White Paper for 2010 Mary Kay O'Connor Safety Center International Symposium

Effective Management of PSM Data in Implementing the ANSI/ISA-84.00.01 Safety Lifecycle

Carolyn Presgraves, CFSP of
AE Solutions, Greenville, SC USA
Carolyn.Presgraves@aesolns.com

Introduction

Throughout the evolution of Process Safety Management (PSM) engineering, Operations and Maintenance personnel have participated in the identification of process hazards and the mechanisms in place to prevent those hazards. Prevention mechanisms have included both active and passive engineered systems and administrative measures such as relief valves, procedures, operator alarms, Basic Process Control Systems (BPCS) interlocks, and Safety Instrumented Systems (SISs). Process Safety Information (PSI), Mechanical Integrity (MI), Operating Procedure, and Training requirements of 29 CFR 1910.119 provide guidance for many of these prevention mechanisms.

Specifically applicable to the topic of this paper and conformance with ANSI/ISA-84.00.01, PSI requirements for safety systems include complete documentation of the design basis and specification data in accordance with recognized and generally accepted good engineering practices (RAGAGEP). The MI section requires the inspection and testing of safety systems according to recognized and generally accepted good engineering practices, maintenance of testing records, and documented correction of any identified deficiencies.

In June 2007, OSHA issued directive CPL 03-00-004 implementing the Petroleum Refinery Process Safety Management National Emphasis Program. The directive contained specific references to Safety Instrumented Systems and requirements to document all related PSI and maintain them in accordance with the MI portion of the standard and RAGAGEP. The directive also reinforced OSHA's recognition of ANSI/ISA-84.00.01 as RAGAGEP first identified in writing as early as 2001 in a letter of interpretation.

Working to define specific requirements for SIS design and performance, the International Society for Automation (ISA) drafted a performance-based standard, ANSI/ISA-84.01-1996, "Application of Safety Instrumented Systems for the Process Industries." In 2004, ISA adopted the international standard IEC 61511, including a modification to cover systems installed prior to the adoption of the IEC language, ANSI/ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod), "Functional Safety: Safety Instrumented Systems for the Process Industry Sector." Since that time the ANSI/ISA-84.00.01 standard has been widely held to be the compliance target for SIS design in the process industry. While the requirements included in OSHA 1910.119 do not specifically mandate compliance with the ANSI/ISA-84.00.01 (IEC 61511 Mod), two published letters from OSHA to the ISA from March 2000 and November 2005 indicate the performance-based standard can be used as guidance. The 2005 communication from OSHA goes on to say that the ANSI/ISA-84.00.01 standard is RAGAGEP, and the ANSI/ISA-84.00.01 standard could be used as evidence in incident investigations.

As a result of 1910.119 and the interpretations taken by OSHA, an increasing number of organizations have identified the ANSI/ISA-84.00.01(IEC 61511 Mod) standard as their target for compliance with the relevant PSI and mechanical integrity requirements of OSHA 1910.119. Because ANSI/ISA-84.00.01 is a standard for Safety Instrumented Systems, it is often an organization's instrumentation group or automation engineers who are tasked with achieving ANSI/ISA-84.00.01 compliance. Frequently this effort is attempted with very little interaction between the traditional PSM groups and the instrumentation and automation groups. While the base requirements of Safety Integrity Level (SIL) verification, Specification Documentation, Implementation, and Testing can be performed in this isolated fashion, it is not the optimal execution approach for long term sustainability. This paper will examine efficiencies that can be gained by effective PSI and MI data management and coordination.

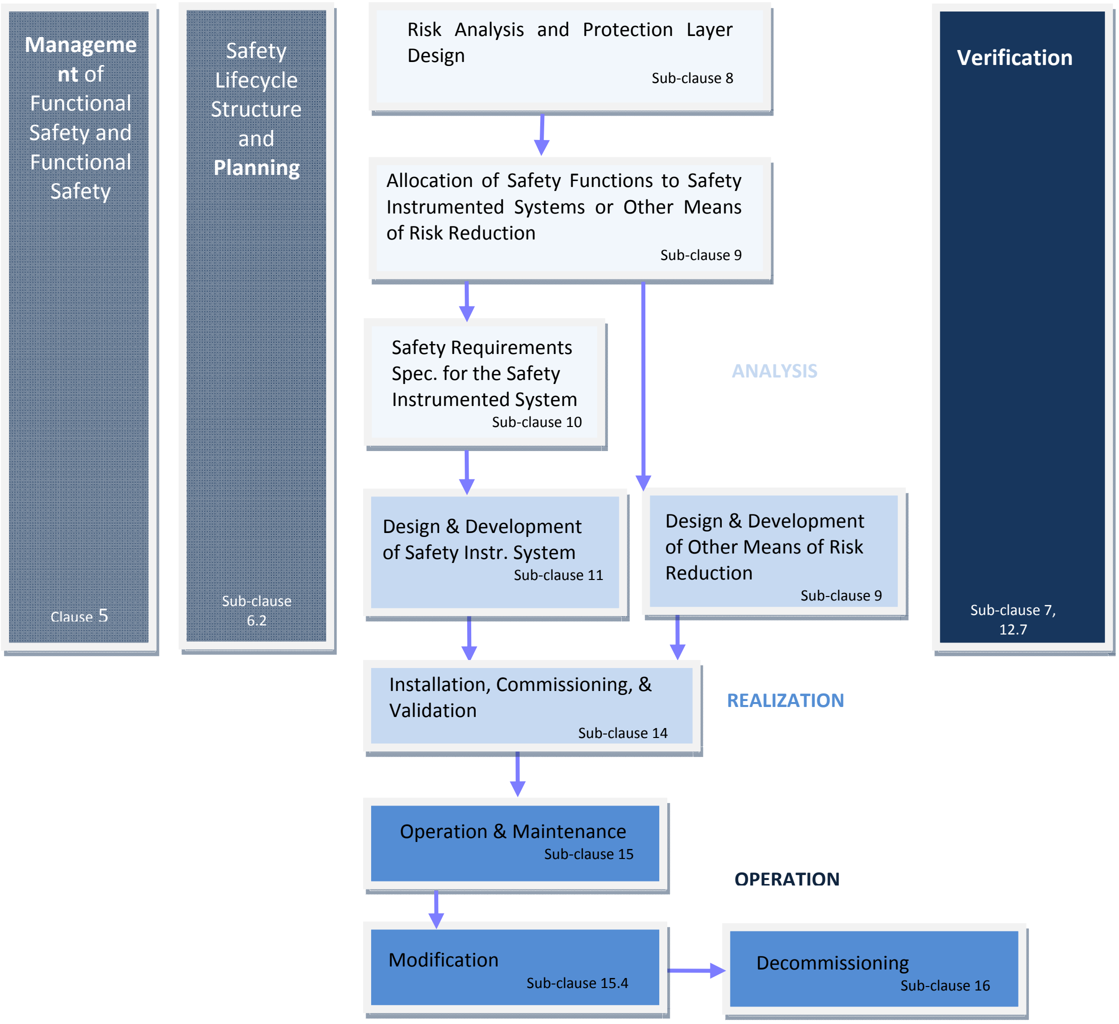
Management of Functional Safety and Functional Safety
Clause 5
Safety Lifecycle Structure and Planning
Sub-clause 6.2
Risk Analysis and Protection Layer Design
Sub-clause 8
Allocation of Safety Functions to Safety Instrumented Systems or Other Means of Risk Reduction
Sub-clause 9
Safety Requirements Spec. for the Safety Instrumented System
Sub-clause 10
ANALYSIS
Design & Development of Safety Instr. System
Sub-clause 11
Design & Development of Other Means of Risk Reduction
Sub-clause 9
Verification
Sub-clause 7, 12.7
Installation, Commissioning, & Validation
Sub-clause 14
REALIZATION
Operation & Maintenance
Sub-clause 15
OPERATION
Modification
Sub-clause 15.4
Decommissioning
Sub-clause 16

Figure 1 - ANSI/ISA-84.00.01 SIS Safety Lifecycle

The ANSI/ISA-84.00.01 SIS Safety Lifecycle

The SIS safety lifecycle as defined in ANSI/ISA-84.00.01 begins with the traditional PSM activity of Hazard Identification and Risk Analysis and follows identification and evaluation of the layers of protection used to prevent those hazards. One of the key protection layer types is the Safety Instrumented Functions (SIFs) provided in the SIS. The remaining phases in the SIS Safety Lifecycle provide guidance to ensure proper design, validation, verification, and maintenance of the SIS to ensure it continues to provide the risk reduction identified in the Layer of Protection Analysis (LOPA), or equivalent target integrity level assessment. At each of these phases there are key benefits to having a comprehensive data management system that ties these phases together and provides accurate access to data from the other phases.

Analysis

As illustrated above, the risk analysis activities traditionally begin with Process Hazard Analysis (PHA). To support identification of the requirements of the SIS, the ANSI/ISA-84.00.01 lifecycle follows the PHA with allocation of protection layers for a specific amount of risk reduction credit. The identification and credit of safeguards has always been part of a PHA with emphasis on qualitatively risk ranking both severity and likelihood of a harmful event.. Through the use of semi-quantitative or quantitative methodologies such as Layer of Protection Analysis (LOPA) or Fault Tree, a more thorough analysis is documented of the integrity of each protection layer and the probability of failure. Using both methods, i.e. PHA and LOPA, a company can assess the existing mitigated hazardous event likelihood against their target mitigated event likelihood (TMEL) in accordance with the organization's risk matrix. Where a gap exists between the existing mitigated event likelihood and the TMEL, a SIF may be used to provide the additional risk reduction. The size of the gap establishes the design basis of the SIF as SIL1, SIL2, SIL3, or SIL4 system.

The Safety Requirements Specification (SRS) documents the design basis requirements of the SIS to meet the SIL selection specified in the LOPA. The SRS document also includes diagnostic requirements and bypassing requirements for use in the design of the SIS. Proper data management and connectivity between the tools used for the PHA/LOPA and the tools used for the SIS design, including the SRS, ensure that the targets for risk reduction are accurate and allow automated updating of downstream data when any changes occur in the PHA/LOPA data. Maintaining the Safety Requirements Specification in a comprehensive data management system offers dramatic benefits over having a static document in terms of management of change, searchability, scalability, flexibility in reporting, and automated checking of the system design—and ultimately actual performance—against the stated requirements.

Clause 10 of the ANSI/ISA-84.00.01 standard also requires a Functional Specification be defined to specify the performance of the SIS. Cause and Effect diagrams are a common method of fulfilling this requirement. Many organizations are also using these Cause and Effect documents to identify where the critical SIFs, interlocks, and alarms are within the system, including identifying which named SIF(s) the Cause and Effect is depicting. They are considered foundational documents by process engineers developing and maintaining safe upper and lower limit tables with consequences of deviation and intended automated actions. Proper data management can assist in creating Cause and Effect documents with such references and in maintaining these records in an efficient manner. If the Cause and Effect document is electronically tied to the PHA/LOPA data, updates to SIL targets as well as documentation of critical interlocks and alarms can be implemented in an automated fashion, increasing efficiency while reducing error.

Realization

The realization activities specified in the standard provide requirements for device selection and SIL verification calculations. These activities are more obviously connected to the LOPA data as they directly verify that the SIL selected in the LOPA is being achieved by the SIF architecture selected and the devices chosen.

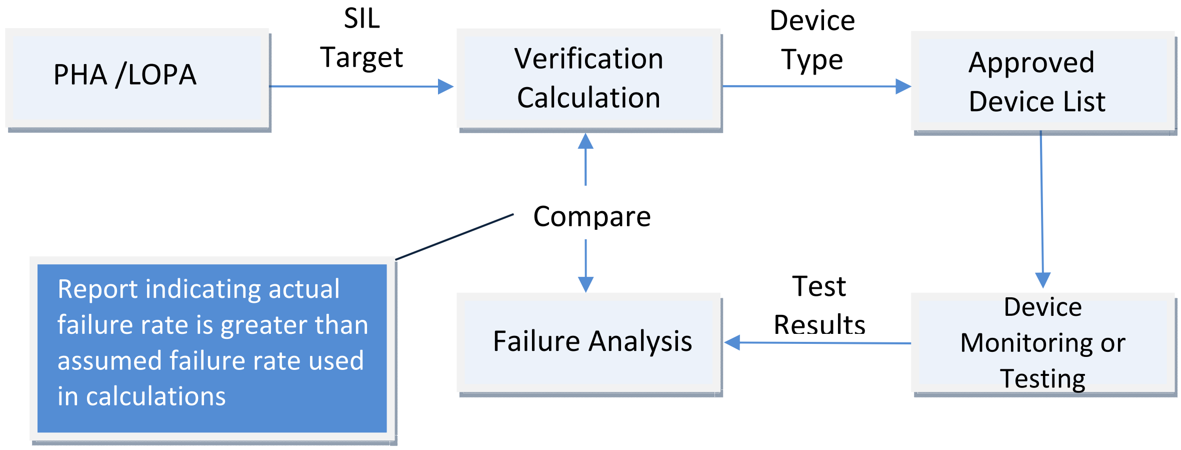
PHA /LOPA
SIL Target
Verification Calculation
Device Type
Approved Device List
Compare
Report indicating actual failure rate is greater than assumed failure rate used in calculations
Failure Analysis
Test Results
Device Monitoring or Testing

Figure 2 - Managed Data Connections Supporting SIL verification

As with the SRS, the SIS design activities can benefit from access to the PHA/LOPA data to more effectively identify the source of the requirements and more efficiently process any changes to those risk reduction requirements. In addition to the risk analysis, SIS design can benefit from automated connections to the asset management system by validating device selection. Connections between these systems can facilitate maintaining common equipment and applying the most accurate failure rate data available to all analysis within a facility or organization, whether it is a result of project work or a revalidation.

Operation

The requirements of the ANSI/ISA-84.00.01 lifecycle extend beyond analysis and realization into the operation of the process. Operators must be trained in the operation and requirements of the SIS and have access to the information required to maintain the SIS in a way that supports fulfillment of the requirements defined in the Risk Analysis and the SIL Selection process. Proper data management tools can support Operations and Maintenance personnel activities. Availability of the data in an accessible format also supports active reporting and management of metrics which communicate the overall health of the risk management system. Examples that illustrate this point include override/bypass reporting, overdue proof testing of safety functions, and trending of “as found” conditions in a dangerous fault state.

During normal maintenance operations it may be necessary to override or bypass safety functions for a number of conditions such as maintenance on equipment or system start-up. Proper identification and visibility of the risk management gap created by these activities can support this by raising the awareness of risk to personnel involved and by providing automated alerts.

It is also a requirement of the standard that all assumptions made in the SIL verification calculations be validated by tracking actual process data. Time in bypass is tied to the Mean Time to Repair (MTTR) value used in the SIL verification analysis. If actual time in bypass is much greater than the assumption used in the calculations, this also creates a gap in risk prevention, causing the SIF to not perform up to the SIL calculated in during SIL verification.

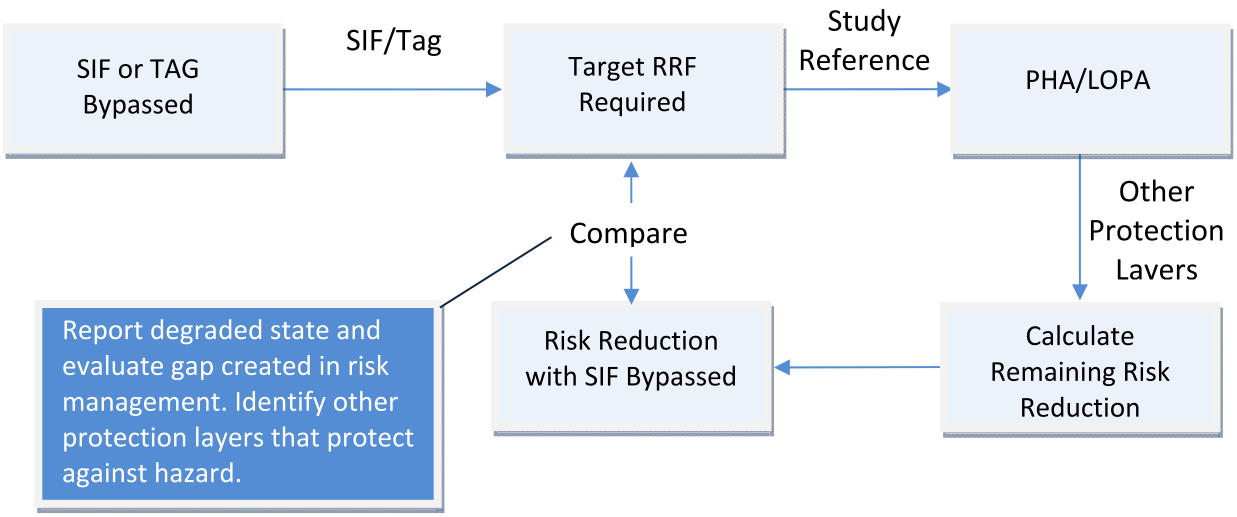
SIF or TAG Bypassed
SIF/Tag
Target RRF Required
Study Reference
PHA/LOPA
Other Protection Lavers
Calculate Remaining Risk Reduction
Risk Reduction with SIF Bypassed
Compare
Report degraded state and evaluate gap created in risk management. Identify other protection layers that protect against hazard.

Figure 3 - Bypass Reporting Supported by Data Management

Proof Tests or Functional Test Plans (Clause 16 - SIS Operation and Maintenance) may differ from standard maintenance and calibration tests in that the goal is not strictly to ensure the device is operating correctly, but that it is functioning correctly for the SIF. Proof testing should be designed to specifically reveal undetected failures of the equipment such as testing for a plugged process tap. Merely calibrating a device may not reveal this failure, but a properly written Functional Test Plan would include specific tests to reveal this failure. The general premise of Proof Test or Functional Test Plans is to reduce the probability that a SIF will fail on demand by detecting some of those failures during a periodic test.

The proof test interval is part of the SIL verification calculation. Sub clause 11.9 of ANSI/ISA-84.00.01 requires that the SIL verification be completed to ensure the requirements stated in the Safety Requirements Specification are met. Proper data management comes into play in verifying that the proof tests are being completed on the interval used in the SIL verification calculations (sub clause 16.3). A risk management gap may be created when testing frequencies do not meet those requirements.

Planning, Management, and Verification

Maintaining the data for the Analysis, Realization, and Operation phases of the Safety Lifecycle greatly improves the efficiency and effectiveness of the Planning, Management and Verification phases. These phases exist at all stages of project or revalidation execution.

Safety Lifecycle planning involves identifying the mechanisms, tools, and timing for the elements of the ANSI/ISA-84.00.01 standard to be completed. A comprehensive data management system that connects risk analysis tools to SIS design tools and the asset management and maintenance systems helps solidify and maintain proper workflow across the organization. The automated checking between these systems made possible with a comprehensive data management system supports verification.

User security and system access can be employed to enforce the safety planning requirement of having competent personnel involved in each step. Having a common location for PSM and SIS data also supports the safety management activities of the functional safety assessment. The electronic logging of who made each change, when they made it, and who approved it provides the audit trail to support verification of each step. Automated reporting can also be used to identify missing components in the lifecycle, as well as provide project tracking to support effective project execution.

A comprehensive data management approach to the Safety Lifecycle also strengthens Management of Change (MOC) controls by enforcing certain workflows and ensuring proper updates across process safety documents and throughout the project lifecycle. Centrally located data allows cross checking ensuring accurate updates are made, as well as providing a single storage location for data. For example, if one software package is used for risk analysis, another for documenting the SRS, another for SIL verification calculations, and a separate system to track maintenance requirements, any update to that selected SIL must be changed in all those locations. A comprehensive data management solution allows electronic references and automatic data transfers to reduce duplicate storage locations for data and provide simultaneous updates to connected systems when changes are made.

All four of the main areas of the SIS Lifecycle depend heavily on the data developed during the first phases of Process Hazard Analysis and Protection Layer Allocation. The greater the access to that data at each of the subsequent phases, the greater the effectiveness of the Analysis, Realization, Operations, and Management activities.

Key PSM Input and Impact

The ANSI/ISA-84.00.01 lifecycle applies to existing installations as well as capital improvement projects and new installations. At a minimum this lifecycle must be revisited every five years through a PHA revalidation. Each revalidation can lead to changes in SIL requirements through modified risk targets of the organization, procedure updates regarding credits taken, or updated information on initiating cause frequencies.

Example of Procedural Updates: During the previous revalidation, operator response to alarms had been taken as an order of magnitude risk reduction in many scenarios. Since that study the organization had adopted new corporate guidelines tightening the requirements for credit taken on operator response to alarms; this occurred in conjunction with an organizational change involving reassignment of operator responsibilities. As a result, several scenarios in the revalidation required that the integrity level of the applicable Safety Instrumented Functions increase from SIL 1 to SIL 2. Following the Safety Lifecycle of ANSI/ISA-84.00.01,the new results of the PHA and LOPA activities flow through to adjusted requirements in the SRS, a different SIF design and SIL calculation, with a potential change in maintenance requirements and testing frequency. A comprehensive data management system that connects the tools used throughout the SIS Lifecycle greatly improves the efficiency with which this change can be made. This improved efficiency is manifested in a number of ways, from automated reporting that can summarize the effect of the changed LOPA criteria on the health of the risk management system, to automated updates, to documentation such as the SRS, Cause and Effects, Test Plans, and the scheduled preventive maintenance on the affected SIFs.

The example cited above demonstrates changes to the SIL requirements caused not by changes to the process or equipment but by other PSM-related changes. There are also SIL requirements that are affected by capital project work. An upgrade to a section of piping may lower the SIL requirement for the overpressure SIF protecting that section. A change in the normal operating range may increase the SIL requirement of a SIF protecting against over-temperature. The addition of new equipment may change the SIL requirement of SIFs in the tie-in area. While it is automatic and intuitive to most PSM professionals that Process Safety Assessments or PHAs be performed early in these projects as a measure of management of change, the trigger to evaluate the SIS-specific impacts of the project is often considered late in project execution. Consideration and evaluation of these impacts earlier in the project can prevent delays caused when the project is forced to pause while these activities are completed or costly redesign when the existing SIF is discovered to be inadequate. SIF design can impact layout of equipment, SIF device selection, and SIS logic solver selection. Comprehensive management of the PSM and SIS data can facilitate evaluation of project impact at each phase of the ANSI/ISA-84.00.01 SIS Lifecycle, as well as support the iterative process which is the real-world experience of project execution. Changes to the SIS required to meet SIL may prompt re-evaluation of other potential protection layers, which may again change the SIL requirement of the SIF, resulting in updated SIL verification calculations.

Device Identification in PSM Documentation

One of the obstacles faced by organizations striving for a more comprehensive system for managing their PSM data and ANSI/ISA-84.00.01 compliance data is the variation in device identification between systems. P&ID device labels and tag names used in the PHA/LOPA studies do not always match the tagging conventions used in the Asset Management System, which also may not match the system used by the data historian for real-time system tracking and collection of first-out indicators.

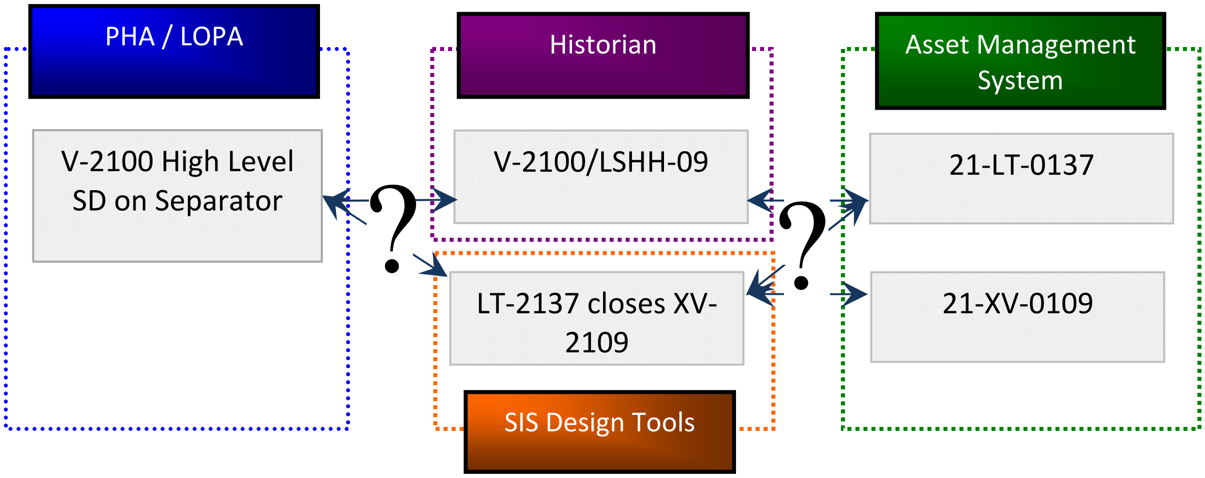

Figure 4 - Connectivity Issues Between Systems Using Different Syntax for Tagname Identification

There are several options for bridging the data gap in device identification:

- Include the unique device names specifically in PHA/LOPA activities
- Create a cross reference that translates “V-2100 High Level SD on Separator” into its components
- Use tag-based tools which allow assignment of individual devices to the text descriptions in the PHA/LOPA study

As critical as it is to create this data connection between the content in the risk studies, the verification and design components of the SIS, and actual performance of the devices in the field, it is equally important to allow the PHA and LOPA teams the appropriate flexibility to identify equipment, initiating causes, and protection layers. For example, a system that forces users to select initiating devices from a drop-down list of equipment already loaded in the system would have to include a mechanism for new entries to be made during execution of the study to account for new equipment identification. Often during initial PHAs for projects, tag names for new equipment have not yet been selected. Organizations have taken several approaches to device identification:

- Text entry during the PHA/LOPA followed by assignment of specific devices to the cause or protection layer at a later time. This allows maximum flexibility during the PHA/LOPA meetings but requires follow-up activities by additional resources. It also introduces the possibility that the resources assigning the devices interpret the notations from the study incorrectly and identify the wrong tag names.
- Procedures requiring tag assignment at an early stage in the design process. This generally leads to a lot of device tag names being pulled for projects and never used, but does cut down on reassignment issues that affect everything from P&IDs to SIL calculations and instrument lists.

- Indentifying unique tag names in the PHA and LOPA documentation. With this method placeholders are used for new devices and then updated after the actual tag name is assigned.

Connectivity Between Systems
There are important benefits, in addition to allowing systems to connect appropriately, to properly identifying devices from the risk study. Risk-based management has been identified as a way to reduce costs and make the most effective use of maintenance and operation time and resources. The information concerning which Safety Instrumented Systems and basic process control components are most critical in risk management is buried in the PHA and LOPA data. Exposing and connecting that data to other management systems in an organization through automated and electronic tools can enhance the capabilities of an organization to correctly identify and maintain those devices which are most critical in the risk management systems. To affect a risk-based management strategy as well as support the ANSI/ISA-84.00.01 SIS lifecycle, it is key to capture device specific identification for:

- Initiating causes named in the PHA/LOPA
- SIF-type protection layers implemented in the SIS
- BPCS protection layers such as interlocks
- Operator alarms and the sensing devices detecting the deviation
- Other protection layers that involve process equipment such as relief valves

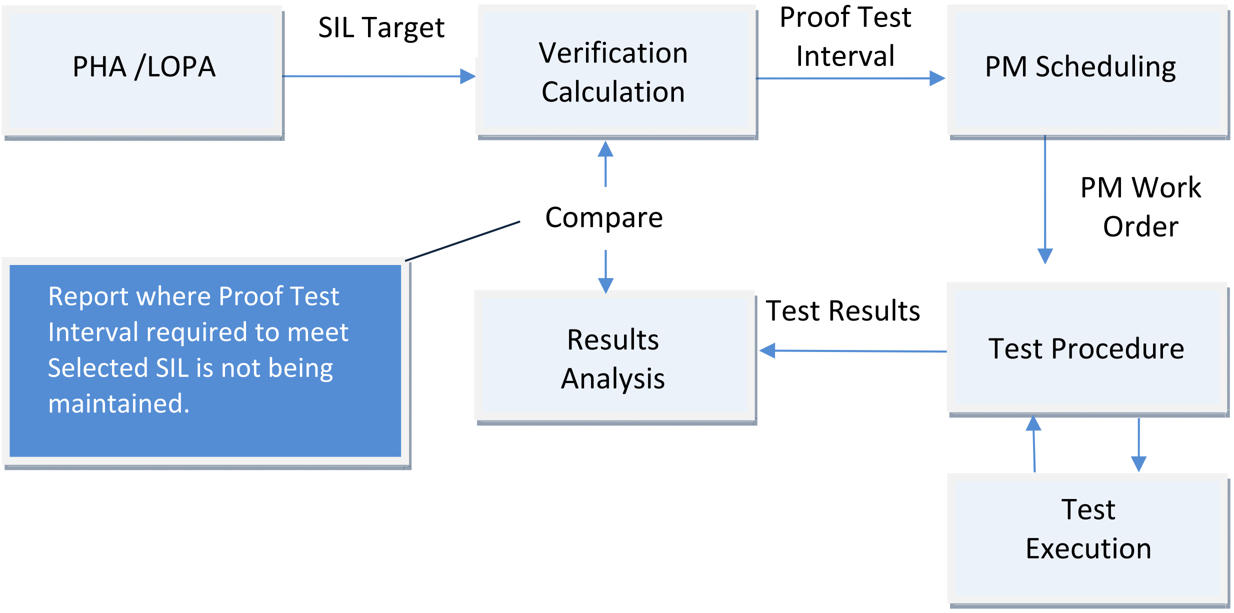

Figure 5 - Comprehensive Data Management Used to Verify Proof Test Intervals

Certain requirements of the ANSI/ISA-84.00.01 standard are difficult to achieve without a comprehensive data management system. Specifically, the requirements that involve periodic review and validation of the assumptions made during the PHA and LOPA studies and assumptions used during the SIL verification calculations illustrate this point. Examples of these PSM data-related activities required by the ANSI/ISA-84.00.01 standard include:

- Validate causes named in PHA scenarios and identify any new causes that need to be evaluated (section 16.2.6)
- Track actual demand rates (events that require SIS to respond) to compare to rates assumed in the PHA/LOPA (section 5.2.5.3)
- Ensure Proof test intervals from original calculations are still valid (section 16.3.1.5)
- Track actual failure rates to validate assumed rate in original verification calculations (section 5.2.5.3)

A key step in implementing effective management of PSM data and maintaining compliance with the ANSI/ISA-84.00.01 standard is to establish a device identification convention and utilize tools that will facilitate communication and reporting between the risk analysis, system design and verification, and maintenance and tracking systems.

Identification of Leading Indicators

In addition to supporting the requirements of the ANSI/ISA-84.00.01 standard, a key benefit of cohesive data management for PSM and Safety Lifecycle data is the enhancement of leading indicators that can be used to gauge process safety health and respond proactively to negative trends. Maximum leverage of these leading indicators can only be achieved through proper identification and tracking of devices used in the risk management strategy. This begins as mentioned earlier with the proper identification of equipment involved in critical protection layers. When the PHA and LOPA identify unique equipment tags or other identifiers matching those used by the applications used for SIS design, and equipment maintenance and monitoring, a direct correlation between the assumptions made and the real-world performance of the equipment is possible.

Centralized reporting can bring attention to negative trends and allow action to be taken to improve risk management prior to an incident occurring. Such visibility is not possible without proper data management and connectivity between these systems.

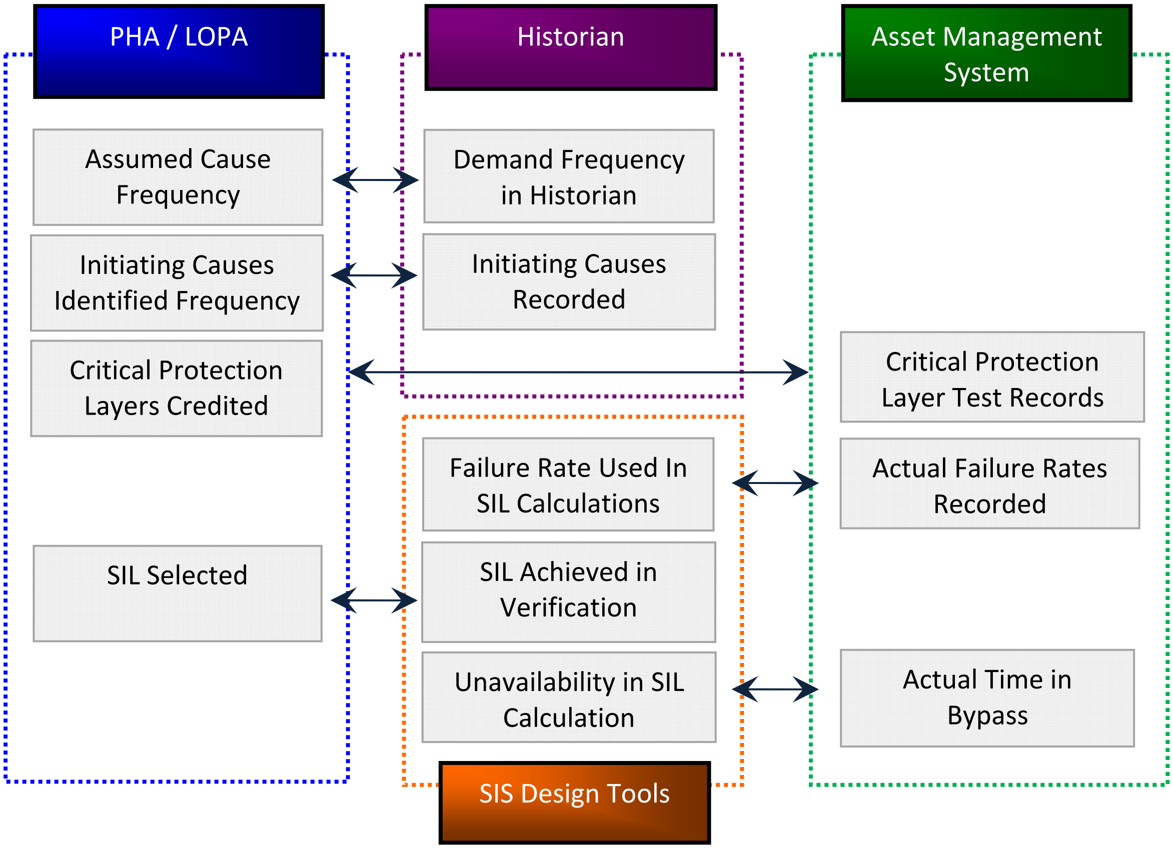
PHA / LOPA
Historian
Asset Management System
Assumed Cause Frequency
Demand Frequency in Historian
Initiating Causes Identified Frequency
Initiating Causes Recorded
Critical Protection Layers Credited
Critical Protection Layer Test Records
Failure Rate Used In SIL Calculations
Actual Failure Rates Recorded
SIL Selected
SIL Achieved in Verification
Unavailability in SIL Calculation
Actual Time in Bypass
SIS Design Tools

Figure 6 - Key Leading Indicators that Can Be Monitored with Proper Data Management

Another benefit realized by organizations establishing proper data management between the tools used for Analysis, Realization, Operation, and Management is the ability to apply risk-based maintenance strategies to the non-SIS components of their risk management systems. Through the same tools used to connect SIS components back to the Risk Analysis data showing the hazard and severity of the hazard that the SIS components are preventing, similar analysis for BPCS interlocks and operator alarms is possible. With increased emphasis on alarm rationalization the benefit of having severity information linked to the alarms allows for an automated analysis of prioritization.

In Summary

Proper management and effective use of data from the Analysis, Realization, Operations, and Management phases can be key in achieving compliance with the ANSI/ISA-84.00.01 standard for Safety Instrumented Systems as well as maintaining the health of process safety management systems. A common method for identifying devices is required to facilitate tracking of the risk targets, from Design and Verification, to Maintenance and Operations, and back to the next Risk Assessment cycle. Electronic data connections between the systems and tools used for these activities, or use of common tools where possible, can enhance the efficiency of the work flow process. Common tools and reporting can support management tracking and response to leading indicators as well as promote awareness of maintenance or project activities on the risk management system. Implementation of better data management processes and tools is an effective step toward reducing the overall risk exposure of an organization.

REFERENCES

1. ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) Functional Safety: Safety Instrumented Systems for the Process Industry Sector, The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 20041996.
3. IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Parts 1-3, Geneva: International Electrotechnical Commission, 2003.
4. U.S. Department of Labor, Occupational Safety and Health Administration (OSHA), Federal Regulation 29 CFR 1910.119, Process Safety Management of Highly Hazardous Chemicals, Explosives, and Blasting Agents; Final Rule, February 24, 1992
5. U.S. Department of Labor, Occupational Safety and Health Administration (OSHA), Directive Number CPL 03-00-004, Subject: *Petroleum Refinery Process Safety Management National Emphasis Program, June 2007*
6. "03/23/2000 - Compliance with PSM and ANSI/ISA-S84.01 for safety instrumented systems" March 2000 Letter from Richard E. Fairfax, Director, Directorate of Enforcement Program, OSHA to Ms Lois Ferson of ISA.
7. "11/29/2005 - Use of ANSI-ISA S84_00_01-2004 Parts 1-3 (IEC 61511 MOD) to comply with OSHA's Process Safety Management standard" November 2005 Letter from Richard E. Fairfax, Director, Directorate of Enforcement Program, OSHA to Ms Lois Ferson of ISA.