SPECIFICA DEI REQUISITI DI SISTEMA CMT

Volume	**Allegato 1**
VOLUME 1	Requisiti di Safety

Rev.	Data	Descrizione	Redazione	Verifica Tecnica	Autorizzazione
A	30/09/2016	Estratto da vol. 1	S. Buonincontri L. Esposito F. Lambardi di San Miniato G. Ridolfi	S. Rosini	F. Senesi

INDICE

1 S, SAFETY

1.1 Descrizione generale del processo di analisi di sicurezza

1.1.1 Limiti di applicabilità dell'analisi

Essendo il sistema SCMT un sistema ATP (Automatic Train Protection), gli elementi principali che lo compongono sono i seguenti:

- Elemento umano operativo e di manutenzione di bordo e di terra
- Sottosistema di terra
- Sottosistema di bordo

Per quanto sopra la presente analisi dovrà essere perimetrata fino a considerare:

- tutte le funzionalità specifiche del sistema SCMT
- tutte le funzionalità di interfaccia del sistema SCMT con il mondo di bordo (interfaccia veicolo) e quello di terra (interfacce apparati di stazione, IS, etc)
- tutte le funzionalità dell'SCMT aventi interfaccia l'elemento umano, operatore e manutentore, di bordo e di terra.

Quanto sopra dovrà consentire di valutare tutti i riflessi per la sicurezza (hazard) che comporta l'implementazione del sistema SCMT.
Non saranno presi in considerazione tutti quegli eventi correlati al mondo di bordo e di terra al di fuori della citata perimetrazione poiché considerati già regolamentati dalle normative vigenti.

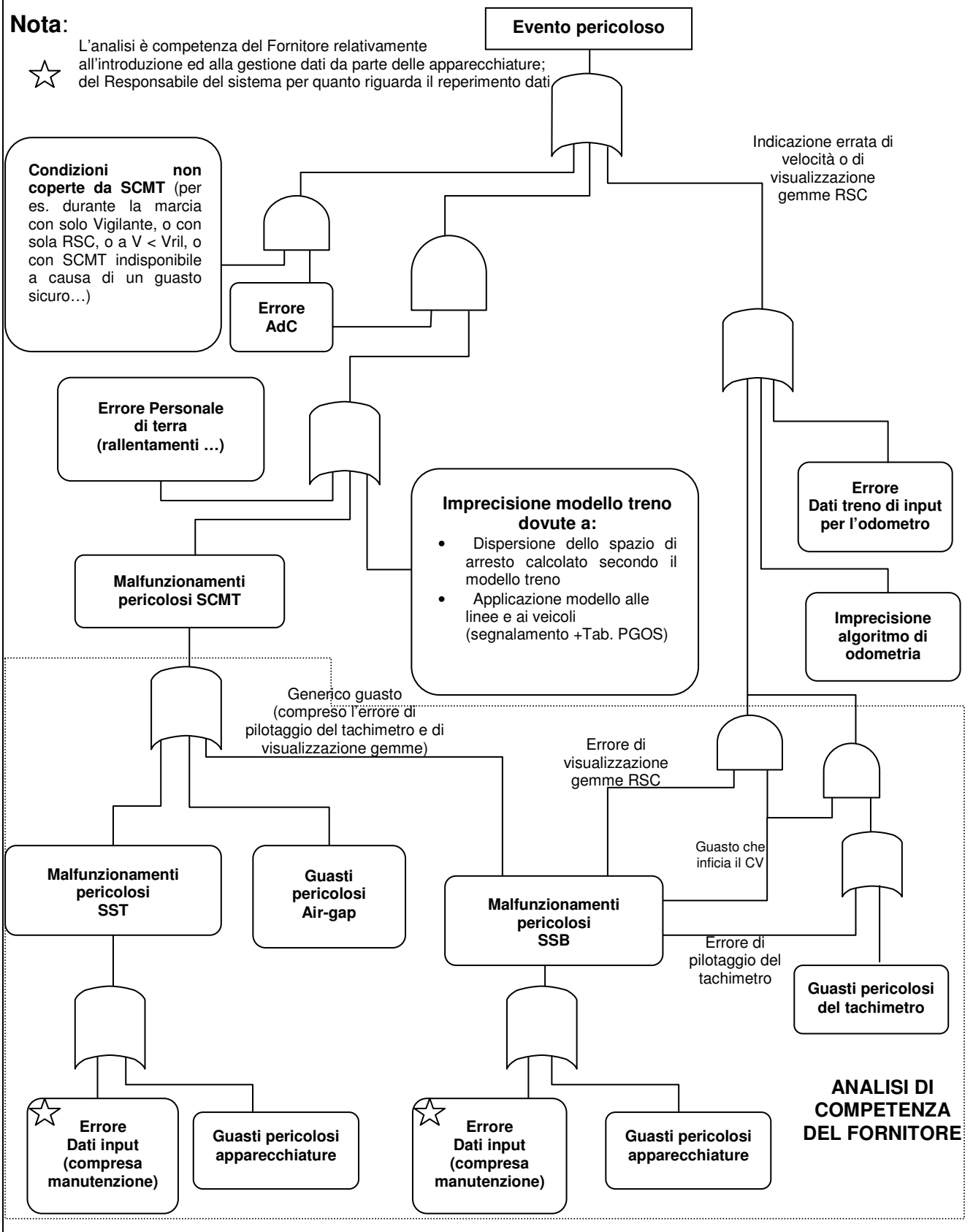
Di seguito si riporta l'albero dei guasti e degli errori che causano il verificarsi di un generico hazard o evento pericoloso limitatamente alle condizioni di esercizio.

Il diagramma considera gerarchicamente i contributi dei guasti delle apparecchiature, l'errore del personale di bordo, l'errore del personale di terra (per es. nella gestione dei rallentamenti e delle riduzioni di velocità) e l'imprecisione degli algoritmi di odometria e del modello di frenatura, tracciando i limiti di responsabilità di analisi da parte dei fornitori.

Si sottolinea come i requisiti quantitativi e qualitativi di sicurezza rivolti al Fornitore non includano l'influenza dell'accuratezza del modello treno (odometria e frenatura) ma solamente le caratteristiche di corretta implementazione di tale modello nel sottosistema di bordo.

Inoltre dal diagramma si possono evincere le due aree di Errore dei Dati di Input, le cui analisi sono di pertinenza del Fornitore e del Responsabile del sistema per le loro parti di competenza.
Quest'ultimo analizza le condizioni a monte dei Dati di Input che possono indurre errori sistematici al sistema SCMT, mentre il Fornitore ha il compito di analizzare gli aspetti di

degrado correlati all'implementazione nel sistema SCMT di tali Dati di Input.


Nota:
L'analisi è competenza del Fornitore relativamente all'introduzione ed alla gestione dati da parte delle apparecchiature; del Responsabile del sistema per quanto riguarda il reperimento dati
Evento pericoloso
Condizioni non coperte da SCMT (per es. durante la marcia con solo Vigilante, o con sola RSC, o a V < Vril, o con SCMT indisponibile a causa di un guasto sicuro…)
Errore AdC
Indicazione errata di velocità o di visualizzazione gemme RSC
Errore Personale di terra (rallentamenti …)
Imprecisione modello treno dovute a:
• Dispersione dello spazio di arresto calcolato secondo il modello treno
• Applicazione modello alle linee e ai veicoli (segnalamento +Tab. PGOS)
Errore Dati treno di input per l'odometro
Malfunzionamenti pericolosi SCMT
Imprecisione algoritmo di odometria
Generico guasto (compreso l'errore di pilotaggio del tachimetro e di visualizzazione gemme)
Errore di visualizzazione gemme RSC
Guasto che inficia il CV
Malfunzionamenti pericolosi SST
Guasti pericolosi Air-gap
Malfunzionamenti pericolosi SSB
Errore di pilotaggio del tachimetro
Guasti pericolosi del tachimetro
Errore Dati input (compresa manutenzione)
Guasti pericolosi apparecchiature
Errore Dati input (compresa manutenzione)
Guasti pericolosi apparecchiature
ANALISI DI COMPETENZA DEL FORNITORE

1.1.2 Definizione del sistema

I confini fisici del sistema e l'ambiente nel quale il sistema deve funzionare sono descritti nel volume 1 delle SRS.
A tale scopo sono stati individuati i seguenti elementi, considerati "interni" al sistema, ed oggetto dell'analisi di sicurezza:

1. le funzioni principali del sistema (appendice B al Vol.1 delle SRS SCMT) la cui tracciabilità rispetto ai requisiti elencati nelle SRF SCMT è riportata all'interno della stessa appendice B;
2. le caratteristiche di base cioè le modellizzazioni atte a garantire le funzionalità in sicurezza del sistema (modello di frenatura del treno, algoritmo di odometria, tabelle B PGOS, ecc.);
3. le interfacce SST-SSB (air-gap/RSC e air-gap/antenna-boa);
4. le interfacce SST-terra (SST-ACEI, SST-ACS,…);
5. le interfacce SSB-treno (SSB-DIS,…);
6. l'interfaccia SST-uomo (manutentore, gestione rallentamenti, …);
7. l'interfaccia SSB-uomo (AdC, manutentore, …)

1.1.3 Prescrizione del SIL di Sistema

Per garantire la salvaguardia dei viaggiatori e dell'ambiente da incidentalità ferroviarie del tipo di quelle definite dalla fiche UIC-A/91, è stato scelto per il sistema SCMT il massimo livello di integrità della sicurezza, corrispondente al livello SIL (Safety Integrity Level) 4 della norma europea EN 50129. Ogni sottosistema si intende che comunque dovrà garantire il detto livello di SIL 4 prescelto per il sistema SCMT.

1.1.4 Perimetrazione del sistema SCMT che i Fornitori devono considerare per il computo della FP (Frequenza di Pericolo o HR-Hazard Rate)

Affinché la stima dei valori di FP dei sottosistemi, calcolati dai Fornitori, sia confrontabile con il valore richiesto (per rispettare il SIL 4) si deve considerare un SSB e le apparecchiature del SST che questo incontra in un ora di funzionamento alla velocità media di 50 km/h.

Per calcolare il numero di boe ed encoder incontrate in un'ora, si prendono a riferimento le tipologie tipiche di attrezzaggio per due linee di 150 km a doppio binario, una banalizzata e con Bacc e l'altra non banalizzata e senza Bacc. Per i dettagli sulle caratteristiche delle linee di riferimento e sulle tipologie A, B, C, D, E, F, G, H ed I di schema dei Complessi Informativi (CI), si veda di seguito.

Le seguenti tipologie di CI sono denominate in base al tipo e numero di boe:

• **Schema A:** un punto informativo (PI) costituito da una boa fissa ed una commutata pilotata da un encoder

• **Schema B:** due PI costituiti da una boa fissa ed una commutata ed entrambe le boe commutate sono pilotate dallo stesso encoder

• **Schema C:** tre PI costituiti da una boa fissa ed una commutata e tutte le tre boe commutate sono pilotate dallo stesso encoder

• **Schema D:** quattro PI costituiti da una boa fissa ed una commutata e tutte le quattro boe commutate sono pilotate dallo stesso encoder

• **Schema E:** un PI costituito da due boe commutate pilotate dallo stesso encoder

• **Schema F:** due PI costituiti da due boe commutate e tutte le quattro boe sono pilotate dallo stesso encoder

• **Schema G:** un PI costituito da due boe commutate pilotate da due encoder differenti

• **Schema H:** due PI costituiti da due boe commutate pilotate da due encoder differenti ed in configurazione a canali incrociati (ciascun encoder pilota due boe appartenenti a punti informativi diversi)

• **Schema I:** un PI costituito da due boe fisse

Se si indica:

- numero CI di tipo A = a
- numero CI di tipo B = b
- numero CI di tipo C = c
- numero CI di tipo D = d
- numero CI di tipo E = e
- numero CI di tipo F = f
- numero CI di tipo G = g
- numero CI di tipo H = h
- numero CI di tipo I = i.

Si considera la seguente distribuzione lungo linea:

- Per la linea di 150 km a d.b. banalizzato **con BAcc** 3/3
  a = 0
  b = 0
  c = 0

d = 0
e = 150 pari a 300 boe commutate e 150 encoder
f = 0
g = 9 pari a 18 boe commutate e 18 encoder
h = 33 pari a 132 boe commutate e 66 encoder
i = 423 pari a 846 boe fisse

- Per la linea di 150 km a d.b. non banalizzato **senza BAcc**
  a = 10 pari a 10 boe fisse; 10 boe commutate e 10 encoder
  b = 12 pari a 24 boe fisse; 24 boe commutate e 12 encoder
  c = 2 pari a 6 boe fisse; 6 boe commutate e 2 encoder
  d = 2 pari a 8 boe fisse; 8 boe commutate e 2 encoder
  e = 0
  f = 25 pari a 100 boe commutate e 25 encoder
  g = 0
  h = 25 pari a 100 boe commutate e 50 encoder
  i = 150 pari a 300 boe fisse

Nell'ipotesi che siano attrezzati 10500 km di linea di cui 4000 con Bacc, si definisce il seguente numero di componenti del SST:

linea attrezzata CON BAcc
- boe commutate = 450 x 4000/300 = 6000;
- boe fisse = 846 x 4000/300 = 11280;
- encoder = 234 x 4000/300 = 3120.

linea attrezzata SENZA BAcc
- boe commutate = 248 x 6500/300 = 5373;
- boe fisse = 348 x 6500/300 = 7540;
- encoder = 101 x 6500/300 = 2188.

Il numero complessivo medio di componenti del SST sulla rete di 10500 km, risulta quindi:
- 11373 boe commutate;
- 18820 boe fisse;
- 5308 encoder.

Per cui, mediamente, un locomotore che viaggia a 50 km/h incontra in un'ora circa:
- 54 boe commutate;
- 90 boe fisse;
- 25 encoder.

Relativamente alla trasmissione terra-treno il numero di air-gap che dovranno essere considerati è pari al numero totale di boe incontrate in un'ora, cioè: 144.

1.2 Descrizione del processo a carico dei Fornitori

1.2.1 Responsabilità e competenze del Fornitore

È responsabilità del Fornitore lo sviluppo della Hazard Analysis per ogni sottosistema del sistema SCMT, in accordo a quanto stabilito nelle EN 50126, EN 50128 e EN 50129.
In base alle responsabilità citate ed al flusso delle attività indicate nel seguente paragrafo, il Fornitore dovrà provvedere a fornire tutte le evidenze oggettive richieste ed il necessario supporto, al fine di conseguire l'obiettivo di Messa in Servizio di ognuno dei sottosistemi del sistema SCMT in base alle citate norme europee.

1.2.2 Descrizione del flusso delle attività

I Fornitori dovranno consegnare una tabella che identifichi per ogni macro-funzione di sistema le relative funzioni dei sottosistemi e quelle di interfaccia con gli altri sottosistemi/impianti esterni ad SCMT.
Da tali funzioni così tracciate, dovranno essere sviluppate le analisi delle cause, in modo da evidenziare le correlazioni tra gli hazard individuati a livello di Safety Case di sistema e le rispettive funzioni dei sottosistemi, registrando nell'Hazard Log le relative proposte di controllo/mitigazione di ogni specifico hazard.

Tra le cause, i Fornitori dovranno considerare le condizioni esterne al sistema SCMT (ad es. avarie del veicolo, elemento umano - escluso l'AdC poiché parte integrante del sistema SCMT, avarie all'infrastruttura ecc.), che possono avere riflesso sul corretto funzionamento dei rispettivi sottosistemi, al fine di completare l'insieme delle analisi di correlazione tra il sistema SCMT e l'ambiente nel quale esso deve essere implementato.
In base agli esiti di tale analisi verranno individuate le azioni compensative di controllo/mitigazione delle cause, che dovranno essere preordinate secondo il loro livello di concomitanza.
Tale processo dovrà fornire evidenza oggettiva del rispetto dei requisiti di integrità della sicurezza prefissati nella Risk Analysis.

Le attività di Hazard Analysis di pertinenza del Fornitore sono descritte di seguito.

1.2.3 Analisi delle cause

Dovrà essere eseguita per ognuna delle apparecchiature che compongono ciascun sottosistema:

A. Software and integration engineering hazard analysis;
B. Hardware engineering hazard analysis;
C. Interface hazard analysis;
D. Operating & Support hazard analysis;
E. Manufacturing hazard analysis.

A. Software and integration engineering hazard analysis

L'analisi dovrà essere indirizzata verso la struttura del SW in modo da identificare eventuali errori che siano cause di hazard aventi riflesso per il livello di integrità della sicurezza prefissato per il sottosistema.
In particolare dovranno essere analizzate le cause relative alle avarie imputabili al SW (operativo, di base, applicativo, diagnostico, etc.) del SST e del SSB che determinano gli hazard di sottosistema individuati nella Risk Analysis svolta a livello di Safety Case di sistema.
Tali hazard dovranno essere riportati negli appositi hazard log di sottosistema.

I dati di uscita da questa analisi dovranno consentire di:
- Verificare e validare la struttura e l'operatività del SW;
- Verificare e validare l'integrazione del SW con l'HW selezionato;
- Verificare e validare i test di integrazione ed accettazione del SW e dell'HW fino al livello di sottosistema.

B. Hardware engineering hazard analysis

L'analisi dovrà essere indirizzata verso la struttura dell'HW in modo da identificare eventuali errori/guasti che siano cause di hazard aventi riflesso per il livello di integrità della sicurezza prefissato per il sottosistema.
In particolare dovranno essere analizzate le cause relative alle avarie imputabili all'HW delle apparecchiature del SST e SSB, che determinano gli hazard di sottosistema individuati nella Risk Analysis svolta a livello di Safety Case di sistema.
Tali hazard dovranno essere riportati negli appositi hazard log di sottosistema.

I dati di uscita di questa analisi dovranno consentire di:
- Verificare e validare i componenti, gli stress e la struttura HW;
- Verificare e validare le condizioni operative ed ambientali dell'HW;
- Verificare e validare i test di accettazione dei componenti dell'HW.

C. Interface hazard analysis

L'analisi dovrà essere indirizzata verso le interfacce interne ed esterne alle apparecchiature dei sottosistemi, in modo da identificare eventuali errori di progettazione che possano causare riflessi per il livello di integrità della sicurezza prefissato per il sottosistema.

In particolare dovranno essere analizzate le interfacce interne ed esterne delle apparecchiature di ogni sottosistema per verificare se le relative avarie possono influenzare gli hazard di sottosistema individuati nella Risk Analysis svolta a livello di Safety Case di sistema.

Tali hazard dovranno essere riportati negli appositi hazard log di sottosistema.

I dati di uscita di questa analisi dovranno consentire di:

- Verificare e validare la funzionalità e la consistenza delle interfacce esterne ed interne;
- Verificare e validare l'integrazione del SW con l'HW delle interfacce ove applicabile;
- Verificare e validare gli eventuali test di integrazione ed accettazione delle dette interfacce.

D. Operating & Support Hazard Analysis

L'analisi dovrà essere indirizzata verso gli ambienti: operativo (procedure e normative di impiego), installazione, montaggio (cablatura, connessioni, tarature…) e manutenzione (procedure e normative di manutenzione) delle apparecchiature dei sottosistemi, in modo da identificare eventuali errori di progettazione che possano causare avarie aventi riflessi per il livello di integrità della sicurezza prefissato per il sottosistema e per la sicurezza del lavoro (aree ad alta tensione etc.).

In particolare dovrà essere analizzato se il mancato rispetto delle procedure/normative di impiego e manutenzione può comportare cause che determinano gli hazard di sottosistema individuati nella Risk Analysis svolta a livello di Safety Case di sistema.

Tali hazard dovranno essere riportati negli appositi hazard log di sottosistema.

I dati di uscita di questa analisi dovranno consentire di:

- Verificare e validare le procedure/normative d'impiego e manutenzione del Fornitore;
- Verificare e validare le procedure/normative per garantire la sicurezza del lavoro (precauzioni, verifiche di messa a terra etc.);
- Verificare e validare le tipologie di test d'accettazione della diagnostica delle apparecchiature.

E. Manufacturing hazard analysis

L'analisi dovrà essere indirizzata alla fase di produzione relativa al ciclo di vita delle apparecchiature dei sottosistemi, in modo da identificare eventuali punti critici sul processo, sugli strumenti di riscontro, sui mezzi utilizzati e sulle misurazioni effettuate, ai fini di garantire l'integrità del processo produttivo prescritto in aderenza al SIL richiesto.

In particolare dovrà essere analizzato se il mancato rispetto delle procedure/normative di approvvigionamento e produzione può comportare cause che determinano gli hazard di

sottosistema individuati nella Risk Analysis svolta a livello di Safety Case di sistema.
Tali hazard dovranno essere riportati negli appositi hazard log di sottosistema.

I dati di uscita di questa analisi dovranno consentire di:

- Verificare e validare le procedure/normative d'approvvigionamento e produzione del Fornitore;
- Verificare e validare le procedure di gestione della configurazione;
- Verificare e validare le tipologie di test di collaudo per l'accettazione in fabbrica delle apparecchiature.

1.2.4 Analisi delle cause concomitanti

L'analisi delle cause concomitanti svolta dai Fornitori dovrà essere condotta in modo analogo a quella sviluppata a livello di Safety Case di sistema, al fine di rintracciare le cause concomitanti che comportano come conseguenze gli hazard individuati dalla Risk Analysis di cui al Safety Case di sistema.
Tale processo dovrà considerare più modi di guasto alla volta per ogni tipologia di hazard, in modo da fornire una valutazione delle cause concomitanti di tipo latente che possono generare hazard da riportare sull'Hazard log.

1.2.5 Mitigazione degli hazard e reporting

A valle degli hazard log di sistema e delle analisi delle cause di cui ai § 1.2.3 e 1.2.4, dovranno essere individuati dal Fornitore i provvedimenti compensativi e le relative informazioni, atti a controllare/mitigare/eliminare le cause e/o le conseguenze degli hazard di sottosistema.
Tali provvedimenti dovranno essere riportati nei rispettivi hazard log di sottosistema.

1.2.6 Calcolo dell'Hazard Rate (HR) ed allocazione del SIL di sottosistema

Il calcolo dell'HR e l'allocazione del SIL del sottosistema alle relative apparecchiature devono essere effettuati tramite tecniche e metodologie specifiche previste dall'Hazard Analysis tenendo conto:

- della perimetrazione del sistema SCMT come indicato al § 1.1.4;
- dei THR (Tolerable Hazard Rate) e dei SIL (si veda il § 1.1.3) per ora di funzionamento e

per funzione previsti dalla EN 50129.

Partendo da quanto sopra per il sottosistema, dovranno essere derivati gli HR ed i SIL per le apparecchiature, mediante opportuni criteri conservativi di valutazione qualitativa e quantitativa d'integrità della sicurezza, in modo che gli HR derivati per i sottosistemi siano coerenti con i THR richiesti dal sistema SCMT.

L'implementazione dei SIL dei sottosistemi dovrà essere correlata dal punto di vista quantitativo agli HR calcolati come suddetto, mentre dal punto di vista qualitativo dovranno essere individuati i punti critici, gli strumenti di riscontro, i mezzi utilizzati e le misurazioni effettuate per ogni fase del ciclo di vita del sottosistema, ai fini di garantire l'integrità del processo produttivo, dell'installazione, dell'assistenza tecnica e d'impiego prescritto in aderenza al SIL richiesto.

1.2.7 Attività collaterali

Sarà compito del Fornitore ottemperare alle attività legate all'analisi RAM e all'analisi della qualità dei sottosistemi in modo da rispettare i requisiti enunciati nel presente capitolo.
A tale scopo l'obiettivo del Fornitore sarà quello di sviluppare le Hazard Analysis dei sottosistemi in conformità con i dati e le informazioni derivate dalle attività di seguito riportate:

- la Risk Analysis e le Analisi RAM elaborate per il sistema SCMT;
- le analisi RAM e l'analisi di qualità del sottosistema elaborate dal Fornitore nelle peggiori condizioni operative ed ambientali prescritte. Le analisi RAM dovranno comunque evidenziare per ogni LRU che compongono le apparecchiature, le funzioni di ingresso/uscita (cioè le funzioni che determinano gli input/output per le LRU stesse), le avarie considerate per quelle funzioni, le conseguenze di quelle avarie sulle LRU e gli eventuali provvedimenti intrapresi (diagnostica, ecc.).

1.2.8 Evidenze documentali

Il Fornitore è responsabile della raccolta della documentazione di sicurezza del sottosistema di competenza, ai fini di produrre il rispettivo Dossier di Sicurezza (Safety Case) necessario per le attività di V&V e di Messa in Servizio, in conformità con quanto previsto, in modo indicativo ma non esaustivo, dalle norme EN 50126, EN 50128, EN 50129 e dalla vigente legislazione.
Il Dossier di Sicurezza dovrà fornire evidenza oggettiva del flusso delle attività e dei risultati delle analisi del processo di Hazard Analysis sopra descritto.