Why a run-to-fail strategy is not good practice for SIS?

Keyur G. Vora
Engineering Design Head (Control & Instrumentation) - RPMG Reliance Industries Limited, INDIA

*E-mail: keyurvora2363@gmail.com

Abstract. The Maintenance & Reliability engineers understand pain area that the portion before the “flat” part of the “Bathtub” is where a high number of premature failures can occur: commonly referred to as “infant mortality”. One of the fundamentals of the Probability of Failure on Demand (PFD$_{avg}$) calculations in SIL verification analysis, is the concept of a constant failure-rate during useful life of the equipment. Probabilistic calculations assume that the failure rate of the devices used in a Safety Instrumented System (SIS) remains constant during the “flat” (constant failure rate) portion of the “bathtub” curve. Most manufacturers will perform stringent testing to weed-out, weaker units that could fail prematurely, leading to unwanted warranty claims. When equipment reaches to flat portion of it’s lifetime called as “wear-out” phase then the failures start to rise dramatically & then the integrity of the Safety Instrumented Functions (SIF) is compromised. During the Operation and Maintenance phase of the SIS, periodic performance assessments need to be made in order to ensure the as-designed, installed and commission SIS and its SIFs, still meet the performance requirements of the Safety Requirement Specification (SRS) [1]. Using a run-to-fail strategy will not enable the SIFs to meet the performance requirements once wear-out occurs. This paper will explain why a run-to-fail strategy is not good practice for a SIS, which will lead to the de-graded performance of the SIFs. This paper addresses both the design and operational impacts of a run-to-fail strategy.

1. Introduction
Over the past decade or so, automation has been one of the dominant factors in enabling end users in the process, chemical and petro chemical industries to be able to streamline their costs and improve efficiency; often at the expense of personnel. Most modern plants today have less man power than plants of 1980 and even the 1990s. This means that the burden of running and maintaining a modern plant has fallen on fewer and fewer plant personnel. Coupled with the shortage of skilled employees, this places a significant burden on plant personnel to maintain and improve their skill set in order to maintain the technologically more complex instrumentation and automation systems. Aside from the Basic Process Control System (BPCS), there’s the plant safety system (referred to as the Safety Instrumented System (SIS)).

The advent of the IEC 61511 [2] & ANSI/ISA 84.91.01 [3] standards for the process industries has provided a path to improvements in safety by introducing the concept of a Safety Lifecycle (SLC) and moving away from a strictly prescriptive methodology to a more performance based methodology, with the emphasis being placed on reducing risk and mitigating the potential for hazards that could lead to the loss of life, destruction of property and plant assets. The purpose of this paper is not to define the
application of the standard but to examine one of the most common errors made by operations and maintenance: having a run-to-failure policy for the SIS equipment. The tools such as ProSET, as exSILentia [4] streamlines the Process Safety Management work process and the Safety Instrumented System Functional Safety Lifecycle.

2. The nature of field equipment
Reliability Engineers know that most devices, either commercial or consumer-based, follow what is commonly known as the “Bathtub Curve”. The figure 1 below illustrates an example of the bathtub curve that demonstrates the typical behaviour of control system operating time interval (in hrs) over life time.

![Figure 1. Example of Failures Over Time of 30 Units.](image)

The blue line indicates the average middle value of failures and it can be seen that this “flat” portion of the curve has a constant failure rate over the average. The blue line indicates the average middle value of failures and it can be seen that this “flat” portion of the curve has a constant failure rate over the average.

2.1. The importance of the bathtub curve
Most manufacturers recognise the problems with premature failures and so will devise stress tests to expose the weaker units, causing them to fail. Examples of such tests are: Temperature cycling, Shock and vibration, Humidity, EMI/RFI etc. This will avoid weaker units getting out into circulation and presenting warranty failures for the manufacturers. The Bathtub Curve is important because it identifies two key areas:

- Infant Mortality
- Wear Out

Infant Mortality refers to the first part of the curve where a high level of failures can occur prematurely. Conversely, at the back-end of the Bathtub we can see a sharp rise in failures. This portion of the curve is known as “Wear Out”. At some point there is a sudden increase in failures as the normal operational stresses overcome the strength of the device, which then leads to failure. This portion is known as wear out and is very important for a number of reasons. After “useful life”, equipment/component must be checked, repaired or replaced or refurbished.

2.2. Probabilistic calculations: come basic details
For SIS, the primary concern is a failure on demand of any of its associated SIFs. A SIF has a defined Safety Integrity Level (SIL), which defines how much Risk Reduction the SIF will provide for a given hazard. For the application of layers of protection analysis (LOPA) technique [5], the semi quantitative method is applied for the events involving significant risk where analysis of barrier effectiveness & gaps is critical for risk management. The Safety Lifecycle is specifically geared towards ensuring that the SIS
and its SIFs will be available to perform its intended function and to provide the given level of Risk Reduction required. If a SIF fails, then this could lead to an undesirable outcome (an Accident).

2.2.1. Probability of an accident
If a hazard occurs and the automatic protection function operates correctly, no accident occurs. However, if a hazard occurs and the automatic protection function fails to operate, an accident occur. So, obviously, it is important that we know the probability of failure for an automatic protection function.

\[ P(\text{Hazard}) \times PFD \text{ of SIF} = P(\text{Accident}) \]  
(1)

2.2.2. How a SIF achieves its SIL
From the detailed design of the SIS and its SIFs, a SIL verification calculation is performed to ensure the SIF will meet its target SIL. For process industry applications, SIFs normally operate in Low Demand Mode and there are three design barriers that need to be met before a SIF will achieve its target SIL:

(a)\(PFD_{\text{avg}}\) – a measure of the defence against random hardware failures.
(b)Architecture Constraints – imposes minimum hardware redundancy requirements
(c)Systematic Capability - to show sufficient defense against systematic failures within the equipment chosen for the safety application.

If any one of the three barriers are not met, then the SIF will fail to meet its target SIL. IEC 61511 [2] requires that equipment selection be justified. Two alternative means are allowed, IEC 61508 compliance and Prior Use. The first requirement is to therefore meet the target \(PFD_{\text{avg}}\) for the SIF, which includes all the equipment: Therefore, in order, to calculate the overall \(PFD_{\text{avg}}\), we must first calculate the individual \(PFD_{\text{avg}}\) for each piece of equipment for the SIF and sum them together:

\[ PFD_{\text{avg}}(\text{SIF}) = PFD_{\text{avg}}(\text{Sensors}) + PFD_{\text{avg}}(\text{Logic Solver}) + PFD_{\text{avg}}(\text{Final Element}) \]  
(2)

We must also consider any interfaces and/or signal conditioning as well, since the failure rates of these components will contribute to the overall \(PFD_{\text{avg}}\) result. Taking the simplified formula,

\[ PFD_{\text{avg}} = \lambda dTI \]  
(3)

where: \(\lambda\) = Dangerous Failure Rate, TI = Proof Test Interval.

This formula assumes perfect Proof Testing (i.e. where any dangerous undetected faults are revealed and fixed before the SIF Demand occurs). The \(PFD_{\text{avg}}\) of the SIF will deteriorate over time due to imperfect proof testing. If the equipment is maintained on a run-to-fail basis, then once the Useful Life has been exceeded the \(PFD_{\text{avg}}\) is no longer valid because the premise of Constant Failure rate is not applicable. Beyond Useful Life the SIF will move into the “Wear Out” phase of the Bathtub. Understanding this and building in the Useful Life into a plant’s mechanical integrity program is key to ensuring the ongoing integrity of the SIS and its SIFs.

3. SIL validation/operation & maintenance/modification/de-commissioning
After SIS installation, SIS validation is done to validate that the installed and mechanically completed, SIS and its associated safety instrumented functions, meets the requirements as stated in the Safety Requirements Specification. The objective of SIS Operation & Maintenance is to describe how the SIS shall be operated and maintained to ensure that it functions in accordance with the Safety Requirements Specification, throughout the SIS operational lifetime. All activities concerning operation of the SIS shall be performed by competent personnel. Operators shall have the proper competence and training on the function and operation of the SIS and should undergo regular assessments, as part of the ongoing competency requirements.

A maintenance program shall be available, which includes descriptions for maintaining and testing the SIS, to maintain the required integrity level. The maintenance routines should also describe compensatory measures required (if any) for the testing to reveal faults that are not automatically detected by the SIS diagnostics. In general, it is not allowed to operate with impaired barriers. Necessary actions to correct or compensate the impaired barrier(s) shall be taken upon overrides & failures and the repair and restore times should be in accordance with the SRS [1]. It is important to
record the repair and restore times since this should be a key metric for measuring performance. In order to ensure that the SIS is performing in accordance with the design intent and hence the required integrity level, it is necessary to record non-conformance between the expected behaviour and actual behaviour of the SIS. This will also include ensuring replacement of devices that have reached the end of useful life. This shall be analysed and where necessary, a safety analysis performed and corrective action taken, via management of change procedures and updates to the SRS [1], if required.

It is important that the person responsible for the SIS is able to easily extract functional test documentation and installation trip and shutdown reports. The carrying out of audits and statistical analysis on these data are essential to ensure that the SIS is performing and being maintained as intended, and to ensure that the installation is being operated at an acceptable risk level. The assurance that planned testing is carried out on time and as specified, and that any backlogs are investigated and corrective actions taken, is vital for ensuring the performance of the SIS.

While doing SIS modification, it shall be ensured that modifications to any safety instrumented system are properly planned; reviewed and approved prior to making the change & to ensure that the required safety integrity of the SIS is maintained due to any changes made to the SIS. Personnel affected by the change shall be informed and trained prior to implementation of the change or start-up of the process, as appropriate.

SIS de-commissioning is to ensure that prior to decommissioning any SIS from active service, a proper review is conducted and required authorisation is obtained. It is to ensure that the safety instrumented functions remain appropriate during decommissioning activities. Management of change procedures shall be implemented for all decommissioning activities. The impact of SIS decommissioning on adjacent operating units and facilities or other field services shall be evaluated prior to decommissioning.

4. Challenges & issues after SIF installation in the field
The Final Commissioning and Start-up Phase starts when systems or parts of systems are mechanically completed (pre-commissioning), and is concluded when all systems are handed over to operations and finally accepted by the customer. The Operational Phase starts when the installation is handed over and accepted by operations. The De-Commissioning Phase starts with the decision to shut down the field and remove the installation. Even though, the IEC standards & guidelines clearly specify how to address work after mechanical installation of SIS, the following are the major issues, which can cause reliability concerns, safety issues & non-compliance to standards & codes after mechanical completion of SIF and handing over to operations.

a) Incomplete/Non-availability of Safety Requirement Specification (SRS) [1], resulting in non-availability of critical parameters including process safety response time.

b) Time availability after mechanical completion & before plant start-up/commissioning.

c) Non-availability of certified personnel to carryout SIL validation and subsequent phases

d) Run-to-fail of SIS equipment

e) Risk & fear of operating staff to carryout live SIF loop testing

f) Shutdown availability to carryout SIF test.

g) Implementation of Modification in SIS after mechanical completion & SIL validation

h) Handling of Software upgrades

Above issues are to be addressed during planning stage of SIL study. The SRS [1] document is very important and shall contain three main types of requirements:

1) Functional requirements and response times of SIF

2) Integrity requirements like PFDavg and SIL

3) Operating prerequisites and constraints

Time availability of SIF mechanical installation shall be kept to carryout SIL validation activities by a competent, independent, authority/auditor team who was not involved in this activity. It is a good idea to carryout SIL validation activities immediately after mechanical completion and before plant start-up, during the commissioning stage. Proper format for SIF proof testing shall be developed that
captures the SIL validation requirement. Later, it will be challenging to carryout SIL validation, as the plant is already started. The operation team will perceive this activity as a risk after plant start-up as any operational upset or trip of the plant/unit can result in production / profit loss & safety / reliability issues. Good planning & adherence to standards/codes, documentation/procedures will eliminate other issues as described above from (c) to (h).

5. Summary
The paper has highlighted the importance of understanding Useful Life, as demonstrated by the bath tub curve for SIF components, from which it can be clearly seen that the PFDavg of the SIF will deteriorate over time due to imperfect proof testing. If the equipment is maintained on a “run-to-fail” basis, then once the Useful Life has been exceeded the PFDavg is no longer valid.

Beyond Useful Life the SIF will move into the “Wear Out” phase of the Bathtub. Understanding this and building in the Useful Life into a plant’s mechanical integrity program is key to ensuring the ongoing integrity of the SIS and its SIFs. Replacement of devices within the SIF that have reached the end of its useful life needs to be built in to any mechanical integrity program. As inconvenient as this may seem, this paper has illustrated that SIL integrity is compromised once the end of useful life of the SIF equipment has been reached.

Therefore, it is important to carryout good planning & execution of SIS maintenance at every phase of the project. The non-compliance to any phase or Run to Fail strategy may result in unplanned failures, Safety & Reliability issues, company’s downtime and profit loss, safety and/or statutory/regulatory issues.

References
[1] Safety Requirement Specification (SRS) guidelines of IEC 61511 Standard for a Safety Instrumented System (SIS) that incorporates all the analysis done during the Risk Assessment, HAZOP/PHA and LOPA reviews. Visit https://www.sp.se/sv/index/services/functionalsafety/Documents/Safety%20requirements%20specification%20guideline.pdf
[2] IEC 61511-1 International Electro technical Commission (IEC) 61511-1 Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements:2016 edition
[3] ANSI/ISA 84.91.01-2012] American National Standards Institute ANSI/ISA 84.91.01-2012 – Identification and Mechanical Integrity of Safety Controls, Alarms and Interlocks in the Process Industry
[4] ProSET & exSILentia software tools
[5] “Layer of Protection Analysis (LOPA)– Simplified Process Risk Assessment”, CCPS 2001