Life Is On | Schneider Electric

Is the risk worth it?

Beware of the new safety instrumented suppliers

by Farshad Hendi

Table of contents

Safety instrumented systems standards

The new ANSI/ISA S84.01 and international standard IEC-61508 have placed great emphasis on safety instrumented systems (SIS) for process industries. These new standards set requirements for performance (safety integrity level, or SIL), design, and maintenance. Furthermore, in the United States, these requirements are not optional and will be enforced by OSHA-PSM and EPA-RMP as good engineering practices.

Ambitious companies that see a tremendous potential for business as a result of these regulatory requirements seem to be coming out of the woodwork in an attempt to offer their products for compliance. Unfortunately, most of the "new" products offer solutions for the logic solver (microprocessors and input/output modules) of the SIS because this is where most of the revenue is. Therefore, those who manufacture electronic programmable devices normally used in noncritical control are hastily modifying their systems to be redundant in an attempt to meet availability requirements.

In the last eight years, we have seen more dual redundant logic systems introduced than in the past 20 years dating back to relay technology. Beware of the new kids on the block. They may be young and energetic, but they have no experience in the area of safety and reliability. If you have a safety, critical control, or equipment protection application, it is recommended to select a company with time-proven performance and experience, and whose only business and specialty is in these applications.

Even companies in the regulatory process control (DCS/BPCS) business are trying to get a piece of the action. After all, they already produce controllers, so why not just put two together and call it a safety system? The authors of the standards, in their wisdom, anticipated this approach and mandated separation of the DCS and the SIS. This separation requirement, however, has not stopped some DCS vendors from convincing clients they can reduce costs by single-sourcing hardware and combining safety system functionality with the BPCS. Combining DCS functionality with safety system applications in the same hardware/software is dangerous and prohibited by the standards. Exposing workers and the community to those risks is irresponsible and unacceptable.

An article written by Basil Balls and published in **InTech** magazine, "The Table Always Wins,"[1] discusses the risks of combining these functions. In Volume 30 of **ISA Transactions**,[2] a paper describes the evolution of safety systems from relay to hardwired solid state, PLCs, TMR, and fault-tolerant TMR technology. It describes in detail the issues surrounding the application of single and dual PLCs for safety systems. The paper also explains that redundancy is necessary in safety applications because of the undetected, unsafe failures of components in the SIS. Dual systems meet minimum safety requirements provided they are in a one-out-of-two (1oo2) voting logic configuration.

The reader is reminded that 1oo2 voting logic refers to two distinct conditions, both of which must be satisfied for safety applications:

- Any one out of the two channels can vote for a shutdown.
- If a fault is diagnosed in any one of the channels, a shutdown must occur.

The dual configuration appears to be safe, but it obviously will be the root cause of many false trips due to the normal and random failures that occur in all microprocessor-based systems. In fact, many companies in the process industry recognized this weakness in dual 1oo2 systems and funded projects for retrofit. Critical processes (e.g., ethylene plants, offshore production facilities, etc.) replaced dual systems with 2oo3 (TMR) because false trips were too expensive. In reality, most process industries will not tolerate nuisance trips to any degree of occurrence.

Some dual manufacturers responded by providing a configuration they called 1oo2D in an attempt to reduce the nuisance trip rate. The letter "D" supposedly stands for diagnostics, which is claimed to be 100 percent. Common sense and conventional wisdom dictate that 100-percent diagnostics is unachievable in any complex electronic system, including aerospace and nuclear. Third-party assessments commissioned by the IEC 61508 Committee show that the highest diagnostics that 1oo2D systems can achieve is 90 percent. Close examination of this architecture even by unsophisticated technologists will show that the system is really a 2oo2 voting system, not a 1oo2. In other words, when a component fails in one of the two channels, the system does not shut down but continues to operate with one channel until the fault location is detected and replaced. Single channel operation in safety systems is not recommended by most experts or safety system certifying bodies such as TÜV.[3] Furthermore, in an article titled "How Reliable Is Your Safety System," in the January 1992 issue of **Chemical Engineering**,[4] Lawrence V. Beckman states that, "The best policy is not to operate in the single, or '1' state for a long period of time." As mentioned above, single-channel operation is irresponsible, and exposes workers and the community to risks that are higher than those associated with driving, smoking, car racing, or rock climbing.

[1] Balls, Basil W. "The Table Always Wins," **InTech**, March 1988.
[2] Adamski, Robert S. "Evolution of Protective Systems in the Petrochemical Industry," **ISA Transactions**, Vol. 30, No. 4, 1991.
[3] Technischer Überwachungs-Verein Rheinland e.V., Technical Supervisory Association, (TÜV).
[4] Beckman, Lawrence V. "How Reliable is Your Safety System?," **Chemical Engineering**, January 1992.

Safety integrity levels

Safety integrity levels (SIL) can be understood this way: SIL and availability are simply statistical representations of the integrity of the SIS when a process demand occurs. The acceptance of an SIL 1 SIS means that the level of hazard or economic risk is sufficiently low that an SIS with a 10 percent chance of failure (90 percent availability) is acceptable. For example, consider the installation of an SIL 1 SIS for a high-level trip in a liquid tank. The availability of 90 percent would mean that out of every 10 times the level reached the high-level trip point there would be one predicted failure of the SIS and subsequent overflow of the tank. Is this an acceptable risk?

A qualitative view of SIL has slowly developed over the last few years as the concept of SIL has been adopted at many chemical and petrochemical plants. This qualitative view can be expressed in terms of the impact of the SIS failure on plant personnel and the public or community.

- "4" - Catastrophic community impact
- "3" - Employee and community protection
- "2" - Major property and production protection; possible injury to employee
- "1" - Minor property and production protection

The assignment of SIL is a corporate or company decision based on risk management philosophy and risk tolerance.

Table 1

Safety Integrity level

Safety integrity level			Availability required	Probability to fail on demand	Mean time between failures
IEC		4	> 99.99%	E-005 to < E-004	100,000 to 10,000
	ISA	3	99.90%	E-004 to < E-003	100,000 to 1,000
		2	99.00 – 99.90%	E-003 to < E-002	1,000 to 100
		1	90.00 – 99.00%	E-002 to < E-001	100 to 10

Technischer Überwachungsverein

TÜV stands for a rather long German name, Technischer Überwachungsverein Rheinland e.V. In short, it is the only independent third-party agency in the world that certifies SISs. TÜV Rheinland is approved and authorized by law as a technical inspectorate for a variety of technical systems, including safety engineering for industrial plants, process, and products during manufacturing and utilization. If the product is tested and meets the strict technical and performance requirements, it is approved and certified for Classes (AK) 1 – 7. This certification is required by most European countries and is being requested more frequently by other countries and the U.S. The manufacturer of the equipment is issued a certificate with a detailed report listing the results of the inspection and testing, and, most important, general and specific restrictions. It is these general and specific restrictions that most manufacturers are hesitant to reveal to the user of the equipment — and most times never do. We can see the correlation between safety integrity levels and TÜV Class in Table 2.

Table 2
SIL vs. TÜV Class (AK)

SIL	1		2	3		4
TÜV Class	AK2	AK3	AK4	AK5	AK6	AK7

As an example, if a process event occurred that could cause personal injury or affect the community (not catastrophic), the SIS designed to mitigate or prevent the hazard would be assigned an SIL "3." The TÜV Class certification for the logic system should be an AK5 or AK6 depending on the quantitative assessment. TÜV has certified many different voting architectures in logic solvers (e.g., 1oo2, 1oo2D, 1oo3, 2oo2, and 2oo3). Depending on the testing results and design, TÜV will certify and approve the logic solver for the appropriate Class of safety service 1 – 7.

As noted above, all approvals and certifications are contingent on operating the device within the general and specific restrictions. TÜV's general restrictions are very clear for all architectures and manufacturers: "The safety system shall never operate in the single channel mode for Class 5 and 6." Classes 1 – 4 also have restrictions and are summarized in Table 3.

Table 3
General and specific restrictions

Configuration	TÜV-approved operating mode with restrictions (see note 1)	TÜV Class approval for safety	Nuisance trip rate		TÜV time requirements for repair of logic solver (see Note 2)
			High	Low	
1oo2	2-0	AK5 AK6	✓		n/a
2oo2	Not approved	Not approved		✓	n/a
1oo2D	2-1-0	AK5	✓		72 hours (Note 2)
1oo2D	2-0	AK6	✓		(Notes 2 and 3)
1oo3	3-0	AK5 AK6	✓		n/a
2oo3	3-2-1-0	AK5 AK6		✓	1500 hours

Note 1: Faults that are detected and localized by the self-tests within one of two channels result in single-channel operation for a limited period of time. In single-channel mode, the system performs a similar set of self-tests. The self-test intervals in single-channel architecture do not differ from the self-test intervals in dual-channel operation. These self-test intervals shall be less than the process safety time.

Note 2: The maximum duration for single-channel operation depends on the specific process and must be specified individually for each application. The times indicated are maximum limits supported by the certification. AK5 = 72 hours. AK6 = Immediate shutdown (one hour in special cases; see Note 3 below). These times for single-channel operation are not allowed, however, for a miscompare of microprocessors, inputs, or outputs. If a miscompare occurs, the system must switch to a safe state (shutdown) immediately.

Note 3: As a general rule, single-channel operation is not envisioned for AK6. In some very rare system conditions, however, it is recognized that process shutdown itself is a potentially dangerous process or should follow a well-defined shutdown sequence. In this case, the reduction in the equipment safety levels resulting from short-term single-channel operation (degraded mode) during the shutdown sequence state should be offset by additional measures. For example, the process could be monitored and, if necessary, brought to a defined safe condition.

As seen from the above examples and tables, the purchaser of a safety instrumented system should be cautious in choosing a logic system vendor, especially if nuisance trips or time to repair are important to your plant. If, however, you have an informed selection process, you will meet the regulatory standards, be safe, avoid economic losses through high-availability systems, and have time to schedule repairs.

Our advice is to follow this simple checklist:

- Know what your SIL target is for the application.
- Select a corresponding TÜV classification.
- Select a logic solver vendor that has the appropriate TÜV certification and approvals.
- Carefully follow and understand the TÜV report and restrictions.
- Select a logic solver vendor that has the experience and reputation in safety and critical control.
- If nuisance trips are important, and/or maintenance scheduling for repair is an issue, do not select a dual (1oo2 or 1oo2D) logic system. Select a 2oo3 TMR system. On average, there is an initial 10- to 15-percent cost increase over dual systems, but you can achieve a 10,000-percent in reliability without sacrificing safety.
- Follow S84.01 and IEC 61508 standards and verify quantitatively that your entire SIS, including field sensors, logic solver, and final elements, meet the Probability to Fail on Demand (PFD) for the selected SIL. See Table 1.

If you follow this checklist, utilize the appropriate redundancy in the field sensors, and select a fault-tolerant TMR system, you will have made a sound decision that protects workers and the community. You can also calculate that the TMR solution cost you on average, one-half of one-tenth of 1 percent of capital build-out costs, and protect 25 – 50 percent of your operating assets.

References

Balls, Basil W. “The Table Always Wins”
InTech, March 1988

Adamski, Robert S. “Evolution of Protective Systems in the Petrochemical Industry”
ISA Transactions, Vol. 30, No. 4, 1991

Technischer Überwachungsverein Rheinland e.V.
Technical Supervisory Association, (TÜV)

Beckman, Lawrence V. “How Reliable Is Your Safety System?”
Chemical Engineering, January 1992

Standards/ regulations

“Programmable Electronic Systems in Safety Related Applications”
Health and Safety Executive, UK, 1987

ANSI/ISA-S84.01-1996 “Application of Safety Instrumented Systems for the Process Industries”
Instrument Society of America S84.01 Standard, Research Triangle Park, NC 27709, February 1996

29 CFR Part 1910, “Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents”
Occupational Safety and Health Administration, 1992

IEC-61508, “Functional Safety: Safety Related Systems”
International Electrotechnical Commission, Technical Committee No. 65, Draft/June 1995

Other references

Adamski, Robert S. “Design Critical Control or Emergency Shut Down Systems for Safety AND Reliability”
Automatizacion 96, Panamerican Automation Conference, Caracas, Venezuela, May 1996

Adamski, Robert S. “Status of SP-84 and How This Standard Will Affect Your Business”
50th Annual Symposium on Instrumentation for the Process Industries, Texas A&M University, 1995

Boykin, R.F. and Kazarians, M. “Apply Risk Analysis to Identify and Quantify Plant Hazards”
InTech, July 1986

Martel, Troy J. “Safety System Engineering”
International Symposium and Workshop on Safe Chemical Process Automation, Houston, Texas, 1994

About the author

(Farshad Hendi) Safety Industry Manager