

When a SIL Rating is not Enough

Robin McCrea-Steele, TÜV FSExp
Invensys-Premier Consulting Services
www.premier-fs.com

A common misconception is that the SIL claim limit of a safety PLC is the main, or sometimes the only, criteria for selection in a process safety application.

Although it is true that the SIL rating is a measure of the risk reduction capability and probability of failure on demand, it only measures the “Fail Safe” nature of the device.

There is no doubt that a plant that is “shut down” is relatively safe. However, apart from the economical / quality / lost production and other negative implications, it is important to consider the higher risks associated with an unplanned shutdown and subsequent re-start of the process.

So the question begs, what measures the process up-time capability of a subsystem? The answer is certainly not in the safety standards or in the classic third party certifications. In fact, with today’s technology, it is not too difficult to design a “fail safe” PLC with a SIL3 certification. The challenge begins when process up-time is a simultaneous requirement.

MTTF_{spurious} rates may not be critical in a discrete manufacturing plant where a light curtain protects an operator at a punching press, but they are extremely critical in a process plant.

Dual PLC’s in a 1oo2 configuration were the initial solution of choice for “fail safe” applications. Subsequent variations of dual systems were developed (1oo2D , 1oo2DR, 2oo4D) in an attempt to minimize the false trips inherent with the limited hardware available (a man with two watches never knows the time).

Industry soon found out the limitations in self diagnostic coverage of microprocessors and now rely on the strength of comparative diagnostics between the channels. The limitations of diagnostics then reached a second limit, but the bottom line is that on any undiagnosed miscompare between channels the system must shutdown spuriously. There is so much you can do with 1oo2D or 2oo4D dual systems. They are “fail safe”, mind you, but have an unreasonable tendency to fail spuriously.

On the other hand, fault tolerance and process up-time are both inherent in TMR technology. The military and aerospace industry have used triplicated systems for decades. What Triconex successfully accomplished is optimize this technology for implementation in process plants. By combining the power of 2oo3 majority voting with the strength of self and comparative diagnostics, Triconex 2oo3D systems have maintained the leadership in process safety and process up-time for over 20 years. The same Triconex 2oo3D PLC has been approved for 1E critical safety applications in the nuclear industry.

It is interesting to note that although Triconex TMR systems have received certification to a SIL3 claim limit, 86 % of Triconex applications in the process industry are being used in SIL1 and SIL2 SIFs’. Triconex TMR is SIL neutral, or in other words, used in any safety integrity level 1 though 3 safety instrumented functions.

Another misconception is that a SIL3 safety PLC is an overkill for a plant that has no SIL3 SIFs'. Safety practitioners recognize that there is an "accumulated" residual risk associated with an SIS that has a safety PLC shared between a number of SIFs' (Safety instrumented functions). Although safety standards' target measures do not consider overlapping risks, experts in this field recommend increasing the safety requirements of the common subcomponents shared by more than one SIF (i.e. ESD valves as well as safety PLCs'). Even process applications with all SIL1 and SIL2 SIFs' are better served with a SIL3 certified PLC, for the above reasons.

Regarding the field instrumentation associated with a safety PLC, it is important to note that the redundancy is not dictated by the PLC technology. Some may believe that a dual PLC requires dual redundant transmitters and that a TMR PLC requires triplicated transmitters. There is absolutely no correlation. The field redundancy is defined by the SIL of the SIF and not by the PLC technology. A certain SIF could require single, dual or triplicated transmitters, irrespective of the PLC technology being 1oo2D, 2oo4D or 2oo3D.

Conclusions:

When selecting a safety PLC for a process industry application, take in to consideration more than just the SIL certification and initial price.

- 1- Consider a manufacturer with a certification by TÜV Rheinland, as the recognized Functional Safety center of excellence.
- 2- Select a safety PLC with a SIL3 claim limit, even if you have few or no SIL 3 SIFs'. Remember that the safety PLC is shared by many SIFs' with overlapping associated hazard risks. SIL1 and SIL2 safety instrumented functions sharing a safety logic solver are better served by a higher integrity safety PLC.
- 3- Weigh in highly the $MTTF_{spurious}$ rate. Process up-time is critical not only for economical reasons, but also for safety. Consider the lifecycle cost of ownership by reduced spurious trips, avoidance of lost production, limited damage and/or stress to process equipment.
- 4- Verify the manufacturer's safety track record and make sure there is a substantial installed base over a broad period of time, in order to draw your own conclusions. Trust, but verify!
