ENAC
ENTE NAZIONALE PER L'AVIAZIONE CIVILE

Il Safety Management System (SMS)

Linee Guida e Strategie

Edizione 26 settembre 2005

DIREZIONE CENTRALE REGOLAZIONE TECNICA

Indice

1. Introduzione
Introduzione
Scopo

2. *Safety Management*: Linee Guida e Strategie
Safety Management System
Linee guida per la definizione di un *Safety Management (SM)*
Strategie di implementazione di un *Safety Management (SM)*

3. Documentazione per l'Assicurazione del Programma di Sicurezza *(SAD)*
Introduzione
Documentazione e Procedure

4. La metodologia
Introduzione
Risk Management
Tipo di Rischio

5. Il *Safety Auditing*
Introduzione
Scopo
Sorveglianza di Rispondenza
Aree e Livello di Rischio
Competenze del Personale e *Safety Manager*
Indicatori di misura delle prestazioni
Il processo *di Audit*

6. Linee Generali di Implementazione per Operatori di Trasporto Aereo
Introduzione
Cosa è un SMS per un Operatore di Trasporto Aereo ?
Implementazione

7. Allegati
Allegato 1 *Safety Review Board*
Allegato 2 Safety Action Group
Allegato 3 *Emergency Response Plan*

Bibliografia

1. Introduzione

L'obiettivo principale di questo documento è quello di identificare le linee guida per la definizione di una politica di sicurezza che tenga conto dei più recenti indirizzi internazionali, derivanti dall'esperienza dell'ultimo decennio, relativa ad una casistica di incidenti e disastri, dove le cosiddette "*management failures*" (avarie organizzative) si sono rivelate le cause principali di tali eventi.
Una politica volta all'identificazione dei potenziali rischi, derivanti da carenze organizzative che possono contribuire al verificarsi di un incidente, comporta l'adozione di un effettivo e formale *Safety Management System* basato su principi di minimizzazione del rischio associato a possibili avarie del sistema.
L'ENAC supporta lo sviluppo e l'adozione di un *Safety Management System* per tutte le organizzazioni che operano nell'ambito dell'Aviazione Civile finalizzato a :

- sviluppare un concetto di sicurezza e i relativi programmi di sviluppo proattivi in collaborazione con l'industria, per garantire che la crescita del traffico aereo non comporti un aumento degli incidenti fatali, con conseguente impatto negativo sulla comunità e sull' economia del settore
- promuovere lo sviluppo di una cultura orientata alla prevenzione in tutti i livelli organizzativi sui vari segmenti dell'industria aeronautica
- sviluppare un concetto di responsabilità della sicurezza condiviso e distribuito tra l'autorità e l'intera comunità aeronautica

L'*SMS* è un processo esplicito e sistematico per la gestione dei rischi. Come tutti i sistemi di gestione, determina, pianifica e misura le prestazioni per il raggiungimento degli obiettivi prefissati. Esso richiede una integrazione nel tessuto organizzativo nonché nella cultura e nel modo di lavorare delle persone.

Scopo

Il materiale contenuto in questo documento è applicabile a tutti le organizzazioni che operano nel settore aeronautico per l'istituzione di un *Safety Management System*.

2. *Safety Management:* Linee Guida e Strategie

Safety Management System

Il *Safety Management* è una disciplina, basata sull'applicazione di speciali tecniche di gestione sistematica, finalizzata alla identificazione e al controllo di eventi o condizioni indesiderate lungo tutto il ciclo di vita di un progetto, programma o attività. L'obiettivo principale è la prevenzione degli incidenti.
La prevenzione di incidenti può essere conseguita tramite l'identificazione, la valutazione, l'eliminazione o il controllo dei cosiddetti *safety-related hazards* fino a livelli considerati accettabili e controllabili. L'implementazione di una *SMS* richiede il coinvolgimento dei più alti livelli gestionali al fine di perseguire un programma che assicuri:

- la definizione di una filosofia di gestione che riconosca sempre l'esistenza di potenziali criticità per la sicurezza, definisca gli standard organizzativi e confermi che la sicurezza è responsabilità di tutti
- la determinazione di una strategia per il raggiungimento della sicurezza tramite l'identificazione di chiare responsabilità, ruoli e priorità aziendali
- l'identificazione delle procedure da implementare dirette a tutto il personale, dei mezzi per pianificare, organizzare, controllare e dei mezzi per monitorare e analizzare lo stato della sicurezza e i processi
- verifiche continue sulla realtà aziendale tramite adeguate ed efficaci procedure che valorizzino l'importanza di una cultura positiva della sicurezza e prevedano azioni correttive laddove vengono identificate eventuali criticità.

Definizione di una politica di *Safety Management (SM)*

Il processo di gestione della sicurezza deve essere inserito nella funzione globale di gestione di una organizzazione. Il modo tradizionale di pensare alla sicurezza è di evitare costi elevati, in realtà le spese derivanti da gravi incidenti hanno dimostrato che il binomio sicurezza ed efficienza produce un risultato positivo. La sicurezza paga in termini di riduzione delle spese e di aumento della produttività.
Un *SMS* favorisce in una organizzazione la capacità di anticipare ed indirizzare le criticità prima che esse portino ad un incidente. Le asserzioni alla base di una politica di *SM* dovrebbero definire l' approccio fondamentale da adottare per la gestione sia della sicurezza che dell'impegno profuso dall'intera organizzazione per la sicurezza stessa.
Di seguito sono elencati gli elementi fondamentali per una politica di gestione della sicurezza.

1. ***Safety Objective***
   Il *Safety Objective* definisce l'obiettivo che l'organizzazione intende traguardare attraverso il suo *SMS*. L'elenco degli obiettivi è solitamente documentato in un *business plan* e in specifiche operative.
2. ***Safety Management***
   L'organizzazione deve mostrare un impegno ai livelli più alti all'adozione di un approccio esplicito, proattivo finalizzato ad una gestione sistematica della sicurezza tramite l'utilizzo di procedure e strumenti analitici.
3. ***Safety Responsibility***
   L'organizzazione deve realizzare degli indirizzi atti a confermare che su ogni membro appartenente al sistema è allocata una responsabilità individuale e che la sua attività contribuisce alla prestazione globale dell'intero sistema. In aggiunta occorre identificare la figura e i requisiti del *Safety Manage*r responsabile della sicurezza.
4. ***Safety Priority***
   L'organizzazione deve dichiarare che le considerazioni relative ad aspetti di sicurezza hanno priorità elevata rispetto agli aspetti commerciali, operativi, ambientali e sociali.
5. ***Safety Standards* e rispondenza**
   L'organizzazione deve adottare appropriati standard di sicurezza e documentare i processi e le politiche inerenti alla *safety*.
   La rispondenza ai requisiti richiesti contribuisce a realizzare un *SMS* solido e a facilitare il processo di *safety oversight* tramite l'adozione di un *safety plan* per la verifica e revisione periodica dei *safety processes.* Il processo può essere integrato e completato con il processo di oversight del sistema qualità.
6. **Fornitori esterni di prodotti e servizi**
   L'organizzazione deve garantire che i fornitori esterni soddisfino gli standard di sicurezza e i mezzi di rispondenza da essa adottati internamente.

Strategia di implementazione di un *Safety Management (SM)*

La strategia proposta per l'implementazione di un *SM* riflette la pratica corrente utilizzata per la gestione della sicurezza e propone un'analisi sistematica dei processi per identificare le criticità del sistema sicurezza, in modo da intraprendere azioni correttive preventive, quindi non solo consequenziali ad eventi indesiderati, che assicurino che il livello di sicurezza è mantenuto o elevato.
I tre principi fondamentali sono:

1. **conseguimento della sicurezza**: definizione e realizzazione dei mezzi e dei metodi per il raggiungimento dei safety objectives prefissati;
2. **programma di assicurazione**: identificazione di mezzi adeguati ed efficaci per identificare i rischi e controllarli tramite fattori mitiganti;
3. **promozione di una cultura della sicurezza**: creazione di una cultura della sicurezza di tipo Top-Level e individuazione dei mezzi di

comunicazione interna più efficaci finalizzati all'eliminazione dei rischi e dei possibili errori ripetitivi che li generano.

1. Conseguimento della sicurezza
Livello di sicurezza

Il livello di sicurezza che una organizzazione aspira a raggiungere deve essere definito e globale. Di conseguenza è necessaria una indipendenza ma allo stesso tempo una condivisione di programmi, tra la prima linea di management e la funzione di *safety oversight*. Infatti per valutare e monitorare le prestazioni di un servizio o prodotto è necessario definire gli obiettivi di sicurezza che l'intera organizzazione intende traguardare per quel determinato prodotto o servizio.

System Safety Assessment

Un *hazard* è una condizione, evento o circostanza che può portare o contribuire a un evento indesiderato o imprevisto, e di conseguenza ridurre la capacità di svolgere una funzione prescritta di un sistema.
Il rischio è una espressione dell'impatto dell'evento indesiderato in termini di severità e probabilità dell'evento stesso.
L'utilizzo di un processo di *Risk Assessment* permette di definire le funzioni e le interfacce di un sistema, identificare i potenziali *hazards* associati, misurare il rischio e valutare possibili fattori di compensazione o mitigazione da attuare per riportare il livello del rischio a valori accettabili in relazione agli obiettivi di sicurezza prefissati.

Competenza

La competenza del *top management* e del personale di una organizzazione è l'elemento fondamentale per il conseguimento della sicurezza.
Adeguate procedure di reclutamento e piani di formazione continua devono garantire che tutto il personale sia competente, addestrato e conosca le sue responsabilità. L'adozione di un *emergency response planning* rivolto a tutti i rami dell'organizzazione può facilitare la coscienza della responsabilità.

2. Programma di assicurazione
Audit di sicurezza

Lo strumento degli *audit* è parte integrante del meccanismo proattivo di gestione tramite il quale i rischi potenziali all'interno delle operazioni di una organizzazione vengono identificati e controllati al fine di assicurare e mantenere gli obiettivi prefissati dal *Safety Management System*.
L'implementazione di un piano di audit richiede procedure approvate e pubblicate per la conduzione delle investigazioni. Tale piano non può prescindere dall'adozione di un sistema di comunicazione efficace diretto verso il livello appropriato di *management* finalizzato alla condivisione [illegible] risoluzione dei *safety concern*s.

Monitoraggio della prestazione

I dati di sicurezza di un sistema possono deteriorarsi a seguito di cambiamenti a carico dell' ambiente operativo verificatisi o richiesti nel tempo.
Queste modifiche debbono essere individuate e trattate in modo da assicurare che l'organizzazione continua a rispondere ai suoi obiettivi di sicurezza.
Uno strumento di analisi delle prestazioni e di monitoraggio delle modifiche organizzative richiede dei sistemi di gestione dei dati rilevati da integrare nel processo di *Risk Assessment*.

Occorrenze significative

In aggiunta ai requisiti regolamentari che impongono attività obbligatorie di *reporting* di incidenti e inconvenienti, occorrerebbe istituire un processo di investigazione delle occorrenze significative che identifichi le avarie organizzative nella gestione della sicurezza tramite l'adozione di indicatori di misura della prestazione. I risultati più significativi, condivisi con l'autorità e l'esperienza di altre organizzazioni, dovrebbero indicare le aree che richiedono un monitoraggio più attento finalizzato alla prevenzione e non alla correzione del potenziale evento critico.

3. Promozione di una cultura della sicurezza

Che cosa è la cultura della sicurezza?

La cultura di una organizzazione è definita dal sistema dei comportamenti delle persone che ad essa appartengono.
Le azioni intraprese rispecchiano i valori dell'intera organizzazione. L'impegno dei dirigenti e del resto del personale sulle tematiche di sicurezza richiede una vera rivoluzione di pensiero che impone uno sforzo preliminare sul progetto, programma o prodotto, basato su un concetto di sicurezza attiva e non passiva. Si ottiene così un guadagno in termini di costi gestionali e benefici di prestazione: prevenire un errore costa meno che correggere a posteriori.

Una cultura di sicurezza è:

- una cultura che informa le persone sui pericoli e i rischi relativi alle loro operazioni e su come gestirli
- una cultura di educazione che non tollera violazioni e che condivide con tutto il sistema ciò che è accettabile o meno
- una cultura che incoraggia il *reporting* per correggere deficienze, proporre soluzioni e non per punire
- una cultura di insegnamento e di apprendimento continuo per tutta l'organizzazione

Quanto sopra non giustifica comportamenti collegati a gravi negligenze che nell'ottica di un approccio globale alla sicurezza dovrebbero essere isolati e neutralizzati dall'organizzazione stessa.

Chi è il *Safety Manager*?

Il *Safety Manager,* responsabile della gestione delle problematiche afferenti la sicurezza del volo, è una figura di riferimento che riporta, in materia di sicurezza, direttamente ai più alti livelli organizzativi (*Accountable Manager*).
I requisiti minimi del *Safety Manager* sono:

- adeguata e certificata conoscenza di base ed esperienza nel settore di interesse dell'organizzazione
- adeguata formazione e conoscenza delle tecniche di *Safety* e *Risk Management, Human Factor* e di investigazione degli incidenti
- autorevole capacità di aggregazione e coinvolgimento

Il *Safety Manager* deve avere chiare responsabilità, ad esempio, di:

- gestione dello sviluppo del piano di sicurezza
- promozione di strumenti di *Hazard Management, Risk Assessment e Human Factor*
- gestione dell' *Emergency Response Planning*
- investigazione di incidenti ed inconvenienti
- raccolta e distribuzione di informazioni relative alla sicurezza (tramite il *reporting* ad es. dei *Post Holders*)
- formazione continua del personale sulla gestione della sicurezza e della qualità
- gestione e controllo della documentazione di sicurezza e qualità
- gestione degli incontri del *Safety Review Board* (All.1) e del *Safety Action Group* (All. 2)

3. Documentazione per l'Assicurazione del Programma di Sicurezza (*SAD Safety Assurance Documents*)

Introduzione

Una politica e una strategia efficace di un *SMS* richiedono la definizione ed il controllo delle operazioni e delle modifiche che influenzano la sicurezza. Laddove un *hazard* viene identificato occorre effettuare una valutazione di sicurezza. Le valutazioni effettuate, i loro risultati e le procedure messe in atto per il raggiungimento degli obiettivi di sicurezza devono essere adeguatamente documentate. Indipendentemente dalle forme di presentazione i documenti di assicurazione di sicurezza (*SAD*) devono contenere tutte le informazioni e le evidenze che le operazioni soddisfano gli appropriati standard di sicurezza.
Di seguito sono indicate delle linee guida generali utilizzate per la struttura del *SAD*.

Documentazione e Procedure

La documentazione di assicurazione di sicurezza richiede un sistema di controllo che accerti lo stato di revisione e di implementazione della documentazione,tale sistema può essere in carico al sistema qualità. I requisiti regolamentari e di sicurezza adottati dall'organizzazione debbono essere chiaramente indicati e documentati.
Tali requisiti possono includere sia quelli direttamente derivati dalla politica di gestione della sicurezza dell'organizzazione, sia quelli richiesti dalla normativa nazionale ed internazionale.
La documentazione minima di un *SMS* deve comprendere:

- la pubblicazione della policy di sicurezza dichiarata dal *CEO (Chief Executive Officer)*
- la struttura del *SMS* (organigramma)
- le responsabilità del *Safety Manager*, del *Safety Review Board* (All.1*)* e del *Safety Action Group* (All.2)
- definizione e descrizione delle responsabilità
- processo di *Hazard Identification e Risk Management*
- processo di *Safety Reporting* e *Safety Review*
- *Safety oversight*, *Safety plans*
- criteri di reclutamento e formazione del personale

4. La metodologia

Introduzione

L'adozione di un *Safety Management System* implica la valutazione da parte di una organizzazione delle attività, operazioni e modifiche ad esse associate di influenza sulla sicurezza. Il termine di sicurezza indica genericamente il risultato che riporta la severità e la probabilità, associata al rischio di un evento indesiderato, comunque presente nella attività umana, ad un livello di tolleranza accettabile per la comunità, tramite l'adozione di misure di mitigazione e valutazione del rischio residuo.
Il processo di *Safety Assessment* dovrebbe verificare e documentare che l'intero sistema, analizzato in tutte le sue parti, contribuisce al raggiungimento e al mantenimento del livello di sicurezza richiesto.
Il processo utilizzato è di tipo decisionale, formale e documentato volto a mettere in relazione il rischio e la relativa conseguenza sull'intero ciclo di vita del sistema. La selezione dei metodi di calcolo del rischio è flessibile.

Processo di *Risk Management*

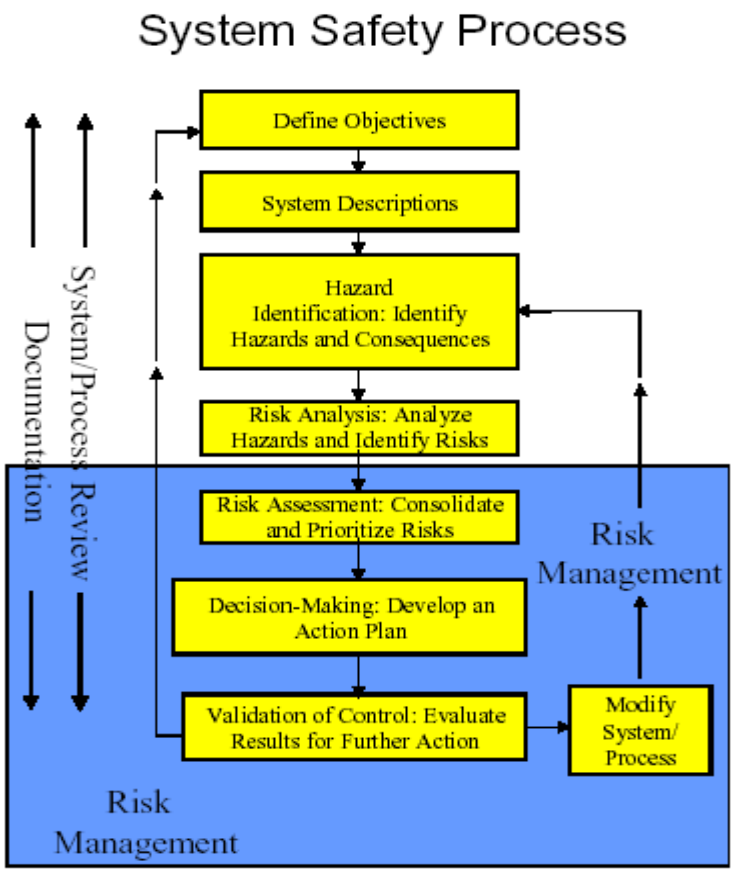
Il Risk Management si colloca all'interno del più generico processo di System Safety, illustrato nel diagramma riportato alla pagine seguente.
I passi fondamentali di un *Risk Management* sono:

1. **piano specifico (*Business Plan*)**
   In primo luogo è necessario compilare un piano specifico per l'individuazione delle componenti del sistema descritto, la valutazione delle singole condizioni di criticità ad esse associate e per l'identificazione dei rischi e dei relativi livelli di tolleranza. Le componenti principali di un sistema riportate in un *business plan* sono elencate di seguito:

   - personale
   - strumenti
   - procedure
   - materiali
   - equipaggiamenti
   - stabilimenti
   - *software*
   - ambiente esterno

Objective	Performance measures
Business Objective: Reduce Costs	Reduction in insurance rates
Safety Objective: Decrease number and severity of hangar incidents	❑ Total number of events ❑ Number of damage-only events ❑ Number of near-miss accidents ❑ Lessons learned from event analyses ❑ Number of corrective action plans developed and implemented

Esempio di un ***business plan***



2. Identificazione degli *hazard*

Il passo successivo è l'identificazione di una lista globale *Preliminary Hazard List (PHL*) delle possibili funzioni, condizioni e attività interne ed esterne ad un sistema che comportano potenzialmente un rischio alla salute umana o alla sicurezza. Allo scenario di ogni *hazard* deve essere associato il relativo effetto indesiderato. Lo scenario deve indicare le risposte alle domande: Chi? Cosa? Dove? Quando? Perché e Come? La *PHL* in definitiva elenca le funzioni di un sistema, individua le possibili avarie, le condizioni in cui esse possono verificarsi e le loro conseguenze sull'intero sistema.

3. Analisi del rischio: severità e probabilità di occorrenza

L'analisi è finalizzata alla individuazione dei due parametri che caratterizzano il rischio: la severità e la probabilità di occorrenza. La severità è determinata dalla condizione potenzialmente più critica che può verificarsi. L'effetto più severo deve essere considerato indipendentemente dalla probabilità associata. La probabilità di occorrenza è determinata da quante volte un pericolo previsto si verifica associato alla severità peggiore. Quando viene determinata la probabilità, il valore di severità peggiore determina gli stati più critici del sistema. Lo stato di un sistema può essere associato a una varietà di condizioni pericolose, che includono ma non sono limitate a: (1) luogo, (2) modo, (3) velocità, (4) procedure operative, (5) tipo di operazioni, (6) energia, (7) ambiente operativo, (8) procedure ambientali e (9) fattore umano.
Gli *hazards* sono solitamente la conseguenza di una o più cause, che possono essere di natura tecnica o procedurale. Il rischio, infatti, è l'espressione dell'impatto sul sistema di un evento indesiderato, in termini di severità e probabilità dell'evento stesso e nella condizione operativa più critica del sistema. Le definizioni riportate nelle pagine seguenti alle tabelle in fig. 1 e 2 sono comuni a livello internazionale; in particolare sono state estratte dalle definizioni riportate nelle norme *EASA Certification Specification/FAA CS/FAR 25*.1309, Eurocontrol ESARR 4 e nell'*FAA System Management Program Document .*
Tali definizioni di severità sono adottate nella *safety e risk analysis* relativa agli aeromobili CS/FAR 25, nel processo di *risk assessment e mitigation* nell'*ATM* (*Air Traffic Management*) e dalla FAA (Federal Aviation Administration) nel trasporto pubblico.

Effect On	Hazard Severity Classification				
	No Safety effect (5)	**Minor (4)**	**Major (3)**	**Hazardous (2)**	**Catastrophic (1)**
General		Does not significantly reduce system safety. Required actions are within operator's capabilities. Includes: (1) Slight reduction in safety margin or functional capabilities; (2) Slight increase in workload such as routine flight plan changes; (3) Some physical discomfort to occupants or aircraft (except operators); - Minor occupational illness and/or minor environmental damage, and/or minor property damage	Reduces the capability of the system or operators to cope with adverse operating condition to the extent that there would be: (1)Significant reduction in safety margin or functional capability (2)Significant increase in operator workload (3)Conditions impairing operator efficiency or creating significant discomfort (4) Physical distress to occupants of aircraft(except operator) including injuries - Major occupational illness and/or major environmental damage, and/or major property	Reduces the capability of the system or the operator's ability to cope with adverse conditions to the extent that there would be : (1) Large reduction in safety margin or functional capability (2)Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (3) Serious or fatal injury to small number of occupants of aircraft (except operators) - Fatal injury to ground personnel and/or general public	Total loss of systems control such that (see below):
Air Traffic Control	Slight increase in ATC workload	Slight reduction in ATC capability, or significant increase in ATC workload	Reduction in separation as defined by a low/moderate severity operational error (as defined in FAA Order 7210.56), or significant reduction in ATC capability	Reduction in separation as defined by a high severity operational error (as defined in FAA Order 7210.56), or a total loss of ATC (ATC Zero)	Collision with other aircraft, obstacles, or terrain
Flying people	No effect on flight crew Has no effect on safety Inconvenience	Slight increase in workload Slight reduction in safety margin or functional capabilities Minor illness or damage Some physical discomfort	Significant increase in flight crew workload Significant reduction in safety margin or functional capability Major illness, injury, or damage Physical distress	Large reduction in safety margin or functional capability Serious or fatal injury to small number - Physical distress/ excessive workload	Outcome would result in: Hull loss Multiple fatalities

Fig. 1 – Definizione Severità

	NAS Systems			Flight Procedures	ATC Operational	
	Quantitative	Qualitative			Periodicity	
		Individual Item/System	ATC Service/NAS Level System		Per Facility	NAS-Wide
Probable A	Probability of occurrence per operation/ operational hour is equal to or greater than $1x10^{-3}$	Expected to occur about once every 3 months for an item	Experienced continuously in the system	$P \geq 1 X 10^{-5}$	Expected to occur more than once per week	Expected to occur more than every 1-2 days
Frequent B	Probability of occurrence per operation/ operational hour is less than $1x10^{-3}$, but equal to or greater than $1x10^{-5}$	Expected to occur about once per year for an item	Expected to occur frequently in the system		Expected to occur about once every month	Expected to occur about several times per month
Remote C	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$	Expected to occur several times in life cycle of an item	Expected to occur numerous times in system life cycle	$10^{-5} \leq P \geq 10^{-7}$	Expected to occur about once every year	Expected to occur about once every few months
Extremely Remote D	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system's life cycle	$10^{-7} \leq P \geq 10^{-9}$	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years
Extremely Improbable E	Probability of occurrence per operation/ operational hour is less than $1x10^{-9}$	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	$P \leq 10^{-9}$	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years

Fig.2 – Definizione Probabilità

Per ogni *hazard* la determinazione della severità e della probabilità di occorrenza può avvenire tramite analisi quantitativa o qualitativa (*Preliminary System Safety Analysis*) in relazione ai dati disponibili. Si riporta di seguito il modello solitamente utilizzato per l'analisi *(Bow Tie Model*) fig.3.
Il modello è un approccio strutturato nel quale cause e *hazard* sono direttamente collegate alle possibili conseguenze.

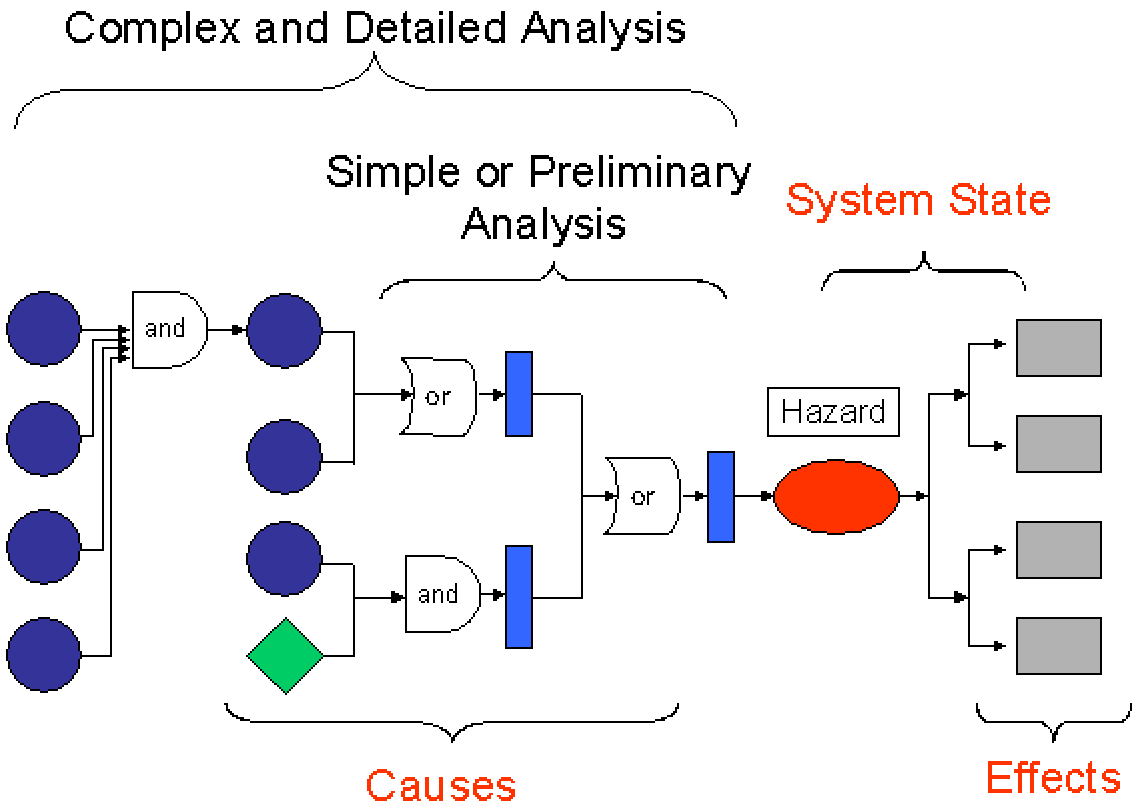


Fig. 3 *Bow Tie Model*

Il modello *Bow-Tie* è di supporto alle fasi generali del processo di SM:

- descrizione del Sistema
- identificazione degli *hazards*
- analisi del rischio
- valutazione del rischio
- mitigazione del rischio

La parte sinistra del diagramma è visualizzata come una *Fault Tree Analysis* (FTA). La *FTA* è utilizzata per modellare i modi possibili in cui un dato *hazard* può manifestarsi come conseguenza di cause identificate in un sistema, considerando i fattori di mitigazione che possono essere utilizzati per prevenire le avarie che causano l'*hazard* stesso. La parte destra del diagramma può essere vista come una *Event Sequence Analysis*. Questa

analisi modella lo stato del sistema e la condizione più sfavorevole, o l'insieme di tali condizioni, che possono ragionevolmente presentarsi durante il ciclo di vita di un sistema, considerando i possibili fattori mitiganti da incorporare per prevenire il verificarsi di un incidente, nel caso si verifichi un evento indesiderato.

4. Risk Assessment (Risk Consolidation – Characterization fig.4*)*

Il *Risk Assessment* è quel processo che compara gli elementi associati al rischio, determinato con l'analisi, ai criteri di accettabilità stabiliti nel *business plan* anche tramite l'associazione di più rischi e l'individuazione di parametri comuni di mitigazione.
Una lista dei rischi classificati e la relativa priorità dovrebbero essere di ausilio nel processo decisionale.

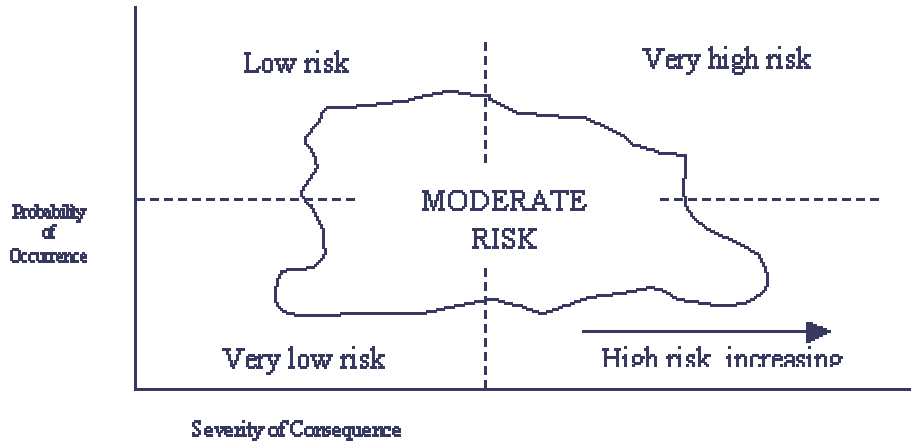


fig. 4 *Risk Characterization*

La matrice riportata di seguito, la cosidetta *Predictive Risk Matrix*, Figura 4.2.1, riflette la definizione di rischio essendo la composizione dei fattori severità (*severity*) e probabilità (*likelyhood*). Questa matrice, comunemente utilizzata, classifica il rischio in tre livelli: alto (*High*), medio (*Medium*) e basso (*Low*). Questi livelli definiscono come il processo di *safety assessment* conduce alla risoluzione del rischio determinato per ogni hazard individuato in accordo con le figure 1 e 2.

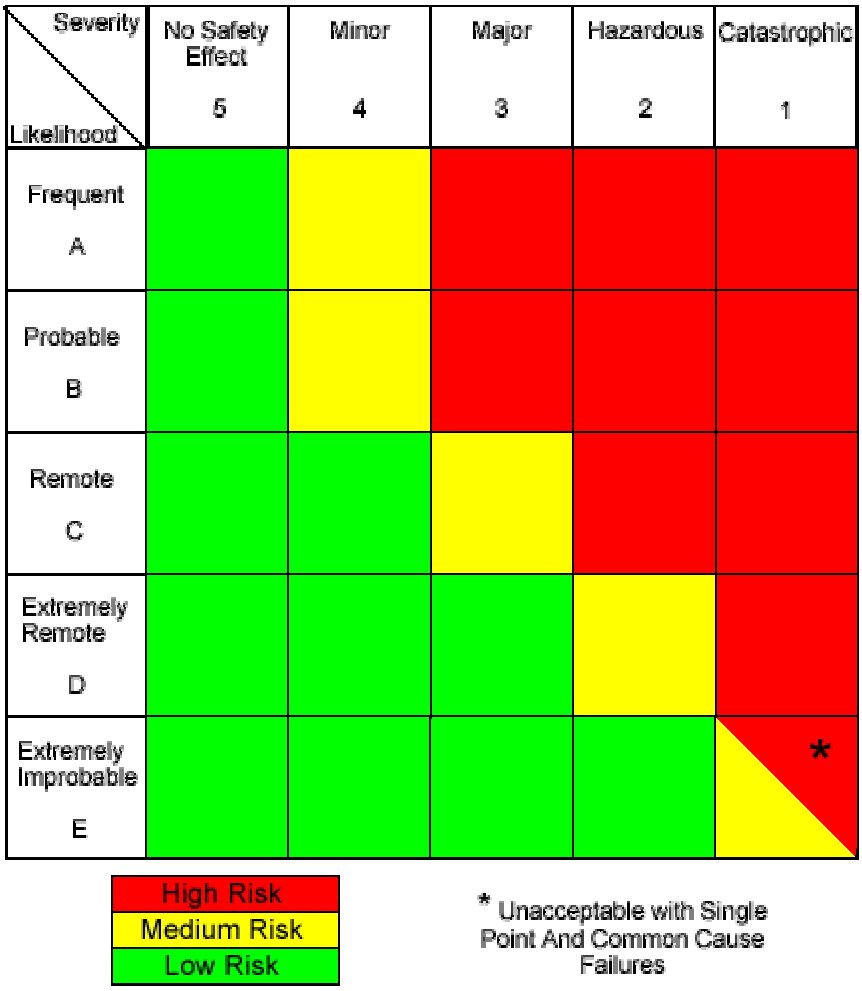


Figure 4.2.1 - Predictive Risk Matrix

High Risk - Unacceptable risk. Tracking in a Hazard Tracking Risk Resolution System is required until the risk is reduced or accepted at the appropriate management level.

Medium Risk - Acceptable with review by the appropriate mangement level. Tracking in a Hazard Tracking Risk Resolution System is required.

Low Risk - Target Level. Acceptable without review, restriction or limitation. Hazards are documented in HTRR System

Figure 4.2.2 - Risk Acceptance Criteria

5. Processo decisionale e sviluppo Piano di Azione

Il processo decisionale è una delle fasi più importanti del *Risk Management* in quanto indica come affrontare ogni rischio in relazione alla priorità assegnatagli.
Le possibili azioni da intraprendere per trattare un rischio sono :

- Trasferire
- Eliminare
- Accettare
- Mitigare e Tracciare

Tali azioni, idonee a trattare ogni condizione di rischio, costituiscono Piano di Azione.

6. Valutazione e controllo del Piano di Azione

A seguito dell'identificazione delle aree di rischio deve essere sviluppato un piano per l'implementazione di strategie di mitigazione o eliminazione del rischio associato.
Il rischio deve essere tracciato e l'efficacia dell'azione di mitigazione deve essere verificata e monitorata al fine di eliminare il rischio o ridurlo a livelli accettabili. Tutte le modifiche apportate ad una parte del sistema, progetto o organizzazione per ridurre il livello di rischio o per mancato effetto dell'azione mitigante, richiedono un nuovo *Risk assessment*.

Tipi di Rischio

I tipi di Rischio possono essere diversi. Generalmente il *Risk Management* classifica il rischio in tre tipi: *Initial Risk, Current Risk* e *Residual Risk.*

Initial Risk: è il rischio associato alla severità e alla probabilità relativa ad un hazard identificato in uno stadio preliminare o iniziale di decisione, programma o analisi dello stato del sistema.

Current Risk: è il rischio associato alla severità e alla probabilità predetta di un hazard relativa allo stadio corrente del sistema. Il *Current Risk* può variare in base alle azioni intraprese dall'organizzazione relative ai controlli o alle verifiche messe in atto.

Residual Risk: è il rischio residuo che continua a permanere a seguito dell'implementazione e della verifica di tutte le tecniche di controllo utilizzate dal sistema. Nella valutazione del *Residual Risk* deve essere considerato che tutti i controlli sono stati attuati e verificati e che, in aggiunta, anche i requisiti di mitigazione raccomandati sono stati implementati e validati.

I metodi di *Risk Assessment* si basano sull'introduzione di S*afety Requirements* da valutare durante il processo di analisi. Infatti in generale si usa con questo termine indicare quei requisiti utilizzati dal sistema per controllare gli hazard associati ad alto e medio rischio. Essi sono specificati e documentati nel *Safety Requirements Verification Table.* Tra i requisiti raccomandati, i cosiddetti *Recomended Safety Requirements*, in particolare, sono quei requisiti che l'ingegneria di analisi di sicurezza introduce come potenziali fattori di mitigazione dell'hazard. Preliminarmente alla fase di validazione di tali requisiti da parte del sistema, la loro introduzione nell'analisi porta alla determinazione di un *Preliminary Residual Risk.* Fino alla verifica e alla validazione della loro efficacia da parte del *SMS* essi possono essere definiti con il termine *Candidate Safety Requirements.* Al termine del processo di validazione essi vengono identificati come *Validated Safety Requirements.* I *Recommended Safety Requirements* associati alla descrizione degli hazard sono documentati e mantenuti nel documentio di tracciamento degli *hazard* (*Hazard Tracking System*) fino quando tutti i *Candidate Safety Requirements* risultano validati e verificati.

5. *Safety Auditing*

Introduzione

L'implementazione di un *Safety Management System* richiede una verifica continua sui processi e sui risultati dell'organizzazione al fine di garantire il raggiungimento e il monitoraggio dei livelli di sicurezza prefissati. Il processo di auditing è lo strumento di verifica utilizzato dal sistema di assicurazione di qualità. Nell'ambito di un *SMS* esso è finalizzato alla verifica dei parametri di sicurezza dei processi e delle funzioni ad essa strettamente connessi. Il *Safety Auditing* può essere integrato nel Sistema Qualità.

Scopo

Un sistema di *safety regulatory audit* è basato su quattro elementi fondamentali:

1. sorveglianza continua di rispondenza del sistema ai principi del *SMS*
2. aree e livello di rischio
3. competenza del personale e del responsabile addetto alla sicurezza
4. indicatori di prestazione

Ognuno di questi elementi deve essere applicato sia alle operazioni e/o aree del sistema che a tutte le modifiche ad esse apportate nel corso del tempo.

Sorveglianza per la verifica continua di rispondenza del *SMS*

Le aree di un sistema da sottoporre ad *audit* sono tutte quelle riconducibili al *SMS* e ad eventuali approvazioni o licenze rilasciate dall'autorità all'organizzazione, in conformità alla regolamentazione internazionale EASA/JAA e/o nazionale.

Il piano di *audit* deve considerare:

- le aree, i processi e le funzioni
- la documentazione e le procedure
- i mezzi di rispondenza utilizzati
- i piani di formazione del personale

Aree e Livello di Rischio

Le attività di una organizzazione che adotta un SMS devono essere adeguatamente sicure e tutte le procedure e i processi significativi, dal punto di vista della sicurezza delle operazioni, devono essere oggetto di revisione per dimostrare la conformità continua nel tempo agli obiettivi di sicurezza dell'organizzazione. Il risultato del *risk assessment* e il conseguente piano di azione sono oggetto di verifiche programmate.

Competenza del Personale e del *Safety Manager*

Nella sezione 2 è riportata una breve descrizione della responsabilità e del ruolo ricoperto dalla figura del *Safety Manager* in una organizzazione che adotta un *SMS.* Il *Safety Manager* risponde direttamente all'*Accountable Manager* dell'organizzazione ed è responsabile del programma di sicurezza aziendale a cui devono rispondere tutti i settori coinvolti. Di seguito sono riportate le competenze ritenute fondamentali per questo ruolo:

- possedere una conoscenza generale dell'organizzazione (Missione, attività, processi, procedure, operazioni)
- possedere una adeguata esperienza manageriale e una capacità di analisi/sintesi con particolare attenzione ai possibili settori di attività (es. Operazioni Volo, Manutenzioni, Operazioni di Terra)
- possedere una formazione specifica di base tale da permettergli di governare i processi di *risk management* aziendali
- possedere adeguata formazione sulle tecniche di *safety management* e di investigazione degli incidenti

Il personale coinvolto negli *audit* di sicurezza deve possedere adeguate competenze di base sui processi dell'organizzazione, sulle tecniche di *audit*. Deve inoltre conoscere e condividere le politiche di *SMS* aziendali.

Indicatori di misura delle prestazioni

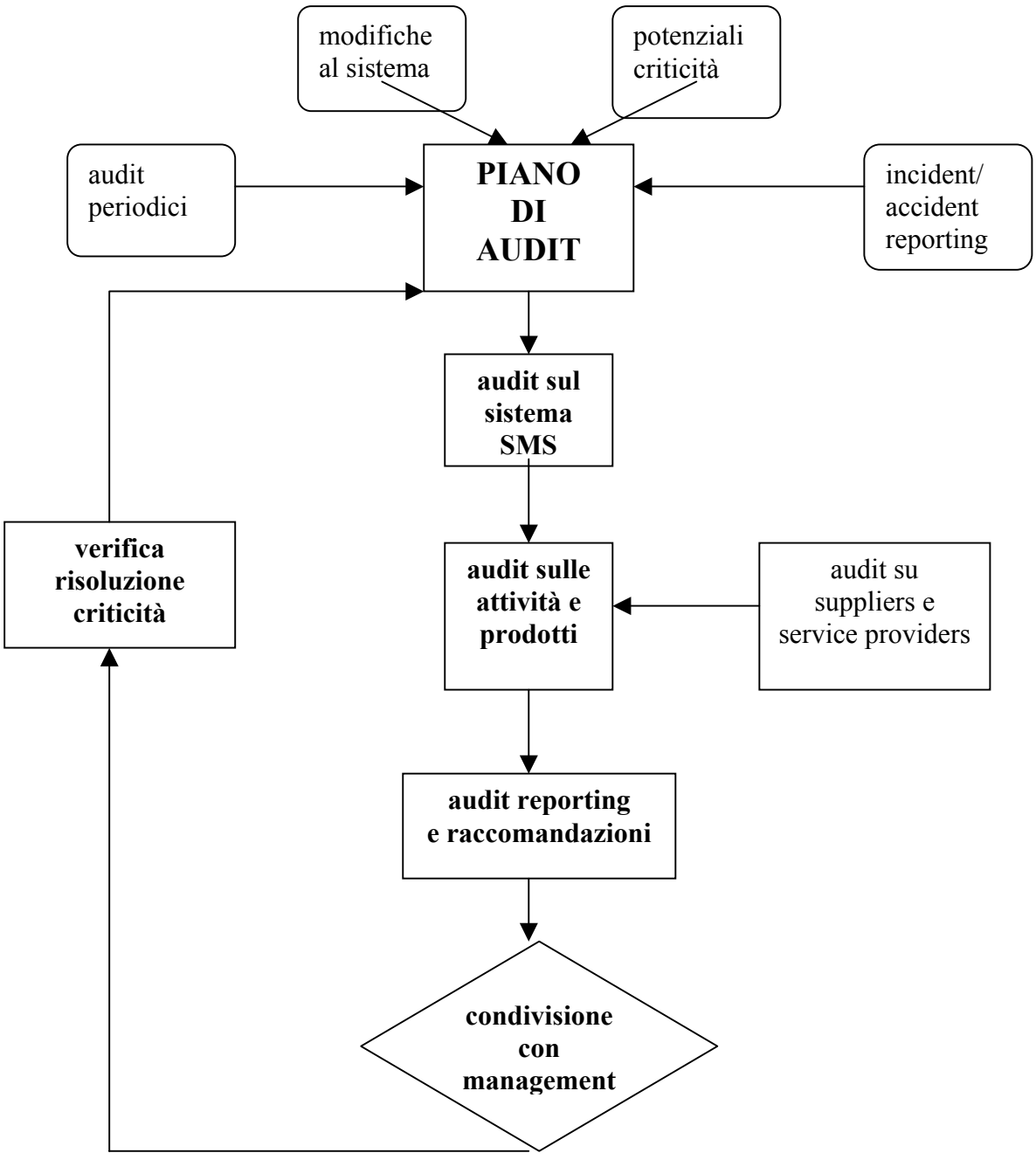
Gli indicatori di prestazione sono uno strumento che può essere usato da una organizzazione per verificare e misurare l'efficacia delle procedure di *safety management*.
L'identificazione di adeguati indicatori permette ad una organizzazione di trattare gli aspetti relativi alla sicurezza con un approccio proattivo e non reattivo. Infatti, i dati relativi agli indicatori selezionati, nel caso di una tendenza negativa, richiedono una azione immediata da parte dell'organizzazione.
I tipici indicatori di sicurezza sono basati sul numero di incidenti, di inconvenienti e sulle occorrenze. Fortunatamente questi eventi indesiderati non sono frequenti nella vita di una organizzazione, abbassano notevolmente il livello di prestazione del sistema e lasciano la possibilità di intervenire solo a posteriori. L'organizzazione dovrebbe, invece, individuare indicatori di prestazione addizionali che diano un riscontro immediato del decremento di prestazione del sistema prima che si determini l'evento indesiderato, anche tramite la condivisione dell'esperienza maturata da altre organizzazioni del settore.
In aggiunta, il sistema deve assicurare, laddove pertinente, l'informazione all'Autorità sulle eventuali modifiche apportate alle sue operazioni, sui risultati delle valutazioni effettuate e le implicazioni connesse alla loro implementazione.

Il processo di *Audit*

Il processo di *audit* è composto da varie fasi

1. preparazione
2. pianificazione
3. ispezione
4. gestione delle modifiche
5. *audit reporting*: azioni e raccomandazioni
6. condivisione con il Management

Le azioni e le raccomandazioni scaturite dall'attività di *auditing* richiedono una condivisione ai più alti livelli organizzativi al fine di ottenere una azione efficace volta alla risoluzione delle criticità individuate e alla riduzione o eliminazione dei rischi associati. Nel caso le azioni da implementare avessero come oggetto fornitori esterni all'organizzazione, gli accordi commerciali e i piani di qualità devono chiaramente individuare le assolute priorità delle tematiche attinenti la sicurezza, favorendo azioni di mitigazione ed eliminazione di potenziali criticità anche in seno ad organizzazioni terze.
Si riporta di seguito un generico diagramma che descrive le fasi principali relative ad un processo di *audi*t per un *SMS*.


modifiche al sistema
potenziali criticità
audit periodici
PIANO DI AUDIT
incident/ accident reporting
audit sul sistema SMS
verifica risoluzione criticità
audit sulle attività e prodotti
audit su suppliers e service providers
audit reporting e raccomandazioni
condivisione con management

6. Linee Generali di Implementazione di un *Safety Management System* per Operatori di Trasporto Aereo

Introduzione

La norma JAR-OPS 1.037 richiede che "*an operator shall establish an accident prevention and flight safety programme, which may be integrated with the Quality System: including programmes to achieve and maintain risk awareness by all persons involved in operations……* ". Tale requisito è basato sul documento ICAO *Recommended Practice* (Annex 6 Pt 1) e il materiale di guida e descrizione del concetto di Safety Management System è fornito nel documento ICAO Doc 9422 (*Accident Prevention Manual*).
Nelle sezioni precedenti sono riportati i concetti generali di una politica di *Safety Management*.
L'ENAC ritiene fondamentale la condivisione di tali concetti nei settori relativi alle operazioni e alla manutenzione.

Cosa è un *SMS* per un Operatore di Trasporto Aereo?

Il *Safety Management* di un Operatore è in particolare la gestione sistematica dei rischi associati alle operazioni di volo, operazioni a terra e alle attività di *aircraft engineering* e manutenzione, finalizzata ad ottenere elevati livelli di prestazione della sicurezza. La perdita di un aeromobile è un evento indesiderato che nessuna compagnia desidera si presenti nel corso della sua attività sia per ragioni di sicurezza che finanziarie. Un *SMS* tende a rendere la sicurezza un bene finanziario e non un onere a se stante, esso si integra o interfaccia con il Sistema di Qualità dell'Operatore ed insieme costituiscono il *core management* dell'organizzazione.
Il successo delle prestazioni di una compagnia è direttamente collegato all'esistenza di una cultura positiva della sicurezza a tutti i livelli organizzativi. I concetti elaborati nelle sezioni precedenti si applicano direttamente anche all'organizzazione di un operatore aereo e ai suoi fornitori di servizi.

In particolare sono da sottolineare i seguenti punti fondamentali:

1. l'*SMS* di un operatore comporta un approccio pragmatico costruito laddove possibile sulle procedure e i processi del Sistema Qualità, in particolare l'SMS identifica e indica le priorità di utilizzo delle risorse allo scopo di trattare il rischio e aumentare il livello di efficienza
2. promuove l'adozione nelle attività del concetto di "*best practice standards"*
3. l'SMS richiede come visto in precedenza una formalizzazione ed una integrazione a livello di organizzazione. Tutte le aree contribuiscono individualmente e globalmente al raggiungimento dei livelli di sicurezza stabiliti. Le Operazioni Volo, l'*Engineering*, la Manutenzione e le Operazioni a Terra insieme alle altre aree devono avere i loro processi e procedure approvate nell'ambito del *SMS* della compagnia

4. il contratto di servizi stipulato dall'Operatore per eventuali funzioni date in *outsourcing* (es. manutenzione, *handling*), richiede un esplicito requisito da parte del fornitore di servizi relativo all'adozione di un proprio *SMS* conforme a quello dell'operatore

Molte procedure e pratiche stabilite attualmente dagli operatori sono di tipo reattivo, e vengono messe in atto a seguito di eventi non desiderati. Il sistema di gestione previsto da un *SMS* richiede una evoluzione della gestione della sicurezza di tipo proattivo, senza escludere l'aspetto reattivo in quanto fornisce i mezzi per anticipare, prevenire o ridurre l'effetto dei rischi. A tale scopo è necessaria una stretta collaborazione con la gestione Qualità dell'operatore.

Implementazione

A completamento di quanto indicato nella sezione 2 sono riportati i punti chiave per l'implementazione del *SMS* in un Operatore:

1. approccio globale alla sicurezza
2. principi organizzativi e gestionali volti alla assicurazione di sicurezza
3. adozione di sistemi per la s*afety oversight*

Approccio globale alla sicurezza

La compagnia deve definire e documentare tramite il *Safety Management System Manual* il diagramma dell'organizzazione, le responsabilità, i processi e le procedure attinenti la sicurezza. Il manuale deve essere condiviso dal *Top Management* e firmato dall'*Accountable Manager.* La responsabilità individuale e collettiva deve essere definita, documentata e considerata uno dei parametri per la misura delle prestazioni del sistema. A tale scopo deve essere indicata la figura del S*afety Manager* e stabilito un *Safety Plan* (vedi se. 1 e 2) che descriva il modo in cui l'organizzazione intende traguardare il suo obiettivo di sicurezza e rispondere ai requisiti formativi previsti dall'Autorità.

I processi ritenuti fondamentali sono:

- *Safety Oversight*
  Adozione di un programma indipendente di *oversight*, strutturato eventualmente anche all'interno del programma di assicurazione qualità ma focalizzato sulle prestazioni dei processi relativi agli aspetti di sicurezza
- *Formal safety review*
  Introduzione di due funzioni distinte all'interno del SMS: *Safety Review Board*
  (*SRB*) (vedi all.1) e *Safety Action Group* (SAG) (vedi all.2).
  L'*SRB* assicura che il *SMS* funzioni correttamente, in modo che i rischi siano adeguatamente trattati nei tempi stabiliti.
  Il *SAG* è un gruppo che supporta il processo di risk assessment e i task di sicurezza relativi

Il *Safety Review Board* è composto dai più alti livelli manageriali, compreso il *Safety Manager*, è solitamente presieduto dall'*Accountable Manager* o da un suo delegato.
Il *Safety Action Group* è composto da rappresentanti del *line management* e dal personale di supervisione di tutti i settori della compagnia, dal settore delle Operazioni e della Manutenzione a quello Finanziario e Commerciale.
In una grossa compagnia possono essere istituiti diversi *SAG*s. Questi gruppi dovrebbero, attraverso incontri pianificati, supportare la linea per la valutazione dei rischi e indicare i possibili metodi o fattori di mitigazione.

Principi organizzativi e gestionali volti alla assicurazione di sicurezza

I principi di base sono riassunti in:

- responsabilità e processi chiaramente identificati
- procedure di selezione e formazione continua del personale sulle norme di sicurezza nazionali e internazionali (EASA/JAA/ICAO) e sui metodi di *risk management*
- definizione degli standard dei prodotti e dei fornitori esterni
- monitoraggio continuo dell'efficienza degli equipaggiamenti, sistemi e servizi
- *recording* e *monitoring* degli standard di sicurezza della compagnia e delle sue attività critiche tramite l'istituzione di un programma di audit di sicurezza (vedi sez. 4)
- identificazione degli *hazard* e attività di *risk management*
- sistemi di comunicazione efficace per la risoluzione di criticità ai livelli appropriati di management
- istituzione di un *Emergency Responce Planning (ERP)* allo scopo di facilitare la gestione di un evento pericoloso e indesiderato e di mitigare il suo impatto sulle normali operazioni dell'Operatore (vedi All.3)

Adozione di sistemi per la *Safety Oversight*

I sistemi utilizzati per la *Safety Oversight* sul sistema sono:

- analisi continua dei dati relativi alle operazioni, all'engineering e alla manutenzione tramite l'utilizzo di programmi quali *l'Engineering o Operational Flight Data Monitoring* (*OFDM*), come parte integrante del *SMS,* allo scopo di assicurare la rispondenza alle procedure standard operative (*SOPs*). Questi dati possono essere usati per misurare la prestazione del sistema, identificare i rischi e monitorare l'efficacia dell'azione di mitigazione implementata dall'organizzazione

- sistemi già comunemente stabiliti per il *reporting*, come ad ad esempio *Air Safety Reports (ASRs), Flight Reports* e *Maintenance Management Error.* I principi del *flight operation reporting* dovrebbero essere estesi ad altre aree critiche dell'organizzazione
- *safety auditing*: il sistema di gestione della qualità di un operatore da trasporto aereo in accordo con la Parte 145 e alla JAR-OPS richiede già l'istituzione di un piano di audit relativo alla sicurezza volo e alle attività di manutenzione e aeronavigabilità. Nel caso di un *SMS* lo scopo di questo piano potrebbe essere esteso alle attività, processi o sistemi identificati come potenzialmente critici dalla *risk analysis* o dal *SAG*
- investigazione interna sugli incidenti
- analisi delle prestazioni del sistema tramite l'utilizzo dei *safety data* finalizzata alla valutazione dell'adeguatezza del *SMS* istaurato
- sistemi efficaci di *Lesson Learned Communication* da parte del *Safety Manager*, *SRB e SAG* o altri
- revisione periodica dell'efficacia dell'intero *SMS* da parte del *SRB*
- monitoraggio dei *Line Managers:* la pratica comune usata dal personale di volo, della manutenzione e da altri soggetti (es. *handlers*, gestori aeroportuali) è la chiave vincente per il raggiungimento di una cultura positiva della sicurezza. L'organizzazione deve promuovere l'attività di *reporting* a tutti i livelli anche tramite strumenti di incentivazione.

Allegato 1 *Safety Review Board*

Il *Safety Review Board* (*SRB*) è un comitato stabilito ai più alti livelli organizzativi di un Operatore Aereo o di una Organizzazione di Manutenzione e risponde direttamente al Consiglio di Amministrazione.

Presidente:

La figura del Presidente è ricoperta dall'*Accountable Manager.*

Componenti del Comitato:

In un Operatore Aereo i membri del Comitato sono, oltre il Presidente, i responsabili delle *Flight Operations*, *Ground Operations*, *Aircraft Maintenance/Engineering*. Il *Safety Manager* ricopre solitamente la figura di Segretario.

Responsabilità:

- monitorare le prestazioni di sicurezza delle operazioni rispetto al programma di sicurezza stabilito
- monitorare l'efficacia e la tempistica delle azioni correttive necessarie
- monitorare l'efficacia dei processi di gestione della sicurezza che hanno effetto sulla gestione del *business plan*
- monitorare l'efficacia del processo indipendente di *Safety Oversight* che valida le prestazioni di sicurezza dell'organizzazione
- monitorare l'efficacia della *Safety Oversight* dei fornitori esterni
- fornire le indicazioni strategiche ai *Safety Action Groups*

Allegato 2 *Safety Action Group*

In un Operatore i *Safety Action Groups (SAGs)* sono stabiliti all'interno delle *Flight Operations, Ground Operations* e *Aircraft Maintenance/Engineering* (aree funzionali).

Presidente:

La figura del Presidente in ogni SAGSs è ricoperta dal corrispettivo responsabile di area.

Componenti del Comitato:

In un Operatore Aereo i membri del Comitato sono, oltre il Presidente, normalmente identificati tra i responsabili e il personale specialistico delle aree *Operations*, *Ground Operations* e *Aircraft Maintenance/Engineering, Human Factor* e in alcuni casi dell'area Finanziaria/Amministrativa. Il *Safety Manager* normalmente partecipa come osservatore o coordinatore dei vari gruppi di *SAG*.

Responsabilità:

- monitorare la sicurezza operativa in ogni area funzionale
- assicurare che le azioni correttive vengano implementate nei tempi indicati
- riportare e condividere le strategie e le politiche organizzative indicate dal *Safety Review Board*

Compiti:

- assicurare che l'identificazione degli *hazard* e il *risk assessment* siano formalizzati e indirizzati al personale competente del processo o attività interessata
- assicurare che ci sia coerenza tra i dati di sicurezza rilevati e le azioni di riscontro del personale
- assicurare che i valori degli indicatori di prestazione di sicurezza siano sviluppati e regolarmente revisionati da ogni area funzionale
- assicurare che il piano di *audit* mandatori del sistema qualità sia indirizzato a fornire anche un contributo sulla verifica delle prestazioni di sicurezza e che piena cooperazione esista tra l'area Sicurezza e Qualità per rendere efficaci i *safety audits*
- incentivare la responsabilità del personale dell'Operatore, tramite incontri programmati che promuovano la cultura positiva della sicurezza come priorità della Compagnia, utilizzando in particolare il reporting volontario di ogni eventuale falla del sistema anche in termini di prestazioni o errori umani
- assicurare una adeguata investigazione su possibili eventi o criticità afferenti la sicurezza delle operazioni e tracciare le azioni intraprese
- assicurare appropriata formazione al personale per rispondere o superare i requisiti minimi regolamentari sia nazionali che internazionali

Allegato 3 *Emergency Response Planning*

Il piano di emergenza (ERP) è definito al fine di favorire la gestione di uno o più eventi critici e mitigare il loro impatto sulle normali operazioni.
Tutte le basi operative di una compagnia devono sviluppare adeguati *ERP* coordinati con il piano generale.
Il piano deve:

- individuare univocamente le responsabilità del personale indicato
- contenere le procedure di emergenza da attuare nel caso di un evento indesiderato
- controllare e definire la notifica dell'inconveniente all'autorità preposta
- indicare i flussi ed i centri di comunicazione all'interno della compagnia
- indicare le modalità di coordinamento con altri soggetti in sede aeroportuale
- indicare gli strumenti e mezzi di comunicazione con l'utente e i media nel caso di incidenti seri
- indicare gli enti preposti alla gestione delle pratiche assicurative e amministrative
- indicare procedure per isolare immediatamente, laddove identificata, la causa che ha originato l'evento indesiderato

Il programma di formazione del personale dell'Operatore deve essere indirizzato alla gestione e alla conoscenza delle procedure e degli strumenti indicati nell'*Emergency Response Planning*.

Bibliografia

1. **CAA CAP 712** *Safety Management System for Commercial Air Transport Operation*
2. **CAA CAP 728** *The Management of Safety: Guidance to Aerodromes and Air Traffic Services Units on the development of safety Management Systems*
3. FAA *System Safety Handbook*
4. FAA Order 8040.4 *Safety Risk Management*
5. ICAO Doc 9422 *Accident Prevention Manual*
6. FAA *Safety Management System Manual*
7. EASA *Certification Specification* 25 *Large Aeroplanes*
8. Eurocontrol ESARR 4 *Risk Assessment and Mitigation in ATM*
9. Trasport Canada *Introduction to Safety Management System*
10. FAA *Guidelines for Investment Analysis Team Alternative Risk Assessment*
11. FAA *Acquisition Management System*
12. ESARR 3 *Use of SafetyMangement Systems by ATM Service Providers*