Recommendations to align safety and security for industrial automation control systems

ISA99 WG7 TG1


30 January 2015
# Contents

1 Introduction and scope of work

1.1 Challenges addressed by TG1

1.2 Technical approach

2 Background and related activities

2.1 Why we need to integrate safety and security into IAC development and operations

2.2 ISA 84 alignment initiatives

2.3 IEC TC65 AHG1 alignment initiatives

2.4 Australian initiatives

2.5 LOGIIC initiatives

3 Definition of terms, acronyms, and conventions

3.1 Definition of terms

3.2 Definition of acronyms

3.3 Conventions used in this report

3.3.1 Reference citations

3.3.2 Definition of terms

4 Findings and recommendations

4.1 Summary of findings

4.2 Summary of recommendations

5 Recommended models and their use

5.1 Hierarchical control structure

5.2 Applicable conditions for safety and security constraints

5.3 Controlling constraints

5.4 Recommendation for 62443

Annex A Bibliography

Annex B Possible relationship between SIL and SL

B.1 Background

B.2 A better understanding of safety integrity level

B.2.1 Safety life cycle

B.2.2 Relationships to hardware fault tolerance

B.2.3 SIL and related measures

B.2.4 Parameters of safety integrity and the possible relationship to security

B.3 Three Mile Island incident analogy

B.4 Two scenarios using the chemical truck loading example

Annex C Chemical truck loading example – use case
Figure 1 Organizational control structure ................................................................. 7
Figure 2 Distribution of control flaws........................................................................... 9
Figure 3 Safety live cycle - sequential approach.......................................................... 13
Figure 4 Chemical truck loading example - use case .................................................. 16

Table 1 Intersection of safety and security objectives .................................................. 3
Table 2 Applicable conditions for safety and security constraints ................................ 8
Table 3 Relationship between SFF and hardware fault tolerance for a type B device .... 13
Table 4 SIL and related measures .............................................................................. 13
1 Introduction and scope of work

ISA99 in cooperation with IEC TC65 is responsible for developing security standards and related products for industrial automation control systems (IACS). Their focus is cybersecurity, not physical security1. ISA84 is responsible for developing safety standards and related products for IACS.

ISA99WG7 commissioned TG1 to investigate the potential coupling between safety and security. Initially, TG1 sought to find a mathematical coupling between safety integrity level (SIL) and security level (SL). The technical difference between SIL calculation and SL calculation methods proved too difficult – see Annex B. Safety systems have a well-defined process for determining and making use of the concept of SIL [1-6]. SL on the other hand is less well defined and more qualitative than quantitative in nature. For this reason, TG1 expanded their approach to develop a framework to harmonize or align safety and security using more traditional system engineering approaches.

The issue of integrating safety and security into systems lifecycle is currently under active investigation[7]. IEC TC65 commissioned an ad hoc working group (AHG1) to pursue this investigation – see IEC 65/569/DC. TG1 closely monitored the work products of AHG1 to avoid duplicating their work.

1.1 Challenges addressed by TG1

Formulating a framework to seamlessly integrate safety and cybersecurity protection into a well understood system engineering approach created several challenges.

- Little information is available to evaluate likelihood using historical information.
- Evaluating severity of hazards induced by cybersecurity threats requires consideration of worst-case loss associated with the hazard.
- Alignment with mandatory requirements specified in local laws and regulations introduced variables that differ significantly from country to country.
- Given the severity rating and hazard analysis for a specific use case, the framework must provide the capability to map ISA99/IEC62443 technical requirements specified in part 3-3, conformance requirements specified in part 2-4. This capability is necessary to identify requirements and requirement enhancements (REs) to mitigate the consequence of a successful interruption or disruption of operations.

1.2 Technical approach

TG1 adopted Leveson’s technical approach[8] which uses the mitigation potential of the hazard as an estimator of, or surrogate for, likelihood for two reasons:

1) The potential for eliminating or controlling the hazard in the design or operations has a direct bearing on the likelihood of the hazard occurring.
2) Mitigation potential of the hazard can be determined before architecture or design is defined.

2 Background and related activities

2.1 Why we need to integrate safety and security into IAC development and operations

Leveson identified the reasons that a new approach is needed to build safer systems that departs in important ways from traditional safety engineering.TG1 selected and modified a subset of Leveson’s approach to include cybersecurity mitigation technologies of security engineering.

1 Physical security (guns, guards, gates, locked cabinets, monitors, cameras, etc.) must be addressed by the asset owner and system integrator in their comprehensive security program.
1) **Fast pace of technological change:** Both safety and cybersecurity technologies are changing faster than our engineering techniques are responding to these changes. New technologies, particularly cybersecurity threats, introduce unknowns into IACS that create new paths to losses resulting from safety failures or cybersecurity protection failures.

2) **Increasing complexity and coupling:** Industrial automation control systems include interactive complexity, dynamic complexity, decompositional complexity, and nonlinear complexity with inherent vulnerabilities. Cyber-induced exploitation of these vulnerabilities is the common means to interfere with or disrupt normal IACS operation.

3) **Difficulty in selecting and making trade-offs:** Asset owners/operators, product suppliers, and service providers are coping with aggressive and competitive environments in which cost and productivity is the major consideration in short-term decision making. This situation is further exacerbated with the integration of cybersecurity protection solutions which are a mix of vendor solutions and operator solutions.

4) **Changing regulatory and public views of safety and security:** The responsibility for establishing safety and security requirements is shifting from the individuals to government, while implementation responsibility remains with the asset owner/operator, system integrator, product supplier and service provider.

### 2.2 ISA 84 alignment initiatives

ISA 84 published technical report ISA-TR84.00.09-2013 “Security Countermeasures Related to Safety Instrumented Systems (SIS).” This technical report describes performance criteria to guard against internal and external security threats to the safety instrumented system and provides guidance on how to comply with IEC 61511 and ANSI/ISA-84.00.01-2004 with respect to cybersecurity.

The authors concluded that without addressing cybersecurity throughout the entire lifecycle, it is impossible to adequately understand the relative integrity of protection that involve instrumented systems, including the SIS.

The underlying premise of this technical report is that the means to implement, operate, and maintain system security should not compromise the performance of the safety instrumented systems (SIS). To this end, SIS installations should be designed and maintained using the foundational requirements found in IEC 61511 and ANSI/ISA-84.00.01-2004, and in the ISA/IEC 62443 series. This document assumes that the applicable requirements and recommendations specified in the ISA/IEC 62443 series of standards have been implemented by the user (asset owner/operator, system integrator, product supplier, or service provider).

### 2.3 IEC TC65 AHG1 alignment initiatives

IEC TC65 commissioned an ad hoc group to review the current research addressing the alignment between safety and security. AHG1 maintains minutes of meetings and related documents on their IEC web site. ISA99WG7TG1 carefully monitors their work to leverage their recommendations to support the recommendations offered in this report.

### 2.4 Australian initiatives

The Australian IT006 committee reported the coupling between safety objectives and security objectives in Table 1. Their concern is that strong alignment and integration can lead to ineffective or conflicting controls [7]. Some members of TG1 agreed with the Australian concern and others were sceptical. Regardless, TG1 decided that Leveson’s technical approach [7] provides a reasonable framework for aligning safety and security in a coherent systems engineering approach.
2.5 LOGIIC initiatives

The LOGIIC partnership, which is an acronym for “Linking the Oil and Gas Industry to Improve Cybersecurity”, was created in 2004 to improve cybersecurity in digital control systems and to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector. The program objective is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality. LOGIIC functions as a collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, with the Automation Federation serving as the host organization.

LOGIIC has undertaken a number of important studies since its inception. These include, in part,

- the Correlation Project, which demonstrated an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating and analyzing abnormal events to identify and prevent cyber security threats;
- A public report on the use of wireless communications in control systems; and
- Cybersecurity implications of SIS integration with control networks.

Recognizing the importance of Safety Instrumented Systems (SIS) in the oil and gas industry, and the rapidly emerging vendor solutions that offer varying degrees of integration with control networks, LOGIIC conducted the third-listed project, which consisted of the security evaluation and study of several SIS architectures and was presented at ISA Automation Week in 2011. Although details of the study are not provided here, the general conclusions are:

- Greater integration may introduce greater risk;
- Default configurations are not secure;
- Defense in depth reduces risk;
- Clear guidance is needed.

The full report, as presented at ISA Automation Week in 2011, can be found at http://www.automationfederation.org/filestore/af/logiic/LOGIIC%20SIS%20REPORT%20for%20ISA%20August%2025%202011%20mod%20Jan%202013.pdf.
The project demonstrated an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating and analyzing abnormal events to identify and prevent cyber security threats.

After a successful first project, the LOGIIC consortium was formally established as a collaboration between DHS, the Automation Federation, and five of the major oil and gas companies. The LOGIIC program has completed several R&D projects, and more projects are being planned and started.

3 Definition of terms, acronyms, and conventions

3.1 Definition of terms

3.1.1 accident
an unplanned and undesired loss event

NOTE TO ENTRY An accident is also described as a process upset.

3.1.2 availability
probability that equipment will perform its task

3.1.3 decompositional complexity
structural decomposition of safety and security is not consistent with their functional decomposition

3.1.4 dynamic complexity
cybersecurity protection component degradation over time

3.1.5 fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors [IEC 61508-4]

NOTE TO ENTRY Therefore, hardware fault tolerance is the ability of the hardware (complete hardware and software of the device under consideration) to continue to perform a required function in the presence of faults or errors.

3.1.6 hazard
a system state or set of conditions that, together with a particular set of related environmental conditions, will lead to an accident (loss) [modified IEC 61784-3-18, ed. 1.0 (2011-04)]

NOTE TO ENTRY Leveson qualifies related conditions as “worst case.”

3.1.7 high complexity safety related systems
part of an E/E/PE safety-related system for which:

• the failure mode of at least one component is not well defined, or
• the behavior of the subsystem under fault conditions cannot be completely determined, or
• there is insufficient field failure data to show that the claimed failure rates are met

EXAMPLE A FS-PLC. This is derived from type B subsystem as described in IEC 61508-2:2010, 7.4.4.1.3.

Note 1 TO ENTRY Refer to Type A (9.4.3.2.2) and Type B (9.4.3.2.3) systems.
[IEC 61131-6, ed. 1.0 (2012-10)]
3.1.8
**interactive complexity**
interaction among safety and security system components

3.1.9
**likelihood**
quantitative estimation that an action, event or incident may occur

[IEC 62443-2-1, ed. 1.0 (2010-11)]

3.1.10
**nonlinear complexity**
cause and effect are not related in a direct or obvious way [8]

NOTE TO ENTRY See high complexity safety related systems

3.1.11
**probability of failure on demand**
probability of a system failing to respond to a demand for action arising from a potentially hazardous condition

NOTE TO ENTRY The average PFD is used to calculate safety system reliability.

3.1.12
**safety instrumented function**
sensors, logic solver and final control elements designed to achieve or maintain a safe state.

NOTE TO ENTRY Devices used in the SIF are based on their required SIL.

### 3.2 Definition of acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHG</td>
<td>ad hoc group</td>
</tr>
<tr>
<td>CP</td>
<td>communication processor</td>
</tr>
<tr>
<td>DuC</td>
<td>device under consideration</td>
</tr>
<tr>
<td>FMEDA</td>
<td>failure modes, effects and diagnostic analysis</td>
</tr>
<tr>
<td>IAC</td>
<td>industrial automation control</td>
</tr>
<tr>
<td>IACS</td>
<td>industrial automation control system(s)</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society for Automation</td>
</tr>
<tr>
<td>LOGIIC</td>
<td>Linking the Oil and Gas Industry to Improve Cybersecurity</td>
</tr>
<tr>
<td>LOPA</td>
<td>layer of protection analysis</td>
</tr>
<tr>
<td>RE</td>
<td>requirement enhancement</td>
</tr>
<tr>
<td>SCAI</td>
<td>safety controls, alarms and interlocks</td>
</tr>
<tr>
<td>SIF</td>
<td>safety instrumented function</td>
</tr>
<tr>
<td>SFF</td>
<td>safe failure fraction</td>
</tr>
</tbody>
</table>
3.3 Conventions used in this report

3.3.1 Reference citations

Although references are provided, an attempt is not made to cite or describe everything ever written on the topics or to provide a scholarly analysis of the state of research in this area. The goal is to select those references that have a direct bearing on the alignment of safety and security for IACS. References are cited using the IEEE notation “[xx].”

3.3.2 Definition of terms

The order of preference for terminology definition follows:

- ISA99 master glossary
- ISO/IEC glossary
- IEEE glossary
- Webster discretionary
- Common usage found in Wikipedia

When required to better fit TG1’s technical approach, definitions were modified as documented in the bracketed note appended to the definition.

4 Findings and recommendations

4.1 Summary of findings

1) The subject matter experts participating in this study could find no algebraic relationship between security level and safety integrity level.

2) The experts agreed with Leveson that strong alignment and integration can lead to ineffective or conflicting controls [7].


4.2 Summary of recommendations

1) With explanatory text, the intersection of safety and security objectives described in Table 1 is recommended for 62443-1-1.

2) A hierarchical safety/security control structure shown in Figure 1 (with explanatory text) is recommended for 62443-1-1. Figure 2 is also recommended. The text in clause 5.4 is recommended as the introduction to these control structures.

3) The applicable conditions for safety and security constraints shown in Table 2 (with explanatory text) is recommended for 62443-1-1. More work is needed to identify the applicable requirements and requirement enhancements in other parts of 62443 that address the constraints.
5 Recommended models and their use

5.1 Hierarchical control structure

Leveson introduced a hierarchical safety control structure with feedback mechanisms for adaptive control [8]. TG1 modified this model to include security – see Figure 1. Leveson noted, and TG1 included security, that at each level in the hierarchical structure, inadequate control may result from missing constraints (unassigned responsibility for safety and security), inadequate safety and security control commands, commands that were not executed correctly at a lower level, or inadequately communicated or processed feedback about a constraint enforcement. Not shown in Figure 1 is the input and feedback with government bodies and legislatures. Also, for simplicity, multiple interactions between system development and system operations are not shown.

Figure 1 Organizational control structure

5.2 Applicable conditions for safety and security constraints

TG1 expanded the operating process shown in Figure 1 and the list of required conditions for safety constraints [9, 10] to include security constraints. TG1 tried, without success, to find the applicable technical requirements in the 62443 series. A future work effort is needed to identify the existing 62443 part, clause and paragraph. In the interim the requirements column in Table 2 is left blank or a recommendations is offered.
Table 2 Applicable conditions for safety and security constraints

<table>
<thead>
<tr>
<th>Constraint ID</th>
<th>Constraint description</th>
<th>Applicable 62443 requirement (part, clause, paragraph)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The control must have a goal or goals (e.g., to maintain the validity of safety and security constraints)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The controller must be able to affect the state of the IACS</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>The control must be (or contain) a model of the process. Every model-predictive controller incorporates into its design two models:</td>
<td>62443-1-3</td>
</tr>
<tr>
<td></td>
<td>a) A process model that relates its measured output to the manipulated control input (e.g., a valve that regulates a flow)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) A model of external disturbances and how they affect the value of the regulated output. If the external disturbances are unmeasured an estimate must be provided.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The controller must be able to ascertain the state of the IACS. Whether the process models are embedded in the control logic of an automated, model-predictive controller, or in the mental maintained by a human controller they must contain the same type of information:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) The current state of the safety constraint</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) The current state of the security constraint</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) The relationship between the state of the safety constraint (output) and the two inputs, that is, manipulated input and external disturbance(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) The relationship between the state of the security constraint (output) and the two inputs, that is, manipulated input and external disturbance(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) The ways that state of the safety constraint can change</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) The ways the state of the security constraint can change</td>
<td></td>
</tr>
</tbody>
</table>

5.3 Controlling constraints

Leveson and Stephanopoulos developed a model describing the distribution of control flaws [11]. TG1 modified this model to include security flaws. What caught TG1’s interest was their approach to no decompose the process into its structural elements and defining process upsets\(^2\) as the result of flow of events, as prevailing methodologies do, but to describe processing systems and upsets in terms of the hierarchy of adaptive feedback control systems as shown in Figure 2. At each level of the hierarchy a set of feedback control structures ensures the satisfaction of the control objectives, that is, of the safety and security constraints. The applicable conditions were discussed in Table 2.

\(^2\) Levenson, et al uses the term accidents. TG1 prefers to use the term process upset.
5.4 Recommendation for 62443

Based on TG1’s understanding of the control-inspired view to process safety developed by Leveson, the following perspective needs to be included in the preface to all 62443 products. This recommendation is aligned with the lessons learned from TG1’s special study on security-safety coupling.

ISA99 (IEC 62443) offers a system theoretic view and approach to a rational all-encompassing framework for addressing process safety as it relates to the consequences resulting from the exploitation of IACS vulnerabilities. Specifically, those vulnerabilities exploited by cyber-induced interruptions. This framework is based on a control-inspired statement of the process safety problem, which is amenable to modern model-predictive control approaches and can encompass all potential systemic constraints associated with operations management, relations by government agencies or standards that govern plan operations.
Annex A

Bibliography

Annex B

Possible relationship between SIL and SL

B.1 Background

TG1 discussed at length the possible relationship between SIL and SL. There is a possible common
ground in the failure mode analysis.

1) Safety examines the hardware failure of components to determine the probability of such a
   failure. The estimated probability expression is $10^x$. SIL index is the difference in order of
   magnitude in the probability of failure.

2) Security examines the vulnerability of components that interfere with or disrupt their operation.
   This again is a failure analysis, but the process of analysis is significantly different. The result
   requires improvement of security mitigation functions, but does not require an improved SIL.

If safety and security risk is determined by the severity of the consequence of failure, disruption
or interference of a critical mission function, intuitively the common ground between safety and
security is found in the details resulting from a failure mode analysis. Although there is not a
“1-to-1” mapping between safety integrity and security levels, an argument could be made that a
high SIL corresponds to a serious consequence. Given the seriousness of the consequence, an
argument could be made that a higher SL related to implementation of requirements and
requirement enhancements for technical control is needed.

Finding this model and building a quantitative relationship is needed.

B.2 A better understanding of safety integrity level

B.2.1 Safety life cycle

Magnetrol paper offers a better understanding of safety integrity level [3]. The safety life cycle
shown in Figure 3 is a sequential approach to develop a safety instrumented system [12-14].
Magnetrol described how this process expects to provide a framework to design fail safe systems.
They describe how a SIL is a measure of the safety risk of a given process. Technically it is
accurate to say that a device is “suitable for use within a given SIL environment.” Each level
represents an order of magnitude risk reduction. The higher the SIL, the greater the impact of
failure and the lower the failure rate that is acceptable.

The SIL assignment is based on the amount of risk reduction that is necessary to maintain the risk
at an acceptable level. This ensures that the SIS can mitigate the assigned process risk. IEC
stratifies SIL into four discreet levels of safety. Each level represents an order of magnitude of risk
reduction. The higher the SIL level, the greater the impact of a failure and the lower the failure rate
that is acceptable. All SIS design, operation and maintenance choices must be verified against the
target SIL.

B.2.2 Relationships to hardware fault tolerance

IEC 61508-4 defines “fault tolerance” as the “ability of a functional unit to continue to perform a
required function in the presence of faults or errors.” A hardware fault tolerance of 0 means that if
there is one fault the device under consideration (DuC) will not be able to perform its function. A
hardware fault tolerance N means that N+1 faults could cause a loss of the safety function. When
someone does a failure modes, effects and diagnostic analysis (FMEDA) on a device, the resultant
safe failure fraction (SFF) has an associated hardware fault tolerance of 0. IEC 61508 describes
how SFF and hardware fault tolerance are related to SIL – see Table 3.
B.2.3 SIL and related measures

Several other measures come into play when attempting to mathematically associate SIL with SL. Both IEC and ANSI/ISA standards utilize similar tables covering the same range of values for the probability of failure on demand (PFD). Loebl noted that estimates of a system’s PFD are usually affected by some uncertainty. This can in theory be rigorously described by a subjective probability distribution for the value of the PFD. However, an assessor has seldom a clear idea of this distribution, and many calculations are de facto performed by just assuming that the expected PFD, say $q^*$, is the true PFD of the system, which is an incorrect procedure.

- From the viewpoint of predicting probability of failure-free operation over multiple demands, i.e., predicting a system’s reliability function, using the mean PFD instead of its distribution is guaranteed to err on the side of pessimism.
- A bound of optimism can also be determined by assuming that the system has a probability $q^*$ of having PFD equal to 1 and a probability $1-q^*$ of having PFD equal to 0.
- Having these two bounds one can both perform pessimistic calculations and have an idea of how large an error the approximation may imply.

ANSI/ISA however, does not show a SIL 4. No standard process controls have yet been defined and tested for SIL 4. One description of these relationships is shown in Table 4. Other relationships are discussed in [3].

Table 4 SIL and related measures

<table>
<thead>
<tr>
<th>SIL</th>
<th>Availability</th>
<th>$PFD_{avg}$</th>
<th>Risk Reduction</th>
<th>Qualitative Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>&gt;99..99%</td>
<td>$10^{-5}$ to $&lt;10^{-4}$</td>
<td>100,000 to 10,000</td>
<td>Potential for fatalities in the community</td>
</tr>
<tr>
<td>3</td>
<td>99.9%</td>
<td>$10^{-3}$ to $&lt;10^{-2}$</td>
<td>10,000 to 1,000</td>
<td>Potential for multiple on-site fatalities</td>
</tr>
<tr>
<td>2</td>
<td>99 to 99.9%</td>
<td>$10^{-2}$ to $&lt;10^{-1}$</td>
<td>1000 to 100</td>
<td>Potential for major on-site injuries nor a fatality</td>
</tr>
<tr>
<td>1</td>
<td>90 to 99%</td>
<td>$10^{-1}$ to $&lt;10^0$</td>
<td>100 to 10</td>
<td>Potential for minor on-site injuries</td>
</tr>
</tbody>
</table>

The relationships between SIL and hardware fault tolerance and between SIL and related measures illustrates the difference in basic methods used to assign SIL and the methods used to assign SL. TG1 concluded that these differences made it nearly impossible to create an algebra linking SL as a function of SIL.

B.2.4 Parameters of safety integrity and the possible relationship to security

Medoff and Johnson addressed the question “why do we think that there should be a relationship between SIL and SL” [4]. The relationship comes from the similarity of possible consequences. The failure of a safety system could be severe (such as damage to equipment) and a cyber-induced...
attack could do the same by either altering the database or disabling the safety system. One consequence is a result of hardware failure and the other is the result of a specific external communication to the IACS. Potential similar consequences exist, but with completely different root causes.

Medoff and Johnson continued their argument by addressing the question “how is the consequence of a cyber-induced attack related to safety.” A cyber-induced attack on the IACS is a planned event; a safety failure is an unplanned event. Both are difficult to predict although statistical studies have provided methods that can help quantitatively determine safety system failure likelihood, whereas the likelihood of a cyber-induced attack can only be qualitatively determined. Both can have similar consequences. The higher the consequence of a cyber-induced attack, the higher the likelihood that such an attack will occur (because it is more desirable to the attacker).

Thomas supported these conclusions and expanded the argument to state that sampling mapping SIL of a safety integrity function (SIF) is too limiting [5]. In various ISA SC84 documents and the Center for Chemical Process Safety, the term SCAI (safety controls, alarms and interlocks) is used. There may be a possible mapping between SCAL and SL. This approach requires an in-depth study of all the layer of protection analysis (LOPA) for a specific manufacturing site. These LOPAs indicate how much risk reduction is required by SCAI to meet the defined risk criteria in quantitative terms. In some cases, there will be layers of protection that are not vulnerable to a cyber-induced attack; the only risk reduction is afforded by SCAI. Thomas offered the following reasons for this approach.

1) The approach is well-suited for situations that are judged low likelihood of occurrence and low risk.

2) Only focusing on SIF ignores the common mode aspect of a cyber-induced attack relative to other layers of protection, including the trip rate protection. In the case of cyber-induced attacks, this would not be spurious as it would be an attack, but it is an analogous consideration and a safety concern as a sudden shutdown can add safety issues on their own.

Joel Langill with support from Swarandeep Sing added another issue [6].

3) How is this coupling between safety and security to be mapped to measurements for a particular security zone or conduit? The added complexity will impact the IACS community’s acceptance of the 62443 series.

**B.3 Three Mile Island incident analogy**

Leveson offered a simple description of the a design flaw that that was a factor in the Three Mile Island incident [8]. An indicator misleadingly showed that a discharge valve had been ordered closed but not that it had actually closed. In fact, the valve was blocked in the open position.

Rather than attributing the incident to a design flaw, it could be caused by a cybersecurity vulnerability which allowed for an insider to change the set points or to disrupt the communication of the discharge valve’s true state. A similar analogy developed for the Stuxnet incident [15].

**B.4 Two scenarios using the chemical truck loading example**

TG1 used the chemical truck loading example (Annex C) to examine different possibilities that influence the requirement for safety integrity. They examined several cyber-attack scenarios to examine the cyber mitigation requirements to protect the SIS and data it depends on for proper operation.

1) A safety instrumented system air-gapped from the plant network. Given the target level for the probability of failure, which is based on the potential consequence (loss of life, cost of damage and repair, etc.), a SIL requirement is set for the SIS. For instance the SIL could be as low as 1, corresponding to $10^x$. 
2) A safety instrumented system IP-connected to the plant network and control system.

   a) A properly designed cyber-attack could interfere with or disrupt the communication processor (CP) operation to the extent that the data delivered to the SIS is either corrupted or not delivered. In either case the SIS is blind.

   b) Such a scenario requires cyber-based mitigation functions to improve protection, but does not change the hardware probability of failure (and SIL) for the SIS. Adding cyber-based mitigation functions increase the SL by making the cyber-attack more difficult to execute, but does not change the SIL. It does impact the security requirements for software, access control, etc.

In the future, other scenarios need to be examined. For example consider the insider threat to examine the possible failure mode parameters for safety and security. Furthermore, future work should focus on the development of functional flow diagrams that identify the input parameters to the failure mode analysis that generate the SIL and the parameters that generate the SL. In both cases, the constant factor for consideration is the consequence of failure (called the hazard), not the probability of a cyber-attack.
Annex C
Chemical truck loading example – use case

IEC/DFC 62443-3-2:2013 requires grouping SIS components into separate zones and conduits. Figure 4 shows the zones and conduits for the chemical truck loading control and emergency shutdown safety system. This use case illustrate the security dependency of the SIS safety zone on the containment zone, the control system PLC security zone, and the conduit containing the router with an embedded firewall.

There are two points of access to the SIS logic solver, a dedicated point-to-point Ethernet connection to the SIS engineering station and a RS-485 based MODBUS communication link with the control system PLC. The control system PLC provides the basic control and monitoring functions for the chemical truck loading operation, while the safety PLC is an emergency shutdown system to stop the truck loading operation when detecting a hazardous situation.

Figure 4 Chemical truck loading example - use case