POLITECNICO DI TORINO

Collegio di Ingegneria Chimica e dei Materiali

Corso di Laurea Magistrale

in Ingegneria Chimica e dei Processi Sostenibili

MSc Thesis

Requirements for a web-based tool for operational risk management

Relatori

firma del relatore (dei relatori)

prof.ssa Micaela Demichela

prof.ssa Maria Chiara Leva

Candidato

Peritore Paride

Luglio 2018

Index

Figures Index

Tables Index

Symbols Index

E(t): Mean time to failure function

F(t): Unreliability function

f(t): Density function

h(t): Failure rate function

i: Return rate

R(t): Reliability function

t: Time

X: Generic Element

λ: Failure rate

1. Italian abstract

Viviamo in un mondo con un avanzamento tecnologico continuo e progressivo, un avanzamento tecnologico finalizzato a soddisfare ogni bisogno, piacere e necessità dell'essere umano. Tuttavia, la tecnologia per la gestione del rischio sembra aver difficoltà a svilupparsi così rapidamente come in molti altri settori.

Lo scopo del seguente lavoro, svolto in collaborazione con l'Istituto di Tecnologia di Dublino (DIT) e Tosca Human Factor Solutions LTd, con sede al Trinity College di Dublino (TCD), è stato quello di creare un software tecnologicamente avanzato in grado di identificare, analizzare, valutare e monitorare il rischio usando le linee guida presenti e ampiamente discusse in letteratura.

Il termine rischio, dal francese *risqué,* è stato descritto in diversi modi nel corso degli anni e risulta impossibile darne una definizione univoca. Generalmente la definizione di rischio utilizzata, e quella adottata in questo lavoro, è ricavata dalla normativa ISO:31000:2009, che definisce il rischio come "*Effect of uncertainty on objectives"*. L'effetto degli obiettivi non è però da intendersi prettamente come un evento negativo, quindi come un incidente, una perdita finanziaria, un problema di sicurezza. Gli *objectives,* d'altra parte, fanno riferimento ad eventi di diversa origine ed aspetto: sia eventi della vita quotidiana, sia incidenti dal decorso più o meno spiacevole.

L'attenzione crescente da parte delle compagnie per la gestione del rischio ha portato, a partire dagli anni '80, alla nascita di vere e proprie banche dati, addette alla raccolta dei principali incidenti nei luoghi di lavoro. Col passare degli anni, inoltre, si è cercato di fornire sempre maggiori informazioni relative al rischio, al fine di avere dati più dettagliati e che sappiano descrivere efficacemente il rischio in tutte le sue sfaccettature. Per questo, le compagnie registrano (o almeno dovrebbero registrare) in un apposito registro dei rischi, ogni rischio che si presenta all'interno dei loro stabilimenti. Il registro dei rischi si presenta a questo punto come un valido strumento di reportistica, ampiamente discusso in letteratura, che permette di analizzare, valutare e monitorare qualsiasi tipo di rischio all'interno della compagnia.

Al fine di identificare, analizzare, valutare e monitorare il rischio, è necessaria una approfondita conoscenza del processo e una notevole esperienza da parte degli analisti. Generalmente, la valutazione del rischio può essere eseguita tramite l'utilizzo di diverse tecniche e metodologie. Questi metodi sono ampliamente descritti dalla ISO 31010:2009 che accuratamente descrive gli svantaggi, i punti di forza e la migliore applicazione per oltre trenta metodi di valutazione del rischio. Solo dopo l'utilizzo di una o più tecniche sarà possibile un corretto inserimento del rischio valutato all'interno del registro dei rischi. Una limitazione del registro dei rischi evidenziata in questo lavoro è l'impossibilità di avere una analisi funzionale legata alle fasi operative del processo, in quanto esso si focalizza soltanto sulle apparecchiature e le unità tecniche dell'impianto, senza tener conto di procedure correlate tra di loro.

In questo lavoro di tesi è stata accolta la richiesta di una società elettrica irlandese, addetta alla generazione e vendita di energia alla Repubblica di Irlanda e al Regno Unito, di modernizzare il loro registro dei rischi (GRR) esistente e il loro registro delle apparecchiature critiche (CAR). Questi due registri sono attualmente sviluppati come fogli di calcolo condivisi tra i singoli impianti e gli uffici amministrativi tramite l'utilizzo di Microsoft SharePoint. I fogli di calcolo contengono una mole di informazioni non indifferente e una struttura tale da non consentire all'utente inesperto di interfacciarsi con semplicità con i dati presenti. Lo scopo di questo lavoro è stato quindi quello di sviluppare un nuovo prototipo di registro dei rischi che possa fungere da sintesi tra GRR e CAR, cercando di evitare perdite di informazioni. Le linee guida del prototipo, dettate dal *Risk Project Manager* della società di generazione elettrica irlandese, sono state seguite quanto più possibile dagli sviluppatori informatici di Tosca Human Factor Solutions ai fini delle loro analisi: essi hanno infatti cercato di riadattare alle necessità della compagnia il loro già preesistente registro dei rischi. Tale registro, come mostrato più avanti in questo lavoro, è un *web-based* software di nuova generazione, con una interfaccia *user-friendly* e già usato da un aeroporto regionale italiano. Il software di recentissimo sviluppo ha inoltre catturato l'attenzione di numerose compagnie in diverse parti del mondo, specializzate in vari settori, dal petrolchimico all'industria mineraria, passando per la gestione della sicurezza aeroportuale. Secondo richiesta della società elettrica irlandese, gli sviluppatori di Tosca Solutions hanno anche creato un ulteriore modulo che permetta la valutazione delle opzioni di investimento, aiutando l'utente a decidere quale investimento possa portare maggiori benefici all'impianto. La scelta del migliore piano di investimento si è basata sulla comparazione dei diversi indici di investimento, calcolati come NPV (*Net Present Value*) dei benefici rapportati al NPV dei costi. L'opzione di investimento viene valutata attraverso la sua evoluzione in diversi anni, al fine di poter stimare come il valore del rischio e la relativa perdita monetaria vari durante tale periodo e quindi come un investimento mirato possa permettere di ridurre tale rischio.

Il registro dei rischi creato da Tosca Solution, però, essendo ancora in continuo sviluppo, mira ad ampliarsi ulteriormente, in particolare per l'inserimento di un nuovo modulo che permetta l'analisi funzionale di procedure. Questo modulo, ancora non esistente, si baserà sul modello logico probabilistico affiancato da un modello fenomenologico già utilizzato da IDDA (*Integrated Dynamic Decision Analysis)*. IDDA è un software ideato da Remo Galvagni, che consente di conseguire un'analisi integrata di procedure all'interno degli impianti, ma è anche un sistema capace di indicare la possibilità di accadimento di ogni sequenza di eventi che è possibile trovare all'interno del processo. Un secondo caso studio quindi è stato condotto per approfondire come il nuovo modulo di analisi dinamica decisionale possa affiancare un registro dei rischi nella valutazione e gestione del rischio all'interno di un impianto. Il suddetto caso studio si basa sulla fase di scarico/carico di ammoniaca all'interno di un impianto predisposto. Dopo un'iniziale identificazione delle procedure che vengono eseguite nell'impianto e le possibili conseguenze che potrebbero scaturire da ognuna di esse, è necessario convertire in corretta sintassi la serie di operazioni, e il modo in cui esse siano correlate tra loro, per permettere al software di poter analizzare il processo. A questo punto, la sequenza di informazioni che IDDA restituisce è compatibile con un albero degli eventi "potenziato" che tiene conto dinamicamente di come ogni procedura possa influenzare una o più diverse operazioni del processo.

Nel primo capitolo di questo lavoro si è deciso di fare una introduzione al concetto di rischio, andando a ripercorrere le varie definizioni che gli sono state assegnate nel corso degli anni in

letteratura e come la definizione della organizzazione internazionale di standardizzazione, nella sua ISO 31000 pubblicata nel 2009, venga universalmente riconosciuta come definizione più rigorosa, ma nel contempo altamente versatile. La stessa normativa fornisce una misura quantitativa del rischio, definendolo come combinazione lineare di probabilità e conseguenza dell'evento (Equazione 1). Nel testo è anche riportata una interessante rappresentazione grafica (vedere Figura 3.1 all'interno del testo) nella quale su un grafico severità su probabilità sono tracciate delle curve "iso-rischio". Agendo su un generico punto della curva, cercando di diminuire la probabilità, si parla di prevenzione; cercando di diminuirne le conseguenze, si parlerà di protezione. In ogni caso si vuole sottolineare come, anche cercando di agire contemporaneamente su probabilità e conseguenze, è impossibile annullare il rischio e parlare di "rischio zero". Come si nota dalla Figura 3.1, tramite gli assi è inoltre possibile andare a definire tre possibili categorie di rischio:

- Rischio Tollerabile: rischi con elevata frequenza di accadimento e bassa severità di impatto. Sono rischi largamente accettati nella vita quotidiana;
- Rischio convenzionale (ALARP): eventi moderatamente frequenti con una intensità di danno medio-elevata. L'acronimo ALARP (*As low as reasonably practicable)* è un principio finalizzato a ridurre il rischio nella maniera più ragionevole possibile;
- Rischio Intollerabile: sono rischi causati da anomalie maggiori, caratterizzati da una grave conseguenza ma probabilità di accadimento molto bassa.

Gli stessi rischi possono essere anche collocati all'interno di quella che è comunemente definita la piramide dei rischi, una struttura che permette di avere una definita e chiara visione di insieme.

La probabilità di accadimento, così come la severità di un rischio, sono generalmente stimate su una scala di numeri interi. In questo testo verrà usata sempre una scala numerica che spazia da uno a cinque, nella quale il valore più basso rappresenta la probabilità/severità minore. In questo modo, quindi, diventa possibile quantificare numericamente il rischio tramite la moltiplicazione algebrica tra valore di probabilità e valore di severità. Utilizzare la matrice di rischio come mezzo di supporto per quantificare il rischio è una pratica largamente diffusa e accettata in ogni compagnia e azienda, in quanto fornisce una rappresentazione grafica di facile comprensione. In letteratura sono state analizzate diverse matrici di rischio e sono stati studiati i vantaggi e gli svantaggi che l'uso ne comporta. Tra i problemi principali riportarti troviamo sicuramente la cosiddetta "*range compression"*, ovvero la categorizzazione del rischio all'interno di un'errata casella della matrice a causa di un errore in fase di valutazione del rischio, e la mancanza di oggettività nell'utilizzo della matrice di rischio, in quanto la probabilità e la severità sono stimate in modo soggettivo dagli analisti.

Colore	*Valori*	*Livello di rischio*	*Commento*
Rosso	16-25	Estremamente alto	Inaccettabile. Richiesti immediati provvedimenti
Arancione	11-15	Alto	Necessari immediati controlli
Giallo	6-10	Moderato	Necessari giudizi a riguardo
Verde	1-5	Basso	Monitorare e gestire

Tabella 1.1: Da una matrice del rischio è possibile estrarre tali informazioni.

In letteratura esistono svariate informazioni riguardo le tecniche e i metodi analitici comunemente usati per la gestione del rischio: specialmente la ISO 31010:2009 esegue una lodevole trattazione in merito, che sarà discussa più avanti in questo testo. Fondamentalmente possiamo dividere i metodi in tre categorie:

- Metodi induttivi;
- Metodi deduttivi;
- Metodi basati su processi stocastici.

I metodi induttivi sono basati sulla domanda "Cosa succede se …?", generalmente posta da un team di analisti con diverse conoscenze del sistema. Un esempio di metodo induttivo riportato all'interno della normativa ISO 31010 è il *Brainstorming,* spesso supportato da una check-list per avere un'analisi quanto più dettagliata possibile del sistema. I metodi deduttivi, d'altro canto, sono basati sulla domanda "Perché...?" posta sempre da un team di esperti del sistema. Un metodo deduttivo descritto nella normativa ISO 31010 è il *Fault Tree,* che si basa sulla rappresentazione grafica degli eventi che hanno portato ad un evento indesiderato, definito *Top Event*. Infine, i metodi basati su processi stocastici tengono conto del comportamento dinamico del sistema.

Tra questi, i metodi più utilizzati sono generalmente le catene Markoviane e il metodo Montecarlo. Non tutte le tecniche possono però descrivere efficacemente rischi di diversa origine, quindi il team di analisti deve essere in grado di decidere quale metodo conviene usare in base al rischio in esame. I rischi dovuti a procedure, infatti, prevedono un'analisi funzionale del sistema ed un approccio di tipo dinamico, che tiene conto delle relazioni tra i diversi eventi del processo. Le tecniche comunemente più usate e riconosciute, generalmente trattate anche in ambito accademico sono:

- HazID, ovvero *Hazard Identification studies:* è un metodo utilizzato per identificare rischi di qualsiasi tipo ed usato spesso nelle fasi preliminari di progetto dell'impianto, tenendo conto di tutte le apparecchiature tecniche e le procedure di sicurezza presenti nel sistema in esame;

- HAZOP, ovvero *Hazard and Operability stuedies:* permette di avere una analisi funzionale qualitativa del sistema basata sull'identificazione delle possibili deviazioni del sistema rispetto al processo ottimale. È richiesta una notevole conoscenza del sistema per poter realizzare un'analisi sistematica e metodologica delle procedure;

- FMEA, ovvero *Failure Mode and Effect Analysis:* è un metodo induttivo basato sulla domanda "Cosa succede se…?". Questo metodo è stato largamente discusso in letteratura e analizzato dalla ISO 31010, in quanto permette di identificare tutte le possibili modalità di guasto delle varie parti del sistema, gli effetti che tali guasti hanno sul processo, i meccanismi di guasto e come evitare e mitigare gli effetti del guasto analizzato;

- FTA, ovvero *Fault Tree Analsysis:* è un metodo deduttivo basato sulla domanda "Perché…?". Questo genere di analisi parte da un evento indesiderato, definito *Top Event* a partire dal quale ricercare tutti i possibili percorsi che hanno portato a tale evento. L'albero dei guasti, così definito in italiano, permette sia un'analisi qualitativa

del sistema, andando a ricercare tutte le possibili cause di fallimento del sistema, ma anche di calcolare la probabilità che tale evento accada conoscendo i tassi di guasto di ogni singolo componente. La presenza di porte logiche, specialmente *OR* e *AND,* permette di collegare tra loro i vari eventi e possibili fallimenti all'interno del processo. Una limitazione dell'albero dei guasti è quella di non poter andare a considerare i fallimenti del sistema causati da errori umani (ISO 31010:2009);

- ETA, ovvero *Event Tree Analysis:* è un metodo logico induttivo che permette un'analisi del processo, sia in caso di fallimento che di successo del sistema, tramite un'analisi funzionale degli eventi che si susseguono cronologicamente partendo da un evento scatenante. L'albero degli eventi può essere analizzato anche nelle fasi iniziali di progetto del sistema per conoscere la probabilità che un determinato evento accada o meno. Fondamentalmente ogni evento ha una uscita binaria, a meno che gli eventi non siano mutualmente esclusivi.

Un concetto teorico che è stato introdotto dalla UNI 9910 nel 1991 è la fidatezza, ovvero l'affidabilità che può essere attribuita ad un sistema in un determinato periodo di tempo. La fidatezza è fine alla valutazione di vari elementi all'interno del sistema, tra cui:

- Valutazione del rischio e della sicurezza;
- Specifiche di progetto;
- Assistenza tecnica e manutenzione;
- Costo del ciclo-vita del sistema;
- Competizione sul mercato.

La fidatezza è da vedere però come un insieme di concetti teorici e misure che definiscono l'affidabilità del sistema. L'affidabilità, comunemente abbreviata come $R(t)$, è definibile come l'attitudine di un sistema a compiere la sua funzione di origine rispettando le specifiche tecniche in un certo intervallo di tempo. Matematicamente è possibile definire l'affidabilità come la probabilità che un elemento compia la funzione richiesta in un intervallo da zero ad un tempo generico t, considerando i fattori di stress e le condizioni ambientali in cui l'elemento lavora.

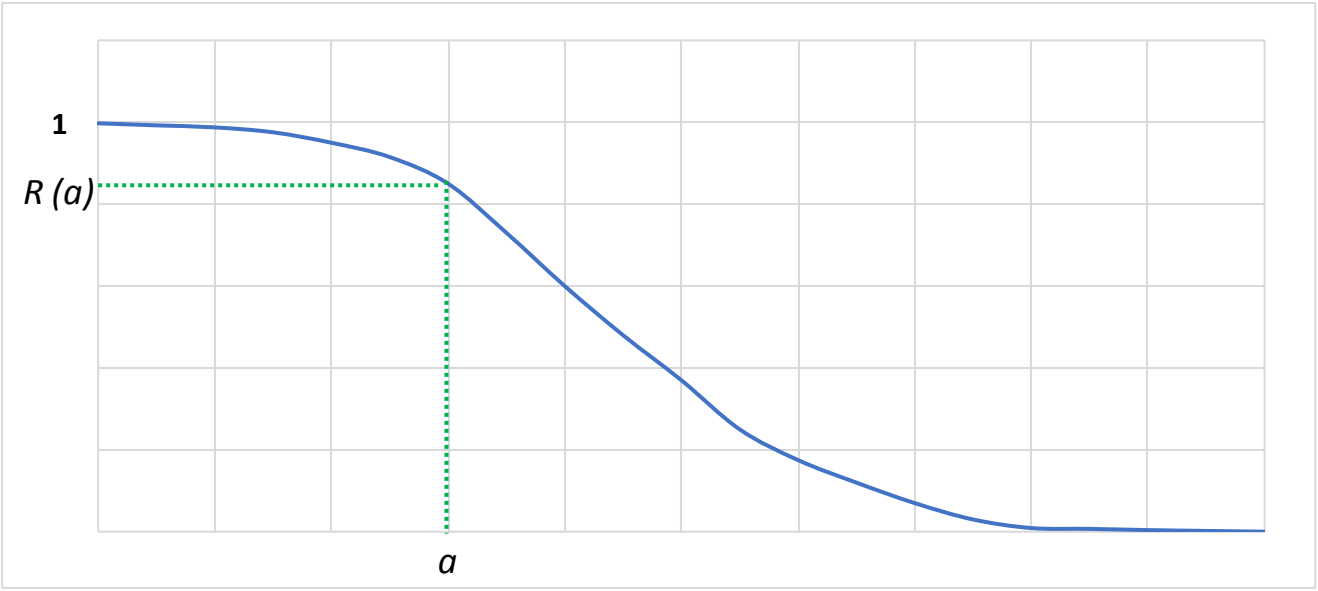

Figura 1.1:Andamento matematico dell'affidabilità di un componente nel tempo.

L'inaffidabilità, abbreviata comunemente come $F(t)$, d'altro canto, è il complemento ad uno della affidabilità ($F(t) = 1 - R(t)$), quindi la probabilità che un componente non riesca a compiere la funzione richiestagli nell'intervallo di tempo. Un'altra definizione base necessaria da introdurre con il rischio è la distribuzione statistica dei fallimenti, comunemente chiamata densità.

$$f(t) = \frac{d\,F(t)}{dt} \tag{4}$$

Conoscendo il valore della $F(t)$, ovvero dalla inaffidabilità del sistema, è possibile integrare la funzione della densità e determinare il tempo medio di fallimento (MTTF) di un componente, definibile anche come il valore atteso della distribuzione statistica di fallimenti nel tempo:

$$MTTF = E(\tau) = \int_0^\infty t\, f(t)dt = \int_0^\infty R(t) \tag{6}$$

Infine, un ultimo termine fondamentale per calcolare l'affidabilità o inaffidabilità di un sistema è il tasso di guasto, ovvero il rapporto matematico tra la distribuzione statistica dei fallimenti in un determinato intervallo di tempo (quindi la densità) e l'affidabilità del sistema.

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} = \lambda \tag{7}$$

Il tasso di guasto è un valore fondamentale che permette di determinare in modo agevole tutti i termini necessari a descrivere la fidatezza.

Fino a questo punto è stato brevemente trattato il rischio e la teoria che vi sta dietro, senza definire però l'importanza della gestione del rischio.

Le prime normative a supporto della gestione del rischio vennero introdotte a partire dagli anni '80. La prima pubblicazione ISO a riguardo è stata la ISO 8402:1988 ed è oggi nota come ISO 9000 che è fine al controllo della qualità del prodotto, allo scopo di soddisfare il più possibile le esigenze e i desideri del cliente. Parallelamente allo sviluppo della normativa per il controllo e gestione della qualità, nacque la normativa di gestione ambientale, nota oggi come ISO14000 ed aggiornata nel 2015. Varie normative sulla gestione del rischio, invece, si sono susseguite negli anni ma sicuramente la più interessante in materia è la ISO 31000, che definisce la gestione del rischio come "Quell'insieme di attività svolte per gestire e controllare il rischio di una compagnia o organizzazione".

Bisogna sottolineare però che un sistema integrato di gestione deve prevedere l'azione sinergica delle tre normative citate, ovvero è necessario un lavoro congiunto di gestione della qualità, dell'ambiente e del rischio al fine di avere un business competitivo ed elevati standard operativi. La gestione del rischio è un caposaldo per i sistemi di gestione della sicurezza, ampiamente descritti in letteratura, ovvero quei sistemi basati sulla gestione del rischio che monitorano in maniera sistematica le prestazioni degli operatori, delle apparecchiature e dell'ambiente fisico in cui il lavoro viene svolto, al fine di identificare e valutare i pericoli principali.

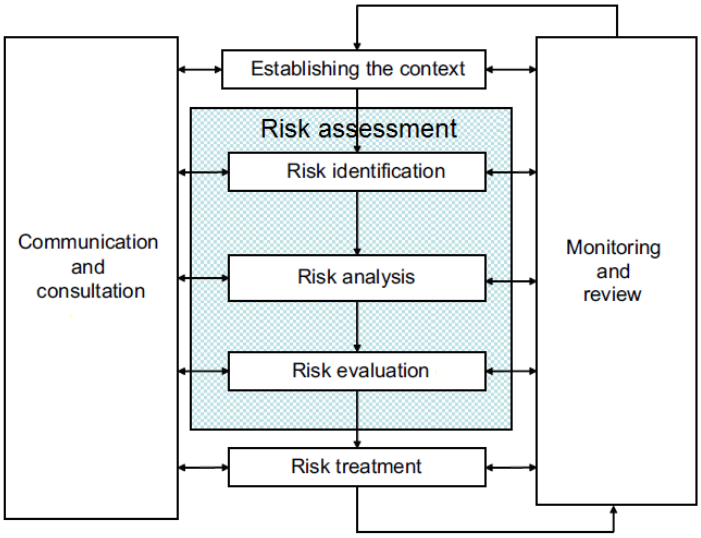

Figura 1.2: Sistema di gestione di rischio così come descritto nella ISO.

Prima di tutto risulta fondamentale stabilire il contesto nel quale il rischio verrà gestito, così come valutare tutta quella serie di parametri interni ed esterni al processo che bisogna prendere in considerazione durante la fase di gestione del rischio. I contesti che agiscono da struttura per la gestione del rischio sono il contesto interno ed il contesto esterno alla compagnia. Il contesto interno fa riferimento alle politiche aziendali, cioè alla struttura e alle strategie di processo della compagnia. Il contesto esterno, invece, tiene conto dell'ambiente esterno alla compagnia, quindi della cultura, delle leggi, della politica, della tecnologia e di tutto ciò che è riferibile al territorio in cui la compagnia ha sede.

Fondamentale risulta anche la comunicazione e consultazione con tutte le parti interessate, sia interne che esterne al processo. Le fasi di comunicazioni avvengono in una fase preliminare della vita dell'impianto, al fine di assicurare che tutti gli interessati dal processo abbiano chiaro quali decisioni siano state prese in fase di progetto e quali requisiti sono necessari da mantenere durante la vita dell'impianto. Come già accennato precedentemente, in letteratura, specialmente nella ISO 31010, sono elencate più di trenta tecniche fini alla gestione e valutazione del rischio. In Tabella 4.1 all'interno del testo è possibile apprezzare una visione d'insieme di tutte le tecniche, con i punti forza e debolezze di ogni metodo sulla base della loro applicabilità in fase di valutazione del rischio. In termini generali, la ISO 31010 suggerisce che la tecnica appropriata, che deve essere utilizzata in fase di valutazione del rischio, deve avere le seguenti caratteristiche:

- essere giustificabile e appropriata per la situazione;
- dovrebbe fornire risultati che favoriscono nel comprendere la natura del rischio;
- dovrebbe essere tracciabile, ripetibile e verificabile.

La valutazione del rischio, in accordo con la ISO 31000, è allora il cuore pulsante della gestione del rischio. Così come descritto nella normativa, è un processo sistematico di valutazione dei potenziali rischi che possono presentarsi all'interno del processo. La normativa definisce la valutazione del rischio come "quella parte della gestione del rischio che prevede un processo strutturato che identifica come gli obiettivi possono essere affetti e analizza i rischi in termini di conseguenza e probabilità". La normativa ISO 31000 sottolinea anche che la valutazione del rischio prevede la risposta a quattro semplici domande:

1. Cosa potrebbe succedere e perché?
2. Quali sono le conseguenze?
3. Qual è la probabilità di un futuro accadimento?
4. Ci sono dei fattori che possono mitigare le conseguenze o ridurre la probabilità del rischio?

Fondamentalmente le risposte a queste domande sono identificabili nelle fasi di valutazione del rischio secondo la ISO 31010, ovvero:

- Identificazione del rischio;
- Analisi del rischio – Conseguenze;
- Analisi del rischio – Probabilità;
- Analisi del rischio – Livello del Rischio;
- Valutazione del rischio.

La fase di identificazione del rischio è fine al riconoscimento della fonte del rischio, le sue aree di impatto, le azioni e tutte le possibili e potenziali cause. La fase di identificazione del rischio viene condotta in maniera tale da definire dei rischi che potrebbero teoricamente impedire al processo, impresa o investimento di raggiungere gli obiettivi prefissati, documentando e comunicando ogni possibile evento indesiderato registrato all'interno del processo.

L'analisi del rischio comporta infine delle considerazioni riguardo la causa determinante il rischio, le sue conseguenze e probabilità, oltre che una serie di utili informazioni per determinare e descriverlo al meglio. L'analisi del rischio è un processo soggettivo durante il quale l'analista ricerca la probabilità e la severità che potrebbero al meglio quantificare il

rischio. Essendo appunto una pratica soggettiva, generalmente le analisi vengono condotte da un team di esperti che comunicano ogni decisione presa alle parti interessate. Partendo da conseguenze e probabilità, tramite la matrice del rischio, è possibile dare una stima quantitativa del rischio.

Anche se in commercio sono presenti diversi software che permettono di analizzare il rischio, in questo lavoro si è deciso di utilizzare come esempio il modulo di identificazione e analisi del rischio sviluppato da Tosca Solution per il loro registro dei rischi. In Figura 4.2 all'interno del testo, si nota come, tramite l'utilizzo di un'interfaccia molto semplice ed essenziale, si riescano a convogliare tutte le necessità dell'analista. La possibilità di far scegliere all'utente il valore di probabilità e conseguenza da un menù a tendina composto da "definizioni" e non da valori numerici gli è sicuramente d'aiuto. Chiedere ad un utente, infatti, se la probabilità di rischio ha un valore "3" crea sicuramente maggiori incertezze rispetto a chiedere se la probabilità ha una frequenza "Occasionale". Lo scopo della stima del rischio, la fase successiva all'analisi del rischio, tiene conto dei valori di tutti i rischi che sono stati analizzati e aiuta l'analista a decidere quale rischio ha priorità in fase di mitigazione. In accordo con la ISO 31000:2009, ogni decisione deve essere presa in conformità con i requisiti legali, normativi e di altro tipo. Tutte le decisioni per il trattamento di un rischio sono influenzate dall'atteggiamento della compagnia nei confronti del rischio e dai criteri e dal contesto precedentemente stabiliti.
L'ultima fase della valutazione del rischio è lo sviluppo di opzioni fini a mitigare e ridurre il valore di rischio. La scelta del trattamento più adeguato dipende da un accurato bilanciamento tra i costi per mitigare il rischio e i benefici che ne si otterrebbero. Il trattamento prevede la riprogettazione di sistemi di controllo e di sicurezza già esistenti, ma anche l'introduzione e il monitoraggio di nuovi sistemi. In letteratura sono descritte cinque possibili strategie di trattamento al rischio:

- Evitare il rischio;
- Azioni fini a ridurre le conseguenze e/o la probabilità del rischio;
- Trasferimento del rischio;
- Accettare e monitorare il rischio;
- Condividere il rischio.

Evitare il rischio è una sorta di "occultamento" della situazione rischiosa, non praticando alcuna attività che potrebbe generare un rischio. L'esempio riportato nel testo principale aiuta facilmente a comprendere tale concetto: usare un forno per cucinare potrebbe causare situazioni di pericolo, quindi non usare il forno sarebbe una situazione ideale per evitare il rischio. Le azioni per ridurre il rischio, invece, agiscono direttamente sulla probabilità o sulle conseguenze cercando di moderare tali variabili. Se per esempio usare il forno fosse un'attività pericolosa, indossare guanti protettivi aiuterà a mitigare le conseguenze di eventuali situazioni spiacevoli. Il trasferimento del rischio coinvolge terze parti, come ad esempio un'assicurazione o compagnie esterne. Accettare il rischio prevede la noncuranza davanti ad una situazione di pericolo. Infine, la condivisione di un rischio, prevede la distribuzione del rischio tra diverse organizzazioni o persone. La scelta del trattamento ideale quindi risulta fondamentale nella fase di valutazione del rischio anche se, spesso, l'utilizzo di un trattamento induce alla formazione di rischi secondari che a loro volta necessitano di essere identificati, analizzati e trattati. L'ultima fase della valutazione del rischio, in accordo con le normative ISO, è la fase di monitoraggio e revisione, ovvero il mantenimento e il controllo che tutte le operazioni,

trattamenti e processi siano svolti in sicurezza praticando in modo efficace ed efficiente le misure correttive messe in atto.

Dopo che un rischio è stato identificato, analizzato, valutato, mitigato e rivisto, le compagnie sono solite registrare tali rischi con annessi trattamenti e numerose altre utili informazioni all'interno di quello che viene definito, come si è detto, registro dei rischi. In letteratura sono state descritte numerose applicazioni del registro dei rischi in diversi settori industriali: dal settore automotive al chimico passando per il campo edile e la gestione dei trasporti. L'efficacia di un registro dei rischi non è assolutamente messa in dubbio, anzi in letteratura scientifica sono numerosi gli autori che lodano il suo utilizzo. Principalmente possiamo dividere il registro dei rischi in tre diverse sezioni:

- Il registro dei rischi in quanto tale;
- Informazioni del gestore dei rischi;
- Piani di mitigazione del rischio.

Il registro dei rischi in quanto tale ha diversi elementi cruciali, che sono fondamentali al fine di soddisfare le esigenze informative della compagnia e di permettere ad un "non addetto ai lavori" di capire esattamente il sistema e i rischi correlati. Tali requisiti necessari sono:

- **ID del rischio**: numero di identificazione unico per ogni rischio;
- **Descrizione del rischio**: una breve descrizione del rischio per rendere noto il problema;
- **Stima del rischio**: una quantificazione del rischio basata sui valori di probabilità e impatto;
- **Proprietario**: la persona responsabile nella gestione del rischio;
- **Azioni:** lista di azioni necessarie a mitigare e trattare il rischio;
- **Data**: la data di tutte le azioni e eventi che hanno coinvolto il rischio.

Un completo registro dei rischi deve presentare altre informazioni utili: per esempio risulta molto importante la presenza di uno stato del rischio attuale e la stima di uno stato del rischio futuro, il tipo di rischio che si sta trattando, l'apparecchiatura coinvolta, il pericolo correlato ed altre informazioni che aiutano l'azienda a gestire e focalizzarsi a pieno su quello che è il rischio nella sua interezza. Il caso studio di questo lavoro, che verte sullo sviluppo di un nuovo registro dei rischi per una società elettrica irlandese, mostra come essa attualmente monitori i propri rischi tramite dei fogli di calcolo e Microsoft SharePoint. Non c'è da stupirsi se tale azienda utilizzi un registro "fatto in casa" in quanto in letteratura è certificato come il 78% dei registri dei rischi comunemente usati siano sviluppati *ad hoc* dalle aziende per monitorare i loro rischi.

La compagnia di generazione elettrica presentata nel caso studio è una delle principali compagnie di generazione e sistema di *networking* all'interno della Repubblica di Irlanda. L'azienda opera sul suolo irlandese e britannico con oltre 19 stazioni di produzione e 18 impianti eolici che servono oltre 1 milione di famiglie e 95 mila imprese.

L'attuale registro dei rischi usato dalla società elettrica irlandese, gergalmente chiamato GRR, utilizza fogli di calcolo di Microsoft SharePoint ed esportati come fogli di calcolo di Microsoft Excel. Il GRR ha tutte quelle caratteristiche di un registro dei rischi ben strutturato, anche se le informazioni sono distribuite in modo male organizzato e la lettura di tali dati risulta difficile ad un lettore che non ha familiarità con il sistema. Il sistema ha diverse carenze per la gestione dei rischi e dovrebbe quindi essere migliorato attraverso alcune strategie, come per esempio:

- Aggregazione dei rischi dal livello di stazione al livello di amministrazione centrale;
- Supporto dei controlli sulle misure di mitigazione a livello di stazione e di amministrazione;
- Supportare meglio le stime basate sui dati per probabilità di situazioni basate su incidenti;
- Integrazione con il registro delle attività e apparecchiature critiche (CAR);
- Supportare un collegamento migliore con il flusso di lavoro attorno alla comunicazione del rischio;
- Un possibile collegamento con la pratica operativa quotidiana.

Con il passare degli anni sono state aggiunte opzioni nuove che ne hanno incrementato l'efficienza e la quantità di informazioni che il GRR fornisce all'utente. Un punto di forza del registro dei rischi della società elettrica è l'analisi, non solo del valore del rischio, ma anche dell'impatto al rischio monetizzato per cinque diverse aree di lavoro:

- Finanza;
- Sicurezza;
- Reputazione;
- Tecnico;
- Ambientale.

La stima dell'impatto monetario per le diverse aree di lavoro si basa su una scala di numeri interi da uno a cinque, associando ad ogni numero un valore espresso in euro come mostrato di seguito.

	Finanza [€]	*Sicurezza [€]*	*Reputazione [€]*	*Tecnico [€]*	*Ambientale [€]*
1	< 100 K	< 10 K	< 10 k	< 100 k	< 10 k
2	< 1 M	< 250 k	< 250 k	< 1 M	< 250 k
3	< 10 M	< 1 M	< 1 M	< 10 M	< 1 M
4	< 50 M	< 10 M	< 10 M	< 50 M	< 10 M
5	> 50 M	> 10 M	> 10 M	> 50 M	> 10 M

Tabella 1.2: Stima dell'impatto monetario per le diverse aree di lavoro.

Inoltre, nel GRR, è presente pure la probabilità che avvenga una determinata esposizione monetaria (probabilità comune alle cinque diverse categorie): anche in questo caso la frequenza di accadimento è valutata da una scala di numeri interi da uno a cinque, associando ad ogni numero un valore di probabilità.

Conoscendo quindi la probabilità e l'impatto monetario per ogni categoria è possibile calcolare l'esposizione al rischio monetizzato secondo la formula:

$$Probability\ x \sum Monetised\ Risk\ Impact \quad (13)$$

Il calcolo di questo valore permette, quindi, di non quantificare soltanto il rischio (che, utilizzando una matrice del rischio 5x5, ha un valore compreso tra uno e venticinque), bensì permette di stimare una perdita monetaria dovuta ad un determinato rischio. Come esempio viene riportata la Tabella 6.5 del testo principale per meglio aiutare a comprendere l'importanza di tale esposizione monetizzata al rischio.

Attività	*Rosso*	*Arancione*	*Giallo*	*Verde*	*Totale*
Organisational conditions	€ 121.192.500	€ 2.865.005	€ 305.437	€ 8.877	€ 124.371.819
External safety	€ 27.203.000	€ 3.374.250	€ 121.907	€ 127.209	€ 30.826.366
Gas turbine	€ 10.040.250	€ 1.283.205	€ 209.544,5	€ 373	€ 11.533.373
Finance	€ 5.507.700	€ 3.816.945	€ 829.257	€ 8.944	€ 10.162.846
Internal standards and procedures	€ 4.950.660	€ 742.830	€ 288.024	€ 45.228	€ 6.026.742
Switchgear	€ 4.984.155	€ 118.250	€ 160.490	€ 311	€ 5.263.206
C&I	€ 2.227.500	€ 2.470.380	€ 72.798	€ 563	€ 4.771.241
Process safety	€ 0,00	€ 4.395.435	€ 171.292	€ 45.172	€ 4.611.899
Generator	€ 478.500	€ 2.733.208	€ 115.615	€ 401	€ 3.327.725
Steam turbine	€ 2.794.000	€ 468.490	€ 0,00	€ 353	€ 3.262.843
Transformers	€ 2.794.000	€ 229.020	€ 157.943	€ 165	€ 3.181.129

Tabella 1.3: Esempio di perdita monetaria dovuta ad un determinato rischio .

La mole di informazioni che fornisce il GRR permette di intrecciare valori di diversa origine per avere una visione di insieme di tutti i rischi, con la loro esposizione monetizzata, per ogni attività, pericolo, conseguenza, causa, stazione e proprietario del rischio. Comparando tra loro i GRR di diversi anni è inoltre possibile stimare come il rischio (o il suo valore monetizzato) sia cambiato nel corso del tempo come mostrato in Tabella 6.6 (all'interno del testo in inglese) la quale compara il rischio monetizzato per tutte le stazioni della compagnia elettrica nel gennaio 2017 e nell'aprile 2018. La tabella fornisce anche una stima della differenza tra i due diversi valori. Bisogna sottolineare il fatto che molte stazioni hanno presentato un incremento del loro rischio monetizzato totale. Questa particolarità, che ad una prima occhiata potrebbe

risultare alquanto sgradita, in realtà è causata da una maggiore attenzione durante la fase di valutazione del rischio da parte della compagnia.

La compagnia irlandese però non utilizza soltanto il GRR, bensì sfrutta un secondo registro, denominato CAR (Registro delle attività critiche), nel quale raccoglie le informazioni di tutte quelle attività ed apparecchiature tecniche che sono soggette ad un rischio critico. La definizione di attività critica è normata nella ISO 55001:2014 che definisce che "Un componente o sistema di una compagnia è definito critico se la sua funzione è di prevenire un anormale decorso verso un incidente maggiore". Con la definizione di "incidente maggiore" si vuole intendere un evento risultante da sviluppi incontrollati nel corso dei processi di un impianto, che comporta gravi pericoli per l'ambiente, per l'impianto o per il personale, sia interno che esterno alla compagnia.

Le informazioni che fornisce il CAR rispetto al GRR si focalizzano meno sugli aspetti economici o sulle conseguenze, bensì sono più incentrate su ogni particolare tecnico dell'impianto che potrebbe causare l'incidente. Per capire meglio il diverso grado di dettaglio dei due registri, basti pensare che nel GRR viene riportato un possibile guasto di una turbina con tutte le conseguenze, cause, perdite monetarie che ne conseguono. Nel CAR, invece, viene esaminato quale componente della turbina è più soggetto al guasto, stimando il costo di un eventuale sostituzione e riparazione del componente interessato per evitare un incidente maggiore. La possibilità di stimare il costo di un eventuale sostituzione o riparazione del componente è una caratteristica interessante del CAR, che Tosca Human Factor Solutions Ltd. intende sviluppare in maniera dinamica e attualizzata al fine di lanciare sul mercato un software con una sezione dedicata alla valutazione delle opzioni di investimento. I punti principali per il suddetto modulo sono l'analisi dei possibili investimenti e l'esposizione al rischio monetizzato a cui la compagnia è soggetta durante gli anni. Prima di tutto è fondamentale analizzare il profilo di rischio del componente o unità che si vuole valutare, al fine di comprendere meglio come il rischio muti negli anni, valutando le cinque aeree di possibile impatto: finanza, sicurezza, tecnico, reputazione e ambiente. La stima del profilo di rischio viene eseguita per un periodo di tempo variabile a seconda dei bisogni della compagnia, della vita dell'impianto, dalla conoscenza del sistema da parte degli analisti o da eventuali manutenzioni periodiche già stabilite. Gli investimenti che la compagnia può attuare sono generalmente di due tipi: *Downtime cost* e *Capex*.

Il *Downtime cost,* definibile in italiano come "costo di fermo", si riferisce al periodo durante il quale un'apparecchiatura o macchinario non è funzionale a causa di guasti tecnici o meccanici, manutenzione o altri fattori. Il costo medio di fermo è generalmente valutato come il costo dei beni che non sono stati prodotti e quindi non è stato possibile vendere. Il *Capex (Capital Expenditure),* definibile come spesa di capitale, è l'investimento messo in atto dalla compagnia per acquistare, aggiornare, cambiare i componenti soggetti a rischi tecnici.

Possono essere messi in atto altri possibili investimenti che non richiedono periodi di fermo o investimenti di capitali notevoli: un esempio di questi è il NDT *(No Destructive Testing).* Il calcolo del NPV (*Net Present Value*), ovvero del valore attuale netto, risulta fondamentale per la stima dell'efficienza dell'investimento. Il valore attuale netto è calcolato come rapporto tra il valore dei flussi monetari in ingresso sul valore dei flussi monetari in uscita in un determinato periodo di tempo. Da un punto di vista matematico è possibile definirlo come:

$$NPV\ (i,N) = \sum_{t=0}^{N} \frac{R_t}{(1+i)^t} \qquad (14)$$

In cui:

- R_tè il flusso monetario al tempo t;
- i è il tasso di rendimento, ovvero il profitto guadagnato dall'investimento (per il caso studio verrà usato un valore pari a 8,4%);
- t è il tempo in cui avviene il flusso monetario.

Comparando quindi i benefici che si ottengono praticando l'investimento rispetto ad una situazione in cui non era previsto (quindi rispetto al profilo di rischio) è possibile determinare l'indice di investimento, definito *Evaluation Index* secondo la seguente formula:

$$Evaluationi\ index = \frac{\sum_{t=0}^{N}(NPV + benefit)}{\sum_{t=0}^{N} NPV} \qquad (15)$$

Fino a questo punto si è parlato di Tosca Human Factor Solutions Ltd. senza però definire di cosa si occupa questa piccola start-up irlandese. Tosca Solutions è una compagnia con sede al Trinity College of Dublin, che offre supporto per implementare sistemi di gestione del rischio adattandoli ai bisogni dell'utente e seguendo i principi delle normative vigenti. Gli scopi principali di Tosca Solution sono:

- Fornire un sistema efficace per controllare e supportare che tutto sia in regola con le norme vigenti in un ambiente complesso al fine di offrire una sicurezza totale;
- Focalizzarsi sulle attività critiche, aiutando a praticare attività chiave, formando i lavoratori e attuando pratiche efficienti di sicurezza;
- Aggiungere valore su formazione e ottimizzazione.

In questo contesto, Tosca Solution ha sviluppato un registro dei rischi conforme alle vigenti normative in merito a qualità, ambiente, rischio e sicurezza. Il sistema permette principalmente all'utente di redigere una lista di tutti gli eventi e le attività, identificando quelle critiche e valutandone il rischio. Inoltre, il registro dei rischi di Tosca Solution aiuta a coordinare l'esecuzione e il completamento di piani e strategie per mitigare i rischi registrati all'interno dell'impianto. Il registro dei rischi di Tosca Solution provvede a:

- Avere traccia delle operazioni e delle attività per capire perfettamente il processo e come ogni attività potrebbe evolversi in una situazione rischiosa;

- Provvedere ad una visione di insieme di tutti i rischi principali associabili alle operazioni della compagnia;
- Identificare, valutare e cercare una rapida mitigazione a diversi tipi di rischio, che potrebbero compromettere gli obiettivi dell'organizzazione;
- Allineare il rischio con norme interne ed esterne alla compagnia;
- Effettuare un controllo finanziario;
- Effettuare un monitoraggio continuo, segnalando eventuali rischi all'interno della compagnia, monitorando anche le azioni preventive e le performance della attività.

La versione attuale del registro dei rischi di Tosca Solutions, usato da un aeroporto regionale italiano per monitorare le attività, ha attirato su di sé l'attenzione di numerose compagnie in varie parti del mondo. Principalmente è possibile distinguere sei moduli che compongono il menù principale:

- *Dashboard;*
- *Context;*
- *Risk Assessment;*
- *Risk Treatment;*
- *Monitoring;*
- *Communication.*

La dashboard fornisce una visione di insieme di tutte le informazioni che sono state caricate all'interno del sistema. Sono presenti diversi elenchi e grafici che permettono all'utente di osservare la distribuzione dei rischi e il loro livello. Altre sezioni permettono di avere una panoramica degli ultimi rischi e trattamenti che sono stati caricati all'interno del sistema ed eventualmente di usare questa sezione come collegamento rapido per modificare le informazioni contenute in tale modulo. Altre informazioni che si trovano all'interno della *dashboard* riguardano i *DORs* (*Daily Operation Routines), shift handovers* e *anomalies.* Questi strumenti fanno parte delle sezioni di monitoraggio e comunicazione e saranno analizzati più avanti all'interno di questo abstract in italiano.

La sezione di *Context* potrebbe essere definita la sezione principale del registro dei rischi. Qui l'utente ha la possibilità di iniziare ad inserire informazioni riguardanti le procedure generali, le apparecchiature o le aree oggettive. In questo lavoro sarà esaminata la sezione di procedure, definite all'interno del software *Macro Procedures.* Per ulteriori dettagli si rimanda alla figura 7.3 del testo in lingua inglese.

Durante la fase di creazione di queste procedure generali è possibile riconoscere i seguenti elementi:

- Numero identificativo;
- Nome della procedura;
- Un collegamento rapido che permetta all'utente di inserire rischi collegati già a questa fase;
- In parentesi il numero di rischi associati a tale procedura;
- La possibilità di aprire, modificare e cancellare la procedura selezionata

Aprire una *Macro Procedures* (procedura generale) porta l'utente alla sezione *Procedures*. Le informazioni contenute all'interno di questa sezione appena aperta sono le stesse per la sezione

"padre". A sua volta, aprendo la sezione *Procedures,* l'utente è portato ad una sezione contente tutte le task che caratterizzano la procedura selezionata. Un esempio è riportato di seguito.

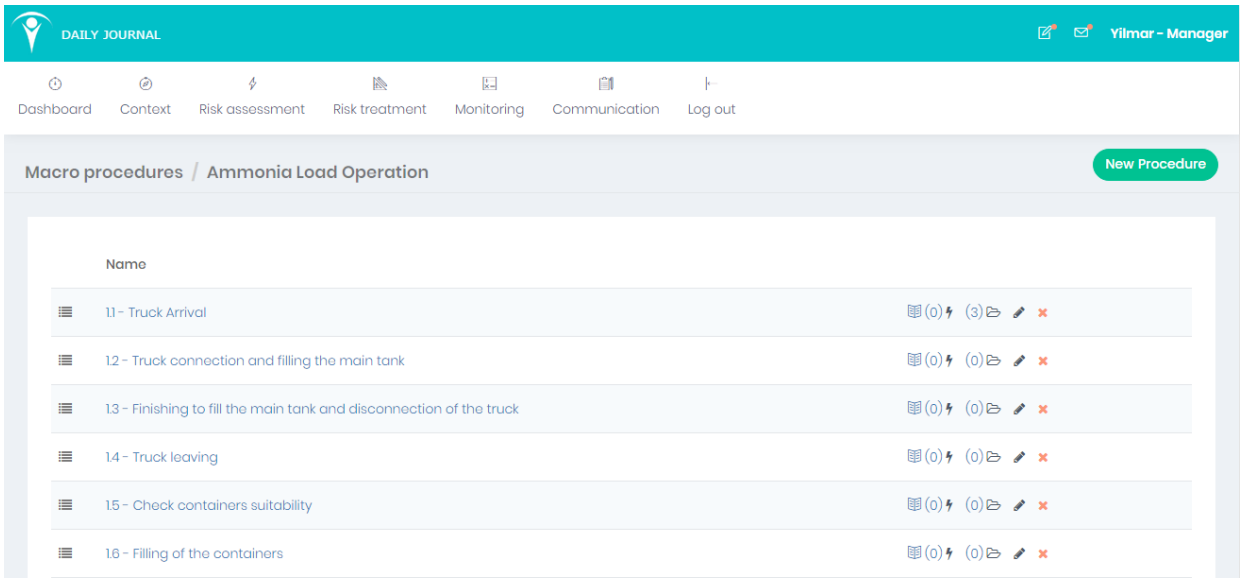

Figura 1.3: Sezione ad albero contenente le task che caratterizzano la procedura.

La sezione di *Risk assessment* è caratterizzata dalla possibilità di avere una panoramica sui rischi inseriti, il responsabile ed il livello del rischio. Oltre a questo è possibile:

- Aprire una cartella di lavoro contenente varie informazioni sul rischio, come files e i messaggi lasciati dal responsabile;
- Collegare il rischio ad un trattamento esistente o creare, eventualmente, un nuovo trattamento;
- Collegare il dettaglio del rischio, visualizzando le conseguenze, a cause, impatto, probabilità, ecc;
- Modificare il rischio, modificando la descrizione precedente;
- Eliminare i rischi.

La sezione di *Risk Treatment* è quella parte del registro dei rischi di Tosca Solution che raccoglie, monitora e analizza tutti i trattamenti per mitigare i rischi che sono presenti nella compagnia. Anche in questa sezione è presente una cartella di lavoro contenente una *To do List*, ovvero una lista delle azioni da compilare al fine di mitigare il rischio. Più azioni della lista sono completate, più l'avanzamento della mitigazione tende verso il completamento. Quando la barra dell'avanzamento è completa, l'utente può decidere di archiviare tale trattamento nella sezione apposita.

Di seguito è mostrato il layout della sezione di *Risk Treatment* dove è possibile apprezzare la barra dell'avanzamento e il collegamento al rischio, che rendono il registro dei rischi di Tosca davvero di facile comprensione.

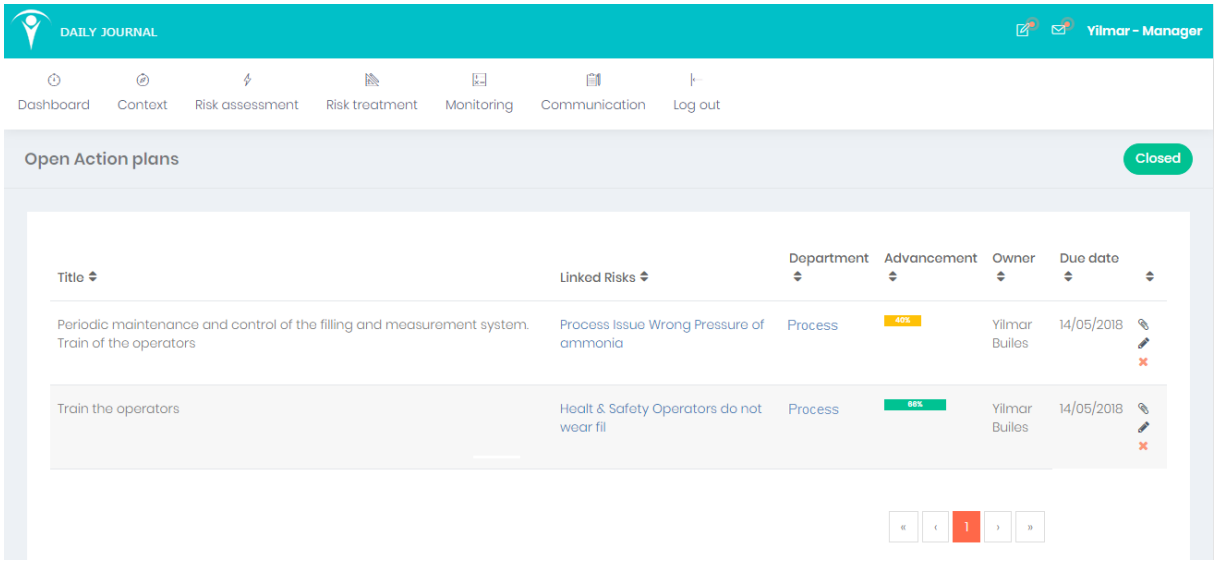

Figura 1.4: Layout della sezione di Risk Treatment.

La sezione di monitoraggio è composta da cinque diversi moduli:

- *Reports;*
- *Audits;*
- *Surveys;*
- *DORs;*
- *Risk Charts.*

Il modulo di *Reports* è fine a riportare quelle situazioni rischiose che non sono propriamente definibili come rischi, ma che necessitano di essere monitorate prima che degenerino come rischi veri e propri. La sezione di *Audits* permette di elencare e riassumere le revisioni discusse negli incontri aziendali, con rispettive domande e discussioni che sono state poste. Nel modulo *Surveys* sono presenti quell'insieme di informazioni che sono state estratte da discussioni di gruppo tra specialisti del sistema che si sta analizzando, valutando insieme i loro dubbi, pensieri ed opinioni in merito agli eventi che caratterizzano il processo. I *DORs* sono degli strumenti usati per riassumere lo stato di un progetto o le operazioni che è necessario vengano compiute, riportando gli obiettivi da perseguire secondo una scadenza giornaliera/settimanale/mensile. Alcuni esempi di *DORs* all'interno dell'impianto potrebbero essere il controllo delle valvole, la sostituzione di sistemi di sicurezza o il controllo della temperatura e delle pressioni delle apparecchiature dell'impianto.

Per quanto riguarda la sezione di *Communication*, è composta da due moduli:

- *Shift Handovers;*
- *Anomalies.*

Shift Handovers è quel modulo che fa fronte al cambio turno dei lavoratori che si passano l'un l'altro le responsabilità e i doveri necessari a portare a termine il lavoro in sicurezza e con efficienza. La condivisione di informazioni rilevanti tra i lavoratori in uscita e quelli in entrata ha una influenza chiave sulla riuscita della missione lavorativa. La sezione di *Anomalies* è dedicata alla comunicazione di irregolarità e problemi che sono stati segnalati nella sede di lavoro.

Fin ora, descritto così, il registro dei rischi non presenta particolari innovazioni rispetto ai registri dei rischi comunemente descritti in letteratura. Si è deciso quindi di elencare espressamente i principali vantaggi che il sistema di Tosca Solutions presenta:

- Checklist con un sistema integrato di reportistica nel sistema, con il beneficio di avere report in tempo reale e il vantaggio di poter segnalare immediatamente potenziali anomalie;
- Azioni correttive suggerite dal sistema per una migliore organizzazione ed esecuzione di azioni correttive;
- Analisi di anomalie passate e future per avere un'analisi strategica e prevenire problemi giorno dopo giorno;
- Revisioni in tempo reale delle operazioni principali con controlli interni ed esterni;
- Efficienza nel trovare risorse e seguire i trattamenti, coinvolgendo tutto il personale in una partecipazione attiva durante la gestione del rischio;
- Un sistema di tracciamento del rischio efficiente, che assicura un migliore monitoraggio del rischio tramite notifiche e indicatori di performance;
- Ottimizzazione dei trattamenti al fine di ridurne il numero per migliorarne l'efficacia.

Proprio per questa sua versatilità tecnica, questo suo adattamento ad ogni situazione e a questa ricerca di miglioramento continuo e costante, la compagnia elettrica ha deciso di rivolgersi all'esperto team di analisti e sviluppatori di Tosca per progettare un nuovo prototipo che possa servire come sistema di gestione del rischio e come sintesi tra il GRR e il CAR. La richiesta del *Risk Project Manager* della azienda irlandese è stata abbastanza chiara: un prototipo che permetta l'ottimizzazione delle decisioni per la gestione delle attività, aiutando gli analisti nel prendere decisioni, aggregare i rischi, monetizzare i rischi, supportare investimenti sulle apparecchiature e definire le strategie di manutenzione. Il prototipo richiesto, quindi, deve essere capace di accogliere la gestione del rischio sia da un punto di vista di gestione delle apparecchiature, ma anche per ciò che riguarda le operazioni di processo. Gli output richiesti dal processo sono:

- Report dei rischi a fini amministrativi;
- Processo decisionale basato sui rischi per revisione di investimenti.

Fondamentalmente le richieste del *Risk Project Manager* si sono incentrate sulla visualizzazione dei rapporti legati al rischio, specialmente ai rischi "*Top 10"* per le diverse stazioni e aggregati. È stata anche richiesta una visualizzazione di tipo *heat-map* per studiare la distribuzione del rischio e una tracciabilità del rischio attraverso le attività dell'impianto. Altre richieste riguardanti l'innovativo modulo di *option evaluation* sono state fatte dal responsabile della sicurezza della compagnia. Alcune di queste sono state:

- Piani di azione correttivi per i prossimi anni;
- Per ogni piano di investimento, una stima del rischio per i futuri quattro/cinque anni;
- Calcolare e comparare il valore attuale netto (NPV) per i diversi scenari;
- Archiviare livelli di rischio passati e presenti per facilitarne il tracciamento.

Nella figura sottostante è sintetizzato lo schema del prototipo richiesto dalla compagnia elettrica. Si nota come nella prima fase identificativa dell'impianto, definito *Risk Centre*, si sono suddivise le attività tecniche da quelle non tecniche. Per ogni attività si distinguono tre livelli di dettaglio (come si vedrà trattando dati reali, questi livelli di dettaglio possono anche

essere molti di più). A quel punto per ogni attività deve essere fornita una descrizione e una storia, per avere una panoramica della situazione. Successivamente si procede con il calcolo del valore di rischio e una valutazione delle azioni richieste per mitigare tale rischio. Una completa identificazione di cause, conseguenze e la stima del valore monetizzato sono anche richieste nel prototipo come funzione basilare. Dopo di che, il rischio, così come è stato caricato nella sezione di data entry, sarà analizzato in una sezione di revisione del rischio, definita *Risk Report,* e in una sezione dedicata alla scelta dell'investimento più efficiente, definita *Option Evaluation.*

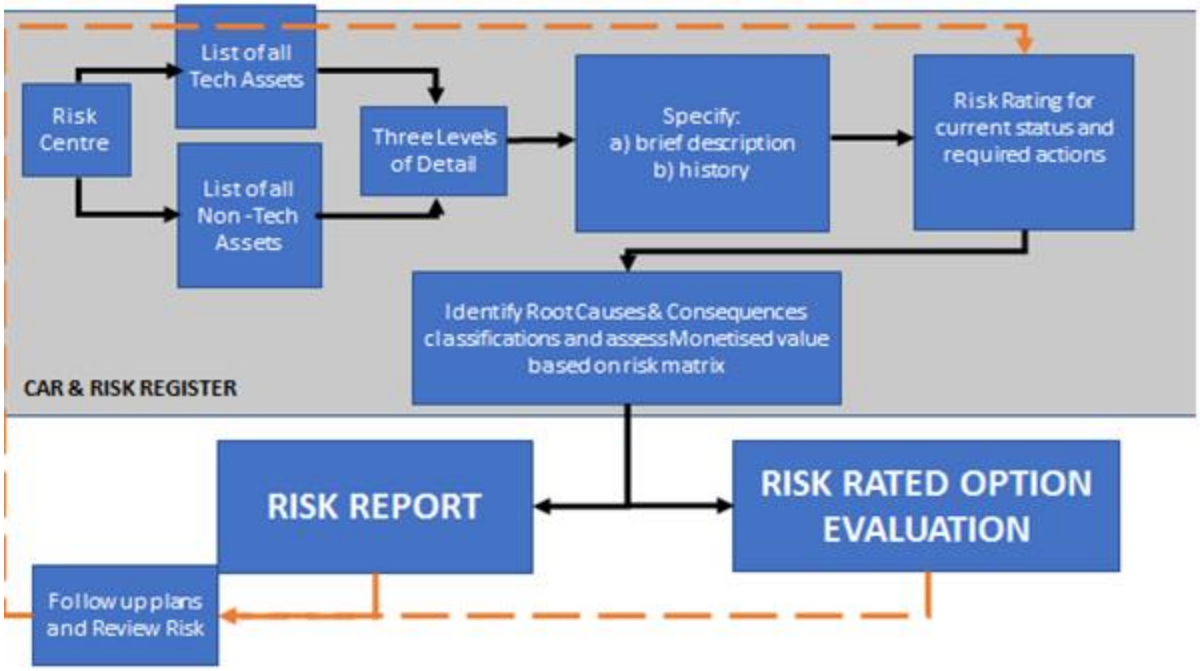

Figura 1.5: Linee guida per il prototipo

I punti salienti del prototipo risiedono nella distinzione delle attività non tecniche da quelle tecniche e quindi la distinzione dei livelli di dettaglio per ogni attività tecnica.

Seguendo la bozza preliminare del prototipo fornita dal *risk project manager* della società elettrica, gli analisti di Tosca Solutions hanno potuto lavorare attivamente sulla realizzazione di un *mock-up* quanto più *user-friendly* possibile basato su un'interfaccia grafica quanto più simile possibile al registro dei rischi già usato.

All'apertura del prototipo viene chiesto all'utente di eseguire l'accesso all'interno del sistema, come mostrato in Figura 7.10 all'interno del testo in inglese, inserendo un nome utente, una password e scegliendo da un menù a tendina per quale impianto si intende accedere. A quel punto l'utente ha accesso direttamente alla *Dashboard* del prototipo (Figura 7.11) la quale riprende dal registro dei rischi la visualizzazione grafica ad anello con annessa scala cromatica per differenziare i rischi. Altre informazioni contenute nella *dashboard* riguardano le principali conseguenze, le apparecchiature con la più elevata esposizione al rischio monetizzata ed una classifica degli impianti con la maggiore esposizione al rischio. Nel momento in cui l'utente decide di spostarsi sul modulo *Assets* dal menù principale, ha la possibilità di decidere se visualizzare, inserire o modificare le attività tecniche e quelle non tecniche all'interno del

sistema. In questo lavoro ci si è focalizzati sulle attività tecniche, in quanto parte più corposa del lavoro.

L'utente che ha compiuto l'accesso, in fase di *log-in*, in una determinata stazione, potrà aggiungere, modificare o eliminare attività solamente per tale stazione. L'utente può inoltre visualizzare, e visualizzare soltanto, le attività che sono caricate all'interno del sistema delle altre stazioni. Dopo aver selezionato l'impianto di interesse, supponiamo che si sia entrati all'interno della stazione con cui si è eseguito il *log-in* in fase iniziale, sarà possibile visualizzare l'insieme di tutte le unità presenti all'interno di tale impianto. L'utente può aggiungere, modificare, eliminare o inserire maggiori informazioni riguardanti le unità presenti (vedere Figura 7.13 del testo). Selezionando l'unità di interesse è possibile visualizzare il livello inferiore di dettaglio, quindi il livello di attività tecniche presenti all'interno dell'unità selezionata. Come si nota in Figura 7.14 del testo, per ogni attività presente in questo livello, due tabelle editabili sono disponibili: una denominata *Main* e l'altra *Risk Rating*. Nella tabella *Main* di questo livello sono disponibili diverse informazioni non visibili nei livelli sottostanti, come *Hazard, Consequences, Root Causes*. Tali informazioni sono estratte dal GRR e sono disponibili solo per questo livello di dettaglio. Le ultime colonne evidenziate nella parte finale della tabella sono le informazioni di Roll-up. Queste informazioni sono direttamente ricavate dai livelli più bassi per l'attività selezionata. Per esempio, la colonna *Roll-up RR* dell'attività denominata *Electrical* mostrerà all'utente il valore di rischio più elevato tra quelle attività che sottostanno all'interno di *Electrical*. Per visualizzare tali attività (quindi per visualizzare il livello inferiore) l'utente deve cliccare sul nome della apparecchiatura di interesse (vedere figura 7.17). In altre parole, il sistema funziona come un sistema di scatole cinesi, o se si preferisce come un sistema di matrioske, con livelli di dettaglio sempre più piccoli man mano che ci si inoltra nel sistema cliccando sul nome dell'attività di interesse. Ad esempio, un possibile percorso all'interno del sistema che si sta analizzando potrebbe essere: Station 1 – AD2 –Electrical – MV Equipment- Circuit Breaker. Per ogni livello l'utente può eseguire una analisi e valutazione del rischio usando la tabella denominata *Risk Rating* (vedere Figura 7.16 all'interno del testo). Le informazioni di valutazione del rischio sono le stesse per ogni livello e sono le stesse che normalmente vengono riportate nel GRR e nel CAR, quindi la probabilità di accadimento e livello di impatto monetizzato per le cinque aree di lavoro: finanza, sicurezza, tecnico, reputazione e ambiente. Il sistema automaticamente calcola il livello di rischio e la somma dell'esposizione monetizza al rischio.

Durante la fase di input di tale dati, così come mostrato in Figura 7.18 all'interno del testo, l'utente dovrebbe completare tale modulo in tutte le sue sezioni al fine di fornire più dettagli possibile riguardo il rischio correlato all' attività tecnica selezionata. All'utente viene data la possibilità di selezionare la probabilità e l'impatto da un menù a cascata contente la scala a cinque numeri interi descritti ampliamente in questo lavoro oppure dare una stima di tali valori tramite campo di testo. L'utente inoltre può fare una stima grossolana dei costi che un eventuale lavoro di manutenzione/mitigazione comporterebbe per eliminare tale rischio. La possibilità di fare una valutazione approssimativa dei rischi per più anni è una opzione che aiuterà l'utente nelle fasi di valutazione delle opzioni di investimento, dando già un'idea, anche se grossolana del profilo di rischio. Il modulo di Figura 1.6 è utilizzato per ogni livello di attività.

Nella sezione di *Risk Report* sono disponibili tre possibili visualizzazioni dei rischi: *tramite heat-map* (Figure 7.19), per via tabellare (Figura 7.20) o per via grafica (Figura 7.22). La visualizzazione tramite *heat-map* risulta sicuramente la più innovativa permettendo all'utente

di visualizzare i rischi direttamente dalla matrice di rischio e di valutarne l'andamento rispetto la situazione in cui era stato riportato il rischio precedentemente. Anche la via tabellare e la via grafica permettono di comparare i rischi di diversi anni all'interno della stessa struttura grafica.

La sezione di *Option Evaluation* permette all'utente di valutare quale investimento sarà il più vantaggioso considerando le spese e i benefici ottenuti. Prima di tutto, l'utente dovrà selezionare per quale attività vuole analizzare le possibili opzioni di investimento (Figura 7.23 all'interno del testo). A quel punto l'analisi di investimento viene fatta attraverso il modulo nella Figura 1.7 sottostante.

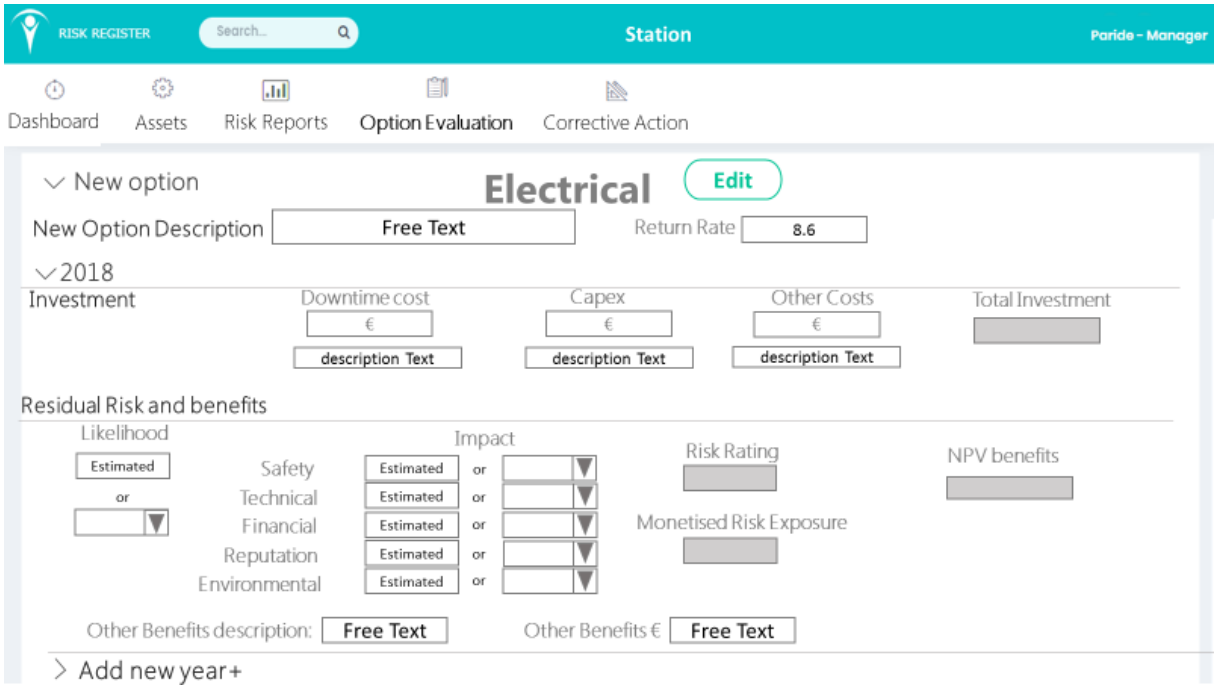

Figura 1.6: Modulo per le opzioni di investimento

Ogni elemento della Figura sopra riportata è stato già descritto all'interno di questo riassunto in italiano, motivo per cui si presuppone che il lettore abbia dimestichezza con i termini riportati in Figura 1.7. Fondamentale non confondere il *Residual risk* con il profilo di rischio, infatti il primo fa unicamente riferimento all'andamento del rischio dopo l'investimento. Dopo l'inserimento dell'opzione di investimento per l'anno desiderato (di default viene visualizzato l'anno corrente ma l'utente ha la possibilità di aggiungere piani di investimento per tutto il periodo di vita dell'impianto) all'utente non rimane altro che salvare quanto è stato appena inserito e visualizzare la panoramica delle situazioni di investimento, così come riportato in Figura 7.25 all'interno del testo. Proprio tale panoramica permette di confrontare diverse opzioni di investimento, usando come valore di paragone l'indice di valutazione (*Evaluation index,* formula 15). L'opzione con l'indice di valutazione più elevata sarà la più vantaggiosa. Infine, la sezione di *Option Evaluation,* non ancora caricata all'interno del prototipo, sarà ampliamente estratta dal registro dei rischi correntemente utilizzata dal Tosca Solution, in quanto il modulo richiesto dalla società elettrica non si discosta da quanto già sviluppato precedentemente.

Infine, l'ultimo capitolo concerne l'analisi funzionale che si esegue per rischi operazionali. La sezione di analisi decisionale inserita all'interno di questo lavoro sottolinea l'importanza della gestione dei rischi operativi e la necessità, quindi, di sviluppare e introdurre tra le aziende un software che permetta la valutazione delle procedure.

IDDA è un software sviluppato sul finire degli anni Novanta e permette di eseguire una analisi decisionale basata sulla dinamica del sistema. IDDA sfrutta un modello logico decisionale e fenomenologico che crea una sorta di albero degli eventi "potenziato", fornendo all'utente una panoramica delle probabilità di uscita dal sistema per ogni possibile catena di eventi. In questo lavoro di tesi si è usato un esempio di travaso di ammoniaca da autocisterna a serbatoio fisso in impianto con conseguente riempimento delle bombole destinate alla vendita come caso studio per dimostrare l'efficacia di un software per l'analisi procedurale. Tale procedura è eseguita dalla società elettrica irlandesi in diversi impianti di loro gestione.

I risultati ottenuti tramite l'analisi funzionale di IDDA hanno mostrato come la probabilità globale che un evento indesiderato accada abbia una probabilità totale notevolmente elevata (61%) ma risulta importante sottolineare che l'evento più rilevante in termini probabilistici sia il ritardo del processo (55%). Infatti, il rischio al personale e la sicurezza del processo presentano una probabilità di accadimento notevolmente più bassa (meno del 15%). L'uso di un modello probabilistico come IDDA garantisce consistenza e completezza durante la fase di valutazione di rischio già a partire dalle fasi iniziali di progettazione dell'impianto anche grazie alla possibilità di eseguire un calcolo sul ritardo globale dovuto ai rischi occupazionali e di processo e il calcolo del valore monetizzato del rischio per ogni procedura all'interno del processo. La fusione di queste funzionalità di IDDA con il registro dei rischi attualmente in commercio permetteranno a Tosca Solution e a tutto il mondo della HSE (*Health Safety and Environment)* di avere un software innovativo e del tutto completo che permetta di fornire un livello di dettaglio di rischi tecnici ed operazionali del tutto unico ed innovativo.

2. Introduction

Every workplace presents several risks: some of them could have a low likelihood but a high severity, others could happen frequently, and they have a very low impact. Anyhow all the detected risks founded must been monitored independently of their likelihood and severity. The word "risk", from the French "risqué", in accord with the Oxford English Dictionary, could be defined as "*A situation involving exposure to danger*". Although other definitions of risk are also trusty and reliable, like the one from the Occupational Health & Safety Advisory Services (OHSAS) that says: "*Risk is a combination of the likelihood of an occurrence of a hazardous evet or exposure and the severity of injury or ill health that can be caused by the event or exposure*", the most realistic definition of risk is the one according to the International Organization of Standardization publication ISO 31000:2009, that defines the risk as the "*Effect of uncertainty on objectives*". This definition may be applied for every kind of risk, that it is possible to be listed in 4 generic categories: Technical, Environmental, Financial and Human risk.

During the previous years the normative related to the risk and its assessment and mitigation have been developed in order to increase the safety of every workplace. In fact, since the 80s, all around the world has observed the increase of stricter normative and the recording of the most important accidents throughout the years. An example is the database *eMARS* which is monitoring all the European accidents since 1982 and it has recorded more than 816 accidents. The more accurate records of the risks during the previous years led to the need to develop risk registers with increasing complexity. Indeed, the amount of information requested by the companies for managing the risk is continuously increasing and the use of informatic spreadsheets needs a moderate amount of knowledge of the tool and of the system.

In some cases, the companies try to split the risk information into different spreadsheets for managing different kinds of risk in different ways. It remarks the coherence of the Irish power generation company that is using two different spreadsheets for managing its risks. Although the development of a new user-friendly interface for a risk register is severely required and suggested, the amount of information requested involves a considerable amount of knowledge of the system by the user. It means that the development of the system requires a strong consideration of the users and company needs. Furthermore, the creation of an easily understandable mock-up with logical links through all the paths of the risk management involves an intensive work of the safety analysts in order to conciliate the companies need and the developer's difficulties. In the risk register some of the risks are related to tasks being carried out. Those tasks can be analysed using task analysis as a mean of functional analysis, where every step needs to led to either another step or an event or a final state. The method that can be used is a dynamic event tree where the probability of outcomes could be estimated on the basis of existing databases values or using the data stored in the risk register if the tasks are also used to inform checklist where operator can report anomalies related to each step.

Despite the substantial worldwide interest in risk management in the last years, the risk in the workplace is still a threatening presence in which it is necessary to be always focused. Several techniques were developed in the last years and the ISO 31010:2009 can offer a clear overview of those methods aimed at risk management. Some of those techniques are commonly used for estimating risk for technical assets, and others are used for financial and/or for assessing procedural risks. The operational risk assessment presents numerous vacancies of knowledge especially related to the temporal sequences and how some events that are happening could influence other ones that are not strictly related. Several approaches have been tried during the previous years and in literature it is easy to find how the researchers all over the world studied how to find a user-friendly way to understand the decision dynamic analysis. Moreover, the technology progress in the informatic systems and the large daily use of electronical devices has led to the need to develop a product for everyone. For this reason, the Irish campus-based company Tosca Human Factor Solutions Ltd aims to developing an innovative concept of risk management in accord with the last updates of the international safety normative. The aim of Tosca Solution is to improve an advanced multifunctional software which connects the risk register information with an innovative operational analysis tool. IDDA (Integrated Dynamic Decision Analysis) is a tool developed in Polytechnic of Turin a few years ago aimed at analysing dynamic procedures and calculating the probability of each possible events inside the whole operations range. A logical-probabilistic model integrated with a phenomenological model is employed to describe the physical behaviour of the process for each step.

The present work aims to better understand the need of the companies for risk management, by trying to provide a complete and tailored software in order to meet the technical and operational need of the plants. The work is basically divided in two parts, each of which consists in three chapters.The purpose of the first chapter of this work is to give a brief overview about the risk, its definition and its characteristics, some literature reviews behind it and the different approaches in managing risks related to technical assets and procedures. Chapter two is built around both the definitions of ISO 31000:2009 and ISO 31010:2009 related to risk management and the techniques commonly used for risk assessment. The last theoretical notions chapter provides a literature overview about risk register for introducing the last three chapters of the work where the risk register is plenty analysed. The first chapter of the second part is an introduction the case study, and there is also a briefly description of the actual used spreadsheets of the Irish power generation company (CAR and GRR). Moreover, in this chapter, there is description of the most important output that currently is possible to use from the data contained in GRR and CAR. Chapter five is aimed at outlining the Irish company needs of an advanced prototype that is useful to identify, analyse, monitor, and find a mitigation to the risks. As a result, the company requested an evaluation module for helping the manager to choose properly the best option for a future investment. Finally, the last chapter analyses a case study of an ammonia plant for procedural risks by using a dynamic decision tool that will be soon a new feature of the Tosca's risk register.

PARTE I

THEORETICAL NOTIONS

3. Risk definition and overview

3.1 Definition of risk

Even the rigid application of the existing technical standards does not always guarantee an adequate level of safety, especially the maintenance of the safety standards over time, by considering that incidental events sometimes occur in the chemical industry as well as other workplaces. A constant verification of the equipment and process procedures in order to maintain the risk within certain tolerable limits is necessary to successfully manage the risk in a long-time period. The definition of risk is not unique and different interpretations exist in literature: for someone, the risk is measured by the probability of having a damage, for others, instead, the measure of the risk is provided by the damage itself, such as the number of victims that a possible accident can cause. In this text the risk will be define in accord with the description of ISO 31000 that expresses the risk as "*Effect of uncertainty on objectives*" (ISO 31000, 2009). These objectives, referenced by the ISO, can have different origins and have various aspects: even in everyday life, it is possible to encounter several risks such as financial, health and safety and environmental risks. Moreover, this definition of risk gives the possibility of being able to quantify the risk: this advantage is not granted by many other definitions and this leads to judgements on the magnitude of the risk in a very highly subjective way, because it does not derive from a rigorous scientific analysis.

3.2 The risk evaluation

The quantitative measure of risk is possible thanks to the definition provided by the note 2.1 of ISO 31000:2009, where the risk is defined as "*The risk is often expressed in terms of combining the consequences of an event and the associated likelihood of occurrence*". From this definition it possible to write:

$$R = f(F, S)$$

Where:

- F represents the frequency of occurrence, which is the likelihood of an event occurs in a certain time interval;
- S represents the severity, which is the extent of the consequence of an event.

The link between these two variables was proposed by Professor Rasmussen in 1975 in the well-known "Rasmussen Report", where he proposed the following expression:

$$R = F \cdot S \tag{1}$$

By using the above expression, it is possible to obtain an interesting graphical representation as shown in Figure 3.1. It helps to understand the substantial difference between protection, that is a reduction in severity, and prevention, that is a reduction of the likelihood of an occurrence.

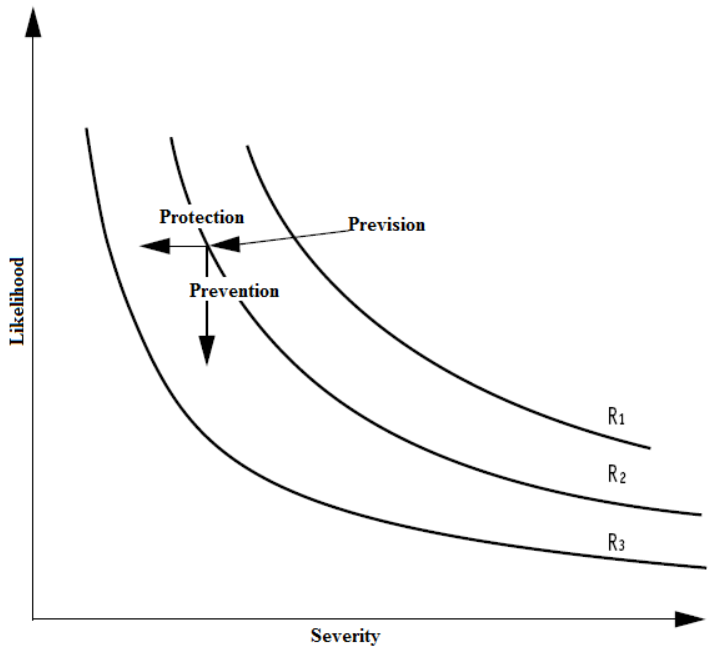

Figure 3.1: Severity vs Likelihood curves, by maintaining constant the risk level

It worth to keep in mind that cancelling the risk is an utopian concept, achievable only in the case of complete inactivity. In fact, trying to reduce the risk beyond a certain limit, would mean increasing the number of sequences of critical events with unexpected consequences. Although some companies nowadays attain a zero accident or injury record for a certain period of time, it does not mean that the operations that they use to perform are risk-free.

The categorization of risk allows the analyst to get a precise idea of which risk should be mainly treated for its high severity-frequency combination. Generally, in literature, the risk can fall into one of the following three categories:

- **Tolerable risk:** Very common risk but with a very low severity. This risk is widely accepted as part of the daily life.
- **Conventional risk (ALARP):** Fairly frequent event with medium-intensity damage. The acronym ALARP (*"As low as reasonably practicable")* is a principle aimed at reducing the risk in the most reasonable way. To consider a risk ALARP, it has to show that the costs of reducing the risk must guarantee a monetary return by reducing the risk.
- **Intolerable risk:** Resulting from major anomalies, it has a very low likelihood but a very high severity. For this category of unacceptable risks, design and/or management changes are strictly recommended.

A useful representation of those three categories of risk listed above, according to the ALARP criteria, is often reported in textbooks with the Pyramid of risk (Figure 3.2).

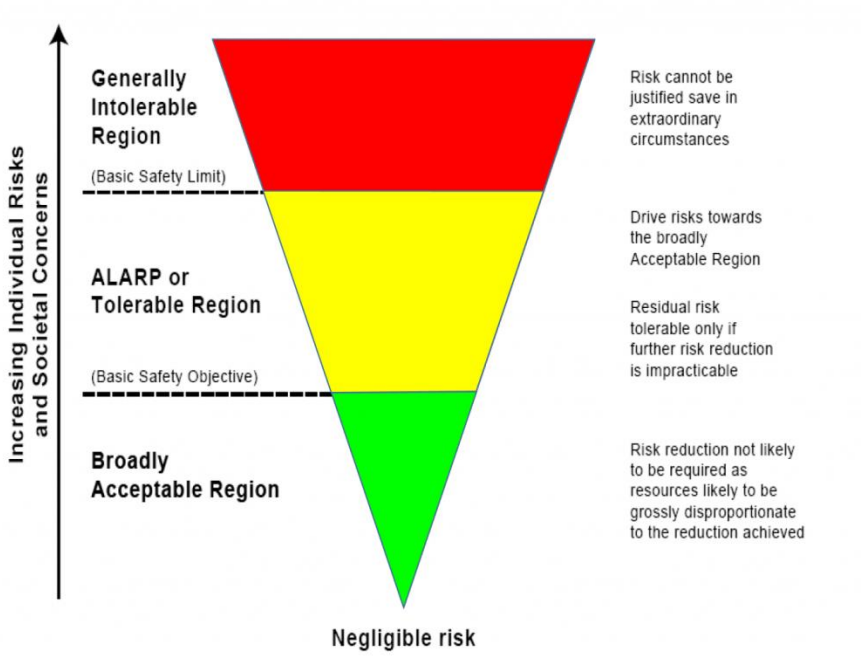

Figure 3.2: Pyramid of risk helps to understand the risk categories

3.2.1 The categories of the likelihood

It is crucial to estimate the frequency of an annual event to be able to quantify the risk. The scale that is generally taken to measure the probability varies from a value of one, which represents the least probability of occurrence, to a probability of five that is the highest probability of occurrence of the considered event. The term likelihood is used to indicate the plausibility of a given parameter evaluated and is not to be confused with the term probability which is used as likelihood that an event could happen. The estimation of likelihood is a subjective operation but strongly influenced by the experience of the analyst and the empirical models described in the literature. Generally, the operator of a plant knows the problems occurred in the past in its plant (archives, cards related to accidents, occupational diseases, production interruptions) and therefore it has the possibility to carry out an effective estimation of the probability of occurrence.

	Likelihood
1	Very Rare
2	Rare
3	Occasional
4	Often
5	Very Often

Table 3.1: Likelihood categories of the risk

3.2.2 The categories of the severity

The severity is a rough estimation of the potential for a certain risk of injury, death, economic loss, environmental problems and other possible unpleasant events for the activity. The evaluation that analyses the severity of the consequences generated by a certain danger situation based on a subjective analysis. The analyst, even though experienced, is a person who is able to recognize in an accurate manner the severity of a certain risky situation. The consequences of a risk are not necessary related to technical or process aspects of the productive activity, but it extends to all those processes that have a financial, environmental and reputational implication.

	Severity
1	Very low
2	Low
3	Medium
4	High
5	Very high

Table 3.2: Severity categories of the risk

Risks could have different consequences depending on the viewpoint of an individual/group (Leva, Balfe, Mc.Aleer, & Rocke, 2017). For example, in the energy industry, a transformer failure would have high consequences for an individual generation station as they cannot export the electricity generated. However, it is not necessarily an issue for the business as they may be able to compensate with another station and can even be a benefit to those other stations that will receive a higher payment for exporting more electricity. These different perspectives must be reconciled by monetizing values of those risks and aggregating them at overall business level. (Patterson & Neailey, 2002)

3.3 The Risk Matrix

The risk matrix is without a doubt a useful support needed to quantify the risk approximately through a subjective interpretation of probability and magnitude. Typically, a 5x5 matrix is used with three or four colours required to diversify the level of the estimated risk. Even though it is a useful tool for the estimation of risk, in the literature (Cox, 2008) are equal risk value analysed several mathematical problems related to the use of the matrix for the evaluation of risks. Considering that equal risk values are assigned for quantitatively different risks, it can generate some problems related to risk assessment errors or poor matrix: this phenomenon is called "range compression". Another common issue of the risk matrix that normally supported in literature is the ambiguity of inputs and outputs, because the estimation of likelihood and magnitude requires a subjective interpretation by users.

Table 3.3 shown a series of information obtained from a 5x5 four-colours risk matrix.

Table 3.4 is an example of a typical matrix of risks is shown instead.

Colour	*Range values*	*Risk level*	*Comment*
Red	16-25	Extremely High	Unacceptable. Action plan urgently needed
Amber	11-15	High	Apply Immediate Controls
Yellow	6-10	Moderate	Apply judgment
Green	1-5	Low	Monitor and manage routine procedures

Table 3.3: Risk matrix information

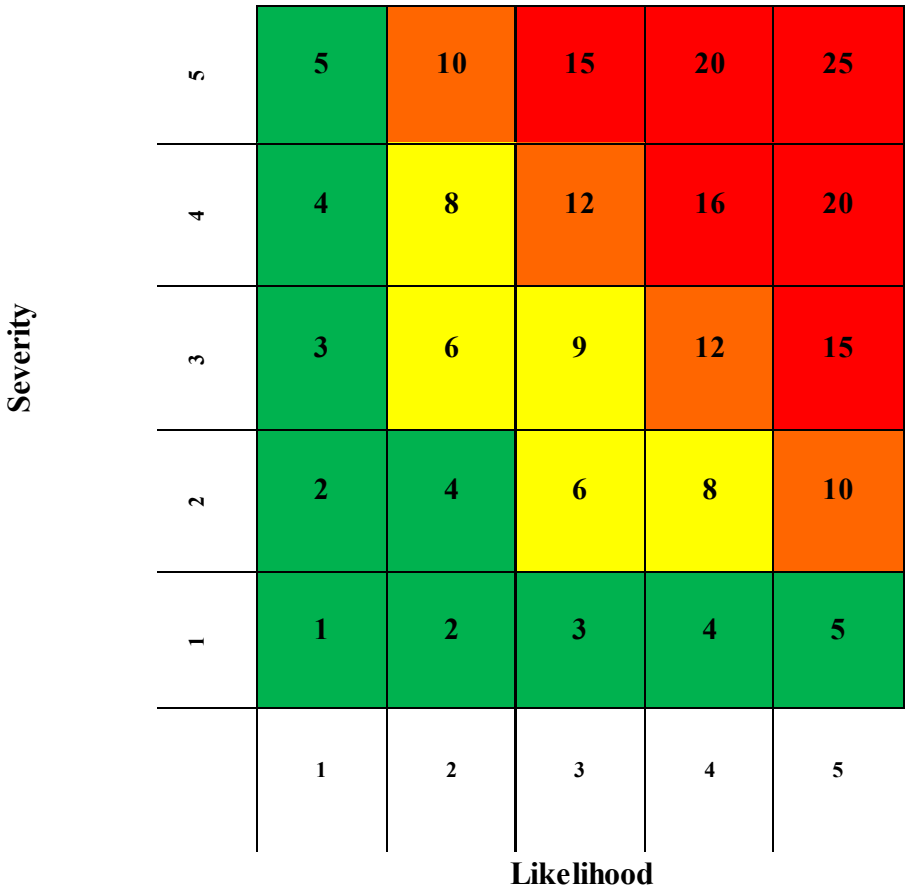

Table 3.4: 5x5 Risk Matrix with four colours

3.4 Analytical techniques and tools

There are several techniques that allow the analysis of risk; these techniques are generally divided into:

- Inductive methods

- Deductive methods
- Methods based on stochastic processes

Inductive methods, or descending methods, are based on the question "What happens if...?". This question is asked by a team of people with different backgrounds but also with a strong familiarity with the case of study. This technique, definable also as a sort of brain storming, is often supported by a check list in order to reach a best complete analysis. Deductive methods, also called ascending methods are based on the question "Why...?" which is asked, as in the case described above, by a team of experts. A tool based on this kind of method is the Fault Tree (FT), which is a graphical representation of the combination of basic events that led to a major unwanted event. Finally, the methods based on stochastic processes are techniques that use a dynamic system supported by a probabilistic type behaviour. Without doubts, the most widespread used stochastic analysis techniques are the Markov chains and the Monte-Carlo method.

It is possible to recognize different techniques for a complete assessment depending on the kind of risk. By dividing the risks assessment for two different categories: technical assets and procedures/operations. Risk assessment for technical assets is referred directly with the data base being employed and its technical aspects including understanding, reproducibility and similar. It is possible to define Technical Risk as "*the risk that the project will not achieve its objectives due to risks which arise in the integration of critical technologies, and/or sub-systems dependent on them*" (J O'Neill, 2007).

On the other hand, the definition adopted by the EU in Solvency II Directive for the operational risks is: *"operational risk is the risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses"*

The normative ISO 31010:2009 divides types of risk assessment techniques in different groups depending of their application:

- Look-up Methods
- Supporting Methods
- Scenario Analysis
- Function Analysis
- Controls Assessment
- Statistical Methods

A partially list of the most used techniques for risk assessment of technical asset and for risk assessment of procedures is described in the paragraphs below, though the full list is reported in Chapter 2: Risk Management Requires in this work.

3.4.1 HazID

The HazID (Hazard Identification studies), is a tool used for identifying occupational, facility and external hazards. It is often used early in a project plant in order to help the HSE (Health, Safety and Environment) deliverables in a project. The HazID aim at reducing and preventing all the possible consequences that could cause damage or loss of property, production products,

environment or injuries to personnel. An HazID study usually takes in account all the technical assets and equipment designers in order to ensure a full identification of hazard and safeguard procedures. Several benefits of HazID are:

- Revealing of hazard at an early phase before they happen.
- Hazards are recorded and managed to be avoided, mitigated or highlighted.
- Preventive actions are controllable.
- Risk screening criteria are recognized.
- Non-critical hazards are documented to demonstrate the events in question could be safely ignored.

3.4.2 Hazard and Operability Studies (HAZOP)

The HAZOP (Hazard and Operability studies) is a qualitative function analysis based on a general procedure of risk identification to express possible deviations from the intended performance. Usually, all the criticalities of the deviations are assessed in the analysis that is carried out by a multi-disciplinary team during a set of meetings. The HAZOP analysis is an organized and methodical method of an existing product, process, procedure or system. Mainly, HAZOP process is used to analyse every kind of system and complex procedures since the detail design stage. The process of an HAZOP analysis is aimed at discovering all the potential deviations in which the intended performance can occur, all the potential causes and all the probable consequences of each deviation. The ISO 31010:2009 wants also to outline the importance to use simple guidewords for technical systems, in order to identify human error modes. The steps in an HAZOP analysis include the nomination with the necessary skills to conduct the hazard operability studies, the definition of the study goals and the establishment of guidewords for the study. Moreover, it is required to define a multidisciplinary HAZOP study team, not necessarily involved in the system, in order to include design and operation personnel with an appropriate knowledge range. The advantages of an HAZOP analysis are several, by providing a systematically and methodically examination of the procedures involving a team with real-life process experience. Furthermore, the applicability of HAZOP is possible in a wide range of systems and processes and also it permits to have explicit consideration of the causes and consequences of human error. The HAZOP process has some disadvantages such as the time-consumption and the cost, by requiring a high level of system documentation and process specification.

3.4.3 FMEA

The FMEA method (Failure Mode and Effect Analysis) allows analyse using the failure mode or a system through an inductive analysis based on the question "What happen if..." and other theoretical considerations. The Method can be modified in FMECA by adding a further analysis related to criticality, making a quantitative analysis instead of purely qualitative (Dağsuyu, Göçmen, Narlı, & Kokangül, 2016). FMEA uses three risk factors: or occurrence, that is the probability of occurrence of a risk, detectability or the likelihood of predicting the risk before it happens, and severity or the danger of the consequences generated by the risk. The output parameter, defined as Risk Priority Number (RPN), is the product of the three risk factors that classifies the risk evaluated on a 10-base value scale. The RPN with the highest value will be

examined by analysts. Generally, action plans are required to mitigate the risk when the value of RPN is greater than 100.

According to ISO 31010 FMEA identifies:

- All potential failure modes of various parts of a system
- The effects these failures may have on the system
- The mechanisms of the failures
- How to avoid the failures, and/or mitigate the effects.

3.4.4 Fault Tree Analysis (FTA)

The Fault Tree Analysis is a method based on the knowledge of based event failure or failure rate. Thais kind of analysis is a deductive one, by starting from a general and undesired event, commonly called *Top Event*, of the main failure, arrives to recognize the factors that can partly contribute to cause the *Top Event*. Fault Tree Analysis is frequently used as qualitative investigation of the potential causes and pathways to the *Top Event* and it is used as quantitative analysis to calculate the probability that the main unexpected event happens, given information of the probabilities of causal events. This kind of analysis is very similar to FMEA, in which the purpose of the analysis was to reach the system failure by starting to define the failure of the single components. For the construction of a fault tree is required a plenty understating of the system and the causes of failure as well as a technical knowledge of the system in order to have the faculty to build a detailed diagram. FTA is a method with several applications and could be used for preventing the failure as well as to identify the causes already detected. The key elements of a Fault Tree Analysis are:

- Combination of causes: combination of the failures that bring the system to the *Top Event*.
- Examined unit: the system to analyse with main characteristics and functionality.
- Component: lower level unit that can cause to the *Top Event*

During the construction of a fault tree, the use of logic gates, especially *OR* and *AND is* necessary in order to connect the failure of the system to the base components. The FTA use permits the focus of attention on those effects of failure which are directly related to the top event, by analysing also systems with many interfaces and interactions. All of the pathways can lead to the cut sets in a varied simple way through the system results are very complex. The inability to analyse the domino effect or conditional failure and the binary states (failed/not failed) are a few examples of limitations of the FTA. Furthermore, the fault tree is a static model and it does not consider failures caused by human errors (ISO 31010, 2009).

3.4.5 Event Tree Analysis (ETA)

The Event Tree Analysis is an inductive logical modelling technique that permits the analysis both success and failure by responding at a single initiating event through an idea of *chronology* (or at least of ordering). Two fundamental points of an Event Tree are:

- Allowance given to the events encountered in the progression of the accidental transient.

- Branching in the tree depending on the occurrence of each considered event.

It is possible to consider the Event Tree Analysis as the basis of the probabilistic safety analysis through the identification of the accident scenarios and their consequences. Moreover, it is possible to evaluate a hierarchy of the vulnerabilities of a plant by estimating the occurrence probabilities of the scenarios identified. It is remarkable that a tree analysis is generally valid for practically any kind of risk assessment application, but its results are most effective when safeguards are in place as protective features. The Event Tree Analysis can be also applied to a system early in the project process to identify potential issues that could occur. An event tree starts with a set of initiating events (or just one) that change the state of the system, for example an increase of temperature/pressure or a release of a hazardous substance. Each initiating event leads to another event that again leads to another one. Each path is assigned with probability of occurrence and a probability of various possible outcomes which can be calculated. This path will continue across the intermediate events until an end state is reached. Usually the intermediate events are split into a binary mode (success/failure of the system) but they could be split also into more than two if the events are mutually exclusive. The results of an event tree are used in decision making: for each result of the event tree, determine the appropriate frequency and consequence that characterize the specific outcome. In Figure 3.3 below an example of the graphical structure is shown, with the starting event on the left, from where the different branches grown.

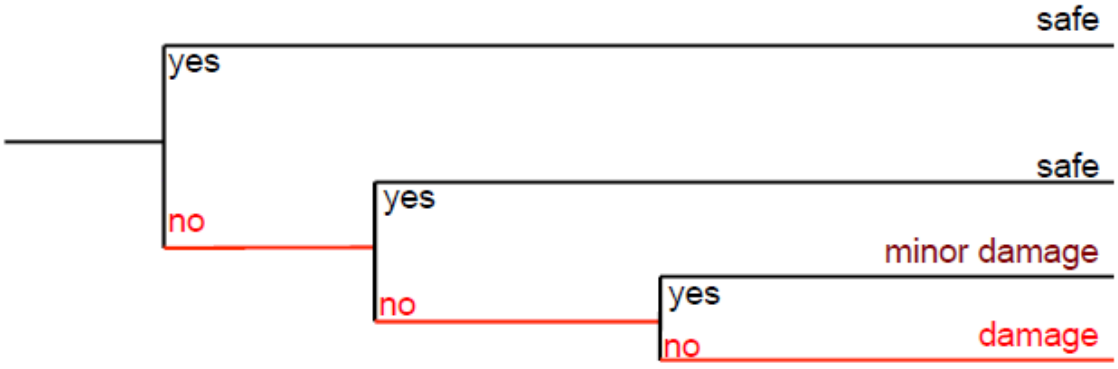

Figure 3.3: Event tree example

3.5 The Dependability

The safety of an operation, also known as dependability in accordance with UNI 9910 legislation of 1991, is the reliability that can be attributed to a system in a period of time, as regards its proper functioning. The dependability is a concept that extends throughout the life cycle of the system in question, then from the design and construction phase to the operational phases. (UNI, 1991)

With the term dependability it is possible to designate several operations:

- Measures: Reliability, availability, maintainability, safety, and security (RAMS)
- Means: Fault prediction, fault tolerance, fault removal, and fault prevention.
- Threats: faults, errors, and failures.

It is good to remind that the dependability, as a quantitative analysis, is aimed at an evaluation of different elements:

- Risk assessment and security
- Project specifications
- Technical assistance and maintenance
- Life cycle cost
- Market competition

The planning of all the activities related to technical assistance and maintenance are related to the dependability and then the expected number of failures in a certain period. The cost of technical assistance, the purchase of spare parts and the organization of maintenance are elements that affect the trust of the system, both from a preventive and responsive point of view.

3.6 Unreliability, reliability, density, and failure rate

Reliability is a measure attributed to dependability and is briefly defined as the aptitude of a system to perform the required function respecting to the technical specifications in a certain amount of time. In more specific mathematical terms, we can define the reliability $R(t)$ of an item on time as the probability that this item performs the required function in an interval (0-T) considering the stress factors and the ambient conditions in which it operates.

Considering a generic variable X as the failure time of an element, it can derive the function of the cumulative distribution (CDF) of the component's unreliability:

$$F(t) = \Pr\{X \leq t\} \tag{2}$$

The calculated value F (t) represents a probability distribution function.

By calculating:

$$F(0) = 0$$
$$\lim_{t \to \infty} F(t) = 1$$
$$F(t) = non - decreasing$$

It is possible to graphically construct the function of system unreliability

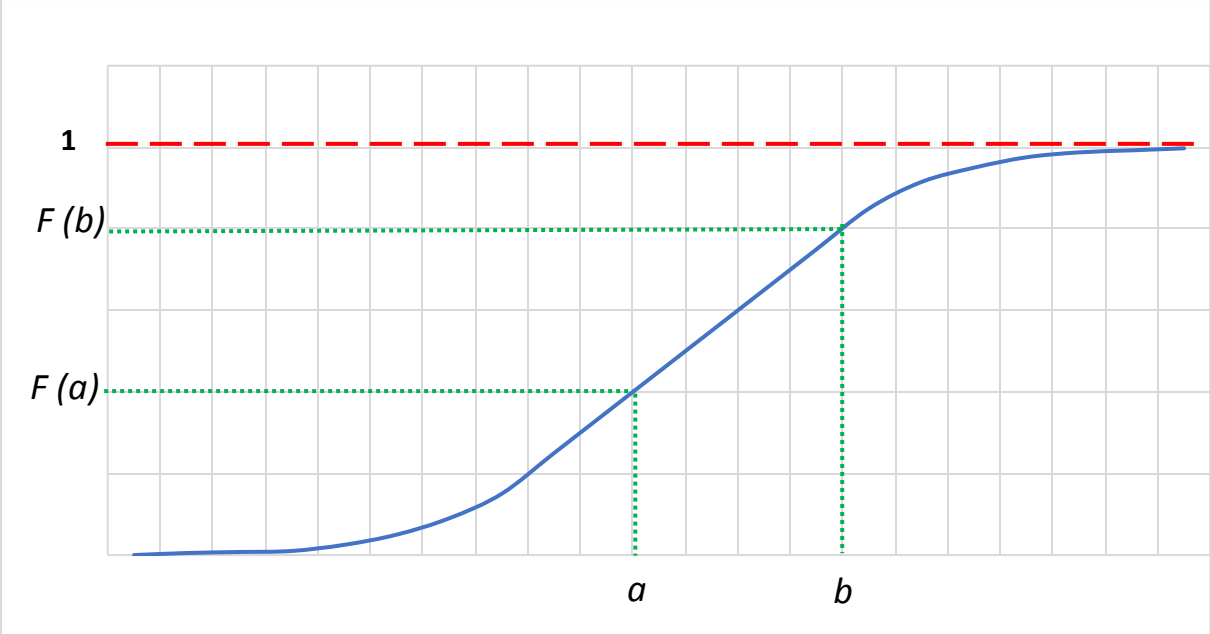

Figure 3.4: Unreliability

Then it is possible to determine the survival function (SF) $R(t)$ of the generic variable X that refers to as the failure time of an element. The function is definable as:

$$R(t) = \Pr\{X > t\} = 1 - F(t) \tag{3}$$

The Survival Function $R(t)$ represents the probability that the element works correctly during a time interval. This function, which is nothing more than the complement to one of the unreliability, is definable as a function of reliability.

Considering that:

$$R(0) = 1$$
$$\lim_{t \to \infty} R(t) = 0$$
$$R(t) = non - increasing$$

It is also possible to graphically build the function of system reliability

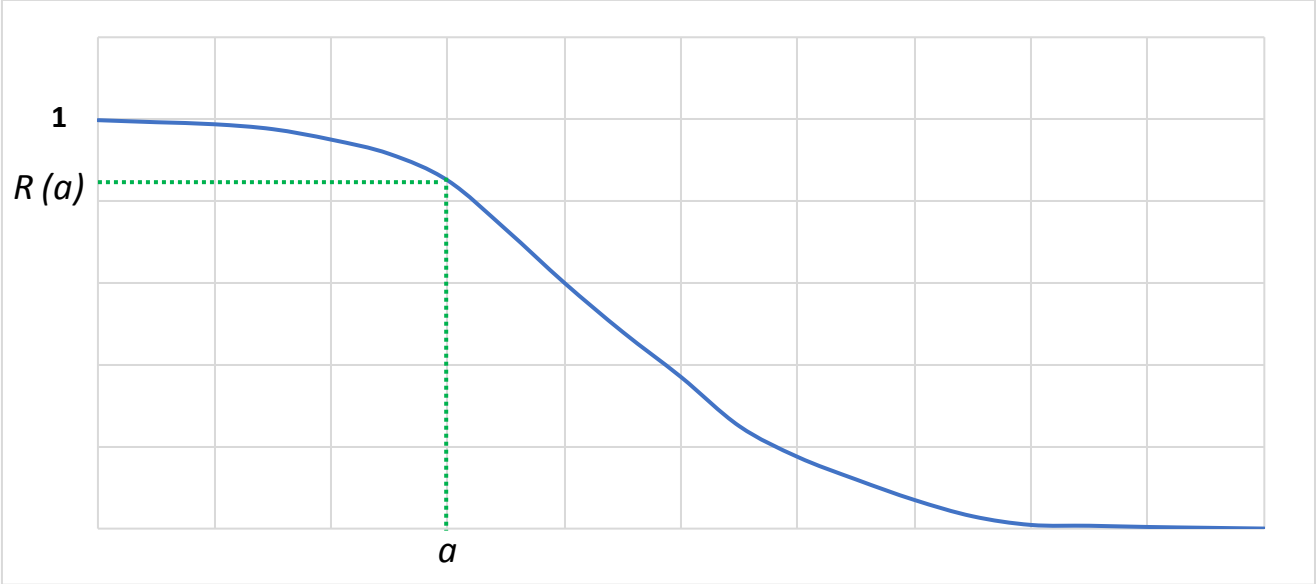

Figure 3.5: Reliability

Another basic definition to be introduced with risk is the statistical distribution of failures, also called function of density. Again, considering X as a generic variable referred to as the fault time and considering the unreliability $F(t)$ derivable as a function of time, it is possible to define the density as:

$$f(t) = \frac{d\,F(t)}{dt} \tag{4}$$

By knowing the value of $F(T)$ from the equation 3 it is also possible to write:

$$f(t)\,dt = \Pr\{\,t \leq X < t + dt\} \tag{5}$$

By integrating the function of the equation 4, it is possible to determine the mean time to failure (MTTF) of the element, which can also be defined as the expected value of the failures statistical distribution function.

$$MTTF = E(t) = \int_0^\infty t\, f(t)dt = \int_0^\infty R(t) \tag{6}$$

Another fundamental term for the calculation of reliability, or unreliability, is the failure rate, defined as the mathematical division between the statistical distribution of failures in a certain range of time (t, t + Dt) and the system reliability:

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} = \lambda \tag{7}$$

The failure rate calculated above provides a conditional probability that a certain element fails in the time interval (t, t + DT) whereas it is working at time t. It is not to be confused with the unconditional probability that the element fails in the interval (t, t + DT), because the last definition does not guarantee that the element in question is working at time t.

Summarizing all the terms listed above in chapter related to dependability and placing them dependent on the failure rate (λ), which resulted independent of the aging of the element.

- Unreliability: $F(t) = 1 - e^{-\lambda t} \quad t \geq 0$ (8)
- Reliability: $R(t) = e^{-\lambda t} \quad t \geq 0$ (9)
- Density function: $f(t) = \lambda e^{-\lambda t} \quad t \geq 0$ (10)
- Failure rate: $h(t) = \frac{f(t)}{R(t)} = \lambda$ (11)
- Mean Time of Failure: $MTTF = \frac{1}{\lambda}$ (12)

4. Risk Management Requirements

4.1 Standards and requirements about risk management

The first management systems were introduced and normed in the 1980s by the publication of ISO 8402:1988 and today known as ISO 9000, aim at controlling and implementing the quality, through the efficient and effective realization of a product that fully satisfies the customers. Today, the ISO 9001 standard, with its latest revision dated 2015, is the standard reference for those who want to control their production process quality. Besides the quality management, even environmental management systems, regulated by ISO 14000, with the latest review dated 2015, are now known and commonly applied. Regarding the standardization of risk management, has been standardized both by the OHSAS 18000 legislation enacted from British Standard Organization (BSI) in 1999 and ISO 31000 published in 2009 by the International Organization for Standardization. Risk Management is definable as *"the set of activities for managing and controlling the level of risk in a company or organization"* (ISO 31000, 2009). An integrated management system based on synergic actions of quality, environment and security control, could allow greater management efficiency and greater business competitiveness, by considering that the above-mentioned regulations have several points in common, and being the company's need to fulfil such standards. The first step in risk management is to establish a context: that means that it is necessary to define external and internal parameters in order to establish the political criteria with which the risk must be administered, namely to define the organisation, the responsibilities, the objectives, the structure and the elements of the system in question. A well-regulated risk management allows organizations to have a greater guarantee of compliance with laws and regulations, in addition to an improvement in production activities and relationships with external interlocutors.

According to ISO 31010, risk management includes the application of logical and systematic methods for:

- communicating and consulting throughout this process;
- establishing the context for identifying, analysing, evaluating, treating risk associated with any activity, process, function or product;
- monitoring and reviewing risks;
- reporting and recording the result appropriately.

4.2 Safety Management Systems (SMSs)

A risk management system sometimes represents a rough SMS focused on managing risk. Although the risk is not only relating to safety but also to economics, i.e. financial risk, the principles are comparable of any kind of risk management system. There are many examples of SMSs in which a risk management system is an important component, even though some

regard a safety management system as phase of risk management. In particular, the safety management system may be described as "*Identification and evaluation of major hazards*" attends to the *"adoption and implementation of procedures for systematically identifying major hazards arising from normal and abnormal operation and the assessment of their likelihood and severity"* (Demichela, Piccinini, & Romano, Risk analysis as a basis for safety management system, 2004). A safety management system (SMS) is either a system which manage and control safety or it is a management system specifically aimed at safety. Safety is a comprehensive and abstract notion, which is best defined in a specific situation. The situation is free from "something" that might have negative consequences, such as damage to individuals or animals, financial loss, or any other form of harm or loss. That means safety is the condition whereby unpredicted events, such as accidents and incidents, are being involved. This work concerned with engineering safety; hence, the unforeseen events and risks arise within the context of industrial activities. When comparing safety with safety management, the former refers to a state or condition, the latter is a process or a series of certain activities (Li & Guldenmund, 2018). Moreover, safety is free from intolerable consequences and safety management is the procedure to realise certain safety functions. Safety management system is a very practical notion widely used in different industries and it means "a systematic control of worker performance, equipment performance and the physical environment".

4.3 Establishing the context

Establishing the context is necessary to define the internal and external parameters to be take into account when managing risk and sets the scope and risk standards for the remaining procedure. Although many of these parameters are similar to those considered in the design of the risk management framework, when establishing the context for the risk management process they need to be considered in greater detail. There are two distinguished contexts:

- external context
- internal context

The external context is the external environment in which the organization seek to achieve its objectives (ISO 31000, 2009). It is founded on the organization-wide context, but with specific details of legal and regulatory necessities. Examples of external context could be the society and culture, politic, the law, the finance, the technology, the nature, whether international, national, regional or local. Moreover, the external context looks forward to establishing relationship with external stakeholders.

On the other hand, the internal context aims at supporting the risk management process with the organization's culture, process, structure and strategy. Internal context is anything within the organization that could impact the technique in which an organization will manage risk. Governance, organizational structure, organizations culture, roles and accountabilities are examples of organization's internal context. Furthermore, policies, objectives and the strategies that are in place to achieve them are included in the internal context as well as the relationship with the internal stakeholders and the guidelines adopted by the organization.

In general, the context has to been established to regulate all the objectives, define goals and responsibilities for the risk management process. Additionally, it is necessary to define the risk assessment procedures, the strategies and all the activity and functions of the organization.

These precautions written above should help to guarantee that the risk management method adopted is proper to the circumstances.

4.4 Methodology

Managing a risk is a five-step procedure for controlling exposure to health and safety, finance, environmental, reputational risk related with hazards in the workplace. The steps are:

1. Establishing the context.
2. Risk identification.
3. Risk analysis.
4. Risk Evaluation.
5. Risk treatment.

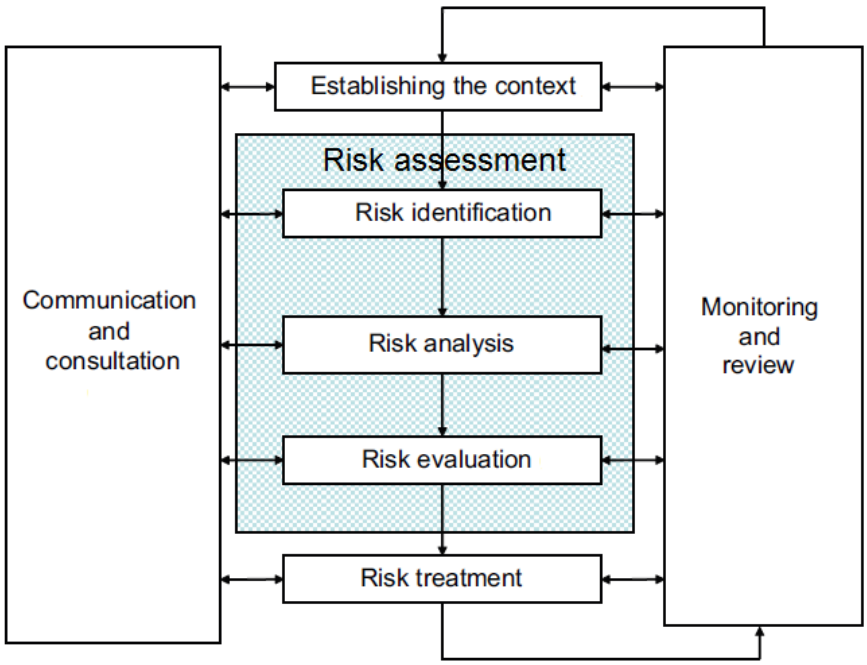

Figure 4.1: Risk management process (ISO 31000)

As shown in Figure 4.1, the risk management is a process based on several key points and steps. First of all, the communication and consultation with external and internal stakeholders should take place during all phases of risk management process. Consultation and communication are very important steps that have to be developed at the early stage. These should address issues relating to the hazard itself, its causes, its consequences, and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required (ISO 31000, 2009). A consultative team approach may help create the context properly and ensure that the interests of stakeholders are understood and considered. Then it is very important to help ensure that risks are adequately identified. Bringing different areas of expertise together for analysing risks ensures that different views are appropriately considered when defining risk criteria and in evaluating risks. It also represents a strong core duty of the

consultative team. Finally, it is necessary to secure endorsement and support for an action plan, enhance appropriate change management during the risk management process and develop an appropriate external and internal communication and consultation plan. The normative ISO 31010 provides guideline on selection and application of systematic techniques for risk assessment. This normative shows the use of different techniques, by referring to other international normative, in which the concept and the application have been described in detail. ISO 31010 reported thirty-one, not strictly related to safety, different techniques. The techniques extracted from the ISO and their common applicability are described in Table 4.1:

Tools and techniques	**Risk assessment process**				
	Risk identification	**Risk analysis**			**Risk evaluation**
		Consequence	**Likelihood**	**Risk Level**	
Brainstorming	SA	NA	NA	NA	NA
Structured or semi-structured interviews	SA	NA	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Check-lists	SA	NA	NA	NA	NA
Primary hazard analysis	SA	NA	NA	NA	NA
HAZOP	SA	SA	A	A	A
HACCP	SA	SA	NA	NA	SA
Environmental risk assessment	SA	SA	SA	SA	SA
Structure "What if?"	SA	SA	SA	SA	SA
Scenario analysis	SA	SA	A	A	A
Business impact analysis	A	SA	A	A	A
Root cause analysis	NA	SA	SA	SA	SA
FMEA	SA	SA	SA	SA	SA
Fault tree analysis	A	NA	SA	A	A
Event tree analysis	A	SA	A	A	NA
Cause and consequences analysis	A	SA	SA	A	A
Cause and effect analysis	SA	SA	NA	NA	NA
Layer protection analysis	A	SA	A	A	NA
Decision tree	NA	SA	SA	A	A
Human reliability analysis	SA	SA	SA	SA	A
Bow tie analysis	NA	A	SA	SA	A
Reliability centred maintenance	SA	SA	SA	SA	SA
Sneak circuit analysis	A	NA	NA	NA	NA
Markov analysis	A	SA	NA	NA	NA
Monte Carlo simulation	NA	NA	NA	NA	SA
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA
FN curves	A	SA	SA	A	SA
Risk indices	A	SA	SA	A	SA
Consequence/probability matrix	SA	SA	SA	SA	A
Cost/benefit analysis	A	SA	A	A	A
Multi-criteria decision analysis	A	SA	A	SA	A
SA= Strongly applicable **NA=Not applicable** **A=applicable**					

Table 4.1: Risk assessment techniques and their application (ISO 31010:2009)

Risk assessment could be done in different level of detail and using one or more simple / complex methods listed in Table 2.1. The process of evaluation and its results have to be coherent with the risk criteria that has been defined during the establishing of the context.

In general terms, the appropriate techniques have to show the following characteristics:

- The techniques must be justifiable and appropriate to the situation or organization
- The techniques should give results which increase the comprehension of risk nature
- The techniques should be used in order to be traceable, repeatable and verifiable

The choice of a technique for risk evaluation should be based on relevance and suitability of the risk and, moreover, the results of different studies should be comparable. Several applicable factors guarantee the right choice of a technique, though the resources availability, the nature of the information and the complexity of the operations are the most valuable factors. Following is reported a rough explanation about the kind of techniques that are commonly used and are described in ISO 31010.

According with the ISO 31010, the first step is the risk assessment and its phases are:

- Risk identification
- Risk Analysis – Consequences
- Risk Analysis- Probability
- Risk Analysis – Level Risk
- Risk Evaluation

Moreover, the second step is related to the choice of the factors which influence the selection of techniques for the risk assessment. The choice of the methodology is described in terms of:

- The complexity of the problem and the necessary modes for analysing it.
- The nature and level of uncertainty of the risk assessment based on the quantity of available data
- The amount of necessary resources in terms of time, information, costs and level of competence.
- The availability of the technique to provide a quantitative output.

4.5 Risk Assessment

A risk assessment is a systematic process of evaluating the potential risks that can be involved in a projected activity or undertaking. In other words, risk assessment is the overall process for helping to identify, analyse and evaluate the risk. As described in ISO 31010 "*the risk assessment is that of the risk management which provides a structured process that identifies how objectives may be affected and analyses the risk in term of consequences and their probabilities*". The same normative above described wants to outline the importance of the risk assessment as answer to four simple questions:

1. What can happen and why? (risk identification)
2. What are the consequences? (risk analysis)
3. What is the probability of their future occurrence? (risk evaluation)

4. Are there factors that mitigate the consequence or reduce the probability of the risk? (risk treatment)

Moreover, the normative outlines the importance of the tolerability and acceptability of the risk after the treatment, trying to understand if further treatments are required after the mitigation.

4.5.1 Risk Identification

The identification of a risk should identify the sources of the risk, areas of the impacts, actions and all their causes and their potential consequences. The risk identification is the process of defining risks that could theoretically prevent the process, enterprise, or investment from achieving its objectives, by documenting and communicating the concerns. It is possible to create, avoid, reduce, accelerate or delay the accomplishment of objectives that a certain risk caused, by generating a comprehensive overviewing list of risks. Risk identification should include an examination of the knock-on effects of consequences, including cascade and cumulative effects, though a wide range of consequences does not mean that the risk source may be always clear. All causes and consequences should be considered in order to have a clear overhaul of the identified risk.

4.5.2 Risk Analysis

Risk analysis involves developing an understanding of the risk, by providing an input to risk evaluation and for deciding on whether, and how, risks need to be treated. Risk analysis has to involve consideration about the risk causes, their consequences and likelihood and all the other useful attributes for determining a risk. The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. Risk analysis is a subjective investigation of likelihood and severity that might cause divergences of opinion among experts or limitation on modelling should be stated and can be highlighted. Every assumption should be considered in the analysis and communicated affectively to decision makers and other stakeholders.

Risk analysis can be assumed with varying grades of detail, depending on the risk, the purpose of the analysis, and the data, information and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances (ISO 31000). The used tool for the risk analysis is the risk matrix (Figure 1.3) that permits to obtain a rough risk evaluation from the estimated likelihood and severity.

Below is shown a user-friendly layout for a basic, but useful, risk analysis, developed on autumn 2017 in Republic of Ireland by Tosca Human Factor Solutions Ltd.©:

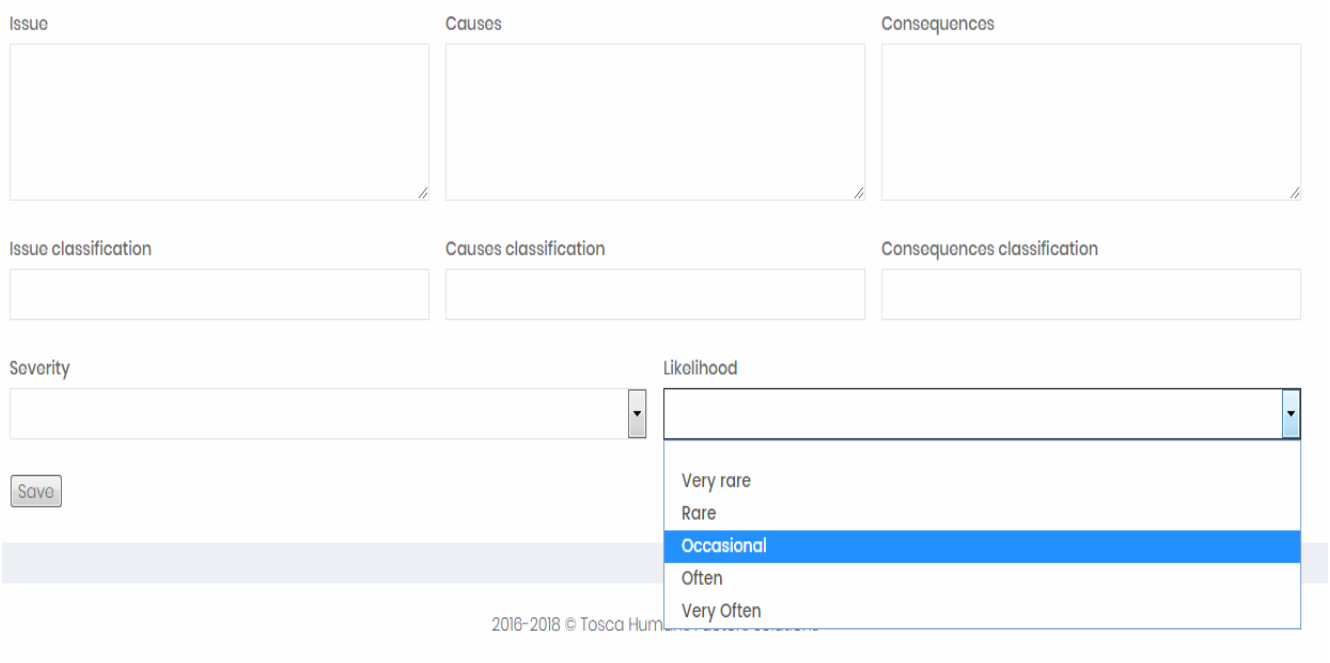

Figure 4.2: Risk assessment developed by Tosca Human Factor Solutions LTD

This very simple interface allows the users to easily classify the risk by inserting in the text field the essential information about the risk to have a fully overview of the situation:

- Issue: description of the hazard
- Causes: description of the cause/s that generated the risk
- Consequences: description of the consequence/s of the risk

First of all, the system asks to insert the procedures and/or the assets where the risk has been found for helping the user and the manager to easily individuate the risk in a complex system as could be a chemical plant or a refinery but also an airport or an hospital.

The required text field for the classification for issue, causes, and classification wants to help the users to easily classify the risk in simply and recognized categories, for example: Human Error, Safety, Environment, Damage, Financial, etc.

Then, after that the risk has been defined, it is necessary to give a qualitative rough evaluation of the risk so, how as it is possible to see in Figure 2.2, the system allows to choose from a drop-down menu the estimated level of severity and the likelihood based on a scale between one and five, where "Very rare" is the event with the lower probability and "Very often" is the one with the higher probability. An equivalent drop-down is also available for the severity. As expected by the theoretical analysis, the risk automatically evaluates by the software after the insertion of the two variables listed above. E.g. the user who chooses a risk with a *"Medium"* severity and an *"Occasional"* likelihood means that it selected both variables with a level of 3/5. So, the system inserts those values inside an incorporate and not viewable risk matrix and it finds that the risk level is 9/25, then it is a risk with a *"Yellow"* status and treatments are required in order to reduce the risk level until *"Green"* status is reached.

4.5.3 Risk Evaluation

Comparing the level of the risk determined during the risk analysis process when the context was considered, it is possible to consider which risk has to been treat based on the determined risk level. So, in other words, the purpose of risk evaluation is to assist making decision, in order to choose which risk needs priority for the treatment. Decisions should consider the context of the risk and embrace consideration of the tolerance of the risks borne by the company or the industries which the risk is linked. Decisions should be made in accordance with legal, regulatory and other requirements (ISO 31000:2009). The decisions to treat a risk are influenced by the organization's risk attitude and the risk criteria that have been established in the previously step of risk management.

4.5.4 Risk Treatment

Risk treatment could be considered the last step of risk assessment, by developing a variety of options for mitigating the risk and implementing actions plans. The choose of the more properly risk treatment means balancing the cost of implementing each action against the benefits resulting. A risk treatment could involve the redesign of existing controls, introduction of new ones or monitoring existing ones. Risk with a lower status may require periodic monitoring while risk with a higher risk status are likely to require more intense management focus. (AS/NZS ISO 31000:2009) By the way, present and planned mitigations for each risk are taken and are classified using the following outline:

1. Avoidance
2. Action to reduce the impact and/or probability of the risk;
3. Transferring the risk;
4. Accepting and monitoring;
5. Sharing

The avoidance is a kind of "hiding" from the hazard by do not practicing a dangerous activity that could be generate a risk. For example, if using an oven could be dangerous, would not using an oven will be a perfect way to avoid the risk. For reduce the risk, on the other hand, it need to implement a strategy that is designed to reduce the likelihood or/and consequence of the risk. For example, if using an oven could be dangerous, wearing protective gloves will reduce the severity that an unpleasant event happened. The transferring means that the risk could be transferred to a third party: the two main types of transfer are insurance and outsourcing. Accept the risk means face the risk without take care of it and do not mind about the possible danger that it means for the company. Usually, it is implausible thinking to earn in business or have a dynamic life without to take on risk. Finally, share a risk means that it can be distributed to multiple organization or persons for several possible reasons, including insurance products and self-insurance strategies.

Choosing the most appropriate risk treatment decision involves balancing the costs and efforts of implementation against the benefits derived and regarded to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. Although the application of a combination of treatment options is more expensive, the companies can usually earn form the adoption of a multiple risk treatment. When the company chooses a treatment option, has to consider the standards and perceptions of stakeholders and

the most proper ways to communicate with them and let they know how a risk treatment can impact. The treatment action plan could evidently recognize the priority order in which individual risk treatments should be implemented. Furthermore, it is important to consider that a significant risk can be the failure or ineffectiveness of the risk treatment measures that has been previously taken. Monitoring the risk treatment needs to be an important part of the action plan to give guarantee that the actions remain operative in a significant period of time. Risk treatment could also introduce secondary risks that need to be assessed, treated, monitored and reviewed and those risks have to be incorporated into the same treatment plan as the original risk and not treated as a new risk.

4.5.5 Monitoring and Reviewing

Monitoring and reviewing should be a planned part of the risk management process that involve regular inspection or surveillance performed periodically or *ad hoc*. Responsibilities for monitoring and review should be clearly defined. The are several purposes for the monitoring and review process: first of all, it need to ensure that controls are effective and efficient in both the phase of design and operations. Moreover, it is necessary obtaining additional information to improve risk assessment by considering and analysing events, variations, tendencies, successes and fails which happened in the past. Finally, the identification of new emerging risks and the detection of changes in the external and internal context, represent one of the most important aim of the process. A periodic review of the effectiveness of the risk treatment process is necessary in order to ensure a continuous improvement of risk management in the firm, so a progress implement of risk treatment plans provides a performance measure.

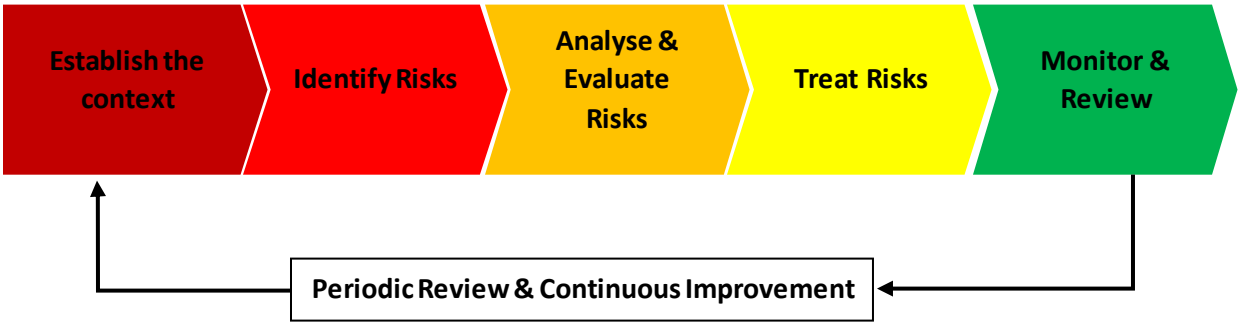

Figure 4.3: Risk management process

5. The use of Risk Registers in the literature

5.1 Risk Register: definition and features

In literature has several applications of risk register in modern industries have been described: automotive, chemical, pharmaceutical and also in the field of construction project and transport system. The risk register is a tool which helps companies to deal effectively with the management of risk (Webb, 2003). According to Webb in his publication titled "The Project Manager's Guide to Handling Risk" a risk register is described as: *"The most popular method of recording and ordering risks [...] specifying all perceived risks with the outcomes, likelihoods and countering strategies"*. In another book, published by (Reiss, 2007) and titled "Project Management Demystified", the author states *"A risk register can [...] discuss at length the nature of the risk, the impact and the things that can be done to prevent or reduce the impact of the risks"*. From the literature above, it becomes apparent that the risk register is an effective tool that contributes towards project risk management. Moreover, Reiss (2007) mentions that one of the most important features of a risk register is to ascertain the impact of each risk.

Furthermore, (Baccarini & Archer, 2001) state in their paper how project risk management literature *"describes the need to rank and prioritise risks in a project"* and this statement is confirmed and developed by (Lambert, 2001) in their paper, where they note that *"prioritize sources of risk in terms of the likelihood of occurrence, the potential consequences to the program, and the efficacy and immediacy of risk-reduction efforts"*. Although those factors correspond with the five principles also described by Webb (2003), (Patterson & Neailey, 2002) reiterate these points in their paper by describing the risk register as "*A formal mechanism to document the identified risks, their associated probability and impact values as well as their ranking in the project"*.

As suggested by the literature above, the risk register is a highly effective tool designed to monitor, review and reduce risks that contains all the information about hazards, procedures and assets. Risk register itself is a useful and effective instrument to enable everyone involved in the project to consciously evaluate and manage the risks as the part of the decision-making project (Patterson & Neailey, 2002). The risk register consists of three entities: the register of the risks itself, which is the main focus of the system, and two supporting documents, to include information of the risk owner and the risk reduction and/or mitigation plans. It is currently and widely used by several types of industries and organizations, as well as high hazard industries such as oil and gas (Hasle, Kjellen, & Haugerud, 2009) and electricity generation. The purposes are either to support safe processes and efficient project management. The presence of suggestion of mitigations in order to maintain safe operation or estimations about the future exposure of the risk, represent also a key role in a well-designed risk register. The risk register is used as a formal method of identifying, quantifying and categorising the risks, as well as

providing the means of developing a cost-effective method of controlling them (Bruce, Hancock, Morin, & Carter, 1996). There are different crucial components that are necessary to manage the risk in an easily understanding layout in every kind of risk register. Those components are fundamental to permit who does not have confidence with the risk, to have a rough knowledge of the problem.

It necessary that a risk register has:

- **Risk ID**: Unique identification number for each risk
- **Risk Description**: A brief description or title for the risk, to make it easy to discuss
- **Risk Ranking**: A quantification of the risk, based on severity and likelihood rated on an integer scale
- **Owner**: The person responsible for managing the risk
- **Actions**: List of actions to mitigate and treat the risk
- **Dates**: The date of any action regarded to the risk

Furthermore, there are several useful information that the risk register should have: for example, the presence of a current/future risk status, risk type (safety, financial, reputational, environmental, etc.), assets involved in the risky situation, hazards related to the risks or mitigations that are already in place from previously analysis. Moreover, it is important to remind that the main aim of a risk register is to be used as risk management tool and to fulfil regulatory compliance acting as a source for all risks identified. (Balfe, Leva, Mc.Aleer, & Rocke, 2014)

In this work has been analysed and described the results of a case study in which a risk register was established in an electricity generation company across its multiple stations in the Republic of Ireland. Research conducted by the Bristol University found that 78% of Risk Register computer systems were developed in-house (Crossland, McMahon, & Williams, 2001). Risk registers in-house result in the systems being applicable to the need and requirements of the type and form of risk management A majority of the computer-based risk registers were, however, developed within the individual organisations, giving rise to the conclusion that each organisation made their own decisions on the style and design of their individual ‘risk register’.

PARTE II

CASE STUDY AND RESULTS

6. Power utilities in generation and the need to use risk register for option evaluation

6.1 The power generation company

The power generation company evaluated in the case study is one of the main electricity generation and networking system in the Republic of Ireland. The generation company operates across the electricity market: from generation, through transmission and distribution so supply. Moreover, the company extracts further value at certain points along this chain: supplying gas, using their networks to carry fibre for telecommunications, developing electric vehicle public charging infrastructure and more.

The power generation company is actually composed of several different, distinct and legally defined companies which the principal ones are:

- The section related to the networking that is the holder of all the functions related to the electricity distribution system in Republic of Ireland.

- The section related to Generation and Wholesale Markets that develops, operates and trades electricity generation assets. It competes on the global wholesale energy trading market in electricity, gas and coal. The generation assets operate across Republic of Ireland and UK includes 9 hydro stations, 10 thermal stations and 18 wind farms

- Another section is the retail division of the company, it supplies electricity, gas and energy services to over 1.2 million households and 95 thousand businesses across Ireland and Great Britain

- The company is also a leading global engineering consultancy specialising in the utility sector.

6.2 GRR (Generic Risk Register)

GRR is the actual risk register used by the company and it is currently based on a Microsoft SharePoint spreadsheet that is often downloaded as an excel spreadsheet. Although the GRR presents all the features required as a well-designed risk register, it is disorganized and difficult to read for someone that has never worked with it before. For simplicity each risk is detailed in one complete record including categorisation, pre- and post- mitigation scoring and current and

planned mitigation action. The system serves also to highlight the shortcomings of the risk register concept, particularly in relation to develop a solution better able to handle knowledge management capabilities for the following aspects (Leva, Balfe, Mc.Aleer, & Rocke, 2017):

1. Aggregation of risks from station level to central level
2. Support controls over mitigation measures at station and central level
3. Support better data-based estimated for the probability of situations based on accident data;
4. Incorporation with company critical asset register (CAR)
5. Support a better link with workflow around risk communication
6. A possible link with day to day operational practise

The rating scheme of the risks based on the risk matrix is currently used for the purpose of sorting and screening. The risk register needs to include a further criterion to estimate corresponding classes of monetised risk values to be able to aggregate risks that are in common across multiple stations with different likelihood and exposure in the various impact categories.

Moreover, with the passing of the years, several options have need added in order to improve continuously the efficiency and the amount of information that the risk register can provide. In addition to the evaluation of the risk, by analysing likelihood and severity, another fundamental part in the GRR is the Monetized Risk Impact for five different areas of work:

- Financial
- Safety
- Reputational
- Technical
- Environmental

The estimation of the Monetised Impact for the different sections listed above is based on an integer scale from one to five, by associating to each number a monetised value (in €), as it is shown in Table 6.1 below.

Rating	*Financial [€]*	*Safety [€]*	*Reputational [€]*	*Technical [€]*	*Environmental [€]*
1	< 100 k	< 10 k	< 10 k	< 100 k	< 10 k
2	< 1 M	< 250 k	< 250 k	< 1 M	< 250 k
3	< 10 M	< 1 M	< 1 M	< 10 M	< 1 M
4	< 50 M	< 10 M	< 10 M	< 50 M	< 10 M
5	> 50 M	> 10 M	> 10 M	> 50 M	> 10 M

Table 6.1: Monetised equivalence of the impact categories and levels

Moreover, the likelihood that a certain monetised risk exposure happens is based on the same integer scale from one to five, by associating to each number a certain probability that the unpleasant event happens, as it is shown in Table 6.3

Rating	*Name*	*Likelihood per year*	*Mean value of range considered*
1	Unlikely	< 0,001 %	Mean value: 0,0055%
2	Remote	0,01 % - 0,1 %	Mean value: 0,055%
3	Possible	0,1 % - 1 %	Mean value: 0, 55%
4	Probable	1 % - 10 %	Mean value: 5,5%
5	Frequent	> 10 %	Mean value: 55%

Table 6.2: Range of the likelihood in the GRR

So, as it is usual for calculating a risk, also for calculating the total monetised risk exposure, it is necessary do the sum of the products between the likelihood and the impact of each kind of risk.

Below is shown a practical example of the calculation of the total monetised risk exposure.

ID RISK	*Financial*	*Safety*	*Reputational*	*Technical*	*Environmental*	*Probability*
157	4	2	1	2	1	3

Table 6.3: Example of a risk reported in the GRR

By using both Table 4.1 and Table 4.2, it is possible to compare the integer scale numbers in the economic value in order to calculate the value of the monetised risk exposure, so:

$$Probability\ x \sum Monetised\ Risk\ Impact \tag{13}$$

So:

$$0{,}0055\ x\ (20000000 + 150000 + 10000 + 450000 + 10000) = 113410€$$

This value assesses a risk not merely from a risk assessment point of view, by giving a value related to a "coloured status", but also by giving a tangible and economic explanation of the risk.

Risk Centre	*Current Exposure*	*Monetised Risk Exposure*
Station 1	20	100375000
Station 2	20	17242500
Station 3	20	17165500
Station 4	15	10037500
Station 5	15	5062585
Station 1	15	4984155
Station 6	15	4977665
Station 7	15	3575000
Station 8	15	2794000
Station 9	15	2794000
Station 10	10	2475000
Station 5	16	2201650
Station 1	16	2201650
Station 1	10	1490582,5
Station 2	16	1376650

Table 6.4: Risk Level and Monetised Risk Exposure across the stations

The risk register used by the power generation company, besides all the several features required from a risk register, presents additional requirement related to the future status, future exposure, future mitigation and future impact/likelihood for the monetised risk exposure.

The prevision of a future exposure may be convenient to better understand if the investment actuated to reduce the risk has been efficient. Anyway, the estimation of the future exposure should not be taken as a reliable value, but it has to be considered as a goal for the future.

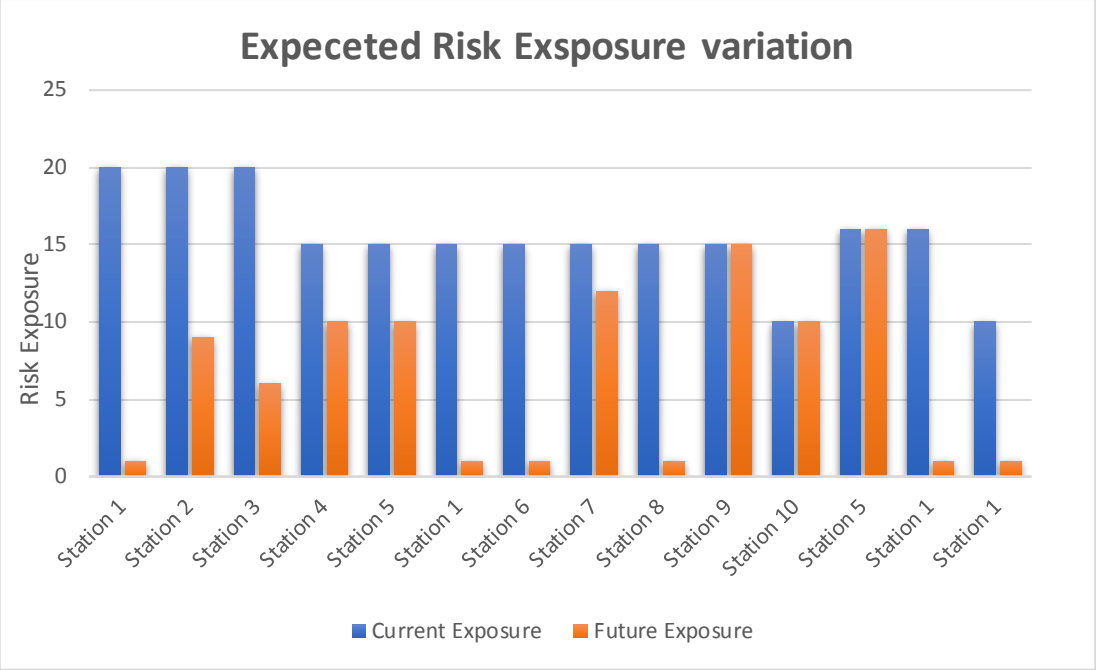

Figure 6.1: Existimation of the exposure across the station according with the GRR

Moreover, results necessary recognize the assets involved in the risk and specifically, the affected units of the plant in order to find involved equipment and a faster solution. The example in Table 6.5, provides better understanding the importance of indicating the assets where the risk has been reported.

Assets	Red	Orange	Yellow	Green	Total
Organisational conditions	€ 121.192.500	€ 2.865.005	€ 305.437	€ 8.877	€ 124.371.819
External safety	€ 27.203.000	€ 3.374.250	€ 121.907	€ 127.209	€ 30.826.366
Gas turbine	€ 10.040.250	€ 1.283.205	€ 209.544,5	€ 373	€ 11.533.373
Finance	€ 5.507.700	€ 3.816.945	€ 829.257	€ 8.944	€ 10.162.846
Internal standards and procedures	€ 4.950.660	€ 742.830	€ 288.024	€ 45.228	€ 6.026.742
Switchgear	€ 4.984.155	€ 118.250	€ 160.490	€ 311	€ 5.263.206
C&I	€ 2.227.500	€ 2.470.380	€ 72.798	€ 563	€ 4.771.241
Process safety	€ 0,00	€ 4.395.435	€ 171.292	€ 45.172	€ 4.611.899
Generator	€ 478.500	€ 2.733.208	€ 115.615	€ 401	€ 3.327.725
Steam turbine	€ 2.794.000	€ 468.490	€ 0,00	€ 353	€ 3.262.843
Transformers	€ 2.794.000	€ 229.020	€ 157.943	€ 165	€ 3.181.129

Table 6.5: Monetised risk exposure for some assets by dividing per risk level

Although the monetised risk exposure results are very useful to recognize which risky situation causes relevant economic loss, other significant information that the GRR could report are the

hazards, risk symbol/title, affected units, consequences and root causes types. The combination of the categories listed above, linked to the monetised risk exposure, may give a plenty overhaul of all the risk that has been reported in the GRR.

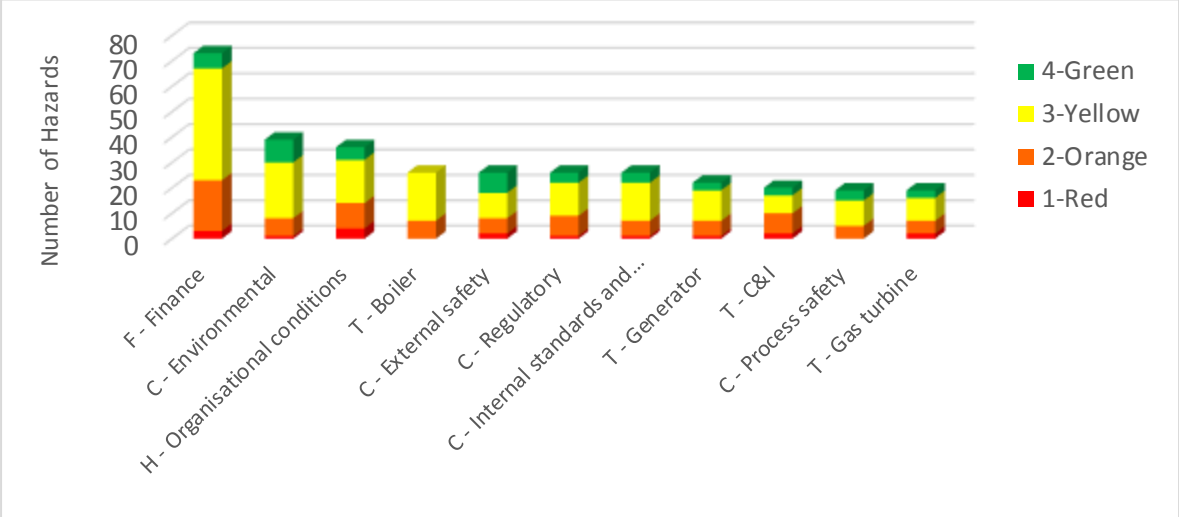

Figure 6.2: Assets vs number of hazards

In Figure 6.2, is shown a top ten league of assets ordered by number of hazards. By comparing Table 6.5 with Figure 6.2, it is possible to notice that despite its highest monetised risk exposure H-Organisational Condition has low number of hazards.

Furthermore, a quarterly upgrade of the GRR can be particularly useful in order to recognize how the intervention for reducing the risks is working or not. Table 6.6 below shows the behaviours of the monetised risk exposure for the different stations across the country.

Risk Centre	Jan 2017	Apr 2018	Diff (%)
Station 1	64586260	113223795,9	43,0%
Station 2	1146629	19313305	94,1%
Station 3	173910,9	21246860,6	99,2%
Station 4	1981976,7	9167472,5	78,4%
Station 5	10873848,5	6864230,5	-36,9%
Station 6	170951	5148715	96,7%
Station 7	1720378	4676933,3	63,2%
Station 8	215337,3	5389287,8	96,0%
Station 9	2892760,9	3060554,3	5,5%
Station 10	3049860	1133968	-62,8%
Station 11	971850	3601576	73,0%
Station 12	1243757,5	10302340	87,9%
Station 13	6361850	1391986,7	-78,1%
Station 14	312471,5	584155	46,5%
Station 15	4461423,4	2469568,6	-44,6%
Station 16	177215,3	864302,8	79,5%
Station 17	406919,7	1173289,7	65,3%
Station 18	2066143,6	881204,4	-57,4%
Total	102813543,3	210493546,1	51,2%

Table 6.6: Comparison of the monetised risk exposure in two different years.

As shown in the table above, just a few stations present a strong decrease in their monetised risk exposure. On the other hand, the relevant increases of other stations are not necessarily related to the increase of the risk itself, but it could be related to a better reporting system or periodic expense.

GRR is continuously being developed in order to have a clear report of the situation in the stations, by adding new features and taking more care of details. In Table 6.7 below, even though the total amount of the hazard increases, it is possible to appreciate how the uncertainty about collocating some risk has been overcome. In fact, although in 2017 the total amount of "Unknown" consequences was twenty-six, in 2018 it has been registered only one unknown consequence. This clarification has been due to a better definition of the risk during the reporting phase.

Consequences	2017	2018	Diff
Health & safety hazard	53	70	↑
Reduced income	64	64	→
Damage to asset	39	58	↑
Unavailability of asset - short term	45	54	↗
Increased investment	7	36	↑
Catastrophic failure	22	31	↗
Unavailability of asset - long term	34	29	↘
Increased running costs	16	29	↗
Reduced output	21	22	→
Legal action	10	22	↗
Asset loss	7	15	↗
Environmental discharge	8	15	↗
Contained failure	9	10	→
Project delays	8	7	↘
_Unknown	26	1	↓
Total	**369**	**463**	↑

Table 6.7: Comparison between the reporting of the number of hazards in 2017 and in 2018

The risk management process around the GRR consists of three main sections:

1. Monthly Risk Update – at station level;
2. Quarterly Risk Validation – involving both station level and organisation level risk specialists,
3. Quarterly Risk Reporting – at organisation and senior management level – involving risk reporting managers and members of the senior management team

Several KPIs (Key Performance Indicators) have been identified to monitor the use and content of the risk registers as reported in Table 6.8 below:

No.	Key Performance Indicator	Frequency
1	Percentage of Risk Updated within Last 90 days	Monthly
2	Average Mitigation Effectiveness (Self-Assessed)	Monthly
3	Mitigation/Control Measures in place and functioning	Quarterly
4	Number of red and amber risks	Monthly
5	Number of open risks	Monthly

Table 6.8: KPIs in the GRR

6.3 CAR (Critical Asset Register): risks related to physical equipment and their reliability

According to ISO 55001-2014 "*A component or system in the company is defined as Safety Critical if its function is to prevent an abnormal escalating into a major incident*" (ISO 55001, 2014). It is possible to define a major incident as an occurrence resulted from uncontrolled developments in the course of the processes of the plant, that involve serious danger to the environment, equipment or personnel, either inside or outside the station. Initially the company adopted the industry standard PAS 55 released by the Institute of Asset Management and published by BSI (British Standards Institute) in 2004, it was aimed at guaranteeing the best practice in terms of safety and efficient asset management, by providing guidance across different aspects throughout the lifecycle strategy to everyday maintenance. Then the company had a natural transition to an international standard as ISO 55001 to cover management of physical assets. The Irish power generation company is currently using a common structured spreadsheet as a critical asset register (CAR) for all stations, held in a spreadsheet format stored in an integrated on-line shared location. The tool reported above gives the user the minimum mandatory information for each station and calculates a risk rating, but without detailing the failure modes and their consequences upon which the risk rating is based. Failure mode and consequences are actually information coming from GRR. The CAR can cover all the requirements to serve the purpose of asset risk register for the company and for each station considering the technical asset risks. The necessity to move the currently CAR toward a web-based tool trying to find a management IT solution can be considered a module of the risk register. It is a natural step for the development of a complete system.

6.4 The need to use a risk register for option evaluation

The necessity to better organizing under the same system of the GRR and CAR comes from the needing of the power generation company to find a solution for their option investment evaluation. Several key points for the evaluation and validation are required at the risk register:

- How well the data structure supports the identification and categorisation of risks;
- How the assessment outline is used to manage and prioritise risks;
- The attitude of the stations to use the final tool, including disposition to fill data;
- The apparent effectiveness and efficiency of the tool across the different stakeholders;
- Valuation against the high-level necessities

It is also important for the feedback of the stakeholders. It can be achieved in two possible ways: through a review answered by a sample of the main asset experts in each station who are in charge of reporting towards the generation risk register and by the feedbacks collected in the annual risk review workshop held in each station.

For asset-intensive organization, as the Irish power generation company, the use of asset investment planning processes is a fundamental requirement per either prioritisation and optimisation.

The option evaluation requested from the power generation company has to analyse either the investment and the monetised risk exposures that the company has to afford throughout the years. First of all, the risk profile has to be analysed in order to better understand where the risky situation has a higher severity between the five categories of impact: Technical, Financial, Safety, Environmental and Reputational. This kind of analysis has to be done for all the estimated life of the plant (e.g. ten years) and then it will be possible to evaluate that the risk rating will increase progressively during the years if investment to reduce the risk will be not done. Then, the option evaluation is aimed at comparing the different option of investment that is possible to afford in the plant when it will be required. There are two different kind of investment that the power generation company uses to report:

- Downtime cost;
- CAPEX

It is also possible to add other costs as NDT (No Destructive Testing)

Downtime cost is referred to the period during which an equipment or machines is not functional or cannot work. It can be due to technical failure, machine adjustment, maintenance, or non-availability. So, the average downtime cost is usually built into the price of goods produced, to recover its cost from the sales revenue. CAPEX (Capital Expenditure) is the money a company spends to acquire or upgrade productive assets in order to increase the capacity or efficiency for more than one accounting period.

The evaluation of the best investment option has to compare the monetised risk exposure, adding potential other benefit (e.g. reselling the used asset when the new one has been bought), with the Net Present Value. The NPV is the difference between the present value of cash inflows and cash outflows over a period of time. In other words, it is possible to describe the NPV as the measure of the investment's return. The formula for calculating the NPV is:

$$NPV\ (i,N) = \sum_{t=0}^{N} \frac{R_t}{(1+i)^t} \tag{14}$$

, where:

- R_t is the cash flow at the time t
- i is the return rate, that is the profit earned from the investment (for the case study of the power generation company a return rate of 8,4% is use)
- t is the time of the cash flow.

Therefore, the comparison between the total monetised risk exposure with benefits and the NPV cost can evaluate which option should be the best one. The option with the higher Evaluation Index will be the best compromise between monetised risk exposure and investment.

$$Evaluationi\ index = \frac{\sum_{t=0}^{N}(NPV + benefit)}{\sum_{t=0}^{N} NPV} \tag{15}$$

In literature, there is a lack of documented evidence of the tangible benefits of advanced asset management techniques (Tamimi, Beullens, & Sadnicki, 2016). In their paper, they want to outline the importance of using mathematical optimisation in order to obtain prioritisation results for achieving higher value outcomes.

In Table 6.9 below are shown five different options of investment for a period of 10 years with their own evaluation index:

Profile/Option	*NPV cost*	*NPV with benefits*	*Evaluation Index*
Risk Profile	-	€ 79.336.752	-
Option 1	€2.108.222	€ 47.475.450	**22,52**
Option 2	€4.711.586	€ 41.885.628	**8,89**
Option 3	€11.084.904	€ 45.270.775	**4,08**
Option 4	€7.463.701	€ 42.853.385	**5,74**
Option 5	€4.531.228	€ 44.058.350	**9,72**

Table 6.9: Option evaluation example

7. Tosca Solutions and the development of a prototype for the selected case study

7.1 Tosca Human Factors Solutions LTD

Tosca Solutions is campus company based in Trinity College Dublin to offer support for implementing risk management tools customised specifically to the need of highly regulated environment.

Tosca provide solutions to optimize core operations for safety critical activity to achieve higher efficiency, productivity and total safety management. Tosca furnish this solution with the use of specific methods and tools developed internally. As a result, the solution is sustainable for the client as mentoring and training on the methods and tools will enable the clients to support the continuous development process internally.

Tosca Solutions is aimed at:

- Offering an effective way to take control, and support compliance in a complex environment for total safety
- Focusing on critical activities. Helping to improve enhance the key activities, engaging operators on actual efficiency and safety improvements.
- Adding value on training and optimizations.

The risk register consists of a set of specific areas that can be combined to offer a one stop shop for managers to address the issue of monitoring and reviewing operational safety and quality on core tasks for the business, all those in real time. This simple tool enables users to have a list of all tasks and assets identify the critical activities and assess risks. Then, the tool provides parameters to coordinate the execution and completion of effective plans and strategies to mitigate the issues, in which the appropriate employees will be involved for each intervention. At the same time, the software furnishes a method to monitor the effectiveness of these possible countermeasures and safety barriers besides the monitoring of performance evaluation. And therefore, the software guarantees corporate compliance, as well as legal and other requirements. One of the main goal of the risk register is to support an organization to stay in line with ISO 45001, ISO 9001, ISO 14000, and ISO 31000.

7.2 Tosca's Risk Register

The Risk Register (RR) is a web tool capable of helping any organization interested in achieving of ISO 45001 certification, (for a first certification) or recertification of ISO 9100, ISO 14001 or simply to have a better risk management and maintain corporate revenues. The main benefits of risk register that Tosca provide are:

- Have an operations and assets register to perfectly understand of what is happening and how is risky each activity.
- Provide an overview of all the main risk associated to a company operation.
- Identify, assess and quickly mitigate of different kind of risks that could affect the objectives of the organization.
- Timely identification and mitigation of risks.
- Aligning risk with internal and external norms
- Financial control
- Carry out continuous monitoring and reporting of risk within the organization, effectiveness of preventive actions and a performance evaluation.
- Control of documented information for a continual improvement process

Tosca's RR can be used as based one stop shop to cover all the different aspects needed in highly regulated environments: risk assessment activities, monitoring of day-to-day performance, reporting testing of possible changes, and management of assets. The RR of Tosca Solutions is a web application capable of reporting events and anomalies in real time, ensuring constant monitoring of business processes and faster and more effective information delivery to competent offices. Furthermore, Tosca's Risk Register is an easy-to-use software for non-experts and people without specialist education or extensive training and it can integrate with existing planning methods and management software.

7.2.1 Dashboard

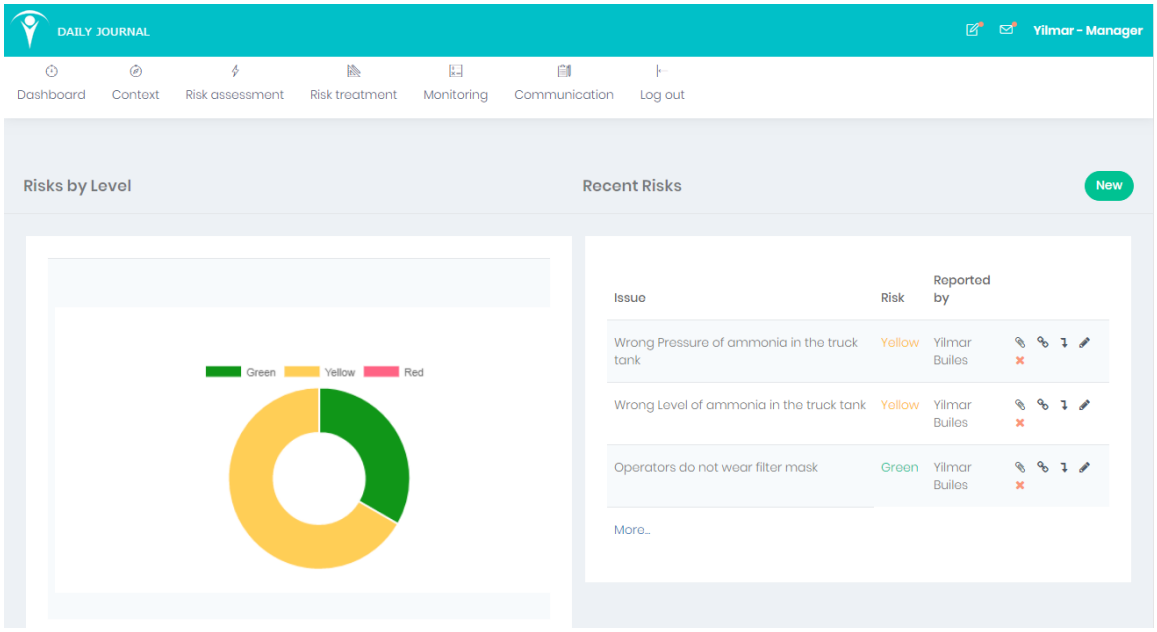

Figure 7.1: Dashboard Example in Tosca's Risk Register

The *Dashboard* gives an overview of the situation described in the Risk Register. In the main chart, a ring graph shows the distribution of the risk by their own level. Other sections of the dashboard can have an overhaul of the recent risks and recent action plans to be modified and edited eventually. In the example of Figure 7.1 the graph and the recent risks are referred to three risks reported in a real case of study about an ammonia plant.

Moreover, in the Dashboard, other features of the Risk Register are briefly shown:

- DORs
- Handover notes
- Anomalies

Daily Operation Reports are instruments used to summarize the status of a project or operations by reporting daily/weekly/monthly goals that must been achieved in order to appraise the performance and the safety of the workplace. Checking valves, replace safety system, checking temperatures or pressures are examples of DORs.

Handover notes, like anomalies, is a tool of the "*Communication"* module in the Risk Register. Shift Handover is referred to a process that involve the passing and acceptance of responsibility for some or all aspects of the work, and the sharing of relevant information for the continuity care of the work. Shift Handover takes place between oncoming and outgoing staff when there is a shift change and it is influenced by organisational factors, including the design of the coverage schedule and organizational culture (Randell, Wilson, & Woodward, 2011). This feature of the tool effectively supports performance appraisal and feedback for the workers. (Leva & Builes, The benefits of task and cognitive workload support for operators in grund handling, 2017)

Anomalies is a tool aimed at communicating irregularities and issues that has been noted in the workplace. An example of anomalies is reported in Figure 7.2

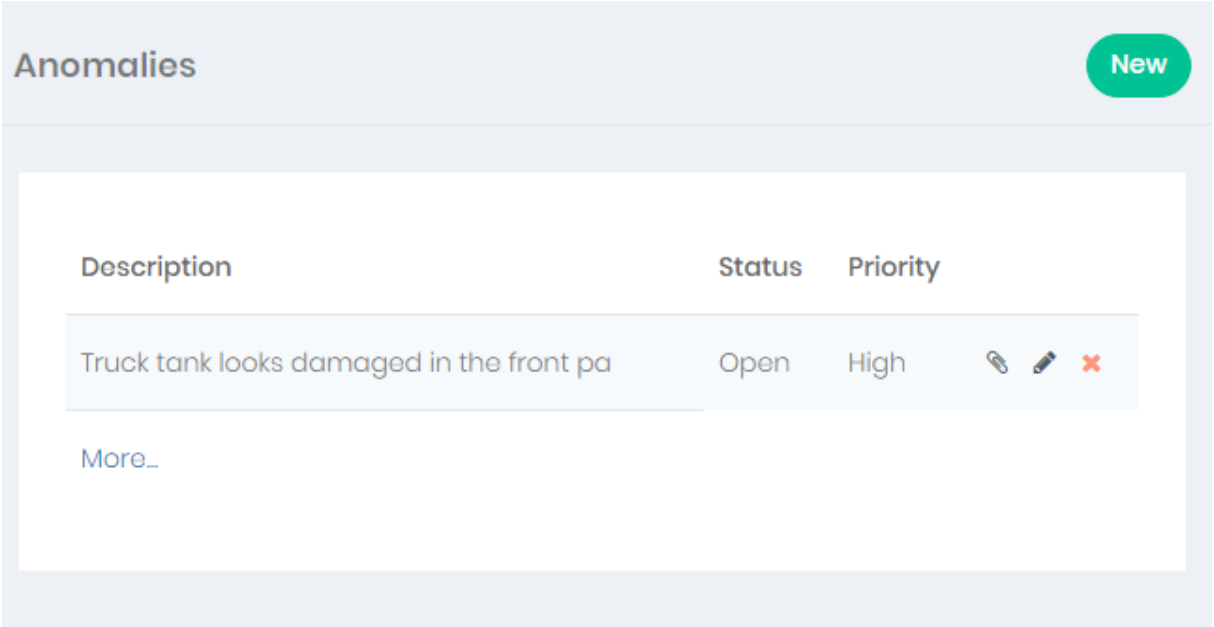

Figure 7.2: Anomalies Example in Tosca's Risk Register

7.2.2 Context

The *Context* module represents the starting point for the description of the work, the procedures and the aim of the company. *Context* is divided in three sections:

- Macro Procedures

- Assets
- Objective Areas

MacroProcedures defines the group of main processes that are performed in the plant/company. *MacroProcedures* could be considered as the "father element" in a procedures tree grown from it. In this work only *MacroProcedures* section will be analysed, because it is the most relevant section.

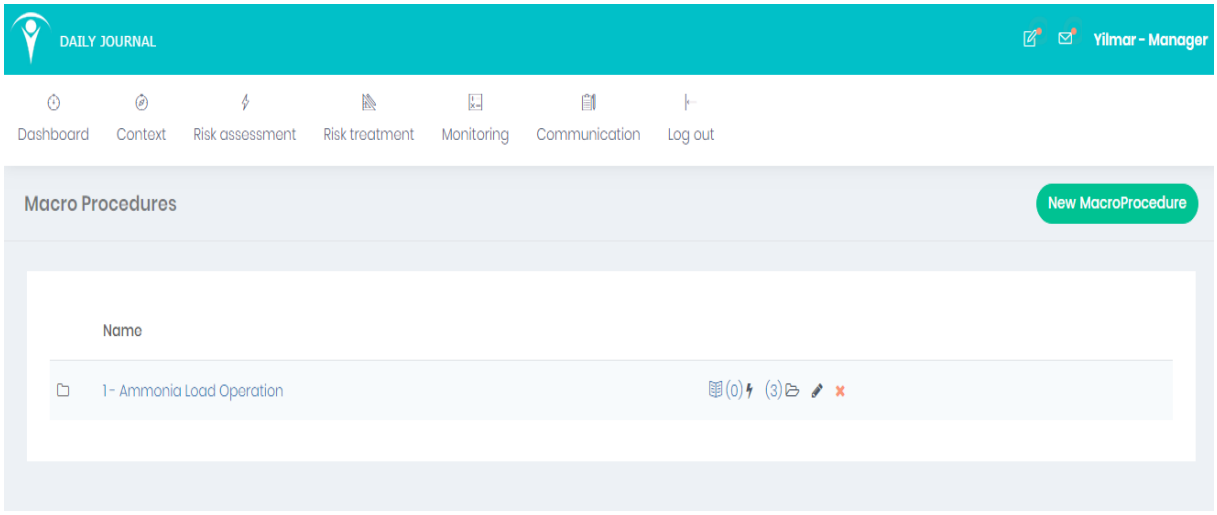

Figure 7.3: Macroprocedures section in Tosca's Risk Register

In Figure 7.3 is reported an example of *MacroProcedure* for a chemical plant in the phase of download/load of ammonia from/to a truck tank. It is possible to recognize some useful elements:

- The Identification numbers (located in the left side)
- The name of the *MacroProcedure (*located in the middle)
- The fast button for inserting (if it is necessary) any reports or risks
- In brackets, the number of reports and risks related in that *MacroProcedure*
- The possibility to open, edit and delete the *MacroProcedure*

By opening the selected *MacroProcedure* the tool shows the set of *Procedures* that compose the whole *MacroProcedure.* It is possible to find in Figure 7.4 below the same elements described above for the overview of every single procedure.

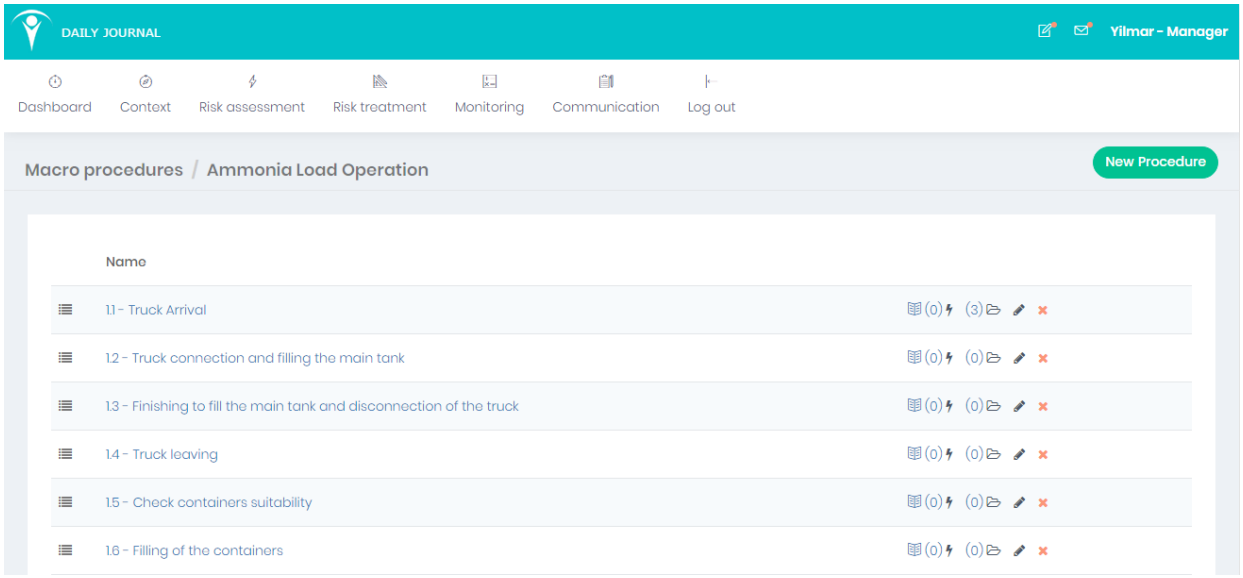

Figure 7.4: Procedure section in Tosca's Risk Register

By opening the first *Procedure* named *1.1 Truck Arrival,* the system brings the user directly to the set of tasks for the selected *Procedure.* In addition to the elements on the right that are present also in the previously section of *Procedures* and *MacroProcedures*. In this section it is possible to order the tasks by using up or down arrows. Moreover, it is possible to say that *Procedure* and *MacroProcedures* are aggregated forms of the system, i.e. a kind of roll-up. In Figure 7.5, that represent the lower level of detail of the system, it is possible figure out in which task of the process the risks have been reported.

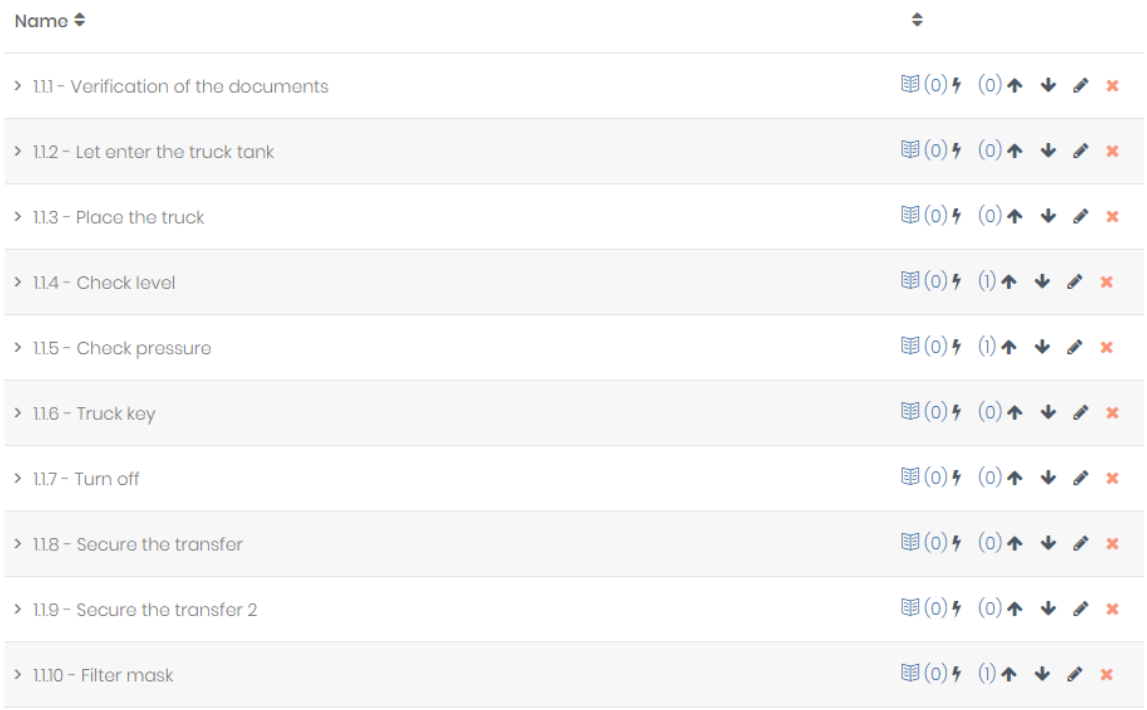

Figure 7.5: Overview of the Tasks section in Tosca's Risk register

Clicking on the little bolt on the right (the button for adding new risks) the tool will open a new page interface that permits the users to add a new risk or visualize the existing one. For example, by selecting the task named *1.1.5 Check pressure*, the system will show to the operator the existing risks and it will permit to insert a new risk by using the button *New* as shown in Figure 7.6. The overview of the existing risk informs the user about the risk rating, the owner of the risk and the *Issue*, namely the reporting risk. If the user decided to insert a new risk, the interface after the selection of the button *New* is reported in this work in Chapter 4 - Figure 4.2.

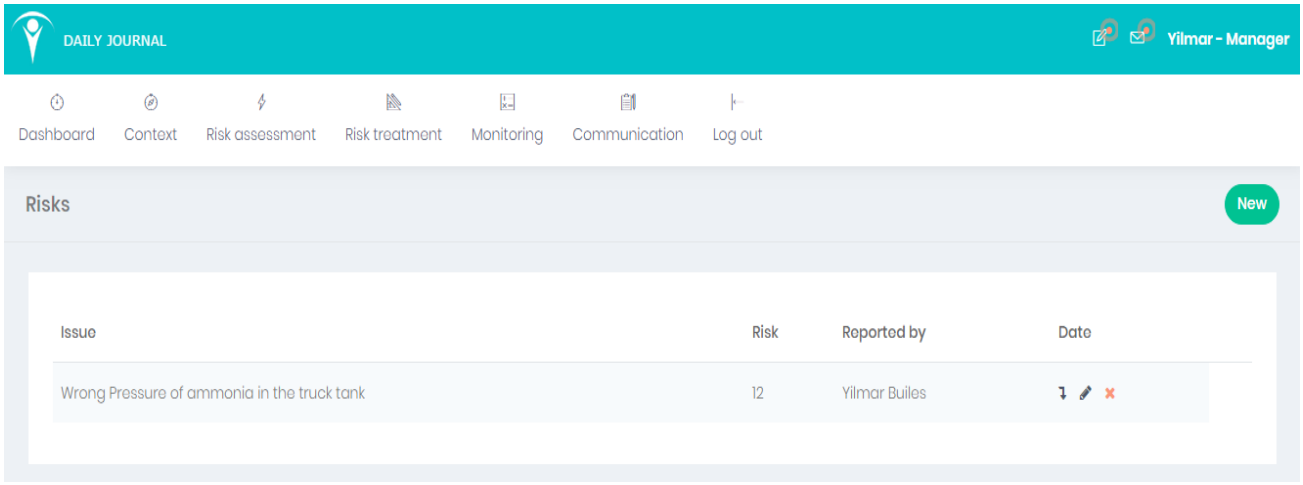

Figure 7.6: Visualization of the risks for a single task and the possibility to add a new risk

7.2.3 Risk Assessment

The full list of the risk present in the system and reported in the tool is in the main section, named *Risk Assessment*. As showed in Figure 7.7, in this module of the tool, it is possible to visualize a rough description of the risks, with their risk level, owner and linked treatment. The buttons on the right permit the users to:

- Open a *Workbook*, which contained several information about the risk, such as files or messages left by the owner;
- Link the risk to an existing risk treatment or create a new one in order to mitigate the risk;
- Check the detail of the risk, by visualizing consequences, causes, severity, likelihood, etc;
- Edit the risk, by modifying the previous description of the risk that was presented.
- Delete the risk

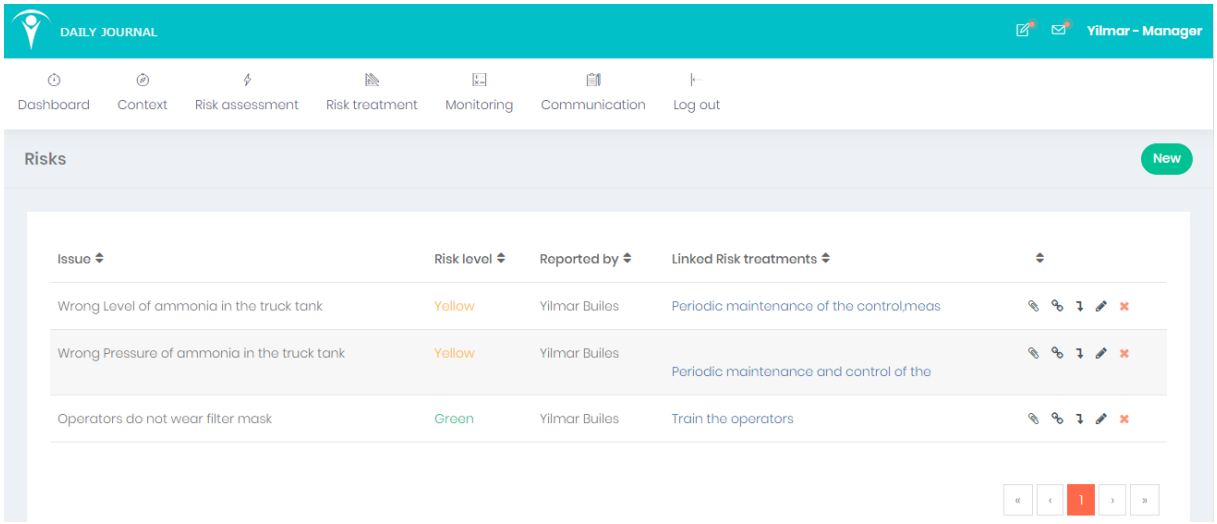

Figure 7.7: Risk Assessment Overview

7.2.4 Risk Treatment

As written above, every risk is (and has to be) linked to a risk treatment, where the Tosca Risk Register has another section, called Risk treatment. A risk could be linked to different treatments and each treatment could be shared between different risks. In Figure 7.8 below, is shown the module of Risk Treatment. In this module, new useful elements have been inserted such as the advancement of the action plan for mitigating the risks and the date when the risk treatment started. Furthermore, it is possible to visualize the related risk and this module also presents the *Workbook* for more information about the risk. The advancement of the risk treatment is calculated automatically by the tool analysing the tasks of a "*To do List*" that the user has to add in the section *Workbook*. Every task passes through three different status: *open*, *in progress* and *close*. The users in *Workbook* can also display messages and files that has been upload in relation with the risk.

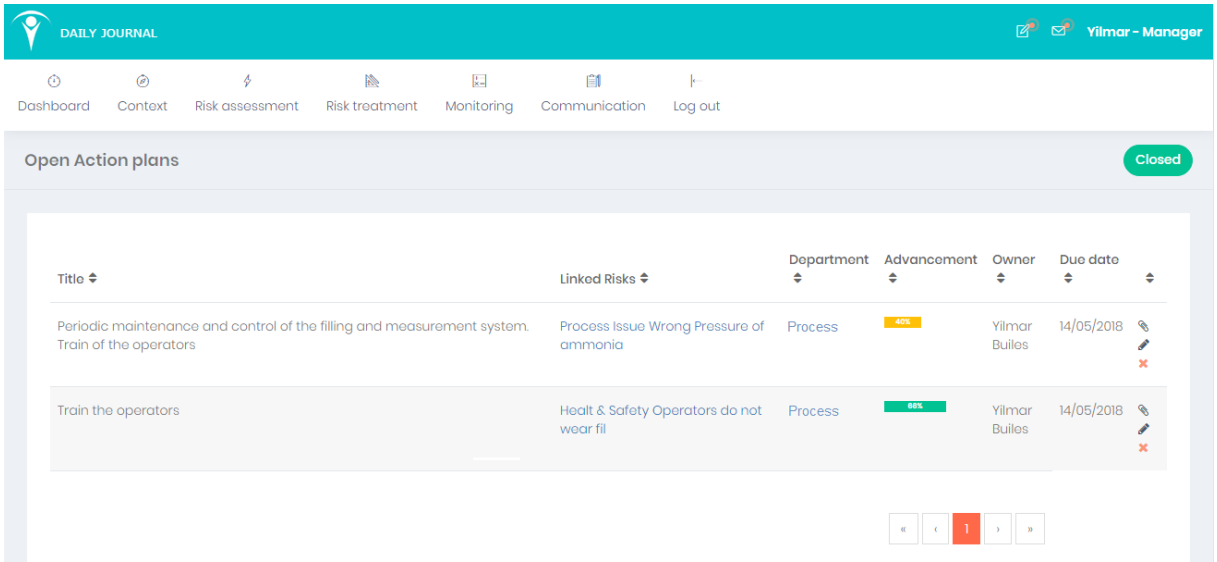

Figure 7.8: Risk Treatment Overview

When the *Advancement* bar is complete, the user can close definitely the risk treatment. In that case, the Risk Treatment will be moved to another section where all the closed risk treatments

are saved. When a risk treatment is closed, the users will receive a massage and a notification for informing that someone (logged in the risk register) has closed a risk treatment. In that case, the risk will be assessed again, and the user will see the new risk level and discover that the risk has been mitigated.

7.2.5 Monitoring

Monitoring is the section for reviewing the risk and all the concerned features and tools. The monitoring section is constituted from five different modules:

- Reports
- Audits
- Surveys
- DORs
- Risk Charts

The *Reports* module is aimed at reporting risky situations that are not properly classified as a risk. That means the user interface is the same of Figure 7.8 but without the categorization of the likelihood and the severity. In this case the system in the section of reporting permits the user to add eventual mitigations on recommendations considering that it is not planned to have a treatment module for the report. The scope of *Audits* module is to help the auditor to perceive and recognise the audits in order to exam, obtain evidence and evaluate on the basis of the judgement of the author about the audit reports. *Surveys* module is aimed at collecting specific data that have been extracted from a particular group of people whose previously have been assessed together. Such data describes their thoughts, opinions and feelings about issues or any events related to the process. *DORs* have been described in the section 7.3.1, to report the daily, weekly and monthly task that has to be performed in the plant. *Risk Charts* is a summary section where it is possible to visualize different kind of information that has been inserted during the assessment of the risk, such as charts related to: consequences, causes, issues, level, status and treatments.

7.2.6 Communication

In this module there are just two sections: *Anomalies* and *Shift Handover* that have been also described in the previously chapter (the *Dashboard).* These features of the risk register are also divided in *Open* or *Close*.

7.3 Why Tosca's Risk Register

The Irish spin-out campus company Tosca Solutions has developed an IT tool to increase operational efficiency, decrease operational issues and have a continuous improvement. The competitive advantage of the Tosca Solution tool is based on some particular aspects such as:

- Checklist with built-in reporting system, with the benefit to have report inspections in real-time and to inform about potential anomalies

- Corrective actions suggested by the system for a better planning and execution of action plan with a greater staff participation
- Pre and post anomaly analysis in order to have a strategic analysis to prevent issues and for having a faster report about irregularities day by day
- Real-time audit of the main operations with internal and external controls to analyse and verify the management trend
- Reduction of the time spent in processing disjointed information based on paper with the benefit to have a data collection and reporting in real time
- Efficiency in finding resources and following action plans, involving all the personnel in an active participation during the risk management
- Efficiency tracking system to ensure better monitoring of risk management through notifications and performance indicators system to inform about the management progress
- Reduction of corrective action through functions by using qualitative methods to execute high efficiency action plans
- Optimized workflow management for efficient risk data analysis, giving more support to the users with a reduction of errors and better efficiency

Tosca Solution's goal is to provide a tool that can assist small, medium and large companies in the creation, planning and management of safety-critical activities, in highly regulated industries.

7.4 Guidelines for the Prototype

The Prototype is an IT Project for achieving a definition of a *cloud-based digital harmonised solution* to deliver an integrated risk/critical asset register to encompass technical and non-technical risks. It includes the facility to trend exposures and conditions over time and the evaluation of investment decisions based on monetised risk exposures.

At present there are multiple systems/individual spreadsheets (station asset registers including risk analysis) and a separate risk register hosted on a SharePoint platform. The multiple inconsistent systems do not facilitate the much-needed analytic capability in respect of asset management processes and decision optimisation.

The proposed cloud-based solution is to deliver better analytics on monetised and aggregated risk exposures across different stations and at Central level. The tool will allow comparison analytics across different quarters and time periods in a way that the SharePoint and or Microsoft Excel based solutions are not able to support. These better analytic solutions are required to allow optimisation of asset management decisions looking across the portfolio of assets, including harmonisation of risks, consistency of risk reporting to support senior management in making decisions, aggregation of risks, monetisation of risks, supporting asset investment decisions and maintenance strategies. Analytics is also required to trend the results of asset investment and support the optimisation of balancing Cost, Risk and Performance for the Generation business.

The objective of the prototype is to develop a process and associated IT system that embeds risk management within the power company generation asset management and generation

operations, by remembering that the users of the system are Stations and Central Head Office functions.

The two main outputs required from the process are:

1. Reporting of risk for Governance purposes
2. Risk based decision making to overhaul investments and other significant station asset investments

It results are necessary to split the system deliverables in two categories:

- Governance
- Asset Management

About governance, one of the deliverables is a system where users at station and central level can input risks as either Technical (via CAR interface) and Non-Technical risks. Besides, another request for the prototype is a well-designed reports risk that includes:

- Location based "Top 10"
- Aggregated "Top 10"
- Dashboard with Heat Maps
- Risk Tracking (e.g. risk versus time for each asset group)
- Assurance regarding review compliance by location (quarterly) – KPI for station signals.

Moreover, a facility is required for specialists to enter generic risks and means of documenting that risks were considered at plant level

Concerning Asset Management, other features are required: first of all, it is important to standardise CAR and GRR input fields by a list of all critical assets, by using three levels of detail and by a status history of the system. Other significant features requested for the standardisation are:

- A risk rating for the current status of each asset result needed also by improving required action
- A final roll-up for level one and level two asset and assessment of risk status based on max risk index and overall monetised risk exposure.
- Asses root causes and a consequences classification.

Then, a risk rated option evaluation will result mandatory for the prototype. Several keys options are required for this feature:

- Input corrective action plan 1, and/or 2 and/or 2
- For each plan project cost and risks over a 4 or 5 year
- Calculate and compare net present value of each scenario
- When an option evaluated is selected, update risk profile upon implementation of plan plus ask user to update individual item risks
- Archives past and current risk levels to facilitate tracking.

Figure 7.9 below shown the guidelines of the prototype synthetized by a blocks diagram.

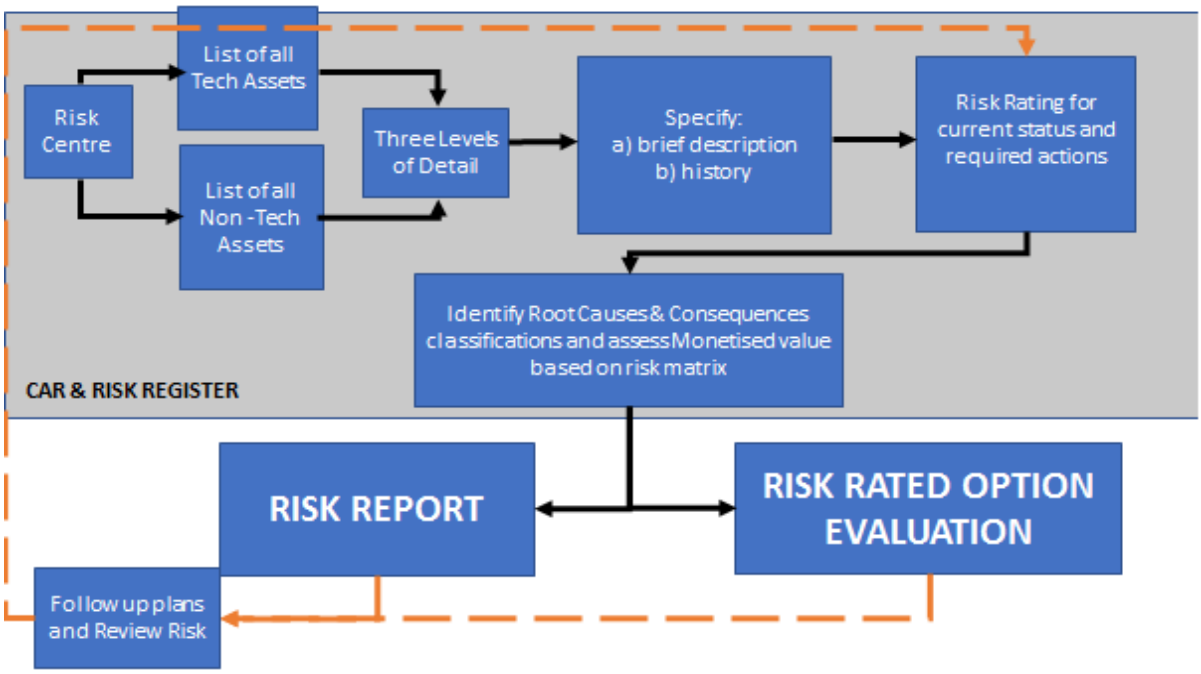

Figure 7.9: Prototype guidelines

The first step requested in the guidelines is to split the assets in Technical and Non-Technical ones. For that reason, the requested prototype need to be used for the given Station and Head Office Area. Therefore, that the single station can just analyse and manage their own technical assets without taking in care of the non-technical ones which will be responsibility of the Head Office Area.

The Non-Technical Assets		
Compliance	**Human**	**Finance**
Environmental	Behavioural	Finance
External safety	Organisational conditions	
Internal standards and procedures	Work activities	
Process safety	Work environment	
Regulatory		

Table 7.1: Non-Techinical Assets

Table 7.1 lists all the Non-Technical assets that are reported in the GRR. *Compliance* include all the assets conforming to the rules, such as laws, regulations, policy and standardizations. *Human* is referred to all those risk that happened for human errors. *Finance* is the asset referred to the economical expenses.

On the other hand, Table 7.2 below reports the full list of Non-Technical assets and the related number of hazard that has been reported for each of them in GRR 2018

Technical Asset	Number of hazards
T - Abatement equipment	3
T - Ash handling equipment	1
T - Batteries	3
T - Boiler	**26**
T - Buildings	5
T - C&I	**20**
T - Cooling water systems	5
T - Fire protection systems	**4**
T - Gas handling equipment	2
T - Gas turbine	**19**
T - Generator	22
T - Grounds	**3**
T - High energy pipework	2
T - Hydro ancillary equipment	**14**
T - Hydro structures	13
T - Hydro turbine	**8**
T - Hydro water control equipment	3
T - Motors	**5**
T - Peat handling equipment	1
T - Steam turbine	**6**
T - Switchgear	9
T - Transformers	**10**
T - Water treatment systems	1
T - Wind Turbine	**12**

Table 7.2: List of Technical assets and related number of hazards

The three levels description is an idea derived from the CAR and it is aimed at having a complete idea of the assets by analysing every unique component.

The first level is the main and generic unit level, analysed globally by not entering in to the details: *Turbine*, *Boiler*, *Motors* etc. It is easier consider that the level one is exactly a technical asset contained in Table 7.2. The second level includes all the controls sand safety systems, modules or parts of the main unit and all the valves system present in the process. Every single component which is included in level two has to been considered in level three, that is the most accurate level of details where it is possible to focus. Table 7.3 shows an example of those levels for the main component *Turbine:*

LEVEL 1	*LEVEL 2*	*LEVEL 3*
TURBINE	**HP Valves**	LHS Main Stop Valve
		Moog Servomotor to LHS Main Stop Valve
		Actuator to LHS Main Stop Valve
		LHS Main Stop Valve Strainer
		LHS Main Stop Valve Pilot Valve
		RHS Main Stop Valve
		Moog Servomotor to RHS Main Stop Valve
		Actuator to RHS Main Stop Valve
		RHS Main Stop Valve Pilot Valve
		RHS Main Stop Valve Strainer
		LHS Stop Valve Actuator Mounting Studs
		RHS Stop Valve Actuator Mounting Studs
		LHS Main Stop Valve Cover Bolts
		RHS Main Stop Valve Cover Bolts

Table 7.3: Example of the three level of detail

LEVEL 1	*LEVEL 2*	*LEVEL 3*	*HISTORY*
TURBINE	**HP Valves**	LHS Main Stop Valve	**2015:** The stop valve was removed, overhauled and inspected and found to be in good condition - no defects reported. The flat washers for the valve cover had become deformed and did not have the required thickness so were replaced with new. The insert and sleeve installed in 2011 were visually inspected and ok. **2011:** Intermediate piece had damage to its bore surface, erosion and scratches near the packing area. The valve cover also had deep erosion and scoring in the packing area around the whole circumference. The area was machined both damaged parts of the intermediate piece and cover were replaced with an insert and a new sleeve reverse engineered and fitted in accordance with Fuji instruction. Some scratches on the spindle were polished. 2 actuator studs were replaced due to damaged threads. **2009: […]** **2008: […]**

Table 7.4: Briefly history for a component of the third level, it is requested for all components

ITEM	STATUS	L	I	R	EQUIVALENT MONETIZED EXPOSURE
HP/LP Module	2014: A camera inspection of the last row of rotating blades was carried out via the inspection hatch at the HP exhaust. The rotor was hand barred through 360 deg and the full blade profile was visually inspected. No defects noted and no signs of impact damage or erosion.	3	4	12	XXXX.00 €

Table 7.5: Roll-up for a level two

LEVEL 1	*LEVEL 2*	*LEVEL 3*	*HISTORY*	*L*	*S*	*R*	*REQUIRED ACTION*
TURBINE	**HP Valves**	LHS Main Stop Valve	**2015:** The stop valve was removed, overhauled and inspected and found to be in good condition - no defects reported. The flat washers for the valve cover had become deformed and did not have the required thickness so were replaced with new. The insert and sleeve installed in 2011 were visually inspected and ok. **2011: […]** **2009: […]** **2008: […]**	2	4	8	Medium (valve) inspection should take place after 32,000 EOH or 4 years following major inspection. Therefore, no further inspection due before 2019.

Table 7.6: status and required action for a component of the third level

After the analysis for each component as showed in Table 7.4, 7.5 and 7.6, it will be necessary synthetize all the information in a roll-up for level one or level two asset. An assessment of risk status based on max risk index and overall monetized risk exposure as showed in Table 7.6will be also mandatory.

Most of the features requested at the prototype, till this very point, are commonly present in the commercial risk registers. The innovative part of the proposal protype is the risk rated option evaluation. This part is aimed at evaluating the correction action for all the components of the plan that presents a risk and at estimating the plan project costs and risk over a four or five years time period.

	R 2018	Cost 2018	Residual Risk 2019	Cost 2019	Residual Risk 2020	Cost 2020	Residual Risk 2021	Total Cost	Average Risk
1	12	20	4	0	8	10	4	**30**	**7**
2	12	20	4	0	8	0	10	**20**	**8,5**
3	12	20	4	10	3	0	5	**30**	**6**
4	12	20	4	10	3	5	3	**35**	**5,5**
5	12	0	12	30	4	10	3	**40**	**8**
6	12	0	12	30	4	0	6	**30**	**8,5**
7	12	0	12	0	15	50	6	**50**	**11**
8	12	0	12	0	15	0	20	**0**	**15**

Table 7.7: Plan project cost and residual risk over four years

Table 7.7 describes eight different scenarios among four years with different approaches for the required works and different expenses. The cost is just a casual numerical example and not a real monetised expense. This example is aimed at understanding how the company is involved in the investment and in the mitigation of the risk. By using the tool can better invest money in order to reduce the risk itself. Starting from an actual situation in where the assessed risk has a risk exposure of *12* and a related status of *Amber,* several possible cases has been evaluated:

- Invest in the first year for reducing risk to a lower level since the first moment;
- Invest in the second year for reducing risk after one year, but maintaining a high level of risk for two years in a row and having a higher expense;
- Invest in the third year, but having a risk increase during the previously years and a very high expense;
- Not invest at all, continue risk increasing during the years

From the results in Table 7.7, evidently the best compromise between total expense through the years and average risk level could be a continue investment during the years (since the first one) in order to maintain a *Green* status with a little investment per year.

7.5 The prototype

The guidelines for the prototype requested from the power generation company of republic of Ireland have been extensively analysed from the risk safety analysts and developers of Tosca solution whose propose a tailored version of their Risk Register in which it is possible to include all the needs of the Irish Company.

By basically using the same user-friendly interface, the new customised prototype helps the power generation company users, either manager or workers, to insert all the same information uploaded before in two different spreadsheets: CAR and GRR. In fact, trying to maintain always the same separation between the CAR, that provides information about the technical critical assets, and the GRR, that provide technical and non-technical assets information, the new prototype wants to permit the user to evaluate every single asset, by dividing them between technical and non-technical as first step.

When the user opens the software, the first screen he finds is the *Login* page, as reported in Figure 7.10 below. The login page permits also to connect to a single station system.

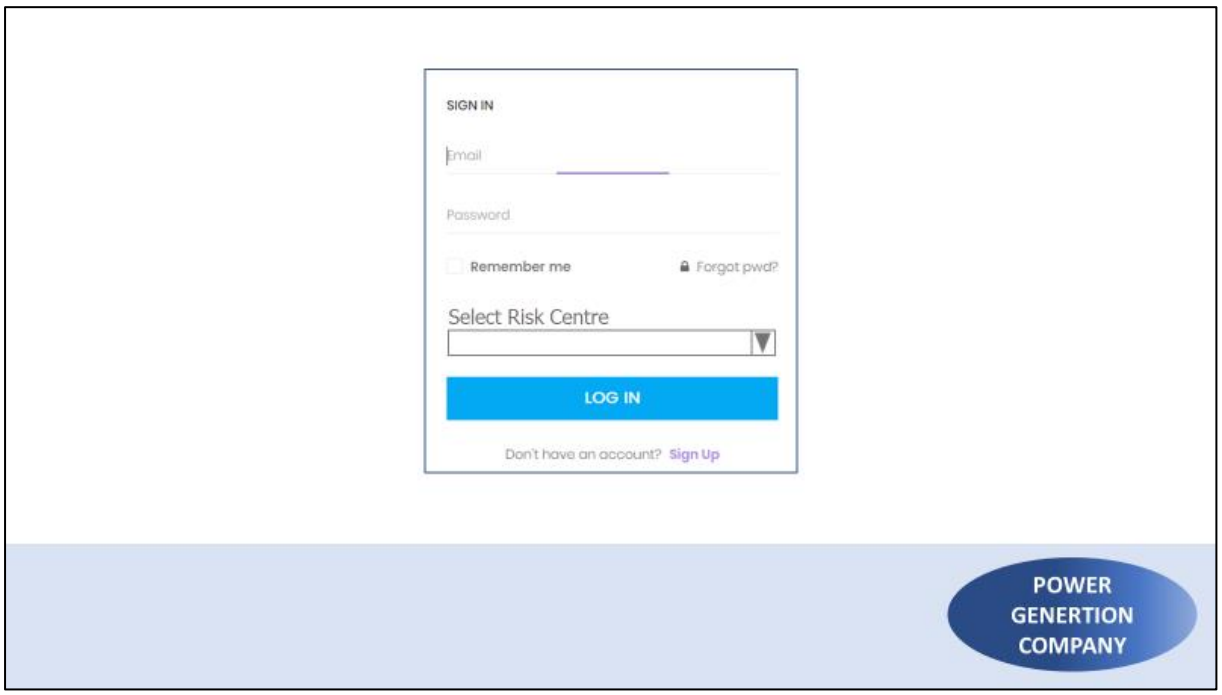

Figure 7.10: Prototype Login Page

After the login-in, the system directly brings the user to the introductive view of the software: the *Dashboard*. The scope of the dashboard is to give a generic system overview by reporting, in a very user-friendly layout, the most relevant information concerned the risks that have been already reported in the software.

In Figure 7.11 below is reported the dashboard module of the prototype. Basically, it is composed of two modules: a donut chart and some bar charts.

The donut chart permits the user to have an overview of the monetised value, risk rating and action plan. The action plan view for the donut chart is a four-colour chart which describes the timeline of the action:

- Green: action is in time
- Yellow: action is in delay of 1 month or less

- Orange: action is in delay of more than 1 month but less than 4 months
- Red: action is in delay of more than 4 months

The bar charts essentially give information about the "Top 10" in terms of Consequences, Monetised Risk Exposure and Risk Exposure in the pre-selected station. It is important to outline that the same view presents in Figure 7.11 for a single station, can be suitable for all the station and for the headquarter as well.

Moreover, the bar charts permit the user to navigate easily across the levels of the station and therefore it is possible to visualize the "top 10" reports for different degrees of details inside the same risk centre.

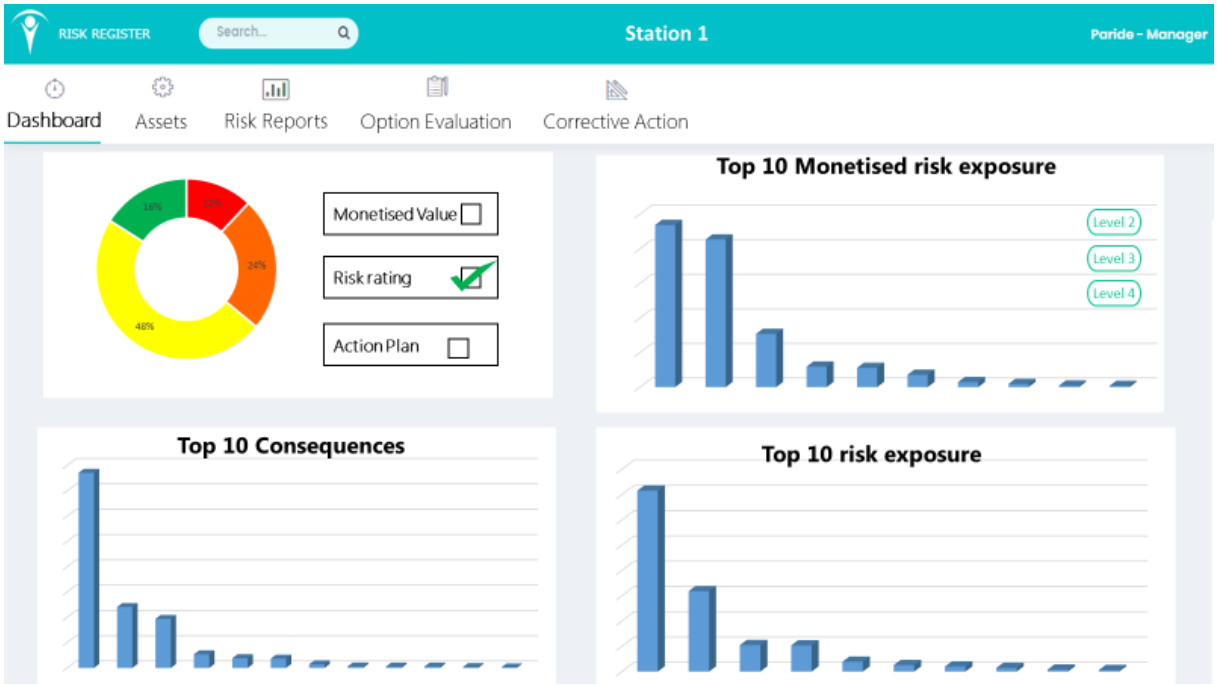

Figure 7.11: Prototype Dashboard

When the user decides to visualize, edit or add a new asset of any level, it has to click on *Assets* in the horizontal main menu. After the selection of the Asset module, the user can choose to open the *Technical Assets* and *Non-Technical Assets*, as showed in Figure 7.12. In the following pages, *Technical Assets* module permits the user to visualize all the stations and the user has the possibility to open, edit or delete the station of its interest. If a user is logged for a station,

it possible for the user to insert or edit the risks that has been uploaded in its station. The possibility to manage and edit risk for all stations is a privilege for the head office.

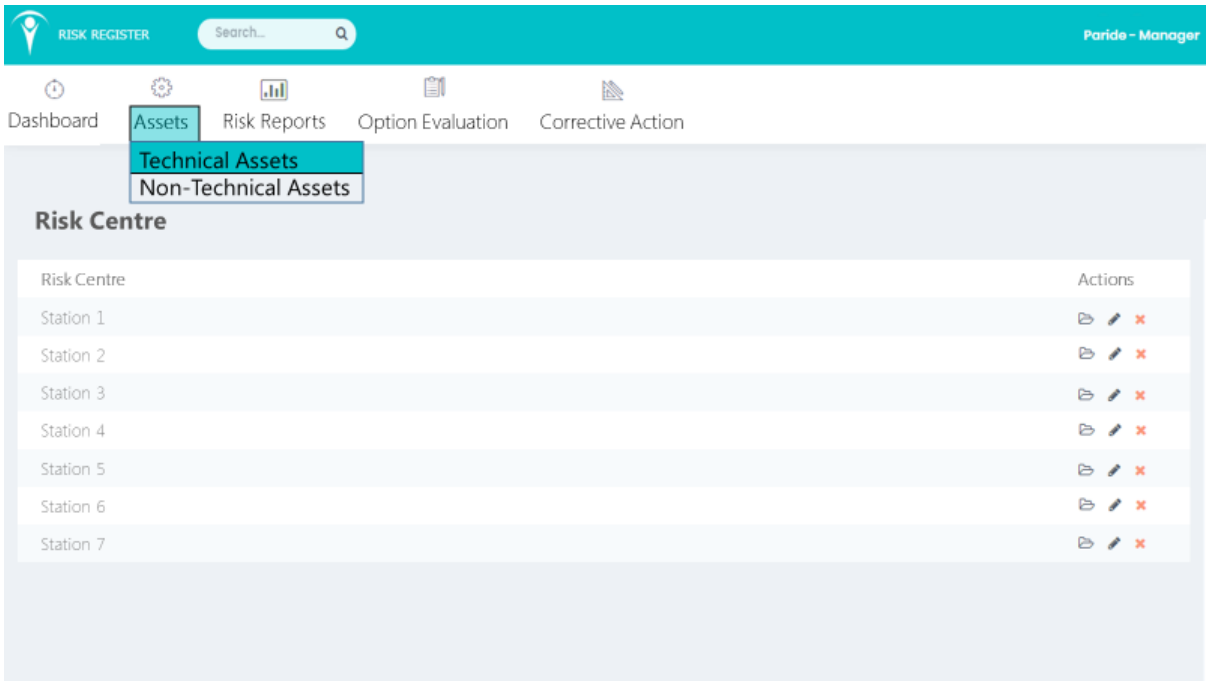

Figure 7.12: Risk centre and kind of assets chose

After selection *Technical Asset,* the user can visualize in Figure 7.13. Here there is a list with all the units that there are in the selected station. It is also possible add a new unit. On the right of the screen the system offers the possibility to open, edit and eventually delete the selected unit.

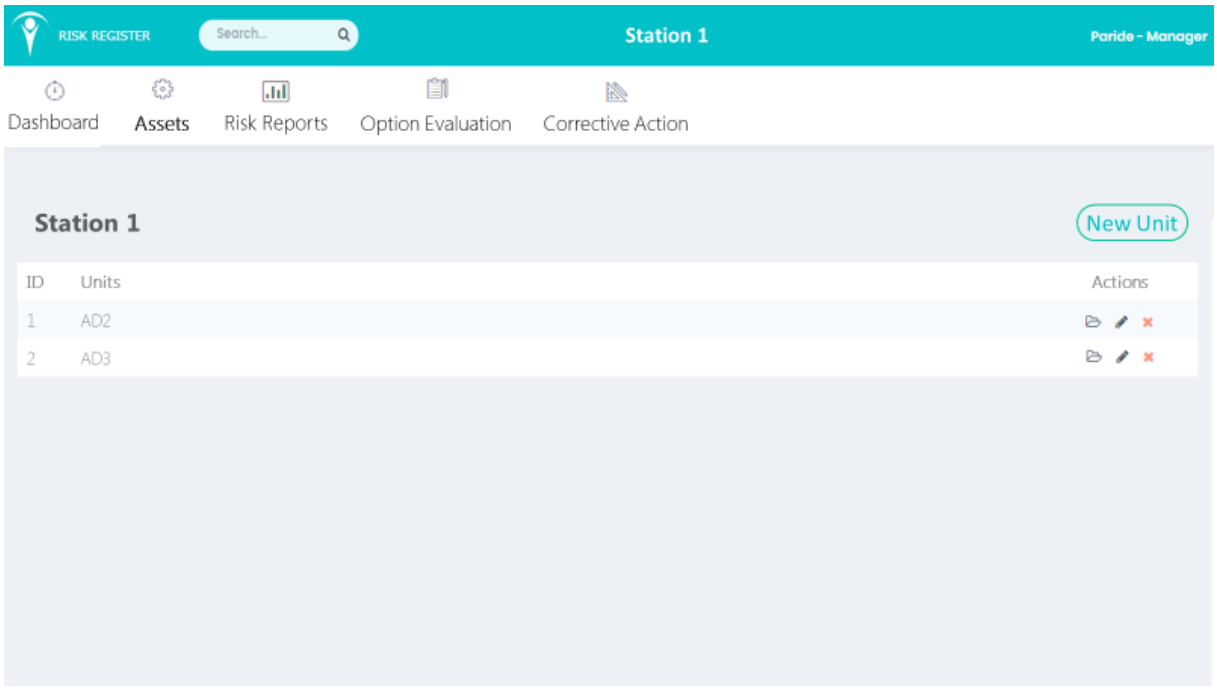

Figure 7.13: Unit overview for the selected station

It is possible to see all the lower levels of each unit by clicking on the unit's name. The system works like a "Chinese Box": it is a cascade of assets one inside the higher one. That is mean that inside the unit *AD2* is possible to visualize all the assets and all the *Level 3 assets* belonging to it, as shown in Figure 7.14.

The section shown in below is the *Main* section and it provides information about causes, consequences, hazard but it does not provide further or complete information about risk rating.

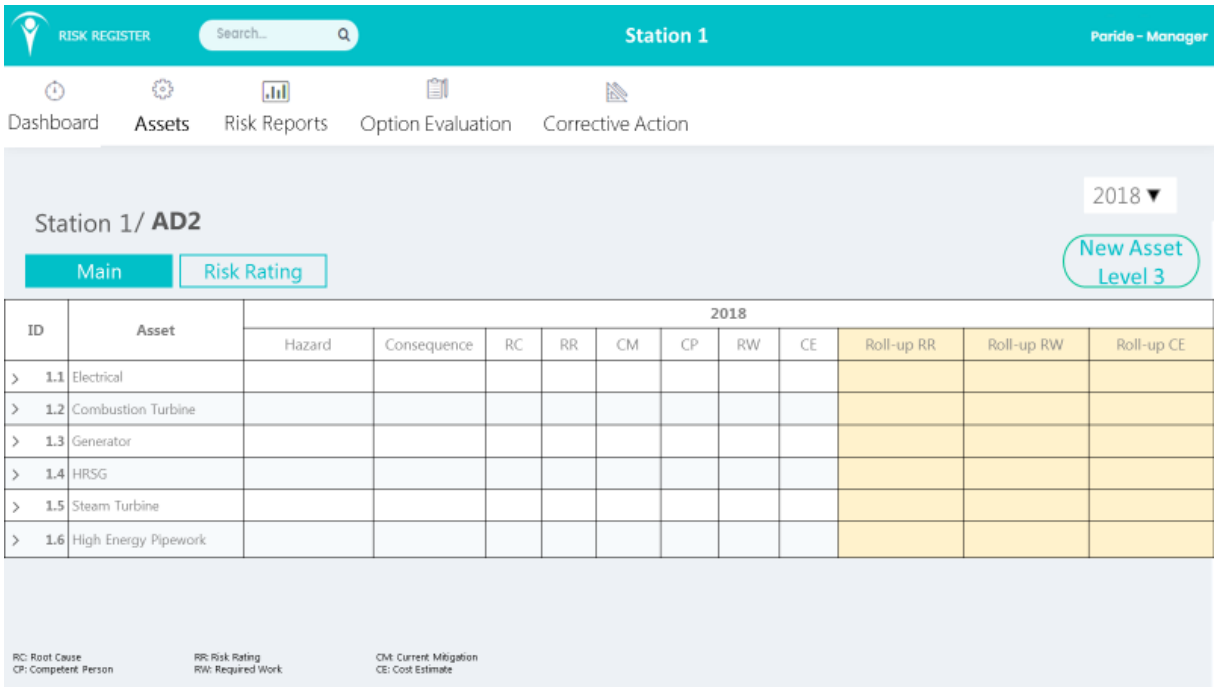

Figure 7.14: Main table for Level 3 assets

For each asset it is possible to check some crucial information in the main table that automatically appears. The coloured columns are referred to the Roll-up module, in which are displayed the information about risk rating, required work and cost estimate of the lower for the selected asset. This table is an editable table, that means that the user could visualize and edit data on it. Furthermore, it is also possible to visualize more information about the preferred asset just by clicking on the little arrow near the ID number. An additional row will appear just under the select asset to inform the user about: Identifier, Risk description, status description, history as it is shown in Figure 5.15 below. The decision to add an additional row for that five information results necessary for avoiding to overload the main table with excessive columns and data.

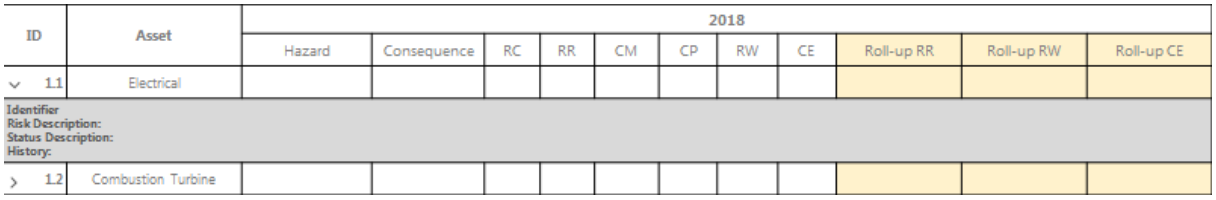

Figure 7.15: More available details for each unit

The risk rating section is allowed by clicking on the button named "*Risk Rating*". This section allows the user to visualize all the details concerned the risk rating and it gives the possibility to edit the values directly from the table as it is possible to see in Figure 7.16

below. On the right part of the table it is possible to visualize information about the risk rating and the total monetised risk exposure related to the lower levels for that asset. In the roll-up risk rating, the higher risk rating between the underpinning levels for that assets is shown. In the roll-up total monetised risk exposure, the sum of all the monetised risk exposure of the underpinning levels for the selected assets is shown.

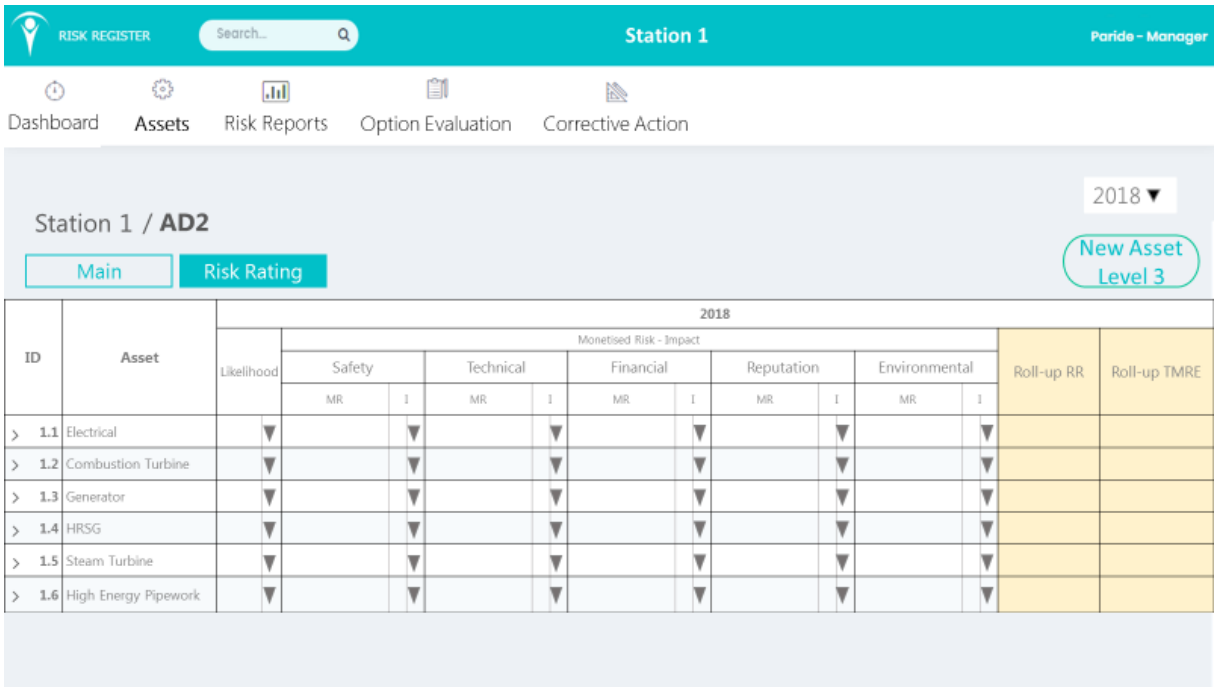

Figure 7.16; Risk rating section for the cascade of assets in AD2

For each asset, where expected, it is possible to visualise lower assets easily by clicking on the asset name. Although the original prototype guidelines ask for three levels of details for each asset, it results are necessary to permit the user to have more detail levels. By selecting *New Asset Level 3* the user is allowed to create a new asset for the current level.

For each asset the user has the possibility to manage the assets as shown in the previous level three example. It is important to outline that the information of level three come from GRR and CAR as well, hence the main table visualises some information that for the lower levels are not available, such as hazards, consequences and root causes. Inside each level, the user can create, visualize, edit and delete as it is possible in level three.

In Figure 7.17 below is shown the groups of level four assets inside *1.1 Electrical.*

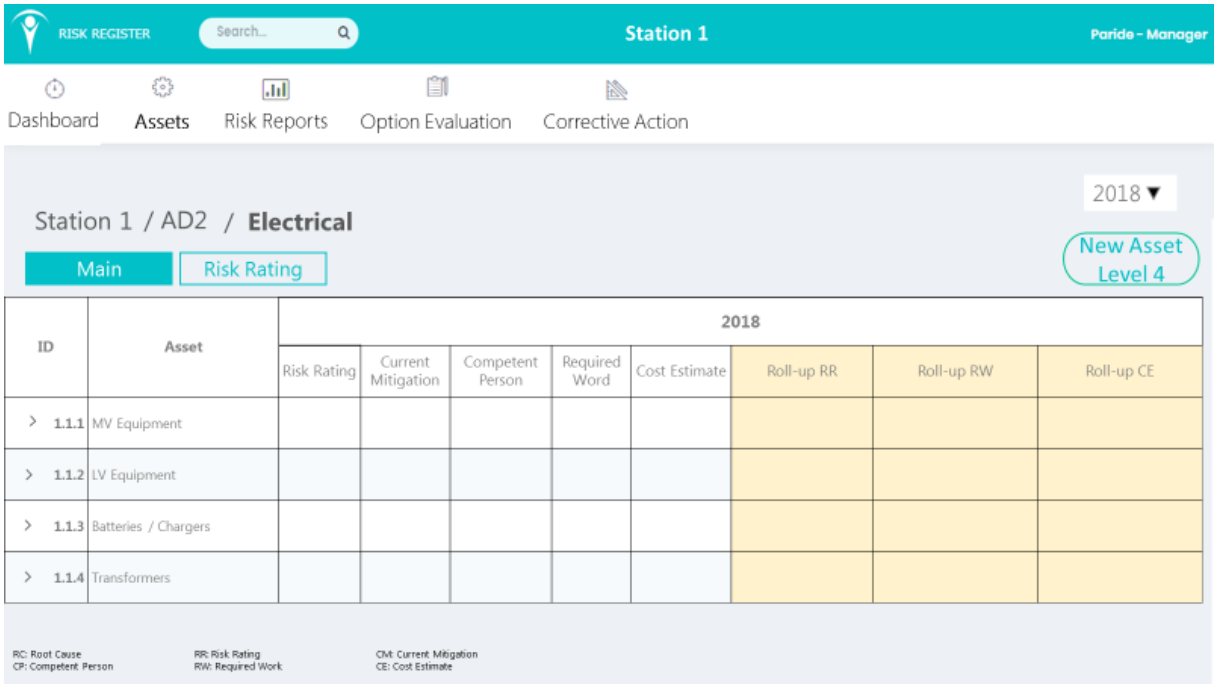

Figure 7.17: Example of level four assets

It is possible to show all the possible levels of assets, but it results are unnecessary considering that the layout of all the underpinning levels is exactly the same of Figure 7.17. Furthermore, the creation of every level is possible by using the same date entry form as shown in Figure 7.18.

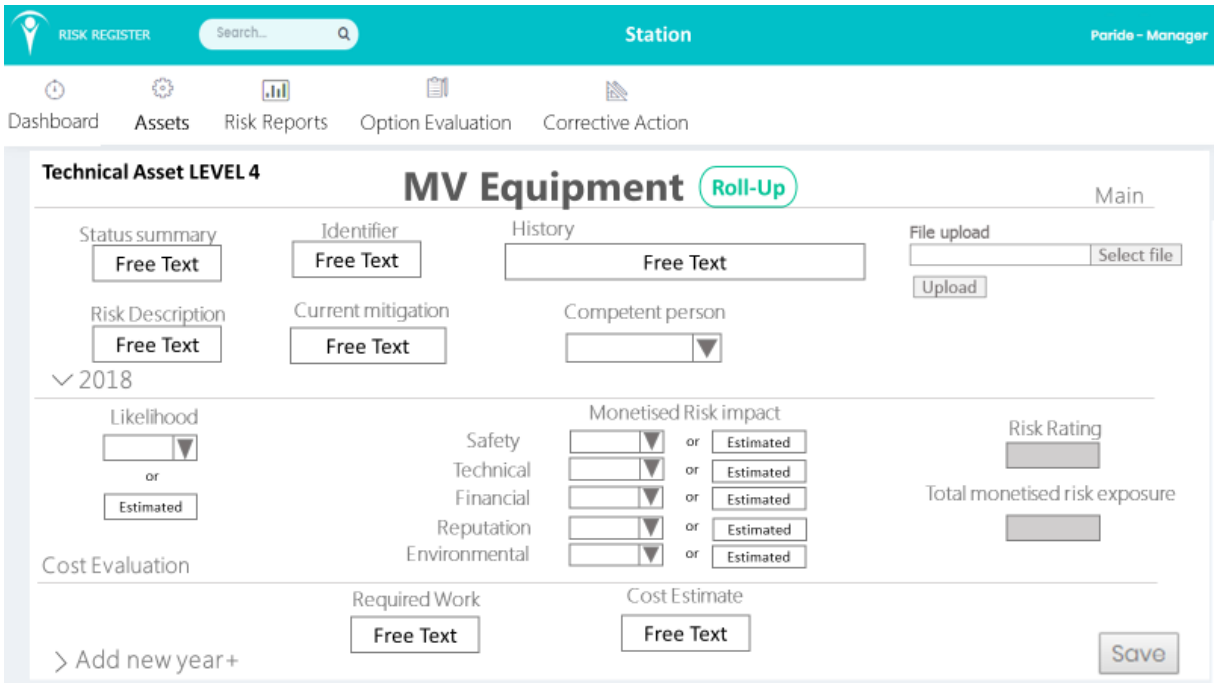

Figure 7.18: Data entry for a technical asset

First of all, the user has to complete different free text queries:

- *Status Description*: optional;
- *Identifier*: mandatory if exist;
- *History*: optional;
- *Risk Description*: mandatory;
- *Current Mitigation*: optional;
- *Competent Person*: mandatory;

The above listed queries are information commonly shared through all the assets and levels of the stations. At that point the user can assess year by year the risks already described, by using the risk evaluation section. That section is available for every new year that the user decides to add in the software. For each year the user has to add information about the likelihood and the impact of the risk. This information can be added in two different ways: by choosing from a dropdown list the value in a numerical range from one to five or by typing an estimated value as a "free text". In both cases, the system can calculate the risk rating and the monetised risk exposure, by using the conversion tables. Those tables are already described in this work and they permit the user to define a real likelihood or impact value in a short integer range.

At the completion of asset section, module risk report can visualize and compare all the risks that have been inserted in the software. Mainly the risk reported is divide in:

- Heat-map visualization
- Table visualization
- Chart visualization

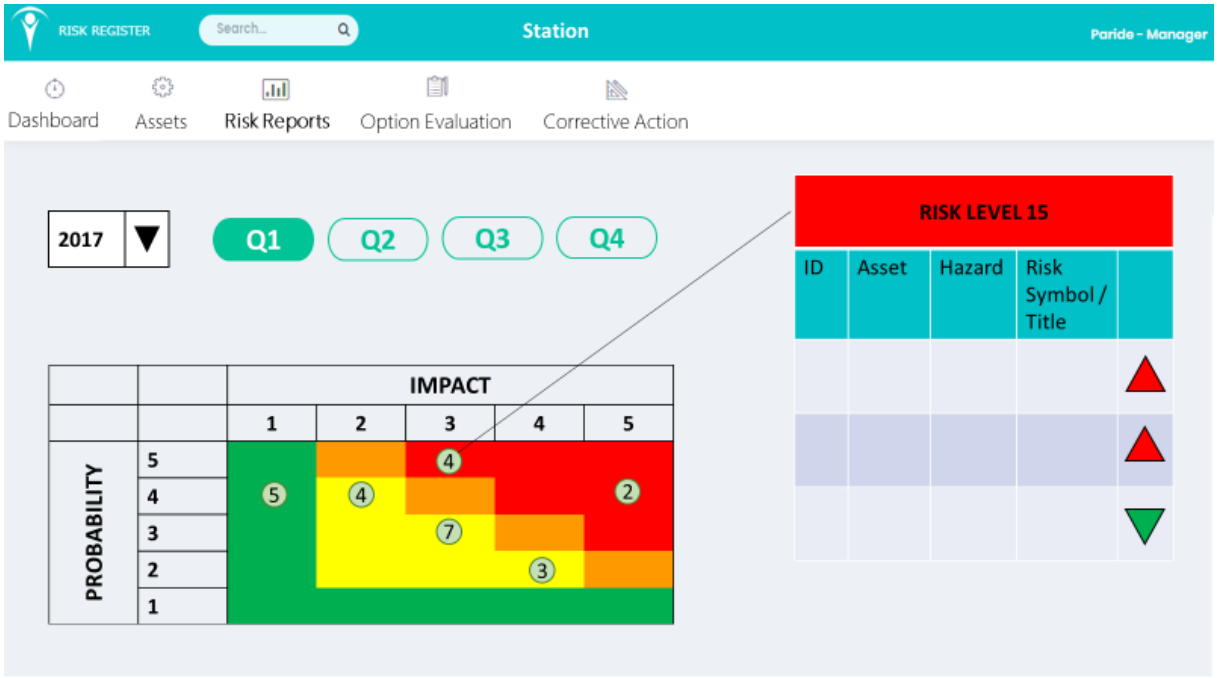

Figure 7.19: Risk matrix in heat-map version for output in the prototype

Figure 7.19 presents an example of a heat map used as risks report. In the middle of the screen there is a risk matrix divided by colour which represents the heat-map. With the matrix, the

system gives the user the availability to choose year and quarter for the representation. The numbers inside the circle, located on the heat-map, represent the number of risks that have that level of exposure. This user-friendly interface permits the user, by clicking on the selected risk pin, to visualize the details of the risk that present that level of exposure by opening a pop-up table where the identification number of the risk, the asset, the name of the hazard and the risk symbol are shown. The coloured arrows in the pop-up table permit the user to know if the level is increased or decreased compared with the previous quarter.

The Figure 7.20 below shows the table visualization for risk reporting. On the left of the screen the user can choose, as in the example of the heat-map reporting, the year and the period that he wants to visualize. In the middle of the screen is shown the main table, that presents a list of the top ten hazards that have been inserted in the *Assets* module. In the example below, the table that is shown, is referred to the top *Risk Symbol/Title* and ordered by the decreasing risk rating. Moreover, the table permits to visualize the monetised risk exposure and the ID of the risk. Other possible visualizations are:

- Top Ten risk- Listed by Root Causes Type
- Top Ten risks- Listed by Assets
- Top Ten risks- Listed by Hazard
- Top Ten risks- Listed by Consequences

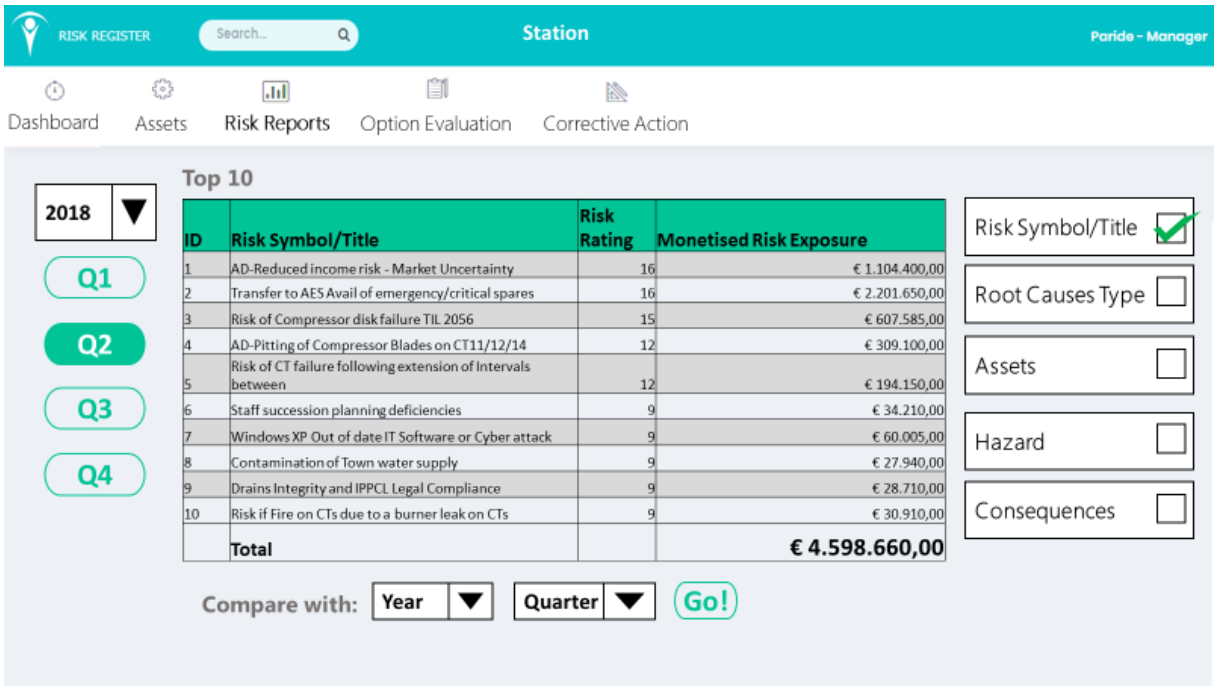

Figure 7.20: Table output for the prototype

Another relevant function of the risk reported related to the table visualization is the possibility to compare risks of different periods. In Figure 7.21 there is an example of this features which results are useful for better understanding of the variation of the risks throughout the years. The understanding of the comparison is facilitated for the user by using coloured upward and downward arrows depending on the case. In Figure 7.21 it is also shown how the user can

choose a view of Technical Assets, non-Technical Assets or both of them, depending on the interest of the user.

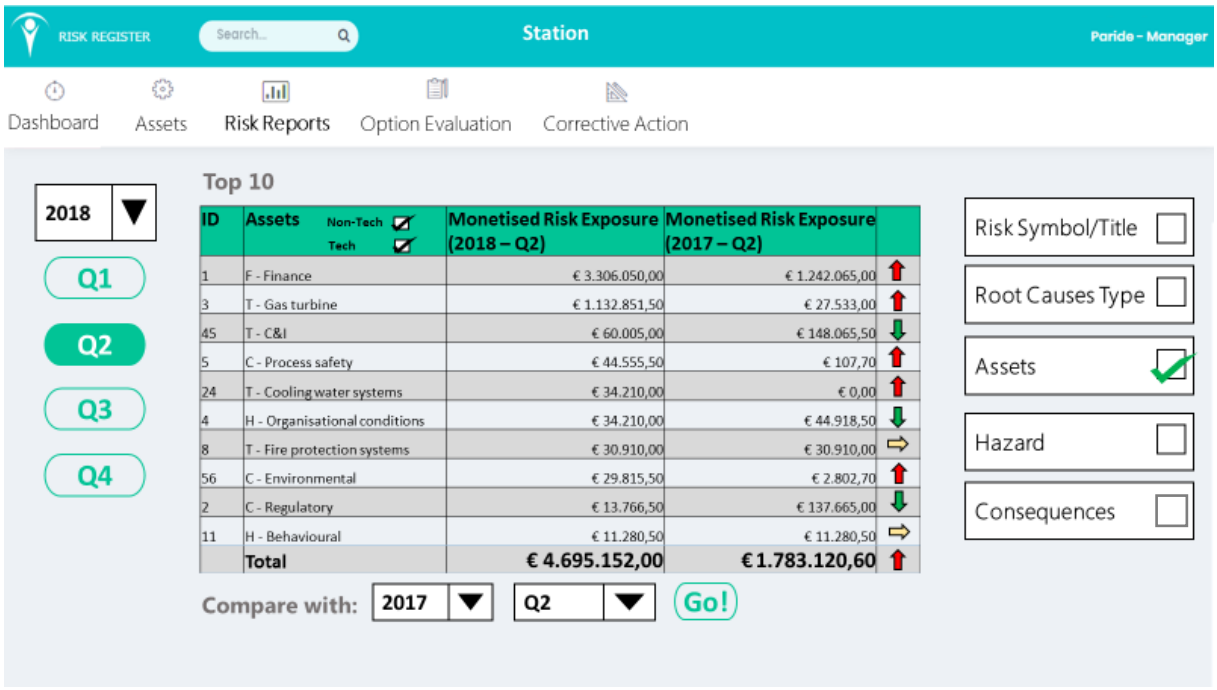

Figure 7.21: Comparison of monetised risk espoure for two different years in the prototype

An alternative view for risk reporting is the chart visualization. This feature uses the same concept of the Table visualization, by using five categories of risk reporting on the right side of the screen that permit users to decide which class wants to be shown in the main view:

- Risk Symbol/Title
- Root Causes Type
- Assets
- Hazard
- Consequences

The kind of chart used in the system is usually a bar chart that offers the user a better comprehension of the situation. The comparison between different years inside this chart is possible through the use of different colours.

In Figure 7.22 below is shown a chart with the importance of every asset (either Technical and not) and it is noticeable how the chart can outline the impact of the worst assets related to the others: e.g. Finance, with a monetised risk exposure over 3 million euros, has n heavy impact compared to the other assets

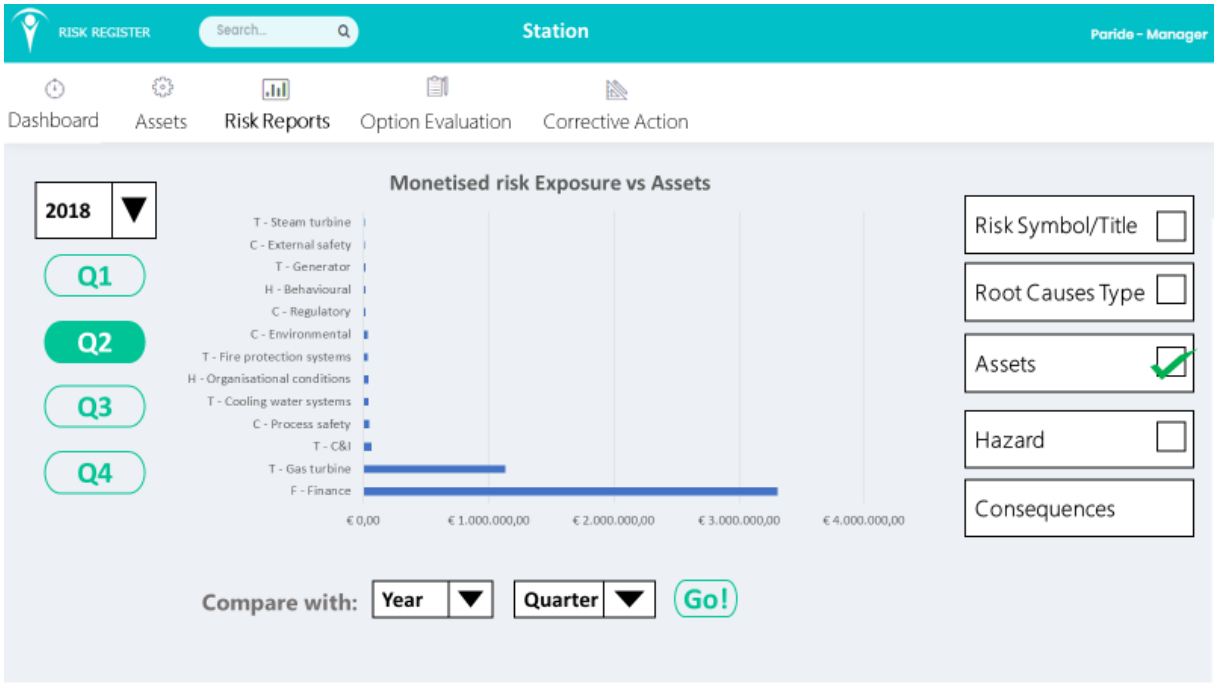

Figure 7.22: Bar chart output for the prototype

Option evaluation module is a section aimed at recognizing all the investment possibilities that the company can afford throughout the years.

First of all, during the creation phase for a new option, the user has to choose which asset to be evaluate as it is shown in Figure 7.23 below.

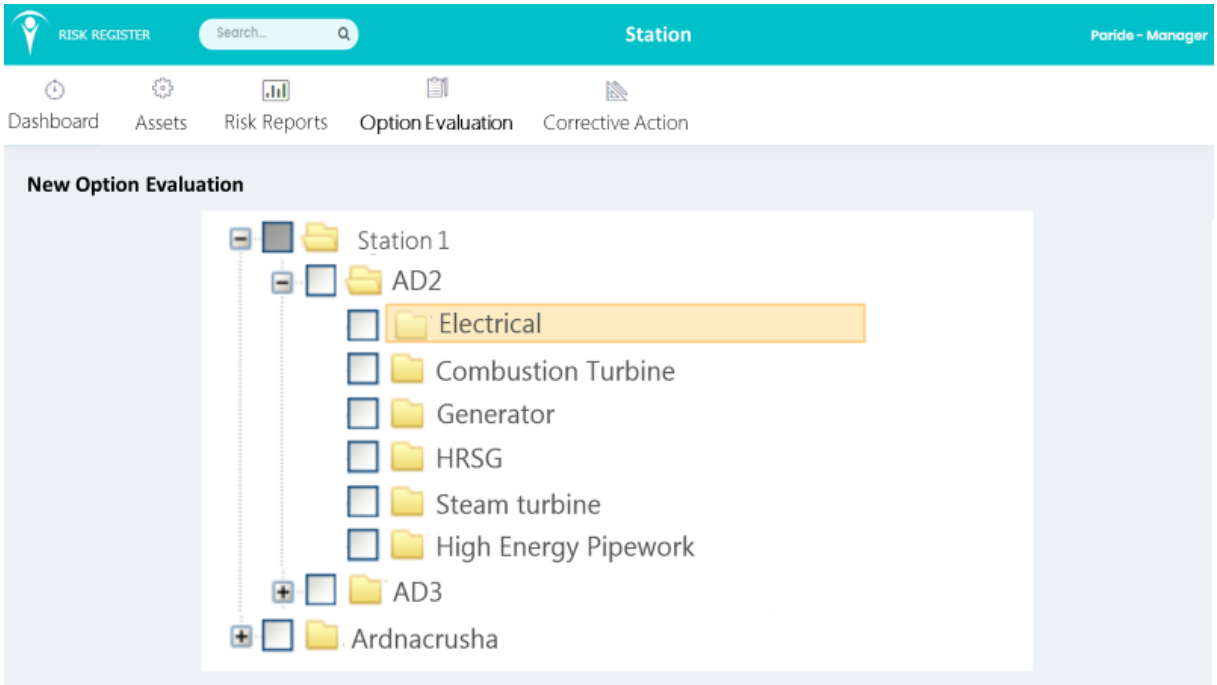

Figure 7.23: New option evaluation

After choosing of the asset which the user intends to evaluate for a new investment option, the system permits the user to begin the data entry. First of all, it is fundamental to insert a brief

description of the option that the user is going to create. Then, the user has to specify the return rate value, which represents the efficiency of the investment and it will be the same throughout the considered years. In Figure 7.24 is shown the data entry module for option evaluation:

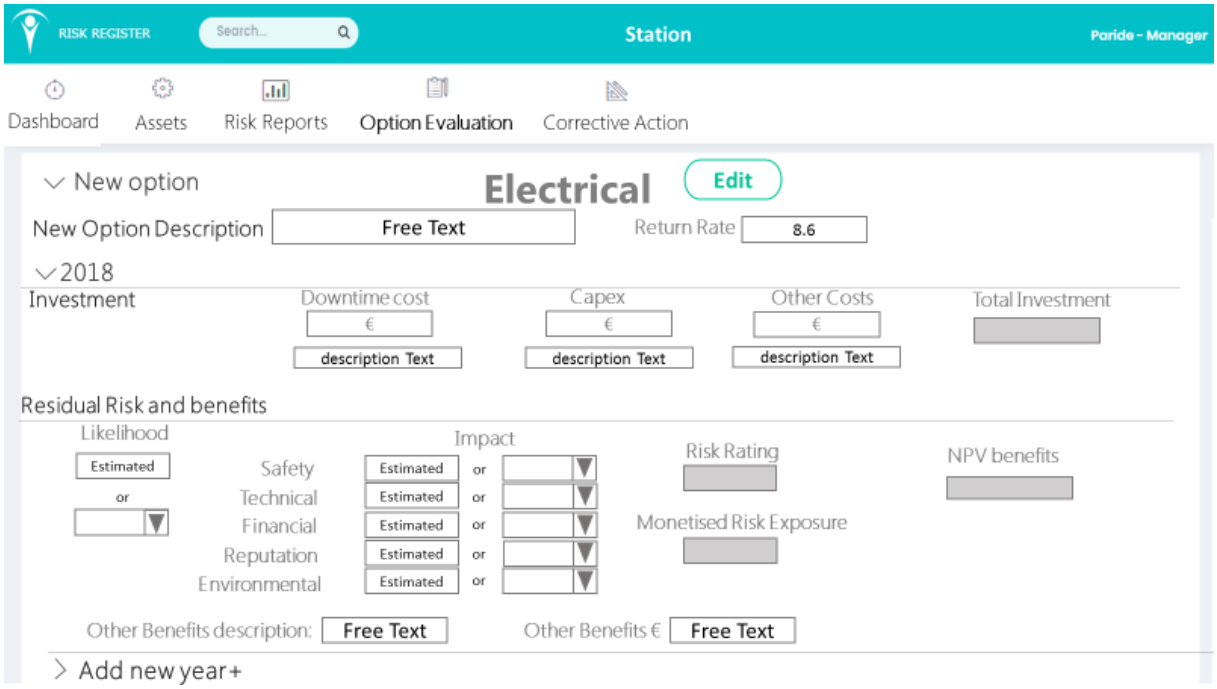

Figure 7.24: Data entry for option evaluation

The user has to complete two different sections: investment and residual risk & benefit. In the investment section, it is possible to complete two different kind of cost section: downtime cost, capex, and eventually other costs, such as NDT costs. If the user adds an investment, he has also to insert a rough description of it. The system provides also a method to calculate automatically the amount of the total investment. The residual risk & benefit section asks the user to estimate the risk after the investment described in the section above. Evaluating the risk level is necessary to evaluate the new likelihood and the estimated impact for each category. The system calculates automatically the risk rating and the total monetised risk exposure. If some benefits are available, it requests the user to add them in the provided space. After the completion of the data entry module, the users can visualize the table containing all the assets level three with their own option evaluation as reported in Figure 7.25.

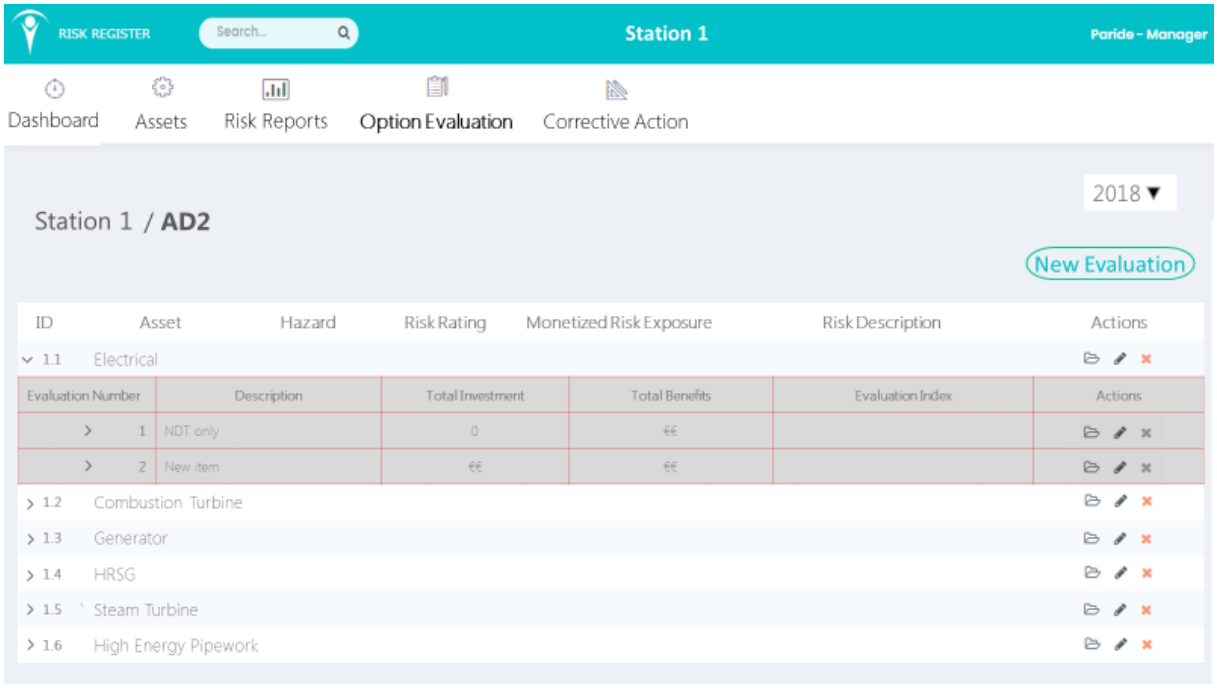

Figure 7.25: Data entry for option evaluation

Moreover, the system provides at the function to calculate the NPV benefits as a measurement of profit for every year by using the following formula:

$$NPV\ (i,N) = \sum_{t=0}^{N} \frac{R_t}{(1+i)^t} \qquad (14)$$

The user can evaluate the investment cost and the residual risk for several years by choosing to add new year in its option evaluation. Finally, when the user fills all the required field for the necessary years , it is possible to compare the different options and choosing the one with the best evaluation index. It necessary to remind that evaluation index is calculated as:

$$Evaluationi\ index = \frac{\sum_{t=0}^{N}(Monetised\ exposure + benefit)}{\sum_{t=0}^{N} NPV} \qquad (15)$$

The option with the higher evaluation index could be chosen as an option for a future investment.

The module of *Corrective Action* will be developed by using the same scheme and features already used in Tosca's risk register described in the previous pages.

8. A new module to evaluate operational risks: The use of a Dynamic Event Tree (IDDA)

8.1 The new approach: Dynamic assessment

Chapter three presents some methods and techniques that are consolidated and widely accepted and used, though they can hardly take into account time-dependent events, that always exist in process plants. Moreover, in the risk register some of the risks are related to tasks being carried out. Those tasks can be analysed using task analysis as a mean of functional analysis, where every step needs to lead to either another step or an event or a final state. The method that can be used is a dynamic event tree where the probability of outcomes could be estimated on the basis of existing values in databases or using the data stored in the risk register if the tasks are also used to inform checklist where operator can report anomalies related to each step.

The literature offers different examples of dynamic analysis which considers how the probability of different events is affected by the existence of previous one. Examples of dynamic event tree and dynamic fault tree have been suggested as well as event sequence diagrams to allow a dynamic simulation. In recent years, thanks to the advancing of technology capabilities in on-line monitoring and data elaboration, the focus is gradually moving toward early warning signal deviations and past events.

An interesting case study, that has been conducted during the last months for writing this work, was the evaluation of an operational risk in an ammonia plant, by using a software for dynamic analysis that has been developed in Polytechnic of Turin. IDDA (Integrated Dynamic Decision Analysis), that uses a kind of analysis based on a logical-probabilistic model, has been applied to the risk assessment of rare procedures in major hazard installation (Gerbec, Baldissone, & Demichela, 2016), the analysis of plant modification (Demichela, Baldissone, & Gianfranco, Risk-Based Decision Making for the Management of Change in Process Plants: Benefits of Integrating Probabilistic and Phenomenological Analysis, 2017) and the comparison between competing technologies for environmental protection (Baldissone, Fissore, & Demichela, 2016). The main scope of IDDA is to incorporate all the capabilities of the methods commonly used and described above in ISO 31010 by using a logical-probabilistic model integrated with a phenomenological modelling of the system behaviour, roughly explained in Figure 8.1 below.

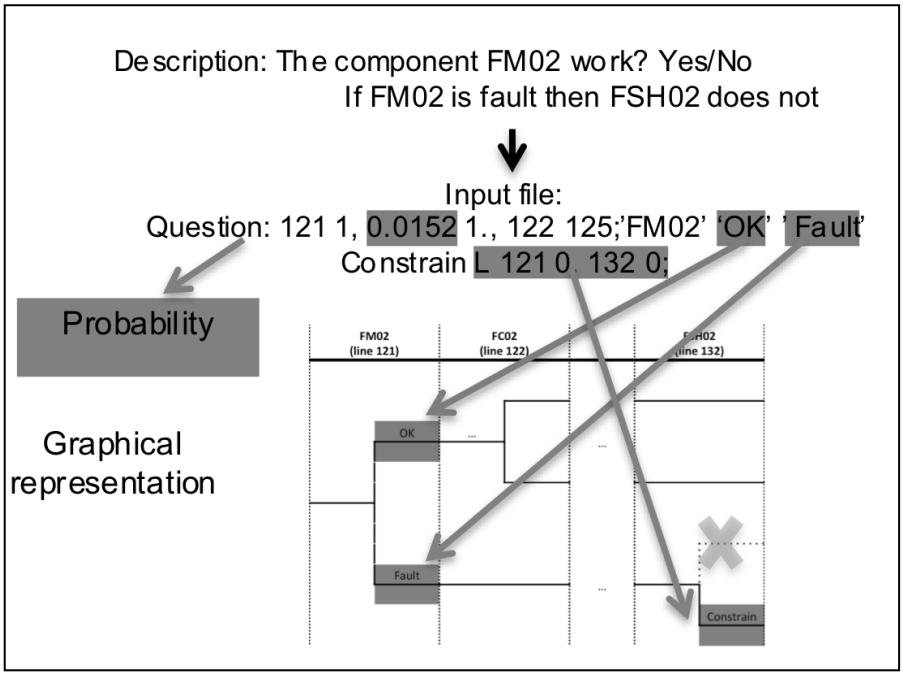

Figure 8.1: Logic of IDDA

Different steps are associated for the identification and the assessment of the risk:

- Identification of the events associated to the process and creation of a list of levels, with queries and affirmations, which represents the basic elements of the logical model as well as the nodes in the event tree.
- Creation of a 'reticulum' which represents (subsequent level) to be reached after each answer in each level, and a comment string that lets the analysts to read the logical development of a sequence.
- Association of each level with a probability which characterizes the expectation degree of the failure or undesirable event with an uncertainty ratio, which represents the distribution of the probability.
- Description of all the constraints, logical and probabilistic ones, which may change the model, based to the current information.
- Following this type of description of the system, it is possible to obtain all the possible sequences of events that the system could undergo: each sequence may define the probable dynamic of the system.
- Both the probabilistic and phenomenological models can run together for describing the physical behaviour of the process for each step.

On one hand, the phenomenological model can simulate the performance of the process and, on the other hand, according to the results obtained, it could update the logical model, adapting it to the level of knowledge acquired by the model itself. E.g., the phenomenological model allows analyst to check if the other components of the plant are to compensate a failure of a component. Furthermore, the system can continue till the end or, if cumulative effects appear, it could diverge the system from its standard performance. Moreover, the phenomenological model described above can offer a direct evaluation of the impact for several sequences for obtaining a direct risk assessment. Finally, it is important to outline that the use of IDDA helps

the user to decide the best design and operative solution by implementing the software with the other innovative techniques of risk-based decision making.

Furthermore, IDDA use a programme tool named SPACCO (Probabilistic Solver Coupled with Consequences Evaluation) which is based on the IDDA approach. The software is used as a solver for complex probabilistic and phenomenological models of risks by allowing consideration of all logically possible alternative sequences of relationships among defined levels. (Gerbec, Baldissone, & Demichela, 2016)

8.2 IDDA application in the case study

The case study is the routine procedures of ammonia storage in a plant, where consecutively the chemical will be stocked in little cylinder containers intended to be sold. In the plant mentioned above there are:

- N.2 main tanks for anhydrous ammonia storage
- N.2 pumps
- N.1 sorting framework
- N.1 load line ramps
- N.1 vacuum line
- N.1 download line
- N.1 hydroxide tank
- N.1 electric panel
- N.1 nitrogen line

The first step of the case study is to recognize all the procedures and the operation that are normally performed inside the plant, since the moment when the truck tank containing ammonia arrives in the main gate of the plant. This phase, called task analysis, distinguished eight main tasks:

1. Truck entry
2. Truck connection and filling the main tank
3. End to fill the main tank and disconnection of the truck
4. Truck exit
5. Containers suitability check.
6. Load the containers.
7. Finish to load the containers
8. Movement and stocking of the containers.

Each of the task above contains a different amount of subtasks: there are more than sixty basic event of interest (subtasks) that have been recognized in order to complete the whole procedure. The majority of the identified events are related to some kind of human erroneous actions. For investigating about those actions, the probabilities inserted in the input files have been calculated by using a HEART (Human Error Assessment and Reduction Technique) approach, that is a human error quantification method (Williams, 2015). Part of the failures of the systems are related to equipment failure or their combination with human erroneous actions. All the conditional probabilities for a given basic failure to occurred are in all cases modelled according

to time-at-risk model and anticipated equipment exposure to risk (Gerbec, Baldissone, & Demichela, 2016).

Table 8.1 shows the analysis conducted for all the subtasks related at the main task number one named *"Truck entry"* .

Level	Task Description	If yes	If no	Failure rate	Force
101	Are the documents of the truck driver correct?	102	102	0,00000216	delay
102	Is the entrance gate opened, and can the truck go inside the plant?	103	103	0,00000228	delay
103	Can the driver stop the truck in the intended location?	104	104	0,00000242	delay
104	Is the level of the truck tank correct?	107	105	0,0042	delay/process
105	Is it possible to restore the level in a safe way?	107	106	0,000592	delay/process
106	Can the operation go ahead?	107	end	0,00000216	end of op.
107	Is the truck key in the driving position?	108	108	0,00000232	process
108	Can you turn off the truck engine?	109	109	0,00000256	process
109	Can you connect the earthing?	110	110	0,00000228	process/personnel
110	Is portable shower and is the water bucket in place?	111	111	0,00000296	personnel
111	Are the drawer and the driver wearing the filter mask?	201	201	0,000424	personnel

Table 8.1: Task analysis for ammonia case study

Some of the tasks reported in Table 8.1 are not real procedural risks, but they just present a delay in the process. Moreover, it is necessary to outline that this analysis has not been conducted in a strong detail level: i.e. task 104 reported a general "wrong level" , without specify if the deviation is referred to a high or low level. It is not a leak of information, but it has been decided in order to not overload the information and the system itself, by trying to give a generic explanation of the process. Each question as shown in Table 8.1 is aimed at transporting the analyst from a sequence to another one or, if there are no-possibilities to run away from the hazard, directly to the failure of the system.

. The analysed kind of failures are:

- Process Safety
- Personnel Hazard
- Delay

After the creation of links between sequences, the identification of consequences and the possible kind of failure, it is possible to start to create the input for IDDA in its syntax.

```
!
! TASK 1
!

101 1, 0,00000216 1., 102 102, 'Are the documents of the driver correct?' 'Yes' 'No - Delay'
L 101 1, 192 1 !Delay

102 1, 0,00000228 1., 103 103, 'Is the entrance gate opened, and can the truck go inside the plant?' 'Yes' 'No - Delay'
L 102 1, 192 1 !Delay

103 1, 0,00000242 1., 104 104, 'Can the driver stop the truck in the intended location?' 'Yes' 'No - Delay'
L 103 1, 192 1 !Delay

104 1, 0,0042 1., 107 105, ' Is the level of the truck tank correct?' 'Yes' 'No - Delay and process safety'
L 104 1, 192 1 !Delay
L 104 1, 190 1 !Process Safety

105 1, 0,000592 1., 107 106, ' Is it possibile to restore the level in a safe way?' 'Yes' 'No - Delay and process safety'
L 105 1, 192 1 !Delay
L 105 1, 190 1 !Process Safety

106 1, 0,0042 1., 107 193, ' Can the operation go ahead?' 'Yes' 'No - End of operations'
L 106 1, 193 1 !End of operations

107 1, 0,00000232 1., 108 108, ' Is the truck key in the driving position?' 'Yes' 'No - Process Safety'
L 107 1, 190 1 !Process Safety

108 1, 0,00000256 1., 109 190, 'It is possibile turn off the engine?' 'Yes' 'No - Process Safety'
L 108 1, 190 1 !Process Safety

109 1, 0,0000028 1., 110 110, 'Is the earthing connected?' 'Yes' 'No - Process safety and Personnel hazard'
L 109 1, 190 1 !Process Safety
L 109 1, 191 1 !Personnel Hazard

110 1, 0,00000296 1., 111 111, 'Is the portable shower and is the water bucket in place?' 'Yes' 'No - Personnel hazard'
L 110 1, 191 1 !Personnel hazard

111 1, 0,000424 1., 201 201, 'Is the personnel wearing the filter masks?' 'Yes' 'No - Personnel hazard'
L 111 1, 191 1 !Personnel hazard

190 1, 0. 1, 191 191, 'T1 Process safety?' 'No' 'Yes'
L 190 1, 290 1
L 190 1, 1000 1
A 190 1, 191, 1000 1000

191 1, 0. 1, 192 192, 'T1 Personnel Hazard?' 'No' 'Yes'
L 191 1, 291 1
L 191 1, 1001 1
A 191 1, 192, 1000 1000
```

By choosing *Level 109* from the input structure above, it is possible to analyse every single number easily.

```
109 1, 0,0000028 1., 110 110, 'Is the earthing connected?' 'Yes' 'No - Process safety and Personnel hazard'
L 109 1, 190 1 !Process Safety
L 109 1, 191 1 !Personnel Hazard
```

- The first number, *"109"*, represents the level numerical label. It has to be and integer
- The second number, *"1"*, is the level order and it represents the number of the possible level failure modes, it has to be an integer having value in the range 1-8
- The third number, *"0.0000028"*, is the failure modes probability. It must be a real number
- The fourth number, *"1."*, is the failure modes probability uncertainty ratio. In the reliability problems the analyst uses the failure rate to provide the failure probability assessment in a given analyst period
- The fifth number, *"110"*, is the next level address in case of success of the level
- The sixth number, *"110"*, is the next level address in case of fail of the level

In the second row of the structure the letter *"L"* represents a logical constraint that allow to compelled run time the output of the constrained level, as the effect of a level give output achievement. In the logical constraint constructions there are the following fields:

- *"L"* is the logical constraint
- *"109"* is the level index, therefore is the level which outputs activate the constraint
- *"1"* activation word flag, identifies the outputs that activate the change.
- *"190"* target level index, therefore the level which output must be forced
- *"1"* forced target level output word flag,

In the specific case of a failure of the reported level 109, there are two possible logical constraints: one of them is referred to process safety, the other one to a personnel hazard.

IDDA permits the users to choose between different constraints:

- Logical constraint
- Probabilistic constraint
- Bayes constraint
- Time Factor constraint
- Time Factor Variation constraint
- Mission time reset constraint
- Constraints clear constraint
- Link constraint

The probabilistic constraint allows to change expectation degree spreading relevant to a constrained level, changing its failure mode probability values as the effect of a level given output achievement. The Bayes constraint allows to change the expectation degree spreading relevant to a constrained level, modifying the probability of its outputs based on their likelihood, given a level output achievement. The time factor constraint is defined as "time dependent" a set of failure modes. It results are useful when it analyses a system in a given time window, therefore it is possible to use this facility to represent failure modes having a critical time and to inspect possible contemporary critical events. The Time factor variation constraint allows to change the time factor value relevant to constrained time dependent level outputs, as the effect of a level given output achievement. The mission time reset constraint allows to set the current mission time value as the effect of a level given output achievement. The mission time represents the current size of the relative time window on which you are interested in verifying level output occurrences. The "constraints clear constraint" allows to reset all the constraint effects produced during the previous sequence evolution. This constraint restores the probability, the uncertainty ratio, the next level address and the time factor initial values of all the constrained levels. Last but not the least, the link constraint can link a level to an event file that explains the values of the logical and the probabilistic parameters. All the changes described above are performed during run time. (Software Oriented System Engineering, 1996-200)

Table 8.2 reports the overall probabilities for delays, personnel hazard and process safety risk categories.

The overall probabilities suggest that at least one type of risk will occur is about 61%. It is important to notice that the *delays* are much more likely to occur than the other kind of risk. In fact, there is a probability of 55% that a delay occurs, instead the probability of a personal hazard is not more than 10% and the probability of a risk related to the process is less than 5%.

Risk Category	**Probabilities**
Delays	0,55
Personnel Hazard	0,094
Process Safety	0,038
Overall	0,608

Table 8.2: Overall results for the IDDA case study and probabilities related to each consequence.

The SPACCO model related to the case study generates a list of all alternative accident sequences leading to an enormous number of events. For the practical reasons a cut-off criterion can be specified, meaning that all alternative sequences with the resulting probability lower than criteria are omitted from further consideration (Gerbec, Baldissone, & Demichela, 2016).

Table 8.3 shows the details of the cut-off criteria.

Risk Category	Cut-off criteria	Number of the alternative sequences	Residual Probability
Delays	5×10^{-14}	8.295.957	$2{,}60 \times 10^{-7}$
Personnel Hazard	0	339	0
Process Safety	0	84	0

Table 8.3: Number of the alternative sequences, their applied probability cut-off criteria and the residual probability

Other possible results obtained from IDDA and its functional analysis have not been conducted in those case study.

8.3 Further information available from IDDA

Below it is shown a part of further information that is possible to obtain from the integrated decision analysis of another case study reported in literature. First of all, it is worth to keep in mind that a well-built IDDA input provides an *Original* and an *Optimized* version. That information is necessary to understand why in Figure 8.2 below it is shown the aggregation of the risk for the main task for the *Original* and the *Optimized* version.

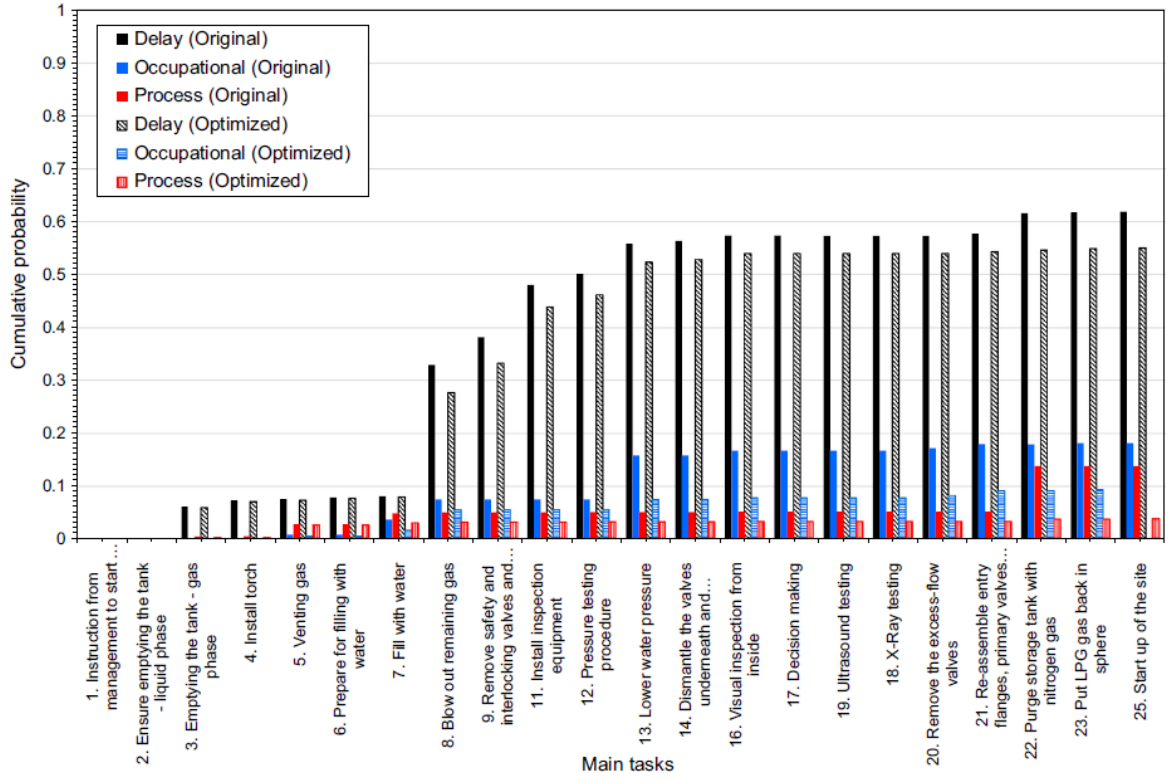

Figure 8.2: Results that are possible to obtain from IDDA

The risk is divided for three different categories that are aggregated at main task level. It is possible to notice from Figure 8.2 that a massive amount of alternative procedures outcomes is considered and that minor residual probabilities applied only for delay risk category (Gerbec, Baldissone, & Demichela, 2016).

Further information that are possible to obtain from IDDA are firstly the duration of each of the procedural alternative and secondly the monetary value at risks are considered.

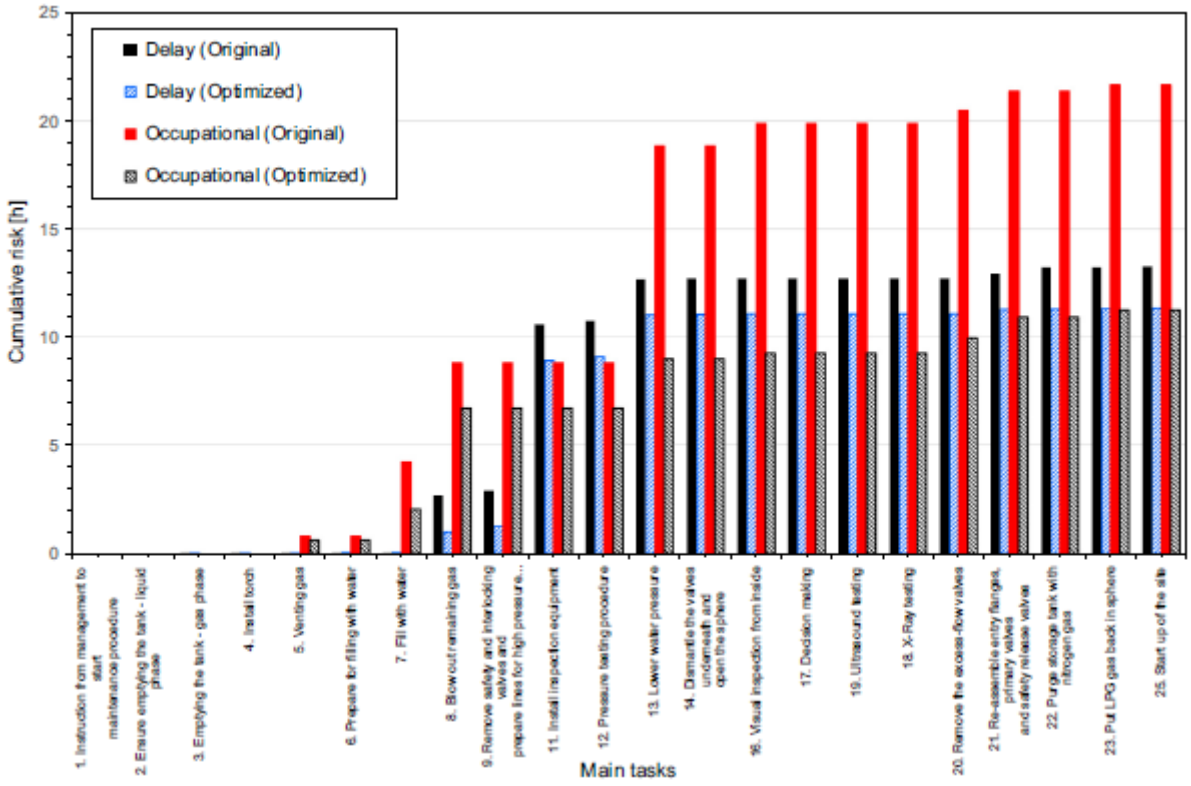

Figure 8.3: Cumulative delay risk profile

Figure 8.3 shows the delay for occupational safety risk. The process safety risks are noted but excluded from the estimation of expected delays because usually they lead to equipment damage and very long shutdowns. By the optimization of the process, in the analysis conducted in the case study which we are referring, has been possible a 7% reduction of the potential total delay.

The monetised cost of implementing test procedures considering both alternatives (the original and the optimized version) shows a strong reduction with a total assessed difference in related costs is about -40% as it is shown in Figure 8.4 below. Furthermore, it is possible to display the monetised cost in a bar chart. In both cases in the analysis conducted has been outlined as within 14 events the most important gains come from two events.

Category[a]	Item category	Procedure specific costs (€)	
		Original	Optimized
Direct costs			
1.1.1	Procedure (work & material)	70,918	69,976
1.1.2	Lost production at planned duration	54,886	52,747
Values at risk			
2.1.1	Lost production from delays[b]	1255	1093
2.2.1	Lost production from occupational accidents[c]	3214	1668
2.2.2, 2.2.3	Lost GDP from occupational accidents[d,e]	8970	3147
2.3.1.1	Direct damage from process safety accidents[f]	132,274	33,335
2.3.2.1	Indirect damage from process safety accidents	(not evaluated[g])	
	Total	**271,517**	**161,966**
	Index	100	59.7

Figure 8.4: Summary of monetised cost of implementing test procedure

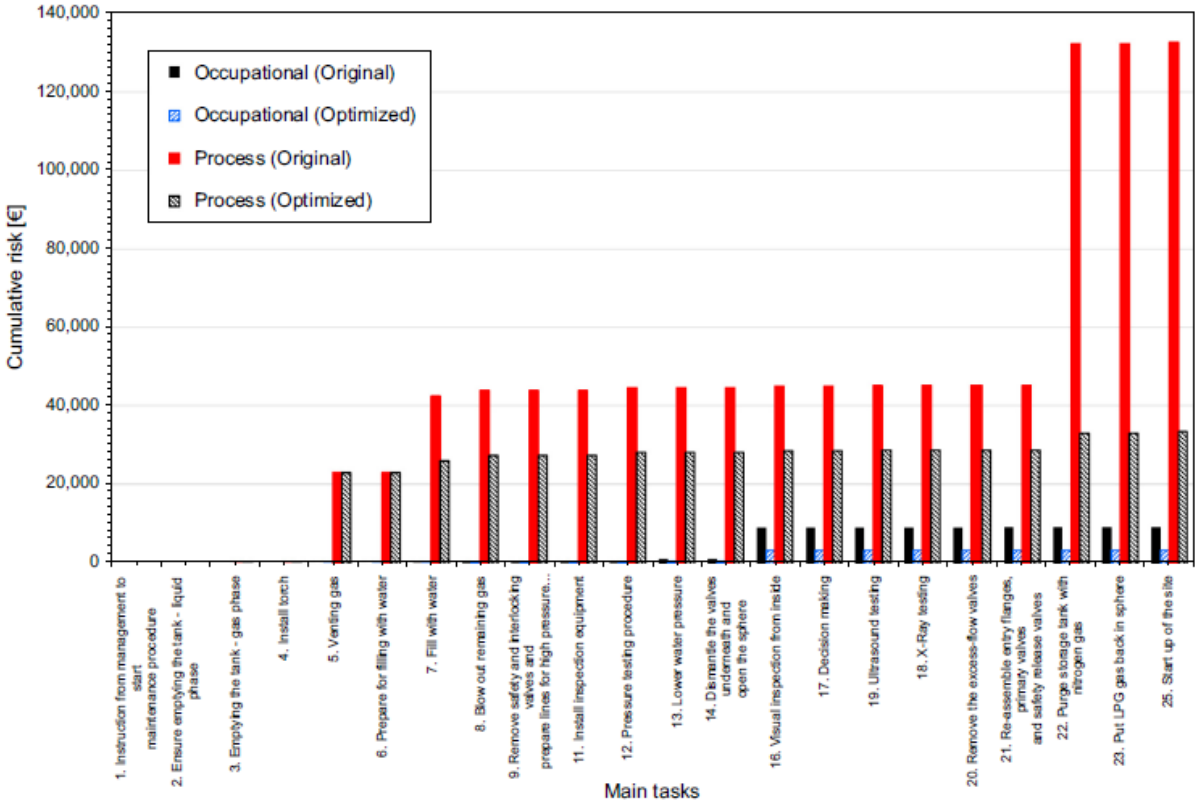

Figure 8.5: Cumulative monetarized damages risk profiles for both procedure alternatives

9. Interim results and future work

This work tried to analyse the features that a web-based tool for operational risk management needs. For that reason, a quantitative and qualitative analysis has been conducted by using two different case studies: the development of a new prototype based on Tosca Risk register and a functional analysis of procedures by using a dynamic decision analysis software. This work integrates the previous knowledge in the literature related to risk reporting and the advanced software technology and user-friendly interface software.

The new risk register developed by Tosca Human Factor Solution in collaboration with DIT, introduces a new concept of risk register, by using a user-friendly interface and technological features that do not exist in other commercial software. This innovative risk register helps the goal to provide a real-time support and a description for routine procedures aimed at performance improvement and predictive risk management. As already stated the risk register is used as a real time sign off for the procedures and delivered workload management support and it gives the possibility to report quickly any possible risk, anomalies or event that inside the plant. Therefore, the new system presents the advantage of perfect integration in a pre-existing workflow. Several industries around the world are asking for to purchase the last version of the Tosca risk register, in order to have an innovative tool which effectiveness is ensured. Some key factors in the risk registers have been relevant for its success:

1. Enthusiasm and positive attitude of many stakeholders and companies, the desire to obtain a new tool for a change of risk assessment and a new way of supporting their operations and the appraisal of their risk treatment, different from the obsoleted method of risk reporting.
2. Continuous support, proactive and positive attitude toward the tool which is also used to put in order the sequences of procedures and tasks inside the plant in order to have a clear overview of the system
3. The opportunity of take care of records of information collected over time.

On the other hand, the development of the prototype for the power generation company has improved the capacity of the analysts to modify and tailor the existing risk register for the needs of different companies. The amount of work behind the construction of the prototype is a very important part of this thesis, that involved several hours for discussions with the risk project manager of the Irish company.

However, in the next stages of the prototype project it is necessary to permit the user to:

- Import/export of data across the new tool and GRR and CAR to allow the user to check the information in a spreadsheet in which it is familiar.
- Add *non-technical risks* in the software by taking data from GRR.
- Organize the *Roll-up* section in order to avoid leakage of information and keeping as much as possible traceable data inside the system.

Moreover, it is necessary to complete the module of *Option Evaluation* with bar charts and graphics that allows the users to have a practical and easier to understand view of all the investment options that have been inserted into the system.

Concerning the functional analysis, it is necessary to remind that in the risk register some of the risks are related to tasks being carried out. Those tasks can be analysed using task analysis as a mean of functional analysis, where every step needs to lead to either another step or an event or a final state. The method that can be used is a dynamic event tree where the probability of outcomes could be estimated on the basis of existing databases values or using the data stored in the risk register if the tasks are also used to inform the checklist where operators can report anomalies related to each step (Leva & Builes, The benefits of task and cognitive workload support for operators in grund handling, 2017).

The results of the tasks analysis for the case study show that the overall probabilit of uncertain events happened has a very high value (61%). It is necessary to outline that the most relevant part of those uncertain events is led from delays (55%) and the personnel hazard and process safety represent together less than 15% of probability. The use of a probabilistic model such as IDDA guarantees consistency and completeness in a risk assessment used as a basic for a proper plant design. It is possible to obtain more information by using IDDA with the modules related to the monetised risk value and the global delay. Those features, linked to the others already developed for the prototype, will bring the level of a risk register used for operational and technical risk to a new and unique level of detail and completeness, usable from all the kind of companies and organizations.

References

Baccarini, D., & Archer, R. (2001). The risk ranking of projects: A methodology. *International Journal of Project Management*, 139-145.

Baldissone, G., Fissore, D., & Demichela, M. (2016). Catalytic after-treatment of lean VOC-air streams: Process intensification vs. plant reliability. *Process safety and Environmental Protection, 100*, 208-219.

Balfe, N., Leva, M., Mc.Aleer, B., & Rocke, M. (2014). Safety Risk Registers: Challenges and Guidance. *CET: Chemical Engineering Transactions*, 571-576.

Bruce, Hancock, T., Morin, J.-M., & Carter, N. (1996). *Introducing Riskman: The European Project Risk Management Methodology.* Blackwell Pub; New Ed Edition.

Cox, L. A. (2008). What's Wrong with Risk Matrices? *Society for Risk Analysis*, 497-512.

Crossland, R., McMahon, C., & Williams, J. (2001). Suvery of current practice in managing technical desing risk. *Proc. 13th International Conference Engineering Design ICED01* (pp. 585-592). Glasgow: Professional Engineering Publishing.

Dağsuyu, C., Göçmen, E., Narlı, M., & Kokangül, A. (2016). Classical and fuzzy FMEA risk analysis in a sterilization unit. *Computer & Industrial Engineering*, 286-294.

Demichela, M., Baldissone, G., & Gianfranco, C. (2017). Risk-Based Decision Making for the Management of Change in Process Plants: Benefits of Integrating Probabilistic and Phenomenological Analysis. *Industrial & Engineering Chemistry Research 56(50)*, 14873-14887.

Demichela, M., Piccinini, N., & Romano, A. (2004). Risk analysis as a basis for safety management system. *Journal of Loss Prevention in the Process Industries*, 179-185.

Gerbec, M., Baldissone, G., & Demichela, M. (2016). Design of procedures for rare, new or complex processes: Part 2 – Comparative risk assessment and CEA of the case study. *Safety Science*, 100, 203-215.

Hasle, J., Kjellen, U., & Haugerud, O. (2009). Decision on oil and gas expoloration in Arctic Area: Case study from the Norwegian Barents Sea. *Safety Science*, pp. 832-842.

ISO 31000. (2009, 11 15). International Standard ISO 31000. *Risk Management - Priciples and guidelines*.

ISO 31010. (2009, 10 09). International Standard IEC/FDIS 31010. *Risk Management - Risk assessment techniques*.

ISO 55001. (2014). International Organization of Standardization ISO 55001. *Asset management-Management System Requirements*.

J O'Neill, N. T. (2007). Technical risk assessment: a practitioner's guide. Edinburgh , South Australia, Australia: Defence Systems Analysis Divisoin.

Lambert. (2001). Indentification, ranking, and management of risks in a major system acquisition. *Reliability Engineering and System Safety*, pp. 315-325.

Leva, M., & Builes, Y. (2017). The benefits of task and cognitive workload support for operators in grund handling. *International Symposium on Huma Mental Workload: Models and Applications*, pp. 225-238.

Leva, M., Balfe, N., Mc.Aleer, B., & Rocke, M. (2017). Risk registers: Structuring data collection to develop risk intelligence. *Safety Science*, 143-156.

Li, Y., & Guldenmund, F. W. (2018). Safety management systems: A broad overview of the literature. *Safety Science*, 94-123.

Patterson, F. D., & Neailey, K. (2002). A Risk Register Database Syste, to aid the management of prokect risk. *International Journal of Project Managament*, 365-374.

Randell, R., Wilson, S., & Woodward, P. (2011). The importance of the verbal shift handover report: a multi-site case study. *International Journal of Medical Informatics*, 803-812.

Reiss, G. (2007). *Project Management Demystified.* New York: Taylor & Francis.

Software Oriented System Engineering. (1996-200). *IDDA 2.1 USER GUIDE.*

Tamimi, I., Beullens, D. P., & Sadnicki, S. (2016, Nov. 23-24). Quantifying the benefits of investment portfolio optimisation versus prioritisation for asset intensive organisations. London, UK: IET.

UNI. (1991, 10 31). UNI 9910:1991. *Terminologia sulla fidatezza e sulla qualità del servizio*. Italy.

Webb, A. (2003). *The Project Manager's Guide to Handling Risk.* London: Routledge.

Williams, J. (2015). Heart—A Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology. 5-25.