

Redundância e Disponibilidade características no SYSTEM302

Rodrigo Aznar Mendes
 Divisão de Desenvolvimento da SMAR

A utilização de redundância de hardware (ou de equipamentos) é um dos recursos mais empregados quando tolerância a falhas é requerida. Maior tolerância a falhas corresponde a maior disponibilidade da planta e maior segurança operacional e ambos os aspectos são importantes. A disponibilidade está diretamente relacionada ao tempo em operação e à lucratividade do negócio. E a segurança operacional diz respeito à preservação dos ativos e da vida das pessoas próximas ao processo.

O SYSTEM302 foi concebido tendo em consideração o tratamento para redundância em diversos níveis de seus componentes de hardware e software. Ou seja, é uma arquitetura de sistema concebida para ser redundante. Desta forma, o System302 vem se consolidando como solução de sistema para maior disponibilidade e segurança operacional.

Neste artigo são ressaltados alguns aspectos para apresentar melhor de que forma a redundância é tratada no System302 e o que pode ser esperado da mesma.

Redundância Hot Standby

Nos controladores DF1302 é empregada a estratégia de redundância Hot Standby. Nesta estratégia, o controlador Primário é o que executa todas as tarefas e o controlador Secundário é aquele que, continuamente sincronizado com o Primário, permanece pronto para assumir todo o processo caso ocorra alguma falha no controlador Primário. O processo de troca de função de Secundário para Primário, ocorre sem nenhum sobressalto e de maneira automática, ou seja, não requer ação do operador da planta.

Os controladores que suportam redundância atualmente são: DF62, DF63, DF73, DF75 e DF89.

Troca de função (switch over) dos controladores

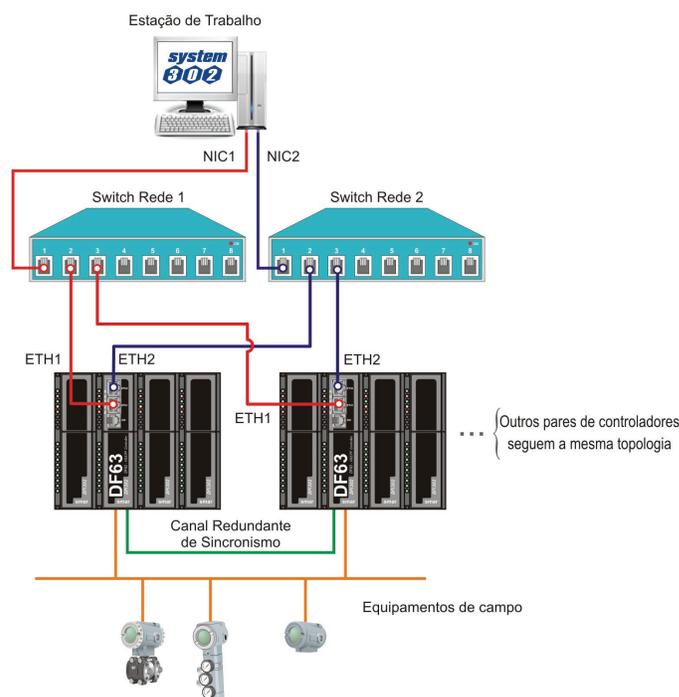
Através da troca de função (chaveamento ou switch over) a redundância dos controladores DF1302 pode detectar e cobrir diferentes tipos de falha:

Falhas gerais

- Falha de hardware.
- Falha na alimentação.
- Remoção do controlador do rack.

Falhas de interface / má condição

- Quando uma das interfaces do controlador Primário falha;
- Falha de ambas as interfaces Ethernet (falha dos cabos ou hardware).
- Falha de um canal H1 (DF62/DF63, falha de cabo ou hardware).
- Falha na comunicação Modbus quando operando como mestre (DF62/DF63, falha de cabo ou hardware)



Arquitetura básica de redundância para controladores DF1302 com duas portas Ethernet

Redundância da rede Ethernet de automação

Os controladores DF1302 possuem duas portas Ethernet (exceto DF62) possibilitando assim uma topologia redundante (ver figura ao lado). Havendo falha de algum elemento de rede (cabos ou portas Ethernet), esta será coberta pela troca de caminho de rede ou de porta Ethernet e não pelo chaveamento dos controladores.

Assim, a redundância de rede visa cobrir uma falha de caminho, seja ela em um cabo ou em uma porta Ethernet (do controlador, do switch ou da estação de trabalho).

Funcionalidades abordadas pela redundância

Seja qual for o tipo de falha ocorrida, a redundância no sistema garantirá o funcionamento sem sobressaltos dos seguintes aspectos do sistema:

- Supervisão por OPC;
- Operações solicitadas pelas estações de trabalho (downloads de configuração / parametrizações);
- Controle discreto e controle contínuo;
- Controle centralizado nos controladores (com blocos funcionais ou FFB/Ladder);
- Controle distribuído ou parcialmente distribuído no campo (links H1 entre equipamentos de campo e entre controlador e equipamentos de campo);
- Links HSE para a integração de controle entre diferentes pares de controladores;
- Acesso a cartões de entrada/saída convencionais (4 a 20 mA);
- Supervisão/controle por Modbus (integração com sistemas legados);

É suportada uma falha por vez, seja falha de controlador ou de rede. Ou seja, havendo uma falha, é necessário que esta seja reparada para que o sistema possa cobrir outra falha (redundância disponível novamente).

Transparência operacional

Nos configuradores Syscon e LogicView for FFB a redundância é vista de forma transparente para o usuário, ou seja, o par redundante é visto como um único equipamento. Este é o conceito conhecido como transparência operacional da redundância.

Na prática, o configurador sempre estará conectado ao controlador que estiver como Primário no momento. Assim, todas as ações de download ou configuração realizadas terão como destino o Primário atual. O sincronismo implementado no firmware dos controladores é responsável por atualizar constantemente o Secundário.

Definição automática de funções durante a inicialização

Os controladores definem as funções de Primário ou Secundário de forma autônoma durante a inicialização, não sendo necessária nenhuma ação ou escolha do usuário.

Diagnóstico específico para Primário e Secundário via SNMP

Como complemento à transparência operacional, por SNMP (Simple Network Management Protocol) é possível ter acesso a atributos de diagnóstico específicos de cada um dos controladores que formam o par redundante.

Diferentes tipos de falhas, como as falhas nas interfaces de comunicação (Bad Conditions), são indicadas mesmo que ocorram no controlador Secundário permitindo a manutenção proativa da redundância.

Através do SNMP OPC Server do System302, todas as informações de status e diagnóstico de redundância estão disponíveis para serem apresentadas em qualquer aplicativo supervisorio ou IHM que seja um cliente OPC.

Redundância de canal de sincronismo

Os controladores DFI302 têm o diferencial de possuir redundância de canal de sincronismo, o que significa maior disponibilidade da própria redundância do equipamento.

O sincronismo entre os controladores ocorre pela porta serial sobretudo durante a inicialização. Em condição de regime, o sincronismo é realizado através das portas Ethernet, o que garante uma maior taxa de transferência. Havendo falha na comunicação em uma porta Ethernet, o sincronismo é estabelecido pela outra porta.

Facilidade de uso

Os procedimentos para as fases de partida, operação e manutenção são tão simples quanto para sistemas não redundantes, economizando tempo durante os principais casos de uso:

Partida do sistema

Apenas um download de configuração é suficiente para configurar o par de controladores. Toda a configuração recebida pelo Primário é transferida para o Secundário através do canal de sincronismo.

Substituir um módulo controlador com falha

Não é necessário um novo download de configuração ou intervenção do usuário. O novo controlador inserido é automaticamente reconhecido, recebendo toda a configuração e parametrizações online do controlador em operação, a partir do canal de sincronismo redundante.

Adicionar controladores redundantes a um sistema não-redundante

Um sistema não-redundante em operação pode ter controladores redundantes adicionados posteriormente sem interrupção do processo. O processo de migração é simples, utilizando o mesmo princípio do caso de substituição de um controlador com falha.

Atualizar a versão de firmware dos controladores sem interrupção do processo

É possível realizar o upgrade de firmware dos controladores para agregar novas características sem interrupção do processo. O procedimento consiste em atualizar o firmware de um controlador por vez, sempre aguardando o sincronismo ser completado entre cada atualização de firmware.

Para conhecer em detalhes os parâmetros de status e diagnóstico da redundância, acesse <http://www.smar.com/brasil2/products/dfi302.asp> e consulte o manual do usuário, seção Adicionando redundância aos controladores DFI302 HSE.