

[ANEXO 3]

Arquitecturas de votación

Las arquitecturas comerciales que se encuentran actualmente en el mercado son las siguientes:

- Arquitectura 1oo1
- Arquitectura 1oo2
- Arquitectura 2oo2
- Arquitectura 2oo3
- Arquitectura 1oo1D
- Arquitectura 1oo2D
- Arquitectura 2oo2D

A3.1. Arquitectura 1oo1

Esta arquitectura consiste en un solo elemento, donde cualquier falla segura des-energiza la salida y cualquier falla peligrosa impide que una señal de alarma válida no sea procesada correctamente. Esta arquitectura no es tolerante a fallas ni posee modo de protección de falla. La ventaja del sistema 1oo1 es que tiene el costo inicial de instalación más bajo de todas las configuraciones. En la figura A3.1 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo1.

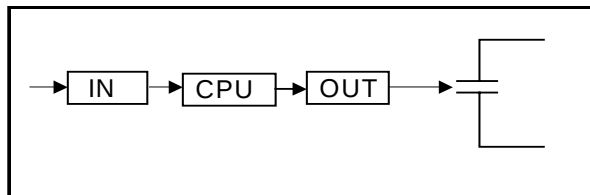


figura A3.1. Arquitectura 1oo1

A3.2. Arquitectura 1oo2

Esta arquitectura consiste en dos elementos conectados en serie en donde cada elemento puede comandar un disparo a la salida. Por lo tanto, debe haber una falla peligrosa en ambos elementos antes de que una señal de alarma válida no pueda ser procesada. El sistema ofrece una baja probabilidad de moverse al estado de falla peligrosa, pero incrementa la probabilidad de moverse al estado de falla segura. Se asume que cualquier prueba de diagnóstico sólo reporta las fallas encontradas y no cambia el estado o la votación de la salida. Las ventajas del sistema 1oo2 es que presenta buena inmunidad en contra de las fallas ocultas y, por lo tanto, una mayor disponibilidad de seguridad que un diseño 1oo1. Su desventajas son: mayor costo que el diseño 1oo1 y mayor susceptibilidad a disparos en falso (una señal falsa en cualquiera de los elementos resultará en un disparo del sistema). En la figura A3.2 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo2.

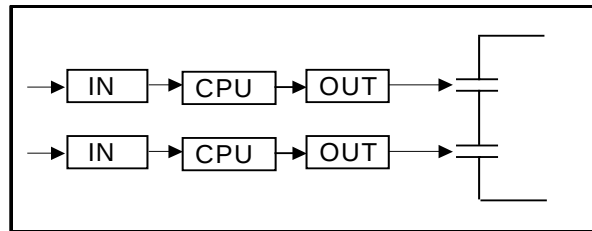


figura A3.2. Arquitectura 1oo2

A3.3. Arquitectura 2oo2

Esta arquitectura consiste en dos elementos conectados en paralelo en donde ambos elementos tienen que demandar un disparo antes que un disparo pueda llevarse a cabo. Se asume que cualquier prueba de diagnóstico sólo reporta las fallas encontradas y no cambia el estado o la votación de la salida. El diseño 2oo2 presenta la mejor inmunidad contra los disparos en falso (es usado principalmente en sistemas de control de producción en el cual el costo de una parada del proceso es extremadamente alta). Tiene como desventaja que una falla oculta o no de un elemento puede impedir un disparo válido desde el otro elemento. Por ejemplo, si los

dos elementos necesitan detectar una condición de disparo y uno de los sensores ha fallado de forma tal que nunca producirá una señal de disparo, este elemento fallado impedirá la ocurrencia de un disparo válido.

La arquitectura 2oo2 es buena para prevenir disparos en falsos pero es una arquitectura pobre para sistemas de seguridad. En la figura A3.3 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 2oo2.

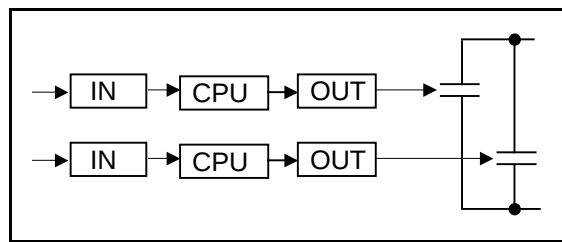


figura A3.3. Arquitectura 2oo2

A3.4. Arquitectura 2oo3

Esta arquitectura consiste en tres elementos conectados en paralelo con un arreglo de votación mayoritario para las señales de salida, en donde el estado de salida no cambia si sólo un canal entrega un resultado diferente al de los otros dos canales. Se asume que cualquier prueba de diagnóstico sólo reporta las fallas encontradas y no cambia el estado o votación de la salida. El diseño 2oo3 es una arquitectura robusta en contra de las fallas ocultas y disparos en falso. Un elemento puede fallar, sin iniciar un disparo en falso, y los dos elementos restantes continúan ofreciendo protección contra una condición de disparo válida. El diseño 2oo3 también ofrece la capacidad de colocar un elemento fuera de servicio para prueba o mantenimiento mientras mantiene el resto de la protección activa. La habilidad de comparar las señales de tres elementos incrementa ampliamente el diagnostic coverage (*DC*). La desventaja del diseño 2oo3 es que tiene el costo inicial más alto. El espacio y las conexiones necesarias para instalar tres elementos son mayores que el

que se necesita para instalar las configuraciones 1oo1 o 1oo2. Aunque el costo inicial de tres elementos es alto, el costo típico global del ciclo de vida es sustancialmente menor debido a la eliminación o reducción de los disparos en falsos. En la figura A3.4 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 2oo3.

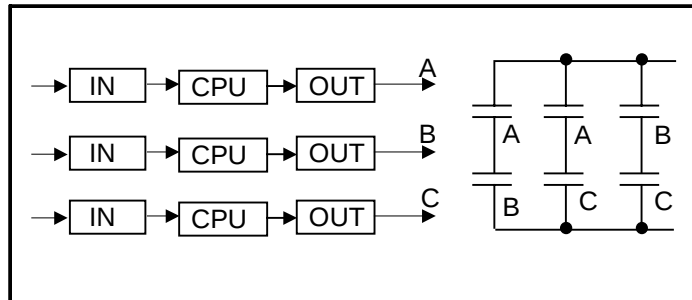


figura A3.4. Arquitectura 2oo3

A3.5. Arquitectura 1oo1D

Esta arquitectura consta de un solo elemento con una salida controlada por diagnóstico. Este sistema representa un uso de gran valor para aplicaciones de seguridad. En algunos sistemas la salida controlada por diagnóstico es un watchdog timer externo. Este timer controla una salida serial independiente que lleva al sistema a un estado seguro cuando el timer no es actualizado. En sistemas más avanzados, el diagnóstico integrado controla una salida en serie independiente que lleva al sistema a un estado desenergizado cuando una falla dentro del módulo es detectada. En este modelo, el diagnóstico permite que una falla peligrosa detectada sea convertida en una falla segura. En la figura A3.5 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo1D.

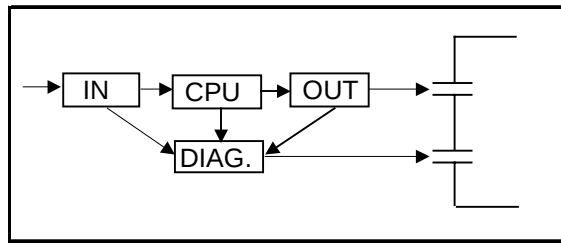


figura A3.5. Arquitectura 1oo1D

A3.6. Arquitectura 1oo2D

Esta arquitectura consiste en dos configuraciones 1oo1D colocados en un estilo 2oo2. Debido a que 1oo1D protege contra las fallas peligrosas, dos unidades son cableadas en paralelo para proteger contra las fallas seguras. Adicionalmente, con esta configuración, si las pruebas de diagnóstico en cualquiera de los elementos detectan una falla, entonces la votación de salida es adaptada de forma tal que el estado de salida del sistema sigue lo indicado por el otro elemento. Si las pruebas de diagnóstico encuentran fallas en ambos elementos entonces la salida se coloca en el estado de disparo. En la figura A3.6 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo2D.

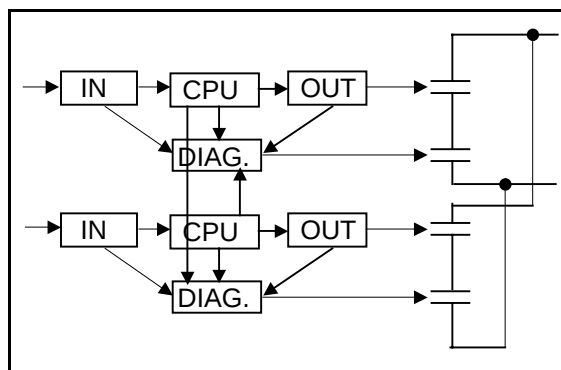


figura A3.6. Arquitectura 1oo2D

A3.7. Arquitectura 2oo2D

Esta arquitectura es básicamente igual a la arquitectura 1oo2D pero con menos líneas de diagnóstico, como se puede apreciar en la figura A3.7 en la cual se presenta el diagrama esquemático de un logic solver con arquitectura de votación 2oo2D.

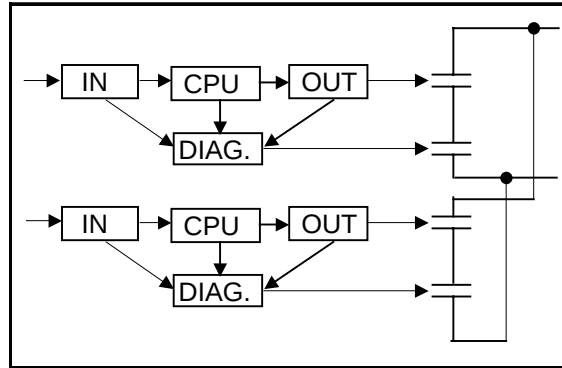


figura A3.7. Arquitectura 2oo2D