MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

75th Annual Instrumentation and Automation Symposium
For the Process Industries
January 21-23, 2020 | College Station, Texas

Methodologies in Reducing Systematic Failures of Wired IPLs

aeSolutions Technical Team
aeSolutions
Greenville, SC

Tab Vestal
Eastman
Kingsport, TN
tvestal@eastman.com

Abstract

The history of high consequence incidents in industry reveals that most accidents were the result of systematic failures, not hardware failures. However, a higher degree of focus in engineering is often on the quantifiable failures of hardware. Process Safety risk gaps are often closed or reduced by several types of Independent Protective Layers (IPLs). Two common types are Safety Instrumented Functions (SIFs) and Basic Process Control System (BPCS) functions. The SIFs typically reside within a SIL-rated programmable logic controller, and their achieved quantitative performance is calculated based on random hardware failures of the SIF hardware components. Conversely, BPCS protective layers are assigned generic industry-accepted probability of failure credits. The BPCS generic industry-accepted probabilities of failure are conservatively assigned and consider unquantifiable human-induced systematic failures.

In either case, the likelihood of systematic failures can be reduced by recognizing design, specification, maintenance, and operations activities that are potential sources, and applying measures to prevent or reduce them. By reducing systematic failures, you reduce the risk in the industrial process and increase confidence in meeting the intended integrity requirements. This technical paper will discuss the common sources of systematic failures and preventative or mitigative measures to prevent their occurrence.

Keywords: Systematic failure, random hardware failure, Independent Protective Layer, IPL, SIF, SIS, BPCS, common cause, Human Factor Analysis, SIL Verification

INTRODUCTION

Since its inception in 1996, ISA-S84.01 and its subsequent standards (IEC 61511:2004-Mod and the most recent version of IEC 61511 v2.0:2016 - also accepted and published in 2018 as ISA 61511) have been widely adopted by industry as the performance-based foundation of risk-based process safety. In 2003, IEC 61511 was developed as the Safety Instrumented Systems specifically for the process industry sector, under the parent standard IEC 61508. Conformance to the standards has been considered and confirmed by the US Occupational Health and Safety Association (OSHA) as "recognized and generally accepted as good engineering practice" (RAGAGEP). From ISA 84 and IEC 61511, the engineering discipline of Safety Instrumented Systems Engineering has emerged. This most recently formed discipline of conceptual project and plant engineering (in contrast to detailed design engineering that follows) has grown from a very specialized engineering field to a more commonly practiced discipline. The various forms of risk assessment, most predominantly in the form of Layer of Protection Analysis (LOPA) and Quantitative Risk Analysis (QRA) have evolved from the traditional hazard classification and safeguard application methods such as Process Hazard Analysis (PHA) and Hazard and Operability Analysis (HAZOP). From these risk assessments, the performance targets of Risk Reduction Factor (RRF) and Safety Integrity Level (SIL) are derived.

Risk assessment can be qualitative, quantitative, or semi-quantitative. Risk Matrices and risk graphs are qualitative, whereas QRA is typically a detailed mathematical (quantitative) analysis of hazard scenarios. LOPA meets middle ground as semi-quantitative, as it applies a combination of initiating event frequencies, conditional modifiers, and protective layers usually in orders-of-magnitude. From these assessments, numerous initiating events, including Basic Process Control System (BPCS) are defined, and Independent Protective Layers (IPLs) are credited to hazard scenarios, using industry-accepted rulesets. In order to further close risk gaps, Safety Instrumented Functions (SIF, which are also IPLs) are assigned, and conceptually defined. Their integrity targets are predominantly semi-quantitatively derived. The SIF general structures and their RRF and SIL targets are the feedstock to SIS Engineering. SIS Engineering then produces the SIL verification calculations, Safety Requirement Specifications (SRS), and additional documentation to meet the Safety Lifecycle requirements defined in IEC 61511.

The explanation above is to reiterate that the protective layers, including SIFs, their targets, and the verification calculations are mathematically-applied and derived. The Process Safety professionals, most especially SIS Engineers, are immersed in SIL verification calculations that involve random hardware failure rates, diagnostic credits, proof test intervals, common cause, and a variety of parameters thereof. The objective of this technical paper is to examine a more predominant factor usually overlooked that gets lost in the math and immersion of IEC 61511 documentation and focus: Systematic failures – and how we as SIS professionals, integrators, manufacturers, and end-users can make efforts to minimize and in some cases, prevent their occurrence.

Systematic failures come in many forms, and there is one common element: Humans. Human oversights, lapses, errors, mistakes, and decisions. Anyone reading this document is prone for error and has made errors. Often, we are immersed in the details, and have an excellent understanding of the subject matter, but are involved as one of many team members, as contractors, subcontractors, or as end-users. The systematic failure can be bigger than any of the parts, such as organizational structure causes of systematic failure. Or the systematic failure can be as granular as not removing a sensor or final element bypass after testing. Competence of practitioners in all phases of the Safety Lifecycle is essential. The authors of this publication have witnessed firsthand (or learned from others' unfortunate experiences) the results of systematic failures at various levels. Other compelling examples that we learn from came at the cost of loss of life and/or environmental impact.

This paper does not cover Human Factors and quantitative approaches to model them into the overall hazard scenarios. It is however focused on minimizing systematic failures of BPCS IPLs and SIFs (collectively, "wired" IPLs) based on over 55 years of combined experience in plant operations, plant and process engineering, process control design, configuration, risk assessment, E&I maintenance and SIS Engineering. With this experience, lessons have been learned, and weak spots in our various practices have been identified and corrected. Systematic failures are often covert until a deviation, significant cost, near-miss, or incident opens an investigation as to the root cause(s). Although we can be engaged in activities, performing our jobs well, we can be a smaller part of a larger systematic failure. Our mission is to increase the awareness of systematic failures, help the reader identify their potential occurrences, and take corrective action. And in doing so prevent hazardous incidents.

SYSTEMATIC FAILURES vs. RANDOM HARDWARE FAILURES

Random failures are hardware failures. According to IEC 61511:2016, clause 3.2.59, they are failures "occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware." Although they occur randomly, their probability of occurrence can be quantified through the testing of a sufficient quantity of devices over an appropriate time period. The probability of the occurrence of a random failure is related to only the failure rate and time. "A systematic failure can be eliminated after being detected while random hardware failures cannot." (IEC 61511:2016, clause 3.2.59)

Systematic failures are not necessarily related to component wear, but are related to the systems under which SIFs and the components that comprise them are developed. Human errors, resulting in faults, lead to systematic failures. Rather than occurring randomly, a classic systematic failure would occur reliably under the same conditions (100% probability). Of course, no one would design a system with a fault that they knew would result in a failure.

There is some disagreement concerning the exact definition of a systematic failure; thus, it is instructive to examine definitions from the guiding standards. IEC 61511:2016, defines a systematic failure is a "Failure related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors." (Clause 3.2.81) This leads one to believe that a systematic failure will always occur under the right conditions, thus can be potentially revealed by appropriate testing and eliminated. Notes

4 and 5 in Clause 3.2.81 provides "examples of faults leading to systematic failure include human error that originate in: the SRS; the design, manufacture, installation, operation or maintenance of the hardware; the design or implementation of software. Similar devices designed, installed, operated, implemented or maintained in the same way are likely to contain the same faults. Therefore they are subject to common cause failures when the particular conditions occur."

IEC 61508:2010 defines it slightly differently: "Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors."

Those seem pretty clear. However, what about a fault in design where an aluminum body solenoid is installed outside, where low temperature extremes exceed its rating. It has a certain failure rate within its design temperature range. At temperatures well below its design range, it will not immediately fail, but the failure rate will be significantly higher, and outside of the failure rate published by FMEDA assessments. Isn't this a systematic failure which results from a fault in engineering design?

HISTORICAL INCIDENTS INVOLVING SYSTEMATIC FAILURE

Several industrial incidents discussed below depict systematic failures. These incidents generally are not the exception, but fit in a large category of where human failure is a root cause or a significant contributor to industrial incidents. Many readers of this paper have worked in an industrial process plant (chemical, petrochemical, oil exploration, power, pulp & paper, food & beverage, etc.) We have learned in our careers that incidents and near miss events usually do not have one root cause, but rather multiple causes - or more often, one cause (initiating event) and several contributors (enabling events) that intersect at a single point in time to collectively lead to a hazard to personnel safety, the environment, asset investment, and corporate reputation.

July 6, 1998 - 120 Miles NE of Scotland - Piper Alpha Oil Platform: An alarm with one of the rig's redundant condensate pump (B) sounds. Pump A was already offline for maintenance. The decision was made to postpone maintenance on Pump A. But when Pump A was brought back into service, a safety valve had been removed and blanked. When Pump A restarted, pressure built up, volatile gasses leaked from the pipe, and contacted an ignition source, resulting in an explosion. This incident caused 110 fatalities and numerous injuries. (Source: CSB)

March 23, 2005 - Texas City, TX - Isomerization Unit: The CSB concluded that the underlying causes were the organizational structure, a degradation of process safety culture, cost-cutting measures, and allowing warning signs prior to the event to not be considered in preventing future accidents. There was also an oversight of facility siting, which resulted in the high consequence of fatalities of those within the proximity of potential harm. The normal raffinate splitter tower unit level transmitter did not read above 9 feet. This tower was being filled manually. A high level switch in the tower failed (a loss of a safeguard), which if properly addressed, may have resulted in a very different outcome. The level switch had a history of failures, and numerous maintenance work orders were completed - although in some cases, no corrective action had taken place. Additionally, no instructions or situational details were turned over from night shift to day shift. The event was a result of an overfill of the raffinate tower and downstream blowdown drum,

that eventually overflowed flammable liquid product to grade forming a pool. The volatile vapors from the spill engulfed a large area and were ignited by a vehicle resulting in a vapor cloud explosion. Workers in the nearby contractor trailer were killed. This incident caused 15 fatalities and numerous injuries. (Source: CSB: Anatomy of a Disaster)

June 1, 1974 - Flixborough, England – Caprolactam Production Unit: Although root cause data is not prevalent, it is theorized that an unconfirmed vapor cloud of cyclohexane contacted an ignition source causing an explosion. The most prominent theory is that a process bypass pipe had been broken, and a temporary reduced-diameter bypass pipe was installed with an unusual angular configuration referred to as a "dogleg." The design team did not include a skilled mechanical engineer to calculate the stresses exerted by thermal expansion. A breach of the piping occurred, releasing cyclohexane, which eventually contacted an ignition source. The severity of the consequences could have been minimized by relocating the control room that was too close to the process. This incident caused 29 fatalities and numerous injuries. (Source: Cik Aqilah: Group 5 - Flixborough Explosion 1974, Evan Hale: Flixborough Disaster (Team 3).

The examples of major industrial incidents are abundant. But the majority of them are not due to equipment failure, but rather failure in specification, design, maintenance, and operational activities, decisions, or overlooking potential lessons learned. Although not as apparent as those of those involving specific actions in the maintenance, installation, and plant operation, the underlying causes (or contributors) can also manifest as a result of organizational structure and/or an inadequate process safety culture.

Even for those causes of "random" failure, there is almost always a human error involved with the initiating cause or affecting the reliability of the safeguards involved. And for each reported event, we have seen in our careers that there are multiple near misses that may or may not be officially reported which could have resulted in lesson learning and major incident prevention.

SIL VERIFICATION CALCULATIONS AND SYSTEMATIC FAILURES

The simplified equations for the four most common subsystem voting architectures per ISA-TR84.00.02 – Part 2 clause 5.1.5 are as follows. Notice that the intention for inclusion of the systematic failure term of the equation certainly is intended:

For a 1oo1 voting architecture:

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\lambda^{DU} \times \frac{\mathrm{TI}}{2}\right] + \left[\lambda_F^D \times \frac{TI}{2}\right]$$

For a 1oo2 voting architecture:

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\left((1-\beta)\times\lambda^{DU}\right)^2 \times \frac{TI^2}{3}\right] + \left[(1-\beta)\times\lambda^{DU}\times\lambda^{DD}\times MTTR\times TI\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

For a 2oo2 voting architecture:

$$\text{PFD}_{\text{avg}} = \left[\lambda^{DU} \times TI\right] + \left[\beta \times \lambda^{DU} \times TI\right] + \left[\lambda_F^D \times \frac{TI}{2}\right]$$

For a 2oo3 voting architecture:

$$\text{PFD}_{\text{avg}} = \left[(\lambda^{DU})^2 \times (TI)^2\right] + \left[3\lambda^{DU} \times \lambda^{DD} \times MTTR \times TI\right] + \left[\beta \times \lambda^{DU} \times \frac{TI}{2}\right] + \left[\lambda_F^D \times \frac{TI}{2}\right]$$

λ^{DU} is the undetected dangerous failure rate

λ_F^D is the dangerous systematic failure rate, and

TI is the time interval between manual functional tests of the component.

MTTR is the mean time to repair

λ^{DD} is dangerous detected failure rate, and

β is fraction of failures that impact more than one channel of a redundant system (common cause).

The formulas clearly acknowledge the contribution of systematic failure. The definition of Safety Integrity in IEC 61508 is congruent, and states that both random failures (represented by the lambdas) and systematic failures together determine the safety integrity. Some SIL Verification tools on the market attempt to provide parameters for a fraction of the contributors of systematic failures, but as a whole, systematic failures are not considered in the calculations, and rely on the various roles in the safety lifecycle to conform to all aspects of the governing standard – in this case IEC 61511- in reducing them. And as SIS Engineering practitioners, a very important part of our job is to eliminate or minimize systematic failures. Accounting for systematic failure (stemming from human errors) is effectively explained and does have significant effects on the achieved safety integrity, especially in safety functions requiring SIL3 integrity. (*Can we achieve Safety Integrity Level 3 (SIL 3) without analyzing Human Factors* – Grattan and Brumbaugh)

There are three performance requirements to consider when confirming that a SIF meets its integrity. The first is purely quantitative, and based on random hardware failures:

1. Achieved Risk Reduction Factor (RRF) or Average Probability of Failure on Demand (PFDavg) – which are reciprocals of one another;

The second is either quantitatively-derived or qualitatively derived:

2. Achieved Hardware Fault Tolerance – the achieved performance can be based on one of three routes:
    a. Per Table 6 of ISA 61511:2018 (along with meeting other requirements) based on the required SIL and demand mode

b. IEC 61508 Route 1_H, based on quantitative analysis of random hardware failures to determine the Safe Failure Fraction, and using IEC 61508 Table 2, Table 3, and related requirements of subclauses of 7.4.4.2;
c. IEC 61508 Route 2_H, based on field feedback performance data and rigorous analysis requirements validating that the components are suitable for use and the integrity levels for which they are assigned, or in combination under stringent rules for combinations with other devices to achieve the required SIL.

3. The third performance requirement is a qualitative achievement of SIL Systematic Integrity as defined in IEC 61508 Clauses 7.4.6 through 7.4.10, the most relative to our topic. Systematic integrity can be achieved by one of two ways:
   a. the Systematic Capability (SC), and is expressed as a qualitative achievement of meeting SIL2, SIL3, (and very rarely and questionably) SIL4 qualitative integrity – which then requires SIL-certified devices, meeting the SIL Systematic Capability levels for which they are assigned, or in combination under stringent rules for one additive credit with other devices to achieve the required SIL. Systematic Capability is an evaluation of each devices' resistance to systematic failures (manufacturing flaws, suitability for intended service, etc.). SC certification is most often based on the assessment of an outside industry-recognized certification body, and they are performed (at a substantial cost) for manufacturers who wish to promote their products in SIL-rated applications. An analysis of the manufacturer's quality program, functional safety management program, and methodologies of identifying and eliminating poorly-performing components is performed. In doing so, the effort is highly focused on eliminating common cause between identical components in the manufacturing of their products.
   b. Alternatively, this requirement can also be achieved by extensive Proven-In-Use justification, which involves extensive history and classification of failures under operations, and from functional testing – based on the same type of device used in similar applications, vast quantities of samples, over years of operation. This requirement is very difficult to achieve for numerous reasons. Two significant obstacles are the lack of resources required to gather and analyze the data, and the complication of manufacturers' upgrade and obsolescence of any given device (for example, firmware) over years, which invokes a "reset" of the data-gathering and analysis timeclock.

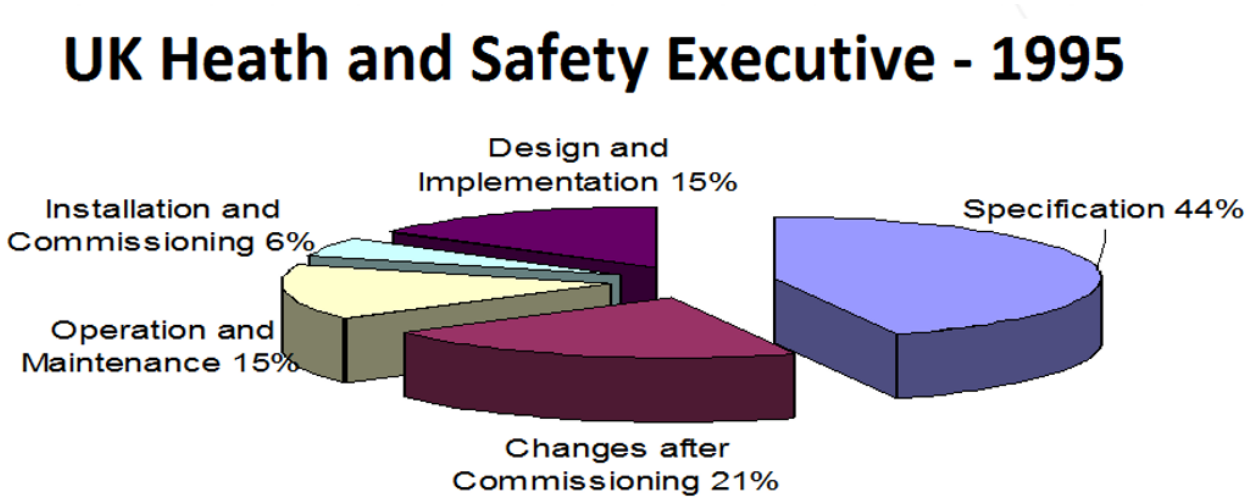
Due to the difficulties in achieving Proven-In-Use data, the vast majority of industrial process facilities have no choice but to choose SIL Systematic Capability-certified devices. Therefore, it is most important that engineers involved in specifying instrumentation (sensors), logic solvers, and final elements (typically on-off valves and motor control circuits and components) are tuned-in to the systematic capability for which these components achieve relative to the required SIL. Selection of appropriate devices requires a thorough understanding of the process and environmental conditions, without which instruments can be selected which are not fit for the applications, resulting in systematic failures.

GENERAL CLASSIFICATION OF SYSTEMATIC ERRORS

Systematic errors fall into those widely recognized by the process industry, and also those that are less obvious. The following chart depicts the area of contributing causes and activities of industrial

accidents - the "more commonly recognized". (We'll expand later on the less-commonly recognized contributing causes.)

Process Industry Accidents Involving Automation



Since 1995, the worldwide fractions of these contributors may have changed, but they all represent the contributions of systematic failures. One may ask why there is not a slice of the pie designated to random hardware or equipment hardware failures. The authors admit that random failures are a wedge of the overall causes of industrial incidents, although the proportion of pure equipment failures would be small. However, it should be noted that errors in specifications, design, and installation contribute significantly to equipment failures – not only in the areas of initiating causes, but also safeguards and protective layers of all types – including wired IPLs.

SYSTEMATIC ERRORS: SPECIFICATION

Clause 10.3.2 lists numerous specific requirements for the Safety Requirements Specification (SRS). Inadequate attention to nearly any of these requirements creates opportunities for the introduction of faults, resulting in systematic failures of SIFs. The following section provides examples of situations where inadequate attention to requirements for the SRS could result in the introduction of faults leading to systematic failures.

Failure to describe all SIFs, process measurements, and final element actions necessary to achieve required functional safety (e.g., a cause and effect, logic narrative) and criteria for successful operation, (e.g., leakage rate for valves, and identification of individual safe state) can result in inadequate designs and/or those which do not address all hazards, potentially leading to failures of the protective system. Failure to define safe states for SIFs which can occur concurrently, and design for the resulting total load to flares or other effluent handling systems, can create a separate hazard. Achieving that requires a thorough PHA, a thorough understanding of the initiating event(s) and required action(s) that the LOPA Practitioner intended, and clear and concise

communication with the IPL design team. Even with a thorough PHA using seasoned personnel who are very familiar with the processes being studied, and a likewise experienced LOPA Practitioner, sometimes communication with the IPL design team is not perfect. The result can be SIFs not adequately detailed in the SRS, and risk gap closure not being addressed. Some companies have implemented tasks with names such as IPL Select or LOPA Reconciliation to provide a SIS and BPCS IPL conceptual design "refinement" and optimal selection of the IPLs identified by the risk assessment. This refinement activity always involves a senior SIS conceptual design engineer, resulting in a more coordinated handoff from risk assessment to SIS conceptual design, and closing risk gaps more effectively. Additional scenarios and modifications identified by the IPL Select results are communicated back to the risk assessment team for incorporation, and are used in the overall safety design. Informal studies reveal that on medium and larger projects, the IPL Select team usually uncovers additional scenarios and situations in which the IPLs have to be modified to address things such as identifying additional SIF final elements to avoid the hazard, eliminating shared use of instrumentation, addressing response time issues, and assessing credited BPCS IPLs for full independence of the SIF against other IPLs and against the Initiating Event.

Communications with the PHA team, and discussing potential conflicts between multiple SIFs is critical to eliminate systematic failures. A trip of a pump BLEVE prevention SIF on a reactor that uses a single reactant cooler pump could stop the pump, protecting against BLEVE, but can place the reactor in an over-temperature condition. Such a configuration, if not noted by the PHA team should be identified by the IPL select team, and reported back to the PHA team for redesign. Likewise, the team should identify any dangerous combinations of output states to be avoided, consult with the PHA team, and note these states in the SRS.

Failure to identify both normal and abnormal process operating modes can result in hazardous scenarios not being adequately addressed. Many SIFs are designed considering normal continuous plant operation, and it is easy for a PHA team to only think about normal operation of the plant. Yet the most dangerous situations for a plant are in times of transition, which include startup and shut down. Additional SIFs may be required to support these process operating modes. Those are also the most complex situations for designing safety interlocks, because it is much easier to simply bypass interlocks in startup and/or shut down situations, leaving the LOPA gaps potentially not covered during those times, and perhaps not re-activating the SIFs when normal operating conditions have been achieved. The much more challenging, but frequently safer designs, are implemented to either operate during transitions, or sense the transition to normal operating conditions and automatically activate.

Sensor calibration is frequently required when the plant is operating. Installation of redundant sensors, with individual manual bypasses which issue repeated timed alarms, and which allow only one sensor in a pair to be in bypass at one time, not only eliminate the problem of running with sensors offline, but also provide fault tolerance so that the process can continue running protected if one sensor faults.

Failure to identify and take account of common cause failures can lead to significant overestimation of the capability of the SIF. The beta factor is used in SIL reliability calculations to account for this common cause; however, one of the concepts behind systematic failures is that faults are introduced in the design resulting in failures under specific conditions. Utilizing diversity in designs, for instance, in initiator (sensor) types, not only reduces the beta factor, but

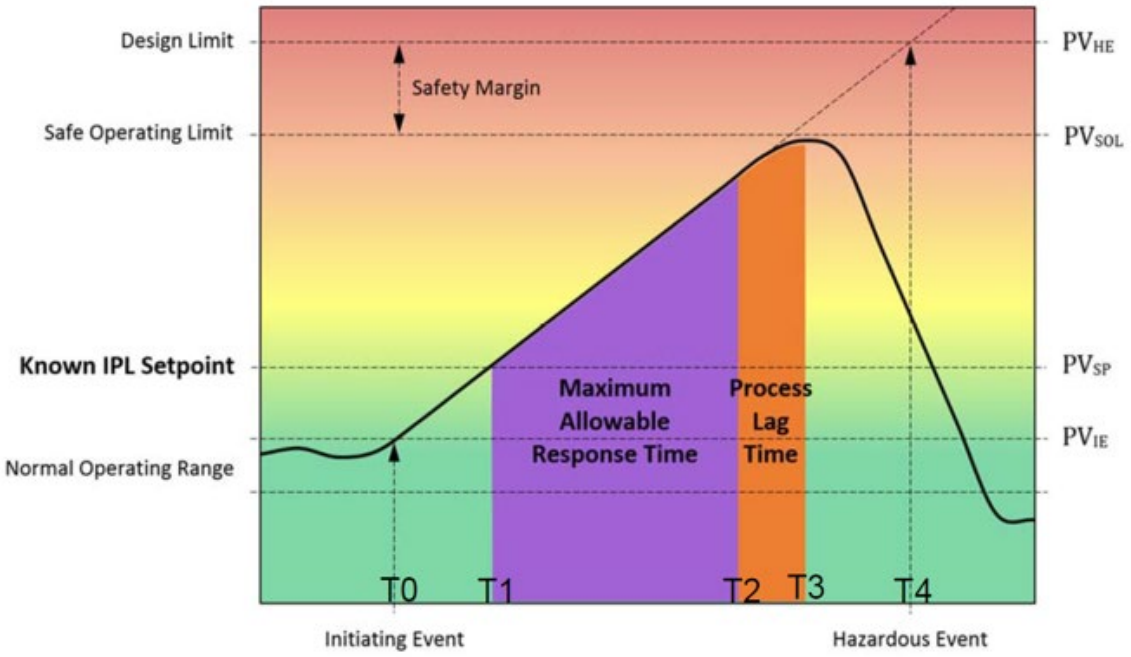
also reduces the chance that design faults will result in failures which affect all initiators rather than a fraction of them. Common cause is usually the dominant factor in 1oo2 voting arrangements, and not recognizing potential common cause failures in conceptual design, or assigning too low a beta factor are systematic failures that may occur in a SIF that does not have the functional integrity as intended.

The hazard analysis team and LOPA practitioner must frequently make assumptions concerning the SIF demand rate. Significant inaccuracies in these estimates can result when new processes are designed. Underestimates can result in undercalculation of the LOPA gap, and subsequently under-designing of the SIF. This estimating fault does not result in an immediate systematic failure, one which repeatedly causes failure of the SIF under certain conditions, but the probability is significantly higher that it will in time. This also emphasizes the importance of feedback of the future historical challenge rate to subsequent PHA revalidations, which is a component of the safety lifecycle.

Not adequately defining the requirements for proof test intervals and details of proof test implementation can lead to faults in design, which can prevent adequate proof testing. That does not cause the SIF to be unable to function, but it prevents the user from revealing a fault during testing, which increases the devices' probability of failure on demand. For instance, consider the following proof test for a pressure transmitter involved with a low pressure trip. In this case, the instrument utilizes a chemical diaphragm seal, with no way to calibrate it in the field. It is removed and sent to the instrument shop, where it is calibrated, then re-installed. Burnout direction, output upon detection of an internal fault, is confirmed to be above 20 mA. Before the analog wiring is re-attached, a signal generator is used to confirm that the safety logic solver receives the 3.2 to 22 mA signal. The safety logic solver is confirmed to trip at correct input signal, and is confirmed to alarm over 20 mA. However, the test never confirmed that the sensor itself could actually drive the signal over 20 mA. In a subsequent test, a communicator was connected to the transmitter, and it was revealed that the transmitter could not drive the signal over 17 mA. This would have repeatedly prevented the safety logic solver from issuing an alarm for transmitter fault. The cause was inadequate testing or design that manifested in the inability of the transmitter to overcome the high resistance in the long wiring run back to the safety logic solver.

Some applications require leak testing of valves during functional proof testing. Did the team adequately address and determine acceptable leakage rates? Does the design require additional valving, etc. to facilitate testing?

A commonly under-addressed parameter in the SRS is the calculations required to determine the Maximum Allowable Response Time (MART) of the SIF. Clause 10 of IEC 61511:2016 includes "Response time requirements for each SIF to bring the process to a safe state within the process safety time." But Process Safety Time (the time between times t0 and T4, below) and MART (the time between T1 and T3) are two different values, and a systematic error could be invoked if the SIF cannot respond fast enough to prevent the hazard, which must take into account the process lag time as well. Specifying a SIF that responds in less than (0.5 * MART) is considered Recommended and Generally Approved Good Engineering Practice (REGAGAP). Response time problems classically fit the definition of systematic failure, because of the inability of the SIF (or BPCS IPL) to transition fast enough to prevent the encroaching hazard is typically a combination of specification and/or design errors. Refer to the diagram below depicting the difference in Process Safety Time and Maximum Allowable Response time.



Timeline of IPL response to a hazardous condition, determining MART

$$PST = \frac{PV_{HE} - PV_{IE}}{PV_{ROC}} \qquad MART = \frac{PV_{SOL} - PV_{SP}}{PV_{ROC}} - PLT$$

TIME DEFINITIONS AND PROCESS VARIABLE (PV) DEFINITIONS (Refer to diagram above):

T0	Time at initiating event (identified in the Initiating Event of the LOPA scenario)
T1	Time at which the process reaches trip point of the SIF
T2	Time at which the PV has reached the safe operating limit (SOL)
T4	Time at which the hazard is imminent
PV_{IE}	PV at Initiating Event
PV_{SP}	PV at SIF Trip Point
PV_{SOL}	PV at Safe Operating Limit
PV_{HE}	PV at the Point of No Return (Hazardous Event is Imminent)

Consider the scenario where the initiating event is BPCS loop failure involving the steam flow control in the steam line to a reboiler. The steam valve fully opening leads to excessive heat input to the reboiler, which results in high pressure in a distillation column. Once the column pressure has reached the SIF trip point, the SIF trips, and opens the contacts to one or more solenoids on automated block valves to stop the steam flow. A good rule of thumb is that automated block valve closure time is two seconds per inch of line size - approximately twelve seconds for a six-inch line. Granted, the steam flow will start to taper off prior to complete valve closure, and valves can be designed to close more quickly, so some conservatism is included in this analysis. Even after the steam flow stops, heat input continues due to remaining thermal energy in the exchanger from the mass of hot metal in the exchanger and remaining uncondensed steam in the chest, resulting in additional process lag. These two factors, time to complete the action and stored thermal energy, can be significant, and must be taken into consideration when determining the maximum allowable value for the SIF trip point.

Failure in addressing fault detection and response issues, including requirements for bypassing if devices are to be replaced while the process is operating, could result in the introduction of systematic faults. Lack of written bypass procedures, including whether compensating measures are required during the bypass, the details of those measures, how the bypasses will be administratively controlled and then cleared, how the SIF will be re-enabled, bypass alarm messages, which classifications of personnel are able to affect bypasses, mean repair times, locations and quantities of spares, and a host of other issues can all introduce faults leading to systematic failures. For BPCS IPLs, inadequate application security introduces a greater likelihood of systematic failure due to an operator leaving the IPL in bypass for extended periods of time, or even changing the trip value or other critical parameters.

Failure to identify extremes of all environmental conditions, including temperature, humidity, vibration, electromagnetic interference, flooding, and other factors can introduce systematic failures. Environmental extremes must be considered not only those during operation of the process, but also during shipment of components, construction, and outages. Lack of thorough consideration of environmental extremes could allow the specification and installation of solenoid valves with metallurgy, and associated temperature ratings, which are not sufficient for low temperature extremes. This design fault will not result in immediate failure of the devices when the temperature is outside of the ratings of the solenoids, but the random failure rates will probably exceed those noted in the device certification. Lack of consideration of local temperature extremes, in locations near a hot reactor, can result in much shortened life of sensors such as nuclear level detectors. This qualifies as a systematic failure since the devices will predictably have shorter lives, thus much higher failure rates, when devices not specifically designed to significantly elevated temperatures are exposed to those conditions. Use of nuclear level detectors in areas which are also subject to radiographic inspection of nearby piping and equipment, even in neighboring buildings, can lead to temporary blinding of those detectors during radiographs. A nuclear level detector receives less radiation when the path between it and the source is blocked by process liquid. If extended radiographing of heavy-walled piping was taking place where the detector would not be shielded, the detector would be potentially blinded, and not sense a high level occurring during testing of that nearby piping.

Closely related to the consideration of environmental extremes are requirements for any SIFs to withstand major accident events, such as the amount of time that a valve must remain operational in case of a fire.

Failure to provide sufficient details in the application program safety requirements can lead to the personnel developing the application program making their own assumptions and judgements, some of which may not align with those of the owner's design team, resulting in systematic failures. The application program safety requirements may be derived from the SRS, and must align with it. Voting, fault detection and response, alarming, time delays, bypass initiation and clearing, reset logic, performance requirements, allowances for various modes of operation, requirements for addressing conflicts between SIFs, and other issues must all be clearly defined. It should be noted that Cause and Effect diagrams (C&Es) are sometimes adequate in depicting SIF and IPL logic. But C&Es cannot depict complex algorithms and sequential logic effectively. Sequential function charts, Boolean logic and/or logic narratives are often required to convey the logic clearly and unambiguously to the programmer. The application program requirements must be clear and defined, enabling adherence to those requirements to be checked prior to acceptance, checkout, and startup.

In the case of the purchase of packaged equipment, the purchaser may not have complete control over the functionality that is programmed into the system. The purchaser must insist on a complete understanding and documentation of the performance of the system. These are necessary to insure the system meets reliability requirements and acceptable interfacing with existing systems is provided. The purchaser must conduct necessary safety reviews, and if the purchased system falls short of expectations, address any remaining safety gaps before startup.

SYSTEMATIC ERRORS: DESIGN AND IMPLEMENTATION

Clause 11 provides a great amount of detail concerning designing the SIS to meet the requirements provided in the SRS. It is important that the SRS is thorough and clear, and that the owner insure the requirements are well understood and addressed. Numerous faults in design and implementation can manifest themselves as systematic failures if requirements are not clear.

Failure to implement appropriate response for fault detection, alarming, initiator voting changes in response to faulty devices, and procedures for addressing reported faults can result in faulty devices continuing to remain in service for times far exceeding the Maximum Permitted Repair Time (MPRT). Operations and maintenance personnel need sufficient training and procedures, with periodic reinforcement training, to ensure that priority is given to addressing faulty devices. Likewise, alarming must be configured such that these diagnostic alarms are given priority, and that the actions to be taken are clearly communicated. Inadequate collaboration between operations, maintenance and engineering during the design phase could result in misunderstandings concerning the intended actions, constraints and compensating measures to be utilized in the event of SIF faults. Insufficient compensating measures could increase the uncovered risk during the period of the SIF fault, increasing the probability of a hazardous event. Detailed descriptions of the compensating measures, thoroughly discussed prior to or no later than Stage 2 FSA, significantly minimizes chances for this misunderstanding.

To address Hardware Fault Tolerance (HFT) requirements for specified SILs, many SIF designers will utilize Table 6, referred to in clause 11.4.5 of ISA 61511:2018 Part 1. Neglecting the HFT requirement for SIL 3 can result in an inadequate SIL 3 SIF design, using a single level switch, meeting the random hardware reliability requirements. However, relying on only one sensor significantly increases the probability of systematic failure of the SIF due to inadequate placement

of the level switch. This could occur in a heavily-agitated vessel, where the liquid level varies from one side to the other, if the switch were located in a zone with a lower liquid level, potentially resulting in overflow from the side experiencing the higher level.

Failure to properly account for human capabilities can introduce systematic failures. In the case of an IPL which credits operator response, the operators must have time to recognize an alarm, determine appropriate action, complete the action, and return to a safe location, including plenty of cushion in case the action in the field, such as manipulating one or more particular valves, takes much more time than originally anticipated. Alarm Rationalization can identify inadequate alarm IPL credits, but must rely on the comparison of the alarm plus operator response time duration in comparison to the calculated Maximum Allowable Response Time.

Multiple appropriate configurations exist for communications between the SIS and the BPCS. These communications are required for items such as triggering BPCS actions to prevent loop windup after SIF trips, taking additional BPCS actions that are not required to meet the LOPA requirements, but which facilitate a more orderly restart, and SIF reset requests. Failure to define an overall plan, closely matching the configuration of existing systems if the purpose of the project is to expand existing facilities, implement the plan, and train operators and maintenance personnel concerning any changes in the new system introduces greater probability of systematic failures. Reset configurations need adequate attention. Auto-resetting of SIFs to prevent pump BLEVE may be appropriate with local start and local seal-in circuits. With remote start capabilities, BPCS seal-in configuration, and high pressure initiators, insufficient attention to the design can result in pumps automatically restarting once the discharge pressure drops below the setpoint.

Failure to insure independence between components utilized in the Initiating Event (IE), frequently the BPCS, and the SIF result in overcalculation of SIL achievement. There are times when sensors utilized by the BPCS can be shared with the SIS, typically via the use of optical isolators on the BPCS side, but these configurations must be closely examined to insure appropriate separation between the IE and protective layers. If failure of the device used by the BPCS can lead to a challenge of the SIF also utilizing that device, then the device cannot be shared. ANSI/ISA 84.00.01-2004 allowed for same logic solver involved with an IE in the BPCS to be used for a BPCS ILP as long as the BPCS demonstrated a sufficient level of reliability. IEC 61511:2016 requires additional independence in the BPCS logic solver involved with the IE and one that is utilized for the IPL.

Failure to properly account for all failures, particularly utilities, associated with Energize To Trip (ETT) SIFs can lead to systematic failures. A site-wide power outage may create a demand on a safety interlock, yet that same interlock could be unable to sense the scenario and/or respond if the power outage also results in loss of instrument air, or control power to sensing or action devices. Backup power supplies must also be regularly tested, or they provide no benefit. If the facility is scared to test the backup power for fear that it will fail and cause a shutdown, they are probably correct – it is likely unreliable.

Failure to address the intent of having a safety manual covering operation, maintenance, intended configurations of the devices, intended operating environment, fault detection and constraints can lead to systematic failures during maintenance of SIF components. As with other requirements of the standard, the important concept related to systematic failures and this requirement is to ensure that the appropriate personnel have sufficient information concerning the system so that they do not introduce systematic faults. A number of facilities address this with a combination of software

and printed documentation, rather than one safety manual. An example of a documentation fault, which could result in a systematic failure, is insufficient or difficult to access information on a sensor in a higher temperature application. Lacking documentation on requirements for a specific model, well-intended maintenance personnel could replace the device with one not designed for the operating environment, resulting in a predictable and significantly shortened life.

Process and maintenance experts must be involved in instrument selection rather than simply leaving the choice up to engineering personnel who may not have sufficient understanding of the process challenges. For SIL 3 applications, the bar is higher for FPL field devices, in that "an assessment of the FPL device shall be carried out to show that" the device is suitable for the application including that it "has been used or tested in configurations representative of the intended operational profiles." (FPL devices, those which use Fixed Programming Language, include items such as smart sensors and smart final elements.) Requirements on PE logic solvers include not only prior use assessments, but also those to detect systematic programming faults.

The person writing the Factory Acceptance Test (FAT) plan should not be the developer of the application program. FAT testing must be by a plan that specifies not just pass and fail criteria, but exception cases as well. The best test is with a full complement of I/O (wired) simulation panels, and interfaces to BPCS and foreign devices intact, with testing of bad quality and out-of-range of all hard and soft signals. Testing should be performed for full SIF functionality in all modes and all conceivable cases within those modes, as well as bypassing, bypass re-alarms, first-outs, and resets. Not testing these facets at FAT will require that they are addressed at Site-Acceptance Testing (SAT), where faulted state testing will be more cumbersome or impracticable.

SYSTEMATIC ERRORS: INSTALLATION AND COMMISSIONING

The installation of a control system is based on the detailed design drawings, and documentation as well as the manufacturer's installation requirements for sensors, logic solvers, final elements, and interfaces. The management and coordination of installation is key, as there are often many contractors onsite performing installation within their scope. It is expected that any given contractor is trained and competent within their scope of installation; however there are factors that increase the probability of installation errors. Long work hours days on end, compressed schedules result in fatigue. Also, the ratio of trainees and apprentices to highly-experienced installation staff should be appropriately managed based on the complexity and/or repetition of the installation tasks.

Training of employees perfuming installation is important, especially confirmation that they understand the 'why' of installation details. Personnel installing instrumentation of all types need to understand the ramifications incorrect installation. Installing pre-assembled actuated valves may sound routine, but they are often installed backwards, as are flowmeters, differential pressure transmitter hi/low impulse lines, check-valves, etc. Piping instrument air to the wrong solenoid valve port is also fairly common. The removal of welding rods and welding slag is very important on newly installed piping. Welding rods are notorious for causing equipment malfunctions and 2AM call-ins.

The tie-in between systems is a key design effort that is often installed by a general electrical contractor, and a heightened awareness and interaction with construction management can help assure installation is proceeding as planned.

Commissioning is a team effort, and its success and efficiency is contingent on a solid plan and orchestrated by a competent leader. The commissioning plan is paramount, and is typically the source of most systemic failures in the commissioning process. Omissions in the commissioning plan can result in untested attributes of sensors and final elements to faults and loss of power. Commissioning also tests the action of the logic solver upon loss of power and remote I/O communications, and communications to external systems – and the response upon loss of communications. A solid commissioning plan should systematically test all attributes of rangeability from the field to the SIS or BPCS, Bad signal (BadPV), loss of electrical signal, and all I/O-related and functional requirements specified in the SRS. The interfaces must be tested between systems (between the SIS and the BPCS, vendor skids, HMI confirmation of correct reading and operation of final elements from the operator stations, etc.) Test fault conditions of BPCS communications to SIS to make confirm the SIS and all SIF integrity is in not compromised.

Commissioning teams are also vulnerable to systematic failures, especially if the schedule is compressed. Instead of taking the commissioning plan and drawings out to the field, the commissioning team will sometimes leave the bulk of the paperwork back in the office, and "rubber stamp" the paperwork at the end of the day. Without the documentation in the field to immediately capture testing results, the attention to detail can be compromised.

It should be noted that systematic failures in specification or design are often not detected in commissioning.

SYSTEMATIC ERRORS: OPERATION AND MAINTENANCE

During PHAs and LOPAs, the participation of operations is mandatory. Operations is usually represented by a senior operator. And often, Electrical/Instrumentation & Controls (E/I&C) personnel participate in LOPA. These personnel obtain excellent exposure to initiating events, all types of protective layers, and risk gap closure. However, they represent only a small fraction of the operations and maintenance workforce. Unless a rigorous training program is implemented, the operations staff may know 'how to do' new tasks now required to comply to IEC 61511, but maybe not 'why'. New operating procedures and drilled training for operators, as well as new proof test procedures for maintenance and operations are overwhelming to try to cram into weeks before startup. Bypassing, resets, manual modes of shutdown that overrides the SIS, and numerous other requirements of the SRS must be in the training curriculum for all operators. Train and drill operators well ahead of commissioning. Involve them in FAT witnessing. If the 'why' is not part of the training, then they are likely missing the bigger picture. It most important that operating procedures are developed, and drilled or otherwise tested. It is also required in Stage 3 FSA that the procedures be in place, and that documentation of training is available. Seasoned operators have a good knowledge of the hazards in the process, and how to adapt to new processes and modifications. So, involving younger staff and assigning them roles in the IEC 61511 lifecycle grooms their understanding of 'why' as they take over the supervision and managerial positions.

An important retro-active requirement of the Safety Lifecycle is updating the demand frequency of the initiating events (causes) that the layers of protection are assigned to protect against. Higher actual demand frequencies than predicted SIF challenge rates not only affect the LOPA, but also the SIL reliability calculation. For example, if a SIF designed with an initiating event assumed to be 1 in 10 years (appropriate BPCS loop failure rate) is found to be challenged more frequently than once per year, the initiating event factor in the LOPA changes, resulting in a higher LOPA gap and a SIF that now operates in the high-demand mode, requiring additional calculations based on the frequency of dangerous failures, rather than the probability of failure on demand. Re-design to implement Inherently Safer Design practices, dramatically reducing the SIF challenge rate, may prove to be a wiser and safer choice.

In a similar retro-active fashion, feeding back actual failure rate and failure classification data to the assumed failure rates in the SIL Verification calculation can also reveal underperforming devices, and gaps in the achieved integrity of the SIFs. Dangerous detected failure rates, dangerous undetected failure rates, and safe failure rates collected during operation, as well as dangerous undetected and safe failures during proof testing validates the assumed failure rates, or invokes selection of more highly-reliable devices.

SYSTEMATIC ERRORS: CHANGES AFTER COMMISSIONING

A section later in this document discusses a plant safety culture that focuses on the trips, slips, falls, and PPE-related focus or personal safety. And years ago, when it seemed like personal safety was almost the only focus, our awareness of process risks was overshadowed, until occurrence and re-occurrence of industrial incidents. And in time, this invoked OSHA 29CFR1910.119 Mechanical Integrity and Management of Change (MOC) requirements. Management of Change set rigorous assessments, communications, and signoffs of process changes after installation and commissioning. Gone are the days (in BPCSs, and most importantly in SISs) of napkin sketches of control changes. What a scary thought now, but 25 or more years ago, it was not uncommon. We all had an idea of what changes were riskier than others, and held off on the really complex control algorithm changes until 3rd shift or at nights during a turnaround. Some of the most catastrophic industrial process incidents were due to changes made after commissioning.

Common modifications to interlocks include changes in trip value, initiator time delay, and additional actions. In the case of a SIF set to trip on high temperature, which is challenged much more frequently than anticipated in the original PHA, a well-meaning operations engineer may want to "slightly" increase the trip value to avoid the "spurious trips." In fact, these may not be spurious trips at all, but actual challenges to the SIF. Increasing the trip value may shorten the response time below that required, making the SIF no longer effective. A root cause analysis is in order, providing the possibility of redesign, hopefully attacking the initiating event, and not only reducing the challenge rate, but making the process safer. According to requirements in clause 5.2.1.9, prior to a proposed change being made to a safety interlock, a FSA must be completed to confirm that the new design still meets the requirements of IEC 61511. Failure to conduct an FSA prior to SIF modifications not only puts the plant in violation of the IEC 61511 standard, but also introduces the possibility of making the SIF no longer effective.

TECHNICAL CHECKS, FUNCTIONAL SAFETY ASSESSMENT, AND AUDITS

Most organizations involved in the implementation of the process safety lifecycle (including manufacturers, integrators, contract engineering, procurement, and end-users) employ programs

to assure the quality of documentation, specifications, and drawings. Often, the finger is pointed at the checker when an error or omission is detected downstream, or even worse, manifests through design and installation, into the field. This series of failures can (immediately, or over a span of years) lead to a significant incident involving loss of life, serious environmental impact, financial impact in numerous forms. But where did the systematic error occur? The answer primarily is the "doer" (the persons, departments, or organization performing the work in the safety lifecycle phases), and the failure of the checking task is secondary – a recovery failure. Checking, audits, squad checks, and other technical quality-reviews are only a recovery measure to identify and correct errors, oversights, and omissions.

The requirements of independence in regard to Functional Safety Assessment of Safety-Related Systems is depicted in IEC 61508-2 Tables 4 and 5, and relevant subclauses of 8.2, and Organizations in general would benefit from considering and applying these levels of independence in the checking process. Based on the required safety integrity and criticality requirements (or criticality of control loops as recommended in this publication), the level of independence is increasingly assigned:

- A person independent of the project team
- A department within an organization independent of the project team
- An independent organization

There are many other requirements of the FSA team depicted in Clause 5 of ISA 61511. A key ingredient is competency of the FSA facilitator (or lead technical representative). An error detected after design is complete (Stage 2 FSA) or after installation is complete (Stage 3 FSA) can be very costly for capital projects, PHA/LOPA revalidation projects, system upgrades, and modifications after commissioning and startup.

Process Safety Audits for facilities requiring OSHA 29CFR1910.119 Mechanical Integrity and Process Safety Management compliance assess corporate, organization, divisional, or local facility against the pertinent requirements. Highly-experienced professionals can assist in revealing organizational structures and practices that "open a door" for systematic failures to occur. This topic provides a segway to the "not so obvious" systematic errors in process safety that occur above the level of the UK Health and Safety Executive – 1995 pie-chart.

SYSTEMATIC ERRORS INVOLVING BPCS INITIATING EVENTS AND BPCS IPLs

As noted above, in the field of process safety engineering, much effort is spent on quantifying and accounting for random hardware failures – this applies to the control loops and functions involved in control loops, as well as BPCS IPLs. In risk assessment (identification of hazards and the allocation of protective layers - Clauses 8 and 9 of IEC 61511) industry-accepted initiating event frequencies and independent protective layers (IPL) are allocated. It should be noted that a typical initiating event frequency of a BPCS control loop (pressure, temperature, level, single loop, cascade, and numerous other types of control, as well as sequential batch / recipe control) is 1 in 10 years (0.1 failure per year). This failure rate value includes all components of the control loop – the sensors, the logic solver, and the final elements. There is a divided opinion in practitioners of risk assessment that the initiating event frequency is conservatively assigned. A value assigned for such a vast array of control loop complexities cannot be accurate. (Consider a simple single

control loop with one process variable and one final element, such as a flow control loop, and a complex feed-forward distillation column level controller, or a batch program that may employ many sensors and many final elements. (The single loop at 1 failure every 10 years is likely conservative.) Thus conservativism of the initiating event decreases as the BPCS application gets more complex.

Consider the components of a BPCS control loop. For example, a pressure single loop PID controller – a pressure transmitter 4-20mA signal interfacing a BPCS input module, processed by the BPCS CPU, and adjustment of the analog output module channel current (4-20mA) based on the process variable error vs. controller setpoint and tuning parameters. Industry has assessed that the vast majority of hardware failures are the field devices (the sensors and/or the final elements), and most typically the final elements. Systematic errors however come into play with all three: the sensors, the logic solver, and the final elements. The random hardware failure rates of logic solvers are typically orders of magnitude lower than that of the field devices. If the logic solvers are "left alone" after a detailed Factory Acceptance Test (FAT) with identification and elimination of systematic errors in the application software development, then the main source of failure after installation is systematic failure – involving the changes invoked by humans. It is very true that maintenance activities with sensors and final elements have invoked systematic errors, but the logic solver in particular is generally a highly consistent and reliable component, with complex components and processing logic especially vulnerable to human interaction. SIS logic solvers therefore have higher integrity requirements and security to minimize unauthorized or online changes.

Measures to avoid systematic failures in BPCS:

- Indoctrinate stringent MOC procedures and practices for any process-related change in equipment and configuration (including process control loop setpoint range limits).
- No matter how experienced the programmer and maintenance personnel, be diligent in heightening the awareness of the potential impact of an error or process-related interaction that may result from the changes you and coworkers invoke.
- If calibrating or testing online, consider the risk of upset during crossover or return to normal operation. Confirm that redundant devices have been historized and are in good working order before commencing.
- Avoid major processor and output module-impacting changes such as cold-start downloads, CPU reboots, and potential initialization events that (depending on the state of the process) that may pose transitions of final elements that could lead to hazards. Test these actions during Factory Acceptance Testing (FAT) if possible or during Site Acceptance Testing (SAT).
- Test the recovery from power loss of main power and of the uninterruptible power supply (cold restart). If backup generators are utilized, confirm final element actions are to the failsafe position, or as otherwise specified by the functional specification.
- Be meticulous in version control of your application program.
- Annotate code to describe functionality in detail.
- When developing FAT plans, Commissioning, and Site Acceptance Testing, employ both positive and negative testing. Positive testing addresses the expected results, whereas negative testing ensures that the application program responds appropriately to unexpected events, and combinations of conditions. This includes testing in startup mode, normal

operations, offline, maintenance, various batch steps, varying recipes, and alternate operating modes.

- Consider prevention of hardware and software systematic failures by reading and following applicable sections and clauses of IEC 61508 Parts 2 and 3 – even for the BPCS.

BIGGER-PICTURE CONTRIBUTORS TO SYSTEMATIC FAILURES

As professional practitioners in our respective fields within the process industry, it's important to focus on the technical aspects and do our part in reducing systematic failures in our line of work. Whether stated or not in our job description, it is part of our job to avoid errors and omissions, and coordinate with other parties for a clean handoff of information. But there are "bigger-picture" issues that can be unrecognized and contribute to systematic failures.

The Corporate and Local Culture of Process Safety

Most of us have been in industrial plants where banners and safety lunches celebrate milestones of 1,000,000 hours (or more) without a Lost-Time accident. As a young controls engineer in the early 1990's, one of our authors was appointed the Plant Safety Coordinator at chemical plant. We achieved almost 4,000,000 manhours since our previous lost-time accident. Slips, trips, and falls, and avoiding burns and chemical exposure were our focus. Personal protective equipment, various work permits, and situational awareness were our safeguards. As a controls engineer at a Fortune 50 company, one would expect a greater awareness and respect for the hazards in the pipes. However, troubleshooting production problems, annual turnarounds, managing confined space entries, and managing contractors were actually the focus along with expectations to keep the plant running, above all. Until the first PHA of the running facility, the process upsets, equipment failures, and human error usually resulted only in lost production. There were several systemic failures that caused two serious near misses of potentially fatal consequence, and one event of significant equipment damage. Procedures involving control systems emerged, and the plant implemented a Management of Change program that proved to reduce the online changes that had previously been a daily task. ISA 84 (1996) had not yet been released, but the plant culture changed and embraced the concepts.

Like many directives, changes, voluntary programs, and mandatory programs, the leadership comes from the top. This applies to Process Safety as well. Corporate managers, divisional managers, local plant managers, engineering managers, and technical, maintenance, and operations will "buy-in" when they know a culture is changing across the plant, across the division, and across the corporation. There is less incentive to embrace the Process Safety Lifecycle if it is not being promoted by corporate procedures, policies, and guidelines.

Clause 5 of IEC 61511 focus on Functional Safety Management. Although the clause is only a few pages, its contents set the stage for a plant, division, and corporation for establishing roles and responsibilities, competency of all personnel in those roles, method of assessing functional safety (FSA and Audits), and the development and adherence to a Function Safety Management Plan (FSMP). The old phrase "Failing to Plan is Planning to Fail" holds true in systematic failures. The systematic failure may not be apparent immediately without a plan, but they will surface, and loopholes of accountability will emerge, which means that a facet is understaffed, or staffed with

a person not competent for the task. All young engineers need an opportunity to learn, but without mentoring and thorough review of their work, systematic failures are likely to occur. As leaders in the field of Process Safety, we must assure competence of all personnel within their roles and responsibilities.

There are numerous clauses in IEC 61508 that focus on systematic failures and measures to prevent them. IEC 61511 refers to its parent standard, IEC 61508, in a number of areas, but practitioners of the IEC 61511 Safety Lifecycle rarely read (or periodically refresh themselves on) IEC 61508. We can all benefit by understanding and embracing the parent standard instead of concentrating on IEC 61511. IEC 61508 allows a practitioner of the standard of process safety to the bigger picture of functional safety of E/E/PE systems.

Organizational and Project Execution Structures

When decisions are made to introduce hazardous chemicals into the process and start up or re-start a processing plant, or a process within the plant after the installation and commissioning of a capital project, a maintenance turnaround, or after making a change in the process, it is often a Unit Operations Manager call, a Plant Manager call, or a Business Manger call. It is imperative that the persons making the decision to run the process have the appropriate knowledge and understanding of the process and technical factors of process safety risk that are involved. On even a larger scale, a different company (than the owner/end user making the decisions to run) may be performing the engineering, and even a third company may be responsible for testing, commissioning, and/or startup. Pre-Startup Safety Reviews may only be performed by one party, and may not include the contributors that may recognize or have knowledge of a potential hazard to say "not yet" to starting up the process. It is essential that MOCs are signed by all parties, and that the decision to introduce hazardous chemicals into the process is made with the sign-off of top engineering management knowledgeable of the process risk.

An organizational structure that does not include Process Safety Engineering input to the decision to run will either on this startup, (the next, or one months or years later) open the door for an incident. Start-ups are the most vulnerable operational mode at practically all process facilities. It is of utmost importance that we do not short-circuit process safety due to lack of information, lack of knowledge of process risks, or financial (corporate or bonus-incentive) pressures to be online.

Failure to Learn

Numerous industrial catastrophes have occurred when the owner/operator, engineering firm, or vendor have had incidents and near-misses in the past, and yet have not taken corrective actions to effectively and permanently prevent the re-occurrence. Capital projects (engineering, end-users, and contractors) can take into account the hazards, incidents, and near misses of similar processes within the end-user's division on similar processes, allowing them to be properly mitigated during the design process. Near misses are often shared within operating divisions of a corporation, but rarely outside of the organization.

Inherently safer design is the best measure, although it may not be practical. Consider alternative technologies. Strengthen protective layers. Reduce initiating event frequencies, and eliminate or minimize enabling events. Temporary work-arounds need to be carefully evaluated and discussed

with top management, divisional, and corporate engineering and process risk managers, with a plan for corrective action, appropriately prioritized based on the risk (severity x frequency).

CONCLUSION

The potential for systematic failures is abundant in the BPCS and SIS protective layer specification, design, and implementation throughout the life of the function. While risk assessment and SIS engineering professionals focus on the quantifiable aspects of initiating events and IPLs in the form of BPCS (alarms, control loops, and interlocks) and SIS instrumented functions, it is the intangible and covert human failure that emerges after installation, where the root cause is not that a process, equipment component, or protective function failed, but what management system failure allowed that failure to occur. While we continue to solve for the quantifiable results required of our roles in the Safety Lifecycle, we must take an honest look at the work processes in which we are involved and seek improvement within them. Understanding the ramifications of errors in the tasks within our roles is the first step in reducing them.

REFERENCES

[1] ISA 61511:2018-Part 1 equivalent to IEC 61511 v2.1:2017-AMD1+ - Part 1 *Functional Safety – Safety Instrumented Systems for the Process Industry Sector*

[2] IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 2 & 3, edition 2.0. International Electrotechnical Commission, Geneva, Switzerland, 2010.

[3] ISA-S84.01-1996 – *Application of Safety Instrumented Systems for the Process Industries*

[4] ISA-TR84.00.02-2002 – *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations*

[5] D. Grattan and K. Brumbaugh, *"Reverend Bayes, meet Process Safety, Use Bayes' Theorem to establish site specific confidence in your LOPA calculations,"* Available at https://www.aesolns.com/whitepapers/3855/, Accessed on 10-22-2019

[6] CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment,* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001

[7] CCPS, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2013

[8] G. Barnard and W. Creel, *"Impacts of Process Safety Time on Layer of Protection Analysis,"* Available at http://www.aesolns.com/wp-content/uploads/2015/11/impacts_of_process_safety_time_on_layer_of_protection_analysis.pdf, Accessed on 10-22-2019