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

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

A Practical Approach to Preventing Systematic Error in the Maintenance of Instrumented Safeguards

Eloise Roche and Dr. Angela Summers*
SIS-TECH Solutions
12621 Featherwood Dr. Suite 120, Houston, TX 77034
Presenters E-mails: asummers@sis-tech.com*, eroche@sis-tech.com

Abstract

Instrumentation and electrical (I&E) maintenance is typically managed using site-wide policies, practices, and procedures. Since I&E equipment is part of the control system and nearly every other layer of protection, the cumulative impact of poor I&E performance can be a significant contributor to major events. Systemic problems in managing I&E equipment reliability lowers process safety performance across a site.

Practical guidance is needed on how to assess the vulnerability of existing sites to instrumented safeguard failure due to maintenance deficits. This paper leverages Reason's organizational accident model as a framework to discuss site-specific factors that impact a site's susceptibility to maintenance error. A table of more than 60 human factors covering I&E maintenance activities was developed and organized by 4 elements of causality: organizational processes, workplace practices, personnel traits, and enabling conditions. The human factors table can be used to rate an industrial site on a negative-to-positive scale, highlighting those areas where systemic changes would likely improve maintenance performance and instrument reliability.

Keywords:
Instrumentation, safety instrumented systems, electrical systems, maintenance, human factors, human error, systematic

1 Leading or Lagging Indicators

The process industry depends on I&E equipment maintained in a manner that sustains the equipment's ability to act as required, when required, to prevent process safety incidents. While this responsibility is mandated by process safety regulations, it is simply a wise business practice

to be proactive in managing instrument reliability. At many facilities, any one of thousands of instruments could cause operational problems. High reliability organizations understand that tackling these challenges head-on yields the best process availability.

Yet, assessments conducted by the UK's Health and Safety Executive (HSE) [1] and the US's Occupational Safety and Health Administration (OSHA) [2, 3] have found that some companies in the process sector have problems with their maintenance programs, as evidenced by the percentage of maintenance-related findings (Figure 1). These findings echo those published as a series of case studies in Guidelines for Safe Automation of Chemical Processes (Safe Automation) [4].

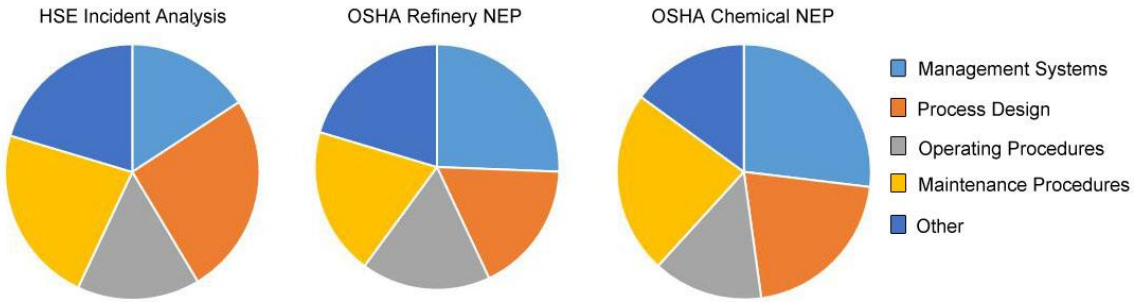

Figure 1. HSE Incident Analysis [1], OSHA Refinery National Emphasis Program (NEP) [2], and OSHA Chemical NEP [3] Findings

Government and industrial organizations have recommended metrics for monitoring the effectiveness of process safety management, including the Health and Safety Executive [5] the Center for Chemical Process Safety [6], and the American Petroleum Institute. API 754 [7] established 4 tiers of indicators (Figure 2). The bottom 2 tiers are leading indicators, because they are measures of the operating discipline, equipment integrity and safety culture. When these tiers are well-managed, it is far less likely that an event will happen. Safe Automation's case studies show that the top 2 tiers are often events where Tier 3 and 4 metrics were not implemented, and site practices did not identify and correct systemic problems.

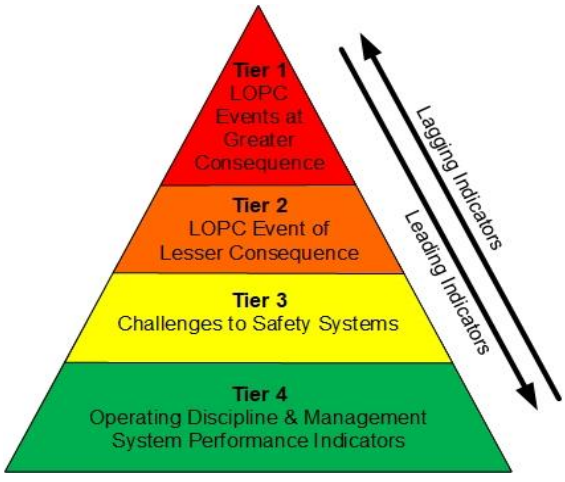

Figure 2 API 754 Metrics

International standards on instrumented safeguards provide more detailed guidance on performance metrics. ISA 61511 [8] requires monitoring the safety instrumented system (SIS) reliability parameters, which are Tier 3 metrics. Quite a few more Tier 3 metrics are recommended by ISA TR84.00.04 in Annex R [9]. Tier 4 indicators, such as using maintenance records as a predictive tool for reliability issues, were introduced into the 2012 edition of ISA TR84.00.03 [10] on asset integrity management of SIS. Recent ISA 84 meetings have included workshops on reducing systematic errors during SIS implementation and discussions on preventing systematic errors during maintenance.

2 Incidents are an Organization Failure

Human factors often play an out-sized role in poor I&E reliability. Safe Automation's case studies demonstrated strong links between the incidents and the failure to manage the on-going reliability of instrumentation and controls [4, 11]. These incidents ultimately were attributed to a series of failures that lined up in a dangerous manner. To prevent incidents, effort is required to sustain the asset integrity of the site's I/E equipment [12]. The errors, violations, and systemic failures in one system, whether control or safety, often repeat in other instrumented systems. If SIS equipment is not maintained, it is highly likely that other I/E reliability deviations are occurring. Systematic issues in maintenance can easily cause a breakdown of multiple IPLs (Independent Protection Layers), even if the IPLs are deemed independent based on an analysis of the equipment and system architecture [13].

The latest industry-published guidance on reducing maintenance errors through diversity is not really helpful. While theoretically attractive, there is no evidence that equipment diversity, staggered testing, or diverse maintenance teams can address the predominant underlying problems that are frequently cited by I&E technicians (Table 1). Rather, the proposed diversity would tend to make many field issues worse by increasing the complexity of the design, installation, testing, and maintenance.

Table 1 Problems commonly cited by I&E Technicians [13]

Unclear roles and responsibilities	Poor procedures
Lack of up-to-date documentation	Lack of warnings or cautions
Poor planning	Poor installation and configuration

3 A Practical Approach to Determining Site Risk for Systematic Error

James Reason, the father of the accident causation model, also known as the "swiss cheese" model, stated "Blaming people for their error is emotionally satisfying but remedially useless [14]." Errors are not inherently bad. There are a multitude of industry stories of errors that birthed significant innovations.

Errors can be made by the best people. No one intends to make them. The more competent the person is, the more likely they will commit a very serious error. This is because the most competent people will seek out assignments with the greatest challenges and risk. All employees should be competent enough to do at least the average job, so error management is not equivalent to competency management. Rather, error management is about understanding what promotes errors and changing the situation presented to the employee to discourage them instead.

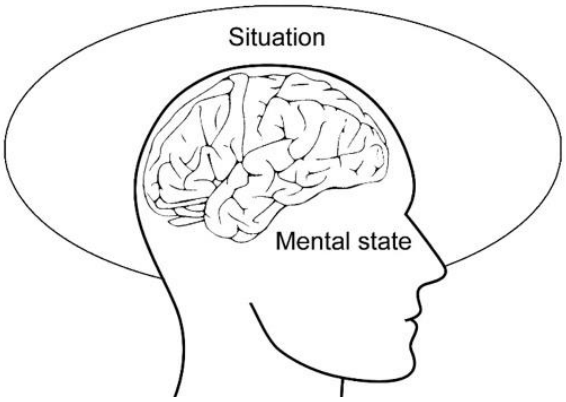

Figure 3 Errors Involve A Mental State and A Situation

Errors are affected by the mental state of the individual and the situation presented to the individual (Figure 3). Functional safety principles cannot control the individual's mental state, but they can influence the individual's decision-making processes. Everyone weighs the costs versus the benefits of complying to policies, procedures, and practices (Figure 4).

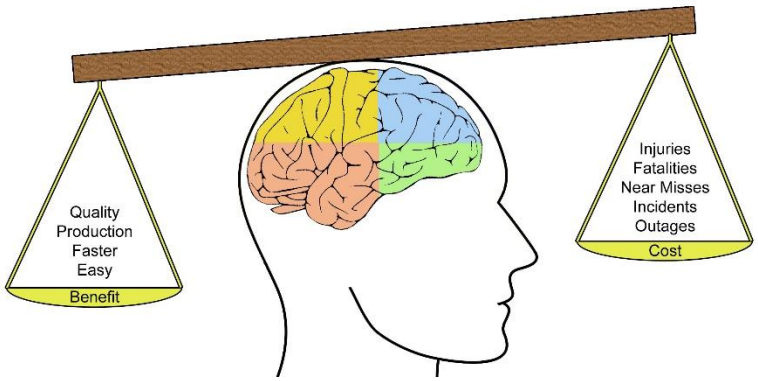

Figure 4 Humans Balance Costs and Benefits When Making Decisions

The perceived costs might include accidents, injuries, and damages, but these may seem like unlikely future events compared to the benefits of doing something an easier way or saving time today. In most cases of non-compliance, the benefits are easy to see immediately with little obvious negative impact.

The cost/benefit balance is rarely shifted by increasing the penalties for non-compliance, because these penalties are already known to be severe in the case of process safety events. Instead, greater

influence on decision-making might be achieved by investing more time in acknowledging the important benefits of compliance.

In contrast to the mental state, the situation can be controlled and managed by functional safety management. The situation can be viewed as what maintenance personnel face when executing the work. The situation involves 4 elements: organizational processes, workplace practices, personnel traits and enabling conditions (Figure 5).

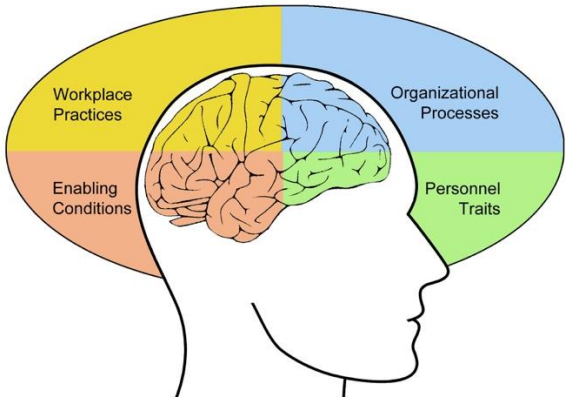

Figure 5 Situations Involve 4 Elements

These elements are external to personnel, but they influence the decision-making process. The situation can vary significantly in ways that promote or discourage human error. For example, the situation could involve a task that is well-planned with detailed procedures in place to achieve quality work execution. Or the situation could involve troubleshooting unexpected behavior with unfamiliar technology in a poorly lit room with no up-to-date specification.

Reason's organizational accident model (Figure 6) used the 4 elements to illustrate the underlying causality [14] of human errors and incidents. Errors occur when a planned action does not achieve the desired result. For example, the maintenance procedure did not define who takes responsibility for the equipment being returned to service, so this critical task was not done. In contrast, violations occur when deviations from an approved practice are intentionally taken.

Violations are rarely malicious acts and are often intended as positive with respect to some aspect of the task. An optimizing violation occurs when someone does something that seems to accomplish the same thing but is easier or faster than the planned way. For example, the deviation meets the deadline or budget, demonstrates a high level of skill, or is simply easier. Routine or optimizing violations can become part of the site maintenance culture when an owner/operator rarely punishes deviations or fails to frequently reward compliance [15].

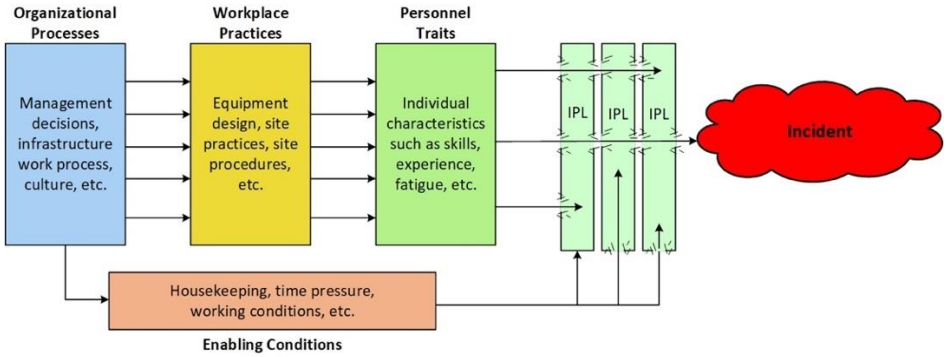

Figure 6 Anatomy of an Organizational Accident (adapted from [14])

Organizational processes focus worker attention on certain behaviors and metrics, while workplace practices impact the quality and consistency by which maintenance activities are accomplished. Organizational processes determine what is considered important or not. These processes feed into management decisions that directly impact the day-to-day work of planning, forecasting, budgeting, communicating, monitoring, and auditing. Many accidents begin with negative organizational processes that promote poor workplace practices and tolerance of poor instrument reliability. For example, effective communication between maintenance and engineering is critical to ensure that reliability issues are addressed comprehensively. The likelihood of unresolved, long-term reliability problems significantly increases when communication breaks down between engineering, operations, and maintenance.

Workplace practices are the written instructions that govern how maintenance is executed. Poor practices, like inadequate instructions, missing specifications, obsolete procedures, and ineffective interface design, increase the likelihood of errors and violations [16]. For example, a test procedure that does not define the required equipment function becomes a source for maintenance error even though the maintenance person has a high degree of skill with the technology.

Personnel traits are intrinsic to the person executing the task. The most important traits are possessing the skills and experience necessary to complete assigned tasks correctly. Hiring competent personnel is essential but sustaining competency as I&E technology changes can be challenging. High turnover can make it difficult to ensure that personnel have the in-depth knowledge of the system design needed for troubleshooting problems or evaluating the impact of management of change activities. Competency can also be off-set when fatigue or poor health impacts decision-making. Accidents become even more likely when poor workplace practices are combined with negative personnel traits, such as inexperience, poor skills, or being tired.

Enabling conditions make errors impacting multiple protection layers more likely. These conditions are triggered by organizational decisions that promote errors and violations, such as high work load, time pressure, unreasonable schedules, poor housekeeping, and poor quality tools. Other task-specific conditions, such as ill-fitting personal protective equipment, dim lighting, poor housekeeping and missing labeling can also exist due to management policies and resource allocations. These enabling conditions potentially increase the likelihood that error will occur regardless of how optimal the organizational processes and workplace practices may be.

The 4 Elements of Causality were used as a framework to develop a list of 61 positive and negative human factors for maintenance activities. The list is based on personal experience and was enhanced by lessons-learned discussions at the Instrument Reliability Network [17], ISA 84 and ISA 61511 committee meetings. A summary of the systematic error sources, subtopics and human factors is provided in Table 2. The detailed human factors table is provided in Appendix A.

Table 2. Hierarchy of Human Factors in Maintenance

Sources	Subtopics	Specific Human Factors
Organizational Processes	Communications	• Clarity of responsibilities • Engineering and maintenance communications • Operations and maintenance communications • Teamwork and communications • Emergency communications
	Instrument Reliability Program	• Process demand tracking • Maintenance priority • Out of service/bypass management • Repeat failure/bad actor management
Workplace Practices	Maintenance Instructions	• Task complexity • Procedure clarity and detail • Return to service procedures • Change management • Quality control and record keeping
	Maintenance Equipment/Interfaces	• Specification and installation drawing availability • Maintenance feature/facility design
Personnel Traits	General	• Knowledge, skills and experience • Fatigue
	Competency Assessments	• Verification of knowledge and skills
Enabling Conditions	General	• Personal protective equipment • Tools and equipment • Working conditions • Housekeeping • Time pressure

Each human factor listed in Table 2 has multiple prompts in Appendix A. These prompts describe negative and positive human factor attributes. Some negative organizational attributes often cited in incident reports are as follows:

- Instrumented safeguard maintenance is frequently delayed, behind schedule, or not prioritized.

- Frequent bypassing of instrumented safeguards with little oversight, time limits, or risk assessment. Bypasses include operator bypasses, manual operation, changing setpoints, and forces.

- High tolerance for poor process control and upsets leading to frequent demands on the instrumented safeguards.

- High tolerance for poor instrument reliability. Unresolved issues, long-term out-service, and frequent fault conditions accepted.

In contrast, the positive organizational attributes associated with these are:

- Instrumented safeguard maintenance is prioritized, executed as scheduled, and is rarely delayed for operational reasons.

- Instrumented safeguards only bypassed under strict controls, including compensating measures and time limits. Bypasses include operator bypasses, manual operation, changing setpoints, and forces.

- Low tolerance for poor instrument reliability. Proactive attitude to taking action to improve reliability.

- Low tolerance for poor process control; particular focus on reducing frequency of process upsets and process demands on the instrumented safeguards.

The attributes can be rated on any desired scale. This paper takes a binary approach where the site is assessed as displaying either negative or positive human factors. Another approach is to use an analog scale of 1 to 5 with 1 being mostly negative and 5 being the mostly positive. The intent is to provide a means to assess the current status of the strategies, processes and activities used by a site to identify and prevent systematic errors.

4 Applying Human Factors Evaluation to a Case Study

Process safety management provides multiple opportunities to assess the adequacy of I&E equipment, including hazards and risk analysis, risk assessments, maintenance monitoring, management of change, and audits. The use of the positive and negative human factor table in Appendix A can be triggered as a result of findings from these activities. Using the table as part of a corrective process is a good way to get started and to demonstrate immediate benefits. However, it does mean that the site is already experiencing sufficient systemic impact to warrant a deeper dive. This is a classic feedback, or lagging indicator, approach to process safety [16]. Another approach would be to use the table as a self-assessment tool to understand site vulnerability to maintenance error before negative performance data piles up.

To illustrate the methodology, the human factors table was applied to the incident commonly known as “Buncefield.” The incident occurred at the Hertfordshire Oil Storage Terminal, which was located in Hemel Hempstead north of London England and was part of a complex of tank terminals known as the Buncefield Depot. The depot had an estimated capacity of 60 million gallons, making it the 5th largest oil depot in the UK [18]. The depot served as a major distribution

center for the UK oil pipeline network [18]. It provided fuel to Humberside, Merseyside, as well as to Heathrow and Gatwick airports [19].

An explosion occurred on December 11, 2005, which injured 43 people and devastated the Hertfordshire Oil Storage Terminal, which was jointly owned by Total UK Ltd and Chevron Ltd [19]. Residences and commercial buildings in the area were structurally damaged with some requiring demolition. The economic impact on regional businesses is estimated to be in the range of £130–170 million [19]. Total losses may have been as much as £1 billion [19, 20].

The incident occurred when the Automated Tank Gauging (ATG) system for one of the terminal tanks failed (Figure 7). The loss of level control allowed fuel to be fed into the tank for 11 hours [21]. The fuel overflowed through the tank conservation vents for approximately 40 minutes [22] prior to ignition, producing a large vapor cloud estimated to be 8 hectares in size [23]. The vapor cloud ignition resulted in the largest peacetime explosion in European history [18] producing a tremor measuring 2.4 on the Richter scale and blowing out windows five miles away from the site [23].

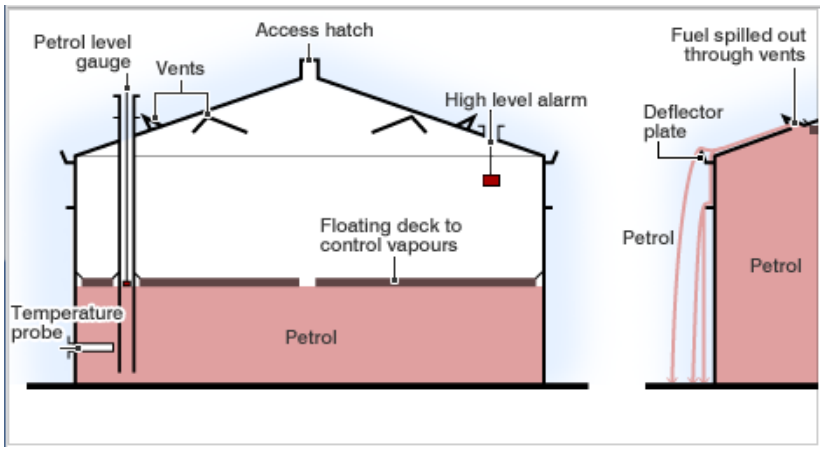

Figure 7. Simplified Graphic of Buncefield Tank

Gasoline was being delivered to the tank on the day before the incident. Early the next morning, the ATG displayed an unchanging level, although the tank continued to fill. By practice, the operator controlled the tank level by terminating transfer upon receipt of the ‘user’ alarm. However, the 'user', 'high', and 'high high' level alarms used the same transmitter. The failure of the shared transmitter rendered all three alarms inoperative. Since the ‘user’ alarm never activated, the operator did not take action to terminate transfer.

An independent high-level switch, set above the ATG high-high level, was designed to close inlet valves and activate an audible alarm, but it also failed. The high-level switch had been disabled when the maintenance organization, due to lack of understanding of the relatively new technology and to insufficiently detailed procedures, did not reinstall a lock on the switch test arm. Without the lock, the level switch was not activated when the float was lifted. By late afternoon, the tank overfilled and contents spilled out of tank roof vents. A vapor cloud was formed and noticed by tanker drivers and by people outside the facility. The fire alarm was activated and firewater pumps

were started. An explosion occurred a short time later, likely ignited by the startup of the firewater pumps.

Reviews of the readily available literature on the incident identified significant problems with I&E equipment. The analog level involved in the incident had 14 dangerous failures (stuck) in the 3.5 months preceding the incident. It appears that the site had a high tolerance for poor process control and poor instrument reliability. The three "failed" alarm measurements came from the same faulty level device, which is an example of a common cause failure for the intended protection layers. The review also identified quite a few organizational and workplace issues:

- Confusion of responsibilities and expectations
- Poor communication between operations and maintenance
- Lack of consistency on who did what and when
- Lack of timely communication between maintenance technicians and supervision
- No reporting structure for escalation of unresolved problems
- Inaccessible installation drawings, specifications, and functional requirements
- No review of installation and configuration of instrumented safeguards after initial validation

The available information in reports on the Buncefield incident were used to assess the site against the human factors in Appendix A. Nearly half (28 of the 61) of the negative attributes were identified. It is also likely that other negative attributes were present; however, these contributors are not discussed in the available literature. The assessment suggests that the organizational processes, workplace practices, personnel traits, and enabling conditions at the Buncefield site significantly increased the likelihood of systematic issues. The negative human factors made an overfill event much more likely than would have been predicted by hazards and risk analysis.

5 Summary

Safe Automation's case studies describe incidents where instrumented safeguards should have intervened in the incident propagation but did not. The underlying causes of these failures were often systematic rather than random. These underlying causes likely impacted the potential for incidents across the site, and perhaps the entire organization. A practical first step in preventing systematic error in instrumented safeguard maintenance can be to perform a qualitative evaluation of the existing maintenance human factors. This evaluation identifies the areas in which the organization might be vulnerable to such errors and where there might be more value to focusing additional organizational resources. A table of positive and negative human factors was created to allow assessment of a site's vulnerability to systematic errors during maintenance. As an illustration, the table was used to assess the Buncefield incident. Based on the published reports, nearly half of the 60 negative human factors were present.

6 References

[1] HSE, Health and safety laboratory report, Loss of Containment Incident Analysis, Great Britain (2003).

[2] OSHA, Process Safety Management for Petroleum Refineries - Lessons Learned from the Petroleum Refinery Process Safety Management National Emphasis Program.

[3] OSHA, Process Safety Management for Chemical Plants - Lessons Learned from the Chemical Process Safety Management National Emphasis Program.

[4] CCPS/AIChE, Guidelines for Safe Automation of Chemical Processes, Second Edition, American Institute of Chemical Engineers, NY, (2017).

[5] Health and Safety Executive, "Developing process safety indicators," 1st edition, (2006) ISBN 978 0 7176 6180 0.

[6] CCPS/AIChE, Guidelines for Process Safety Metrics, Wiley-Interscience, New York (2009).

[7] API, Recommended Practice Process Safety Performance Indicators for the Refining and Petrochemical Industries, RP754, API, Washington D.C. (2016).

[8] ISA, ANSI/ISA 61511-1-2018, Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT), Research Triangle Park, NC (2018).

[9] ISA, Guidelines for the Implementation of ANSI/ISA 84.00.01- Part 1, TR84.00.04-2015, Research Triangle Park, ISA, (2015).

[10] ISA, Asset Integrity of Safety Instrumented Systems, TR84.00.03-20012, Research Triangle Park, ISA, (2015).

[11] Summers, Angela, E. Roche, H. Jin, M. Carter, "Incidents That Define Safe Automation," 61st International Instrumentation Symposium, Huntsville Alabama, May 2015.

[12] Summers, Angela, "Risk Assessment Challenges to 20:20 Vision," Process Safety Progress, pages 119-125, June 2015.

[13] Summers, Angela E. and Eloise Roche, "Mobile Interfaces on the Plant Floor," 73rd Instrumentation and Automation Symposium, Texas A&M University, January 2018.

[14] Reason, James and Alan Hobbs, Managing Maintenance Error: A Practical Guide, Ashgate Publishing Company, Hampshire England (2003).

[15] Reason, James, Managing the Risks of Organizational Accidents, Ashgate Publishing Company, Hampshire England (1997).

[16] CCPS/AIChE, Guidelines for Safe and Reliability Instrumented Protective Systems, 1st edition, American Institute of Chemical Engineers, NY, (2014).

[17] Instrument Reliability Network, Mary Kay O'Connor Process Safety Center, Texas A&M University.

[18] Wikipedia, "2005 Hertfordshire Oil Storage Terminal Fire," http://en.wikipedia.org/wiki/2005_Hertfordshire_Oil_Storage_Terminal_fire.

[19] Buncefield Major Incident Investigation Board, "The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board," ISBN 978 0 7176 6270 8, (2008).

[20] British Broadcasting Station, "Buncefield blast could cost £1 bn," December 11, 2008, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/england/7777539.stm.

[21] British Broadcasting Station, "Buncefield tank was overflowing," May 9, 2006, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/4752819.stm.

[22] The Daily Mail, "Petrol tank 'overflowing' before Buncefield blast," May 9, 2006, United Kingdom, http://www.dailymail.co.uk/news/article-385607/Petrol-tank-overflowing-Buncefield-blast.html

[23] The Guardian, David Fickling, "Faulty fuel gauge caused Buncefield Explosion," United Kingdom, http://www.guardian.co.uk/uk/2006/may/09/buncefield.davidfickling

Appendix A - 4 Elements of Causality

Table 1. Organizational Processes

Topic	Positive Human Factors	Negative Human Factors
Communications		
Clarity of responsibilities	Expectations communicated and rules are consistently enforced	Confusion on expectations or inconsistent enforcement
Engineering and maintenance communications	Clear communication between maintenance technicians and engineering to resolve instrumented safeguard issues	Maintenance lacks support from engineering; tolerance for unresolved instrumented safeguard issues
	Timely communication of negative findings by maintenance to I&E engineering/reliability	Poor or lack of communication of negative findings by maintenance to I&E engineering/reliability
Operations and maintenance communications	Clear communication of instrumented safeguard status between operations and maintenance technicians	Poor/unclear communication of instrumented safeguard status between operations and maintenance technicians
	Reliable operator-to-maintenance technician communication equipment (two-way radios, telephone, etc.) with alternative means	Unreliable, no alternative, may not work in an overloaded situation
	Good communication between operations and maintenance technicians	No/not expected communication between operations and maintenance technicians
Teamwork and communications	Formal communication with turnover log when maintenance shift changes occur. Includes communication of active bypasses, overrides, faulted devices, and other issues relevant to safe completion of tasks.	Informal communication when shift changes occur. No defined expectation on what to communicate at shift change.
	Frequent supervisory reviews and quality assurance checks	No/incomplete supervisory reviews or quality assurance checks
	Good communication of new findings related to instrumented safeguard health, such as obsolescence, end-of-life, and any identified installation, commissioning, or functional issues	Lack of timely communication of new findings related to instrumented safeguard health, so that identified issues are not addressed systematically across a site
	Routine reporting of repeat failures (e.g., bad actors) to maintenance supervision	Lack of timely communication of repeat failures to maintenance supervision
Emergency communications	Clear, unambiguous site-wide emergency warning system	No distinction in emergency warnings based on areas or event types. Not audible or reliable in some locations.
Instrument Reliability Program		
Process demand tracking	Low tolerance for poor process control; particular focus on reducing frequency of process upsets and process demands on the instrumented safeguards	High tolerance for poor process control and upsets leading to frequent demands on the instrumented safeguards
Maintenance Priority	Maintenance priority is established based on device criticality and level of functional impairment	Maintenance priority does not consider device criticality; redundant instrumented safeguard equipment essentially treated as "spares;" level of functional impairment not understood
	Spare parts management program considers the time required to acquire specialized instrumented safeguard equipment and the need to remain within the assumed mean time to restoration	Spare parts purchased on failure detection without regard to lead time and planned mean time to restoration
	Instrumented safeguard maintenance is prioritized, executed as scheduled, and is rarely delayed for operational reasons	Instrumented safeguard maintenance is frequently delayed, behind schedule, or not prioritized
	Instrumented safeguards only bypassed under strict controls, including compensating measures and time	Frequent bypassing of instrumented safeguards with little oversight, time limits, or risk

Topic	Positive Human Factors	Negative Human Factors
Out of service/bypass management	limits. Note: Bypasses include operator bypasses, manual operation, changing setpoints, and forces.	assessment. Note: Bypasses include operator bypasses, manual operation, changing setpoints, and forces.
	Low tolerance for poor instrument reliability. Proactive attitude to taking action to improve reliability.	High tolerance for poor instrument reliability. Unresolved issues, long-term out-service, and frequent fault conditions accepted.
Repeat failure/bad actor management	Minimal false or spurious alarms	Many false or spurious alarms or alarms ignored or disabled
	Instrumented safeguards are known to be reliable and effective	Instrumented safeguards are known to be unreliable or ineffective
	Identified failures are investigated and repaired in a timely manner	Failed equipment remains in-service; repeated failures are not investigated
	Failure reporting and escalation notification for unresolved issues is clearly defined	No/poor reporting structure for identified failures; no escalation of unresolved problems

Table 2. Workplace Practices

Topic	Positive Human Factors	Negative Human Factors
Maintenance Instructions		
Task complexity	Required tasks are well-defined and regularly performed	Infrequently performed or repeated/rapid changes in task expectations
	Manufacturer installation and maintenance manuals are reviewed to ensure that maintenance procedures agree with intended application; manuals are accurately translated, written in native language and written from the perspective of the maintenance technician	Manufacturer installation and maintenance manuals are not reviewed for consistency with application; manuals are not clearly written, in wrong language, or poorly translated
	Units of measure are consistent between provided documents and equipment configuration	Units of measure are not consistent between provided documents and equipment configuration
Specification, installation drawing availability	Procedures include verification of installation and configuration of instrumented safeguards against specification	No review of installation and configuration of instrumented safeguards after initial validation
	Installation drawings, specifications, and functional requirements are accessible when needed	Installation drawings, specifications, and functional requirements are not accessible
Procedure clarity and detail	Procedures are at the right level of detail to ensure consistent execution and record keeping	Too general or too detailed leading to inconsistent maintenance, a tendency to skip steps, or poor maintenance records
	Procedures are written in concise, imperative language	Wordy, inconsistent style
	Procedures include notes, cautions, and warnings where errors could result in impaired equipment	Lack of hazard awareness, unknown impact of error
	Notes, cautions, and warnings set off from procedural steps (e.g., in text boxes placed immediately before applicable steps)	Task criticality not clearly identified
	Procedures/checklists used in the performance of task	Task sequence done by memory
	Procedures contain clear pass/fail criteria	Maintenance determines acceptability based on ad hoc criteria
Return to service procedures	Maintenance procedures include return to service verification by operations	No operations cross-checking or verification of return to service for instrumented safeguards

Topic	Positive Human Factors	Negative Human Factors
Change management	Procedures address change management and version control	Maintenance corrects problems without engineering involvement or change management review
Quality control and record keeping	Procedures include appropriate supervisory checks	No supervisory cross-checking or verification
	Data governance is used to ensure record quality	No data governance
Maintenance Equipment/Interfaces		
Maintenance feature/facility design	Instrumented safeguard equipment is easily accessible for maintenance or accessibility issues are addressed in the maintenance procedures	Instrumented safeguard equipment is not easily accessible; maintenance is known to be delayed by access issues
	Maintenance facilities designed for purpose, arranged in logical order, easy to use, well-labeled, and in-service status is easy to detect	Maintenance facilities are confusing, complicated, unreliable, disablement possible without detection, or in-service status difficult to detect

Table 3. Personnel Traits

Topic	Positive Human Factors	Negative Human Factors
General		
Knowledge, skill and experience	Minimal turnover of maintenance technicians resulting in significant experience with site instrumented safeguards and a high degree of personal knowledge of site systems	High turnover of maintenance technicians resulting in less experience with site instrumented safeguards and less personal knowledge of site systems
	Hiring qualifications are defined and include specific requirements for instrumented safeguards	Hiring qualifications are not defined or do not include specific requirements for instrumented safeguards
	Technicians are well-trained, experienced, and good at troubleshooting the technologies used on site	Technicians are not well-trained, are inexperienced, or lack troubleshooting skills with the technologies used on-site
	Technicians are well-trained on safe work practices, such as lock-out/tag-out, electrical safety, job safety analysis, etc.	No specific/unclear requirements for training on safe work practices, such as lock-out/tag-out, electrical safety, job safety analysis, etc.
	Technicians are well-trained on instrumented safeguard maintenance and required record keeping. Training program includes periodic refresher training.	No specific/unclear training on instrumented safeguard maintenance and record keeping.
Fatigue	Overtime limited by defined policy that ensures reasonable and regular rest breaks	Overtime is extreme and does not ensure sufficient rest
	Permanent shift assignments	Shift rotations
Competency Assessments		
Verification of knowledge and skills	Training verification includes both test and observations	No/inadequate verification of learning

Table 4. Enabling Conditions

Topic	Positive Human Factors	Negative Human Factors
Personal protective equipment	Required PPE does not affect performance of tasks	PPE is heavy, cumbersome, gets in the way of performing tasks.
Tools and equipment	Test equipment is high quality, equipment calibration is verified	Poor quality test equipment; lax tracking of calibration records
Working conditions	Noise level low enough to easily communicate	Hearing protection is required. Noise level hinders ability to hear or use communication equipment.
	Provided with protection from weather; including rain, snow, wind, and sun	Not provided with protection from weather, including rain, snow, wind, and sun
	Task conducted in climate-controlled environment	Task conducted in high temperature and/or humidity extremes
	Clear visibility where task is being executed	Poor visibility where task is being conducted, including fog, smoke, or other sight obscuring element
	Lighting is sufficient to conduct task, including being able to read tags, critical information, procedures, or other documents	Lighting is insufficient to conduct task or to read documents
Housekeeping	Equipment is clearly and uniformly labeled	Equipment is mislabeled or not labeled
	Equipment is installed in the field as would be expected (A to C are upstream to downstream)	Equipment is installed in an unexpected order (C to A are upstream to downstream)
	Equipment criticality is easily distinguished in the documents and in the field	Similar equipment in same area or grouped together without any indication of criticality
	Clearly communicated identifier/location for instrumented safeguard equipment	Ambiguous identifier/location for instrumented safeguard equipment
	Consistent tagging between procedures, P&IDs, and equipment	Inconsistent tagging between installation and documents
	Installation shows discipline toward good labeling, tight wiring connections, and consistent installation practices	Installation shows poor discipline, such as loose wiring connections, lack of consistent labeling, or inconsistent installation practices
Time pressure	Number of tasks well-matched to work force	Required tasks exceed resources
	Pace of tasks is not rushed. Little time pressure on step execution.	Multiple tasks are executed in rapid succession and under time pressure