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

19th Annual International Symposium
October 25-27, 2016 • College Station, Texas

Measuring the Reliability of Safety Controls, Alarms, and Interlocks

Angela Summers, PhD. President
SIS-TECH Solutions
12621 Featherwood Dr. Suite 120, Houston, TX 77034
asummers@sis-tech.com

Keywords: safety instrumented systems, safety controls, safety interlocks, safety alarms, instrument reliability, IEC 61511

Abstract

The risk analysis assumes a level of risk reduction provided by each of the safeguards, including safety controls, alarms, and interlocks (SCAI). After installation, SCAI equipment must be proven to meet the assumptions through examination of maintenance records. As SCAI equipment ages, failures can begin to occur more frequently where few have occurred before. Some equipment may need replacement just to sustain the risk reduction. An instrument reliability program is necessary to:

- Provide feedback to validate risk analysis and functional specification assumptions
- Identify and eliminate systematic failures
- Provide prior use evidence (historical performance) for determining fit for purpose
- Support selection of SCAI equipment
- Ensure that poor performing equipment is identified and actions are taken to correct deficiencies

In order for the risk analysis to not be overly optimistic or pessimistic, the data assumptions need to agree with the actual capability of the installed systems. This paper covers the essential elements of an instrument reliability program that can be applied to both process control and SCAI

equipment. It will discuss the critical activities needed to identify and track failures, so negative trends in performance can be responded to prior to a loss event occurrence. A successful instrument reliability program leverages existing work processes to collect quality data that drives improvement in safety and reliability.

1 Introduction

During the hazard identification and risk analysis process, the process control system is assessed to understand how functional failures give rise to loss events. Process control system failure can initiate events and place process demands on SCAI. The risk analysis makes assumptions about the likelihood of process control failure in order to estimate the potential event frequency. The reliability of process control equipment impacts the safety and profitability of the process. Higher reliability minimizes the number of process upsets, shutdowns and startups. Essentially, the more reliable the process control equipment, the safer the process unit is.

> *The key process safety objective is to identify failures, gaps or conditions and to correct them before they contribute to a major process safety incident [1].*

Detailed tracking of all process control equipment is resource intensive due to the large number of instruments involved. For this reason, many owner/operators establish a classification scheme to identify and prioritize instrumentation. Those instruments that are related to loss events with safety, environmental, or significant business impacts, such as asset, production, or quality, are generally included in the instrument reliability program.

The risk analysis assumes a level of risk reduction for each of the safeguards, including SCAI. From the moment that equipment is installed and commissioned, it becomes existing equipment that must be proven to meet the design assumptions through its maintenance records [2, 3, 4, 5]. New equipment releases may reveal previously unknown failure causes. As SCAI equipment ages, failures can begin to occur more frequently where few have occurred before. Some equipment may require replacement to sustain the risk reduction required from SCAI.

An instrument reliability program is needed to identify and track failures, so negative trends in performance can be responded to prior to a loss event occurrence. Through prompt investigation and corrective action when failures are found, the program assures that device failure does not become normalized. An effective instrument reliability program includes:

- Identifying and tracking failures at the functional location and equipment record level [6]
- Investigating failure causes and the impact of the failure on system performance and process safety [5, 3]
- Comparing actual failure rates with the assumptions of the risk analysis and functional specification [7, 3]
- Comparing actual spurious trip rate with the assumptions of the risk analysis and functional specification [7, 3]
- Identifying bad actors and taking corrective actions [5, 3]
- Tracking and resolving problems found [5, 3]
- Sharing lessons learned [5]

2 Tracking Failure

IEC 61511 [3] requires that procedures be implemented to evaluate the SIS performance against its safety requirements, to identify and prevent systematic failures that could jeopardize safety, and to assess whether the in-service reliability parameters agree with design assumptions. Procedures are also required to assure that prompt corrective action is taken to address identified deficiencies (IEC 61511 clause 5.2.5.1). IEC 61511 clause 5.2.5.3 further clarifies that the owner/operator verify the demand rate on the SIS and the SIS reliability parameters. Refer to ISA TR84.00.03 [5] for more guidance on the instrument reliability plan for SIS. The IEC 61511 instrument reliability requirements and ISA TR84.00.03 guidance are broadly applicable to SCAI.

In order to minimize the likelihood of failures that result in a loss of function, procedures are needed for gathering information about failures and developing useful metrics regarding failures. The owner/operator must define the corrective action to be taken if the rates exceed those assumed during design. Competent people are also necessary to evaluate and analyze the data and then develop and implement plans to improve the SCAI reliability. Consideration should be given to the automated recording of SCAI demands and associated process conditions to support event analysis. ISA TR84.00.04 Annex R [4] and ISA TR84.00.03 [5] provide guidance on selecting metrics for SIS and these metrics can be applied equally as well to SCAI. Many different metrics can be used to assess performance, including:

- Demand rate
- Total failure rate
  - Mean time to failure
  - Mean time to between failure
  - Mean time between unplanned work orders
- Mean time to restoration
  - Work orders with largest repair time
  - Instrumentation cumulative repair time
- Instruments with repeat repairs or multiple work orders
  - Repeat work order requests with no problem found result
- Total time out of service
  - In bypass (or override)
  - In manual mode (e.g., controller output in manual mode)

To collect failure information, a database is needed to log service time and other information defined in the data taxonomy. This database can be as simple as a spreadsheet or as complex as a computerized maintenance management system (CMMS). Data sources include:

- Equipment inspection records
- Preventive maintenance records
- Proof test records (e.g., functions as specified, fails to operate)
- Operational records (e.g., abnormal operation, process demand, spurious trip)

- Records from other installations (e.g., manufacturer, users, integrators, industry data collection efforts)
- Loss events (e.g., near miss and incidents)

Also needed is a collection method that is easy to follow, technicians motivated to correctly document the information, and people assigned responsibility for improving instrumentation reliability. Some owner/operators have reliability engineers specializing in instrumentation and controls, but all too often these people spend most of their time deal with on-going maintenance issues rather than working to improve reliability. If the collection method is too complex or onerous, the data quality will suffer. Technicians need to understand why they are collecting the information, and they need procedures and training on how to create quality records.

Usually the determination of whether the device failure is safe or dangerous is not practical for the person executing maintenance. The effect seen by the maintenance person may be the result of error trapping by the system.

> For example, *a dangerous failure may be detected by the system and configured to take the process to a safe state --- an inherently safer practice. In this example, the facility experiences a safe shutdown (otherwise referred to as a spurious trip), but the device failure is still dangerous*.

The maintenance person should record a description of the failure found when the device was initially inspected. The classification of this failure is best determined during data analysis by those familiar with the system architecture and configuration.

Once sufficient information has been collected, the good and bad actors can be identified, and plans can be formulated and implemented to eliminate the bad actors and improve reliability. Good actors are reliable technologies that have been proven through a volume of operating experience that they are fit for purpose. Good actors provide evidence that the requirements of prior use are met [3]. Understanding what makes a device a good actor can help identify the site practices needed across the lifecycle, such as specification, construction, installation, operation, and maintenance.

Bad actors are instruments that have repeated failures at a frequency inconsistent with design assumptions or operational needs. They are not only a reliability problem; they also increase operating and maintenance costs and consume maintenance resources. Turning bad actors into good ones generally requires a reduction in random and systematic failures. Typically a company will identify bad actors based on repeated failures, accumulated repair time, or a replacement cost threshold. Once identified, more detailed tracking may be needed to identify and resolve underlying issues with specification, design, installation, maintenance, testing, operation, or operating environment. Identifying bad actors and resolving underlying problems substantially improves equipment reliability.

3 Data Taxonomy

Collection of failure rate data requires a data taxonomy that is sufficiently detailed to support metrics. The taxonomy can be based on ISO 14224 [6], which provides a rather detailed taxonomy for all types of equipment. For the purposes of an instrument reliability program, the taxonomy can be very simple, such as the data required to determine the mean time between unplanned work orders or the mean time between failures based on service time and failure records. As bad actors are identified, the taxonomy can be expanded to collect additional information that supports more detailed understanding of the failure mechanisms.

The taxonomy only needs to be as detailed as necessary to track and trend failures so that bad actors can be identified. The taxonomy may include any or all of the following types of information:

- Equipment Taxonomy
  - Equipment functional location
  - Service (or operating environment) description
  - Tag number
  - Classification (e.g., control, safety, asset, production, quality or other)
  - Technology type (e.g., pressure transmitter, trip amplifier, safety PLC, fail-closed block valve)
  - Functional description – may be multiple
  - Total service time (i.e., cumulative time since last repair or replacement)
- Failure Taxonomy
  - How the failure was detected (e.g., operator observation, safety demand, spurious operation, diagnostics, inspection, and proof test)
  - Inspection or test findings
    - Failure description or mechanism (e.g., technology mismatched to the installation, instrument installed settings different from specification, device bypassed during operation, heat tracing left on in summer)
    - Failure mode (e.g., stuck in position, failed upscale/downscale, calibration drift, etc.)
  - Repair action
    - Preventive maintenance performed
  - Test performed to verify correct operation
  - Total restoration time

4 Failure Investigation

In an ideal world, there are limitless resources and unlimited time for analysis. In the real world, the level of investigation must be proportionate to the value of the lesson to be learned. Considerations for more in-depth investigation include:

- SCAI failure under test or demand
- Similar SCAI devices failing in different applications
- Cost impact of SCAI failure
- Safety or environment impact of SCAI failure
- Systematic failures impacting multiple devices

When repeated failure of SCAI is found, a root cause analysis is generally conducted to ensure that the corrective actions are sufficient to prevent it from reoccurring. The instrument reliability program should identify the level of data capture and analysis that should be performed for different types of events, such as when an in-depth investigation is warranted, what resources should be applied, and how to escalate an instrument reliability problem.

Investigations of loss events involving automation failures are typically the responsibility of the environmental, safety, and health organization of a company. Working with them to identify and categorize automation failure helps to ensure consistent failure reporting.

5 Verification

When analyzing the failure data, the objective is to verify that the equipment used meets the performance requirements. The instrument reliability program should receive sufficient data and information from the operational and maintenance records to demonstrate that the actual failure rate is less than the failure rate assumed in the performance calculation. This is accomplished by:

- Ensuring repairs are being done within the mean time to restoration (MTTRes)
- Investigating repeat “no problem found” work orders to prevent normalization of failure
- Responding to repeat failures and taking action to prevent reoccurrence
- Understanding unexpectedly low failures (for positive learning)
- Eliminating systemic failures

Determining the point at which corrective action should be taken involves understanding the degree of uncertainty inherent in the performance requirement established in the risk analysis [8, 9, 10] and in the uncertainty in the performance calculation [11]. When the risk analysis finds risk reduction gaps that must be closed with new or revised protection layers, management often questions [9]:

- What is the uncertainty in the risk analysis results?
- How sensitive are the results to the underlying data?
- How conservative is the risk analysis methodology?
- Should additional protection layers be implemented to provide fault tolerance against a single point of failure?

The risk analysis can be performed qualitatively, semi-quantitatively or quantitatively. The use of numbers and math can make the analytical process seem more certain than it really is. The

analytical methodology actually introduces error in the estimate. For example, most commonly applied risk analysis methods yield values within a factor of 2 to 3 of each other when the same assumptions are made and the methods are properly applied with reasonable input data. The risk estimate can also be significantly wrong if the input data does not reflect the actual operating history.

All of the reliability parameters used in the performance calculation have some degree of uncertainty; generally the more removed the data source is from the actual application, the more uncertain it is that the design achieves the target performance. When redundancy schemes are used, the impact of the uncertainty becomes non-linear. Because of the uncertainty in the reliability parameters and calculation, the design verification should include a safety margin to improve the likelihood that the installation works as intended. It is recommended that this safety margin be defined as a site requirement as part of the functional safety management system. Otherwise, it is likely that each design will differ significantly in the way that risk is controlled and uncertainty is managed.

Uncertainty analysis is useful where there is a lack of confidence in the data. Perceived performance differences may be well within the expected band of uncertainty. Making changes to the implementation in this circumstance will not improve risk and would create an unnecessary opportunity for the commission of a systematic failure.

Standard ranges of failure rates from CCPS [12] can be used as inputs to a variance contribution analysis to determine the typical uncertainty ranges. Freeman [13] showed that the 90% uncertainty band for a SIS designed to provide a risk reduction in the middle of the SIL range nearly spans the full range for that SIL. Table 3 provides the 90% upper and lower confidence limits for SIL 1 to 3.

Table 3. 90% Upper and Lower Confidence Bounds on Design RRF [Freeman 2013]

SIL	**Target Risk Reduction Factor**	**90% Lower Limit**	**90% Upper Limit**
1	50	12	85
2	500	123	847
3	5000	1247	8475

An extension of Freeman's results [2013] would suggest that if the middle of the SIL range is selected as the design target a deviation of 20%-30% in any maintenance reliability parameter is unlikely to significantly impact the certainty that the desired risk reduction is being provided. Any time the actual failure rate exceeds the design assumptions by more than this amount, further analysis should be done, corrective actions taken against the underlying causes. The design calculations must be revised if the performance deficit cannot be resolved.

Regardless of the selected confidence limits, the risk reduction calculated based on the upper bound will always be less than (or worse) than the performance based on calculations using the mean value of the parameters [11]. The hazards and risk assessment establishes the minimum

required risk reduction based on what is needed to manage the process risk to a tolerable level within the company's functional safety management system. The safety requirements specification should define the target risk reduction with a safety margin, which ensures that given the potential uncertainty of the equipment performance that the function still provides the minimum required risk reduction. Good engineering practice is to assure a high probability of successful operation when the process demand occurs.

6 Summary

An effective instrument reliability program leverages existing systems to collect quality data and to monitor performance metrics. An on-going instrument reliability program that seeks to continuously improve performance should address bad actors, excessive failure rates, unusual failure modes, and recognized systematic failures. Records need to be traceable to specific equipment, so negative trends can be corrected at their source. The actions taken to turn around negative metrics can include design and/or management system changes. An instrument reliability program yields a return on investment through improved safety and reliability.

7 References

[1] CCPS. *Guidelines for Process Safety Metrics.* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2010.

[2] ANSI/ISA. *Identification and Mechanical Integrity of Safety Controls, Alarms and Interlocks in the Process Industry,* ANSI/ISA-84.91.01-2012. Research Triangle Park: ISA. 2012.

[3] IEC. *Functional safety: Safety instrumented systems for the process industry sector - Part 1-3.* IEC 61511. International Electrotechnical Commission, Geneva, 2015.

[4] ISA. *Guidelines for the Implementation of ANSI/ISA 84.00.01- Part 1,* TR84.00.04-2015. The International Society of Automation, Research Triangle Park, NC, 2015.

[5] ISA. *Mechanical Integrity of Safety Instrumented Systems (SIS),* TR84.00.03-2012. The International Society of Automation, Research Triangle Park, NC, 2012.

[6] ISO. *Petroleum, petrochemical and natural gas industries - Collection and exchange of reliability and maintenance data for equipment,* 14224:2006. International Organization for Standardization, Geneva, 2006.

[7] ISA. *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions,* TR84.00.02-2015. The International Society of Automation, Research Triangle Park, NC, 2015.

[8] Freeman, Raymond. "What to Do When Nothing Has Happened." Process Safety Progress, pp. 204-11, September 2011.

[9] Freeman, Raymond. "Quantifying LOPA Uncertainty," Process Safety Progress, pp 240-247, September 2012.

[10] Freeman, Raymond. “Simplified Uncertainty Analysis of Layer of Protection Analysis Results,” Process Safety Progress. Vol 32, No 4, pp. 351-360. December, 2013.

[11] Freeman, Raymond and Angela Summers. “Evaluation of Uncertainty in Safety Integrity Level (SIL) Calculations.” Paper presented at 11th Global Congress on Process Safety, Austin, TX, April 27-29, 2015.

[12] CCPS. *Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis*. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2014.

[13] Freeman, Raymond. "Impact of LOPA Uncertainty on Safety Instrumented System Design." Paper presented at Texas A&M 16th Annual International Symposium. College Station, TX, October 22-24, 2013.