The Ten Truths of Safety Instrumented Systems

Truth 7:

Dual SIS Technologies do not cost less than TMR; they almost always cost more.

Many companies advertise their Dual SIS technology (1oo2D (Dual), 1oo2DR (Dual Redundant), 2oo4D) as a lower-cost alternative to Triple Modular Redundant (TMR) systems. This is an unfortunate misrepresentation of the capabilities of Dual SIS architectures. Dual PLCs in a 1oo2 (1 out of 2) configuration were the initial solution of choice for "fail safe" applications, but they cannot overcome an inherent problem with false trips.

1oo2 voting logic causes false trips because if a fault is diagnosed in any one of the channels a shut down must occur.

Performance
Vendor sponsored published authors have concluded that the probability to failure on demand (PFD) of 2oo4 systems is comparable to that of 2oo3 systems. This conclusion is based on Markov models and equations that only apply to a theoretical 2oo4 system where a degradation path of 4-3-2-0 could be ideally conceived. However such performance is not possible in commercial implementations of logic solvers branded as “Quad” 2oo4D.

In all commercial implementations where two processors reside in the same electronic module, such systems can only degrade their processors in a 4-2-0 path. When one fails the two processors that reside in the same module are declared faulted and there is only one pair available, hence the 4-2-0 degradation path.

Furthermore, in most case the I/O modules are NOT “quad” either, they are not even redundant, and the outputs are at best configured as 1oo2D. In all commercial available architectures the desired level of redundancy is created by adding *additional hardware*. The bottom line is that these systems are basically “dual” with some enhancement in the fault tolerance section of their processors.

The publications mentioned above (see references) are based on ISA TR84.02, Part 2 that defines simplified equations to determine PFD, however “The objective of this technical report is to provide users with techniques for the evaluation of the hardware safety integrity of SIF ($\mathbf{PFD_{average}}$) and the determination of $\mathbf{MTTF_{spurious}}$. Methods of modeling systematic failures are also presented so a quantitative analysis can be performed if the systematic failure rates are known” as one of the methodologies presented “ISA-TR84.0.02 - Part 2 provides simplified equations for calculating the SIL values for Demand Mode Safety Instrumented Functions (SIF) installed in accordance with ANSI/ISA 84.01-1996, **“Applications of Safety Instrumented Systems for the Process Industries”. Part 2 should not be interpreted as the only evaluation technique that might be used.”**

We consider it important to highlight some of the assumptions of ISA-TR84.0.02 - Part 2

- 4.6 The logic solver failure rate includes the input modules, logic solver, output modules, and power supplies. **These failure rates are typically supplied by the logic solver vendor.**

- 4.9 The Test Interval (TI) is assumed to be **much shorter** than the Mean Time To Failure (MTTF).

- 4.10 Testing and repair of components in the system are assumed to be **perfect**.

- 4.16 The Beta model is used to treat possible common cause failures. The assumption is made that $1-\beta \cong 1$ which will yield conservative results in the calculation.

- 4.17 The equations developed in this part assume a graceful degradation path, i.e., 2oo4 system is assumed to degrade as **4-3-2-0.**

In the process of simplifying the $PFD_{average}$ equations, some terms are neglected. For example, the term that represents multiple failures during repair in the equation is assumed negligible for short repair times. Also, those terms in the equations representing common cause (Beta factor term) and systematic failures are not included in the calculations.

Therefore the equations used are a simplification of actual performance that does not account for the specific characteristics of the logic solver architectures being compared. These equations also have no relation to commercially available products, possibly leading to inaccurate conclusions.

The performance of a dual system is not better because the degradation path is typically 2-0. Few users can run their process on a single processor and meet the vendor recommendations as documented in the system safety manual. Most dual systems will need to be shutdown after a mis-compare for maintenance, affecting safety and process uptime.

Implementation
In order to get closer to the ideal performance of a 2oo4 system, the end user or system integrator should add the following elements:

- Additional I/O modules to provide redundancy at the I/O level.
- Additional termination panels to wire the same instrumentation to multiple I/O modules.
- Additional application programming to link the additional I/O points to their redundant counterpart.
- Additional application programming to compare or vote inputs.
- Additional logic to select outputs.

Since none of the above mentioned additions are native to the product, the implementation will require additional documentation to comply with safety standards and regulations. Additional documentation will also be needed to facilitate maintenance over the lifecycle of the product. All of the above mentioned additions add cost and complexity to the installation.

Hardware

The cost of additional hardware to meet redundancy requirements is not only the cost of the hardware. It also includes costs for cabinet space, wiring, power distribution, and documentation.

The added hardware alone will not provide the equivalent performance of a purposely designed redundant system. Some form of redundancy broker must be implemented, typically in the application program, to compensate for the lack of embedded diagnostics.

Most commercially available systems cannot handle multiple diagnosed hardware failures. A practical example would be a failure of one output point in a module which would typically drive all points on that module to their safe state. Unless there is a redundant module installed, all those final elements will transition to their safe state, affecting safety and process uptime.

Embedded Diagnostics
A simple analysis of dual architectures will expose the limitations in diagnostic coverage of microprocessors and will prove the value of relying on the strength of comparative diagnostics between multiple channels. The bottom line is that on dual systems any undiagnosed mis-comparison between channels must lead to a spurious shutdown of the system. Despite the name “fail safe” associated with 1oo2D or 2oo4D dual systems, they have a tendency to fail spuriously.

On the other hand, fault tolerance and process up-time are both inherent in TMR technology. The military and aerospace industries have used triplicated systems for decades. Some companies have accomplished an optimal implementation of this technology in process plants.

In all practical implementations the combination of 2oo3 majority voting with the strength of self and comparative diagnostics has proven to be the key advantage of fault tolerant architectures over fail safe architectures.

Application Programming realities
The flexibility of the software in the application programming environment becomes the final frontier in the implementation of SIS. Software flexibility allows the application programmer to represent the actual requirements of the process and its application. It also allows the programmer to compensate for the lack of embedded diagnostics of the system. Logic voters, tag compare logic, dual tag names, and redundancy tables are just a few examples of the challenges the programmer will face when building a diagnostic infrastructure.

Conclusions
Understand the target safety integrity level (SIL) of your application. Make sure to consider start up and unexpected shutdown scenarios, environmental impact, and economic impact.

Don’t compare apples and oranges, try to understand the benefits of each option, and define which option suits the requirements of your application better.

Don’t just consider the initial investment of the hardware. Also factor in the impact of maintenance, the cost of maintaining documentation, the cost of troubleshooting, and the impact of spurious trips on your plant performance.

If nuisance trips are important or scheduling maintenance for repair is an issue, do not select a dual logic system. Select a 2oo3 TMR system. On average, there might be a 10% higher initial

investment over dual systems but you can achieve a substantial increase in process uptime and reliability without sacrificing safety.

Select a logic solver vendor that has the appropriate TÜV Certification and approvals including application specific approval. Follow and understand the safety guidelines and restrictions of the system. Finally, make sure you understand the basic probability to failure on demand (PFD) calculations provided by the manufacturers you're evaluating.

References

A conceptual comparison
Bert Knegtering, Honeywell and Erik Dom, Borealis Polymers
Hydrocarbon Engineering, Dec 2003

The New Quad Architecture: Explanation and Evaluation
Lawrence V. Beckman, SafePlex Systems, Inc
Safety Users Group 2001

ISA-TR84.0.02 Technical Report
Safety Instrumented Functions (SIF) --Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations
Version 5 March 2002

Triconex Availability and Probability to Fail on Demand Calculations for Tricon and Trident Controllers
Velten-Phillipe and Shabe, TÜV
2003-02-03

Is The Risk Worth It?
Beware of the New Safety Instrumented Suppliers
Bob Adamski, Director, Premier Consulting Services

Truth 7 link: http://www.triconex.com/truth7/

Sponsored by Invensys Triconex