

## **ICA 2008 “Achieving Superior Plant Design & Performance through Functional Safety”**

IEC61508 Functional Safety standard [1] was first released a decade ago in 1998. Following that, the sector specific IEC61511 [2] for process industry was released. Since then, Process Plant Operators both onshore and offshore have demanded that engineering consultants, instrument and control equipment suppliers comply to the Safety Lifecycle model from cradle to grave. Equipment Suppliers and Vendors have also jumped onto the band wagon to design and manufacture their equipments with TUV certification according to the IEC61508 and IEC61511.

As the process industry continues to pursue safer processing operations, there is constant ‘struggle’ to optimize the cost of implementation of Safety PLC for SIS while keeping hazardous incidents at bay. Does having SIS (Safety Instrumented System) designed to IEC6108/61511 standards run counter to the objectives of increasing process output performance and profitability? Just as the aviation industry has made air travel possible and thus created an industry and lifestyle that modern mankind cannot do without, all these while safety is of the utmost importance way even before the airplane hits the runway. Therefore before a process plant earn its license to operate, it has to contain risk to a tolerable level. With good working knowledge of functional safety according to the standards, process plants including offshore rigs can attain higher level of safety and at the same time, achieve overall safer plant design and superior performance. That implies that before one can apply the standards effectively, one should be aware of some pre-requisites of implementing SIS in compliance to IEC61508 & IEC61511.

These pre-requisites are the corner stone to an effective application of the standards:

1. To have a good understanding of the Functional Safety Standards and its implications. Functional Safety Standard has brought up some debatable questions as it answers most. One of the main reasons is because it is a performance based standard as opposed to a prescriptive one such as API 14C or NFPA85, thus the onus lies heavily on the operator and designers alike to ensure the target safety integrity level is achieved and not compromised.
2. To know that SIL (Safety Integrity Level) Verification and Calculation of an SIF is actually based on average PFD (Probability of Failure on Demand) within a given mission time, i.e. plant turn-around or till the next proof testing interval. Just to be on the safe side, an inexperienced engineer may have the tendency to specify SIL 3 for an SIS without any SIF (Safety Instrumented Function) identification or SIL assignment. Another problem in calculation is that some failure data may not be available for certain components. Where operating plants has historical records, it is highly recommended to use those data. Systematic failures are also not included in the PFD calculations, these may include software, design reviews and checks, sizing of resistor to the less obvious poor solder due to flawed process or solder flux.
3. Use of TUV or third party certified component/equipment. Safety PLCs are widely used for SIS application since the early 90’s with TUV certification. Following suit, some field devices such as transmitters, I.S. barriers even some valves have third party certifications. Ideally the use TUV certified or Third party certified equipments or component should simplify the design but quite often some may not have TUV certification although it may have been in use for several years

without known problems. It is not part of the normative standard to have such certification but proving SIL may become more difficult without one. Where is none, “proven in use” concept is allowed in the standard thus offering some relief and consolation.

4. Knowing what we know and knowing what we don't know. Given a component or subsystem has been certified by TUV, the implementation according to the Safety Manual has to be strongly stressed and is highly critical as it describes the basis for application and condition in which TUV has issued certification. Apart from the TUV certification, it is imperative to know what the working parameters and assumptions are, bearing in mind not all component or subsystem has been certified by TUV. These are the questions to ask:
  - a. Beta factor – common cause failure
  - b. Fail modes for UPS (Uninterruptible Power Supply), Power supply unit failure mode – assumed as 100% fail-safe (Safe Failure Fraction, SFF =1). An example of failure of power supply unit: its fan coil may burn out and the power source is still good but ambience temperature is rising that may affect surrounding electronics.
  - c. Spurious trip is safe? Think again.
  - d. All alarms can be managed by the operator. Shower of alarms especially during emergency situations have been known to adversely affect operator response.
  - e. TUV approved equipment means it is safe to be used. Reading the fine prints and the safety manual can at time reveal unpleasant surprises.

Having highlighted the pre-requisites in order to successfully implement an SIS, now the benefits that could be reaped resulting in safer Plant Design and increased Performance:

#### **Identification of bad actors by means of sensitivity analysis.**

Knowing the weak links enable the designer to improve the SIL by focusing on the problem areas. To secure a door, one might be attempted to put many locks and latches on the door but then have a weak door hinge that can be pry open easily. To achieve a target SIL, calculation of all subsystems that contributes to the success or failure in this case, will have to be performed with failure rate data for a given time period. Typically, subsystems consist of sensors, logic solver, final elements, isolators or barriers where applicable. From this calculation, one could easily identify which is a largest contributor of undetected dangerous failure and do something about it. That means, where it does not meet SIL, then where to improve. Where SIL is met, then is it over-design and can a component be removed. Loop by loop, all SIFs can be assessed on the same basis and thus the overall SIS can be verified to ensure SIL is met with the fit for purpose design. Fit for purpose design ensures optimum allocation of resources thus resulting in minimal wastage.

#### **Apply LOPA and SIF identification to avoid preconceive SIS requirement too much too soon**

While LOPA is only an informative part of the standard, it is a very useful tool involving a team consisting of operator with experience operating the process under consideration, manufacturing management, process control engineer, instrument/electrical maintenance person with experience in the process under

consideration and a risk analysis consultant. The result is a multi-disciplinary and cross-functional analysis on all independent layers of protection to achieve risk reduction to a tolerable risk level. (Note that risk cannot be eliminated altogether, it can only be reduced). Once, again this exercise prevents costlier investments on SIS where it might be eliminated using other layers of protection, or an SIS becomes smaller having reduce the number of SIFs with lower target SIL each.

### **Fit for purpose Safety PLC-based SIS design**

Without SIL verification and identification of bad actors, it will be almost impossible to have fit for purpose design. Cost of SIS implementation can be reduced by not over designing and not having unnecessary redundancy. Upon the identification of SIFs and its respective SIL targets, each subsystem can be designed and reviewed by considering the following:

1. Redundancy requirements with “architectural constraints”, a term define in the standard to set minimum hardware fault tolerance (redundancy) based on SFF achieved. Voting configuration or logic of redundant component to meet architectural constraints criteria and invariably to achieve fault tolerance. Fail-safe design is usually the result of limitation in providing a reliable means of continued operation without compromising safety. So to both is Fail-safe vs. fault tolerant is possible, then loss production is enough reason to justify going for fault tolerance. Most if not all single points of failure even it if is fail-safe, should be eliminated if higher process uptime is desired.
2. Improved overall system maintainability – better diagnostics, shorter troubleshooting time. With more intelligence built into SIS for self-testing and real-time data quality checks, more equipment or system faults could be detected faster and more accurately. This translates into lower maintenance cost and lower risk hazard exposure during degraded state of any SIF. Pre-determined proof testing interval for each SIF based on SIL verification calculation can be a more educated schedule rather than legacy periodic checks. Longer periods between proof testing results again in lower maintenance cost. Some solenoid valves have partial stroke capability which could extend proof-testing interval even further. However, striking a balance is always key because adding more components into a system also increased the numbers of parts that would fail. At the same time, such technology comes at a price due to upfront investment and the cost of training and keeping technicians or engineers to maintain more complex systems.
3. Reduce spurious trips. A well designed SIS should also take into consideration the need to reduce spurious trip which would then lead to increase higher plant throughput performance. While theoretical calculation assumes that spurious trips are the result of failing safely, an operator would remind us that process shutdown and start-up are the more hazardous as compared to steady state operation. To draw a parallel again with airplanes, “please fasten your seat belt” whenever the plane is taking off or landing.

### **Prevention of incidents**

The single most important objective of SIS is to protection the plant assets, human lives and the environment. Failure to do so can result in catastrophic accident involving heavy casualties, loss of producing assets and pollution of the environment. With these standards, a largely quantitative approach has been adopted and it provides greater

peace of mind by not simply leaving things to chance. Now safer operating plants are also better design and higher performing plants.

[1] IEC61508-1, "Functional safety of electrical/electronic/programmable electronic safety related systems - Part 1: General requirements," IEC 1998.

[2] IEC61511-1, "Functional safety - Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements," International Electrotechnical Commission (IEC) 2003.

### **Professional Biography (Speaker's Background)**

**David Ong** is the founder and Managing Director of Excel Marco, a functional safety consultant and a safety & control systems solutions provider. He has over 19 years of experience and is widely recognized in process safety industry. He is a CFSE (Certified Functional Safety Expert) and also a member of the CFSE Governance Board. During the course of his career, he has executed various major projects both onshore and offshore on Process Automation Safety & Control. Having involved with several major projects for companies such as ExxonMobil, Shell, SBM, Modec, and Total, he is well versed with industrial standards and practices. He is also actively involved in promoting Functional Safety training and education by providing CFSE certified courses in partnership with exida.com.

Contact: [david.ong@excelmarco.com](mailto:david.ong@excelmarco.com)  
[www.excelmarco.com](http://www.excelmarco.com)