SIS Application Note

Fault Tolerance

What does it mean? Is there more than one definition? Why should it matter to an end user?

Objective

Fault tolerance is primarily a matter of operational availability. When used in specifications for SIS systems, the objective is to be able to identify a fault in the Safety Instrumented System (SIS), and continue to run safely without interruption. But, does the term accomplish the objective, or is there ambiguity in the definition of the term?

Traditional Definitions

Perhaps Hewlett-Packard defined availability terms as well as they can be defined. While paraphrased below, H-P, in documentation of its servers, defines fault tolerance in the following way:

- **Fault-Tolerant** - The top rung of the ladder is known as fault tolerance. Whereas the strategy of a high-availability system is to recover from an outage quickly, the strategy of a fault-tolerant system is to prevent the mission-critical system from coming down in the first place - at all costs.

Are SIS Systems Different?

While HP's definition probably works in a computing environment, is it really sufficient for safety instrumented systems (SIS)? Shouldn't SIS users require not only fault tolerance, but the ability to repair the fault online?

Some vendors of Safety Instrumented Systems (SIS) design controllers with redundant processors "in the same controller" and tout fault tolerance as if that were a significant benefit to users. While such fault tolerance assists the vendor in meeting the requirements of IEC 61508, according to ISA84, if the SIS cannot be repaired online, **the only benefit of fault tolerance by the traditional definition is that the user can schedule his shutdown.**

Is a shutdown dictated only by a fault in a "fault tolerant" SIS acceptable when the cost is lost production that could mean the loss of tens or hundreds of thousands of dollars? One of the objectives of an SIS should be to require a shutdown only when safety concerns demand it.

Section 11.3.1 of ISA 84 states that if a fault occurs in an SIS, one of the following actions is required::

a) *a specified action to achieve or maintain a safe state (see note); or*

b) *continued safe operation of the process whilst the faulty part is repaired. If the repair of the faulty part is not completed within the mean time to restoration (MTTR)*

3000 Controller Family

RTP offers a complete family of high-integrity Safety Instrumented Systems, all following the standards of IEC61508. For the highest level of integrity and availability, the 3000-T Triple Modular Redundant System features 2oo3D voting with triple, dual, or simplex I/O to obtain the required SIL rating.

The 3000-D Safety Instrumented System is built on the same advanced technology as the 3000-T, for dual redundant 1oo2D solution. The 1oo2D voting uses advanced diagnostics to assist in results adjudication. According to IEC61508, 1oo2D systems can achieve the same the same SIL rating as 2oo3D systems. The 3000D features dual-redundant processors with triple, dual, or simplex I/O as required.

When processor redundancy is not a requirement, the 3000-S Single processor configuration provides integrity and availability that exceeds that of competing single systems. With its built-in data validation schemes and redundant host communications, secure measurement and control are achieved.

The 3000-T, 3000-D, and 3000-S support up to 16 chassis of I/O providing high availability systems with I/O counts as large as 10,000 I/O.

RTP Corp.

1834 SW 2nd Street
Pompano Beach, FL
33069

Phone

954/974-5500

Fax

954/975-9815

E-mail

rtpinfo@rtpcorp.com

Web

www.rtpcorp.com

> *assumed in the calculation of the probability of random hardware failure, then a specified action shall take place to achieve or maintain a safe state (see note).”*

While the notes have not been reprinted here, it is probable that the “specified action” would be to bring the process to a safe state. And, a safe state must be achieved within the designed MTTR. If the SIS cannot be repaired without a shutdown, that means that a shutdown must be scheduled, and it must be scheduled within the designed MTTR.

Clearly, fault tolerance, by its traditional definition, is of little value in safety systems controlling industrial processes.

A key attribute of fault tolerant systems for the process industry must be the ability to repair the fault without interrupting the operation of the system.

Perhaps the definition of fault tolerance, as applied to SIS systems, should be modified.

In order for fault tolerance to be of benefit to SIS users, online repair capability should be included.

The objective of a fault-tolerant SIS should be to prevent the mission-critical process from shutting down if it can be assured that it can continue to run safely, and to be able to repair the fault and return to designed levels of safety protection without having to interrupt the operation of the mission critical process.

If continued operation of the process is the objective, end users who wish to be able to continue to run their process even in the event of a fault should not be specifying fault tolerance, which can be interpreted in its classic sense. They should be specifying fault tolerant systems with online repair capability. Without that ability, fault tolerance is of little value.

RTP has always viewed online repair as a requirement of fault tolerant Safety and Critical Control Systems.

Fault tolerance is not the only term users should be careful about using.

Safety Instrumented Systems are an emerging field. The is a great deal of information and disinformation in the field at this time.

End users should be sure that they clearly define the functionality desired, not in traditional terms, but by specifying the attributes and functions that need to be present in the system.

The RTP 3000 can be applied in a fault-tolerant manner, meaning:

- Faults will be automatically identified by the 3000 without the need for any user application programming to identify them.
- The 3000 will always continue to operate in a safe manner in the presence of a single fault (and in many cases, in the presence of multiple faults).
- All faults can be repaired without the need to shut down the process the 3000 is protecting.

This should be the standard for all SIS systems.

About RTP

Founded in 1968, RTP Corp. is a developer and manufacturer of high-performance critical control and safety systems. Markets for RTP Corporation's products include process control and safety systems, and nuclear power plant systems. RTP offers a wide range of rugged hardware and a complete suite of software for industrial control