



Corso di SICUREZZA NEL TRASPORTO E NELLE INFRASTRUTTURE STRATEGICHE

*Metodologie di Valutazione e Gestione del
Rischio - parte b*



Cpt. Claudia Brisotto
claudia.brisotto@me.com





Risk Management

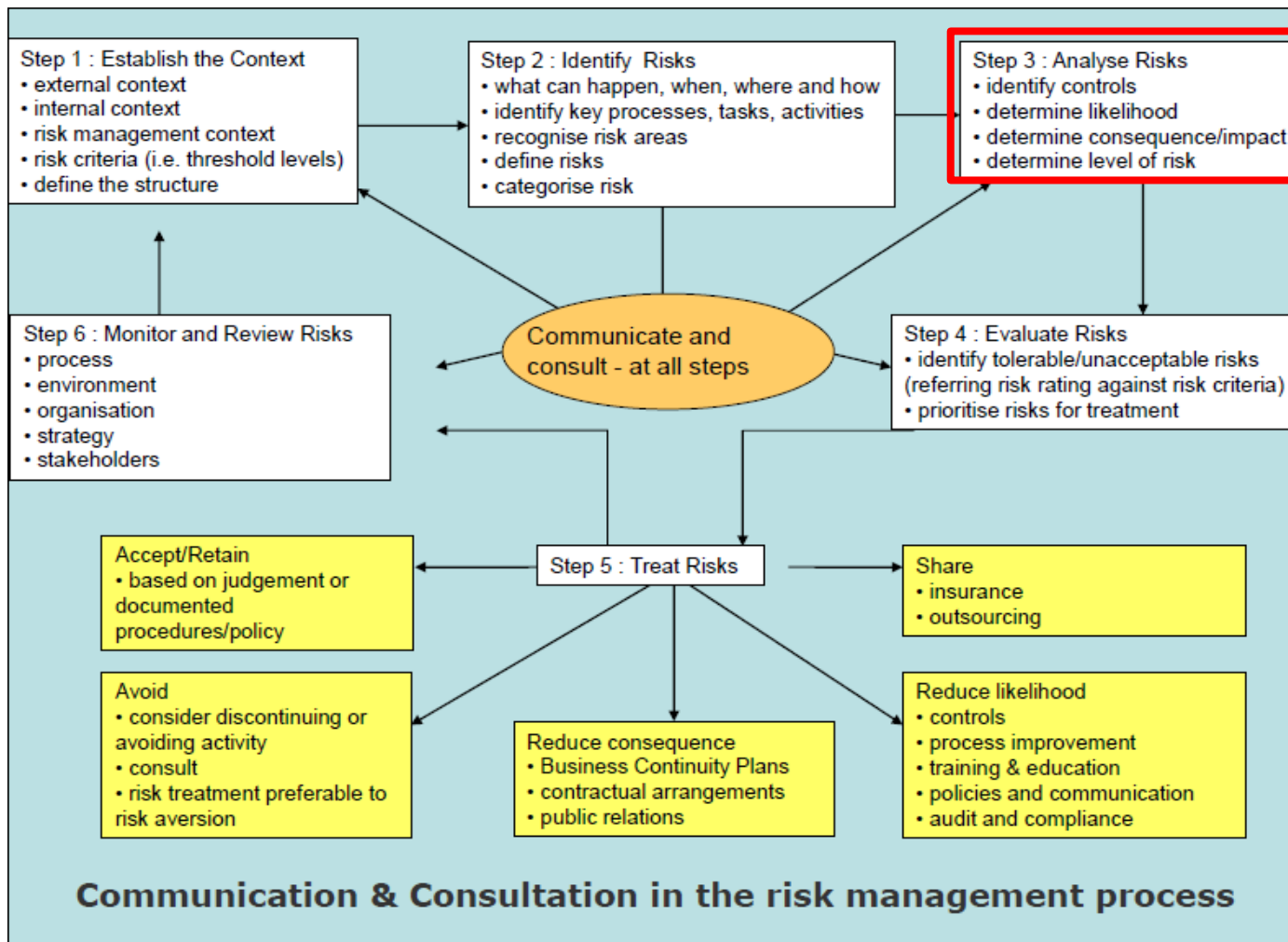
ISO 31010

Risk analysis



Risk Management

ISO 31010





Risk Management

ISO 31000

Definizioni

Analisi del rischio:

- Processo di comprensione della natura del **rischio** e di determinazione del **livello di rischio**
- L'analisi del rischio fornisce la base per la **ponderazione del rischio** e le decisioni circa il **trattamento del rischio**
- L'analisi del rischio comprende la **misurazione del rischio**.





Risk Management

ISO 31010

Risk analysis

L'analisi del rischio consiste nel **determinare le probabilità e le loro conseguenze** di eventi di rischio identificati, **tenendo conto della presenza (o meno) e dell'efficacia di qualsiasi controllo esistente.**

Le conseguenze e le loro probabilità vengono poi combinate per determinare un livello di rischio.



Risk Management

ISO 31010

Risk analysis

L'analisi del rischio comprende

- La **considerazione delle cause e delle fonti di rischio**, le loro **conseguenze e la probabilità** che tali conseguenze possano verificarsi.
- **Fattori che influenzano** le conseguenze e la probabilità devono essere identificati.
- **Il fatto che un evento possa avere molteplici conseguenze e possa influenzare più obiettivi.**
- **I controlli (barriere)*** del rischio esistenti e la loro efficacia

Più di una tecnica può essere richiesta per applicazioni complesse.



Risk Management

ISO 31010

Risk analysis

I metodi utilizzati nell'analisi dei rischi possono essere **qualitativi, semi-quantitativi o quantitativi.***

Il **grado di dettaglio richiesto** dipenderà dalla particolare **applicazione, dalla disponibilità di dati affidabili e dalle esigenze decisionali dell'organizzazione.** *

Alcuni metodi e il grado di i dettagli dell'analisi possono essere **prescritti dalla legislazione.**



Risk Management

ISO 31010

Risk analysis

La valutazione **qualitativa** definisce le conseguenze, la probabilità e il livello di rischio per **significatività** come livelli "**alto**", "**medio**" e "**basso**", può unire conseguenze e probabilità, e valuta il **livello di rischio risultante rispetto ai criteri qualitativi**.

I metodi **semi-quantitativi** usano scale di **valutazione numerica per conseguenze e probabilità** e combinano tali dati per produrre un livello di rischio utilizzando una formula. Le **scale possono essere lineari o logaritmiche, o avere qualche altra relazione**; le formule utilizzate possono anche variare.



Risk Management

ISO 31010

Risk analysis

L'analisi **quantitativa** stima valori pratici delle conseguenze e le loro probabilità, e produce valori del livello di rischio in unità specifiche definite durante la definizione del contesto.

L'analisi quantitativa potrebbe **non essere sempre possibile o auspicabile** a causa di **informazioni insufficienti** sul sistema o sull'attività analizzata, **mancanza di dati**, influenza dei **fattori umani**, ecc. o perché lo sforzo dell'analisi quantitativa non è giustificato o richiesto.

In tali circostanze, una **graduatoria comparativa semi-quantitativa o qualitativa** dei rischi da parte di specialisti, esperti nel loro rispettivo campo, può essere ancora efficace.





Risk Management

ISO 31010

Risk analysis

Fasi dell'analisi

- Valutazione dei controlli (barriere)
- Analisi delle conseguenze
- Analisi di verosimiglianza e stima della probabilità
- Analisi preliminare
- Incertezze e sensibilità



Risk Management

ISO 31010

Risk analysis

Valutazione dei controlli (barriere)

Il livello di rischio dipenderà dall'adeguatezza e dall'efficacia dei controlli (barriere) esistenti.

Le domande da affrontare includono:

- quali sono i **controlli esistenti** per un particolare rischio?
- sono in grado di **trattare adeguatamente** il rischio in modo che sia controllato ad un livello tollerabile?
- in fase pratica, i controlli **funzionano nel modo previsto** e può essere dimostrata la **loro efficacia**?

A queste domande si può rispondere con sicurezza solo se ci sono documentazione adeguata e processi di garanzia in atto.

Il livello di efficacia per un particolare controllo, o un insieme di controlli correlati, può essere espresso **qualitativamente, semi-quantitativamente o quantitativamente.**

Risk Management

ISO 31010

Risk analysis

Analisi delle conseguenze

L'analisi delle conseguenze determina la natura e il tipo di impatto che potrebbe verificarsi ipotizzando che si verifichi un particolare evento o circostanza.

Un evento può avere una gamma di impatti di diversa ampiezza, e influire su obiettivi e parti interessate diversi.

I tipi di conseguenze da analizzare e le parti interessate devono essere stabiliti in fase di contesto.

Gli impatti possono **avere una bassa conseguenza ma alta probabilità**, o una **conseguenza alta e bassa probabilità**, o qualche risultato intermedio. In alcuni casi, è opportuno concentrarsi sui rischi con esiti potenzialmente molto grandi, in quanto questi sono spesso di maggiore preoccupazione per il Management .* MA....



Risk Management

ISO 31010

Risk analysis

Analisi delle conseguenze ...

L'analisi delle conseguenze può comportare:

- prendere in considerazione i controlli esistenti, tutti fattori contributivi rilevanti che possono influire sulle conseguenze;
- correlare le conseguenze del rischio agli obiettivi originari;
- considerare sia le **conseguenze immediate sia quelle che possono insorgere dopo un certo tempo, (LATENTI)***
- considerare le **conseguenze secondarie**, come quelle che hanno un impatto sui sistemi associati, attività, attrezzature o organizzazioni.



Risk Management

ISO 31010

Risk analysis

Analisi di verosimiglianza e stima della probabilità

Tre metodi generali sono comunemente impiegati per stimare la probabilità; possono essere usati individualmente o congiuntamente:

a) L'uso di **dati storici rilevanti** per identificare **eventi o situazioni che si sono verificati in passato e quindi essere in grado di estrapolare la probabilità del loro verificarsi in futuro.**

I dati utilizzati devono essere **pertinenti** al tipo di sistema, struttura, organizzazione o attività considerati e anche agli standard operativi dell'organizzazione .

Se **storicamente** c'è una **frequenza molto bassa** di occorrenza, avremo che qualsiasi **stima di probabilità sarà incerta.**

Questo vale soprattutto quando non abbiamo **alcun report (zero occurrence)*** quando non è possibile presumere che l'evento, la situazione o le circostanze non si verifichino in futuro.

Risk Management

ISO 31010

Risk analysis

Analisi di verosimiglianza e stima della probabilità ...

b) Previsioni di probabilità utilizzando **tecniche predittive** come l'analisi ad albero dei guasti e l'analisi ad albero di eventi.

Quando i **dati storici** non sono disponibili o inadeguati, è **necessario ricavare le probabilità mediante analisi del sistema**, attività, attrezzatura o organizzazione e relativi stati di fallimento o successo.

Dati numerici, dall'esperienza operativa o dati pubblicati, riguardanti attrezzature, essere umano, organizzazioni e sistemi **vengono poi combinate per produrre una stima della probabilità dell'evento principale**.

Possono essere richieste **tecniche di simulazione** per generare **probabilità di guasti** di apparecchiature e strutturali dovuti all'invecchiamento e ad altri processi di degradazione.

Risk Management

ISO 31010

Risk analysis

Analisi di verosimiglianza e stima della probabilità ...

c) L'opinione degli esperti può essere utilizzata in un processo sistematico e strutturato per **stimare la probabilità**.

I giudizi degli esperti dovrebbero **attingere** a **tutte le informazioni disponibili pertinenti, comprese quelle storiche, sistema specifico, organizzativo-specifico, sperimentale, design, ecc.**

Ci sono un certo numero di **metodi formali per sollecitare il giudizio di esperti** che forniscono un aiuto alla formulazione di domande appropriate.

I metodi disponibili includono l'approccio Delphi, il confronto abbinato, il rating di categoria e giudizi di probabilità assoluta.

Risk Management

ISO 31010

Risk analysis

Analisi preliminare

I rischi possono essere esaminati per **identificare** i rischi più significativi o per **escludere** i meno significativi o minori da ulteriori analisi.

Lo scopo è quello di garantire che le **risorse saranno focalizzate sui rischi più importanti**.

Bisogna fare attenzione a **non escludere rischi bassi che si verificano frequentemente** e hanno un significativo **effetto cumulativo**

Lo screening dovrebbe essere basato su criteri definiti nel contesto.

L'analisi preliminare determina uno o più dei **seguenti corsi d'azione**:

- decidere di **trattare** i rischi **senza ulteriori valutazioni**;
- **accantonare** rischi insignificanti che non giustificerebbero il trattamento;
- procedere con una **valutazione del rischio più dettagliata**.

Le ipotesi e i risultati iniziali dovrebbero essere documentati.



Risk Management

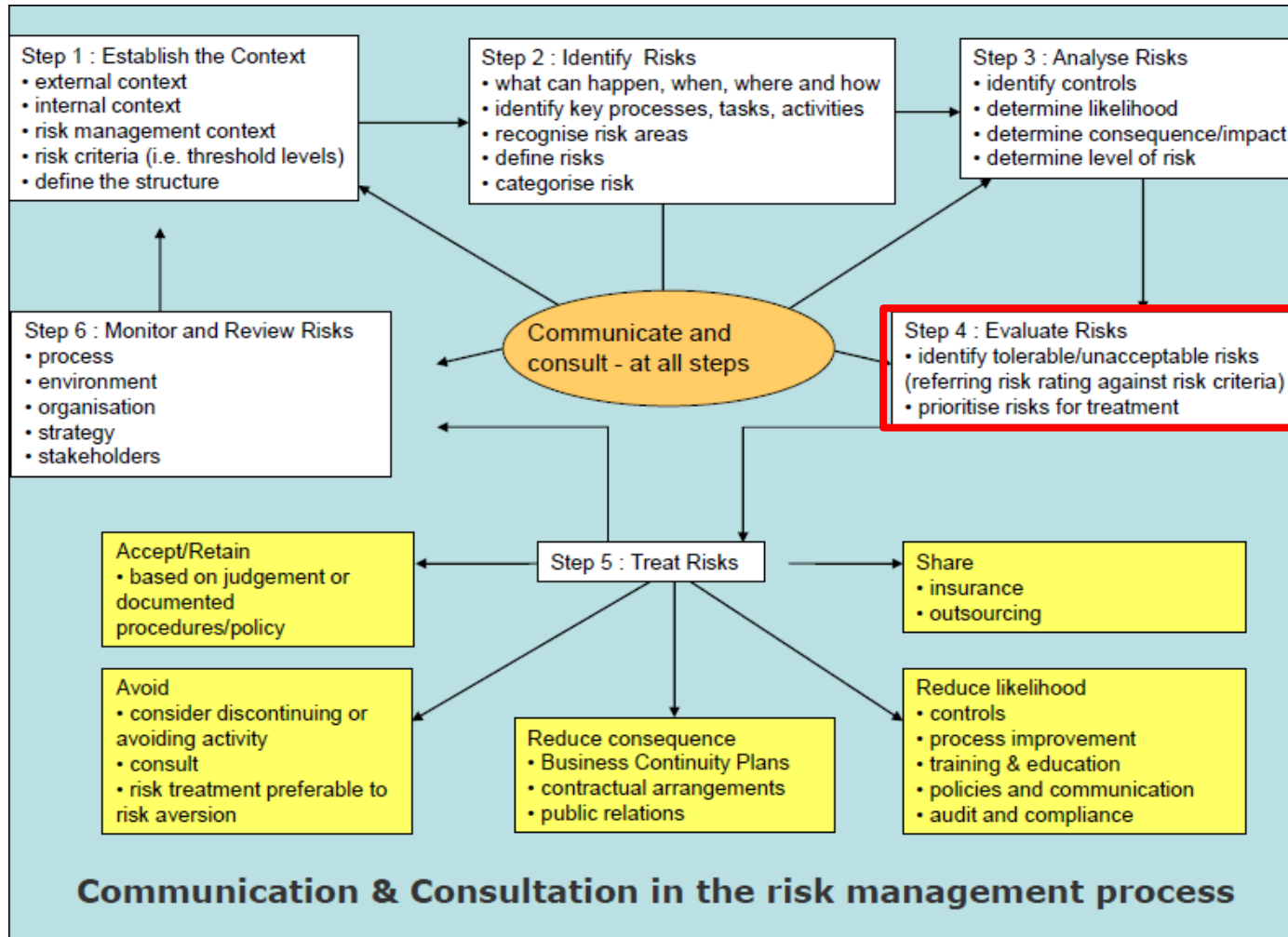
ISO 31010

Risk evaluation



Risk Management

ISO 31010





Risk Management

ISO 31000

Definizioni

Risk evaluation (Ponderazione)

Ponderazione del rischio:

- **Processo di comparazione** dei risultati dell'**analisi del rischio** rispetto ai **criteri di rischio** per determinare se il **rischio** e/o la sua **espressione quantitativa sia accettabile o tollerabile.**
- La ponderazione del rischio agevola la decisione circa il **trattamento del rischio**



Risk Management

ISO 31010

Risk evaluation (Ponderazione)

La valutazione del rischio comporta il **confronto dei livelli di rischio stimati con i criteri di rischio definiti nel contesto**, al fine di determinare l'importanza del livello e del tipo di rischio.

La valutazione del rischio **utilizza la comprensione del rischio ottenuto durante l'analisi del rischio per prendere decisioni sulle azioni future.**

Considerazioni etiche, legali, finanziarie e di altro tipo, compresa la percezione di rischio, sono anche input decisionali.

Le decisioni possono includere:

- **se** un rischio **richiede** un trattamento;
- **priorità** per il trattamento;
- se un'**attività** debba essere **intrapresa**;
- **quale percorso** debba essere seguito.

Risk Management

ISO 31010

Risk evaluation ...

La decisione su se e come trattare il rischio può **dipendere dai costi e benefici di assumersi il rischio** e i **costi e i benefici derivanti dall'implementazione di controlli migliorati**.

Un approccio comune consiste nel dividere i rischi in **tre fasce**:

1. una fascia superiore in cui il livello di rischio è considerato **intollerabile**, qualunque sia il beneficio, **l'attività può comportare rischi** e il **trattamento è essenziale indipendentemente dal costo**;
2. una fascia media (o un'area grigia) in cui vengono presi in considerazione **costi e benefici, opportunità bilanciate contro le potenziali conseguenze**;
3. una fascia inferiore in cui il livello di rischio è **considerato trascurabile**, o così piccolo che **non sono necessarie misure di trattamento**



Risk Management

ISO 31010

Risk evaluation ...

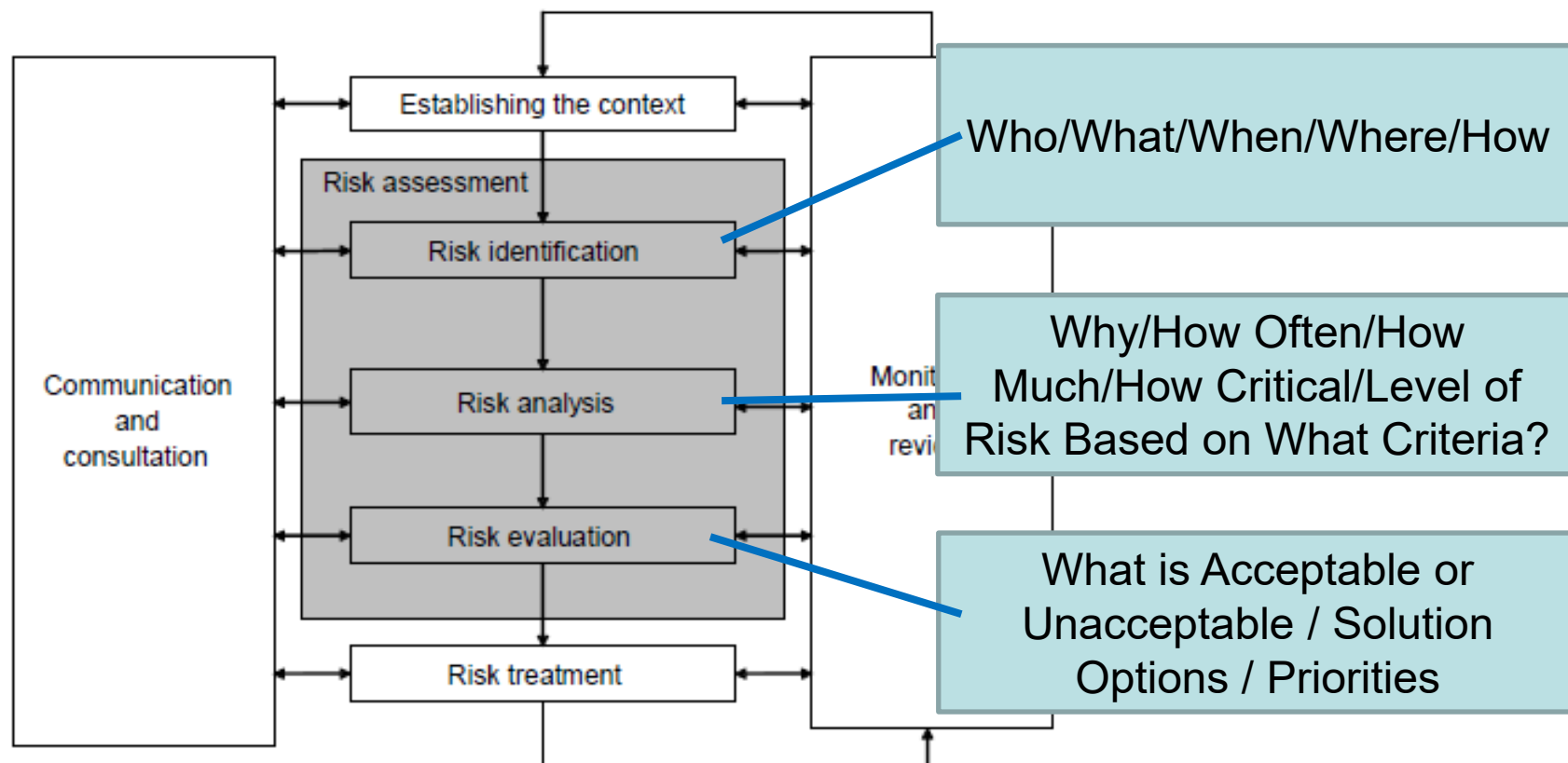
Il sistema di criterio '**as low as reasonably practicable**' o **ALARP** utilizzato nelle applicazioni di **sicurezza** segue questo approccio, dove, nella **fascia centrale**, ci sono rischi relativamente bassi dove costi e benefici possono essere confrontati direttamente, mentre per i **rischi elevati il potenziale di danno deve essere ridotto, fino a quando il costo di un'ulteriore riduzione è del tutto sproporzionato rispetto al beneficio della sicurezza ottenuto.**



Risk Management

ISO 31010

Risk assessment process







Risk Management

ISO 31010

SELECTION OF RISK ASSESSMENT TECHNIQUES





Risk Management

ISO 31010

Selection of risk assessment techniques

La valutazione del rischio può essere effettuata in **vari gradi di profondità e dettaglio** e utilizzando **uno o molti metodi** che vanno dal semplice al complesso.

In termini generali, le **tecniche appropriate** dovrebbero presentare le seguenti caratteristiche:

- dovrebbe **essere giustificabile e appropriata** alla situazione o all'organizzazione in esame;
- dovrebbe **fornire risultati in una forma che migliori la comprensione** della natura del rischio e come possa essere trattato;
- dovrebbe essere in grado di essere **utilizzata in modo tracciabile, ripetibile e verificabile.**



Risk Management

ISO 31010

Selection of risk assessment techniques

Una volta che è stata presa la decisione di eseguire una valutazione del rischio e, gli obiettivi e il campo di applicazione sono state definiti, le tecniche dovrebbero essere selezionate, in base a fattori applicabili quali:

- gli **obiettivi** dello studio
- i **bisogni** dei responsabili delle decisioni
- il **tipo e la gamma** di rischi analizzati
- l'entità potenziale delle **conseguenze**
- il **livello di esperienza, risorse** (umane e altre necessarie)
- la **disponibilità di informazioni e dati**
- la **necessità di modificare / aggiornare** la valutazione del rischio.
- eventuali **requisiti normativi e contrattuali**
- **disponibilità di risorse**
- **complessità**
- se il metodo può fornire un **output quantitativo**.

Risk Management

ISO 31010

Risk Assessment Considerations

Quando si considerano i rischi per rilevanza e importanza, le seguenti **variabili "materiali"** possono aiutare:

qualitative

- **Verosomiglianza:** frequenza, frequenza relativa o probabilità
- **Gravità(severita')**: l'impatto delle conseguenze (può essere espresso in più termini: finanziario, umano, reputazione, proprietà, capacità di continuare le operazioni, ..)
- **Tempistica:** velocità di inizio (velocità), quando si verifica l'evento / tendenza (trigger), quanto dura (durata)
- **Vulnerabilità:** suscettibilità legata alla preparazione, all'agilità e all'adattabilità dell'entità

quantitative

- **Valore atteso:** media, modalità o mediana per previsioni, budget
- **Variabilità:** intervallo, deviazione standard e distribuzione di probabilità
- **Rapporti:** quanto di una cosa ci sia rispetto ad un'altra cosa.



Risk Management

ISO 31010

Applicabilità degli strumenti utilizzati per la valutazione del rischio

[table 1 tools.pdf](#)

[table 1 tools.docx](#)



Risk Management

ISO 31010

Qualità della selezione di strumenti di valutazione del rischio

Ricordiamo

Fattori che influenzano la selezione delle tecniche di valutazione del rischio e che ne descrivono i termini:

- **complessità** del problema e **metodi** necessari per analizzarlo,
- la **natura e il grado di incertezza** della valutazione del rischio sulla base della **quantità di informazioni disponibili** e di quanto è necessario per soddisfare gli obiettivi,
- **l'entità delle risorse necessarie** in termini di tempo e livello di esperienza, necessità o costo dei dati,

Inoltre..

- se il metodo può fornire un output **quantitativo**.



Risk Management

ISO 31010

Qualità degli strumenti di valutazione del rischio

Sono suddivisi in :

- metodi di ricerca
- metodi di supporto
- analisi di scenario
- analisi della funzione
- valutazione dei controlli (barriere)
- metodi statistici

Vengono descritti in funzione dell'influenza che i fattori hanno su di loro

[Type of risk assessment technique.pdf](#)

[Type of risk assessment technique.docx](#)





Risk Management

ISO 31010

FMEA

(Failure Mode and Effect Analysis)





Risk Management

ISO 31010

FMEA

FMEA (Failure Mode and Effect Analysis) è una tecnica che identifica **le modalità di guasto, di difetto o di evento di un processo, prodotto o sistema.**

Esistono **diversi tipi di FMEA**: **Design** FMEA utilizzato per componenti e prodotti, **System** FMEA utilizzato per i sistemi, **Process** FMEA utilizzato per processi di produzione e assemblaggio, **Service** FMEA e **Software** FMEA.

FMEA può essere seguito da **un'analisi di criticità** che definisce il significato di ciascuna **modalità di errore, qualitativamente, semi-qualitativamente o quantitativamente** (FMECA). L'analisi della criticità può essere basata sulla probabilità che la modalità di errore comporti un errore del sistema, o il livello di rischio associato alla modalità di errore o un numero di priorità del rischio



Risk Management

ISO 31010

FMEA...

Il Processo di Analisi FMEA si basa prevalentemente sulla possibilità di:

- **scomposizione del “Sistema Complesso” in “Sistemi Semplici”** (componenti) e **“Legami”** (interazioni) esistenti tra essi
- **ricomposizione del quadro operativo** di interventi come somma di tutte le soluzioni individuate dall’analisi effettuata sugli elementi singoli.

Tali possibilità, che possono essere assunte come principi base, consentono di **concentrare l’attenzione su delle “unità elementari”** perdendo di vista **“l’insieme complesso”** in modo da **generare e rintracciare dei sottosistemi su cui intervenire separatamente** sapendo che una loro ricomposizione ricostituirà il quadro originale e gli interventi individuati risulteranno adeguati ed efficaci.

Risk Management

ISO 31010

FMEA...

La FMEA fu sviluppata dalle forze armate statunitensi **nel 1949**, allo scopo di **classificare i guasti in base all'impatto sul successo della missione e sulla sicurezza del personale e degli equipaggiamenti**. Successivamente è stata applicata negli **anni '60 per le missioni spaziali Apollo** e successivamente nel campo produttivo di industrie civili.

Attualmente l'utilizzo della FMEA è previsto da diversi sistemi di gestione della qualità.

L'applicazione risulta versatile e flessibile in quanto diversi e variegati sono i modi di analisi e gli obiettivi: questi possono riguardare

- **gli aspetti dei singoli componenti o dei sistemi interi**
- **limitarsi alle sole fasi dei processi o ai flussi interi**
- **semplice analisi delle modalità di guasto o alla valutazione degli effetti**

[ESEMPIO FMEA.xlsx](#)

[esempio parte introduttiva fmea.docx](#)

[fmea.docx](#)



Risk Management

BOW TIE MODEL





Risk Management

ISO 31010

[BOWTIE docx.docx](#)

HAZARD = RISCHIO

THREAT = MINACCIA

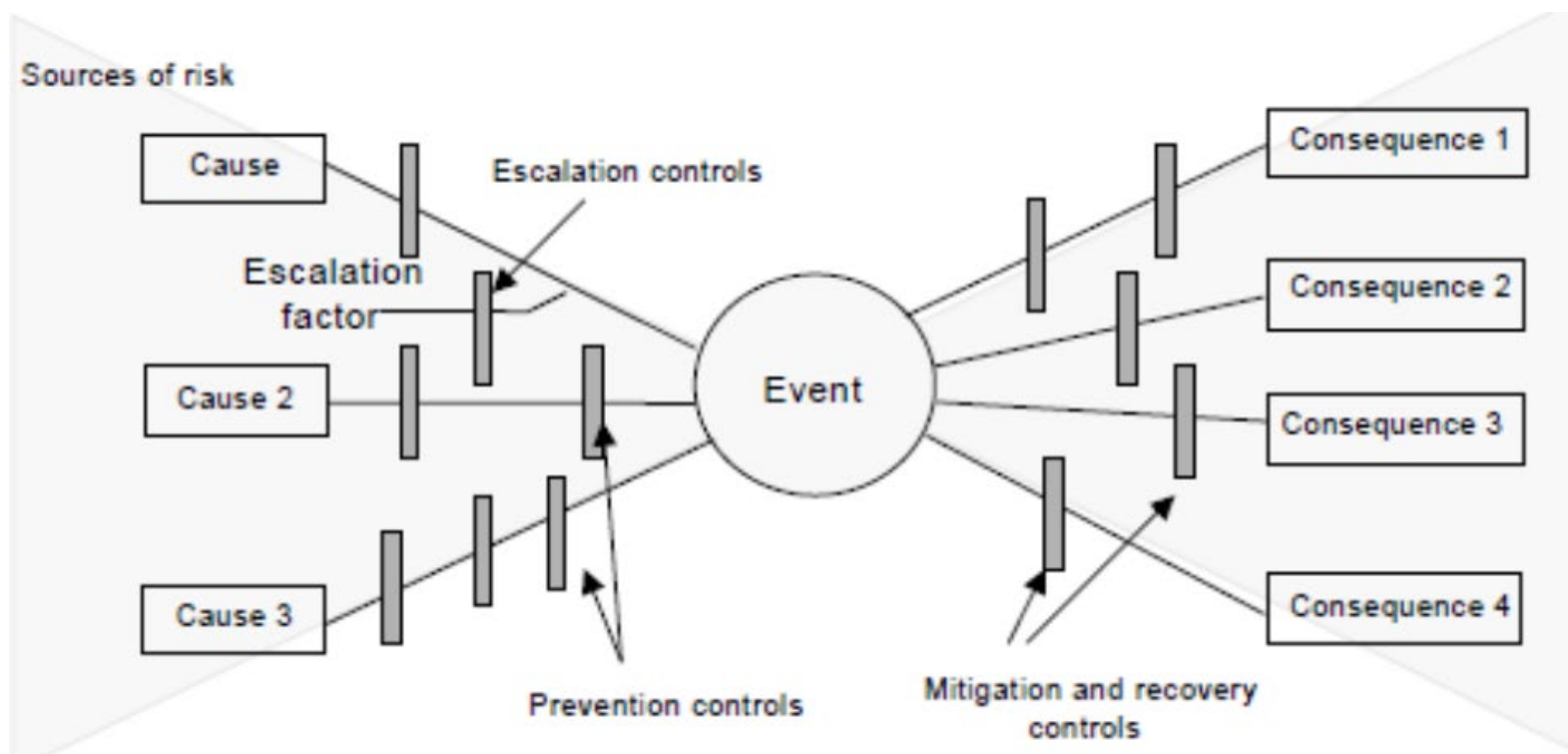


Risk Management

ISO 31010

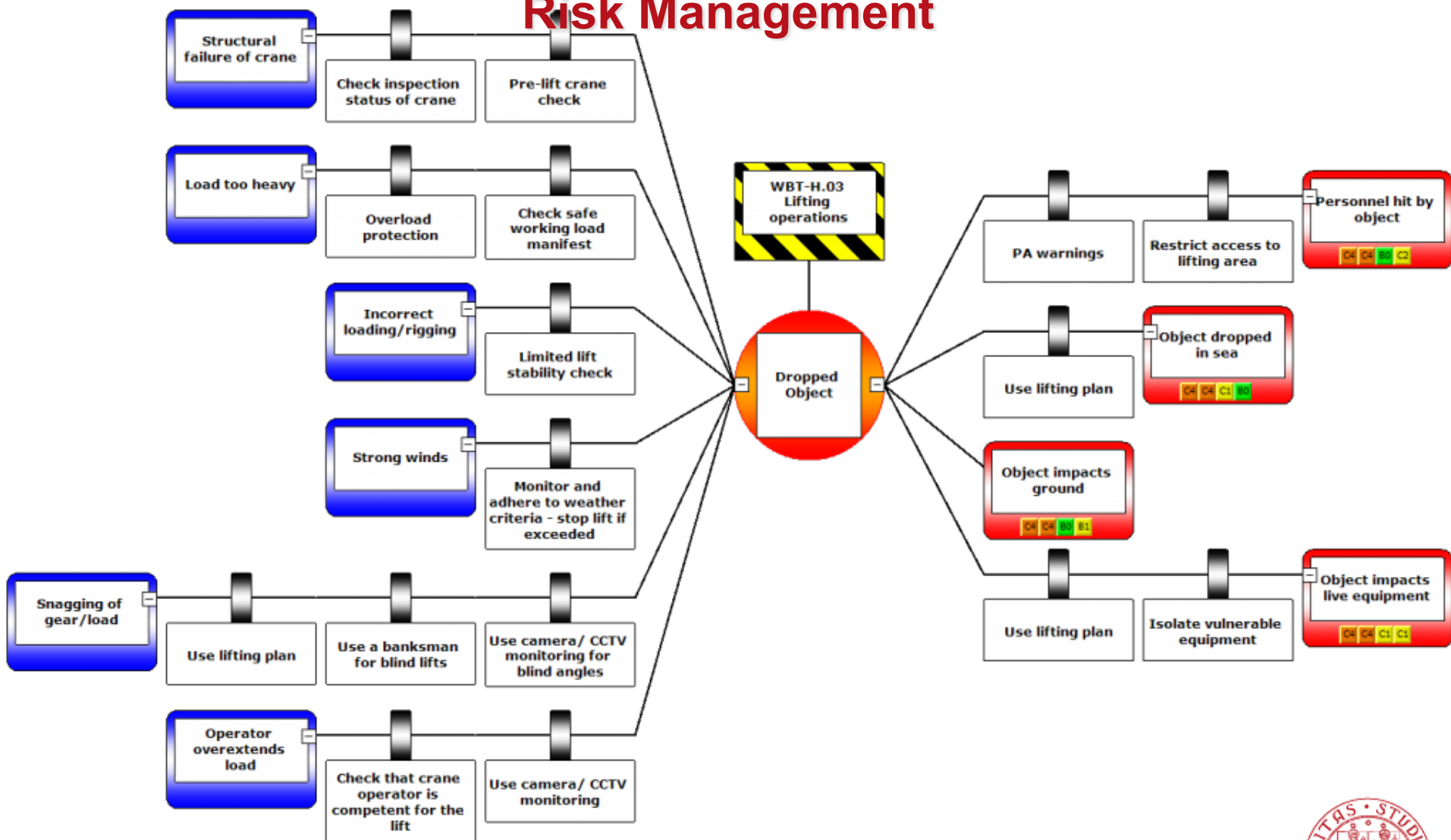
HAZARD = RISCHIO

THREAT = MINACCIA



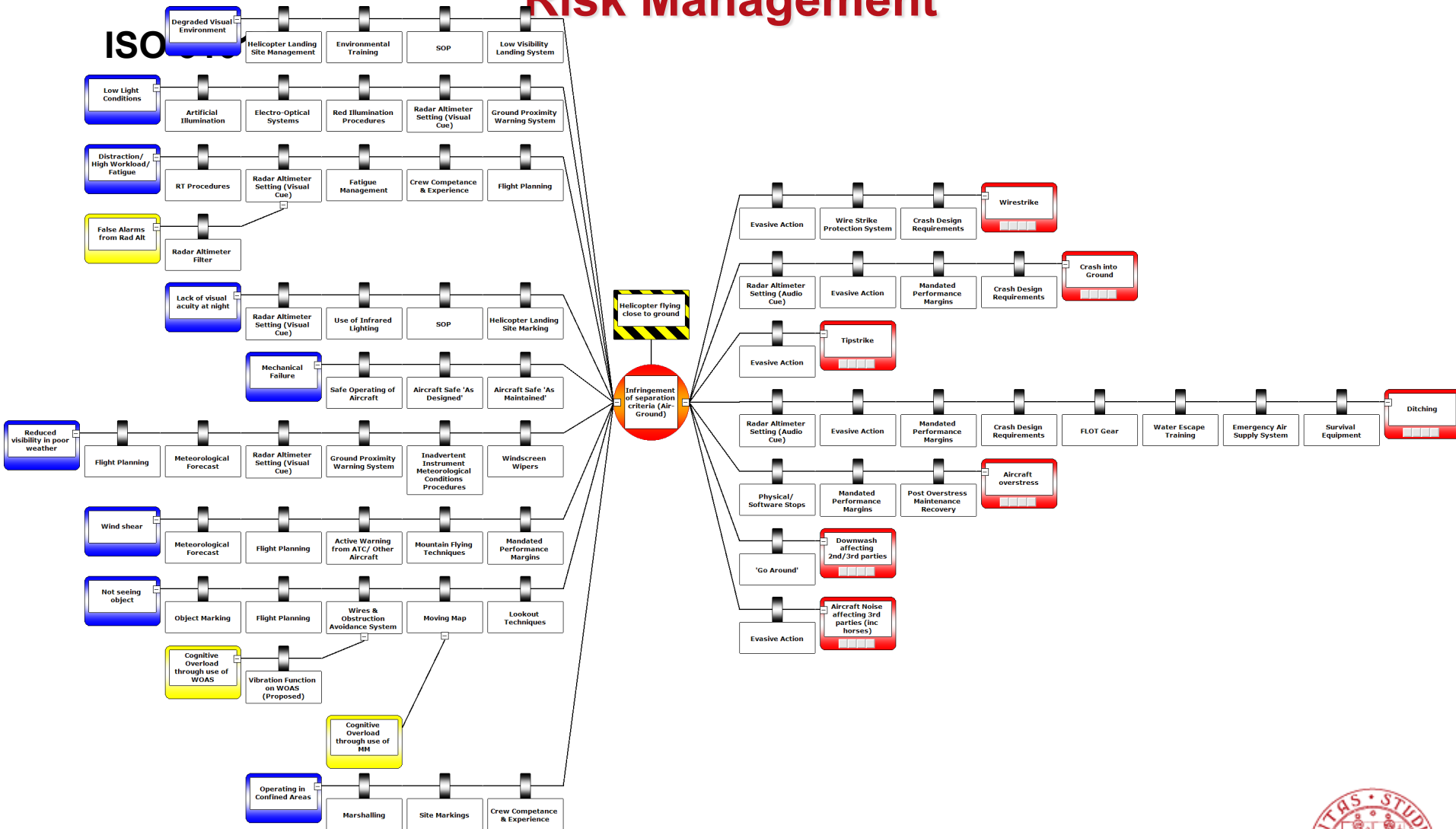
[BOWTIE docx.docx](#)

Risk Management





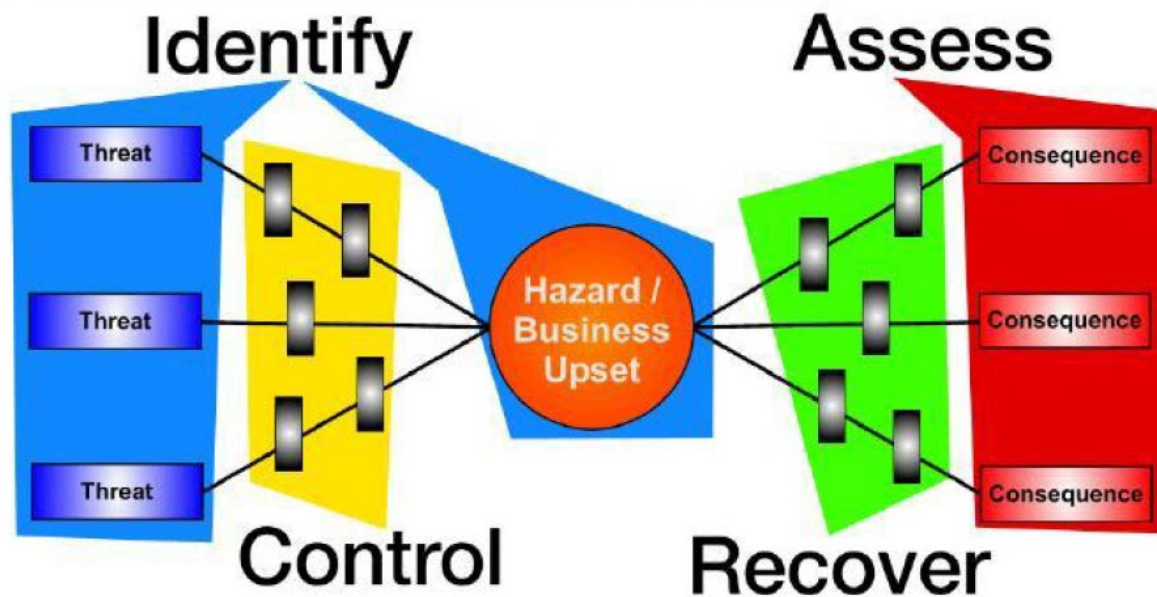
Risk Management



Risk Management

Bow Tie Model and Safety Risk Management

When we look at the bow tie method, we see the four underlying steps of risk evaluation and management implemented:



Risk Management

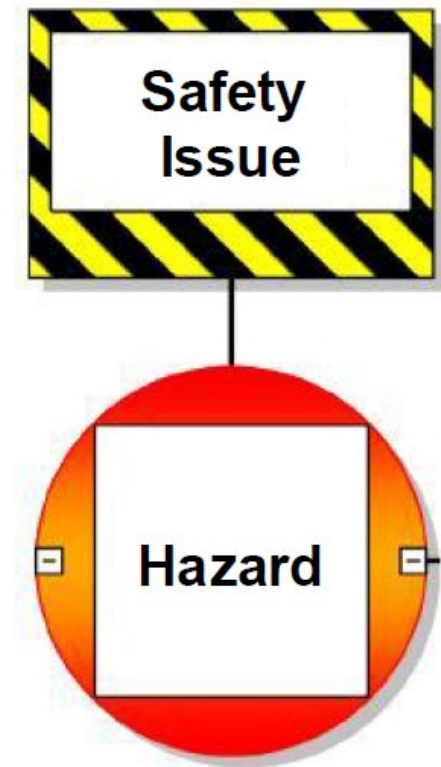
Safety Issue and Hazard

Safety Issue

The potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.

Hazard (Top Event*)

The 'release' of the safety issue. The initial consequence. What happens when control is lost.



Risk Management

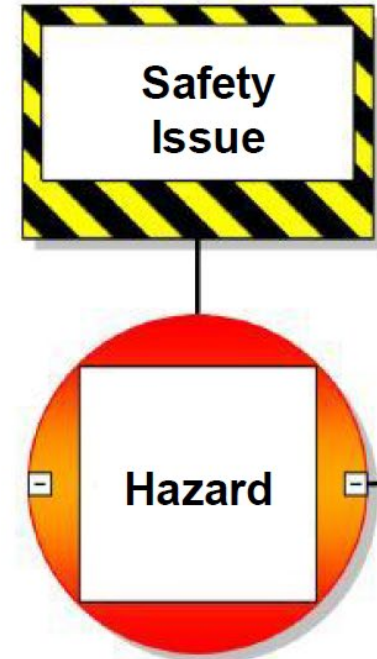
Examples for Safety Issues and Hazards

Some examples of Safety Issues

- Driving vehicle
- Stored materials
- Working at height
- Money transfers
- Electrical systems
- Crowding
- Working at night
- Moving machinery
- Construction work
- System maintenance

Some examples of Hazards (Top Events)

- Loss of Containment
- Structural Failure
- Dropped Object
- Loss of Control
- Electrical Shock
- Falls to Same Level
- Falls to Lower Level
- Oxygen Deficiency
- Loss of Separation
- Contact

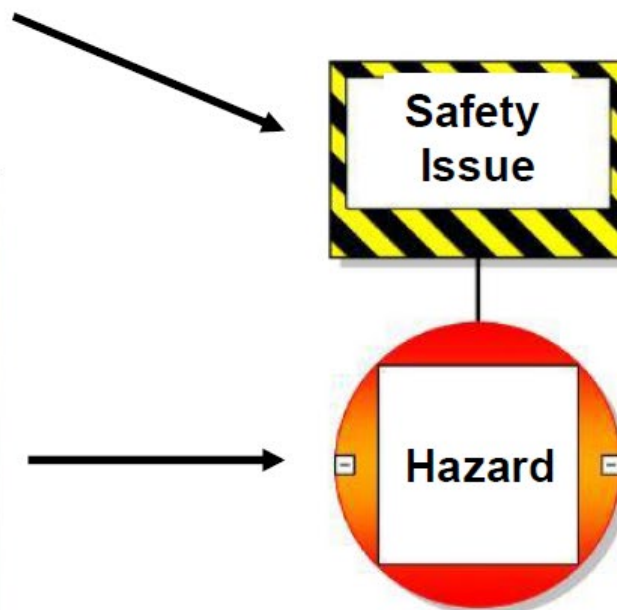


Risk Management

Batterie al litio negli EFB



Fuoco in cockpit/cabina causato da batterie al Litio



Risk Management

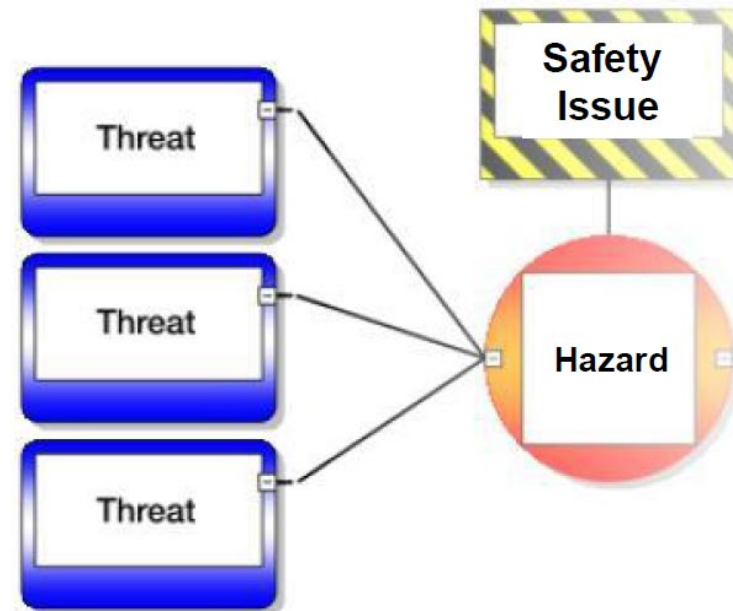
Threat (Cause) Minacce

Threat

A possible cause that will potentially release a hazard

Some threats / potential causes

- Thermal - high temperature
- Chemical – corrosion
- Biological
 - Bacteria
 - Marine growth
- Electrical - high voltage
- Environmental Condition
 - poor visibility
 - Flooding
- Human Factor - incompetence



Risk Management

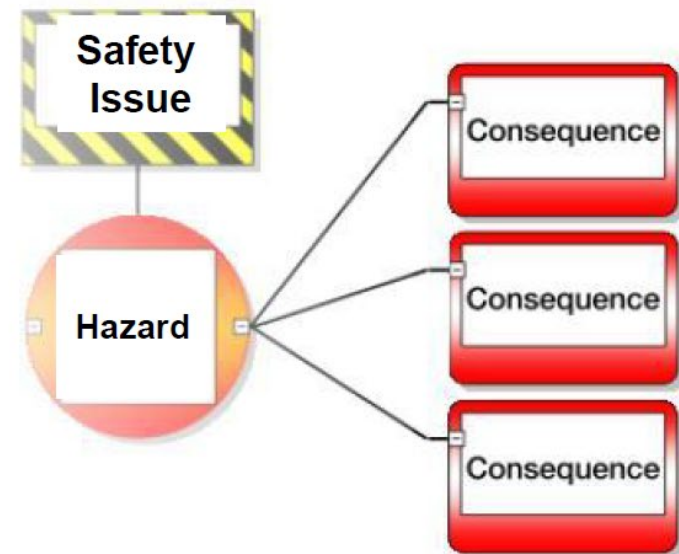
Consequences

Consequence

An event or chain of events that potentially results from the release of a hazard.

Some examples of Consequences:

- Reputational damage
- Financial damage
- Property damage
- Production loss
- Injuries / fatalities
- Distressed personnel
- Unemployment
- Complaints



Risk Management



Firefighters douse a blaze on board a UPS DC-8 at Philadelphia International.



Risk Management





Risk Management





Risk Management





FAA GROUNDS BOEING 787 DREAMLINER
Citing potential battery fire risk on planes



TOP NEWS

Reports: French hostage executed by captors

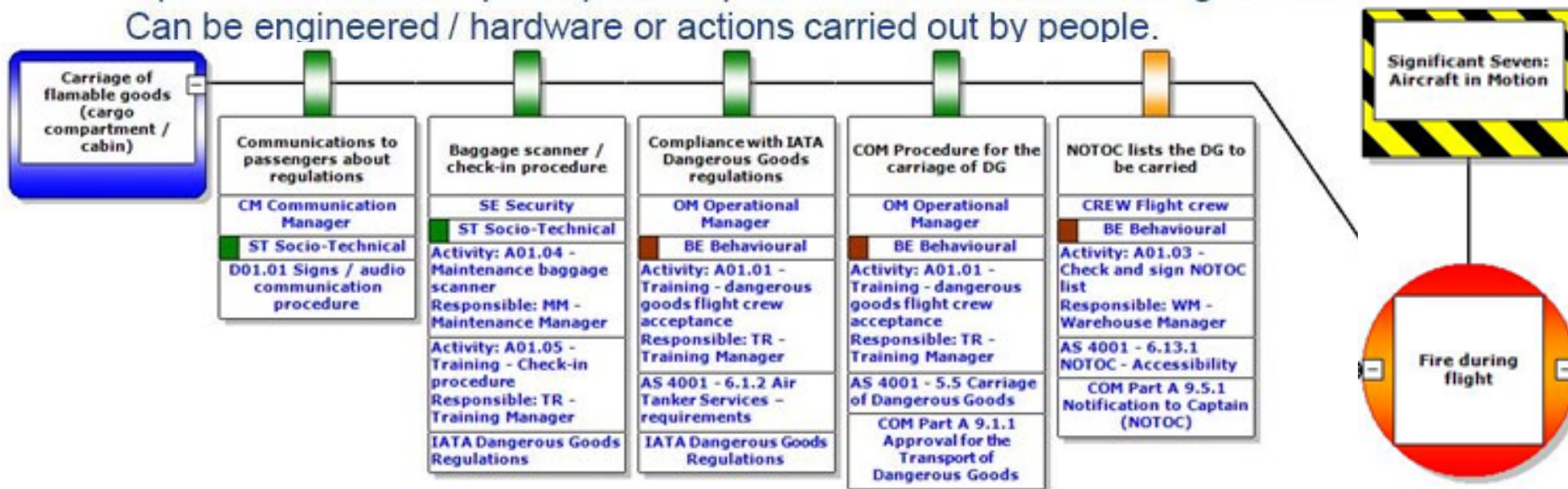


Risk Management

Defences

Control of Threats – Threat Defences

A protective measure put in place to prevent threats from releasing a hazard.
Can be engineered / hardware or actions carried out by people.

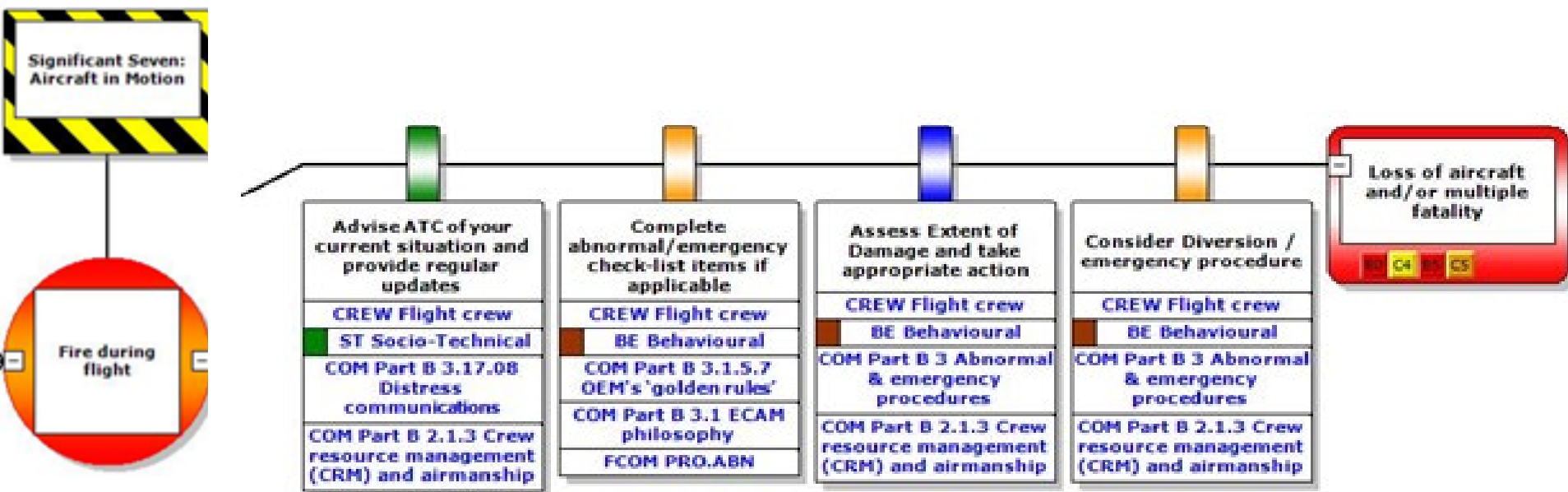


Risk Management

Barriers

Barriers for Each Consequence

All technical, operational and organisational measures that limit the probability of consequences arising from a top event.





Risk Management

Barriers

Some Examples for Barriers:

- Systems to Detect and Abate Incidents
 - *gas, fire & smoke alarms, ESD, deluge*
- Systems Intended to Protect the Safeguards
 - *fire & blast walls, protective coatings, drain systems*
- Operational Systems Intended for Emergency Management
 - *contingency plans, training, drills, clean up, restoration, medical treatment*
- Compensative measures
 - *re-stock fish, financial compensation*





Risk Management

