Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

ISTI Technical Reports

Analisi dello stato dell'arte e individuazione dei criteri per la misurabilità delle performace richieste al manager della sicurezza

Vittorio Miori, CNR-ISTI, Pisa, Italy
Dario Russo, CNR-ISTI, Pisa, Italy
Loredana Pillitteri, CNR-ISTI, Pisa, Italy

ISTI-TR-2020/020

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

Analisi dello stato dell'arte e individuazione dei criteri per la misurabilità delle performance richieste al manager della sicurezza

Miori V.; Russo D.; Pillitteri L.
ISTI-TR-2020/020

Abstract
Nel presente documento viene analizzato lo stato dell'arte dei criteri esistenti in letteratura per la misura delle performance di un sistema per la gestione della sicurezza e delle emergenze. In dettaglio, il documento è strutturato in tre sezioni principali che trattano l'ambito di diagnosi, prognosi e tolleranza ai guasti. In ogni sezione vengono dapprima richiamati i concetti di base principali, e successivamente descritti i principali criteri di misura delle performance che sono potenzialmente applicabili nel caso del manager della sicurezza.

Security, Fault Diagnosis, Fault Prognosis, Tolerance, Performance, Feature, Safety

Citation
Miori V.; Russo D.; Pillitteri L. *Analisi dello stato dell'arte e individuazione dei criteri per la misurabilità delle performace richieste al manager della sicurezza* ISTI Technical Reports 2020/020. DOI: 10.32079/ISTI-TR-2020/020

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1
56124 Pisa Italy
http://www.isti.cnr.it

Analisi dello stato dell'arte e individuazione dei criteri per la misurabilità delle performace richieste al manager della sicurezza

Vittorio Miori (CNR) – Dario Russo (CNR) – Loredana Pillitteri (CNR)

Breve sommario

Nel presente documento viene analizzato lo stato dell'arte dei criteri esistenti in letteratura per la misura delle performance di un sistema per la gestione della sicurezza e delle emergenze. In dettaglio, il documento è strutturato in tre sezioni principali che trattano l'ambito di diagnosi, prognosi e tolleranza ai guasti. In ogni sezione vengono dapprima richiamati i concetti di base principali, e successivamente descritti i principali criteri di misura delle performance che sono potenzialmente applicabili nel caso del manager della sicurezza.

Parole chiave

Safety, Security, Fault Diagnosis, Fault Prognosis, Tolerance, Performance, Feature

Indice

Introduzione 3
Criteri di misura delle performance diagnostiche 3
Criteri di misura delle performance prognostiche 9
Criteri di misura delle performance di tolleranza 11
Indice delle figure 12
Indice delle tabelle 12
Riferimenti 12
Abbreviazioni/acronimi 13

Introduzione

Il manager della sicurezza (*safety and security manager*) integra e gestisce in un unico framework tutti gli aspetti di sicurezza dell'ambiente di vita, siano essi relativi all'incolumità della persona (*safety*) oppure all'ambiente e alle infrastrutture in esso contenute (*security*). La continuità di funzionamento in caso di guasti e la prevenzione degli stessi, ricoprono un ruolo chiave del framework di interoperabilità. Il manager della sicurezza deve quindi essere in grado di rilevare e isolare eventuali guasti (diagnosi) nei dispositivi e negli impianti domestici, gestirli tempestivamente in modo da non pregiudicarne drasticamente le prestazioni (tolleranza ai guasti), e infine prevedere il possibile insorgere di nuovi funzionamenti fuori condizione nominale (prognosi).

Al fine di poter valutare oggettivamente le prestazioni del manager di sicurezza, tuttavia, si rende necessaria la definizione di uno o più criteri di performance dello stesso. Tali criteri possono essere individuati andando a considerare lo stato dell'arte dei supervisori di diagnosi e prognosi a livello industriale, che godono di consolidati criteri di misura delle prestazioni, con gli opportuni accorgimenti per l'adattamento al campo della domotica per gli ambienti di vita.

Criteri di misura delle performance diagnostiche

Un sistema di rilevamento e diagnosi dei guasti (*Fault Detection and Diagnosis*, *FDD*) ha l'incarico di individuare (*fault detection*) e valutare (*fault diagnosis*) i possibili guasti in un sistema, dove un guasto (*fault*) è visto come una deviazione non prevista di almeno una proprietà caratteristica del sistema (*feature*) dalla condizione accettabile, usuale o standard (Isermann, R. (2006)). Un sistema FDD può quindi essere pensato come un sistema di elaborazione dati sulla base della ridondanza delle informazioni, in cui dati e comprensione degli stessi sono i due elementi fondamentali. A seconda della tipologia di dati e di come essi sono processati, i metodi FDD possono essere classificati in tre categorie (Dai, X. & Gao, Z. (2013)):

- basati su modello (*model-based* ovvero *on-line data-driven*);
- basati su segnale (*signal-driven* ovvero *data-driven*);
- basati sulla conoscenza (*data-driven* ovvero *history-data-driven*).

La ridondanza delle informazioni nei metodi FDD basati su modello deriva dalla conoscenza analitica del sistema da diagnosticare, mentre l'informazione di ridondanza nei metodi FDD basati su segnale è la relazione tra i guasti e il pattern di segnale. Quando il processo è troppo complesso per essere modellato analiticamente e l'analisi del segnale non porta ad un risultato univoco, di solito si utilizzano approcci diagnostici supportati da sistemi esperti e intelligenza artificiale (AI), che richiedono però una notevole mole di dati storici per un corretto addestramento e funzionamento.

Il manager della sicurezza opera all'interno di un ambiente di vita, per sua natura complesso, ibrido, caratterizzato da numerosi sensori e attuatori, inoltre il manager deve anche soddisfare vincoli di sicurezza e affidabilità: in tale contesto si opera tipicamente con tecniche FDD basate sulla conoscenza, che vanno ad operare decisioni su uno o più feature del sistema, con approcci euristici o di natura statistica (Katipamula, S. & Brambley, M. R. (2005)). In ambito *Building and Automation Control Systems* (BACS), tali feature sono spesso indicate con il nome di *Performance Indicators* (*PIs*) o *Key Performance Indicators* (*KPIs*): le prime indicano variabili importanti da monitorare, le seconde sono invece combinazioni delle prime. Nati prevalentemente come indicatori per descrivere proprietà di natura energetica, i PIs/KPIs sono feature provenienti dai dati operativi del BACS e che forniscono informazioni importanti riguardo ad uno specifico componente o ad una specifica funzione (Brissman, J. & Ullmann, R. (2011)). Essi possono essere definiti a livello di stanza, dispositivo o edificio, in modo da essere impiegabili in contesti di diversa natura. A livello esemplificativo, la *European Building Automation and Controls Association* fornisce un elenco di 46 KPIs per l'ambito energetico, e.g.: consumo di energia totale dovuto al riscaldamento, temperatura della stanza rispetto alla temperatura della zona, velocità della pompa rispetto alla domanda di riscaldamento, ecc (eu.bac (2015)).

Vista la complessità e l'eterogeneità di un ambiente di vita, si ritiene opportuno

- considerare un insieme di KPIs globali che permettono la valutazione complessiva della safety e della security dell'ambiente di vita supervisionato dal manager della sicurezza (i.e. *reliability*, *MTTF*, *MTTR*, *availability*);
- individuare un insieme di metriche comuni per l'analisi delle performance del manager in ambiti specifici (e.g. energetico, comfort, ecc.) (i.e. POD, POFA, specificità, accuratezza, tempo di rilevamento del guasto).

KPIs Globali (Isermann, R. 2006)

- ***Reliability* (Affidabilità)**| E' la capacità di un sistema (processo o suo componente) di realizzare una funzione richiesta sotto specifiche condizioni, rispettando un determinato obiettivo e all'interno di un dato periodo di tempo. Si misura come

$$R(t) := \frac{n(t)}{N}$$ (funzione di affidabilità)

$$U(t) := \frac{n_f(t)}{N} = 1 - R(t)$$ (funzione di inaffidabilità)

dove *n(t)* indica il numero di elementi (ancora) funzionanti al tempo *t*, $n_f(t)$ indica il numero di componenti guasti al tempo *t,* e *N* il numero totale di componenti.

- ***Mean Time To Failure* (*MTTF*)**| E' il tempo medio alla rottura di un componente (o di un sistema). Si misura come

$$MTTF = \frac{n(t)}{\frac{dn_f(t)}{dt}}$$

Nel caso di sistemi domotici, è utile considerare il tempo di vita medio di componenti connessi in serie o parallelo, ricavabile da

$$R_{tot}(t) = \prod_{i=1}^{m} R_i(t) = e^{-\sum_{i=1}^{m} \lambda_i t} = e^{-\lambda_{tot} t}$$

(per sistemi in serie, λ= 1/MTTF failure rate)

$$U_{tot}(t) = \prod_{i=1}^{m} U_i(t) = \prod_{i=1}^{m} (1 - R_i(t))$$

(per sistemi in parallelo)

- ***Mean Time To Repair* (*MTTR*)**| Rappresenta il tempo medio necessario affinché un sistema soggetto a guasto venga riparato. Esso dipende sia dal tempo necessario per sostituire/riparare un singolo componente, sia dal tempo impiegato dal manager a diagnosticare correttamente il guasto.
- ***Availability* (Disponibilità)**| Probabilità che un sistema o dispositivo operi in maniera soddisfacente ed efficiente in un qualunque istante di tempo. E' una funzione dipendente dal tempo, come la reliability, tuttavia per sistemi che possono essere riparati. Si misura come

$$A := \frac{MTTF}{MTTF + MTTR}$$

Criteri di misura delle prestazioni di un sistema FDD

La misura delle performance di un sistema FDD viene effettuata andando a considerare i seguenti criteri: *Probability Of Detection* (*POD* o sensibilità), *Probability Of False Alarm* (*POFA*), specificità, accuratezza, tempo di rilevamento e *Fault Isolation Rate (FIR)* (Vachtsevanos, G. J., et al. (2006)). Facendo riferimento alla Tabella 1, è possibile definire i seguenti criteri di misura delle performance del rilevamento del guasto:

- La ***sensibilità*** fornisce una misura dei guasti rilevati rispetto a tutti i casi di guasto. Essa è definita come

$$\textbf{sensibilità} = Probability\ Of\ Detection\ (POD) = \frac{a}{a+c}$$

- La ***Probability Of False Alarm (POFA)*** fornisce una misura dei casi in cui viene attivato un allarme senza che ad esso corrisponda un effettivo evento di guasto. Essa è definita come

$$\textbf{Probability Of False Alarm (POFA)} = \frac{b}{b+d}$$

- La ***specificità*** fornisce una misura degli eventi (e.g. campioni di misura) correttamente ignorati in quanto non corrispondenti a guasto. Essa è definita come:

- L'***accuratezza*** misura l'efficacia dell'algoritmo nel distinguere correttamente tra guasti e non-guasti. Essa è definita come

$$accuratezza = \frac{a + d}{a + b + c + d}$$

	Fault (ipotesi H_1)	**No Fault (ipotesi H_0)**	
Rilevato (accettata H_1, positivo)	Guasto rilevato correttamente (vero positivo) # *a*	Falso allarme - errore tipo I (falso positivo) # *b*	*a+b* = numero totale di allarmi
Non rilevato (accettata H_0, negativo)	Mancato allarme – errore di tipo II (falso negativo) # *c*	Evento correttamente ignorato (vero negativo) # *d*	*c+d* = numero totale di non allarmi
	a+c = numero totale di guasti	*b+d* = numero totale di non guasti	*a+b+c+d* = numero totale di casi

Tabella 1: matrice decisionale per il rilevamento del guasto

La determinazione della condizione positiva (H_1 accettata) o negativa (H_0 accettata) è tipicamente fatta mediante l'uso di tecniche probabilistiche, applicate al dataset a disposizione. Una delle tecniche più diffuse è il test di ipotesi (Chiang, L. H., Russell, E. L. & Braatz, R. D. (2000)). Un'ipotesi statistica è un'affermazione che specifica parzialmente o completamente la legge di distribuzione della probabilità di una variabile casuale. L'affermazione può riferirsi sia alla forma funzionale della legge di distribuzione sia ai parametri caratteristici o ai soli parametri caratteristici quando si assume nota la forma analitica della distribuzione stessa. L'ipotesi "da verificare", usualmente indicata con il simbolo H_0, è detta ipotesi nulla o ipotesi zero. Ad esempio: "si ipotizza che l'altezza degli italiani adulti di sesso maschile si distribuisca in modo (approssimativamente) normale con media pari a 1,70 metri e scostamento quadratico medio pari a 0,28 metri". Se invece si dà per acquisito il fatto che l'altezza degli italiani adulti di sesso maschile si distribuisce in modo (approssimativamente) normale, l'ipotesi statistica potrà riguardare i soli parametri caratteristici media μ e varianza σ^2 (o lo scostamento quadratico medio σ).

Un ***test di ipotesi (statistica)*** è una regola attraverso la quale si decide se accettare o meno l'ipotesi formulata sulla base delle analisi dei campioni. Tali dati si riferiscono naturalmente alla variabile

casuale sulla cui legge di distribuzione è stata formulata l'ipotesi. Nello specifico, lo sviluppo di un test di verifica dell'ipotesi consiste in quattro fasi:

1. Definizione dell'ipotesi nulla H_0 e dell'ipotesi alternativa H_1, (i.e. assenza e presenza di guasto, rispettivamente).

2. Identificazione di un test statistico che può essere utilizzato per valutare se l'ipotesi nulla H_0 è vera (e.g. Z-test o t-test per ipotesi sul valor medio, chi-test per ipotesi sulla varianza).

3. Calcolo del p-value.

4. Confronto del p-value con un valore di significatività α.

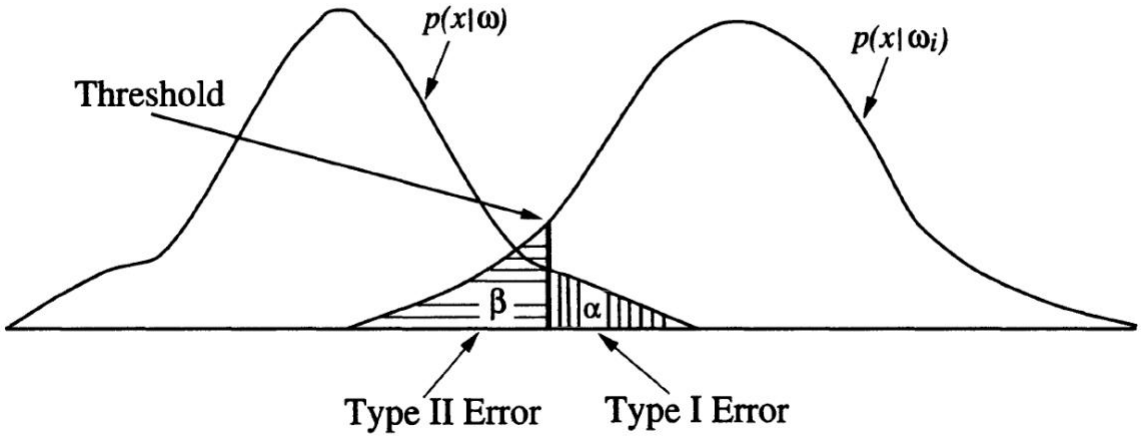

Figura 1: errori di un test di'ipotesi

Per applicazioni non critiche, cioè quelle non correlate alla sicurezza della vita o che non comportano costi enormi in caso di errore, i metodi FDD dovrebbero ridurre al minimo il numero di falsi positivi (falsi allarmi). Se un sistema FDD fornisce agli utenti degli allarmi in gran numero, quando essi non corrispondono a reali condizioni di guasto, gli utenti possono diventare frustrati, perdere la fiducia nel sistema e persino disattivarlo completamente in risposta (Katipamula, S. & Brambley, M. R. (2005)). Di conseguenza, il manager della sicurezza dovrebbe configurare i moduli FDD non critici per avere una bassa sensibilità ed evitare falsi allarmi. Analogamente, il manager dovrebbe configurare i moduli FDD critici per avere un'elevata sensibilità, evitando quindi mancati allarmi.

Un ulteriore importante criterio per determinare la bontà di un sistema di rilevamento guasti è il ***tempo di rilevamento del guasto***. Esso è definito come il tempo che intercorre tra la comparsa del guasto all'interno del sistema in esame, e l'individuazione dello stesso da parte del modulo diagnostico: tempi brevi sono desiderabili, tuttavia un tempo di rilevamento basso introduce una maggiore quantità di falsi allarmi.

Una volta che il guasto è stato rilevato, è necessario isolarlo e identificarlo (diagnosi propriamente detta). I moduli di diagnosi descritti nella letteratura sono prevalentemente basati su approcci di inferenza e approcci di classificazione (Isermann, R. 2006, Isermann, R. (2011)). Se sono disponibili

informazioni sulle relazioni causa-effetto tra guasti e sintomo, allora è preferibile fare affidamento su tecniche di ragionamento e metodi di inferenza. Se tale informazione non è disponibile, allora è possibile utilizzare metodi di classificazione addestrati sperimentalmente per generare le classi dei fault.

La letteratura scientifica presenta diverse metriche per la misura delle performance di un classificatore (Vachtsevanos, G. J., et al. (2006)): si riporta qui quella più comunemente adottata e di possibile implementazione all'interno del manager della sicurezza per ambiente di vita, ovvero la ***matrice di confusione***. La matrice di confusione evidenzia, in forma tabellare, il grado di correlazione tra diversi parametri (e.g. feature, classi, ecc.). E' una matrice quadrata con la stessa intestazione per righe e colonne, i cui campi rappresentano il grado di correlazione tra l'elemento *i* e quello *j*. Esse sono adoperate in diagnosi per misurare le performance di un classificatore, come mostrato in Tabella 2.

		Guasto		
		Guasto 1	**Guasto 2**	**Guasto 3**
Guasto	**Guasto 1**	$\boldsymbol{X_{11}}$	X_{12}	X_{13}
	Guasto 2	X_{21}	$\boldsymbol{X_{22}}$	X_{23}
	Guasto 3	X_{31}	X_{32}	$\boldsymbol{X_{33}}$

Tabella 2: matrice di confusione usata per metriche di diagnosi

La tabella mostra sulle colonne i possibili guasti, e sulle righe le etichette assegnate ai guasti dal classificatore. La diagonale, riportata in neretto, contiene i numeri delle corrette classificazioni dei guasti ad opera del classificatore. In maniera simile, gli elementi fuori diagonale rappresentano i numeri delle classificazioni non corrette (e.g. l'elemento X_{21} rappresenta il numero di volte che il guasto 1 è stato classificato erroneamente come il guasto 2). La probabilità di isolare correttamente un guasto (detta anche ***Fault Isolation Rate, FIR***) rappresenta la percentuale di guasti che il classificatore è in grado di isolare in maniera esatta:

$$FIR = \frac{A_T}{A_T + C_T} \cdot 100$$

$$A_T = \sum_i A_i$$

$$C_T = \sum_i C_i$$

dove A_i rappresenta il numero di guasti rilevati che il classificatore è in grado di isolare in maniera esatta (numeri sulla diagonale principale della matrice di confusione) e C_i è il numero di guasti rilevati che il classificatore non è in grado di isolare in maniera esatta (numeri fuori diagonale nella matrice di confusione).

Il metodo appena descritto associa lo stesso peso a tutti gli errori di tutte le classi. Criteri di performance più sofisticati possono essere basati sul concetto di *misclassification cost*, oppure su concetto di *Receiver Operating Characteristic (ROC)* (Hand, D. J. (2009)).

Criteri di misura delle performance prognostiche

La prognosi può essere definita come

- la rilevazione di un sintomo precursore di una rottura;
- la predizione della vita utile del componente analizzato (in inglese *Remaining Useful Life, RUL*);
- la definizione di un intervallo di confidenza della predizione.

La prognosi è un campo di ricerca attivo, e gli sforzi maggiori si concentrano sullo sviluppo di algoritmi che possano fornire una stima della RUL, generare un intervallo di confidenza della bontà della precisione e nell'integrazione di tali algoritmi nei sistemi di diagnosi (Saxena, A., et al. (2008)). Da un punto di vista applicativo, la misura delle prestazioni di un sistema diagnostico si opera nel tempo: con l'aumentare dei dati (esperimenti) la stima della RUL e dell'intervallo di confidenza tendono a migliorare, e a fornire dati sempre più vicini alla realtà.
Allo stato attuale non c'è ancora una standardizzazione dei metodi di misura delle performance di un sistema di prognosi (Vachtsevanos, G. J., et al. (2006)), e in letteratura si trovano metriche diverse a seconda del campo di applicazione e delle performance specifiche da misurare.
Due sono gli indicatori più utilizzati, e che per la loro natura sono potenzialmente applicabili al caso in esame del manager della sicurezza: l'accuratezza e la precisione.

- L'***accuratezza*** misura la vicinanza del valore predetto a quello attuale, Se si assume che per un *i*-esimo esperimento (finestra di acquisizione del manager della sicurezza) gli istanti di rottura di un componente, effettivi e predetti, sono rispettivamente $t_{af}(i)$ e $t_{pf}(i)$, allora l'accuratezza di un algoritmo di prognosi al tempo di predizione t_p può essere specificata come

$$\boldsymbol{accuratezza}(t_p) = \frac{1}{N}\sum_{i=1}^{N} e^{D_i/D_0}$$

  dove $D_i = |t_{af}(i) - t_{pf}(i)|$ rappresenta la distanza tra il valore predetto e quello effettivo dell'istante di rottura, D_0 è un fattore di normalizzazione e N è il numero di esperimenti.

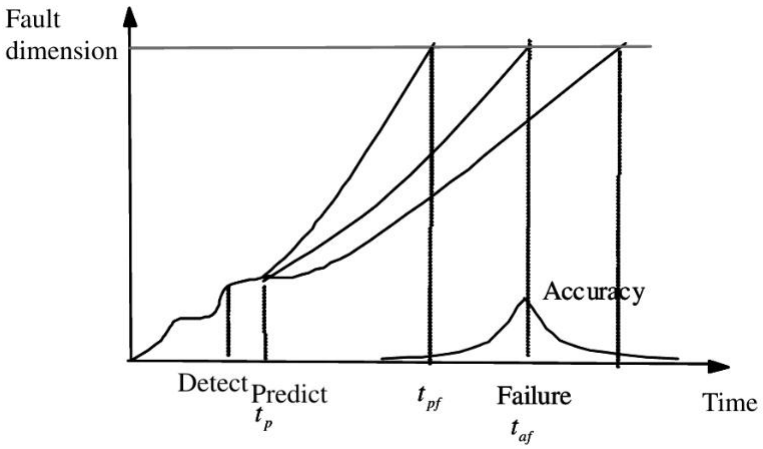

Figura 2: tempo di rottura predetto ed effettivo, con la relativa accuratezza

Il valore effettivo del tempo di rottura può essere conosciuto solo a posteriori, oppure stimato in ambiente simulato: è quindi necessaria una conoscenza teorica oppure storica della componente in esame, in modo da poter determinare il criterio. In Figura 2 (Vachtsevanos, G. J., et al. (2006)) è riportata l'evoluzione del guasto e la prognosi: si possono notare tre curve che partono al tempo di predizione t_p le quali rappresentano tre possibili evoluzioni della dimensione del fault (dipendono dai dati ricevuti dopo il tempo di predizione).

- La ***precisione*** indica quanto le predizioni (nel tempo) siano tra loro vicine. La precisione è definita sulla base della varianza dei risultati predetti per una serie di esperimenti: è alta se i valori predetti sono tra loro vicini, bassa altrimenti. Se si definisce l'errore di predizione come $E_i = t_{pf}(i) - t_{af}(i)$, con $\overline{E}$ il suo valor medio, e σ la sua deviazione standard, allora la precisione di un algoritmo di prognosi al tempo di predizione t_p può essere specificata come

$$\boldsymbol{precisione}(t_p) = \frac{1}{N}\left(\sum_{i=1}^{N} e^{-R_i/R_0}\right) \cdot e^{-\sigma^2/\sigma_0}$$

dove σ_2 e R_0 sono fattori di normalizzazione, e R_i è l'intervallo di confidenza per ogni esperimento.

Da un punto di vista formale, è possibile individuare ulteriori criteri legati ai concetti di accuratezza e precisione: essi costituiscono di fatto metriche di accuratezza e di precisione (Saxena, A., et al. (2008)). Esistono poi criteri basati su metriche diverse, ad esempio metriche di robustezza, computazionali o costo-beneficio. In letteratura esistono anche criteri più sofisticati, quali ad esempio similarità, tempi di predizione del guasto, l'orizzonte prognostico, metrica α-λ. Maggiori approfondimenti a riguardo possono essere trovati in (Goebel, K., et al. (2011)).

Criteri di misura delle performance di tolleranza

Diagnosi e prognosi operano online durante il funzionamento del sistema e permettono di individuare e/o prevenire la comparsa di un guasto nel sistema. La possibilità di gestire tale guasto, tuttavia, richiede una progettazione a monte ad hoc, come riportato in Figura 3 (Isermann, R. (2006)). Tale progettazione richiede l'utilizzo del concetto di ridondanza, ovvero la duplicazione dei componenti per poter garantire il funzionamento completo del sistema anche in presenza di rotture. Per elementi attivi (quali attuatori), la ridondanza hardware è l'unica in grado di garantire performance del sistema in caso di rottura. Nel caso invece di elementi passivi (quali sensori), è possibile fare affidamento anche sulla ridondanza analitica, nella quale le misure sono provenienti da uno o più componenti (anche diversi tra di loro) e da un insieme di relazioni analitiche (e.g. modello). A prescindere dal tipo di ridondanza, il manager della sicurezza deve essere in grado di garantire la funzionalità del sistema in caso di guasto (riconfigurazione) nei limiti individuati in fase di progettazione (*fault-tolerant design*).

Non esistono criteri specifici per la misura delle prestazioni del sistema di riconfigurazione, generalmente si richiede però al sistema

- un **tempo massimo di commutazione**;
- una **commutazione a priorità**, ovvero le funzioni non critiche vengono progressivamente abbandonate in favore delle funzioni più critiche nel momento in cui uno o più sottosistemi subiscono una rottura.

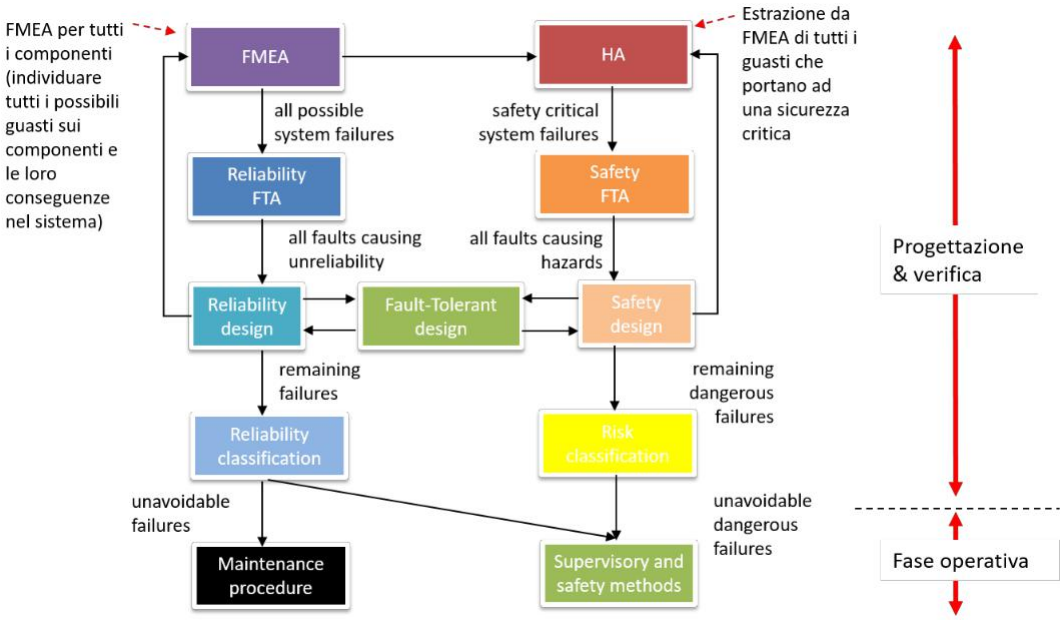

Figura 3: fasi di progettazione, verifica e operativa per sistemi tolleranti ai guasti

Riferimenti

Brissman, J. & Ullmann, R. (2011). Improving Energy Efficiency with Building Automation and Control Systems (BACS). *REHVA European HVAC Journal*.

Chiang, L. H., Russell, E. L. & Braatz, R. D. (2000). Fault detection and diagnosis in industrial systems. *Springer Science & Business Media*.

Dai, X. & Gao, Z. (2013). From model, signal to knowledge: A data-driven perspective of fault detection and diagnosis. *IEEE Transactions on Industrial Informatics*, 9(4), 2226-2238.

Ding, S. (2008). Model-based fault diagnosis techniques: design schemes, algorithms, and tools. *Springer Science & Business Media*.

European building automation control association – eu.bac (2015). System Certification Scheme Certifying Energy Efficiency of Building Automation and Control Systems, at first delivery and during the lifetime - Part 4: Specification of Key Performance Indicators. http://www.eubac.org/home/index.html

Goebel, K., Saxena, A., Saha, S., Saha, B., & Celaya, J. (2011). Prognostic Performance Metrics. *Machine Learning and Knowledge Discovery for Engineering Systems Health Management*, 147.

Hand, D. J. (2009). Measuring classifier performance: a coherent alternative to the area under the ROC curve. *Machine learning*, 77(1), 103-123.

Isermann, R. (2006). Fault-diagnosis systems: an introduction from fault detection to fault tolerance. *Springer Science & Business Media*.

Isermann, R. (2011). Fault-diagnosis applications: model-based condition monitoring: actuators, drives, machinery, plants, sensors, and fault-tolerant systems. *Springer Science & Business Media*.

Katipamula, S. & Brambley, M. R. (2005). Methods for fault detection, diagnostics, and prognostics for building systems—a review, part I. *Hvac&R Research*, 11(1), 3-25.

Katipamula, S. & Brambley, M. R. (2005). *Methods for fault detection, diagnostics, and prognostics for building systems—a review, part II*. *Hvac&R Research*, 11(2), 169-187.

Saxena, A., Celaya, J., Balaban, E., Goebel, K., Saha, B., Saha, S. & Schwabacher, M. (2008). Metrics for evaluating performance of prognostic techniques. In *IEEE International Conference on Prognostics and health management*.

Vachtsevanos, G. J., Lewis, F., Hess, A. & Wu, B. (2006). Intelligent fault diagnosis and prognosis for engineering systems. *Wiley*.

Indice delle figure

Figura 1: errori di un test d'ipotesi

Figura 2: tempo di rottura predetto ed effettivo, con la relativa accuratezza

Figura 3: fasi di progettazione, verifica e operativa per sistemi tolleranti ai guasti

Indice delle tabelle

Tabella 1: matrice decisionale per il rilevamento del guasto

Tabella 2: matrice di confusione usata per metriche di diagnosi

Abbreviazioni/acronimi

AI – Artificial Intelligence

BACS - Building Automation and Control Systems

CBM – Condition Based Maintenance

FD – Fault Detection

FDD – Fault Detection and Diagnosis

FI – Fault Isolation

FIR - Fault Isolation Rate

KPI - Key Performance Indicator

MTTF – Mean Time To Failure

PHM - Prognostic Health Management

POD - Probability Of Detection

POFA - Probability Of False Alarm

ROC - Receiver Operating Characteristic

RUL - Remaining Useful Life