SEAR – Seminari FuSa – Ing. Bastoni

Esempi di esercizi d'esame (preappello)

Esercizio 1

Un sistema elettronico di sicurezza monitora la pressione e la temperatura di un gas contenuto in un tank. Se sia la pressione che la temperatura superano le relative soglie, una valvola di sfogo viene aperta. La valvola viene richiusa appena una delle due grandezze misurate torna sotto la soglia. La funzione di sicurezza (safety function) e' infatti "impedire che sia la temperatura che la pressione del gas nel tank superino le soglie prederminate attraverso l'apertura della valvola".

Effettuare un assessment dei requirements implementativi riportati nella tabella, indicando se (e quali) caratteristiche di base per la buona scrittura di un requirement sono violate, indicando anche il perché'.

Caratteristiche di base:

Atomicity (Atomici)

Unambiguity (Non ambigui)

Completeness (Completi)

Consistency (Consistenti)

Verifiability (Verificabili)

Tabella 1

Requirement text	
[REQ001] The system shall interface with a pressure sensor capable of measuring the gas pressure within the tank.	[REQ001] Il sistema deve interfacciarsi con un sensore di pressione in grado di misurare la pressione del gas all'interno del serbatoio.
[REQ002] The pressure sensor output may be analog (e.g., 0-5 V) or digital (e.g., I2C, SPI).	[REQ002] L'uscita del sensore di pressione può essere analogica (ad esempio, 0-5 V) o digitale (ad esempio, I2C, SPI).
[REQ003] The system shall sample the pressure sensor frequently.	[REQ003] Il sistema deve campionare frequentemente il sensore di pressione.
[REQ004] The board shall interface with a temperature sensor to measure gas temperature inside the tank.	[REQ004] La scheda deve interfacciarsi con un sensore di temperatura per misurare la temperatura del gas all'interno del serbatoio.

[REQ005] The temperature sensor output may be analog (e.g., thermocouple, RTD) or digital (e.g., I2C, SPI).	[REQ005] L'uscita del sensore di temperatura può essere analogica (ad esempio, termocoppia, RTD) o digitale (ad esempio, I2C, SPI).
[REQ006] The system shall sample the temperature sensor at a minimum rate of 1 Hz.	[REQ006] Il sistema deve campionare il sensore di temperatura ad una frequenza minima di 1 Hz.
[REQ007] The system shall continuously monitor the acquired temperature and pressure values.	[REQ007] Il sistema deve monitorare continuamente i valori acquisiti di temperatura e pressione.
[REQ008] The relief valve shall be controlled via a relay output.	[REQ008] La valvola di sicurezza deve essere controllata tramite un'uscita relè.
[REQ009] The relay shall be energized to open the relief valve only if temperature exceeds the maximum temperature threshold and pressure exceeds the maximum pressure threshold.	[REQ009] Il relè deve essere alimentato per aprire la valvola di sicurezza quando la temperatura supera la soglia massima di temperatura e la pressione supera la soglia massima di pressione.
[REQ010] If either temperature or pressure drops below their respective thresholds, the relay shall be de-energized (valve closed).	[REQ010] Se la temperatura o la pressione scendono al di sotto delle rispettive soglie, il relè deve essere disalimentato (valvola chiusa).
[REQ011] Pressure sensor accuracy shall be ±1% full scale or better.	[REQ011] La precisione del sensore di pressione deve essere ±1% del campo di misura o migliore.
[REQ012] Temperature sensor accuracy shall be ±1°C or better.	[REQ012] La precisione del sensore di temperatura deve essere ±1°C o migliore.
[REQ013] The system shall detect threshold exceedance and actuate the relay within 500 ms.	[REQ013] Il sistema deve rilevare il superamento delle soglie e attivare il relè entro 500 ms.
[REQ014] The board shall operate from a DC external power supply (e.g., 12 V or 24 V, or different one) and it shall include an internal voltage generator to supply the components	[REQ014] La scheda deve funzionare con un'alimentazione esterna in corrente continua (ad esempio, 12 V o 24 V, o diversa) e deve includere un generatore di tensione interno per alimentare i componenti.
[REQ015] Relay coil voltage and current rating shall be adequate.	[REQ015] La tensione e la corrente nominale della bobina del relè devono essere adeguate.
[REQ016] The system shall react to temperature and pressure violations within 2 seconds	[REQ016] Il sistema deve reagire alle violazioni di temperatura e pressione entro 2 secondi

[RISPOSTA]:

[REQ001] Corretto

[REQ002] Ambiguo (lascia la scelta all'implementazione)
[REQ003] Ambiguo ("frequentemente" non consente di stabilire un tempo esatto)
[REQ004] Non consistente – indica requisite per una "scheda" mentre nel resto del documento ci si riferisce ad un "sistema", quindi scheda=sistema oppure la scheda e' una parte del sistema?
[REQ005] Ambiguo (lascia la scelta all'implementazione)
[REQ006] Corretto
[REQ007] The system shall continuously monitor the acquired temperature and pressure values.
[REQ008] Non complete (non indica quale stato del rele' apre la valvola), vedi anche REQ009
[REQ009] Non atomico – nello stesso requisito si indica quale e' lo stato dele rele' che pilota l'apertura valvola, ed il criterio per la chiusura della valvola.
[REQ010] Corretto
[REQ011] Corretto
[REQ012] Corretto
[REQ013] Non consistente – l'informazione fornita dal requisito è il tempo (500msec), per la condizione di attivazione del relè è meglio fare riferimento al requisito esistente (REQ009, rivisto), anziché ripetere. Inoltre non è consistente con il REQ006, che indica una frequenza di campionamento di 1Hz, con la quale sarebbe impossibile garantire la risposta del sistema entro 500 msec/
[REQ014] Ambiguo (non indica un range certo per l'alimentazione esterna)
[REQ015] Non complete (non indica i valori di rating da soddisfare)
[REQ016] Non completo - indica requisite per una "reazione" del sistema a violazioni senza indicare in modo univoco cosa significhi. Non consistente, nel caso si riferisca alla reazione a violazione delle soglie, indica un tempo diverso rispetto ad un altro requisito (REQ013)

Esercizio 2

Rispetto al sistema descritto nell' Esercizio 1, rispondere alle seguenti domande:

2.1 : E' stato definito un safe state?

[RISPOSTA]: No

2.2: Se la risposta a 2.1 e' affermativa, indicarne il requirement. Altrimenti, formulare una proposta di safe state, qualora sia possibile in base alle altre informazioni fornite.

RISPOSTA]: non e' possibile formulare una proposta di safe state in base alle informazioni fornite. Non viene dettagliato se in caso di guato (es. sensori guasti) la HARA abbia indicato la condizione valvola aperta oppure chiusa come mitigazione accettabile del rischio, non è possibile determinarlo. Non sono stati forniti informazioni di possibili modi di segnalazione guasti all'esterno (da cui un possibile safe state).

2.3: quali sono le necessarie informazioni implementative che mancano dalla lista dei requirements in Tabella 1?

[RISPOSTA]: Valori di soglia di temperatura e pressione; definizione esplicita del safe state; informazioni su possibili diagnostiche

Esercizio 3

Rispetto ai requirements di Tabella 1 nell' Esercizio 1, riscrivere i REQ009/010/013 usando il seguente Structured Natural Language: [actor] shall [action verb] [object] [if/when condition] – [attore] deve [verbo attivo] [oggetto] [condizione]

RISPOSTA]:

[REQ009A]: Il sistema deve alimentare il relè per aprire la valvola di sicurezza

[REQ009B]: Il sistema deve aprire la valvola di sicurezza se la temperatura del gas supera la soglia di temperatura e la pressione del gas supera la soglia di pressione

(nota: requisito diviso in due distinti, in base al difetto originale, ovvero non era atomico)

[REQ010] Il sistema deve disalimentare il relè nel caso che la temperatura del gas oppure la pressione del gas oppure entrambe scendano sotto le rispettive soglie

[REQ010] Il sistema deve alimentare il relè entro 500 msec dal verificarsi della condizione espressa nel requisito [REQ009B]

Esercizio 4

Rispondere alle seguenti domande:

4.1: Una scheda elettronica contiene due microcontrollori identici che effettuano funzioni diverse. In produzione si scopre che su tutte le schede, i due microcontrollori smettono di funzionare quando la temperature ambiente supera 50 gradi, sebbene il sistema fosse specificato dover lavorare sino a 70 gradi. Di che tipo di failure si tratta (motivare la risposta)

4.2 Un sistema elettronico a display smette "ogni tanto" di funzionare. Spegnendo e riaccendendo, funziona di nuovo sino al prossimo blocco. Che tipo di guasto (failure) puo' essere? Scegliere una delle risposte sottostanti, motivando:

a) guasto permanente all'hardware (permanent fault)

b) guasto transitorio all'hardware (transient fault)

c) guasto sistematico del sw applicativo

d) le informazioni fornite non consentono di rispondere in modo certo

RISPOSTA]: d) – potrebbero essere vere ognuna delle tre ipotesi a), b), c)

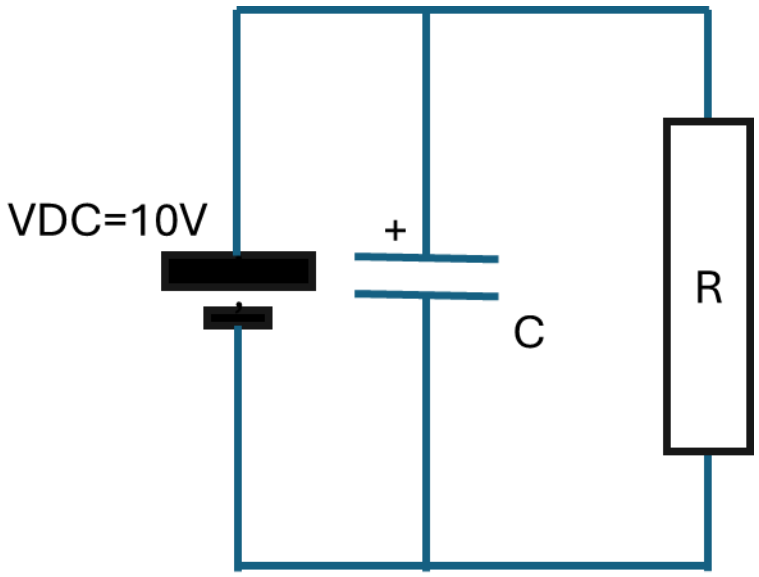
4.3: In un sistema elettronico che effettua la seguente funzione di sicurezza (safety function): "rilevare la presenza di oggetti o persone nel raggio d'azione di un cancello a scorrimento orizzontale motorizzato ed impedirne la chiusura tagliando l'alimentazione al motore", quale potrebbe essere un possibile safe state? Cosa cambierebbe nel safe state se il cancello fosse a scorrimento verticale?

RISPOSTA]: un possibile safe state e' "motore disalimentato" in quanto il cancello rimane fermo (non ci sono pericoli). Nel caso di un cancello verticale, "motore disalimentato" e' ancora corretto in presenza di un sistema che "freni" la caduta in caso di motore disalimentato, altrimenti il safe state in realtà aggiunge dei rischi.

4.4: Nel seguente circuito, determinare i valori minimi (per la scelta del componente a catalogo) di

- Potenza massima dissipabile dal resistore (R=500 Ohm)
- Tensione massima ammissibile del condensatore elettrolitico (C=100uF)

Affinché' il sistema possa essere considerato utilizzabile per l'implementazione di funzioni di sicurezza



[RISPOSTA]: qua deve esser usato il concetto di de-rating (i componenti debbono essere sovradimensionati in modo tale da essere utilizzati a 2/3 dei loro maximum ratings. Pertanto:

- Condensatore: sottoposto permanentemente a tensione di 10V, deve avere una tensione max a specifica di 15V
- Resistenza: nel circuito dissipa una potenza di 0.2W, quindi deve avere un max rating di 0.3W (in realtà' in commercio si trovano da 0,25W o 0,5W, quindi la scelta cadrebbe sulla 0,5W)

Esercizio 5

Descrivere in poche righe le differenze tra FTA e FMEDA.

[RISPOSTA]: La FTA è una analisi top-down, che discende dalla violazione del top safety requirement per discendere di causa in causa sino a trovare eventi primari. La FMEDA invece e' uan procedure bottom-up: si parte dal componente e se ne ricercano le relative failure, da ricollegare alla violazione del top safety requirement.

Esercizio 6

Dati due sistemi che implementano la stessa identica funzione di sicurezza (safety function) ma con safety integrity levels (SIL) diversi, si rileva che il costo totale di un sistema SIL3 e' molto maggiore di quello di un sistema SIL1. Quali sono i tre motivi dietro questa differenza?

[RISPOSTA]:

1) Target di metriche assolute. Per SIL3 il limite massimo tollerabile di residual failure rate e' molto piu' basso che per SIL1, il che implica per SIL3 l'uso di componenti migliori (con tecnologie e a bassa failure rate) e l'adozione di maggior numero di diagnostiche
2) Target di metriche relative. Per SIL3 i taget di DC e SFF sono piu' alti di quelli per SIL1, il che implica l'adozione in SIL3 di un numero maggiore di strutture diagnostiche, e quindi costo maggiore.
3) Implicazioni sul V-model e safety lifecycle. Il livello SIL pilota anche il tipo e numero di tecniche di progettazione e verifica da adottare. Un processo per SIL3 richiede una quantita' molto maggiore di tecniche, evidenze, documentazione rispetto al caso SIL1, ed anche un livello maggiore di indipendenza per reviews e assessments. Questo implica costi maggiori di progettazione.

Esercizio 7

Argomento: risk assessment. Ipotizziamo di avere una bombola di gas ad uso medicale che presenta un pericolo, perché presenta una certa probabilità "intrinseca" (ovvero al netto di condizioni esterne tipo urti o temperatura) di esplodere, ferendo chi si trovasse nei paraggi. In quale delle due situazioni operative si può stimare un rischio maggiore (motivare la risposta)?

a) Bombola stoccata in un corridoio di un reparto di ospedale attivo
b) Bombola stoccata (in attesa di essere utilizzata altrove) in un piccolo riparo ad un lato di un parcheggio del medesimo ospedale

[RISPOSTA]: generalmente, il rischio è il prodotto della severità (conseguenze) di un pericolo, per la probabilità che il pericolo si manifesti. Quindi a), vedi tabella

Situazione	Severità	Probabilità	Rischio
a) Reparto ospedale	Alta (fino a molte persone possono trovarsi nei paraggi)	Alta (e' molto probabile che nel caso la bombola esploda ci sia qualcuno vicino)	Alto
b) Riparo	Bassa (normalmente nessuno o forse una persona nei paraggi)	Bassa (molto improbabile che qualcuno si trovi vicino alla bombola proiprio quando esplode casualmente)	Basso

Esercizio 8

Mettere in ordine temporale e logico le seguenti attività del safety lifecycle: Decommissioning, HARA, E/EE/PE design/ E/EE/PE safety requirements writing

[RISPOSTA]:

Decommissioning,

1) HARA
2) E/EE/PE safety requirements writing

3) E/EE/PE design
4) Decommissioning

Esercizio 9

Indicare per le seguenti attività o argomenti tecnici, quali attengono alla Functional Safety, quali alla Security, quali alla Availability

Argomento/attività	Safety	Security	Availability
Tampering protection (cancellazione dei dati sensibili di un dispositivo se l'involucro viene aperto)		X	
Architetture 2oo3	X		X
Architetture 1oo2	X		
Memorie RAM ridondate con correzione di errore	X	X	X

Esercizio 10

Spiegare perché le metriche relative (DC, SFF, SPF) sono espresse in numeri puri (senza unità di misura) dato che le metriche assolute (es. PFH) sono tipicamente espresse in FITs ovvero una probabilità divisa per il tempo)

[RISPOSTA]: tutte le formule delle metriche relative sono rapporti tra failure rates. Quindi sono numeri puri, indipendentemente dalla natura delle grandezze espresse a numeratore e denominatore.