La valutazione del rischio aeroportuale, così come in altri campi, rappresenta uno dei temi di maggiore interesse del trasporto, ed investe un ampio raggio di ricerca.

Volendo fare una prima macro classificazione, possiamo considerare due tipi di intervento necessari a ridurre l'entità del rischio, ossia:

1. La ***security*** intesa principalmente come *security device* ovvero l'insieme dei dispositivi di sicurezza ritenuti necessari a garantire la protezione delle strutture, del personale in esso operante e degli stessi utenti.

2. La ***safety*** intesa come l'insieme delle norme e degli accorgimenti tecnici realizzati sugli impianti perché ritenuti necessari a garantire la sicurezza dei mezzi di trasporto e quindi finalizzata a rendere sicuro il trasporto dei passeggeri e del personale addetto.

Tale distinzione deriva dall'interpretazione anglosassone che attribuisce ai termini "*security"* e "*safety", il seguente significato:*

a) con il termine *security* si intende la protezione dei beni o dei materiali dell'azienda da occhi indiscreti o da azioni volontarie di persone o gruppi che intendono danneggiare un'attività economica;
b) con il termine *safety* si intende invece la parte relativa alla protezione da eventi quali incendi, esplosioni, fughe di gas, rischi causati da rotture di macchinari, rischi derivanti da manipolazione errata di materiale o comportamenti di operatori che causano infortuni di lieve entità, invalidanti o addirittura mortali.

ANALISI DELLA SITUAZIONE ATTUALE DEGLI AEROPORTI

Volendo aumentare la sicurezza nelle operazioni, diventa necessario assicurare una seria e costante operazione di prevenzione, attraverso l'individuazione e la successiva eliminazione di ogni circostanza o condizione di pericolo che possa generare un incidente.

L'incidente, spesso, non è però originato da una singola causa, ma scaturisce dalla combinazione di varie circostanze o "*catena di eventi*".

Va inoltre, tenuto in considerazione il fatto che una singola causa non sempre è significativa ai fini di un incidente, ma può diventarlo se si combina con altre cause.

Per meglio capire ed interpretare le cause di un incidente, bisogna riferirsi a quanto viene detto e considerato nel mondo aeroportuale.

A tal proposito, possiamo elencare tre tipologie di *incidente aereo (Annex 13 - ICAO)*:

1. Accident (incidente):

Un evento, associato alle operazioni di un aeromobile che si potrebbe verificare nel periodo compreso tra il momento in cui il primo passeggero si imbarca ed il momento in cui tutti i passeggeri sono sbarcati.

Tale evento rientra in una delle seguenti circostanze:

- decesso o grave ferimento di una persona;
- danno grave all'aeromobile (con l'eccezione di alcune specifiche avarie);
- l'aeromobile risulti disperso o inaccessibile.

2. Incident (inconveniente aeronautico)**:**

Un avvenimento, non classificabile come "*accident*", che però sia associato alle operazioni di un aeromobile, e che influisce o potrebbe influire sulla sicurezza delle operazioni stesse.

3. Serious Incident (grave inconveniente aeronautico)**:**

Un avvenimento coinvolgente circostanze indicanti che l'*accident* era prossimo a verificarsi.

NOTE

Si ricorda che quanto sopra esposto può, con le dovute modifiche e accortezze, essere applicato in altri campi del trasporto. L'analisi di un incidente è fondamentale perché si eviti il ripetersi di quel tipo di evento ma raramente fornisce indicazioni su come prevenire una classe d'incidenti.

Pur essendo le statistiche l'unico strumento oggi disponibile e da tutti riconosciuto per rendere la sicurezza misurabile, è altrettanto vero che una strategia di prevenzione per essere veramente efficace debba poter contare su strumenti capaci di identificare realmente le carenze del sistema.

Se, per esempio, anziché focalizzare l'attenzione sui fattori causali o primari, si andassero ad analizzare le relazioni che esistono nella catena degli eventi di un incidente, con buona probabilità, si potrebbero ottenere indicazioni più significative per la relativa prevenzione.

La volontà delle più autorevoli istituzioni a livello mondiale di adottare un approccio preventivo mirato all'identificazione e al rimedio di potenziali cause di futuri incidenti, è testimoniato dalla proliferazione di ambiziose iniziative per l'adozione di strategie di miglioramento della sicurezza.

RSING.IT

SAFETY MANAGEMENT SYSTEM
(S M S)

NOTA INTRODUTTIVA

Questo termine racchiude le norme di particolari tecniche di gestione atte ad identificare gli eventi indesiderati che possono insorgere durante il ciclo di un'attività, di un programma o di un progetto di gestione degli aeroporti.

L'SMS vuole pertanto scoprire gli eventuali rischi al fine di potere provvedere alla relativa riduzione, assicurando una gestione il più possibile serena sia per i passeggeri che per gli operatori nel sistema cui si riferisce.

L'obiettivo quindi dell'SMS è quello di identificare preventivamente i rischi, valutarli ed attuare tutte le procedure *standard* per la rimozione e/o il controllo degli *hazard*, raggiungendo un livello di rischio accettabile.

L'SMS vuole stimolare l'impostazione di una gestione della sicurezza aeroportuale in grado di inculcare nei gestori, una filosofia di criticità obiettiva e costruttiva tale da coinvolgere tutti gli operatori.

In questo modo chi gestisce ha una maggiore possibilità di:

- definire ed ottimizzare gli *standard* organizzativi basandosi sul suggerimento di tutti gli operatori facendoli così sentire motivati perché resi consapevoli che una buona gestione non può limitarsi solo al *Manager*, ma si basa sulla responsabilità condivisa da parte di tutti gli operatori;
- identificare i ruoli e le responsabilità di tutti gli operatori e stabilire le priorità della gestione per la determinazione delle strategie mirate alla *safety*;
- individuazione delle procedure atte alla eliminazione delle carenze del personale e dei mezzi, procedendo all'analisi dello stato dei mezzi esistenti ed eventualmente programmare la necessaria sostituzione o integrazione;
- procedere a verifiche periodiche programmate o dettate da contingenti situazioni relazionate dagli addetti, in modo da procedere tempestivamente ad interventi correttivi là dove ciò sia ritenuto necessario.

Là dove viene acquisita una filosofia gestionale in grado di garantire al massimo livello la sicurezza, l'SMS diventa un investimento positivo non solo per la sicurezza, la funzionalità e l'efficienza, ma anche per l'aspetto economico finanziario.

In questo senso l'SMS deve essere inteso, programmato, sviluppato e gestito alla pari di un programma finanziario.

Si spiega pertanto, come una buona filosofia di gestione deve dare risalto all'SMS, sia per la sicurezza, sia per un ritorno economico, sia per un ritorno di immagine.

Certamente una tale filosofia di gestione cozza spesso con il modo tradizionale che mirava alla riduzione dei costi anche a rischio di seri incidenti.

Se consideriamo però le spese derivanti da gravi incidenti, certamente viene fuori che alla fine il male minore è sicuramente la prevenzione.

In questo senso bene si inquadra la filosofia dell'SMS poiché l'Ente che lo adotta, è in grado di prevenire i problemi e quindi di procedere alla rimozione dando sia all'interno che all'esterno un'immagine di funzionalità, di efficienza e di sicurezza.

DEFINIZIONE

Iniziamo con due definizioni appropriate alle operazioni del trasporto aereo commerciale:

1. *Safety Management;*
2. *Safety Management System.*

1. La "*Safety Management*" è definita come la gestione sistematica dei rischi associati alle operazioni di volo, correlate alle operazioni a terra e all'ingegneria dell'aeromobile o alle attività di manutenzione, per realizzare alti livelli di *performance* della *safety*.

2. Un "*Safety Management System*" è un esplicito elemento della corporativa responsabilità gestionale, che mostra un metodo di *safety* della compagnia e definisce il modo gestire la *safety* come parte integrale di tutti gli affari.

   Un SMS può essere paragonato ad un sistema gestionale finanziario alla pari di un metodo per gestire sistema-ticamente una funzione vitale del *business*.
   È importante pertanto tenere conto degli aspetti che seguono:

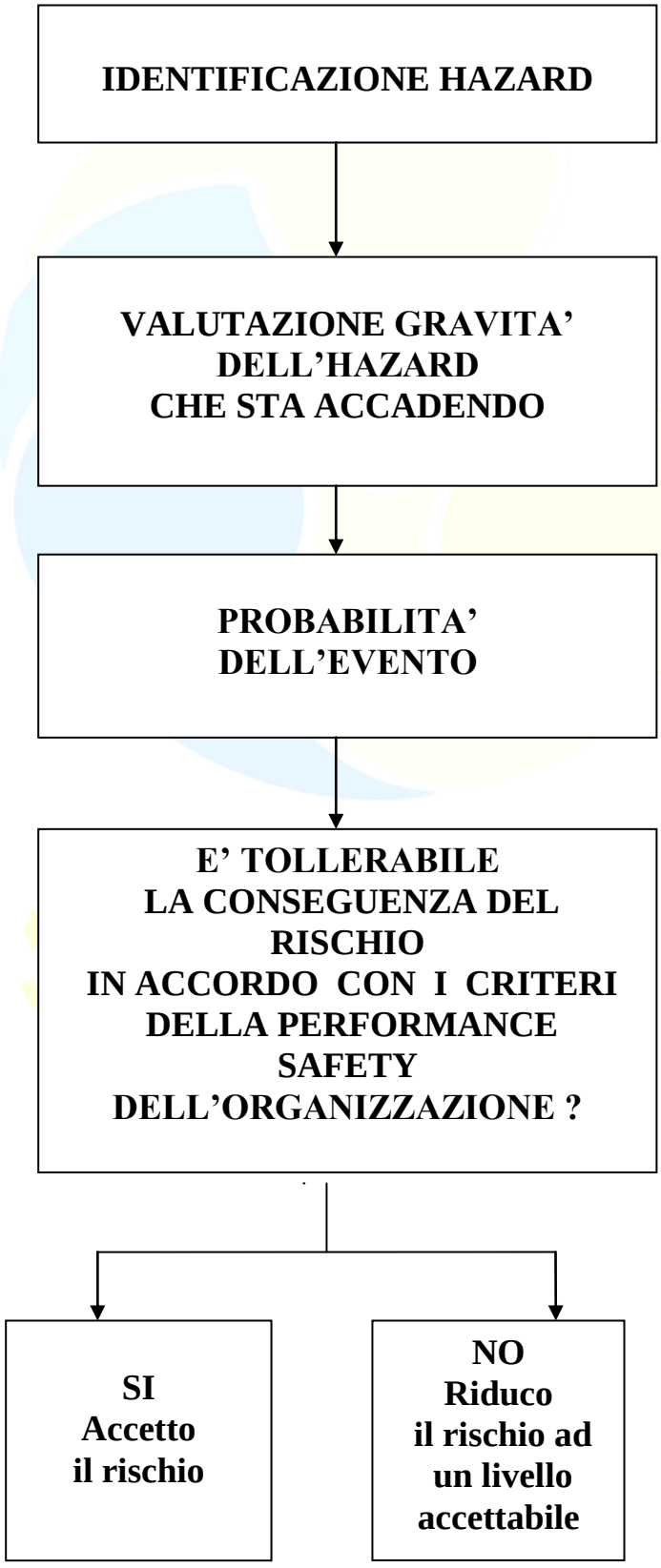
   - le caratteristiche di un sistema di gestione finanziario, sono ben conosciute;
   - i *target* finanziari sono fissati, i *budget* vengono approntati, i livelli di autorità sono stabiliti e così via;
   - le formalità associate al sistema finanziario includono "verifiche e bilanci";
   - il sistema completo comprende un elemento di monitoraggio, cosicché le correzioni possono essere fatte nel momento in cui la *performance* scende un po' al di sotto dei *target* prefissati;
   - i rendimenti di un sistema di gestione finanziario, vengono percepiti solitamente attraverso la compagnia.

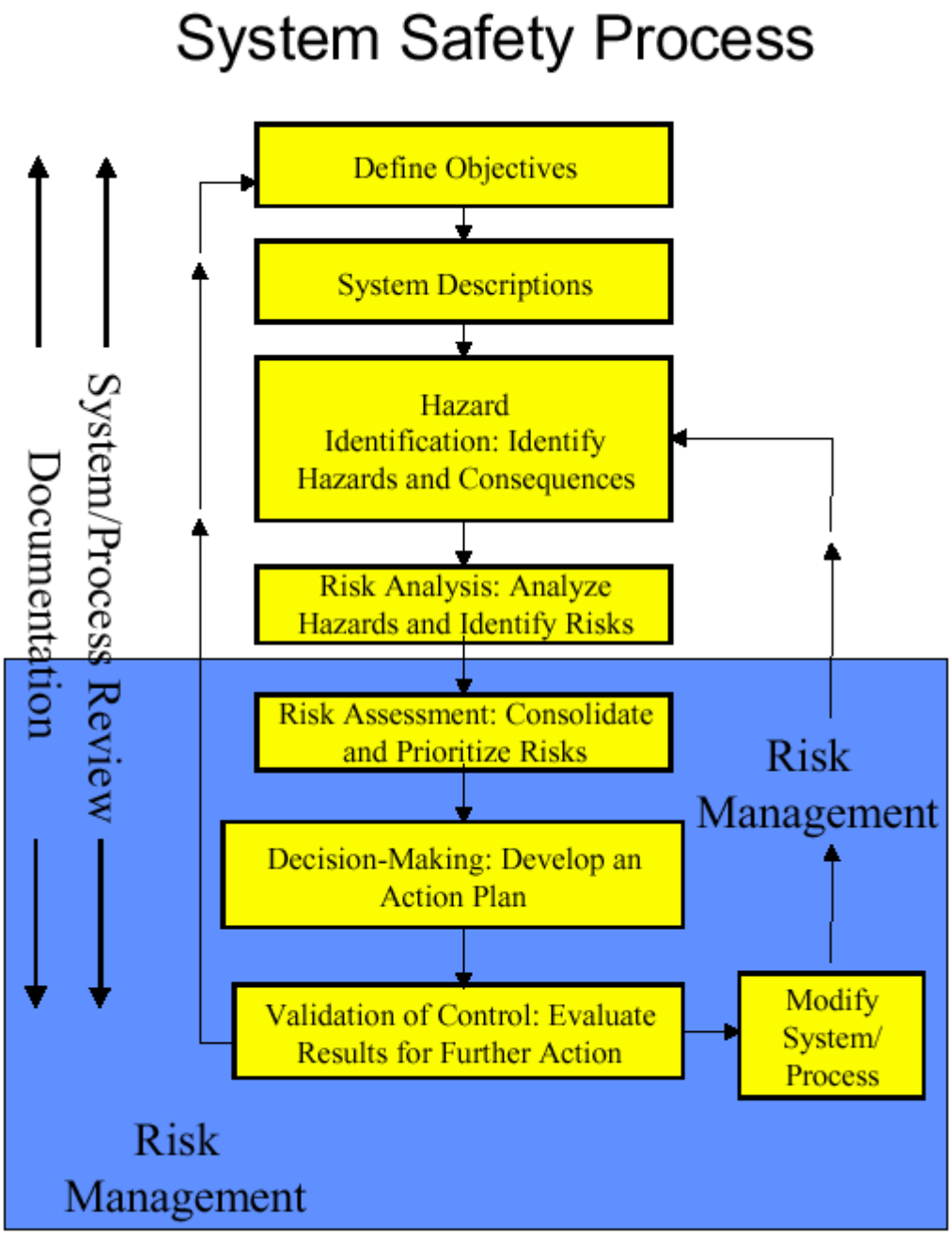
I rischi ci sono ancora, ma le procedure finanziarie dovrebbero garantire che non vi siano "sorprese commerciali".
Se dovessero esserci, potrebbe essere disastroso per un piccola compagnia, mentre per le compagnie più grandi, ad una sgradita attenzione dei media, solitamente, segue solo una perdita inaspettata ma circostanziata.

Anche un *accident* di un aereo è una "perdita inaspettata" e nessuna delle compagnie dell'aviazione civile vorrebbe soffrirne.

L'adozione di un SMS efficace fornirà alla gestione un modo per evitare tutto questo.

Hazard: una condizione o circostanza che potrebbe portare o contribuire ad un non pianificato e/o indesiderato evento.
Likelihood: probabilità
Rischio: possibilità di conseguenze dannose o negative a seguito di circostanze non sempre prevedibili.




System Safety Process
Define Objectives
System Descriptions
Hazard Identification: Identify Hazards and Consequences
Risk Analysis: Analyze Hazards and Identify Risks
Risk Assessment: Consolidate and Prioritize Risks
Decision-Making: Develop an Action Plan
Validation of Control: Evaluate Results for Further Action
Modify System/ Process
Risk Management
Risk Management
System/Process Review
Documentation

Un sistematico approccio al miglioramento del processo richiede una ricerca pro-attiva delle opportunità mirata a perfezionare il processo ad ogni *step* non soltanto attraverso la semplice identificazione delle deficienze dopo un evento indesiderato.

La Gestione del Rischio (*Risk Management*) è stata definita come il processo per il quale i risultati della Valutazione del Rischio (*Risk Assessment*) vengono integrati con le considerazioni politiche, sociali, economiche ed ingegneristiche, affinché si prendano decisioni sul bisogno e sui metodi per la riduzione del rischio stesso.

In riferimento alla figura riportata nella pagina precedente, viene specificato quanto segue:

1. *Define Objective:*

   il primo passo è quello di definire gli obiettivi del sistema. Questi obiettivi vengono tipicamente documentati nei piani commerciali e nelle specifiche operazionali.

2. *System Descriptions:*

   una descrizione delle interazioni tra il personale, le procedure, i mezzi, i materiali, gli equipaggiamenti, le agevolazioni, i *software* e l'ambiente.
   Ciò include anche le descrizioni dei dati disponibili.

3. *Hazard Identification: Identify Hazard and Consequences:*

   gli hazard potenziali potrebbero essere identificati da un numero di sorgenti interne ed esterne.
   Solitamente, gli *hazard* vengono inizialmente messi in una lista PHL (*Preliminary Hazard List*), poi raggruppati con equivalenza di funzioni per l'analisi.
   Prima dell'analisi del rischio si deve includere anche la conseguenza che ne risulta dallo scenario *hazard*.
   Gli scenari *hazard* possono richiamare i seguenti punti: "chi", "che cosa", "dove", "quando", "perché" e "come".
   Questo metodo fornisce un prodotto intermedio che esprime la condizione e le conseguenze che potrebbero essere usate durante l'analisi del rischio.

4. *Risk Analysis: Analyze Hazard and Identify Risks:*

   l'analisi del rischio è il processo per mezzo del quale gli *hazard* vengono caratterizzati per le loro probabilità (*likelihood*) e per la loro gravità (*severity*).
   L'analisi del rischio guarda gli hazard determinando "che cosa" può accadere e "quando".
   Questa può essere un'analisi o qualitativa o quantitativa.
   L'incapacità di quantificare e/o la mancanza di dati storici su un particolare *hazard*, non esclude l'hazard stesso dal bisogno di esser analizzato.
   Per determinare il livello di rischio viene normalmente usata una Matrice di *Risk Assessment*, secondo lo schema della figura seguente.

Example Risk Assessment Matrix

RISK ASSESSMENT MATRIX				
	Severity			
Likelihood	Negligible	Marginal	Critical	Catastrophic
Frequent				
Probable				High
Occasional			Serious	
Remote		Medium		
Improbable	Low			

Severity Scale Definitions	
Catastrophic	Results in fatalities and/or loss of the system.
Critical	Severe injury and/or major system damage.
Marginal	Minor injury and/or minor system damage.
Negligible	Less than minor injury and/or less than minor system damage.

Likelihood Scale Definitions		
Frequent	Individual	Likely to occur often.
	Fleet	Continuously experienced.
Probable	Individual	Will occur several times.
	Fleet	Will occur often.
Occasional	Individual	Likely to occur some time.
	Fleet	Will occur several times.
Remote	Individual	Unlikely to occur, but possible.
	Fleet	Unlikely but can reasonably be expected to occur.
Improbable	Individual	So unlikely, it can be assumed it will not occur.
	Fleet	Unlikely to occur, but possible.

5. *Risk Assessment: Consolidate and Prioritize Risks:*

   la valutazione di rischio è generalmente definita come il processo di combinare gli impatti degli elementi del rischio scoperti nell'analisi del rischio e paragonarli ad alcuni criteri di accettabilità.
   La valutazione di rischio può includere il consolidarsi del rischio in un *set* di rischi che può essere congiuntamente mitigato, combinato e poi usato nel processo decisionale.

6. *Decision Making: Develop Action Plans:*

   questo *step* inizia con il recepimento di una lista di rischi ordinati per priorità.
   Rivede la lista per determinare come indirizzare ogni rischio, iniziando con quello di più alta priorità.
   Le quattro opzioni che potrebbero essere scelte per un rischio sono: *Trasferire, Eliminare, Accettare o Mitigare* (T.E.A.M.).

7. *Validations and Control: Evaluate Results of Action Plan for Further Action*:

   la ratifica ed il controllo iniziano con:

   - i risultati delle analisi messe in lista sull'efficienza delle azioni prese (questo includerà l'identificazione dei dati che devono essere raccolti e l'identificazione degli eventi scatenanti, la dove è possibile, sviluppando poi un piano per rivedere i dati raccolti);

   - lo status corrente di ogni rischio secondo la priorità.
     Se il rischio residuo è accettabile, viene richiesta la documentazione che rifletta la modifica al sistema e la spiegazione logica per accettare il rischio residuo.
     Se invece non è accettabile, potrebbe esserci bisogno di un piano di azione alternativo o una modifica al Sistema/Processo, se necessario.

8. *Modify System/Process*:

   qualora lo status di un rischio dovesse cambiare o la mitigazione non producesse l'effetto desiderato, deve essere presa una determinazione sul "perché".
   Potrebbe capitare che un *hazard* errato era stato indirizzato o il sistema/processo aveva bisogno di essere modificato.
   In entrambi i casi, si rientrerebbe poi nel processo del sistema *safety,* allo *step hazard* identificato.

RISCHIO E VALUTAZIONE DEL RISCHIO

Legato sia alla *safety* che alla *security* è il rischio, di cui si fornisce una definizione qualitativa: “il rischio è una condizione che in potenza può causare infortunio alle persone, danno agli impianti o alle strutture, perdita di materiale o diminuzione delle capacità di svolgere una funzione prestabilita”.

Tenuto conto che il rischio non è eliminabile in senso assoluto, la sua valutazione deve essere di carattere relativo ed il livello di accettabilità dipende dall’evoluzione sociale del paese e muta con essa.

Pertanto la possibilità di conseguenze dannose o negative a seguito di circostanze non sempre prevedibili, varia secondo le specifiche attività e la sua ricerca è importante ai fini di una diminuizione dell’entità delle conseguenze o della probabilità oppure di entrambe.

La definizione quantitativa convenzionalmente adottata di rischio è: $R = f \cdot M$ **,** dove *f* indica la frequenza di accadimento dell’evento incidentale ed *M* denota la magnitudo dei suoi effetti, ovvero la consistenza delle sue conseguenze.
La grandezza *R*, che è quella che rappresenta il rischio, prende il nome di “*indice di rischio*”.
Tale definizione tiene in eguale conto sia le conseguenze provocate da un incidente sia la probabilità che tale incidente si verifichi.

Nella procedura di valutazione di un rischio, la fase più critica e difficilmente quantificabile è la probabilità dell’evento, mentre la valutazione della magnitudo è meno soggetta a grandi errori.
Ne consegue che non è sempre corretto affidare lo stesso peso di affidabilità ai fattori *f* ed *M*. in altre parole, non è vero che 100 incidenti all’anno, ciascuno con un morto equivalgono a 10 incidenti all’anno ciascuno con 10 morti o ad un unico incidente all’anno con 100 morti.

TIPI DI RISCHIO

E' possibile individuare differenti tipi di rischio:

- rischio percepibile *individualmente*;
- rischio percepibile *collettivamente*;
- rischio *calcolato*;
- rischio *reale*.

L'importanza del rischio percepito è che i percettori, anche se non prendono le decisioni principali, sono coloro che probabilmente influenzano le decisioni attraverso il processo politico.
La percezione del rischio dipende da fattori diversi e da considerazioni soggettive ed obiettive.
Alcune di queste sono:

- volontaria/involontaria natura del rischio;
- familiarità con la situazione;
- tipo di evento;
- contesto culturale;
- natura della comunicazione;
- l'esposizione a lungo/breve termine;
- immediatezza o meno delle conseguenze.

La percezione collettiva influenza direttamente le decisioni da prendere e quindi la collettività può orientare le scelte verso soluzioni più o meno rischiose.

Il rischio calcolato è quello ottenuto attraverso procedure di valutazione quantitativa del rischio e finalizzate al calcolo della probabilità di accadimento dell'evento rischioso e delle conseguenze ad esso associate.
Il rischio reale è quello che si può ottenere se tutte le informazioni relative alla probabilità e alle conseguenze proprie di un incidente fossero conosciute.
Per la valutazione delle frequenze incidentali esistono delle procedure basate su una dettagliata analisi della vita e delle condizioni operative della struttura che è candidata ad essere sede dell'incidente.
Per quanto concerne la magnitudo, invece, il discorso si complica a causa degli innumerevoli fattori che intervengono e pesano sulla individuazione di un danno di riferimento che sia accettabile per tutti.

Un'altra classificazione degli eventi è legata alle cause:

- *Eventi naturali*, cioè al di fuori del campo d'azione dell'uomo ed inerenti la natura
- *Eventi causati dall'uomo*; si suole fare riferimento ad una sottoclassificazione che prevede le tre tipologie seguenti:
  1. *accidentale*, se esso è inatteso;
  2. *incidentale*, se esso è non voluto e non previsto;
  3. *intenzionale*, se esso è previsto o voluto.

Riguardo le conseguenze degli eventi, esse possono essere di tipo sanitario , sociale ed ambientale.
In definitiva, per ridurre il rischio si può agire sui due fattori che lo definiscono, cioè la probabilità dell'evento e la gravità delle conseguenze.

LA PERCEZIONE PUBBLICA DEL RISCHIO

La percezione pubblica del rischio è la valutazione sia razionale che emotiva di un dato evento.
Tale percezione gli è data dalla sua cultura, dai media, dal suo atteggiamento psicologico nei confronti delle avversità della vita e anche dalle sue convinzioni politiche.

L'atteggiamento del pubblico di fronte ai rischi spesso è di tipo emotivo e non ha alcuna relazione con la loro entità.
Lo dimostra il fatto che il pubblico percepisce maggiormente il concetto parziale di magnitudo piuttosto che quello più razionale di rischio, che è invece legato alle probabilità dell'evento.

Ci sono attività umane senza dubbio rischiose che prevedono la pubblicità dei piani di emergenza o addirittura la sperimentazione senza che per questo il pubblico ne contesti l'esistenza, l'utilità o l'attività che li ha resi necessari.

E' importante tener presente che in realtà non viene messo in discussione il livello di rischio che l'attività comporta, ma quella che viene rifiutata è la sua imposizione.
In altre parole, il cittadino spesso si assume rischi ben superiori per sua scelta, convinzione e/o convenienza.

RISK MATRIX

L \ S	5	4	3	2	1
A					
B					
C					
D					
E					

LOW Risk
Accettabile senza revisione, restrizione o limitazione.

MEDIUM Risk
Accettabile con la revisione dell'appropriato livello gestionale

HIGHT Risk
Inaccettabile.

Se è vero, come è vero, che la fallibilità fa parte della natura umana e che la natura umana non può essere cambiata, è anche pur vero che possono essere cambiate le condizioni in cui operano le persone.

Detto cambiamento si rende maggiormente necessario se si tiene conto che ciascuna attività svolta dall'uomo, sia nel campo pubblico che privato, è, di per sé, soggetta a rischio.

Diventa quindi estremamente necessaria la ricerca di soluzioni applicative, distinte ed adattate alle singole attività che siano mirate a prevenire, individuare e rimuovere i rischi connessi con l'attività stessa.

Il rischio è una combinazione di probabilità e di gravità di possibili lesioni o danni in una situazione pericolosa.

La valutazione dei rischi è la valutazione globale della probabilità e della gravità di possibili lesioni o danni in una situazione pericolosa. E' necessaria per la scelta delle adeguate misure di sicurezza.

La sicurezza può essere definita come "*complementare del rischio*" e pertanto nelle condizioni di "*rischio zero"* si avrà il massimo grado di copertura del rischio e quindi "*sicurezza massima"*, mentre allorquando la "*sicurezza è pari a zero*", vuol dire "*evento certo*".

Poiché in natura il rischio zero non esiste, non potrà mai essere raggiunta una condizione di sicurezza totale.

Una *definizione quantitativa di rischio* può essere riportata rappresentando il rischio come funzione di tre variabili che rispondono a tre domande ben precise:

a) che cosa può accadere?
b) quanto è presumibile che ciò accada?
c) se accade, qual è la conseguenza?

Rispondendo a tali domande le variabili diventano:

- uno scenario (cosa può accadere),
- una probabilità (quanto è ipotizzabile),
- una misura (la conseguenza dell'evento).

Si può comunque dire che "*un'analisi quantitativa del rischio è essenzialmente una lista di eventi possibili con le loro conseguenze e probabilità di accadimento.*
In realtà tale lista è infinita, mentre qualunque analisi è per forza di cose finita e quindi incompleta.
Allora ne consegue che non ha importanza quanto attentamente è stato svolto il lavoro, perché in ogni caso potrebbe apparire non veritiero o comunque esaustivo.
Quindi serve a poco preoccuparsi degli eventi verificati, ma piuttosto torna più utile attenzionare quelli di cui non si è avuta l'idea.
Il risultato è che nelle analisi di rischio non si dovrà mai essere soddisfatti".

Ciò detto, a conferma che il *rischio zero non può esistere*, poiché esisterà sempre uno scenario S_{n+1} che non è stato previsto e quindi non analizzato.

Le analisi quantitative sono quindi il primo passo per la definizione e l'identificazione delle misure di sicurezza più idonee a proteggere i beni aziendali e a ridurre gli effetti ipotizzati in scenario.

Le soluzioni pertanto devono cercare di quantificare, attraverso un processo a cascata, la probabilità di accadimento, le relative conseguenze ed i costi inerenti l'evento rischioso.

Allora l'aspetto da non trascurare è quello della valutazione finanziaria dei rischi.

Questo significa che se in una organizzazione, l'analisi del rischio viene valutata come un investimento, allora la relativa valutazione sarà fatta tenendo conto dei costi e dei benefici.

Va comunque sottolineato che la valutazione del rischio diventa più prioritaria ed urgente di adeguate normative allorquando investe un elevato numero di persone esposte.

E' evidente che i sistemi di protezione da implementare devono avere un costo inferiore alle conseguenze dello *scenario i-esimo* identificato e ciò perché, ad un evento certo (il costo della prevenzione) si contrappone un evento incerto (il rischio) che può anche non accadere.

Tale analisi di sicurezza economicamente adeguata ai costi necessari per ottenerla, è stata sviluppata sotto il nome di Cost-Effective Security.

L'insieme delle norme inerenti le tecniche particolari di gestione atte ad identificare gli eventi indesiderati che possono insorgere durante il ciclo di un'attività, di un programma o di un progetto di gestione, prende il nome di *Safety Management System* (SMS).

L'SMS mira a scoprire gli *hazard* possibili, provvedere alla relativa riduzione e/o rimozione, assicurando una gestione il più possibile serena sia per i fruitori del servizio, sia per gli operatori del sistema cui l'SMS si riferisce.

METODO DI VALUTAZIONE DEGLI ERRORI (HUMAN FACTOR)

La valutazione degli errori va fatta secondo un modello di natura organizzativa basato su tre "*livelli*".

Al "*primo livello*" si trovano i così detti "***fallimenti attivi",*** ovvero quelli commessi dalle persone che operano nella situazione di *front line* definiti come "l'ultimo anello della catena".

Al "*secondo livello*" si collocano i "*fallimenti organizzativi*", ovvero quei fattori che attengono al sistema di gestione e quindi alle sue difese.

Al "*terzo livello*" vanno catalogati i "*fallimenti inter-organizzativi"* ovvero quelli che hanno a che fare con il sistema degli enti coinvolti nella gestione.

L'esperienza insegna che ognuno di questi livelli non è mai indipendente, ma risulta in un qualche modo, incapsulato nell'altro con la conseguenza che i fallimenti attivi sono favoriti dai fallimenti organizzativi i quali a loro volta sono favoriti dai fallimenti interorganizzativi.

Ogni incidente ha due momenti identificabili di cui il primo è quello riferito al momento in cui avviene e l'altro è invece riferito al tempo più dilazionato in cui l'incidente è stato costruito.

Nel primo momento sono coinvolti i fallimenti attivi, mentre nel secondo, i fallimenti organizzativi e quelli interorganizzativi degli enti di gestione.

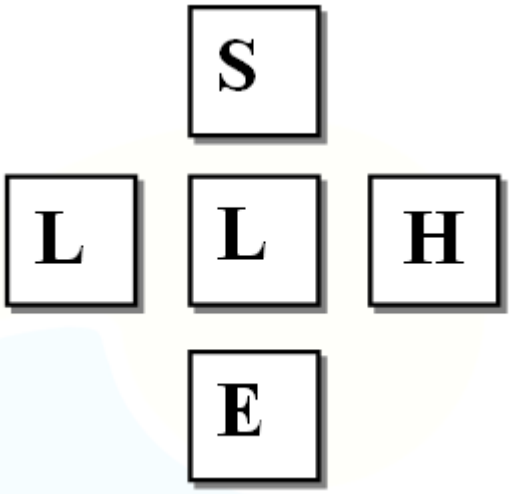
In ogni incidente, la valutazione *a posteriori*, consente una più facile individuazione degli errori.

Un altro aspetto da tenere in considerazione sono "*le intenzioni*", mettendo in evidenza che il fattore stress del personale abbassa notevolmente la capacità di far fronte a compiti complessi.

Così viene naturale chiedersi " come e perché le difese hanno fallito" e non "chi ha sbagliato".

Modello SHELL

Ai fini dello studio del 'fattore umano', considerato che in generale l'uomo risulta sempre al centro del sistema delle interazioni con il contesto di lavoro, è stato elaborato il cosiddetto **modello SHELL** (di Hawkins) per definire uno strumento di analisi delle varie componenti attraverso una visione sistemica delle attività e dell'organizzazione.



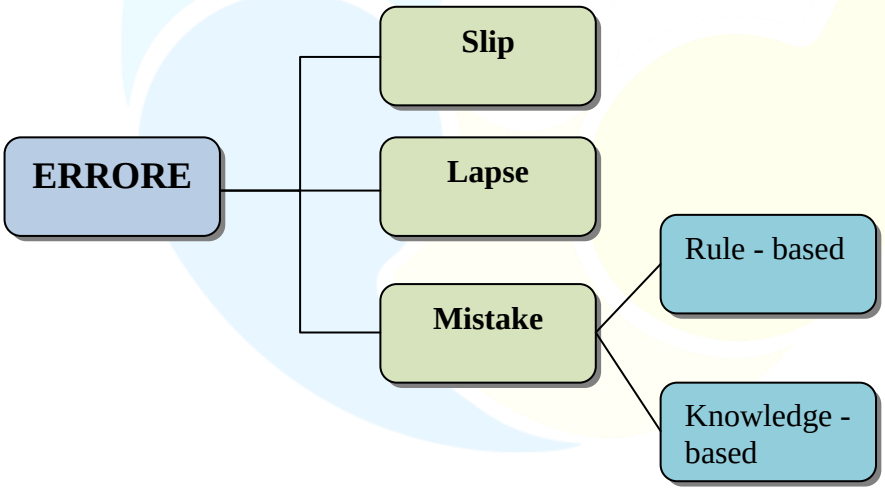
In tale modello di analisi le aree di interfaccia dell'uomo, posto al centro del sistema,sono:
S – **S**oftware – procedure.. Il software è la parte non fisica del sistema, ed include le politiche organizzative, le procedure, i manuali, gli schemi delle check-list, i grafici, le mappe, gli avvisi, e i software informatici.
H – **H**ardware – 'macchina'.. La componente hardware si riferisce alle attrezzature e ai materiali facenti parte dell'ambiente di lavoro. Nel caso di una nave esso comprende per esempio la progettazione di stazioni di lavoro, gli schermi, i controlli, i sedili, ecc.
E – **E**nvironment – ambiente.. L'environment comprende il clima interno ed esterno, la temperatura, la visibilità, le vibrazioni, il rumore e in generale gli elementi che creano le condizioni in cui le persone lavorano. A volte in questo elemento vengono inclusi anche i vincoli politici ed economici in cui l'organizzazione si trova ad operare.
L- **L**iveware – interrelazioni umane.. L'elemento periferico liveware fa riferimento alle interazioni uomo-uomo presenti nel sistema, e comprende fattori come il management, la supervisione, le interazioni tra gli operatori e le comunicazioni.

Lo studio della 'prevenzione' richiede prima di tutto la conoscenza degli eventi accaduti e dei relativi meccanismi incidentali.
Le valutazioni effettuate hanno messo in evidenza che di solito la causa di un sinistro durante il trasporto o di una situazione di pericolo non è unica. Una serie di concause che isolatamente, in genere, non producono l'incidente concatenandosi l'una all'altra finiscono per determinarlo. Quindi per evitare l'incidente, oltre che eliminare o ridurre la causa primaria, bisogna anche eliminare o ridurre le concause o interromperne la concatenazione.

LA TEORIA DEI FATTORI LATENTI DI REASON

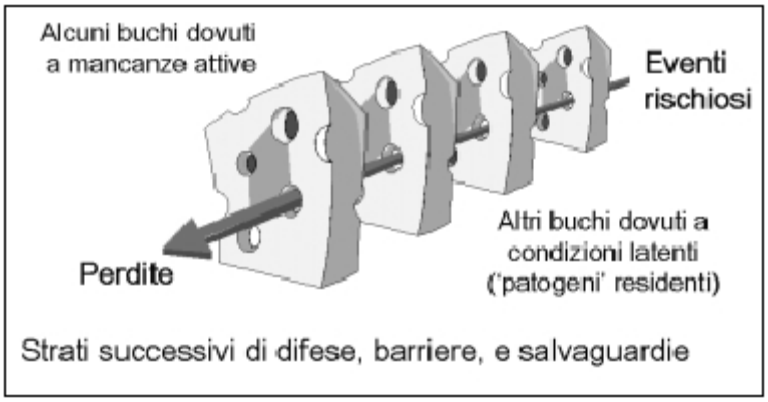
Per errore si intende lo scostamento da ciò che si sarebbe dovuto fare.
Gli errori possono essere classificati come:
- **slips** - errori dovuti al mancato rispetto delle procedure
- **lapses** - errori dovuti a omissioni, dimenticanze, disattenzioni, negligenze
- **mistakes** - errori dovuti a procedure non adeguate o pianificazione non adeguata
- **violations** - errori dovuti a violazioni deliberate di prescrizioni e procedure definite

A seconda dell'immediatezza con cui si manifestano gli errori possono essere divisi in:
- *attivi* - errori o violazioni con immediato effetto negativo, di solito imputabili al personale operativo quale piloti, tecnici, controllori;
- *latenti* - errori le cui conseguenze possono restare a lungo dormienti. Gli errori latenti (non corretta progettazione, organizzazione carente, cattive decisioni gestionali), immessi nel sistema ben prima di un incidente divengono palesi generalmente in corrispondenza di errori attivi, avarie tecniche o condizioni avverse dell'ambiente.



Essendo consapevoli che esistono numerosi fattori che concorrono all'accadimento dell'incidente, va cercata la causa valutando gli eventi all'interno di una imprevedibile combinazione e concatenazione delle debolezze delle barriera di difesa.
In questo, cercando il come e il perché le difese hanno fallito, si possono ridurre la probabilità dell'evento dannoso.
Va in ogni caso tenuto presente che se si aggiungono più "strati" di difesa si rende meno probabile la penetrazione di una sequenza di eventi dannosi, ma sorge il problema che aggiungendo più strati di difesa si aumenta anche l'opacità del sistema rendendo meno trasparente il controllo da parte delle persone che vi operano.

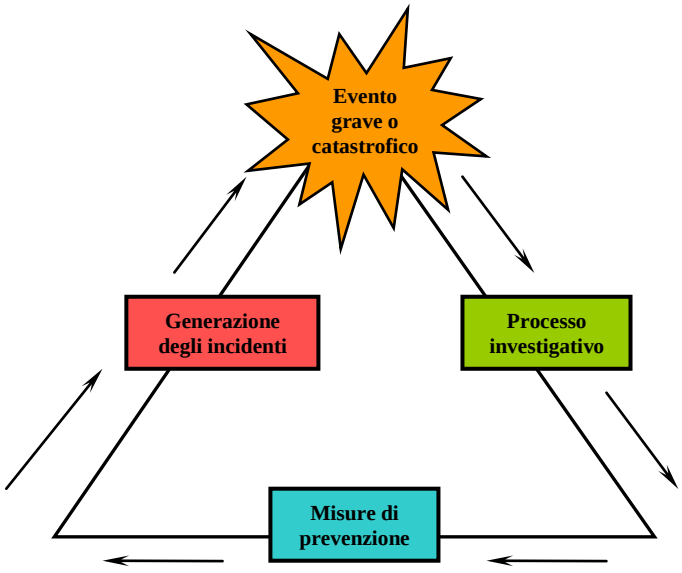
La “metafora del formaggio svizzero - **Swiss Cheese** ” rende bene l’idea delle barriere, delle difese, degli eventi dannosi e delle vittime.
Secondo la figura di seguito riportata, gli “strati” hanno dei buchi, dei vuoti e delle parti molle e quindi, non essendo compatto, permette il passaggio degli eventi disastrosi che si introducono nei fori delle fette attraversando le barriere di difesa, creando danni indesiderati.



Talvolta comportamenti involontari degli addetti comportano un “buco” nelle difese, ma spesso tali comportamenti sono la conseguenza di particolari condizioni di lavoro o di determinate decisioni prese dai vertici che favoriscono l’errore umano.

L’Anello Sequenziale di Prevenzione Incidenti (Accident Prevention Loop)

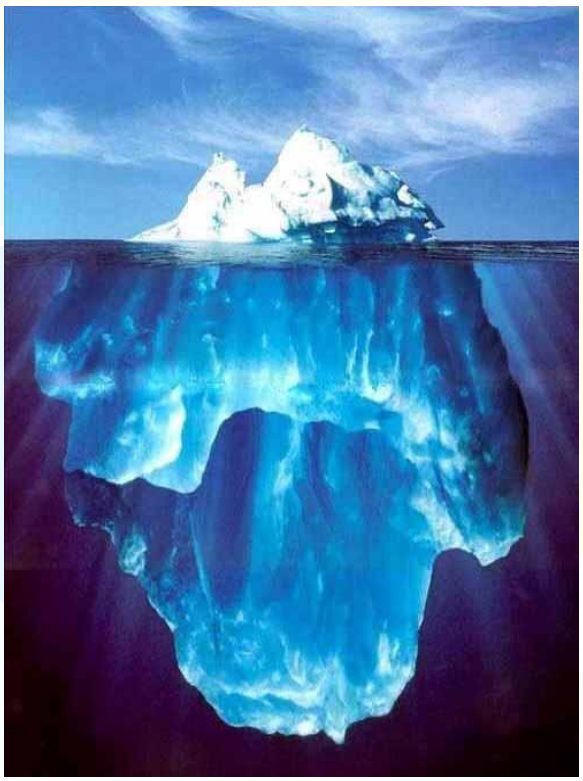
Ponendo in successione le diverse fasi dinamiche del sistema operativo di una organizzazione, si ottiene una configurazione del tipo riportato nella figura che segue.



Nella figura sono riportate le seguenti fasi:

- generazione degli incidenti;
- evento grave o catastrofico;
- processo investigativo;
- attuazione delle misure di prevenzione.

Tenendo conto delle fasi descritte, applicando gli opportuni adattamenti per ogni organizzazione, l'anello sequenziale della prevenzione consente un efficace Sistema di Gestione della Sicurezza (Safety Management System).



Nella figura viene illustrata la logica sequenziale che vede il processo investigativo iniziare dopo un evento grave o catastrofico che prevede l'analisi degli avvenimenti e l'adozione dei correttivi necessari in modo da arrivare al punto in cui il sistema ripropone un nuovo sviluppo degenerativo. La difficoltà di conoscere gli eventi sommersi di un sistema, ci fa venire in mente l'"*iceberg"* dove emerge solo una parte minima della struttura, mentre rende difficoltoso conoscere la parte sommersa che è quella necessaria da osservare per individuare le cause scatenanti del danno. Spetta alle aziende mettersi nelle condizioni di fare investigazione su tutti gli eventi di pericolo cercando di scoprire la parte sommersa dell'iceberg.

Bisogna sempre attuare e cercare di implementare una "***Cultura Proattiva***" atta a migliorare ed ottimizzare il giusto e più adeguato processo di gestione:

Cultura PATOLOGICA	Cultura BUROCRATICA	Cultura PROATTIVA
non si vuole sapere	si può non venire a sapere	si ricerca attivamente l'informazione
chi riferisce è sotto tiro	si ascolta se non si può evitare	si educa a riferire
la responsabilità è elusa	la responsabilità è a compartimenti stagni	la responsabilità è condivisa
chi sbagli viene ignorato e/o punito	gli sbagli portano a rimendi provvisori	gli sbagli provocano riforme attive
le nuove idee vengono attivamente represse	le nuove idee rappresentano un problema	le nuove idee sono benvenute

FATTORE UMANO IN AMBITO AEREO

Le grandi avarie degli impianti e gli errori operativi del personale sono oggi molto rari ma continuano a verificarsi errori decisionali in tutte le varie fasi di intervento umano.
Le statistiche mondiali sugli incidenti nell'aviazione civile individuano tali percentuali da attribuire al fattore uomo, macchina ed ambiente in relazione alla causa ultima che determina l'evento lesivo:

- 57% al fattore umano
- 26% a cause tecniche
- 6% al fattore ambientale
- 10% a fattori accidentali
- 1% a cause imprecisate

Lo studio del fattore umano non si rivolge solo al pilota che in quanto operatore diretto è al vertice della catena operazionale ma comprende progettisti, collaudatori, management, addestratori e ultimi, ma non per ordine di importanza, i controllori di volo (che rappresentano l'interfaccia operativa del pilota).
Recentemente la Flight Safety Foundation (USA) ha pubblicato un'interessante checklist delle motivazioni relazionabili al fattore umano che possono contribuire ad innestare l'incidente:

- Fattori sensoriali e percettivi

- Fattori di natura fisiologica

- Fattori legati a conoscenza e abilità

- Fattori legati alla personalità e alla naturale tendenza alla sicurezza

- Fattori legati al giudizio e al riconoscimento del rischio

- Comunicazione e coordinamento tra i membri dell'equipaggio

- Progettazione del sistema e delle procedure

- Supervisione ed organizzazione

FATTORE UMANO IN AMBITO NAVALE

Il *Capitano* di nave è il protagonista, il fattore prevalente e determinate del processo della navigazione; il suo ruolo centrale e decisivo lo coinvolge necessariamente nella maggior parte degli incidenti e dei sinistri marittimi.
In linea generale sono stati individuati, nelle analisi statistiche, una serie di fattori all'origine degli errori nel settore marittimo e quindi degli incidenti:

a. Scarsa competenza tecnica o imperizia in alcuni compiti e/o operazioni;
b. Esperienza inadeguata (difetto di prudenza, errata valutazione del rischio, …)
c. Prestazioni fisiologiche e psicologiche carenti (fatica, stress, distrazione, missioni…)
d. Organizzazione di bordo e di terra (difetto di comunicazioni, interpretazioni errate, scarsa sinergia, valutazioni difformi…).

Il **Codice IMO** fornisce la definizione di indagine a seguito di incidente, denominata "inchiesta di sicurezza".
L'obiettivo del processo di realizzazione di una indagine su un infortunio marittimo è quello di stabilire le circostanze inerenti l'infortunio, stabilire i fattori causali, pubblicizzare le cause dell'incidente e formulare adeguate raccomandazioni in materia di sicurezza.
Idealmente, un'indagine su un infortunio marittimo dovrebbe essere indipendente e separata da qualsiasi altra forma di inchiesta.
Le procedure da seguire da parte degli investigatori sono così elencate:
1. raccogliere informazioni sull'evento;
2. determinare la sequenza dell'evento;
3. identificare le azioni/decisioni e le condizioni pericolose;
e per ogni azione/decisione pericolosa,
4. identificare la tipologia di errore o di violazione;
5. identificare i fattori alla radice dell'evento ; e
6. identificare potenziali problemi di sicurezza e sviluppare delle azioni correttive.

La circolare MSC-MEPC.3/Circ.3 invece contiene delle modifiche relative alla definizione di incidente grave e alle caratteristiche dei rapporti sugli incidenti e gli infortuni in mare richiesti dalle convenzioni internazionali ***MARPOL*** e ***SOLAS***.
"**Incidente molto grave**": è un incidente relativo ad una unità navale tale da implicare la totale perdita della nave, la perdita di vite umane, o un grave inquinamento ambientale15;

"**Incidente grave**": è un incidente relativo ad una unità navale tale da non potersi qualificare come incidente molto grave, e che può implicare un incendio, una esplosione, una collisione, un arenamento, un contatto, dei danni da cattive condizioni meteo-marine, danni dovuti a ghiaccio, a cedimenti strutturali dello scafo, o a presunti difetti nello scafo, ecc., tali da provocare:
- il fermo dei motori principali, danni estensivi agli alloggi o gravi danni alla struttura della nave, come la sommersione dello scafo in acqua, ecc., tali da rendere l'unità navale incapace di continuare la navigazione senza pericolo per la nave stessa o l'equipaggio, o
- inquinamento ambientale (indipendentemente dalla quantità); e/o
- un guasto tale da richiedere il traino della nave o l'assistenza da terra.

"**Incidente di minore gravità**" è un incidente ad una unità navale tale da non potersi qualificare come incidente molto grave o incidente grave, e che, allo scopo della

registrazione di informazioni utili comprende anche gli “incidenti marittimi” (marine incident)16, che a loro volta comprendono gli incidenti pericolosi (hazardous incidents) ed i mancati incidenti (near misses).