HOW EFFECTIVE ARE YOUR SAFETY CONTROLS, ALARMS, AND INTERLOCKS?

The Importance of Functional Safety Auditing

Monica Hochleitner, Senior SCAI Consultant
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034
mhochleitner@sis-tech.com

Eloise Roche, Senior SCAI Consultant; Angela E. Summers, President
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034
eroche@sis-tech.com, asummers@sis-tech.com

Prepared for Presentation at
American Institute of Chemical Engineers
2016 Spring Meeting
12th Global Congress on Process Safety
Houston, Texas
April 11-23, 2016

AIChE shall not be responsible for statements or opinions contained
in papers or printed in its publications

HOW EFFECTIVE ARE YOUR SAFETY CONTROLS, ALARMS, AND INTERLOCKS?

The Importance of Functional Safety Auditing

Monica Hochleitner, Eloise Roche, and Angela Summers
SIS-TECH Solutions, LP
Houston, TX

Keywords: Auditing, Management Review and Continuous Improvement, Safety Instrumentation Systems

Abstract

Some organizations invest thousands, sometimes millions, of dollars on automation systems in safety applications with the desire to minimize the risk of their enterprise. However, spending dollars does not mean that the plant will reach the desired degree of safety after implementation. Return on investment in safety controls, alarms, and interlocks (SCAI) can be negatively impacted by human error, such as inadequate design, installation, testing, maintenance, and operation of the automation systems. These human errors are systematic failures that can be reflected throughout a site. Organizational discipline and administrative controls are needed to identify and correct these failures.

This paper will discuss important aspects of process safety management and how they are connected to the effectiveness of the SCAI. Functional safety auditing specifically looks at the management systems and procedures required to keep SCAI working effectively. The case studies presented will illustrate how safety system effectiveness could have been improved if a detailed audit of the SCAI documentation and performance records had been conducted and the findings addressed in a timely fashion.

1 Introduction

Many countries have been implementing industrial incident prevention systems over the years. In 1982 the EU adopted a European Council directive, known as the Seveso Directive, containing specific requirements on Process Safety Management (PSM). In 1992 the OSHA PSM regulation was enacted in the USA. After inherently safer design strategies are applied to the process, functional safety through the application of SCAI is often used to manage some or all of the remaining risk.

SCAI projects commonly require significant investment during the analysis and implementation phases. Generally hundreds of engineering hours are used to brainstorm hazard scenarios and identify safety gaps. Even more engineering hours are dedicated to calculate the best way to resolve those gaps.

Numerous industry standards and practices have been published to address different aspects of instrumentation and controls from basic electrical safety through performance-based standards for alarm management, SCAI implementation, and safety instrumented systems (SIS). The international standard IEC 61511 [1] is widely referenced even in countries that do not have specific process safety regulations. In the USA, ANSI/ISA 84.00.01 (the USA adoption of IEC 61511) has been categorized by OSHA as a recognized and generally accepted good engineering practice (RAGAGEP) for SIS. For the purpose of clarity, all clause references made within this paper are to the normative clauses in IEC61511-1 Edition 2.0 Final Draft Industry Standard (FDIS). Similar to ANSI/ISA 84.00.01, ANSI/ISA 84.91.01 [2] and ISA 84.91.03 (draft) [3] provide requirements for safety controls, alarms, and interlocks (SCAI) in general. Functional safety audits are required for all SCAI (of which SIS is a subset), so the rest of this paper will refer to the more general term, SCAI.

Designing SCAI per these standards is not enough. Even if the risk allocation and SCAI specification are performed precisely in accordance with the industry standards and practices for safe automation, this is not a guarantee that process safety risk will remain adequately managed. If assumptions made during these early safety lifecycle phases are not consistent with reality, or if the activities that must be performed periodically are not sustained, the residual risk of catastrophic consequence will remain greater than the targets set in the facility risk criteria. Process safety management systems that assure these assumptions remain valid over time are essential to the sustainability of risk management.

Any PSM program must be subjected to a well-defined and rigorous functional audit process. Otherwise the PSM program will be at risk of losing its effectiveness. Degradation (or complete omission) of various safety system management practices is a common theme in numerous process industry incident reports, such as those published by the United States Chemical Safety Board (CSB). These reports frequently include recommendations related to implementing or improving the auditability of automation installations to ensure adherence to company standards and good practice guidelines. It is not uncommon to see defects in change management, bypass management, safety system procedure use, or in the response to findings from prior assessments or audits.

Functional safety audits are designed to ensure that the SCAI installation remains in conformance both with industry practices and with the functional specification. In this paper, we will introduce the purpose and content of these audits, briefly discuss some of the specialized SCAI management system practices of which a functional safety auditor must be aware, and present summaries of industry incidents where lack of effective functional safety audits contributed to the deterioration of the safety system effectiveness over time, causing companies to face increased health, safety, and environmental risks.

2 Functional Safety Audit vs. Functional Safety Assessment

To begin, it is important to have a clear understanding of what a functional safety audit is. For practitioners who are new to functional safety management, a common terminology error to make would be to use "functional safety audits" and "functional safety assessments" (FSA) interchangeably. However, these are not synonymous terms. As indicated in the IEC 61511 definitions below, they have distinctly different intentions.

> **3.2.24**
> **functional safety assessment**
> **FSA**
> investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers
>
> **3.2.25**
> **functional safety audit**
> systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives
> Note 1 to entry: A functional safety audit may be carried out as part of a FSA.

Indeed, those familiar with financial industry terminology may realize that the use of the terms "assessment" and "audit" within that industry are essentially opposite to what is intended within the SCAI related standards. The functional safety assessor is looking at the specific details for each device and function within the SCAI. A functional safety assessment is a detailed examination of the system design and the management system procedures. In contrast, the functional safety auditor determines whether the SCAI procedures and practices are being followed consistently and whether the overall program is working effectively in a manner consistent with the required functional safety performance.

This difference in intent is further represented within the IEC 61511 safety lifecycle representation (Figure 1). Functional safety assessments (shown as Stage 1 through Stage 5) occur at discrete points during safety lifecycle, while the functional safety audit is represented as part of the functional safety management plan spanning the overall program. Those who may need to perform functional safety assessments are encouraged to read the following whitepaper on functional safety: *"Functional Safety Assessments of Safety Controls, Alarms, and Interlocks."* [4]

In short, functional safety audits look for the evidence of the effective use of the many management system procedures required to sustain performance of the SCAI across their lifecycle. Many of these practices will be familiar to any process safety management auditor, such as checking maintenance schedules and management of change policies. These process safety management practices are well documented elsewhere, and thus will not be addressed significantly in this paper [11]. However, the specialized procedures and practices required by the SCAI standards may not be as commonly understood by the process safety auditing community. For this reason, it is important that the audit team include someone who has expertise in the SCAI design and management practices.

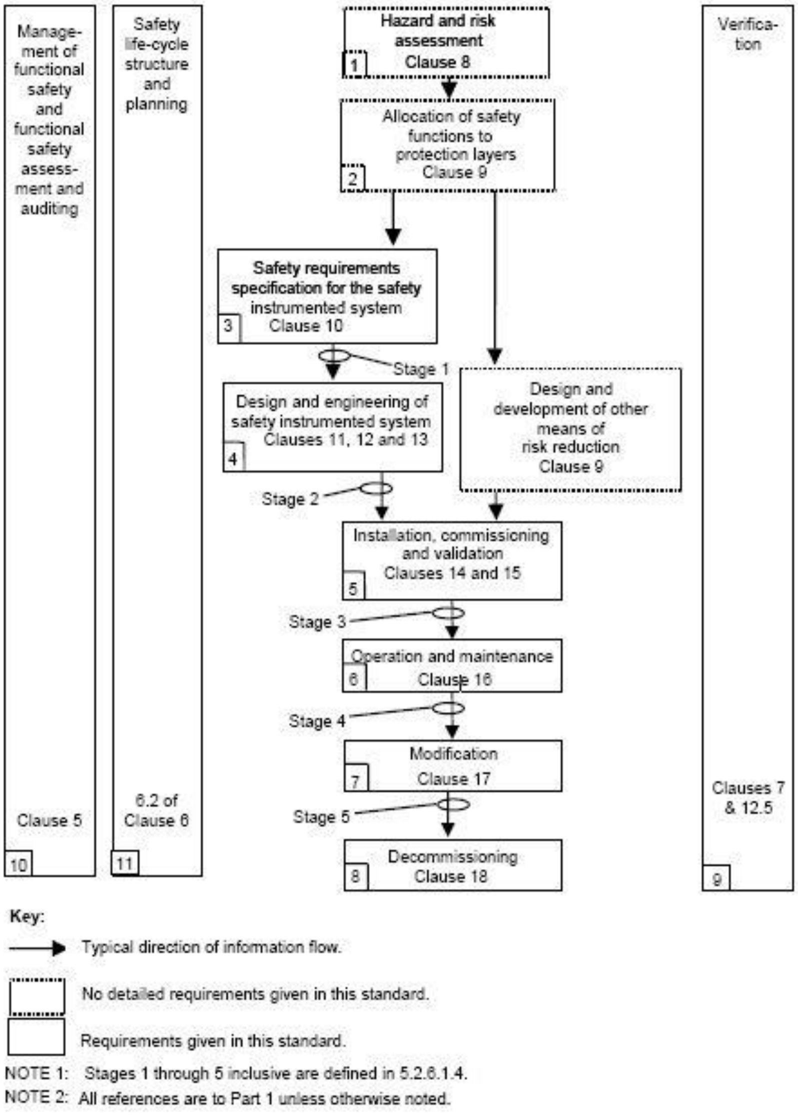
Manage-ment of functional safety and functional safety assess-ment and auditing
Clause 5
10
Safety life-cycle structure and planning
6.2 of Clause 6
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clause 10
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11, 12 and 13
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verifica-tion
Clauses 7 & 12.5
9
Key:
Typical direction of information flow.
No detailed requirements given in this standard.
Requirements given in this standard.
NOTE 1: Stages 1 through 5 inclusive are defined in 5.2.6.1.4.
NOTE 2: All references are to Part 1 unless otherwise noted.

Figure 1: SIS Safety Lifecycle Phases and FSA Stages [1]

2.1 Spot-check in auditing

As discussed above, the purpose of functional safety auditing is to determine whether systematic failures have occurred. The primary scope of the functional safety auditor is to review documentation records for evidence that safety management systems remain active and effective. Additionally, a small sample of individual SCAI installations (field hardware and application program) is typically inspected. This "spot-check" is a technique used to detect potential errors in the design and management processes. Examples of such errors include failure of the instrument reliability program, inconsistent safety system procedure use, or a lapse in SCAI change management discipline. The recommended sample size for auditing process safety management program elements ranges from 2% for very large populations to 100% for populations of 25 or fewer [5]. In the performance of this spot-check, the functional safety auditor might use a subset of the checklists more normally used during functional safety assessment to better facilitate the detection of early signs of program degradation. Beyond this limited spot-check, however, the functional safety auditor does not generally evaluate individual SCAI installations.

2.2 Frequency of the Functional Safety Audit

> *"Safe automation depends on a quality assurance process to ensure correct operation of the process control and safety systems."* [6]

IEC 61511 establishes the recommended, and in some cases mandatory, timing of the various functional safety assessments tasks in reference to the surrounding activities within the safety lifecycle. In contrast, while the functional safety audit is a required activity, IEC 61511 does not comment further regarding the timing of the audit. The audit planner is best advised through the intended purpose of the Functional Safety Audit:

> *The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed.* [Clause 5.2.6.2.1]

It follows that functional safety auditing may take place at any of the completion of any stage of the SCAI lifecycle, as well as being performed at a fixed multi-year interval in the manner of a process safety management audit. An audit at the end of a project stage would ensure the documentation and records were being generated as expected. Performing these more frequent audits may be particularly beneficial in a facility where new or unfamiliar technology is being used, where there is frequent turnover of personnel in roles essential to functional safety performance, or when the teams involved are generally less familiar with the SCAI requirements. In addition, detecting management system gaps early saves money.

2.3 Functional safety audit planning and resources

Any functional safety audit will require a degree of advanced planning to support effective execution. Functional safety audits require written procedures addressing how the audit will be carried out and how timely and satisfactory resolution of resulting recommendations will be assured. Access to all the information related to that audit will need to be arranged.

In addition, each functional safety audit must involve at least one competent auditor that is independent of the work being audited [Clause 5.2.6.2.3]. Just as for any other task in the safety lifecycle, periodic assessments are required to document the competence of the auditors with regards to this activity [Clause 5.2.2.3]. Evidence of the periodic competence assessment and effective resolution of prior assessment and audit findings are critical inputs to a functional safety audit.

2.4 Functional safety audits for other SCAI

While IEC 61511 lists specific audit requirements targeting detection and elimination of errors in the management system procedures, the guidance for other SCAI has historically been much more general. It is reasonable to expect that the auditing of other SCAI functions and devices may have been neglected. It is essential to understand, however, that even with initial robust implementation and functional safety assessment, the field hardware, application program, documentation, and human behavior associated to any SCAI are subject to the exact same degradation mechanisms.

The fundamental principle of entropy applies to all instrumented systems, regardless of the risk reduction that was assigned during allocation. Entropy applies to management systems as much as to the physical installation of hardware. It is therefore not logical to assume that SCAI installations will remain in sufficient working order without similar auditing programs. Indeed, the skills needed to perform such an audit are so similar that it is usually an efficient practice to audit both SIS and the other SCAI systems as part of the same activity.

3 Content of a Functional Safety Audit

In this section, a brief summary of what should be covered in a functional safety audit is provided. In practice, functional safety audits should be performed with more detailed checklists (or other support tools) designed for use by an audit team that in aggregate have the requisite competencies. The procedures should be designed so that all the relevant management systems and procedural practices are addressed and there is clear documented justification for the basis of each finding, whether positive or negative.

Audits that only include reviews of existing documentation and data records are likely to miss more significant systematic deficiencies, such as:

- Detailed changes being made in the instrumentation or application program without using MOC procedures

- Excessive use of bypass/manual control features
- Deterioration of field device condition through insufficient maintenance technician competency
- Misrepresentation (intentional or otherwise) within the instrument reliability program of the actual device field condition
- Approval of unsafe changes or insufficient performance caused by insufficient competence of change approvers
- Failure of the piping and instrument diagrams (P&IDs), human machine interface (HMI) drawings, or other plant safety information (PSI) documents to reflect the actual installation

A high-level review of site documentation, information and records is quite unlikely to reveal the above systematic defects. As discussed in the previous section, this is the reason that a small spot-check of the current installations is typically part of the audit scope. It is worth noting that if functional safety assessment practices have not been implemented effectively at the facility prior to the audit, significant defects may be expected and the functional safety audit team may be tempted to begin performing a functional safety assessment. In the interest of timely execution of the audit, this should be avoided. The revealed defect in the functional safety assessment practices would become a significant finding for the functional safety audit.

3.1 Key input documents

- Procedures and results for all assessment stages
    - Hazards and risk analysis (H&RA) independence and risk reduction limit review and SCAI specification consistency check
    - Detailed design review
    - Pre-startup confirmation of verification and validation results [12]
    - Operation and maintenance competency review and SCAI performance confirmation
    - Proposed SCAI change review
- Procedures and current records for resolution of findings from functional safety assessments and prior audits
- Documentation of MOCs with potential to impact H&RA, SCAI allocation, design, implementation, or procedures
- Current H&RA and Safety Requirement Specification (SRS) documentation
- Current SCAI verification and validation documentation
- Current P&IDs, HMI drawings, application program, and instrument design documentation
- All other current SCAI related procedures

3.2 Typical focus topics for functional safety audit

- Functional safety assessment procedures satisfy intended scope for that stage

- Timely execution of functional safety assessments and prior audits
- Clear documentation of timely, verified, and validated (where applicable) resolution of deficiencies from functional safety assessments and prior audits
- Completeness of documentation, including independently reviewed re-verification and re-validation (where required), of approved changes
- Clear evidence that SCAI procedures are being used in the manner consistent with the requirements of the installation and that resulting automation, instrumentation, and human system performance remains consistent with expectations
- Confirmation of effectiveness of SCAI training and competency management program
- Spot-check small % of SCAI and compensating measure device installations and program applications to audit for failure in change management, instrument reliability, or bypass control programs

4 Potential Consequences of Insufficient Functional Safety Audits

The following subsections present case studies where a functional safety audit did not appear to have been conducted or where findings were not resolved in a timely manner. In these incidents, insufficiency of the audit program likely contributed to the sequence of events that led to unwanted outcomes. As in many process industry incidents, a combination of factors led to the harmful result. This paper does not attempt to address all the contributing causes documented within the referenced reports, but instead focuses on the few deficiencies more directly related to SCAI and their management systems. In the cited events, key defects in SCAI performance or management system practices existed long enough that a robust functional safety audit should have detected them.

4.1 Managing change and procedure use - Case Study: Petrolia, 2008

This case study concerns an incident involving Oleum transfer, at Petrolia, Pennsylvania, that occurred in October 11, 2008. The internal impacts of the event included an oleum release, one person injured, and plant personnel evacuated. Externally the incident resulted in 2500 residents from three towns being evacuated and public road closures.

4.1.1 Case study summary

During a transfer operation, an oleum (a mixture of sulfuric acid and sulfur trioxide) process tank overflowed, filled an exhaust ventilation system, and released the oleum into a storage building. The oleum release created a cloud of sulfuric acid mist that filled the building. The sulfuric acid cloud flowed out to the facility grounds and beyond the fence line into the surrounding community. A sulfuric acid cloud is dense, visible, and slow moving. Inhaling sulfuric acid droplets can irritate the respiratory system, causing airway constriction and spasms. Severe exposure can result in fluid in the lungs, internal bleeding, and even death [7].

Twenty eight years prior to the event, a “temporary emergency” power supply was installed. The intention was to use it only during power emergencies under closely monitored conditions, so the decision was made to use an operator response to alarm safeguard instead of wiring the high level interlocks into the power circuit. The “temporary” change, with the intended limitations, was never incorporated into the facility’s safety related documentation nor was any information on the new power circuit connected to the distributed control system (DCS) or other HMI.

On weekends, this particular part of the facility was lightly staffed for only a few hours. One task during this time was to transfer as much oleum into the feed tanks as possible, to support production at the start of the week.

During the weekend of the incident, operator was pumping oleum from one vessel using the primary power source and from a second vessel using the backup power source. This simultaneous transfer had become a common weekend practice since the "temporary emergency" power supply was installed. CSB report informs that "a former supervisor verbally instructed operators to use the emergency power supply to transfer oleum from the pressure vessels to the process tanks"[7]. However, the same supervisor "cautioned operators to monitor these transfers closely to prevent overfilling."

Status of the pump using backup power was not indicated on the DCS, and the automatic shutoff that was tied to a high-high level switch in the process tanks would not stop a pump powered by the emergency power supply. The pump could only be stopped locally while on backup power.

When the operator stopped pumping from the vessel using the normal power circuit via the DCS at end of the weekend shift, he inadvertently left the pump on backup power running, as shown in Figure 2. A local high level alarm beacon activated on run tank 1502, but the operator had left the building. Five minutes later, the local high high level alarm beacon activated, but no action was taken. Oleum mist (fuming sulfuric acid) was seen leaving the building an hour later by other personnel on the site. An emergency was declared and the facility was evacuated. Three nearby towns were also evacuated. About two hours later, the pump was stopped by cutting power to the oleum storage building.

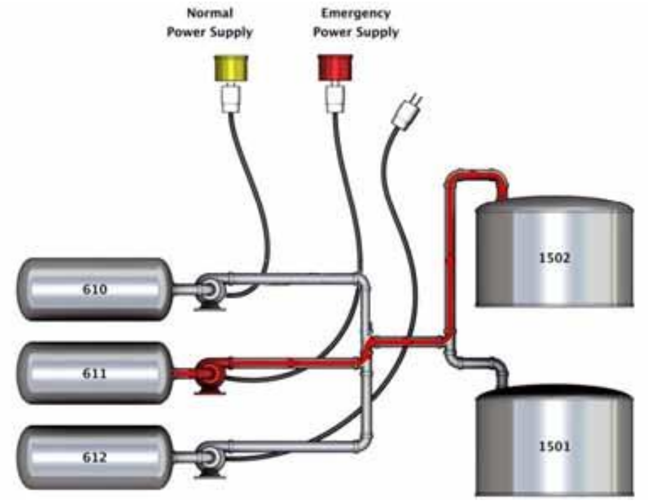

Figure 2: Weekend Power Configuration [7]

4.1.2 Instrumentation and Control Gaps

- Decision to use operator response to alarm as overfill safeguard on the emergency circuit instead of the high level interlocks that were on the primary power circuit (trade safety for project efficiency)
- Change and limitations of use were not incorporated into PHA, PSI documents, or HMI
- Over many years operators developed an undocumented practice of using the “emergency” circuit routinely on weekends, contrary to original intended use
- High level alarm used as normal fill level, and beacon not working

4.1.3 Case study conclusion

Although the CSB report does not mention the specific H&RA methodology that was used or the actual audit frequency practiced, it does mention the "temporary emergency" power supply was considered effectively permanent after a safety audit in the 1980s, replacing flexible electrical cord with wiring in conduit. However, the lack of completeness of the audit in terms of the pump use prevented observing the potential hazard being inserted to the system by this change. Assumptions made during hazard and risk analysis were actually not the same as after implementing the initial safety audit findings.

The functional safety audit recommendations should have included the upgrade going through a Management of Change (MOC) procedure. Such a process would be expected to trigger the functional safety assessments that might have revealed the inconsistency in the safeguard allocation between the two power circuits and the deficiencies in the PSI documentation associated with the "emergency" power circuit. Change documentation, verification and validation should also have been observed. Likewise, a thorough functional safety audit of SCAI procedure use should have eventually identified the operator practices during weekend that were not part of any written company procedure.

More frequent functional safety audits could have identified the lack of timely repair of the local audible alarm signal as well, although this deficiency did not directly contribute to the occurrence of this specific event.

4.2 Bypass control and audit finding resolution - Case Study: Illiopolis, 2004

This case study covers an incident that occurred in April, 2004, at a polyvinyl chloride (PVC) plant located in Illiopolis, Illinois. The internal impacts of the event included five fatalities; three hospitalized; four minor injuries; plant damage; laboratory, safety, and engineering buildings destroyed. Externally the incident resulted in 150 residents being evacuated and public road closures.

4.2.1 Case study summary

On the night of the accident, all PVC reactors were making PVC except reactor D306, which was being cleaned. After washing the reactor from the upper level, the operator went downstairs to drain out the contents of D306. Turning the wrong way coming down the stairs, the operator went to the bottom valve of reactor D310 by mistake and tried to open the bottom valve to empty the vessel (Figure 3).

The reactor pressure safety interlock prevented the reactor bottom valve from opening. The operator, presumably under the belief that he was still on D306 and that the interlock was therefore in error, connected an emergency bypass air hose to the actuator to force the interlocked valve open. He did not request permission to do the bypass or inform anyone of the bypass.

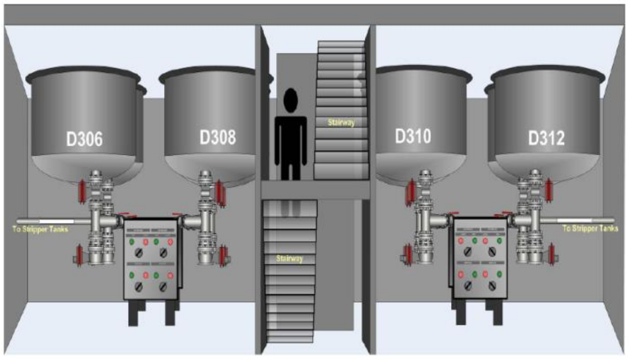

Figure 3: Cutaway of Reactor Building, from CSB Report [8]

The reactor contents rapidly emptied through the bottom valve, forming a vapor cloud. Although area release monitor alarms activated and most personnel evacuated, some operators remained at the equipment in an attempt to mitigate the situation. They were still present when the vapor cloud ignited.

4.2.2 Instrumentation and Control Gaps

- Safety Interlock bypassed with air hose, no authorization, no access controls
- Area alarms ignored by team attempting to mitigate release
- 1992 PHA identified scenario; recommendations not adopted
- 1999 PHA re-identified scenario; rationalized using administrative control
- A similar “near miss” incident had occurred at another facility the prior year and at the Illiopolis facility about 6 months prior; no corrective actions taken

4.2.3 Case study conclusion

Hazard analysis practices assume the SCAI will be operational nearly all the time. However, administrative controls (i.e. operating policies and procedures) on bypasses are subject to the same human errors as the normal operating procedures that may have initiated the event. To avoid errors like this one in Illiopolis, correctly implemented and managed access restrictions (i.e. keys and locks, passwords) may have mitigated that risk.

Access control of bypass capability depends on periodic auditing and, of course, reviews of incident and near miss investigations. Bypass control procedure use should be subjected to short term interval auditing reviewing access restrictions, authorization, communication, and how long the bypass is active, as well as the correct use of compensating measures to manage the existing risk to the target levels during the bypass. The functional safety audit should provide independent confirmation that the bypass management program is being used effectively. However, no functional safety audit or assessment program can remain effective in the absence of independent oversight that insures effective and timely resolution of the resulting recommendations. As noted by Summers and Raney, "There must also be a strong ally in upper management to support the auditing process that will be required to ensure that the EGS [engineering guidelines and standards] are used." [9]

5 Conclusion

As process industry has evolved, automation has taken a crucial role in both the normal control of the facility and in the protection of the personnel, environment, and assets of the facility in the event of loss of normal control. The creation and sustainability of safe automation is essential to the successful, productive and safe operation of these plants. As incident after incident since 1992 demonstrate on a global scale, there are a number of management systems that are critical to the continued effectiveness of safe automation design [10]. However, these management systems will likely deteriorate if not effectively audited and the results of those audits resolved in a safe and timely manner.

While general management systems, such as MOC, will be very familiar to an experienced process safety auditor, effective functional safety auditing requires additional knowledge of the policies and procedure requirements specific to instrumented safeguards. Thus, the functional safety auditor must develop a sufficient understanding of the scope, procedures, and records associated to the various functional safety assessments used throughout the SCAI safety lifecycle. Verification and validation, bypass control, device level change management, and instrument reliability programs are among the management systems whose failure appear with unfortunate frequency in process safety incident investigation reports.

Robust and timely execution of the function safety audit and of the associated functional safety assessment practices required in IEC61511 can help identify and correct such systematic failures and reduce the chance of such a failure contributing to a catastrophic event. Functional safety management gaps will potentially be detected through routine audits that may identify ways to make SCAI more effective.

6 References

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

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

[3] ISA. [draft Rev 3] 2016. Functional Safety: Safety Controls, Alarms, and Interlocks for the Process Sector, ANSI/ISA-84.91.03. Research Triangle Park: ISA.

[4] Hochleitner and Roche. 2016. "*Functional Safety Assessments of Safety Controls, Alarms, and Interlocks*".

[5] CCPS. [2011]. Guideline for Auditing Process Safety Management Systems. New York, NY: Center for Chemical Process Safety.

[6] CCPS. [draft] 2016. Guidelines for Safe Automation of Chemical Processes. New York, NY: Center for Chemical Process Safety.

[7] CSB. 2009. INDSPEC Oleum Release Case Study. Case study 2009-01-I-PA. Washington, D.C.: U.S. Chemical Safety Board.

[8] CSB. 2007. Investigation report - vinyl chloride monomer explosion at Formosa Plastics Corporation. Report 2004-10-I-IL. Washington, D.C.: U.S. Chemical Safety Board.

[9] Raney, Glenn and Angela Summers. [1999]. “Common Cause and Common Sense, Designing Failure Out of Your Safety Instrumented Systems (SIS),” ISA Transactions, 38, pages 291-299

[10] Summers, A. *et all* [2015]. "Incidents that Define Safe Automation", 61st International Instrumentation Symposium, Alabama, May 11-14, 2015.

[11] Summers, A. [2008]. "Lessons Learned in Auditing Automated Systems for PSM Compliance", 1st Latin America CCPS Conference, Buenos Aires, Argentina, March 27-29, 2008.

[12] CCPS. [2007]. Guideline for Performing Effective Pre-Startup Safety Reviews. New York, NY: Center for Chemical Process Safety.