IS THE RISK WORTH IT?
Beware of the New Safety Instrumented Suppliers

Author: Bob Adamski, Invensys Premier Consulting Services

WHAT’S INSIDE:
1. Safety Instrumented Systems (SIS) Standards
2. Safety Integrity Levels (SIL)
3. Tecnischer Überwachungs-Verein (TÜV)
4. References
1. SAFETY INSTRUMENTED SYSTEMS (SIS) STANDARDS

The new ANSI / ISA S84.01, and international standard IEC-61508 has placed great emphasis on safety instrumented systems (SIS) for the 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 who 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 non-critical control are hastily modifying their systems to be redundant in an attempt to meet availability requirements.

In the last three 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, 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 combine safety system functionality with the basic process control system. Combining DCS functionality with safety system applications in the same hardware/software is prohibited by the standards and dangerous. 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, 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 means two distinct conditions, both of which must be satisfied for safety applications:

- Any one out of the two channels can vote for a shut down.

- If a fault is diagnosed in any one of the channels, a shut down 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 industries 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%. Common sense and conventional wisdom dictates that 100% diagnostics is unachievable in any complex electronic system including aerospace and nuclear. Third party assessments commissioned by the IEC-61508 Committee in fact shows that the highest diagnostics 1oo2D systems can achieve is 90%. Close examination of this architecture even by unsophisticated technologists will show that the system is really a two out of two (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 and safety system certifying bodies such as “TÜV” (3). Furthermore, in Chemical Engineering January 1992 (4), the author, 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 driving, smoking, car racing, or rock climbing.

2. SAFETY INTEGRITY LEVELS (SIL)

Safety Integrity Levels (SIL) can be understood accordingly; SIL and availability are simply statistical representations of the integrity of the SIS when a process demand occurs. The acceptance of a SIL 1 SIS means that the level of hazard or economic risk is sufficiently low that a SIS with a 10% chance of failure (90% availability) is acceptable. For example, consider the installation of a SIL 1 SIS for a high level trip in a liquid tank. The availability of 90% would mean that out of every 10 times that 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?

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Availability Required</th>
<th>Probability to Fail on Demand</th>
<th>Mean Time Between Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC</td>
<td>4</td>
<td>&gt;99.99%</td>
<td>E-005 to &lt; E-004</td>
</tr>
<tr>
<td>ISA</td>
<td>3</td>
<td>99.90%</td>
<td>E-004 to &lt; E-003</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>99.00 - 99.90%</td>
<td>E-003 to &lt; E-002</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>90.00 - 99.00%</td>
<td>E-002 to &lt; E-001</td>
</tr>
</tbody>
</table>

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.
3. TECNISCHER ÜBERWACHUNGS-VEREIN (TÜV)

TÜV stands for a rather long German name, Technischer Überwachungs-Verein Rheinland e.V. In short, it is the only independent third party agency in the world that certifies safety instrumented systems (SIS). 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) 1-8. This certification is required by most European countries and is being requested more frequently by other world countries and US. 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 manufactures are hesitant and most times never reveal to the user of the equipment. We can see the correlation between safety integrity levels and TÜV Class in Table 2.

<table>
<thead>
<tr>
<th>SIL</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>TÜV Class</td>
<td>AK2</td>
<td>AK3</td>
<td>AK4</td>
<td>AK5</td>
</tr>
</tbody>
</table>

As an example, if a process event occurred that could cause personal injury or affect the community (not catastrophic), the safety instrumented system designed to mitigate or prevent the hazard, would be assigned a safety integrity level (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.” TÜVs General Restrictions are very clear for all architectures and manufactures. “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>
<thead>
<tr>
<th>Configuration</th>
<th>TÜV Approved Operating Mode w/Restrictions* (see Note 1)</th>
<th>TÜV Class Approval for Safety</th>
<th>Nuisance Trip Rate</th>
<th>TÜV Time Requirements for Repair of Logic Solver (see Note 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1oo2</td>
<td>2-0</td>
<td></td>
<td>AK 5 AK6</td>
<td>√</td>
</tr>
<tr>
<td>2oo2</td>
<td>Not Approved</td>
<td>Not Approved</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>1oo2D</td>
<td>2-1-0</td>
<td></td>
<td>AK5</td>
<td>√</td>
</tr>
<tr>
<td>1oo3</td>
<td>2-0</td>
<td></td>
<td>AK6</td>
<td>√</td>
</tr>
<tr>
<td>2oo3</td>
<td>3-2-1-0</td>
<td></td>
<td>AK5 AK6</td>
<td>√</td>
</tr>
</tbody>
</table>

Note 1: Faults which 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 does not differ from the self-test intervals in dual channel operation. These self-test intervals shall be less than the process safety time.
IS THE RISK WORTH IT?
Beware of the New Safety Instrumented Suppliers

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 shut down. (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 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 safety integrity level (SIL 1-4) target is for the application.
- Select a corresponding TÜV classification. 1-7.
- 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 10-15% cost increase over dual systems but you can achieve a 10,000% increase 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, ½ of 1/10 of 1% of capital build out costs, and protect 25-50% of your operating assets.

4. REFERENCES

IS THE RISK WORTH IT?
Beware of the New Safety Instrumented Suppliers

STANDARDS / REGULATIONS:


OTHER REFERENCES:


