www.system302.com

Redundancy and Availability

Features in the SYSTEM302

Rodrigo Aznar Mendes
SMAR R&D Division

Hardware or equipment redundancy is one of the most used resources as far as failure tolerance is concerned. Higher tolerance to failures implies higher plant availability and operational safety, both aspects being important. Availability is directly related to the operating time and the business profitability, whereas operational safety refers to the preservation of assets and the lives of the persons close to the process.

The SYSTEM302 was devised taking into consideration how to deal with redundancy on its several levels of hardware and software components. In other words, it is a system architecture designed to be redundant. Consequently, the System302 stands out as the solution for more operational availability and safety. This article stresses some aspects that better show how redundancy is treated on System302 and what to expect from it.

Hot Standby Redundancy

DFI302 controllers use the Hot Standby redundancy. In this strategy, the Primary controller executes all the tasks and the Secondary controller, continuously connected to the Primary stays ready to take over the whole process in case a failure occurs on the latter. Switching over from Secondary to Primary occurs smoothly and automatically, without any action by the plant operator. The controllers that currently support redundancy are the DF62, DF63, DF73, DF75 and DF89.

Controllers switch over

Through switching over, the DFI302 controller redundancy can detect and cover different types of failures:

General failures

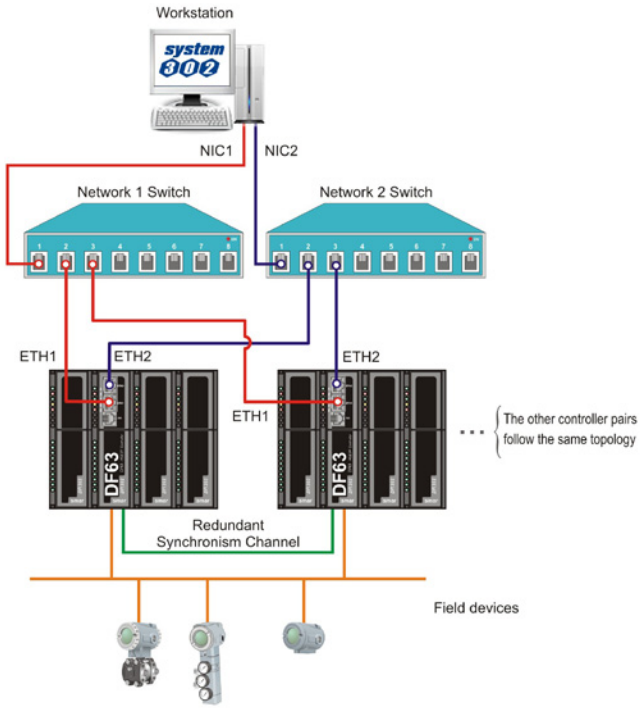
- Hardware failure.;
- Power supply failure;
- Rack controller removal.

Interface / bad condition failures

- When one of the Primary controller interfaces fails;
- Failure of both Ethernet interfaces (cable or hardware failure)
- Failure of a H1 channel (DF62/DF63, cable or hardware failure).
- Failure on Modbus communication while operating as master (DF62/ DF63, cable or hardware failure).

Ethernet automation network redundancy

The DFI302 controllers have two Ethernet ports (except the DF62), which enables a redundant topology (see figure at the side). If a failure occurs on any network element (Ethernet cables or ports), it will be covered by changing the network path or the Ethernet door and not by switching over controllers. Therefore, network redundancy covers path failure, be it a cable or an Ethernet port on the controller, the switch or the workstation.



Basic architecture for DFI302 controllers with two Ethernet ports

Functionalities covered by redundancy

Whatever the type of failure, the redundancy in the system will smoothly guarantee the work on the following system areas:

- OPC supervision;
- OPC requested by the workstations (configuration/parameterization download);
- Discrete and continuous control;
- Centralized control on controllers (with functional blocks or FFB/Ladder;
- Control distributed or partially distributed on the field (H1 links among field devices and also between controller and field devices);
- HSE links for control integration between different pair of controllers;
- Access to conventional input/output 4 – 20 mA cards;
- Modbus supervision/control (integration with legacy systems).

One failure is supported at a time, either on the controller or the network. That is, in case of a failure, it needs to be repaired for the system to cover another failure (available redundancy again).

Operational transparency

On Syscon and LogicView FFB configurators redundancy is transparent to the user, that is, the redundant pair is viewed as one single equipment. This concept is known as operational redundancy transparency. In practice, the configurator will always be connected to the controller working currently as Primary. Therefore, all of download or configuration actions are carried out as the destination of the current Primary controller. The synchronism implemented on the firmware of the controllers is the responsible for the continuous update of the Secondary.

Automatic function definition during initialization

The controllers define the Primary or Secondary functions in an autonomous way during the initialization, without user participation on the action or the choice.

Specific Primary and Secondary diagnostics via SNMP

As a complement to operational transparency, through SNMP (Simple Network Management Protocol) access is possible to specific diagnostics attributes of each controller forming the redundant pair. Different types of failures on the communication interfaces, known as Bad Conditions, are reported even if occurring on the Secondary controller, which permits proactive redundancy maintenance. Through the System302 SNMP OPC Server every information on redundancy status and diagnostics are available for presentation on any supervisory tool or HMI working as an OPC client.

Synchronism channel redundancy

The DFI controllers have synchronism channel redundancy as distinctive feature, which render them more availability for the equipment own redundancy. The synchronism between controllers is performed through the serial port mainly during initialization. In steady condition, the synchronism is carried out through the Ethernet ports, thus ensuring higher transference rate. In case of communication failure on one port, the synchronism is established by the other port.

Easeness of use

The procedures for the startup, operation and maintenance phases are as simple as for non-redundant systems and save time during the main uses:
System startup
Only one configuration download is sufficient to configure a pair of controllers.
The entire configuration received by the Primary is transferred to the Secondary through the synchronism channel.

Replacing a failing controlling module

There is no need for a new configuration download or intervention by user. The new inserted controller is automatically recognized and receives the whole online configuration and parameterization from the operating controller, through the redundant synchronism channel.

Adding redundant controllers to a non-redundant system

A non-redundant system in operation may have redundant controller added later without interrupting the process. The procedure consists of updating one controller at a time, always waiting for the synchronism to be completed between each firmware update.

Updating the controller firmware version without interrupting the process

It is possible to upgrade the controller firmware to add new features without interrupting the process. The migration process is simple and uses the same principle as for replacing a failing controller.

To know in detail the redundancy status and diagnostics parameters, access http://www.smar.com/products/dfi302.asp and consult the user manual, on the section Adding redundancy to DFI302 HSE controllers.