

“Il Safety Management System e metodologia ARMS”

P. Carlo Cacciabue

Safety Management System

- I. SMS come **approccio proattivo**
- II. piani strategici di ICAO, CE e EASA
- III. SMS come sistema di gestione della sicurezza composto da:
 - ✓ un insieme coordinato di processi
 - ✓ coinvolge tutti i livelli dell'organizzazione (top management a tutti i livelli)
 - ✓ continuamente alimentato dalle figure chiave della prima linea

Il Safety Management System è la forma più completa ed integrata dell'approccio alla sicurezza messo in atto in un'organizzazione nei confronti della prevenzione, gestione e contenimento di occorrenze negative, eventi di pericolo, non-conformità e incidenti che si possono verificare nella vita e nei processi produttivi di un sistema.

Componenti principali di SMS

- I. la politica di sicurezza e gli obiettivi istituzionali;
- II. l'analisi e la gestione del rischio;**
- III. la valutazione dei pericoli e della sicurezza reale;**
- IV. la promozione della sicurezza in seno all'organizzazione.

- L'analisi dei rischi e la valutazione reale dei pericoli sono le attività costitutive del SMS.
- Le politiche e gli obiettivi definiti dal management e la promozione della sicurezza forniscono il quadro di riferimento, nonché il sostegno e la garanzia che le attività operative di base di sicurezza e di gestione del rischio possano essere condotte in modo efficace ed indipendente

- Un gruppo di lavoro di esperti del dominio industriale aeronautico ed accademico è stato attivato nel 2007 per sviluppare una nuova e migliore metodologia per la valutazione di rischio operativa.
- L'obiettivo primario del gruppo era di sviluppare una metodologia per le compagnie aeree ma di fatto questa è completamente applicabile ad altre organizzazioni aeronautiche.
- La metodologia prodotta definisce un processo generale per la valutazione operativa di rischio.

- Il processo di valutazione comincia con la classificazione di rischio di evento (“**Event Risk Classification**” - **ERC**), che è la revisione degli eventi realmente accaduti e pertanto rappresenta l’analisi retrospettiva dei pericoli incontrati e del relativo rischio potenzialmente corso.
- Il passo seguente è analisi di dati per identificare i problemi di sicurezza correnti e prevedibili. Questi sono dunque valutati dettagliatamente con la metodologia di analisi predittiva denominata “**Safety Issue Risk Assessment**” - **SIRA**.
- Il processo intero si accerta che tutte le azioni necessarie di sicurezza siano identificate, genera un registro per la valutazione continua dei rischi e delle azioni di controllo, attraverso le barriere di sicurezza, e fornisce una funzione di controllo di prestazioni di sicurezza. SIRA e ERC sono strumenti di base per lo sviluppo di un accurato "Safety Management System" (SMS)

ARMS – Modificato ed adattato

- 5 livelli di severità
 - in ARMS sono 4.
- Inclusione delle barriere consequenziali/mitigative di eventi conseguenza e barriere consequenziali di gravità dell'occorrenza
 - in ARMS si considerano solo barriere orientate alla mitigazione degli eventi conseguenza e nessuna barriera consequenziale

Matrice di Rischio - MdR

Severità \ Frequenza	Trascurabile 1	Minore 2	Maggiore 3	Pericoloso 4	Catastrofico 5
Frequente					
Ragionevolmente Probabile					
Remoto					
Estremamente Remoto					
Estremamente Improbabile					

Hazard Identification – possible safety data sources

- **Safety Reporting**
 - Air Safety Reports (ASR)
 - Cabin Safety Reports (CSR)
 - Maintenance Safety Reports
 - Mandatory Occurrence Reports (MOR)
 - Ground Safety Reports
 - Confidential Reports
 - Human Factors Reports
- **Questionnaires / surveys**
- **Recording**
 - Flight Data Monitoring
(= FDM = FDA = FOQA)
- **Safety and quality auditing**
- **Observing the operation**
 - Line Operations Safety Audit (LOSA)
 - Line Operations Assessment System (LOAS)
- **Learning from your own people**
 - Moderated sessions with groups of internal experts
 - Brainstorm new hazards or elaborate on known hazards
- **External information**
 - Conferences & publications
 - Other operators

Typical sources for safety data.

Event Risk Classification (ERC)

- ❑ L'obiettivo principale di ERC è di fungere da prima selezione di tutti i dati ricevuti di sicurezza ed identificare quando un'azione urgente fosse necessaria.

La tecnica ERC si basa su due domande fondamentali:

1. Se questo evento fosse evoluto in un incidente o inconveniente grave, quale sarebbe stato il risultato più credibile?
2. Quale sarebbe potuta essere l'efficacia delle barriere restanti fra questo evento ed il risultato di incidente più credibile?

Event Risk Classification (ERC)

<i>Typical accident occurrences/scenarios</i>	<i>If this event had escalated into an accident outcome, what would have been the most credible outcome?</i>
Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain	<p>ACCIDENT An occurrence in which: a) a person is fatally or seriously injured or b) the aircraft sustains damage or structural failure which would normally require major repair or replacement, or c) the aircraft is missing or is completely inaccessible.</p>
Engine failure, fires, Terrain and obstacle clearance incidents, Flight control and stability problems, Take-off and landing incidents, Flight crew incapacitation, Decompression, ecc.	<p>SERIOUS INCIDENT An incident involving circumstances indicating that an accident nearly occurred. N.B. Examples of serious incidents can be found in Attachment D of ICAO Annex 13 and in the ICAO Accident/Incident Reporting Manual (ICAO Doc 9156)</p>
High speed taxiway collision, major turbulence injuries	<p>MAJOR INCIDENT An incident associated with the operation of an aircraft, which safety of aircraft may have been compromised, having led to a near collision between aircraft with ground or obstacles (i.e. safety margins not respected which is not the result of an ATC instruction)</p>
Pushback accident, minor weather damage	<p>SIGNIFICANT INCIDENT An incident involving circumstances indicating that an accident, a serious or major incident could have occurred, if the risk had not been managed within safety margins, or if another aircraft had been in the vicinity.</p>
Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)	<p>OCCURRENCE WITH NO SAFETY EFFECT An incident which has no safety significance. N.B. This appears to be a contradiction with the ICAO definition of an incident: An occurrence, other than an accident, associated with the operation of an aircraft which affects or could</p>

Event Risk Classification (ERC)

Domanda 1: Se questo evento fosse evoluto in un incidente o inconveniente grave, quale sarebbe stato il risultato più credibile?

- Si provi ad estendere l'evento in un risultato di incidente. Se fosse virtualmente impossibile che l'evento si possa intensificare in un incidente, allora ci si posiziona nella riga più bassa, a valore 1 di ERC.
- Se si può immaginare uno scenario credibile di occorrenza/incidente (anche se improbabile!), allora il piano d'azione più credibile deve essere considerato e si giudichi la relativa conseguenza tipica, selezionando la riga corrispondente nella tabella. Gli scenari tipici di incidente elencati a destra della tabella possono essere di aiuto.

Event Risk Classification (ERC)

Domanda 2: Quale sarebbe potuta essere l'efficacia delle barriere restanti fra questo evento ed il risultato di incidente più credibile?

Per accedere “al margine di sicurezza” restante, si consideri sia il numero che la robustezza delle barriere restanti fra questo evento ed il piano d'azione di incidente in domanda 1, ivi comprese le barriere consequenziali.

Barriere già venute a mancare sono ignorate. Soltanto le barriere che hanno funzionato e tutte le barriere successive ancora in grado di intervenire e controllare l'evoluzione dell'occorrenza o mitigare le conseguenze sono considerate.

Event Risk Classification (ERC)

What was the effectiveness of the "causal and consequential barriers" between this event and the most credible accident scenario?

Effective	Partly effective	Limited	Minimal	Non effective	Efficacia
					Severità
					Catastrofico
					Pericoloso
					Maggiore
					Minore
					Trascurabile

	Analizzare immediatamente ed agire di conseguenza
	Studiare o effettuare ulteriore valutazione di rischio
	Usare per il miglioramento continuo dell'informazione

Event Risk Classification (ERC)

Per la scelta della colonna della matrice:

- ✓ Sia scelta la colonna di destra estrema, se l'unica cosa che separa l'evento da un incidente è fortuna pura o abilità eccezionale.
- ✓ La 2^a colonna è scelta se alcune barriere esistono ma la loro efficacia è considerata “minima”. Ad esempio un annuncio di GPWS poco prima di collisione con il terreno (CFIT).
- ✓ La 3^a colonna è selezionata se l'efficacia delle barriere fosse “limitata”. Tipicamente, questa è una situazione anormale, più difficile da controllare, ma con ancora un margine di sicurezza restante considerevole - per esempio. un errore moderato nel loadsheet o caricamento contro piccoli problemi di rotazione al decollo.
- ✓ La 4^a e 5^a colonna di sinistra si applicano se il margine di sicurezza fosse parzialmente o completamente “efficace”, tipicamente consistendo di parecchie buone barriere - per esempio. passeggero che fuma nella toilette contro l'incidente di incendio in volo.

Event Risk Classification (ERC)

Typical accident scenarios	If this event had escalated into an accident outcome, what would have been the most credible outcome?	What was the effectiveness of the "consequential barriers" between this event and the most credible accident scenario?					Frequenza Severità
		Effective	Partly effective	Limited	Minimal	Non effective	
Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain	ACCIDENT An occurrence in which: a) a person is fatally or seriously injured or b) the aircraft sustains damage or structural failure which would normally require major repair or replacement, or c) the aircraft is missing or is completely inaccessible.	Yellow	Yellow	Red	Red	Red	Catastrofico
Engine failure, fires, Terrain and obstacle clearance incidents, Flight control and stability problems, Take-off and landing incidents, Flight crew incapacitation, Decompression, ecc.	SERIOUS INCIDENT An incident involving circumstances indicating that an accident nearly occurred. N.B. Examples of serious incidents can be found in Attachment D of ICAO Annex 13 and in the ICAO Accident/Incident Reporting Manual (ICAO Doc 9156)	Green	Yellow	Yellow	Red	Red	Pericoloso
High speed taxiway collision, major turbulence injuries	MAJOR INCIDENT An incident associated with the operation of an aircraft, which safety of aircraft may have been compromised, having led to a near collision between aircraft with ground or obstacles (i.e. safety margins not respected which is not the result of an ATC instruction)	Green	Green	Green	Yellow	Yellow	Maggiore
Pushback accident, minor weather damage	SIGNIFICANT INCIDENT An incident involving circumstances indicating that an accident, a serious or major incident could have occurred, if the risk had not been managed within safety margins, or if another aircraft had been in the vicinity.	Green	Green	Green	Green	Yellow	Minore
Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)	OCCURRENCE WITH NO SAFETY EFFECT An incident which has no safety significance. N.B. This appears to be a contradiction with the ICAO definition of an incident: An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation.	Green	Green	Green	Green	Green	Trascurabile

	Analizzare immediatamente ed agire di conseguenza
	Studiare o effettuare ulteriore valutazione di rischio
	Usare per il miglioramento continuo dell'informazione

Event Risk Classification (ERC)

		What was the effectiveness of the "consequential barriers" between this event and the most credible accident scenario?					
Typical accident scenarios	If this event had escalated into an accident outcome, what would have been the most credible outcome?	Effective	Partly effective	Limited	Minimal	Non effective	Frequenza Severità
Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain	ACCIDENT An occurrence in which: a) a person is fatally or seriously injured or b) the aircraft sustains damage or structural failure which would normally require major repair or replacement, or c) the aircraft is missing or is completely inaccessible.	Yellow	Yellow	Red	Red	Red	Catastrofico
Engine failure, fires, Terrain and obstacle clearance incidents, Flight control and stability problems, Take-off and landing incidents, Flight crew incapacitation, Decompression, ecc.	SERIOUS INCIDENT An incident involving circumstances indicating that an accident nearly occurred. N.B. Examples of serious incidents can be found in Attachment D of ICAO Annex 13 and in the ICAO Accident/Incident Reporting Manual (ICAO Doc 9156)	Green	Yellow	Yellow with +	Red	Red	Pericoloso
High speed taxiway collision, major turbulence injuries	MAJOR INCIDENT An incident associated with the operation of an aircraft, which safety of aircraft may have been compromised, having led to a near collision between aircraft with ground or obstacles (i.e. safety margins not respected which is not the result of an ATC instruction)	Green	Green	Green	Yellow	Yellow	Maggiore
Pushback accident, minor weather damage	SIGNIFICANT INCIDENT An incident involving circumstances indicating that an accident, a serious or major incident could have occurred, if the risk had not been managed within safety margins, or if another aircraft had been in the vicinity.	Green	Green	Green	Green	Yellow	Minore
Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)	OCCURRENCE WITH NO SAFETY EFFECT An incident which has no safety significance. N.B. This appears to be a contradiction with the ICAO definition of an incident: An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation.	Green	Green	Green	Green	Green	Trascurabile

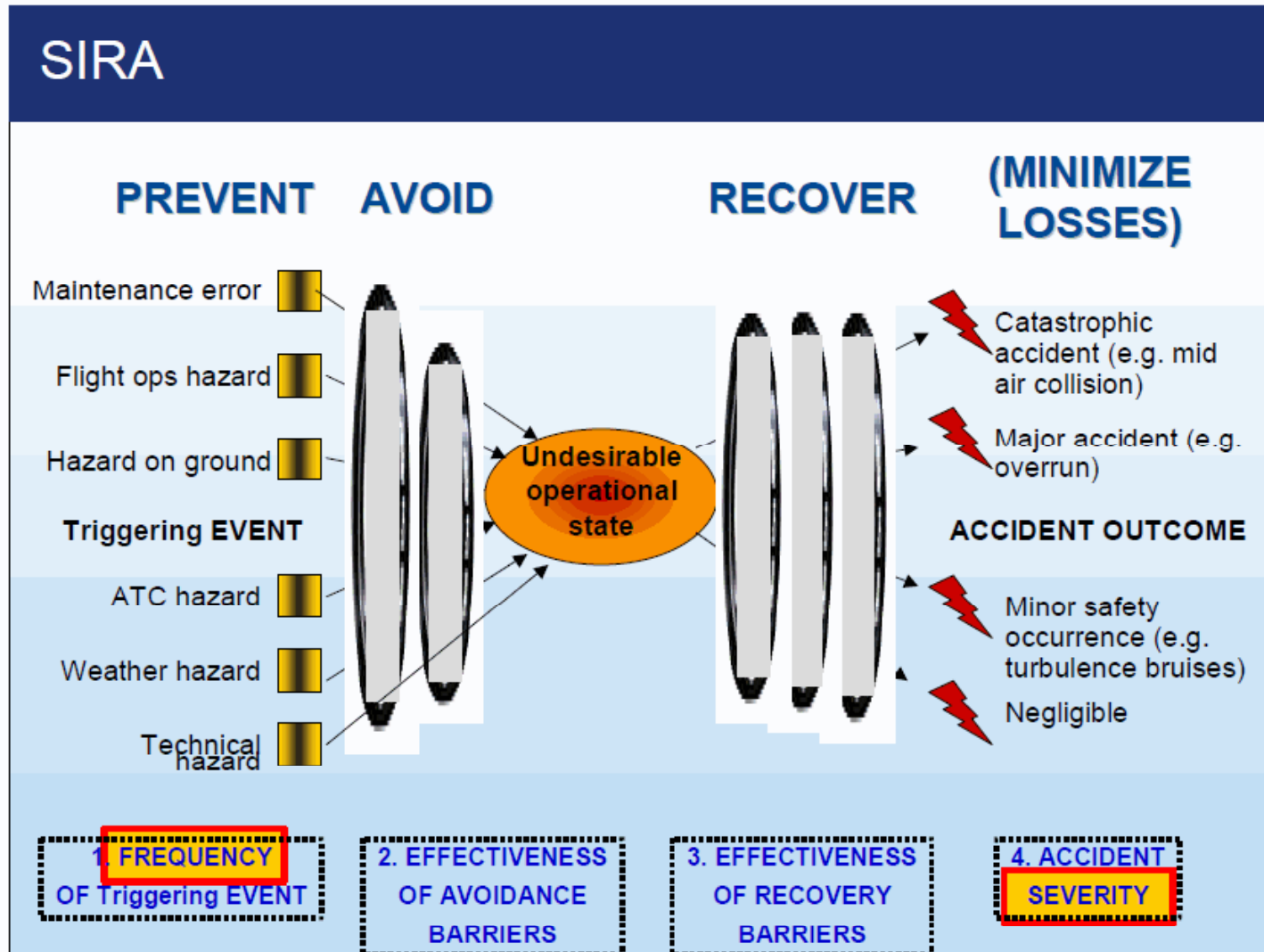
	Analizzare immediatamente ed agire di conseguenza
	Studiare o effettuare ulteriore valutazione di rischio
	Usare per il miglioramento continuo dell'informazione

Safety Issue Risk Assessment (SIRA)

Il processo SIRA modificato applica una formula dove il rischio si basa su 5 fattori.

- 1. Frequenza/probabilità di evento iniziatore/innescante*
- 2. Efficacia delle barriere causali per il la prevenzione dell'evento iniziatore*
- 3. Efficacia delle barriere causali per la prevenzione di eventi conseguenza dell'evento iniziatore ed il recupero della situazione*
- 4. Efficacia delle barriere consequenziali per il contenimento delle conseguenza dell'incidente*
- 5. Severità dell'occorrenza/incidente più probabile*

Safety Issue Risk Assessment (SIRA)



Safety Issue Risk Assessment (SIRA)

Il processo SIRA modificato segue il seguente percorso

1. Una volta che il problema di sicurezza è stato definito, l'analista deve generare gli scenari applicabili in caso di incidente.
2. L'evento innescante può avere varie origini (alcuni esempi sono forniti nella la figura).
3. Il primo passo è una valutazione dell'esposizione a questo evento con la generazione di uno stato operativo indesiderabile ("Undesirable Operational State" - UOS) è definito come: "La fase in uno scenario di incidente raggiunta dall'evoluzione degli eventi tale da rendere l'incidente evitabile soltanto con le misure di recupero di successo".

Safety Issue Risk Assessment (SIRA)

4. I fattori 2, 3 e 4 della formula di SIRA sono valutazioni circa l'efficacia delle barriere di prevenzione, recupero e contenimento.
5. Per concludere, il 5° fattore è la severità del risultato dell'occorrenza, in conformità con la scala di ERC.

Livelli inaccettabili del rischio:

- *Stop*
- *Improve*

Livelli tollerabili del rischio:

- *Secure*
- *Monitor*
- *Accept*

Safety Issue Risk Assessment (SIRA)

- *Stop*: La parte interessata delle operazioni (per esempio, la destinazione, il tipo di velivolo, la procedura) deve essere interrotta immediatamente fino ad effettuare una misura accettabile di riduzione di rischio.
- *Improve*: La questione deve essere attivare il gruppo di azione di sicurezza (“Safety Action Group” - SAG) e viene monitorata dal management. Le misure di riduzione di rischio devono essere identificate ed iniziate all'interno di una struttura in un arco di tempo definito.
- *Secure*: Il livello di rischio e la relativa tendenza deve essere controllato continuamente (almeno al livello di gruppo di azione di sicurezza) per impedire l'escalation al livello inaccettabile.
- *Monitor*: Il problema è seguito regolarmente con la prassi di analisi della base di dati ed il controllo dei valori di SIRA per tutti i problemi di sicurezza nel registro di rischio.
- *Accept*: Nessuna azione specifica è richiesta poiché il rischio è in conformità al livello accettabile.

Safety Issue Risk Assessment (SIRA)

1	Safety Issue title:			
2	Define/scope the SI:			
	Description of Hazard(s)			
	Description of Scenario			
	A/C types			
	Locations			
	Time period under study			
	Other			
3	Analysis of potential Accident Scenario			
	3.1 Triggering event	3.2 Undesirable Operational State	3.3 Accident Outcome	3.4 Consequences Limitation

3.1 Triggering event		3.2 Undesirable Operational State	3.3 Accident Outcome	3.4 Consequences Limitation
Describe the barriers				
	4.1 To avoid the UOS		4.2 To recover situation before the Accident	4.2 To contain Accident consequences
Risk Assessment				
The estimated frequency of the triggering event (per flight sectors) is:	The barriers will fail in AVOIDING the UOS...		The barriers will fail in RECOVERING the situation before the ACCIDENT...	The barriers will fail in CONTAINING the consequences of the ACCIDENT
About every 100 sectors	Once in 100 times		Once in 100 times	Practically always
1.E-02	1.E-02		1.E-02	1.E+00
		UOS frequency:		Mean Accident frequency:
		1.E-04		1.E-06
Result				
6.1 Resulting risk class	Monitor	Monitor		

The accident severity would be...	Tolerability limit	Short definition
Catastrofico	1.E-09	3 fatalities or more
Pericoloso	1.E-07	Serious injuries
Maggiore	1.E-05	Major injuries
Minore	1.E-03	Minor injuries
Trascurabile	1.E+00	Negligible

Difference with tolerability limit	Consequence
1.E-02	Accept
1.E-01	Monitor
1.E+00	Secure
1.E+01	Improve
1.E+02	Stop

Grazie per la Vostra attenzione