,00001326	-74,37%	0,00055198	0,00051351	-6,97%
01/01/2044	0,00005606	0,00001420	-74,67%	0,00055631	0,00051445	-7,52%
01/01/2045	0,00006063	0,00001541	-74,58%	0,00056088	0,00051566	-8,06%
01/01/2046	0,00006544	0,00001692	-74,14%	0,00056569	0,00051717	-8,58%
01/01/2047	0,00007048	0,00001882	-73,30%	0,00057073	0,00051907	-9,05%
01/01/2048	0,00007576	0,00002115	-72,08%	0,00057601	0,00052140	-9,48%
01/01/2049	0,00008127	0,00002398	-70,49%	0,00058152	0,00052423	-9,85%
01/01/2050	0,00008700	0,00002741	-68,49%	0,00058725	0,00052766	-10,15%
01/01/2051	0,00009295	0,00003149	-66,12%	0,00059320	0,00053174	-10,36%
01/01/2052	0,00009913	0,00003633	-63,35%	0,00059938	0,00053658	-10,48%
01/01/2053	0,00010551	0,00004200	-60,19%	0,00060576	0,00054225	-10,48%
01/01/2054	0,00011210	0,00004859	-56,65%	0,00061235	0,00054884	-10,37%
01/01/2055	0,00011890	0,00005618	-52,75%	0,00061915	0,00055643	-10,13%
01/01/2056	0,00012589	0,00006485	-48,49%	0,00062614	0,00056510	-9,75%
01/01/2057	0,00013307	0,00007469	-43,87%	0,00063332	0,00057494	-9,22%
01/01/2058	0,00014043	0,00008576	-38,93%	0,00064068	0,00058601	-8,53%
01/01/2059	0,00014798	0,00009813	-33,69%	0,00064823	0,00059838	-7,69%
01/01/2060	0,00015569	0,00011185	-28,16%	0,00065594	0,00061210	-6,68%
01/01/2061	0,00016358	0,00012696	-22,39%	0,00066383	0,00062721	-5,52%
01/01/2062	0,00017162	0,00014350	-16,39%	0,00067187	0,00064375	-4,19%
01/01/2063	0,00017981	0,00016147	-10,20%	0,00068006	0,00066172	-2,70%
01/01/2064	0,00018815	0,00018089	-3,86%	0,00068840	0,00068114	-1,05%
01/01/2065	0,00019662	0,00020173	2,60%	0,00069687	0,00070198	0,73%
01/01/2066	0,00020523	0,00022396	9,13%	0,00070548	0,00072421	2,65%
01/01/2067	0,00021396	0,00024755	15,70%	0,00071421	0,00074780	4,70%
01/01/2068	0,00022282	0,00027243	22,26%	0,00072306	0,00077268	6,86%
01/01/2069	0,00023178	0,00029852	28,79%	0,00073203	0,00079877	9,12%
01/01/2070	0,00024085	0,00032573	35,24%	0,00074110	0,00082598	11,45%
01/01/2071	0,00025001	0,00035396	41,58%	0,00075026	0,00085421	13,86%
01/01/2072	0,00025927	0,00038309	47,76%	0,00075952	0,00088334	16,30%
01/01/2073	0,00026861	0,00041301	53,76%	0,00076886	0,00091325	18,78%

Tabella 10 Frequenze dei top events e variazioni percentuali, improved model e ageing model

3.10 Considerazioni analitiche sul modello simulativo

Il modello simulativo è stato implementato ed adoperato per permettere, tra l'altro, una valutazione congiunta degli scenari incidentali analizzati al fine di comprendere quali fossero le influenze di ciascuno di essi sulle frequenze complessive di accadimento connesse ai *top events* presi in considerazione, ovvero il rischio di un'esplosione interna al sistema di alimentazione ed il rischio di un incendio diffuso.

Le probabilità per ciascuno scenario incidentale sono :

$$Pr(scenario1) = Pr(overall\ PFD\ of\ prot.layers) * Pr(presence\ of\ a\ flame)$$

dove:

$$Pr(presence\ of\ a\ flame) = Pr(accidental\ presence) + Pr(explosion) - Pr(accidental\ presence|\ explosion) * Pr(explosion).$$

Analogamente, per il secondo scenario valgono le relazioni riportate di seguito:

$$Pr(scenario2) = Pr(failure\ of\ prot.layers) * Pr(rupture\ cooling\ system)$$

dove:

$$Pr(rupture\ cooling\ system) = Pr(flowmeter\ blocked) * Pr(explosion) - Pr(flowmeter\ blocked|\ explosion) * Pr(explosion).$$

Si fa esplicitamente notare che il terzo scenario, ossia quello relativo ad un'eventuale esplosione interna al sistema di alimentazione, influenza indirettamente i primi due poiché contribuisce a creare le condizioni per l'eventuale propagazione di un incendio interno allo stabilimento esaminato.

Comunque sia, nel momento in cui le probabilità, rispettivamente di "presenza di fiamme libere" e di "blocco del flussimetro", sono ritenute stocasticamente indipendenti dagli eventi di *fire occurrence* ed *explosion*, è possibile sostituire alle precedenti relazioni altre due, nelle quali l'intersezione degli eventi citati si concretizzi nel prodotto tra le probabilità assolute di riferimento.

Ovviamente, seguendo il medesimo ragionamento, è possibile particolarizzare ulteriormente le altre grandezze considerate realizzando di fatto un'astrazione matematico/statistica delle interrelazioni naturalmente presenti nel contesto esaminato, sulle quali si è provveduto a realizzare un modello grafico simulativo, sicuramente di più semplice gestione ed utilizzo.

3.11 Conclusioni

Nel presente capitolo è stato mostrato, in maniera rapida ma al tempo stesso esaustiva, quali possano essere gli sviluppi ulteriori di un'analisi del rischio condotta mediante l'ausilio di tecniche strutturate. In particolare ci si è soffermati sulla descrizione della *System Dynamics* e sugli evidenti vantaggi che tale strumento permette di conseguire attraverso uno studio integrato dei differenti scenari "critici" estrapolabili dalle precedenti tecniche a carattere pressoché statico.

Nel dettaglio, è stato mostrato l'intero *framework* nel quale articolare il processo di analisi dinamica del rischio il quale si compone delle seguenti fasi principali: preliminare sviluppo di grafici di causalità che mostrino i legami tra le variabili di interesse, costruzione di un modello tramite l'ausilio di un software basato sulla SD (nel caso specifico la scelta è ricaduta su *Powersim Studio 8*) al fine di ottenere, quale *output* finale, un diagramma che sia in grado di modellare effettivamente la complessa dinamica del sistema oggetto di studio ed un "cruscotto" con il quale il valutatore sia in grado di far variare i valori di riferimento di eventuali variabili di controllo.

In riferimento al primo elemento richiamato, ossia il *Causal Loop Diagram*, va detto che esso ha permesso l'individuazione, senza particolari oneri, dei principali cicli di *feedback* di rinforzo i quali rappresentano la naturale connessione sussistente tra i

rischi d'incendio e di esplosione sui cui si è focalizzata l'attenzione nel corso dello studio; il modello simulativo, poi, ha permesso di particolarizzare da un punto di vista analitico quanto precedentemente osservato nell'ottica di definire chiaramente l'influenza di particolari variabili di interesse.

CAPITOLO IV

LA RESILIENZA NEGLI IMPIANTI INDUSTRIALI MEDIANTE IL SUPPORTO DELLA SYSTEM DYNAMICS

La Resilienza, già ampiamente studiata in precedenza, diventa parte principale per la sicurezza di un impianto. Si propone un modello organizzativo nel quale si mostra come la Resilienza sia fulcro nell'ottica del Safety Management e come tutte le funzioni organizzative aziendali contribuiscano ad essa al fine di ottimizzare un sistema complesso quale è l'impianto industriale e renderlo intrinsecamente sicuro. L'indice sintetico, per valutare la sicurezza dell'impianto è il Resilience Indicator [95].

Nello studio del modello proposto, ciascuna componente organizzativa è legata alle altre e tutte insieme concorrono al rischio globale ed alla Resilienza. Nel corso dell'analisi effettuata, è stato necessario focalizzarsi sugli aspetti relativi agli errori umani che risultano complessi da gestire e che ricoprono un ruolo fondamentale nella sicurezza dei sistemi tecnologici e degli impianti industriali incidendo in maniera determinante sul Rischio e quindi sulla Resilienza che diviene sempre più misura della sicurezza del sistema [96].

4.1 Dal rischio alla Resilienza

"In a world of finite resources, of irreducible uncertainty, and of multiple conflicting goals, safety is created through proactive resilient processes rather than through reactive barriers and defences" [48].

Il paradigma della sicurezza predominante negli approcci tradizionali al Risk Management - The Error Counting Paradigm - mira essenzialmente ad individuare come le prestazioni umane, limitate o errate, possano deteriorare un sistema di

sicurezza ben progettato, focalizzandosi sul calcolo delle probabilità di guasto/insuccesso [74]: l'idea di fondo è che la sicurezza, una volta progettata, ingegnerizzata e realizzata, possa essere mantenuta tale limitando la variabilità della performance umana - intesa come componente non affidabile - attraverso norme e prescrizioni, investendo sulla formazione o incrementando il livello di automazione.

Tuttavia, gli sviluppi registrati nei sistemi socio-tecnici degli ultimi 20 anni hanno determinato un numero crescente di processi intrattabili, per i quali limitare la variabilità delle prestazioni diventa una necessità per il funzionamento degli stessi, piuttosto che un semplice obbligo: un processo è "trattabile" quando ne sono noti i principi di funzionamento e la struttura dello stesso si mantiene immutata nel tempo [74]. Molto spesso la complessità, soprattutto in ambienti fortemente dinamici, quali sono i contesti economico-produttivi, è dovuta anche all'impossibilità di conciliare esigenze di sicurezza, da un lato, e obiettivi fondamentali, dall'altro (es. obiettivi di crescita, economici, produttivi, ecc.).

A ciò si aggiunge una sempre maggiore incertezza e frequenza caratterizzanti gli incidenti industriali, riconducibili a cause naturali, errori tecnici-organizzativi o a negligenze umane [97] molto spesso dalle conseguenze disastrose: l'elevata interconnessione che le aziende presentano al giorno d'oggi fa sì che l'impatto di un simile evento su una di esse abbia ripercussioni sull'intera rete.

Di conseguenza, comprendere la natura del rischio e individuare le modalità attraverso cui è possibile ridurlo costituiscono gli obiettivi principali della gestione della sicurezza (Safety Management) ma di per sé non sono sufficienti a garantire la sicurezza di un sistema. Oltre alla pianificazione di strategie di prevenzione e protezione, si rendono quindi necessari meccanismi in grado di rendere il sistema più resistente e che gli consentano di recuperare rapidamente ed efficacemente da un qualsiasi evento avverso: in tale contesto, la Resilienza si afferma come componente fondamentale per la sopravvivenza di un sistema che opera in condizioni in continua evoluzione.

Nel loro lavoro Steen & Aven (2011) forniscono al concetto di "rischio tecnologico", definito come la probabilità di eventi indesiderati per la magnitudo delle possibili

conseguenze, una prospettiva più ampia in base a quattro parametri: le possibili conseguenze C, la probabilità P, l'incertezza U, e le conoscenze di K, noto l'evento di attivazione.

Questo insieme di variabili permette di rappresentare la Resilienza di un sistema attraverso le variabili intrinseche [98]:

i. rispondere alle minacce regolari e irregolari in modo robusto e flessibile;
ii. controllare che cosa sta succedendo, compresa la propria performance;
iii. anticipare i rischi (eventi di rischio) e le opportunità;
iv. imparare dall'esperienza.

Poiché le variabili di cui sopra hanno bisogno di una quantificazione per essere utilizzate per il processo decisionale, la metodologia che viene proposta per la quantificazione è quella tradizionalmente usata nella valutazione del rischio con l'unico suggerimento di adottare un punto di vista sistemico, quindi non tenendo conto dei singoli eventi, ma delle interazioni tra questi. E' riconosciuto che i metodi basati sulle catene causali e modellazione di eventi (come alberi degli eventi) possono produrre previsioni carenti in alcuni casi, ma ancora questi metodi possono fornire spunti di approfondimenti e rivelano caratteristiche interessanti del sistema. Inoltre questi metodi risultano semplici e permettono di capire repentinamente quali sono le proprietà interessanti.

Proponendo un modo completamente nuovo di ragionare sulla sicurezza e di concepire quest'ultima, la Resilience Engineering (RE) si afferma come nuovo paradigma per il Safety Management. Sotto diversi aspetti, essa può essere considerata come un'integrazione dei processi di Risk Management tradizionali - limitati nei confronti dei moderni sistemi socio-tecnici - in grado di far fronte alla complessità e raggiungere gli obiettivi prefissati in condizioni di incertezza: difatti, mentre la gestione del rischio ha il suo fulcro nell'identificazione e nella riduzione dei fattori di rischio, la Resilienza si pone l'obiettivo di aumentare la robustezza e, al tempo stesso, la flessibilità di un sistema e di impiegare in maniera proattiva le risorse a disposizione in condizioni di funzionamento atipico. Essa riesce, quindi, a compensare le carenze di un sistema, che possono derivare ad esempio da una cattiva

progettazione dei processi o da una scarsa capacità di gestione. La Gestione della Sicurezza, quindi, è una parte integrante per raggiungere la Resilienza. Con specifico riferimento alla sicurezza industriale, Pasman e Knegtering (2008) [52] e Pasman et al. (2013) [53] hanno considerato che l'approccio resiliente dovrebbe essere indirizzato a minimizzare i danni e ripristinare qualsiasi sistema alle normali operazioni subito dopo il verificarsi di un incidente. Inoltre, hanno dichiarato che le analisi tipiche strutturate per la progettazione e per la gestione dei sistemi di sicurezza non sono adatte per la valutazione dei rischi industriali derivate dalla combinazione di diversi fattori, come ad esempio incompetenza, fattori tecnici, o organizzazione. Pertanto risulta necessaria una valutazione del rischio globale. Infine, Hollnagel et al. (2006) [48] hanno definito Resilienza come la capacità intrinseca di un sistema per regolare il funzionamento prima, durante, o dopo modifiche e disturbi in modo che possa sostenere la richiesta sicurezza operativa sia in condizioni attese e inattese. Questo ultimo significato è stato assunto quale definizione quantitativa di Resilienza e come definizione di un livello di resistenza per l'industria di processo, come descritto nel seguito. Inoltre, gli obiettivi descritti da questi autori risultano estremamente complessi da realizzare con strumenti di valutazione del rischio classici. Pertanto si è adottato lo strumento della simulazione dinamica (SD), al fine di poter simulare l'andamento della funzione rischio ed infine del Resilient Indicator. Va riconosciuto che, per quanto riguarda la valutazione del rischio, come già dettagliato nel Capitolo II, alla luce delle ricerche e applicazioni quantitative sulla valutazione della Resilienza, soprattutto nelle industrie di processo, risulta che non esiste una metrica univoca e ben sviluppata, come riassunto in [68].

In particolare, i risultati di questo studio preliminare, effettuato attraverso l'utilizzo di osservazione sul campo e questionari, hanno evidenziato qualitativamente le sfide nel procedimento di costruzione della RE e la sua capacità di adattamento, agendo su diverse categorie: la mancanza di esperienza esplicito sulla RE, l' intangibilità del livello di RE , la scelta di produzione di oltre la sicurezza, la mancanza di sistemi di reporting, le "credenze religiose", l' out-of-date di procedure e manuali, lo scarso ciclo di feedback e problemi economici. Lavorando su questi aspetti gli autori hanno sostenuto che dovrebbe essere possibile raggiungere un livello più elevato di affidabilità e Resilienza.

Questo link di affidabilità risulta rilevante, perché la teoria delle organizzazioni di affidabilità elevate (HRO), è vista come elemento precursore del concetto di Resilienza - e per lo più si sovrappone con esso. Gli HRO sono definiti da Lekka & Sugden (2011) come le organizzazioni che sono in grado di sostenere un eccellente record di sicurezza su periodi di tempo lunghi, in un "senza quasi incidenti" [99].

4.2 Il nuovo modello "Resiliente"

Tutto quanto sopra discusso permette di individuare una serie di pratiche che le organizzazioni possono adottare per raggiungere alti livelli di affidabilità e sicurezza. Queste pratiche sono spesso discusse nel contesto di incidenti rilevanti per evidenziare gli standard di sicurezza che le organizzazioni di alta pericolosità dovrebbero cercare di emulare. L'impegno di gestione per la sicurezza è emerso come un fattore importante alla base della corretta attuazione delle pratiche di affidabilità da migliorare. A partire da questa analisi si è proposto uno studio che prende ispirazione dalla teoria della catena del valore di Porter e che descrive qualsiasi struttura come un insieme limitato di processi. Il modello generale proposto è il seguente :

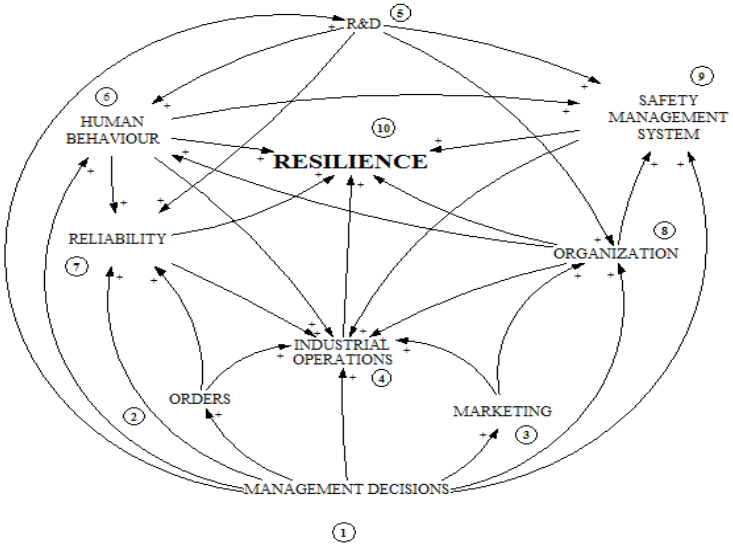

Figura 25 La Resilienza: il Modello organizzativo

Il modello generale permette di visualizzare le macro aree aziendali, le loro interazioni e le loro influenze (di incremento o meno). Tutte le macro aree o funzioni aziendali convergono assieme verso la Resilienza, vero obiettivo di questa parte di presentazione. La rappresentazione grafica immediata ed intuitiva è stata utilizzata per la costruzione della CLD.

La CLD ha posto in evidenza gli aspetti già individuati nel modello generale, individuando i LOOP ed anche inserendo alcuni flussi, descrivendo così di fatto già il modello derivante da *Kawaji.*

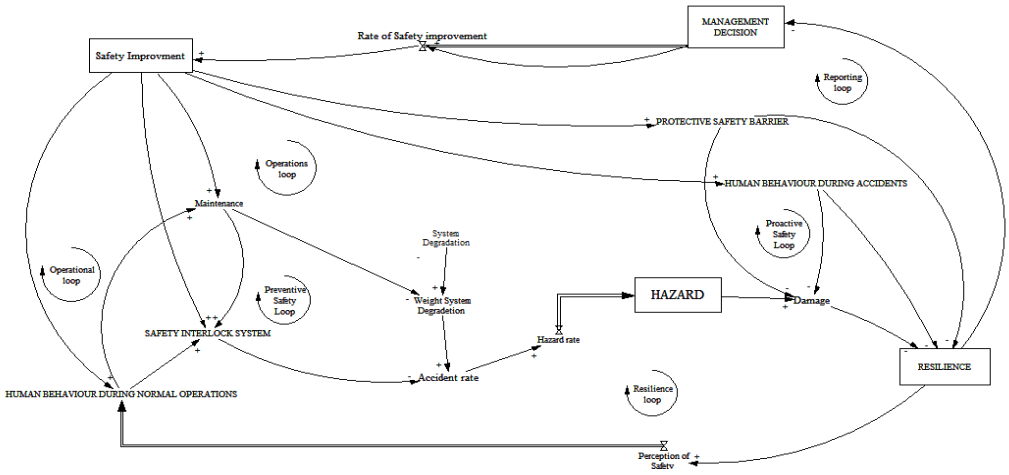

Figura 26 Casual Loop Diagram: Modello Proposto

Al fine di arrivare alla definizione di Resilienza per il modello proposto, in accordo con Hollnagel et al. (2006) [48], si è rilevato che gli eventi incidentali come incendi (flash fire, pool fire, jet fire), esplosioni (vapor cloud explosion, bleeve), o dispersioni tossiche, possono essere considerati eventi catastrofici che mettono a repentaglio la capacità di qualsiasi sistema industriale per operare e far fronte alla rottura, perdita di controllo e alla perdita di contenuti.

La definizione che scaturisce dal ragionamento, fin qui riportato, permette di definire il ***Resilience Indicator (RI***) come il prodotto della vita totale del sistema (inteso come

impianto) per la probabilità di occorrenza di incendio, esplosione e/o dispersione. Questi risultati sono proposti grazie al supporto della SD.

L'operazione di sviluppo del modello organizzativo risulta complessa e comprende l'interazione di ciascun nodo incluso nel ciclo principale e di tutti i relativi sub-nodi (Figura 26). Lo sviluppo iniziale ha riguardato solo il nodo 2 che è collegato ai nodi ed è analizzato secondo i principali aspetti dell'ingegneria di sicurezza dei processi chimici.

4.3 La scelta del Caso studio

L'analisi, per lo sviluppo del modello, è stata condotta in un'azienda di distribuzione di GPL nella zona vesuviana. L'azienda di distribuzione di GPL risponde alle caratteristiche stabilite dalla direttiva Seveso ter, in quanto si tratta di un impianto a rischio incidente rilevante. L'azienda analizzata si trova nell'area vesuviana, zona ad alto rischio sismico e classificata come zona "rossa".

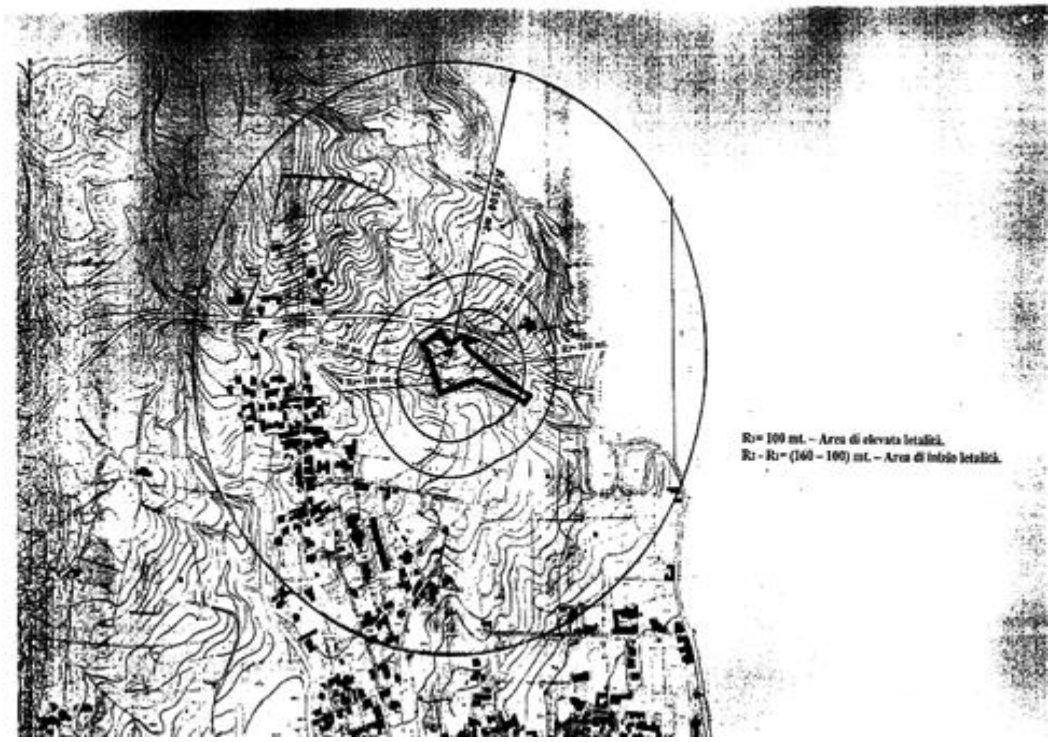

Figura 27 Mappa del rischio

4.4 Breve descrizione del processo produttivo

Si richiama brevemente l'attività produttiva: il carico del GPL all'interno dei serbatoi viene effettuato attraverso autobotti, che vengono fatte posizionare su di una bilancia che effettua il peso in ingresso ed uscita dell'autocisterna. Per poter effettuare lo scarico, il guidatore della cisterna è costretto a dover scendere dall'automezzo e spegnerlo, per poter aprire il vano di attacco dei tubi e delle messe a terra (visto che le chiavi di accensione dell'automezzo sono le stesse per il vano di carico). Tale precauzione, tiene in considerazione la necessità di poter far raffreddare il motore (anche se tali automezzi sono dotati di spezza-fiamme) e di mantenere il veicolo fermo. Aperto il vano, gli operatori possono connettere i bracci mobili della fase liquida e della fase gas, che permetteranno lo svuotamento della cisterna; viene connessa anche la messa a terra colla cisterna, questo in quanto il GPL è soggetto a generare elettricità statica che potrebbe accumularsi sulle pareti del serbatoio ed innescare una possibile miscela che potrebbe andare a ristagnare nei dintorni della zona di scarico.

Il carico dei serbatoi viene effettuato mettendo in pressione il contenuto della cisterna: il contenuto allo stato gassoso presente all'interno del serbatoio viene aspirato dai compressori e immesso in testa alla cisterna. Il liquido, sotto pressione, travasa e si sposta nei condotti che lo porteranno al serbatoio, che quindi sarà riempito dal basso, per gorgogliamento. Una volta terminato il carico, le valvole che collegano i bracci al serbatoio vengono chiuse e i bracci vengono staccati dai connettori; infine viene tolta anche la messa a terra. Va sottolineato che l'attacco dei bracci mobili è del tipo flip-flap, che permette, nel caso di errato attacco del braccio al connettore della cisterna e del suo conseguente distacco, di evitare (sia per la cisterna sia per le condotte di carico del liquido e di travaso del gas) la perdita di materiale infiammabile.

Finita la parte di carico dei serbatoi è possibile passare a quella di scarico. In particolare, come si è detto, l'obiettivo è quello di caricare delle cisternette per la consegna a domicilio di GPL per uso domestico, oppure di caricare delle bombole da

utilizzare per alimentare dei piani cottura oppure stufe per il riscaldamento di piccoli ambienti.

Per quanto riguarda il primo utilizzo del GPL, il riempimento delle cisternette è del tutto simile al riempimento del serbatoio.

Le bombole vengono caricate su di un nastro trasportatore che avvicina le bombole alla prima pompa, dotata di una manichetta con una valvola a molla per poter effettuare il riempimento. Tale pompa è dotata anche di una bilancia che permette di effettuare un riempimento uniforme e a norma di legge (ossia di 10 kg). In maniera periodica poi si effettua una pesa delle bombole (prelevate a caso) per valutare se le bilance sono ancora ben funzionanti, oppure hanno bisogno di essere ritarate. Il gas viene prelevato dai serbatoi tramite delle pompe centrifughe che mandano poi il liquido al capannone di imbottigliamento, la portata in eccesso di liquido viene rimessa in testa alle pompe tramite circuiti di by-pass per un riutilizzo in un riempimento successivo.

Una schematizzazione dell'impianto è la seguente :

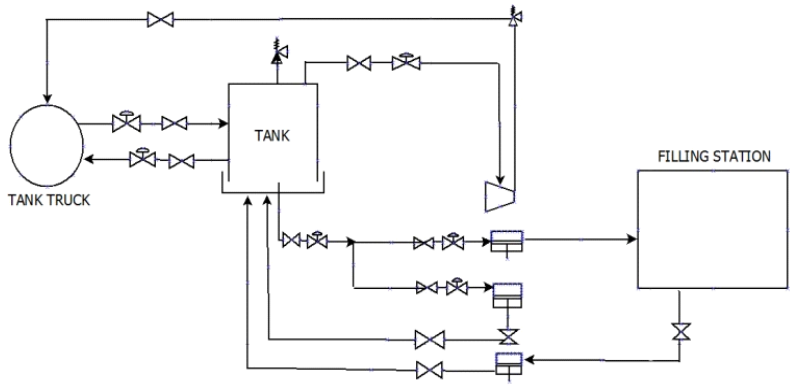

Figura 28 Schema di impianto

4.5 Il modello in Powersim e i risultati delle simulazioni

E' possibile effettuare un'analisi della Resilienza modificando il modello sviluppato in precedenza. La prima particolarizzazione del modello è l'introduzione di un ciclo che misura l'azione proattiva. In questo modo sarà possibile valutare la probabilità di

guasto da questa nuova variabile. Questo modello teorico è stato già utilizzato da *Khawaji* nel suo lavoro ed in parte riportato nella figura sopra (Figura 26). Il modello Powersim per il caso studio è stato il seguente:

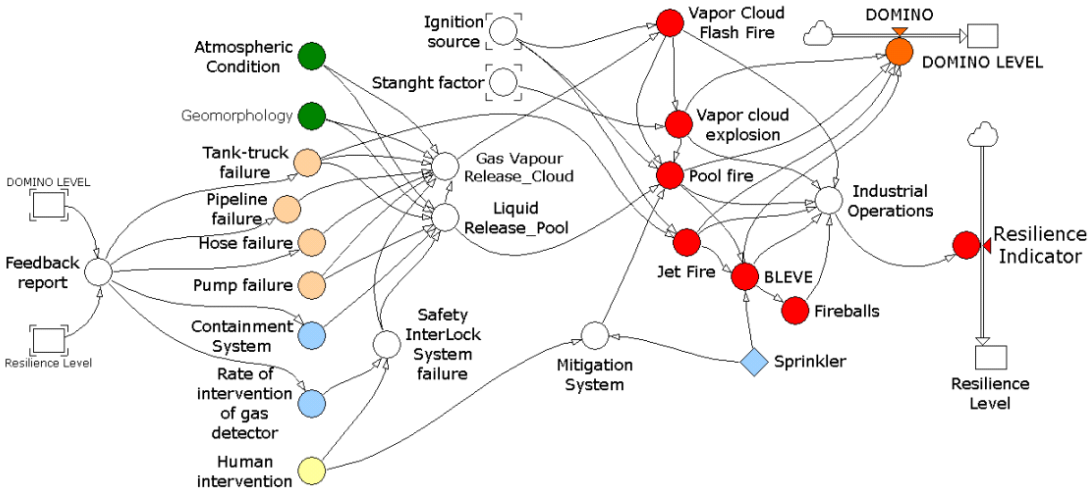

Figura 29 Modello simulativo

Nell' analisi condotta, alcune delle variabili in Figura 29 (ad esempio condizioni atmosferiche, eventi esterni, geomorfologia, e l'effetto domino) sono state trascurate. Altre probabilità sono state valutate secondo i valori riportati nella relazione Rijmond (Mannam, 2005, [99]) e Vilchez et al. (2011) [101]. L'analisi è stata effettuata utilizzando la modellazione sia statica che dinamica.

La prima considera i valori costanti, in termini di probabilità annua, per le variabili e per il cedimento strutturale delle apparecchiature. In questo caso, il risultato della SD è in qualche modo equivalente alla procedura di valutazione del rischio classica o analisi bow-tie. A questo scopo, si sono adottati i dati di probabilità di guasto come nel rapporto Rijnmond [99]. Per la modellazione dinamica, si sono considerate le probabilità di cedimento strutturale delle apparecchiature utilizzando funzioni esponenziali e Weibull. Il modello esponenziale utilizza il tasso λ (t) costante per fornire la probabilità di failure in termini di funzione di densità di probabilità (PFD) e di funzione di distribuzione cumulata (CFD):

$$PFD = P(t) = \lambda e^{-\lambda t} \qquad (1)$$

$$\mathrm{CFD} = \mathrm{P}(\mathrm{t} > T) = 1 - \lambda \mathrm{e}^{-\lambda \mathrm{t}}. \quad (2)$$

Il modello Weibull introduce anche un parametro β che varia nel tempo come nelle seguenti funzioni:

$$\mathrm{PFD} = \mathrm{P}(\mathrm{t}) = \mathrm{e}^{-(\mathrm{t}/\alpha)^{\beta}} \quad (3)$$

$$\mathrm{CFD} = \mathrm{P}(\mathrm{t} > T) = 1 - \mathrm{e}^{-(\mathrm{t}/\alpha)^{\beta}} \quad (4)$$

dove 1 / α risulta pari a λ e β e varia in maniera lineare tra 0 e 5 considerando detto intervallo quale l'intervallo di tempo tra l'installazione e la vita totale del sistema.

Variabile	Funzione	Frequenza di rottura [y^{-1}]
Compressor failure	Rottura del sistema di raffeddamento	$5 \cdot 10^{-4}$
Pump failure	Rottura del sistema di raffreddamento	$5 \cdot 10^{-4}$
HumanBehaviour	Probabilità che l'operatore intervenga al verificarsi di un malfunzionamento o dopo il rilascio di sostanze	0.91
Ground failure	Non funzionamento della messa a terra dovuta a cattiva manutenzione o cattiva progettazione	0.09
Lightning	Probabilità di presenza di fulmini nell'area specifica	$1 \cdot 10^{-6}$
Faraday cage failure	Errore umano nella progettazione e/o manutenzione	0.09
Hot Surface	Surriscaldamento dovuto a cattivo funzionamento del sistema di raffreddamento	Compressor U Pump failure
Ignition Source	L'ignizione possono verificarsi a casusa di elettricità statica o fulmini o rottura della messa a terra	Hotsurface U Lightning ∩ Groundingfailure
Tank truck failure	Rottura strutturale del serbatoio seguito da rilascio del contenuto	$2 \cdot 10^{-5}$
Pipeline failure	Rottura strutturale delle condutture (taglio o squarcio)	$5 \cdot 10^{-6}$
Hose failure	Distacco (guasto, rotture),e conseguente rilascio di contenuto	$4 \cdot 10^{-4}$
Pump failure	Rottura strutturale della pompa seguita dal rilascio di contenuto	$5 \cdot 10^{-4}$
Gas/Liquid Cloud	Formazione di gas infiammabile/ vapor cloud	Tank truck U Pipeline U Hose U Pump failure ∩ SIS
Liquid Pool	Formazione di liquid pool	Tank truck U Pump failure ∩ SIS
Jet Fire	Formazione di jet fire	Ignition ∩Tank truck failure

Tabella 11 Failure Rate used for the SD reported in Figure 5. SIS = Safety Instrumented System

La Tabella 11 riporta i risultati dell'analisi in SD per il Resilience Indicator usando sia l'analisi statica che dinamica. Ovviamente più cresce il Resilience Indicator (RI) maggiore è la Resilienza. L'analisi statica fornisce un valore unico della RI che è più

alto di ciascun valore ottenuto con un'analisi dinamica in quanto non vengono considerati gli effetti dell'invecchiamento sull'impianto e sull'infrastruttura. D'altra parte, il tempo influenza il valore RI dinamica nel tempo a causa delle funzioni di affidabilità dipendenti dal tempo.

RI $\cdot 10^5$	10 y	20 y	30 y	40 y	50 y
Static			0.78		
Exponential	0.49	0.40	0.31	0.24	0.21
Weibull	0.76	0.46	0.46	0.44	0.42

Tabella 12 Resiliens Indicator results

Chiaramente, l'analisi statica dà un unico valore per l'indicatore generale Resilienza. D'altra parte la sequenza storica dei tempi influenza il valore RI perché le funzioni di affidabilità sono dipendenti dal tempo ed influenzano il risultato finale.

4.6 Ulteriori contributi alla sicurezza ed alla Resilienza: il fattore umano

Lo sviluppo del modello generale ha richiesto un approfondimento riguardante il fattore umano. In accordo con quanto stimato negli ultimi anni, il contributo del fattore umano, ovvero l'errore umano, incide con il 60-80% sugli incidenti e soltanto per la restante parte c'è un'incidenza dovuta ad errori tecnici. A sostegno di ciò Reason [18] ha stimato l'affidabilità umana, considerando l'uomo alla stessa stregua di un qualsiasi componente elettronico o meccanico del sistema, anche se permangono delle incertezze nello scegliere le metodologie che portino alla stima della probabilità di errore. Infatti l'efficacia e l'efficienza del sistema dipendono dall'affidabilità di ciascun componente e dalla loro interazione. A tal uopo, nel campo del comportamento umano (Human Behaviour), all'interno dei sistemi socio tecnici ed organizzativi, la ricerca scientifica ha sviluppato diverse metodologie che si basano sui processi e le funzioni cognitive in modo da poter quantificare l'errore umano.

4.7 Risultati preliminari

Dall'analisi e studio della letteratura consolidata, si sono sviluppati diversi metodi al fine di quantificare l'affidabilità umana. Questi metodi chiamati human reliability analysis methods, soddisfano la necessità di un'analisi del rischio di tipo probabilistico (Probabilistic Risk Assessment, PRA) in modo da quantificare il contributo del fattore umano alla probabilità di verificarsi di un incidente. In particolare la HRA (Human Reliability Analysis) risulta essere una specializzazione del PRA [101]. Un'analisi di tipo probabilistico permette di identificare tutti i rischi compreso il fattore umane al quale il sistema è esposto nonché le stime quantitative incluse in un fault tree analysis.

Lo sviluppo delle metodologie HRA sono connesse intimamente all'industria nucleare dove il contributo dell'errore umano alla probabilità di accadimento dell'incidente potrebbe avere severe e catastrofiche conseguenze.

Al fine di quantificare l'affidabilità di un Sistema nella sua interezza è necessario assegnare un valore al problema dell'errore umano. Per questo scopo sono stati sviluppati una serie di metodi che assegnano all'esecuzione di ciascun compito (task) un valore di probabilità di errore e che si differenziano per il loro modo di stimare la probabilità di errore umano (HEP) e in che modo i fattori prestazionali li influenzano (PSF). Sono stati sviluppati diversi metodi HRA, che differiscono per scopo nel modello cognitivo che si assume, per le tassonomie delle azioni errate ed i fattori che influenzano la probabilità di errore.

Si identificano tre generazioni di metodi HRA. I metodi della prima generazione (come THERP, HCR, HEART ecc.) analizzano l'errore umano come un errore di un apparato o di un impianto. Le azioni umane sono considerate in modo binario (Bernoulliane), cioè come il successo o il fallimento di ottenere il risultato richiesto da un'attività.

In particolare i compiti e le attività secondarie hanno una probabilità intrinseca di fallimento o di errore che si modifica grazie a "fattori di forma" che si basano sulla valutazione del contesto aziendale.

La critica a questi metodi di terza generazione risulta nel fatto che questi non considerano i processi cognitivi che portano all'errore umano e non considerano l'impatto del contesto e dei relativi fattori sulla modalità di errore.

Le metodologie di analisi dell'errore umano della seconda generazione (CREAM, SPARH ecc.) mirano a valutare il contributo umano all'evento incidentale focalizzandosi sul contesto. Questi metodi si basano su modelli cognitivi appropriati per descrivere il fattore umano in modo da spostare l'attenzione sull'interazione dei fattori del contesto che incrementano la probabilità di errore umano. I punti di debolezza dei metodi di seconda generazione vanno ricercati nell'uso di una valutazione qualitativa del comportamento dell'operatore; mentre i metodi di prima generazione sono stati validati, quelli di seconda generazione, al contrario, non possono esserlo per la mancanza di dati sperimentali e di riproducibilità essendo fortemente legati alla metodologia utilizzata.

Infine la terza generazione delle metodologie HRA (NARA and BAYESIAN NETWORK) si focalizza sui fattori delle performance umane e le loro dipendenze mirando al superamento delle metodologie di seconda generazione. In particolare si cerca di modellare la mutua influenza attraverso le performance dei fattori di forma in termini di impatto sulle performance umane e la loro interazione. Questi metodi sono chiamati dynamic methods in quanto considerano l'evoluzione dinamica del comportamento umano fino ad arrivare all'errore. Da un punto di vista metodologico si intende creare una sorta di database dell'human failure in modo da limitare le incertezze relative alla valutazione dell'affidabilità umana [103], [104], [105].

4.8 Framework dell'analisi della human reliability

Lo sviluppo dell'HRA metodo richiede una serie di passaggi [101]:

- Lo sviluppo e/o l'applicazione di un modello di riferimento cognitivo per il comportamento umano
- Lo sviluppo e l'applicazione di una tassonomia per una rappresentazione dell'errore umano;

- la data collection dei dati qualitativamente e quantitativamente rilevante della human reliability;
- la descrizione di un metodo dove i passi da seguire sono descritti in questa analisi;
- la valutazione dell'influenza dei fattori di forma sull'errore umano.

4.8.1 Modello cognitivo e tassonomia

Nell'analisi della human reliability risulta necessario formalizzare un modello umano ed il suo collegamento con le performance umane [106]. Un modello cognitivo è supportato da una corrispondente tassonomia che descrive formalmente il comportamento umano e la performance in maniera strutturata. Una tassonomia è una classificazione, applicata alle associate manifestazioni degli errori umani (human errors) e le loro cause maggiori. In particolare Harwood and Sanderson hanno sottolineato che vi è la necessità impellente della creazione di una sorta di vocabolario interdisciplinare per comunicare il ruolo degli esseri umani [107] inteso come azioni, errori etc.

Al fine di "modellare" il comportamento umano nel corso del tempo sono state proposte una serie di classificazioni di azioni incorrette nel campo della Human Reliability. Le più note sono le skill-rule-knowledge (SRK), con le relative tassonomie di errore [108], approfondite da Rasmussen che classifica il comportamento umano in tre macro aree:

- **Skill-based behavior**: comportamenti routinari basati sulle competenze apprese. L'impegno cognitivo richiesto è molto basso e il ragionamento è inconscio (attività automaticamente).
- **Rule-based behaviour**: comportamento guidato da regole che l'operatore deve seguire per svolgere bene il proprio compito. Si tratta di riconoscere la situazione e di applicare la procedura appropriata per svolgere il compito. L'impegno cognitivo è più elevato rispetto a quello necessario nello skill based behavior in quanto implica un certo livello di ragionamento.
- **Knowledge-based behaviour**: comportamento volto a risolvere i problemi in situazioni che non sono di routine o conosciute, nuove o inaspettate, per le

quali non esistono regole o procedure specifiche. Questo tipo di comportamento è definito come conoscenza (Knowledge-based) e richiede un impegno cognitivo alto nella ricerca di una soluzione efficace.

Il processo cognitivo che si basa sullo stimolo all'azione, è strutturato su tre diversi percorsi di crescente complessità che richiedono crescenti livelli di attenzione e di risorse cognitive (Figura 30).

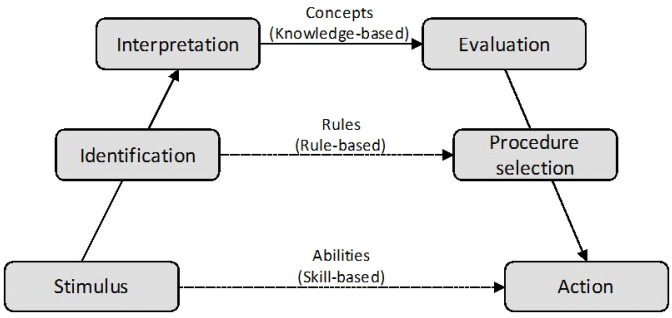

Figura 30 Modello di Rasmussen's skill-rule-knowledge [108]

Alla base del modello c'è il comportamento basato sulle competenze (skill-based) per il quale l'operatore, stimolato da un evento iniziatore reagisce in maniera quasi istantanea nel effettuare un'azione legata ad un procedimento che è stato accuratamente internalizzato.

A livello intermedio c'è il comportamento sulle regole (rule-based) con cui il gestore esegue una serie di azioni attraverso l'uso di procedure sulla base delle informazioni ricevute.

Al livello più elevato c'è il comportamento basato sulla conoscenza nel quale all'operatore è richiesta di utilizzare in maniera autonoma ed indipendente l'uso delle informazioni ricevuti e/o disponibili (senza l'uso di procedure o comportamenti istintivi) in modo da valutare e decidere quali siano le azioni più appropriate da prendere.

Gli errori possono accadere ad ogni passaggio o step del processo cognitivo ed il potenziale errore può essere identificato nell'analizzare ogni step cognitivo in modo da individuare dove possano esserci i problemi. La classificazione di Rasmussen permette di identificare tre tipi di errori:

- **Slips**: fallimenti che si verificano a livello di skill-based. L'operatore esegue in modo errato i compiti ben noti e di routine automaticamente con poca elaborazione mentale.
- **Lapses**: fallimenti in esecuzione causati dalla mancanza di memoria. In questo caso l'azione raggiunge un risultato diverso da quello previsto a causa di un errore di memoria seguendo una procedura nota. A differenza degli Slips, i Lapses non possono essere osservati direttamente
- **Mistakes**: errori non commessi durante l'esecuzione effettiva dell'azione. In questo caso è il piano stesso che non è valido, nonostante le azioni vengono eseguite come previsto.
- **Rule-based mistakes**: errori causati dalla applicazione della regola sbagliata o scorretta applicazione delle buone regole.
- **Knowledge-based mistakes**: errori dovuti alla mancanza di conoscenza o alla sua applicazione non corretta. Questo tipo di errore è insito nella razionalità limitata o comunque nella difficoltà di rispondere ai problemi che hanno una vasta gamma di possibili risposte ([103], [108]).

4.9 Metodologie e raccolta dati

La formalizzazione di un metodo è fondamentale per mettere in pratica i modelli del comportamento umano, le tassonomie e i dati acquisiti sull’ambiente di lavoro. Il metodo guida gli analisti nella decomposizione dei compiti, l'identificazione di potenziali errori umani connesse ai compiti analizzati, l'analisi dei contesti e delle prestazioni e nella quantificazione delle probabilità di errore.

Una caratteristica da considerare nella valutazione di un metodo è la sua capacità nel riprodurre la complessità dei fattori che influenzano il comportamento umano all'interno di modelli relativamente semplici. Pertanto, in generale, il metodo fornisce linee guida per l'identificazione di potenziali errori umani, nell'individuazione dei fattori di forma e di prestazione nonché di quantificazione della probabilità di errore.

Al fine di produrre risultati validi, il metodo di valutazione dell'affidabilità umana richiede che i dati di input significativi sulle probabilità di errore umano possano essere ottenuti da serie storiche, dai dati empirici o dalle sentenze di esperti del settore.

Tuttavia, nel campo della HRA la combinatoria dei dati empirici con il giudizio degli esperti permette di ridurre le incertezze che riguardano le informazioni empiriche. I dati frequentemente utilizzati nell' HRA sono estratti dal database dell'Human Failure nonostante i dati noti per il settore industriale siano meno rispetto a quelli dell'industria nucleare. Sebbene vi siano continui sforzi per raccogliere dati sulle prestazioni umane per applicazioni dell'HRA, il giudizio di esperti rimane una fonte di dati essenziale [109].

4.10 Human Performance: fattori di forma /SHAPING FACTORS

L'affidabilità delle prestazioni umane all'interno di un sistema socio-tecnico dipende da molti fattori che influenzano e descrivono le condizioni per gli errori. Questi fattori, che influenzano l'affidabilità dell'operatore nell' eseguire un compito (task), sono chiamati fattori forma prestazionali (shaping factors). Quasi tutti i metodi dell'HRA cercano di prendere in considerazione i fattori di contesto, in varia misura, con l'introduzione di coefficienti che pesano l'influenza di ciascun fattore sulle prestazioni umane. Secondo il metodo THERP, le PSF possono essere suddivisi in tre categorie principali [109]:

- External factors: Questi sono il risultato di caratteristiche organizzative e fisiche dell'ambiente di lavoro. Le caratteristiche organizzative indicano le procedure, informazioni, comunicazione, livelli gerarchici, strutture organizzative, flussi di lavoro, la pianificazione del lavoro e di esecuzione. Le caratteristiche fisiche, invece, riguardano le persone, e quindi l'affidabilità del sistema, tra cui la luce, rumore, vibrazioni meccaniche, l'interfaccia uomo-macchina, il clima, la sporcizia, umidità, pressione dell'aria, gas tossici e la radiazione.

- Internal factors: Questi fattori riguardano le caratteristiche ed i limiti umani ovvero le caratteristiche personali del singolo operatore (competenze, esperienza, formazione, conoscenza, motivazione e aspettative), le sue caratteristiche fisiche (antropometriche e biomeccaniche) e le sue caratteristiche psicologiche (fatica fisica e mentale, la noia). Altre caratteristiche come la leadership, la partecipazione, la cultura della sicurezza e il clima possono influenzare la motivazione e il comportamento umano.

- Stress factors: Questi includono il tipo e il numero di elementi stressanti che possono essere presenti nelle diverse situazioni.

4.11 Applicazione della System Dynamics all' HRA

Le azioni umane ed il tentativo di poterle quantificare sono utili per controllare, migliorare o regolare il comportamento del sistema; in altre parole, sono parte di un circuito chiuso causa-effetto [111].

L'utilizzo quindi della System Dynamics a supporto delle decisioni in un sistema HRA permette di valutare le possibili influenze e le variazioni sul sistema complesso intero. Infatti nella Causal Loop Diagram proposta si evidenzia lo sfasamento temporale tra causa ed effetto utilizzando l'operatore "ritardo".

La terza generazione di HRA, oggi in evoluzione, si concentra sulla performance umana ed i fattori relazioni e le loro dipendenze. Uno dei cosiddetti HRA dinamici è costituito dalle reti Bayesiane che tentano di superare alcune delle limitazioni dei metodi precedentemente illustrati mediante analisi qualitative che sottolineano l'importanza di rappresentare interazioni tra azioni umane e le dinamiche tra loro [105].

La HRA dinamica diventa oggi l'ultima generazione per HRA. Cacciabue [106] ha delineato l'importanza di simulazione e modellazione di prestazioni umane per il settore della sicurezza sui luoghi di lavoro. In particolare, le reti Bayesiane BBNs

sono messe a disposizione per captare "la natura incerta del rapporto tra prestazioni umane e il suo contesto organizzativo"[112]. Le BBNs sono state utilizzate per comprendere e catturare le relazioni tra PSFs e l'impatto quantitativo delle configurazioni PSFs sulla probabilità di errore

Tuttavia, dal confronto tra le due metodologie, ovvero le reti Bayesiane e System Dynamics, in accordo agli studi di Gregoriades [113], ne deriva che la SD è una metodologia maggiormente favorita nella modellazione e valutazione dell'effetto dell'errore umano anche in previsione futura. Ciò è dovuto al fatto che gli elementi cambiano dinamicamente nel tempo secondo le diverse condizioni. Gli esseri umani come agenti in tali sistemi sono influenzati in modo dinamico dall' ambiente del sistema in evoluzione [113]. L'utilizzo, quindi, della SD permette di superare le mancanze dei metodi di seconda generazione.

4.12 Causal Loop Diagrams (CLD) dell'errore umano

La Casual Loop Diagram costruita per studiare l'errore umano è mostrata nella **Figura 31.** In particolare si pongono in evidenza i seguenti aspetti:

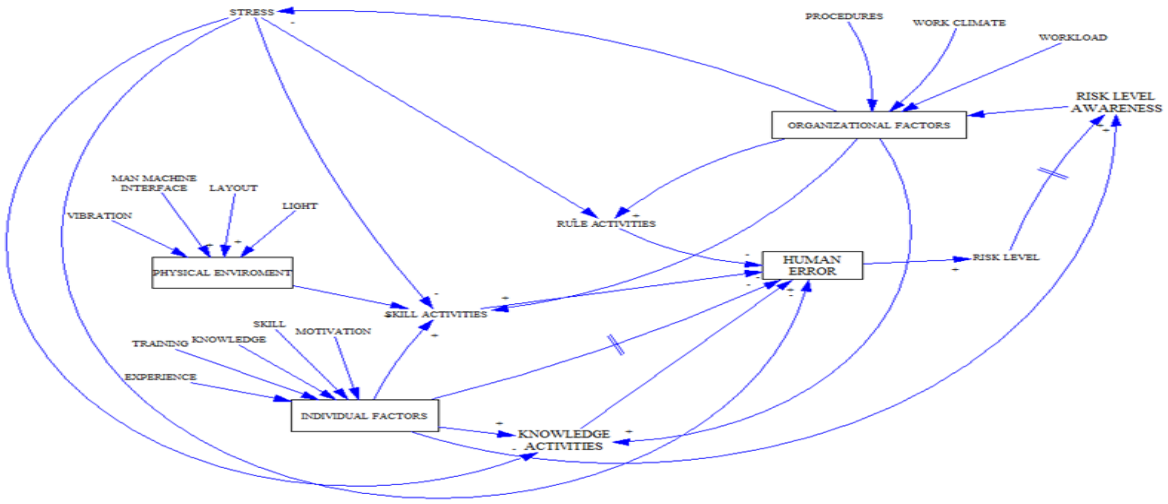

Figura 31 Casual Loop Diagram

- **Organizational factors**. Questi fattori sono definiti come fattori prestazionali di forma e che sono il risultato dei requisiti organizzativi e spesso possono essere descritti qualitativamente. Le caratteristiche organizzative riguardano le procedure, l'informazione, la comunicazione, i livelli gerarchici, le strutture organizzative, i flussi di lavoro, la pianificazione del lavoro e di esecuzione. Il processo organizzativo si riferisce alle decisioni aziendali e le regole che governano le attività quotidiane all'interno di un'organizzazione, compresa la creazione e l'uso di procedure operative standardizzate. Queste, in particolare, devono essere scritte in maniera chiara al fine di garantirne il rispetto da parte dell'operatore. Altre caratteristiche come la cultura della sicurezza e il clima possono influenzare la motivazione e il comportamento umano. La cultura si riferisce alle regole non ufficiali o non dette, valori, atteggiamenti, credenze e costumi di un'organizzazione mentre il clima organizzativo si riferisce a una vasta classe di variabili organizzative che influenzano le prestazioni dei lavoratori. In generale, tuttavia, il clima organizzativo può essere visto come l'ambiente di lavoro all'interno dell'organizzazione [103].
- **Physical environment**. In genere, la stazione di lavoro deve essere progettata per garantire livelli accettabili di benessere mentale, in modo che gli effetti negativi di tutti i fattori fisici (luce, rumore, vibrazioni meccaniche, clima, sporcizia, umidità, pressione dell'aria, gas tossici e radiazione) che interessano gli operatori dovrebbero essere minimizzati. L'interfaccia uomo-macchina deve essere progettata tenendo conto delle caratteristiche fisiche (antropometriche e biomeccaniche) e delle caratteristiche psicologiche (fatica mentale e noia) degli esseri umani. Questa interfaccia dovrebbe migliorare la usabilità della macchina [103].
- **Individual factors**. Questi fattori includono la formazione, abilità, esperienza, conoscenza e fattori motivazionali che, se appropriati consentiranno all'operatore di lavorare in modo più efficace. La motivazione è un fattore importante che influenza direttamente la decisione dell' agire.
- **Stress factors**. Il posto di lavoro resta una delle principali fonti di stress psicologico [113]. Lo stress è uno dei fattori studiati per analizzare il

comportamento del fattore umano nel lavoro. Per gli psicologi, esso è il risultato di qualsiasi emozione e che richiede una risposta o un cambiamento in una situazione specifica. Lo stress [115] può essere rappresentato come un processo in tre fasi principali influenzate da fattori personali, sociali e ambientali. Queste fasi sono: fattori di stress, lo stress e le conseguenze [116]. Fattori di stress sono esistenti nell'ambiente di lavoro. Lo stress, seconda fase del processo, può essere a lungo o a breve termine a seconda della natura dei fattori. Infine, le conseguenze, che sono manifestazioni comportamentali, eventi psicologici, fisiologici e organizzative, sono i risultati dello stress prolungato. La CLD sviluppata in Figura 32 pone in evidenza come l'errore umano sia influenzato da tre principali gruppi di variabili: fattori organizzativi, caratteristiche individuali e l'ambiente fisico. Secondo la tassonomia di Rasmussen ed il modello cognitivo, l'errore umano si verifica quando l'operatore effettua o rule-based activities o skill-based activities o knowledge-based activities.

Ciascuna di queste attività implica un aumento dei livelli di attenzione e risorse cognitive, in modo che ognuno di queste sia influenzata da diversi fattori. Se queste attività sono ben eseguite, può diminuire l'errore umano. A livello di attività skill-based, l'operatore esegue l'operazione automaticamente, in modo che i singoli fattori (capacità innate e la formazione), l'ambiente fisico (interfaccia uomo-macchina di supporto, il layout adeguato e altre caratteristiche fisiche) e fattori organizzativi (carico di lavoro) migliorano queste attività di routine, mentre i fattori di stress potrebbero avere un effetto negativo su di loro. A livello di rule-based activities, l'operatore esegue l'operazione mediante l'utilizzo di procedure, in modo che il grande miglioramento derivi da fattori organizzativi, in particolare dal lavoro ben fatto e da procedure ben seguite.

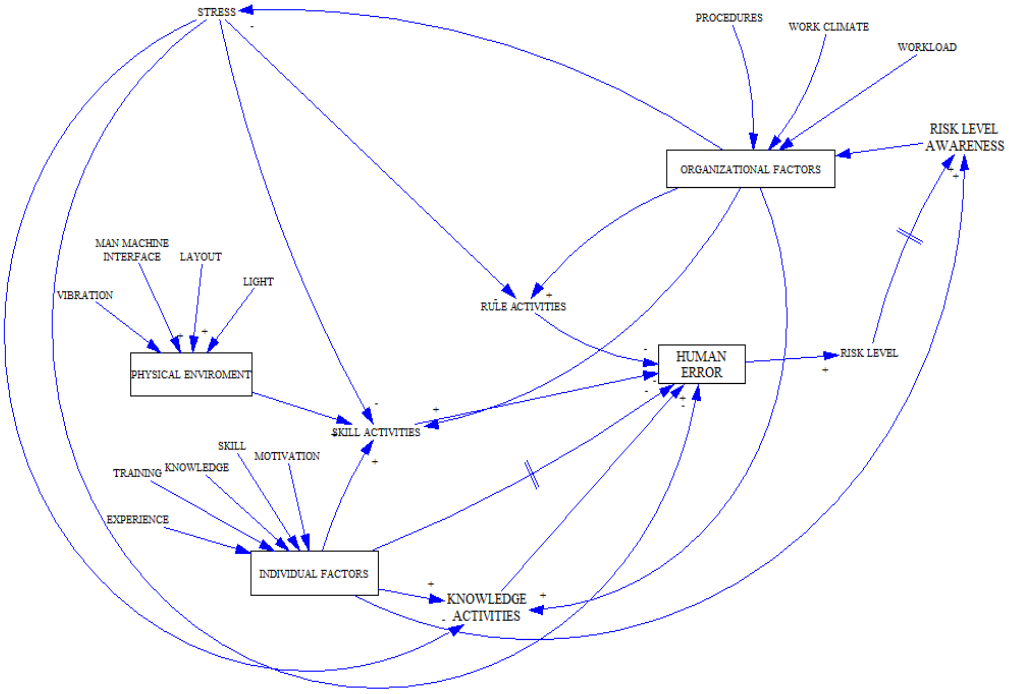

Figura 32 Casual effect diagram for human performance model

D'altra parte un effetto negativo potrebbe derivare da fattori di stress che possono indurre l'operatore a scegliere procedure sbagliate o applicarle in modo sbagliato.

A livello di Knowledge-based activities il gestore è tenuto a utilizzare creativamente e in modo indipendente le informazioni disponibili e la sua conoscenza (cioè senza usare procedimenti o comportamento istintivo), al fine di valutare e decidere quali saranno le azioni appropriate da effettuare, in modo che la maggiore influenza positiva potrebbe derivare da fattori individuali in termini di forte motivazione e di ricchezza di esperienze e conoscenze. Un impatto negativo sulle prestazioni della conoscenza deriva da fattori di stress.

Skill activities, rule activities, knowledge activities, nonché fattori individuali e lo stress contribuiscono alla manifestazione dinamica e danno luogo a errori umani e, indirettamente, aumentano il livello di rischio.

Il ciclo di feedback principale di questo modello incorpora l'errore umano, il livello di rischio, la consapevolezza del livello di rischio, i fattori organizzativi e lo stress. Il ciclo viene avviato dal verificarsi di un errore umano che aumenta successivamente il livello di rischio e la consapevolezza; quest'ultima a sua volta migliora i fattori organizzativi che aumentano il livello di stress. Tuttavia lo stress ha un effetto negativo sul verificarsi di un errore umano; questo costituisce un loop di rinforzo.

Il caso studio implementato ha visto l'applicazione di quanto all'azienda di GPL dell cui ciclo si è già discusso.

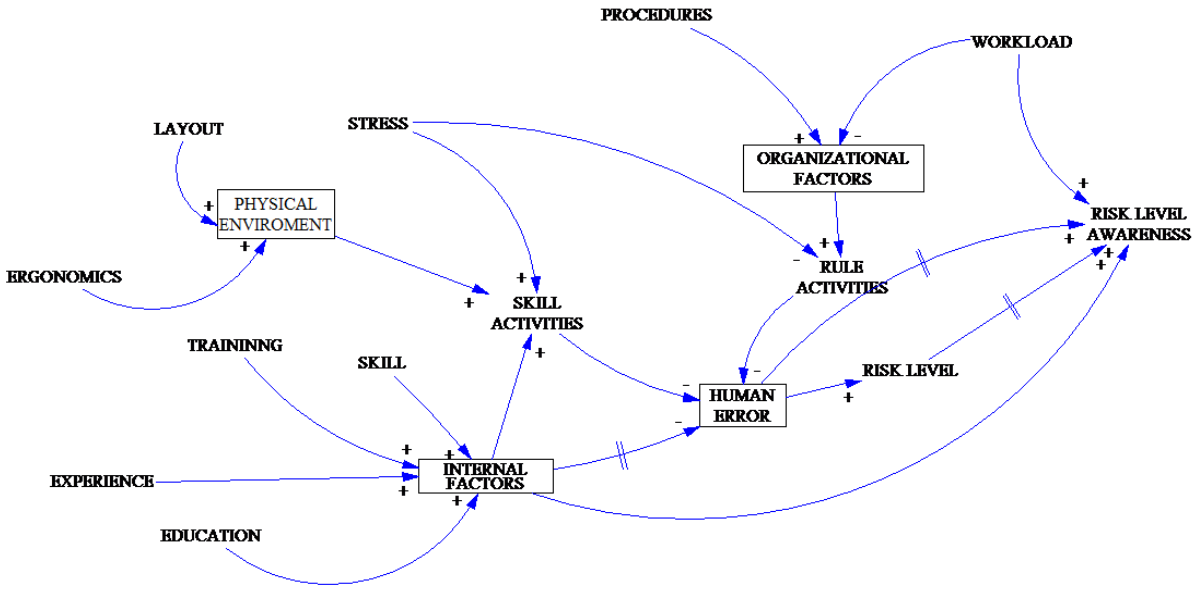

Figura 33 Causal Loop Diagram applied to Case Study

In particolare guardando le attività di carico e scarico, queste sono mnemoniche e di routine per cui si classificano all'interno delle skill activities con poco utilizzo dei processi mentali. Si deve considerare che le attività di routine e mnemoniche potrebbero indurre l'operatore nel fare errori. Pertanto, lo scopo è quello di comprendere, in questo specifico contesto, quali sono le variabili che entrano in gioco e le loro relazioni per valutare il loro impatto sull' errore umano e il livello di rischio. La formazione, le esperienze e competenze, acquisite nello svolgimento dei compiti

di routine, sono i principali fattori individuali che influenzano positivamente la capacità variabile "attività". Un elemento di stress che influenza negativamente le operazioni di routine dei driver è il carico di lavoro in termini di ore di guida che aumenta la probabilità di errore umano; nel CLD viene sottolineata la "ergonomia" ed il "layout". Si prevede un apporto positivo dato dall'ergonomia in termini di adeguata interfaccia uomo-sistema e un layout ben progettato aiuta a minimizzare l'errore umano.

Le fasi produttive, di carico e scarico, già ampiamente trattate sono caratterizzate da ben note procedure scritte che influenzano positivamente le "rule activities", riducendo l'errore umano, ma anche la "consapevolezza del livello di rischio" svolge un ruolo importante in termini di rischio percepito da parte dell'operatore.

Secondo questa analisi risulta evidente la relazione positiva tra consapevolezza del livello di rischio ed i fattori individuali quali l'istruzione e l'esperienza. Ma d'altra parte, il verificarsi di un errore umano aumenta il livello di rischio che incide con un certo *delay* sulla consapevolezza oggettiva del rischio che, per quanto sopra evidenziato, non dipende dai soli fattori individuali legati alla percezione del rischio.

4.13 Implementazione della Causal Loop Diagram

Al termine della trattazione, fin qui svolta, si ribadisce la complessità dello studio proposto. Il concetto di rischio risulta intimamente connesso a quello di Resilienza da un punto di vista safety. Si è proposto un modello organizzativo generale che potesse avere come fulcro la Resilienza. L'analisi proposta in ambito industriale oltre al focus sulle "operations" ha analizzato l'"Human Factor". In particolare quest'ultimo ha necessitato un approfondimento di una serie di problematiche, che solo apparentemente sono lontane dalle logiche ingegneristiche. Al termine si propone la seguente CLD implementata:

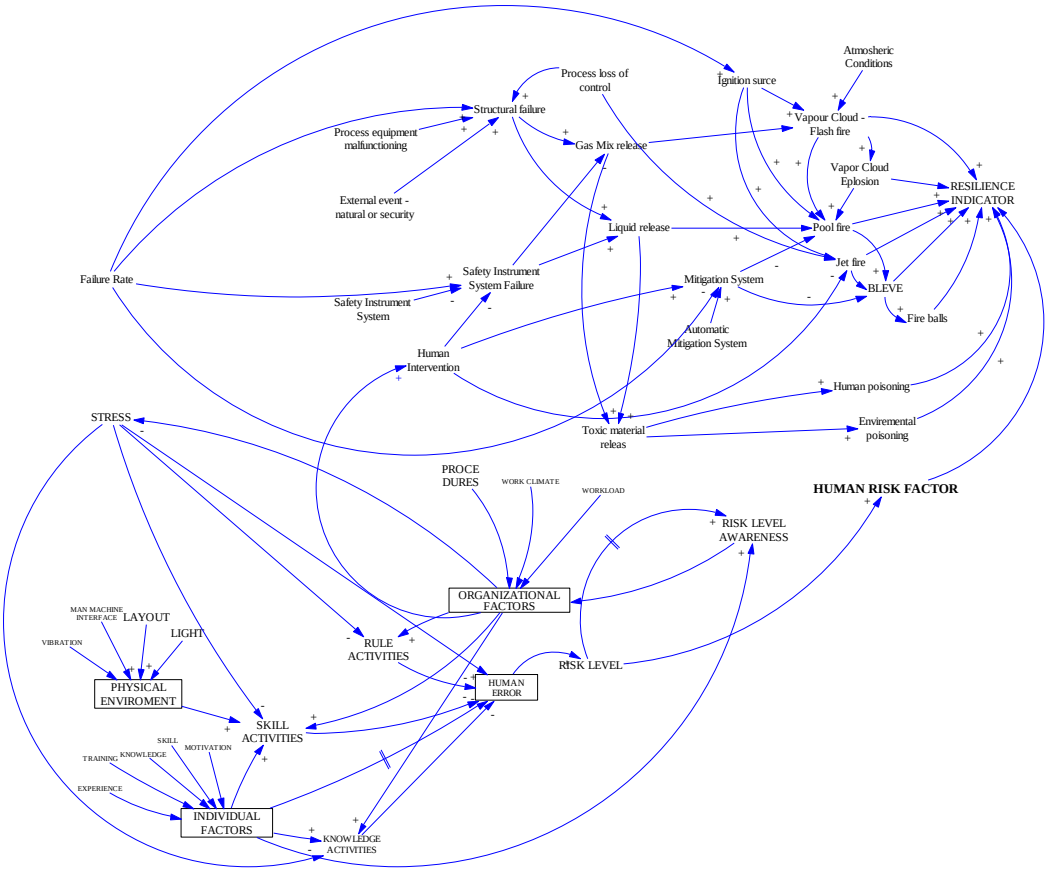

Figura 34 CLD implementata

4.14 Possibili scenari futuri

Il rischio diventa il termine ultimo da valutare e che si collega al modello generale (Figura 25), tenendo in considerazione tutti gli aspetti organizzativi e permette, infine, la valutazione della Resilienza.

Pertanto l'analisi del rischio, analizzando le singole fasi, diventa cosa complessa in quanto ciascuna area organizzativa è connessa alle altre e lo sviluppo del modello di simulazione per il quale si è in corso di approfondimento, risulta delicato. Ciascuna fase organizzativa ha richiesto e richiede un approfondimento che diventa uno studio quasi a se stante e che porta alla composizione del lavoro in generale. L'individuazione di un indice ha sia lo scopo di misurare la Resilienza di un certo sistema, sia quello di monitorarne l'andamento nel tempo, per vedere se esso sia migliorato o meno, permettendo di stabilire dove è più opportuno intervenire.

Una metrica rigorosa universalmente accettata, in grado di valutare in maniera obiettiva la Resilienza di un sistema complesso, come nel caso dell'industria di processo, deve ancora essere pienamente sviluppata per tutta una serie di motivi che vanno dalla dipendenza della Resilienza dal tipo di danno atteso, alle misure adattative che il sistema in esame è in grado di attuare.

Ciò è in parte riconducibile all'eccessivo numero di definizioni fornite dai vari autori e studiosi, molte delle quali non sono allineate col significato basilare del concetto di Resilienza: alcune di esse infatti apportano una visione soggettiva, che porta spesso a confondere la Resilienza con altri concetti, considerati erroneamente come sinonimi, quali flessibilità, robustezza.

Inoltre, gli approcci quantitativi studiati non risultano pienamente utilizzabili per la trattazione di sistemi generali. Pertanto è necessario sviluppare un metodo quantitativo che renda possibile lo sviluppo di sistemi resilienti e l'attuazione di strategie per renderli tali.

Conclusioni

L'attenzione rivolta alla problematica della Sicurezza degli impianti industriali, divenuta sempre più importante nel corso del tempo, ha permesso un decremento degli incidenti sul lavoro.

Questo si deve ad una Safety Culture sempre maggiore e che ha permesso il superamento del concetto stesso di sicurezza quale puro e mero aspetto normativo e che ha richiesto un vero approccio scientifico da parte del mondo della ricerca.

A tale scopo il Quantitative Risk Assessment (QRA) permette l'individuazione dei fattori di rischio (Hazards Identification) e la valutazione della probabilità di accadimento (Hazards Assessment) e le possibili conseguenze implicate (Risk Estimation). L'applicazione del QRA agli impianti industriali ha come fine ultimo la riduzione del rischio e quindi una corretta gestione della sicurezza (Safety Management). Tuttavia esso, mediante l'utilizzo di tecniche di valutazione strutturate, non favorisce una corretta valutazione delle probabilità del fenomeno incidentale. Infatti si è discusso (cfr. Capitolo III) come sia le tecniche quantitative sia qualitative presentino dei limiti che vengono superati grazie all'impiego della System Dynamics. Pertanto il Quantitative Risk Assessment è stato affrontato in modo tale da valutare l'evoluzione del rischio (e della sua gestione al fine di attuare le corrette misure di prevenzione) nel tempo in un'azienda di stampaggio plastico, considerando i possibili scenari incidentali che caratterizzavano tale realtà produttiva. In merito all'obiettivo prefissato (individuazione delle azioni per ridurre/controllare il rischio per la sicurezza nel contesto industriale e analisi della loro efficacia), l'applicazione della System Dynamics ha permesso l'interazione di differenti scenari incidentali e la loro evoluzione nel tempo. Tutto ciò è stato possibile grazie alla rappresentazione delle relazioni causali ovvero la Causal Loop Diagram. Tuttavia l'analisi condotta risulta, ad ogni modo, limitata al "solo" ambito incidentale considerato e non riesce in alcun modo ad analizzare quanto l'impianto sia in generale sicuro. Al fine di superare questo aspetto è stato introdotto (cfr. II capitolo) il concetto di Resilienza applicato ai sistemi industriali, in ambito della sicurezza. La Resilienza

viene definita come capacità a resistere e a riprendersi in seguito ad un evento avverso. Si è proposto un modello organizzativo (cfr.Capitolo IV) al cui centro ci fosse la Resilienza definita come il prodotto della vita del sistema (inteso come impianto) per la probabilità di accadimento di un incidente. L'analisi condotta ha preso in esame la Resilienza come particolare evoluzione del concetto di Rischio focalizzandosi sugli aspetti relativi agli eventi incidentali applicandola al caso studio di un impianto di processo, grazie al supporto della System Dynamics.

Si è notato come, inoltre, l'integrazione e la interazione delle varie funzioni aziendali, tutte concorrenti al risultato finale abbiano necessitato di un approfondimento riguardante il fattore umano e di come questo incida sul Rischio che è connesso alla Resilienza. L'aspetto del fattore umano è stato presentato in maniera sintetica, focalizzandosi sugli aspetti utili ai fini del modello proposto. Si è evidenziata l'influenza del fattore umano sul rischio e quindi sulla Resilienza integrandola nel modello generale. Tuttavia lo studio bibliografico ha posto in luce differenti definizioni di Resilienza

Ciò è in parte riconducibile all'eccessivo numero di definizioni fornite dai vari autori e studiosi, molte delle quali non sono allineate col significato basilare del concetto di Resilienza: alcune di esse infatti apportano una visione soggettiva, che porta spesso a confondere la Resilienza con altri concetti, considerati erroneamente come sinonimi, quali flessibilità, robustezza.

Per il futuro sarà necessario studiare approfonditamente ciascuna funzione organizzativa aziendale del modello proposto, grazie al supporto della System Dynamics, al fine di calcolare un indice di Resilienza completo necessario per analizzare il Resilience Indicator globale. Sarà inoltre necessario sviluppare una metrica rigorosa universalmente accettata, in grado di valutare in maniera oggettiva l'indicatore nel caso di un sistema complesso.

BIBLIOGRAFIA

[1]. I. Sutton, Process Risk and Reliability Management - Operational Integrity Management, Elsevier, 2010.

[2]. Woods D. D., Hollnagel E., Resilience Engineering: Concepts and Precepts, Ashgate Publishing Co., Aldershot, pp. 3-4, 2006.

[3]. Reiman, T., Oedewald, P., Measuring maintenance culture and maintenance core task with CULTURE questionnaire – a case study in the power industry. Safety Science, (2004) vol. 42, pp. 859–889.

[4]. International Nuclear Safety Advisory Group, Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna , 1991

[5]. Advisory Committee on the Safety of Nuclear Installations (ACSNI), Study Group on Human Factors, Third report: Organizing for safety, HMSO, London, 1993.

[6]. Schein, E.H., Organizational Culture and Leadership, second ed. Jossey-Bass, San Francisco, 1992.

[7]. Grote, G., Kunzler, C., Diagnosis of safety culture in safety management audits. Safety Science (2000) vol. 34, pp. 131–150.

[8]. Geller, E.S., Ten principles for achieving a Total Safety Culture. Professional Safety (September), (1994) pp. 18–24.

[9]. Cooper, M.D., Towards a model of safety culture. Safety Science (2000) vol.36, pp. 111–136.

[10]. Glendon, A.I., Litherland, D.K., Safety climate factors, group differences and safety behavior in road construction. Safety Science, (2001) vol. 39, pp. 157–188.

[11]. Neal, A., GriYn, M.A., Hart, P.M., The impact of organizational climate on safety climate and individual behavior. Safety Science, (2000) vol. 34, pp. 99–109.

[12]. Kennedy, R., Kirwan, B., Development of a hazard and operability-based method for identifying safety management vulnerabilities in high risk systems. Safety Science (1998) vol.30, pp. 249–274.

[13]. Richter, A., Koch, C., Integration, differentiation and ambiguity in safety cultures. Safety Science, (2004) vol.42, pp. 703-722.

[14]. Mohamed, S., Scorecard approach to benchmarking organizational safety culture in construction. Journal of Construction Engineering and Management, (2003) vol.1, pp. 80-88.

[15].S. Kaplan, B.J Garrick, On the Quantitative Definition of Risk, Risk Analysis, (1981) vol.1, pp. 11-27.

[16].ISO 31000:2009, Risk management: Principles and guidelines.

[17].L. Jingkai, Establishment of Emergency Management System Based on the Theory of Risk Management, Procedia Engineering, (2012) vol. 43 pp.108-112.

[18].Reason, J.: Human Error. Cambridge University Press, New York (1990)

[19]. R. J. Willey, Layer of Protection Analysis (2014 International Symposium on Safety Science and Technology), Procedia Engineering, (2014) vol.84, pp. 12-22.

[20].D. Besnard, G. Baxter, Human compensations for undependable systems, Technical Report Series, CS-TR-819, Newcastle upon Tyne: University of Newcastle upon Tyne, 2003.

[21].F. Khan, S. Abbasi, Multivariate hazard identification and ranking system, Process Safety Progress, (2004) vol.17, pp.157-170.

[22].M. Madonna et al., Il fattore umano nella valutazione dei rischi: confronto metodologico fra le tecniche per l'analisi dell'affidabilità umana, Prevenzione Oggi, (2009) pp.1-12.

[23].J. Rasmussen, Risk Management in a Dynamic Society: A modeling problem, 1997, Safety Science, (1997) vol.27, pp.183-212.

[24].Z.H. Quereshi, A review of accident modelling approaches for complex socio-techincal systems, Paper presented at the Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-related Programmable Systems (2007) vol. 86.

[25].J. Rasmussen, Risk Management in a Dynamic Society: A modeling problem, Safety Science, (1997) vol.27, pp.183-212.

[26].N. Leveson, A new Accident Model for Engineering Safer System, Safety Science, (2004) vol. 42, pp.237-270.

[27].F. Khan, S. Abbasi, Multivariate hazard identification and ranking system, Process Safety Progress, (2004) vol. 17, pp.157-170.

[28].Z.H. Quereshi, A review of accident modelling approaches for complex socio-techincal systems, Paper presented at the Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-related Programmable Systems (2007) vol. 86.

[29].A. Al-shanini et al, Accident modelling and analysis in process industries, Journal of Loss Prevention in the Process Industries, (2014) vol. 32 pp. 319-334.

[30].A.V. Lamsweerde, Formal Specification: A Roadmap. In Proceedings of the Conference on The Future of Software Engineering, New York , USA, (2000) pp.147-149.

[31].D.M. Woo, K.J. Vicente, Sociotechnical systems, risk management, and public health: comparing the North Battleford and Walkerton outbreaks, Reliability Engineering & System Safety, (2003) vol. 80, pp.253-269.

[32].E. Hollnagel, D.D. Woods, Joint Cognitive Systems: foundations of Cognitive Systems Engineering, New York: Taylor & Francis, 2005.

[33].Steen R., Aven T., A risk perspective suitable for resilience engineering, Safety Science (2011) vol. 49, pp. 292-297.

[34].Devanandham H., Ramirez – Marquez J. E., Generic metrics and quantitative approaches for system resilience as a function of time, Reliability Engineering and System Safety (2012) vol. 99, pp.114-122.

[35].Walker B., Holling C. S., Carpenter S. R., Kinzig A., Resilience, adaptability and transformability in social – ecological systems, Ecology and Society, 2004.

[36].Holling CS., Resilience and stability of ecological systems, Annual Review of Ecology and Systematics (1973), pp.1-23.

[37].Lengnick – Hall C. A., Beck T. E., Lengnick -Hall M. L., Developing a capacity for organizational resilience through strategic human resource management, Human Resource Management Review (2011) vol. 21, pp. 243-255.

[38].Craighead C. W., Blackhurst J., Rungtusanatham M. J., Handfield R. B., The severity of supply chain disruptions: design characteristics and mitigation capabilities, Decision Science, (2007) vol. 38, pp. 131-156.

[39].Junming Z., Matthias R., Exploring the resilience of industrial ecosystems, Journal of Environmental Management (2013) vol. 122, pp. 65-75.

[40].Barker K., Ramirez – Marquez J. E., Rocco C. M., Resilience – based network component importance measures, Reliability Engineering and System Safety (2013) vol. 117, pp. 89-97.

[41].Vlacheas P., Stavroulaki V., Demestichas P., Cadzow S., Ikonomou D., Gorniak S., Towards end – to – end network resilience, International Journal of Critical Infrastructure Protection (2013) vol.6, pp. 159-178.

[42].Baas L. W., Boons F. A., An industrial ecology project in practice: exploring the boundaries of decision – making levels in regional industrial systems, Journal of Cleaner Production, (2004) vol.12, pp. 1073-1085.

[43]. Shirali G. H. A., Motamedzade M., Mohammadfam I., Ebrahimipour V., Moghimbeigi A., Challenges in building resilience engineering (RE) and adaptive capacity: a field study in a chemical plant, Process Safety Environment, (2012) vol.90, pp. 83 – 90.

[44]. Steen R., Aven T., A risk perspective suitable for resilience engineering, Safety Science (2011) vol. 49, pp. 292-297.

[45]. Dinh L. T. T., Pasman H., Gao X., Mannan M.S., Resilience engineering of industrial process: principle and contributing factors, J. Loss Prevent. Proc., (2012) vol. 25, pp. 233-241.

[46]. Costella M. F., Saurin T. A., Macedo Guimaraes L. B., A method for assessing health and safety management systems from the resilience engineering perspective, Safety Science, (2009) vol. 47, pp. 1056-1067.

[47]. Azadeh A., Salehi V., Ashjari B., Saberi M., Performance evaluation of integrated resilience engineering factors by data envelopment analysis: The case of a petrochemical plant, Process Safety and Environmental Protection (2013).

[48]. Hollnagel E., Woods D. D., Leveson N., Resilience Engineering: Concepts and Precepts. Ashgate Publishing Co., Aldershot, (2006), pp. 289-314.

[49]. Saurin T. A., Carim Junior G. C., Evaluation and improvement of a method for assessing HSMS from the resilience engineering perspective: A case study of an electricity distributor, Safety Science (2011) vol.49, pp. 355-368.

[50]. Sheffi Y., Building a resilient organization, The Bridge – The Journal of National Academy of Engineering, (2007), pp. 37-30.

[51]. Storseth F., Tinmannsvik R., Oien K., Buildindg Safety by Resilient Organization – A Case Specific Approach, ESREL (2009), pp. 7-10.

[52]. B. Knegtering, H.J. Pasman, Safety of the process industries in the 21st century: a changing need of process safety management for a changing industry, Journal of Loss Prevention in the ProcessIndustries, (2009) vol.22, pp. 162–168.

[53]. Pasman H. J., Knegtering B., Rogers W. J., A holistic approach to control process safety risks: Possible ways forward, Reliability Engineering and System Safety (2013) vol. 117, pp. 21-29.

[54]. Hollnagel E., The changing nature of risks, Ergonomics Australia Journal (2008) vol.22, pp. 33-46.

[55]. Aven T., On how to define, understand and describe risk, Reliability Engineering and System Safety (2010) vol. 95, pp. 623-631.

[56].R. Steen, T. Aven, A risk perspective suitable for resilience engineering, Safety Science, (2011) vol. 49, pp. 292-297.

[57].Sgourou E., Assessment of selected safety performance evaluation methods in regards to their conceptual, methodological and practical characteristics, Safety Science, (2010) vol. 48, pp. 1019-1025.

[58].Cassano – Piche A. L., Vicente K. J., Jamieson G. A., A test of Rasmussen's Risk Management Framework in the food safety domain: BSE in the UK, Theor. Issues Ergonom. Sci., (2009) vol. 10, pp. 283-304.

[59].Trotter M. J., Salmon P. M., Lennè M. G., Impromaps: Applying Rasmussen's Risk Management Framework to improvisation incidents, Safety Science (2014) vol.64, pp.60-70.

[60].Burtscher M. J., Manser T., Team mental models and their potential to improve teamwork and safety: a review and implications for future research in healthcare, Saf. Sci., (2012) vol.50, pp. 1344-1354.

[61].Carvalho P., dos Santos I., Gomes J., Borges M., Micro incident analysis framework to assess safety and resilience in the operation of safe critical systems: a case study in a nuclear power plant, J. Loss Prevent. Proc., (2008) vol.21, pp. 277-286.

[62].Baruth KE, Carroll JJ., A formal assessment of resilience: the baruth protective factors inventory, Journal of Individual Psychology Fall (2002) vol. 58, pp. 3-12.

[63].Connor KM, Davidson JRT., Development of a new resilience scale: the Connor – Davidson Resilience Scale (CD – RISC), Depression & Anxiety (2003) vol. 18, pp. 234-241.

[64].Reed DA, Kapur, Christie RD., Methodology for assessing the resilience of networked infrastructure, IEEE Systems Journal (2009) vol. 3, pp.174-180.

[65].Ferrario E., Zio E., Goal Tree Success Tree – Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems, Engineering Structures (2014) vol. 59, pp.411-433.

[66].D. Henry, J. E. Ramirez-Marquez, Generic metrics and quantitative approaches for system resilience as a function of time, Reliability Engineering and System Safety, (2012) vol. 99, pp. 114-122.

[67].K. Barker et al., Resilience based-network component importance measures, Reliability Engineering and System Safety, (2013) vol. 117, pp. 89-97.

[68].Shirali Gh. A., Mohammadfam I., Ebrahimipour V., A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a

process industry, Reliability Engineering and System Safety (2013) vol. 119, pp. 88-94.

[69].Zobel C. W. Representing perceived tradeoffs in defining disaster resilience, Decision Support System (2011) vol. 50, pp. 394-403.

[70].R. Francis, B. Bekera, A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliability Engineering and System Safety, (2014) vol. 121, pp. 90–103.

[71].E.D. Vugrin et al., A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane, Process Safety Progress, (2011) vol. 30, pp. 280-290.

[72].S. Kaplan, The words of risk analysis, 1997, Risk Analysis, (1997) vol. 17, pp. 407-417.

[73].H. Pasman et al., Resilience engineering of industrial processes: Principles and contributing factors, Journal of Loss Prevention in the Process Industries, (2012) vol.25, pp. 233-241.

[74].E. Hollnagel et al., Resilience Engineering in Practice. A Guidebook , Farnham, UK: Ashgate, 2011.

[75].P.M. Senge, The Fifth Discipline: The Art & Practice of The Learning Organization, Doubleday; Revised & Updated edition (March 21, 2006).

[76].S. Brambilla, D. Manca, Recommended features of an industrial accident simulator for the training of operators, Journal of Loss Prevention in the Process Industries, (2011) vol. 24, pp. 344-355.

[77].J.W. Forrester, Industrial Dynamics, MIT Press, Cambridge, 1961.

[78].J.D. Sterman, Business Dynamics: Systems Thinking and Modeling for a Complex World, McGraw-Hill, 2006.

[79].C.W. Kirkwood, System Dynamics Method: A Quick Introduction, 2010.

[80].R. Špicar, System Dynamics Archetypes in Capacity Planning, Procedia Engineering, (2014) vol.69, pp. 1350-1355.

[81].J.M. Garcìa, Theory and Practical Exercises of System Dynamics, Universitat Politecnica De Catalunya, Barcelona, Spain, 2006.

[82].Gallo M., Di Nardo M., Santillo L. C., A simulation based approach to support risk assessment, Recent Advances in Automatic Control, Modelling and Simulation, 2013.

[83].M. Bahrami, D.H Bazzaz, S.M Sajjadi, Innovation and Improvements In Project Implementation and Management; Using FMEA Technique, International Conference on Leadership, Technology and Innovation Management, 2012

[84].R. Gowland, The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A stepforward towards convergent practices in risk assessment? Journal of Hazardous Materials, (2006), pp. 307-310.

[85].S.A. Markowski,M.S Mannan, ExSys LOPA for the chemical process industry, Journal of Loss prevention in the process industries, (2010), pp. 688-696.

[86].R.A Bradshaw, G.L. Illaszewiz, Y.G. Avrahamson, Introducing layer of protection analysis for water risk assessments, Water Quality Research Journal of Canada, (2013) vol.48, pp. 76-84.

[87].D.Yu, Z. Pei, Z. Yaqiao, Z. Xuekui, Z. Yunsheng, Simulation experiment of safety experience based on system dynamics, International Symposium on Safety Science and Technology, Procedia Engineering (2012) vol.45, pp. 199-203.

[88].P.M. Myers, Layer of Protection Analysis – Quantifying human performance in initiating events and independent protection layers, Journal of Loss Prevention in the Process Industries, (2012), pp. 1-13.

[89].H. Gang, Simulation Analysis of Coal Mine Safety Management Based on System Dynamics, Energy Procedia (2012), pp. 270- 274.

[90].D. Yu, Z. Pei, Z. Yaqiao, Z. Xuekui, Z. Yunsheng, Simulation experiment of safety experience based on system dynamics, Procedia Engineering, (2012) vol.45, pp. 199-203.

[91].Y. M. Goh, P.E.D Love, G. Stagbouer, C. Annesley, Dynamics of safety performance and culture: A group model building approach, Accident Analysis and Prevention, (2012), pp. 118-225.

[92].J.Michael Spector, Dean L Christensen D., Sioutine A.V, McCormack D., Models and simulations for learning in complex domains: using causal loop diagrams for assessment and evaluation, Computers in Human Behavior, Issues 5–6, (2001) vol. 17, pp. 517-545.

[93].E. Garbolino, J-P Chery, F. Guarnieri, System Dynamics modelling to improve risk analysis in the context of Seveso Industries, Journal of loss in Prevention, AIDIC Conferences, (2009) vol. 9, pp. 149-158.

[94].Dowell III A. M., Layer of protection analysis for determining safety integrity level, ISA Transactions (1998) vol. 37, pp. 155-165.

[95].Salzano E., Di Nardo M., Gallo M., Oropallo E., Santillo L.C., The application of System Dynamics to industrial plants in the perspective of Process Resilience Engineering, Chemical Engineering Transactions, (2014) vol. 36.

[96].Di Nardo M., Gallo M., Madonna M., Santillo L.C., A Conceptual Model of Human Behaviour in Socio-technical Systems, SOMET, Naples, 2015.

[97].F. Kadri et al., The Assessment of Risk Caused by Fire and Explosion in Chemical Process Industry: A Domino Effect-Based Study, Journal of Risk Analysis and Crisis Response, (2013) vol. 2, pp. 66-76.

[98].E Hollnagel , Resilience engineering, PSYKOLOGIA 42 (6), (2007), 493.

[99].Lekka C. and Sugden C., The Successes and Challenges of Implementing High Reliability Principles: a Case Study of UK Oil Refinery. Process Safety and Environmental Protection, (2011) vol. 89, pp. 443-451.

[100]. Mannam S., Lees's Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control, 3rd Ed., Elsevier Butterworh-Heinemman, Burlington, MA, USA, 2005.

[101]. Vilchez J.A., Espejo V., Casal J., Generic event trees and probabilities for the release of different types of hazardous materials, J Loss Prevent Proc. (2011) vol. 24, pp. 281-287.

[102]. Madonna, M., Martella, G., Monica, L., Pichini Maini, E., Tomassini, L., The human factor in risk assessment: methodological comparison between human reliability analysis techniques. Prev. Today, (2009) vol. 5, pp. 67-83.

[103]. IEC 62508: Guidance on human aspects of dependability (2010)

[104]. Di Pasquale, V., Iannone, R., Miranda, S., Riemma, S., An overview of human reliability analysis techniques in manufacturing operations. In: Schiraldi, M. (ed.) Operations Management, INTech-Open Access Publisher, Osaka (2013), pp. 221–240.

[105]. Di Pasquale, V., Miranda, S., Iannone, R., Riemma, S., A simulator for human error probability analysis (SHERPA). Reliab. Eng. Syst. Saf. (2015) vol. 139, pp. 17–32.

[106]. Cacciabue, P.C., Guide to Applying Human Factors Methods. Springer, London, 2004.

[107]. Harwood, K., Sanderson, P., Skill, rules and knowledge: a discussion of Rasmussen's classification. In: Human Factor Society. A Cradle for Human Factors. Proceedings of the Human Factors Society 30th Annual Meeting, Dayton (OH), USA, (1986), pp. 1002.

[108]. Rasmussen, J., Human errors: a taxonomy for describing human malfunction in industrial installation. J. Occup. Accid., Elsevier Scientific Publishing Company (1982) vol. 4, pp.311–333

[109]. Forester, J., et al., The International HRA Empirical Study – final Repot – lessons Learned from Comparing HRA Methods Predictions TO HAMMLAB Simulator Data. HPR -373 OECD Halden Reactor Project, Norway, 2013.

[110]. Swain, A.D., Guttmann, H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, US Nuclear Regulatory Commission. Washington, DC (1983)

[111]. Sterman, J.D., Business Dynamic: System Thinking and Modeling for a Complex Word. Irwin McGraw-Hill, Boston (2000)

[112]. Mohaghegh, Z., Kazemi, R., Mosleh, A., Incorporating organizational factors into probabilistic risk assessment (PRA) of complex socio-technical systems: a hybrid technique formalization. Reliab. Eng. Syst. Saf., (2009) vol. 94, pp.1000-1018.

[113]. Gregoriades, A., Human error assessment in complex socio-technical systems-system dynamic versus Bayesian belief network. In: System Dynamics Conference, Manchester, 2008.

[114]. Marchand, A., Demers, A., Durand, P., Does work really cause distress? The contribution of occupational structure and work organization to the experience of psychological distress. Soc. Sci. Med., (2005) vol. 61, pp. 1-14.

[115]. Hart, P., Cooper, C., Occupational Stress: toward a more integrated framework. In: Anderson, N., Ones, D.S., Sinangil, H.K., Viswesvaran, C. (eds.) Handbook of Industrial Work and Organizational Psychology, vol. 2. Sage, London, 2001.

[116]. Harvey, S., Courcy, F., Petit, A., Hudon, J., Teed, M., Loiselle, O., Morin, A., Organizational interventions and psychological health in the work: a synthesis of Approaches. Report, Institute de Research en Sante et Securitie au Travail (IRSST), Montreal, 2006.