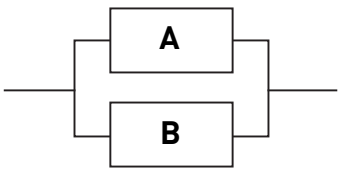
AFFIDABILITÀ E DISPONIBILITÀ

L'AUTORE COMPIE UN'INTERESSANTE ANALISI SUI CONCETTI DI AFFIDABILITÀ E DISPONIBILITÀ APPLICATI AL FUNZIONAMENTO DI UN SISTEMA DI AUTOMAZIONE INDUSTRIALE, EVIDENZIANDO I CRITERI PER PREVENIRE I GUASTI

Nel campo dell'automazione industriale i termini affidabilità *(reliability)* e disponibilità *(availability)* sono impiegati sempre più spesso per illustrare al meglio le funzioni di sicurezza e quelle di conduzione d'impianto. Entrambi i termini sono direttamente correlati fra loro e spesso sono confusi o addirittura considerati sinonimi. Ricordiamo che un sistema è inteso affidabile *(reliable)*, quando è poco suscettibile a perturbazioni che ne comportino un guasto, un blocco o una riduzione nelle sue capacità in modo imprevisto. È inteso invece come disponibile *(available)* quando è in grado di operare all'interno delle proprie capacità in modo continuativo.
Il miglior modo per incrementare entrambe le caratteristiche è di aumentare, duplicare per una o più volte, i componenti che costituiscono un sistema. Quante volte e come aumentare, sarà oggetto di specifiche considerazioni in funzione dell'applicazione cui il sistema è rivolto e della convenienza economica di questo tipo d'intervento nei confronti di una configurazione singola, in quanto con la duplicazione dei componenti crescono il numero degli elementi da acquistare, le complicazioni tecniche, di progettazione, installazione e manutenzione.
Per quanto riguarda le applicazioni, considerando la sola duplicazione dei componenti, si avrà la possibilità di ridondanza in serie o in parallelo con risultati e comportamenti funzionali diversi.

Ridondanza di un **sistema parallelo**

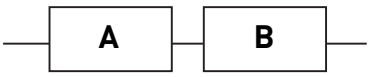


Il sistema funziona sia che entrambi o alternativamente i suoi componenti A e B, indipendenti fra loro, funzionino; per mettere fuori uso il sistema devono guastarsi entrambi i componenti.
Semplificando, per calcolare l'affidabilità **(Q)** e la disponibilità **(R)** dell'ipotetico sistema, si presume che la disponibilità dei due componenti A e B sia uguale e che questa sia pari a 0,1 e, allo stesso modo, che l'affidabilità dei due componenti A e B sia uguale e che questa sia pari a 0,9.

In tale ipotesi si avrà:

Q totale = QA x QB = 0,1 x 0,1 = 0,01 corrispondente all'1% di possibilità che il sistema si guasti
R totale = 1 – (1-RA) x (1-RB) = 1 – (1-0,9) x (1-0,9) = 0,99 corrispondente a una disponibilità del 99%.

Ridondanza di un **sistema seriale**



Il sistema funziona solo se entrambi i suoi componenti A e B, indipendenti fra loro, funzionano; per mettere fuori uso il sistema è sufficiente che si guasti indifferentemente uno dei due componenti.
Semplificando, per calcolare l'affidabilità **(Q)** e la disponibilità **(R)** dell'ipotetico sistema, si presume che i valori di disponibilità e affidabilità dei due componenti A e B siano uguali a quanto considerato nell'esempio precedente, anche per comprendere meglio la differenza tra le due soluzioni. Si avrà così:

Q totale = 1 – (1-QA) x (1-QB) = 1 – (1-0,1) x (1-0,1) = 0,19 corrispondente al 19% di possibilità che il sistema si guasti
R totale = RA x RB = 0,9 x 0,9 = 0,81 corrispondente a una disponibilità dell'81%.

Queste caratteristiche sono alla base delle considerazioni per applicazioni per le funzioni di sicurezza, nelle quali, in caso di guasto, un sistema dovrà assumere un comportamento *sicuro*, portando in uno stato stabile il processo che misura e controlla, per esempio fermandolo *(Fail Safe - a prova di guasto)*, oppure mantenendolo in funzionamento con prestazioni ridotte, assicurando le funzioni critiche, fino alla riparazione del guasto principale *(Fault Tollerant - Tollerante alle Anomalie)*.
Nel primo caso, l'intervento di arresto avverrà de-energizzando gli elementi finali degli attuatori di controllo, poiché l'esperienza maturata nell'industria di processo

dimostra che tali dispositivi, quando operano secondo questa modalità, presentano una percentuale di guasti compresa tra il 60 e il 90%.
Nel secondo caso, il componente guasto diventa ininfluente ai fini dell'operatività del sistema di sicurezza; ciò comporta la ridondanza funzionale dei vari componenti del sistema basata sul confronto dei risultati ottenuti tra due o più componenti. Se la differenza tra i risultati dei diversi componenti esce dal campo di accettabilità, si scarta il risultato che non concorda con la maggioranza dei risultati e si indica come probabilmente guasto ciò che lo ha riportato.
Normalmente, le tipiche architetture (MooN), previste per i sottosistemi sono le seguenti:
1oo1 architettura singola senza ridondanza (votazione 1 su 1);
1oo2 duplicazione parallela (OR con votazione 1 su 2);
1oo2D duplicazione parallela (OR con votazione 1 su 2), supportata da diagnostica;
2oo2 duplicazione serie (AND con votazione 2 su 2);
2oo2D duplicazione serie (AND con votazione 2 su 2), supportata da reciproca diagnostica;
2oo3 triplicazione a ridondanza maggioritaria (votazione 2 su 3).
Il sistema MooN è composto da "N" canali indipendenti connessi in modo tale che almeno "M" di questi siano sufficienti per eseguire la funzione richiesta.

Per ognuna di queste architetture, la Norma CEI-EN 61508-6 fornisce le specifiche PFD (Determinazione della probabilità media di guasto su domanda di intervento) dei sottosistemi.
Considerando le architetture più comuni, rispetto alla soluzione non ridondata (1oo1), risulta che:
1oo2 è più affidabile, però nel contempo è più sensibile ai guasti spuri;
2oo2 è meno affidabile, ma è meno sensibile ai guasti spuri;
2oo3 è più affidabile, meno della 1oo2, ma meno sensibile ai guasti spuri.

Secondo l'*Offshore Reliability Data handbook (OREDA)*, la probabilità di guasto su domanda (PFD) dei componenti di un sistema di automazione è dovuta tipicamente a:

42% sensori di misura;
8% risolutori logici;
50% elementi finali.

I guasti a loro volta devono essere definiti, considerando le conseguenze economiche, a seguito delle possibili interruzioni e quindi della mancanza di disponibilità di un impianto industriale determinata sulla base del tempo necessario per ripristinare completamente le condizioni produttive. Si potranno per esempio avere:
- **indisponibilità minori** - tempo di interruzione inferiore alle *n* ore, se nell'impianto a seguito dell'intervento spurio della protezione non si hanno conseguenze economiche significative entro tali *n* ore considerate;
- **indisponibilità moderate** - tempo di interruzione oltre *n* ore e *x* giorni. La definizione del numero dei giorni dipende strettamente dalla tipologia di processo, da quali ulteriori fermate di impianto comporta e dal costo economico in termini di mancato guadagno dell'impianto;
- **indisponibilità gravi** - tempo di interruzione tra *x* e *y* giorni. La definizione del numero dei giorni dipende strettamente dalla tipologia di processo, da quali ulteriori fermate di impianto comporta e dal costo economico in termini di mancato guadagno dell'impianto, dagli impatti che la fermata dell'impianto può comportare, anche in termini ambientali, e dagli eventuali costi accessori supplementari.

Per quanto riguarda la valutazione economica è necessario individuare il compromesso migliore in funzione della disponibilità o dell'affidabilità in relazione ai costi di manutenzione e di conduzione d'impianto, come illustrato nella figura 1.

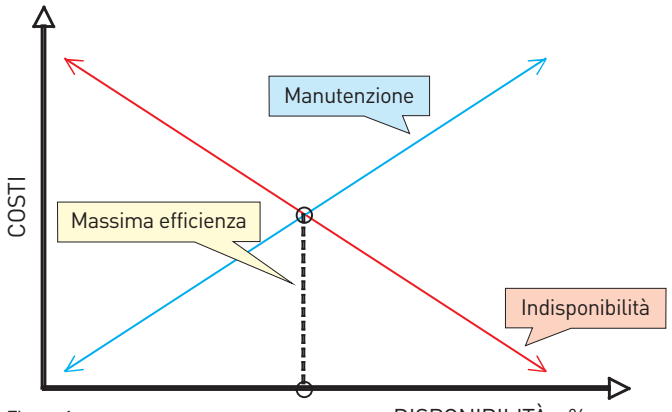


Figura 1

In effetti, esiste una terza via, o meglio una sommatoria di più qualità, per raggiungere comunque il compromesso migliore per quanto necessita. Le norme UNI e CEI (Comitato 56) la definiscono *fidatezza* (in inglese *dependability*). Si tratta della valutazione del livello di fiducia che può essere attribuito alla sicurezza di funzionamento di un sistema, inteso anche come organizzazione, e raggruppa le attività di valutazione dell'affidabilità *(reliability)*, della disponibilità *(availability)*, manutenibilità *(maintenability)* e sicurezza *(safety)*, riassunte con l'acronimo R.A.M.S. Queste valutazioni sono predittive e si basano su analisi dirette e indirette delle disfunzioni, dei guasti e degli errori, permettendo di assicurare che il sistema sia concepito, realizzato e continuamente adeguato al fine della sicurezza del funzionamento.

Bibliografia

CEI-EN 61508 - *Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza*
CEI-EN 61511 - *Sicurezza funzionale: sistemi strumentati di sicurezza per il settore dell'industria di processo*
UNI 9910 - *Fidatezza*

* *Perito Industriale Laureato, libero professionista, delegato del Collegio dei Periti Industriali e dei Periti Industriali Laureati delle Province di Milano e Lodi presso il Comitato Elettrotecnico Italiano (CEI), Sottocomitato 65A - Sistemi*