

Sistemi ridondanti

Contenuto

1. Definizione di sistema ridondante
2. Esempi di sistemi ridondanti
3. Scopo della ridondanza
4. Limiti di un sistema ridondante
5. Limite della ridondanza a due canali
6. Esempio di ridondanza a due canali e verifica esterna
7. Ridondanza nei sistemi critici
8. Logica di maggioranza
9. Limite dei guasti comuni
10. Ridondanza nei sistemi industriali

1. Definizione di sistema ridondante

Un sistema ridondante è un sistema progettato con componenti, canali o funzioni aggiuntive rispetto al minimo necessario, in modo che il guasto di un singolo elemento non provochi necessariamente la perdita completa della funzione.

In pratica:

un sistema non ridondante utilizza un solo componente o un solo canale essenziale;

un sistema ridondante utilizza uno o più componenti di riserva oppure più canali che svolgono la stessa funzione.

Secondo lo scopo del progetto, la ridondanza può permettere al sistema di continuare a funzionare, rilevare un'anomalia, passare a un componente di riserva oppure arrestarsi in modo controllato e raggiungere uno stato sicuro.

La semplice duplicazione dei componenti non garantisce da sola una ridondanza efficace. Servono anche una corretta logica di controllo, la separazione dei canali, la diagnostica e una manutenzione adeguata.

2. Esempi di sistemi ridondanti

Alimentazione ridondante: si utilizzano due alimentatori, ciascuno in grado di sostenere il carico previsto. Se uno si guasta, l'altro può mantenere acceso il sistema.

Dischi ridondanti: alcune configurazioni RAID, come RAID 1, RAID 5, RAID 6 e RAID 10, distribuiscono o duplicano i dati su più dischi. In base al tipo di RAID, i dati possono restare disponibili anche dopo il guasto di uno o più dischi. RAID 0 non è ridondante e un sistema RAID non sostituisce il backup.

Rete ridondante: si utilizzano due connessioni di rete. Se una connessione cade, il traffico può essere trasferito sull'altra mediante una procedura di commutazione.

Sensori ridondanti: più sensori misurano la stessa grandezza. Il confronto tra le misure permette di rilevare eventuali discordanze e individuare un possibile guasto.

Perché la ridondanza sia efficace, gli elementi duplicati devono essere sufficientemente indipendenti. Due componenti che dipendono dalla stessa alimentazione, dallo stesso cablaggio o dallo stesso apparato possono essere colpiti contemporaneamente dallo stesso guasto.

3. Scopo della ridondanza

Lo scopo principale della ridondanza è ridurre le conseguenze di un singolo guasto.

La ridondanza può aumentare:

- la disponibilità, cioè il tempo durante il quale il sistema resta utilizzabile;
- l'affidabilità rispetto a determinati tipi di guasto;
- la tolleranza ai guasti;
- la sicurezza;
- la possibilità di individuare e diagnosticare un'anomalia.

Formula concettuale:

ridondanza efficace = elementi aggiuntivi + controllo + diagnostica + separazione dai guasti comuni

La presenza di elementi duplicati, senza una corretta gestione, può non produrre un reale aumento dell'affidabilità o della sicurezza.

4. Limiti di un sistema ridondante

Un sistema ridondante può ridurre il rischio di fermo o di perdita della funzione, ma non rende il sistema infallibile.

a. Costo maggiore

Servono componenti duplicati, maggiore spazio, più cablaggi, più energia e più attività di manutenzione.

b. Maggiore complessità

Aumentano le parti da configurare, controllare e collaudare. Anche la logica di confronto o commutazione può guastarsi oppure essere progettata in modo errato.

c. Nuove possibilità di guasto

Ogni componente aggiunto può introdurre ulteriori modi di guasto. La ridondanza deve quindi essere progettata e verificata nel suo insieme.

d. Guasti di causa comune

Due o più componenti possono fallire contemporaneamente a causa dello stesso evento.

Esempi:

- due server alimentati dalla stessa linea elettrica senza UPS;
- due sensori contaminati dalla stessa sostanza;
- due controllori che utilizzano lo stesso software difettoso;
- due cavi posati nello stesso punto e danneggiati dallo stesso evento.

e. Manutenzione più delicata

Il componente di riserva deve essere controllato periodicamente. Un elemento apparentemente disponibile potrebbe essere già guasto senza che nessuno se ne accorga.

f. Falsa sicurezza

La presenza della ridondanza può far sottovalutare backup, controlli, prove periodiche, manutenzione e procedure di emergenza.

g. Tempo di commutazione

Il passaggio dal componente guasto a quello di riserva può richiedere un certo tempo. Durante questo intervallo il servizio può interrompersi o il processo può diventare instabile.

h. Ridondanza progettata male

Due componenti identici, installati nello stesso punto e dipendenti dalla stessa alimentazione, dallo stesso software o dallo stesso collegamento, possono essere colpiti contemporaneamente dallo stesso guasto.

5. Limite della ridondanza a due canali

Un sistema con due canali può confrontare due misure della stessa grandezza e rilevare una discordanza.

Per poter parlare di due canali realmente indipendenti non basta utilizzare due sensori. Devono essere valutati anche:

- cablaggi;
- alimentazioni;

- circuiti di acquisizione;
- unità di elaborazione;
- software;
- collegamenti di comunicazione;
- dispositivi di visualizzazione.

Se i due canali forniscono valori differenti, il sistema può stabilire che esiste un'anomalia. Dalla sola discordanza, però, non è normalmente possibile determinare quale dei due valori sia corretto, perché manca un criterio di maggioranza.

Il sistema può talvolta individuare il canale sospetto mediante controlli di plausibilità, autodiagnosi o confronto con limiti fisici noti. In assenza di queste informazioni è necessaria una verifica esterna.

Anche la concordanza tra i due canali non dimostra con certezza che entrambi siano corretti. I due canali potrebbero essere influenzati dallo stesso errore o dallo stesso guasto di causa comune.

La ridondanza a due canali è quindi utile per rilevare una discordanza, ma non garantisce sempre l'identificazione automatica del componente guasto.

6. Esempio di ridondanza a due canali e verifica esterna

Si consideri un sistema formato da due catene di misura separate.

Canale A:

- sensore A;
- cablaggio A;
- alimentazione A;
- circuito di acquisizione A;
- PC A;
- display A.

Canale B:

- sensore B;
- cablaggio B;
- alimentazione B;
- circuito di acquisizione B;
- PC B;
- display B.

I due sensori misurano la temperatura nello stesso punto.

Le letture sono:

Sensore A: 22,0 °C

Sensore B: 28,0 °C

Il sistema segnala una discordanza tra le due misure.

La conclusione corretta è:

«Le due misure non sono coerenti. È presente un'anomalia nel sistema di misura, ma con due soli canali e senza altre informazioni non è possibile stabilire quale misura sia corretta».

Il guasto potrebbe trovarsi nel sensore, nel cablaggio, nell'alimentazione, nel circuito di acquisizione, nel software, nel PC o nel display.

Per individuare il canale guasto si può:

- confrontare le misure con uno strumento terzo affidabile e correttamente calibrato;
- controllare i cablaggi e le alimentazioni;
- verificare i circuiti di acquisizione;
- controllare il software e i dati visualizzati;
- verificare la calibrazione dei sensori;
- scambiare i sensori tra i due canali durante una manutenzione controllata.

Lo scambio dei sensori deve essere eseguito soltanto durante una procedura di manutenzione e dopo avere portato l'impianto in una condizione sicura.

7. Ridondanza nei sistemi critici

Nei sistemi critici non esiste un'unica architettura valida per tutte le applicazioni.

La soluzione dipende:

- dal rischio presente;
- dalle conseguenze di un guasto;
- dalla continuità di servizio richiesta;
- dalla capacità diagnostica;
- dal tempo disponibile per reagire;
- dalle norme applicabili.

Possono essere utilizzate architetture a due canali oppure sistemi con tre o più canali.

Un sistema a due canali può rilevare una discordanza e, quando necessario, arrestare il processo in sicurezza.

Un sistema con tre canali può applicare una logica di maggioranza. Se due canali forniscono valori coerenti e il terzo è discordante, il sistema può identificare il canale sospetto e, se previsto dal progetto, continuare temporaneamente a funzionare.

Nei sistemi più complessi possono essere ridondanti anche:

- le unità di controllo;
- i PLC;
- i computer;
- gli attuatori;
- le reti di comunicazione;
- le alimentazioni;
- i cablaggi.

La ridondanza deve essere anche fisicamente separata. Un incendio, un urto, una perdita di liquido o un danno al cablaggio non deve eliminare contemporaneamente tutti i canali.

In alcuni casi si utilizza la diversità, cioè componenti, software o principi di misura differenti. Questa soluzione riduce la probabilità che lo stesso difetto colpisca tutti i canali nello stesso modo.

8. Logica di maggioranza

Si considerino tre sensori che misurano la stessa grandezza:

A = 100

B = 101

C = 150

Si supponga che il sistema consideri coerenti due letture quando la loro differenza non supera 2 unità.

A e B sono coerenti tra loro, perché differiscono di una sola unità.

C è invece fortemente discordante rispetto agli altri due valori.

Il sistema può quindi applicare una logica di maggioranza:

- rileva la discordanza;
- confronta i tre valori;
- individua C come canale sospetto;
- esegue l'azione prevista dal progetto.

L'azione può consistere nel:

- segnalare un allarme;
- escludere il canale sospetto;
- continuare in modalità degradata;
- richiedere una verifica;
- arrestare il processo in sicurezza.

L'esclusione automatica del canale non è obbligatoria e deve essere prevista e verificata durante la progettazione.

Il fatto che A e B siano coerenti rende probabile che C sia guasto, ma non fornisce una certezza assoluta. A e B potrebbero infatti essere entrambi influenzati dallo stesso errore o dallo stesso guasto di causa comune.

9. Limite dei guasti comuni

Un sistema ridondante può fallire quando più canali sono colpiti dalla stessa causa.

Questo fenomeno viene chiamato guasto di causa comune.

Esempi:

- contaminazione di più sensori;
- errore di calibrazione applicato a tutti i canali;
- software identico contenente lo stesso difetto;
- alimentazione comune;
- cablaggio comune;
- disturbo elettromagnetico;
- temperatura eccessiva;
- incendio;
- allagamento;
- errore umano durante la manutenzione.

La ridondanza numerica, da sola, non elimina questi rischi.

Per ridurre la probabilità di un guasto comune si utilizzano:

- separazione fisica;
- alimentazioni indipendenti;
- percorsi di cablaggio differenti;

- diversità di componenti e software;
- autodiagnosi;
- controlli di plausibilità;
- test periodici;
- manutenzione documentata;
- procedure operative;
- intervento umano quando necessario.

10. Ridondanza nei sistemi industriali

Nei sistemi industriali la ridondanza può avere due obiettivi differenti:

- garantire la continuità di servizio;
- garantire la sicurezza.

Continuità di servizio

In questo caso il sistema deve continuare a funzionare nonostante il guasto di un componente.

Si possono utilizzare:

- doppie alimentazioni;
- reti industriali ridondanti;
- doppi PLC;
- server di riserva;
- pompe o motori di riserva;
- componenti sostituibili senza arrestare l'intero impianto.

Sicurezza

In altri casi la priorità non è continuare a funzionare, ma evitare una situazione pericolosa.

Il sistema deve rilevare il guasto e portare la macchina o l'impianto in uno stato sicuro.

Esempio:

Sensore A = 6 bar

Sensore B = 11 bar

Se la pressione è una grandezza critica per la sicurezza, il sistema non deve necessariamente scegliere quale sensore sia corretto.

La risposta prevista dal progetto può essere:

segnalazione del guasto + arresto controllato + raggiungimento dello stato sicuro

La decisione dipende dalla valutazione del rischio e dalla funzione di sicurezza richiesta.

Nei sistemi industriali sono quindi fondamentali:

- diagnostica;
- soglie di plausibilità;
- test periodici;
- separazione dei canali;
- controllo dei guasti di causa comune;
- gestione delle modalità degradate;
- manutenzione documentata;
- procedure per il ripristino;
- verifica periodica dell'intero sistema.

Fonti

IEC 61508 — Functional safety of electrical/electronic/programmable electronic safety-related systems.

ISO 13849-1 — Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.

IEC 62061 — Safety of machinery — Functional safety of safety-related control systems.

IEC 61511 — Functional safety — Safety instrumented systems for the process industry sector.

IEC 60204-1 — Safety of machinery — Electrical equipment of machines — Part 1: General requirements.

Avizienis, Laprie, Randell, Landwehr — Basic Concepts and Taxonomy of Dependable and Secure Computing.

NASA — Redundancy Management Algorithms.