A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 18, 2017, accepted June 13, 2017, date of publication June 22, 2017, date of current version July 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2718568

A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method

ANGELITO GABRIEL, (Member, IEEE), JUAN SHI, (Member, IEEE), AND CAGIL OZANSOY, (Member, IEEE)
College of Engineering and Science, Victoria University, Melbourne, VIC 8001, Australia
Corresponding author: Angelito Gabriel (allan1226@gmail.com)

ABSTRACT The safe and secure operation of critical infrastructure is dependent on appropriate responses to safety, security, and operational priorities into integrated control and safety systems (ICSS), at design stage and throughout the life of the system. Digitization as well as networked automation and control infrastructures have increased in the past years and are leading to remarkable potential security risks. Recent news about serious security incidents, such as the *WannaCry* ransomware, affecting the whole world are heard more often. The objective of this paper is to come up with an integrated and optimised evaluation framework for ICSS and related subsystems considering cybersecurity and safety. This can be achieved by the alignment of the cybersecurity framework formulated by the National Institute of Standards and Technology with safety and security standards ISA84 (IEC 61511) and ISA99 (IEC 62443), and the novel funnel risk graph method. The need of such alignment between safety and security has been recognized by the research community, the industry, as well as the International Society of Automation (ISA).

INDEX TERMS Integrated control and safety systems (ICSS), National Institute of Standards and Technology (NIST), ISA84 (IEC 61511), ISA99 (IEC 62443), funnel risk graph method (FRGM).

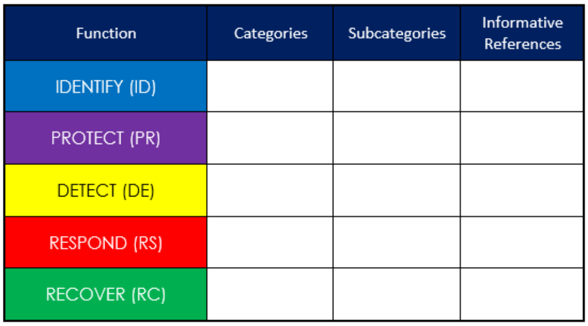
I. INTRODUCTION

Cybersecurity threats exploit the organisation's security, economy, safety and health orchestrated by an augmented complexity and connectivity of critical infrastructure systems. The oil and gas industry has a huge demand to protect multi-billion mega project globally and is projected to spend up to $1.87 billion on cybersecurity by 2018 [1], [2]. Cybersecurity risk affects a company's bottom line similar to financial and reputational risk. It can drive up costs and impact revenue. It can damage an organisation's ability to innovate and to gain and maintain customers. In the past years, separate research communities have dealt with threats to safety versus security [3]. Two international standards have been proposed by the ISA to address ICSS safety and security needs: ISA 84 standard (also called IEC 61511) on safety instrumented systems (SIS) [4] and ISA 99 standard (also called IEC 62443) on control system security [5]. As ICSS are becoming more complex and more integration of systems and subsystems required, the contrast between safety and security is beginning to deteriorate. Collaboration between safety and security [6] are starting to be of interest among researchers [3], [7]. ISA has also identified a need of alignment between safety and security, and formed a working group, Work Group 7 - Safety and Security, to investigate alignment and common issues between security and safety [8].

The remainder of the paper is organised as follows. Section II, III, IV and V describes the NIST framework, ISA 84, ISA 99 and FRGM. Related works is presented in Section VI. Section VII discussed our proposal overview and Section VIII, our novel detailed proposal – the Alignment of NIST framework with the FRGM enables evaluation of both security and safety using an integrated scheme. Finally, Section IX concludes the paper.

II. NATIONAL INSTITUE OF STANDARDS AND TECHNOLOGY FRAMEWORK [9]

In February 2014, as directed by a presidential executive order, the cybersecurity framework was published following a collaborative process involving government agencies,



Function	Categories	Subcategories	Informative References
IDENTIFY (ID)			
PROTECT (PR)			
DETECT (DE)			
RESPOND (RS)			
RECOVER (RC)			

FIGURE 1. NIST framework core.

industry, and academia. The NIST framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component supports the connection between business drivers and cybersecurity activities. These components are as follows:

A. ***NIST FRAMEWORK CORE*** as depicted in Figure 1, is a group of cybersecurity actions, preferred results, and appropriate references that are collective across critical infrastructure sectors.

It refers to practices, guidelines and industry standards in a way that allows for communication of cybersecurity activities and outcomes from top to bottom of the organizational hierarchy. The NIST framework Core comprises of five Functions—Identify, Protect, Detect, Respond, Recover. This can be considered a high-level approach of an organization's cybersecurity risk management.

B. **NIST FRAMEWORK IMPLEMENTATION TIERS** (''Tiers'') defines the extent to which an organization's cybersecurity risk management practices demonstrate the characteristics defined in the NIST Framework. There are four tiers (Partial, Risk Informed, Repeatable and Adaptive) that provide perspective on how an organization assess cybersecurity risk and the activities in place to manage that risk. Definitions of Tiers are as described below:

Tier 1 (Partial):

- *Risk Management Process* – the approach to cybersecurity risk management practices are unplanned, informal, and mitigative. Priority for cybersecurity activities may be low.
- *Integrated Risk Management Program* – the approach to managing awareness of cybersecurity risk is limited or has not been established. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – An organization may not have the practices in place to collaborate with other organizations.

Tier 2 (Risk Informed):

- *Risk Management Process* – the approach to cybersecurity risk management practices are approved by management but may not be strategically throughout the organization.
- *Integrated Risk Management Program* – the approach to managing awareness of cybersecurity risk is at the organizational level but an organization-wide methodology to managing cybersecurity risk has not been established.
- *External Participation* – The organization understand its responsibility in the larger environment, but does not have a formalized approach to impart to external parties.

Tier 3 (Repeatable):

- *Risk Management Process* – The organization's risk management practices are officially approved and communicated as policy.
- *Integrated Risk Management Program* – Management of cybersecurity risk is an organization-wide approach.
- *External Participation* – There is collaboration among partners and risk-based management decisions within the organization in response to incidents.

Tier 4 (Adaptive Risk Management Process): There is a process of continuous improvement wherein the organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.

- *Integrated Risk Management Program* – Cybersecurity risk management is embedded in the organizational culture. Methodology in managing cybersecurity risk is through organizational-wide risk-informed policies, processes, and procedures to address potential cybersecurity incidents.
- *External Participation* – A proactive, accurate and up-to-date information is being distributed and prior to cybersecurity incidents. There is an open sharing of data among partners.

C. ***NIST FRAMEWORK PROFILE (''Profile'').*** The Profile can be considered as the alignment of standards, guidelines, and practices to the Framework Core. Profiles can be characterized as ''gap analysis'' to identify opportunities for improving cybersecurity posture by comparing a ''Current'' Profile (the ''as found'' state) with a ''Target'' Profile (the ''desired'' state). The result of the ''gap analysis'' between the Current Profile and Target Profile can be used to aid prioritization and extent of development.

To enable critical infrastructure suppliers to achieve flexibility, the NIST framework depend on a range of existing standards, guidelines, and practices. Based from these standards, guidelines, and practices, the NIST provides a structure to conduct gap analysis from the current and target state,

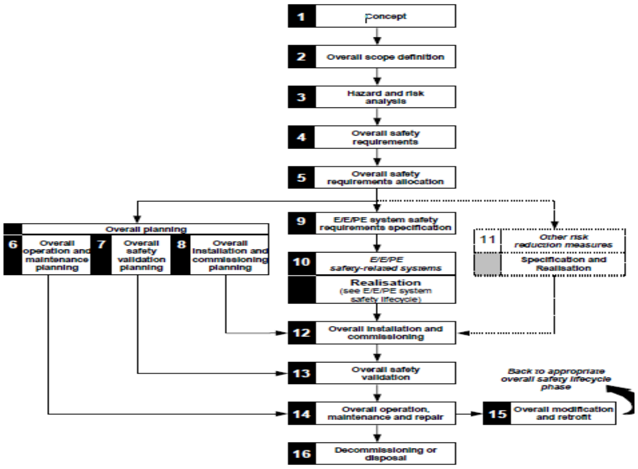

1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation (see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal

FIGURE 2. ISA 84 (IEC 61511) safety lifecycle phases [10].

prioritize improvement action plans, evaluate development to attain the desired target state and communicate among relevant stakeholders about cybersecurity risk.

III. ISA 84 (IEC 61511) - SAFETY INSTRUMENTED SYSTEM (SIS) STANDARD [4], [10]

Part of this proposal is to align safety standard to cybersecurity. In oil and gas, petrochemical and process industries, SIS is implemented to safely 'secure liquid inside the pipe' or keep a process under control from hazardous processes, and ensure that the instrumentation for functional safety is in place. These SIS have been used for many years to perform safety instrumented functions (SIF). It is essential that this instrumentation achieve certain minimum standards and performance levels if instrumentation is to be effectively used for SIF. This standard [10], which safety lifecycle is shown in Figure 2, addresses the application of SIS for the process industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. The risk assessment phase is proposed to be conducted using the Funnel Risk Graph Method (FRGM) and will be discussed in Section V. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s). This standard [10] is well-known and will not be discussed in detail.

IV. ISA 99 (IEC 62443) – INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS SECURITY

ISA 99 (IEC 62443) [11] aims to establish an industrial automation and control system security program, and is inherently referenced with the NIST framework. Figure 3 [5] represents the elements of the cyber security management system, which has three main categories:

- Risk analysis,
- Addressing risk with the Cybersecurity Management (CSMS), and
- Monitoring and improving the CSMS

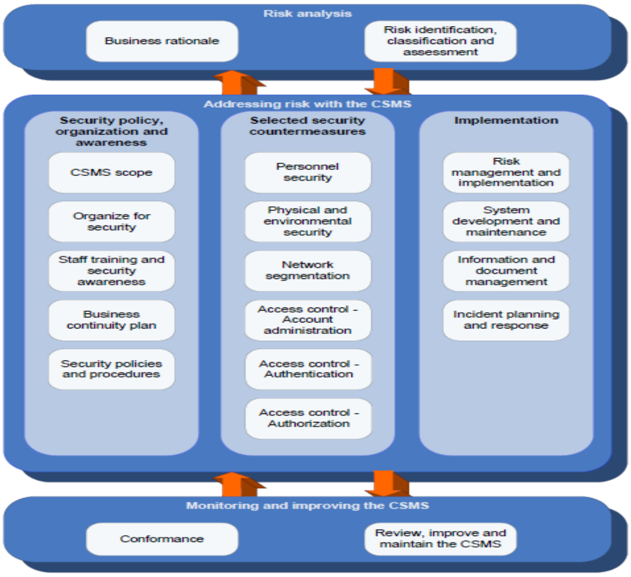

Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control - Account administration
Access control - Authentication
Access control - Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

FIGURE 3. ISA 99 (IEC 62443) [5].

While safety is aimed at protecting the systems from accidental failures to eliminate or minimize hazards, security is focused on protecting the systems from deliberate malicious attacks [6]. Technology in the past did not demand automation systems to be integrated and connected to the Internet. However, due to the proliferation of Internet-connected systems, security has become increasingly important. Even though SIS is typically not connected to the outside world, malicious hacking is still not impossible. With this vulnerability, it is proposed that SIS cybersecurity risk assessment should be included in its design and evaluation. The standard [11] elaborates the elements and provides guidance on what should be included for the establishment of an organization's cybersecurity management system (CSMS) for ICSS as a whole, in which SIS is part of. The CSMS elements pertain in this standard are majority discussed about policy, procedure, practice and personnel management suggesting what should be part of the organization's CSMS.

V. FUNNEL RISK GRAPH METHOD (FRGM) [6]

In [6], an application of a more cost-effective, simplified, and enhanced approach for the design and evaluation of Safety Instrumented Systems (SIS) called the Funnel Risk Graph Method (FRGM) was presented in Figure 4.

Instead of subjecting all SIF one-by-one to a much complex (semi-quantitative or quantitative) assessment process, the FRGM (qualitative) is aimed to use as a funnel or an "initial pass". If the assessed safety-related systems received SIL allocation of greater than SIL2 during the "initial pass" then a semi-quantitative or a quantitative method as a "final pass" should be conducted, or the multi-disciplinary assessment team reached an agreement to justify the "second pass", or pose a high Equipment Under Control (EUC) risk.

The 16 phase IEC61508 safety lifecycle with the inclusion of IEC62061, IEC61511, ISO13849 and AS4024.1 as

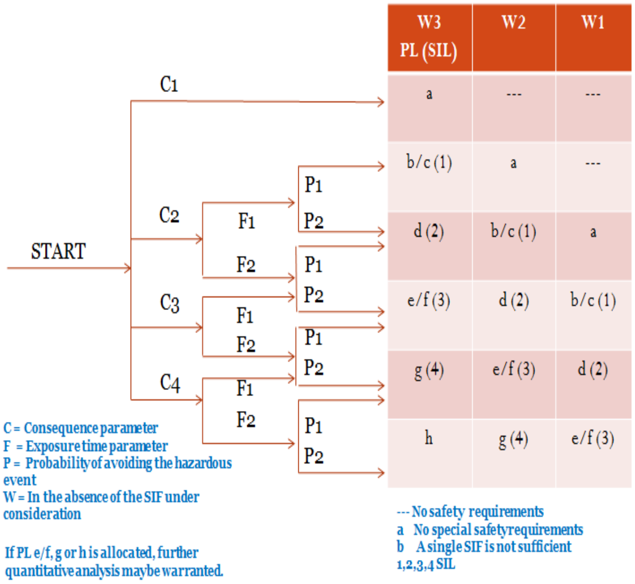

W3
PL (SIL)
W2
W1
START
C1
C2
C3
C4
F1
F2
P1
P2
a
---
b/c (1)
d (2)
e/f (3)
g (4)
h
C = Consequence parameter
F = Exposure time parameter
P = Probability of avoiding the hazardous event
W = In the absence of the SIF under consideration
If PL e/f, g or h is allocated, further quantitative analysis maybe warranted.
--- No safety requirements
a No special safety requirements
b A single SIF is not sufficient
1,2,3,4 SIL

FIGURE 4. **The funnel risk graph method [6].**

a combined safety lifecycle process [12] aims to establish safety requirements for plant, considering the specific circumstances and risks (e.g., environmental, operational, etc.) associated with its use, maintenance until the duration of the life of the plant.

The following phases of the safety lifecycle should be driven by the end-user to ensure that the safety requirements are appropriate for the specific application:

Phase 1: Concept
Phase 2: Scope
Phase 3: Hazard and Risk Analysis
Phase 4: Overall Safety Requirements
Phase 5: Safety Requirements Allocation
Phase 9: Safety Requirements Specification

The following phases of the safety lifecycle should be driven by the end-user to ensure that the safety requirements are adequately implemented and maintained:

Phase 6: Operation and Maintenance Planning
Phase 7: Safety Validation Planning
Phase 13: Safety Validation
Phase 14: Operations and Maintenance
Phase 15: Modification and Retrofit
Phase 16: Decommissioning

The responsibility for some of the realization phases of the safety lifecycle may be assigned to other organisation, however, it remains the end-user's responsibility to ensure that the other organisation complies with the requirements of Phase 8-12. FRGM focuses on *Phase 5: Safety Requirements Allocation.*

Phase 8: Installation and Commissioning Planning
Phase 10: E/E/PE Safety-related Systems Realisation
Phase 11: Other Risk Reduction Measures Specification and Realisation
Phase 12: Installation and Commissioning

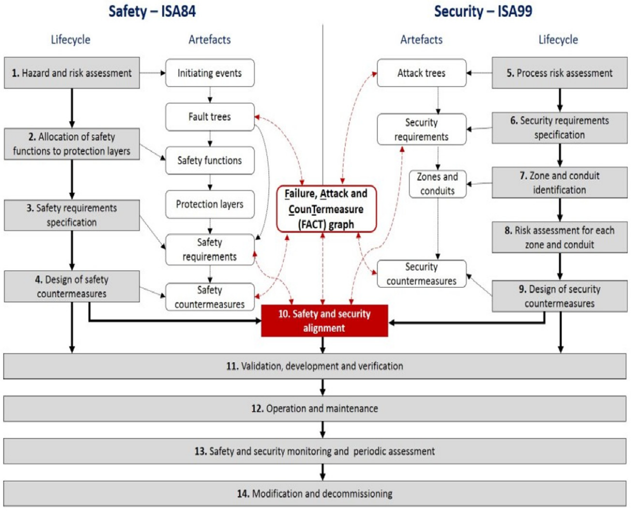

Safety – ISA84
Security – ISA99
Lifecycle
Artefacts
Artefacts
Lifecycle
1. Hazard and risk assessment
Initiating events
Attack trees
5. Process risk assessment
Fault trees
Security requirements
6. Security requirements specification
2. Allocation of safety functions to protection layers
Safety functions
Zones and conduits
7. Zone and conduit identification
Failure, Attack and CounTermeasure (FACT) graph
Protection layers
3. Safety requirements specification
Safety requirements
8. Risk assessment for each zone and conduit
Security countermeasures
4. Design of safety countermeasures
Safety countermeasures
9. Design of security countermeasures
10. Safety and security alignment
11. Validation, development and verification
12. Operation and maintenance
13. Safety and security monitoring and periodic assessment
14. Modification and decommissioning

FIGURE 5. **Merged ISA 84 (IEC 61511) and ISA 99 (IEC 62443) lifecycles [13].**

VI. RELATED WORK

There have been a few studies relating to the alignment of safety and security. Some of them are enumerated below.

A. ALIGNMENT BETWEEN SAFETY AND SECURITY STANDARDS ISA 84 (IEC 61511) AND ISA 99 (IEC 62443) [13]

The alignment is derived by merging safety and security lifecycle phases and is called the Failure-Attack-CounTermeasure (FACT) as the graph shown in Figure 5. It incorporates safety artefacts (fault trees and safety countermeasures) and security artefacts (attack trees and security countermeasures), and can be used during safety and security alignment analysis [13].

This proposed alignment between safety and security aims to ensure consistent implementation and help the organization to scrutinize latest system weaknesses, to ultimately provide necessary level of safety and security countermeasures.

The merged safety and security lifecycle model shown in Figure 5, which composed of 14 phases. The process begins with safety risk assessment and design phases (phases 1 – 4), borrowed from ISA 84 (IEC 61511), followed by security risk assessment and design phases (phases 5 – 9), from ISA 99 (IEC 62443). The alignment between safety and security is conducted in phase 10. The final phase of the lifecycle, phases 11-14 are the merged phases of ISA 84 and ISA 99 lifecycles and include validation, development, and verification, operation and maintenance, safety and security monitoring and periodic assessment, and modification and decommissioning related activities.

B. INTEGRATING INDUSTRIAL CONTROL SYSTEM (ICS) SAFETY AND SECURITY [14]

This study [14] proposes some techniques that can be used, and potentially development of ICS security. This provides a

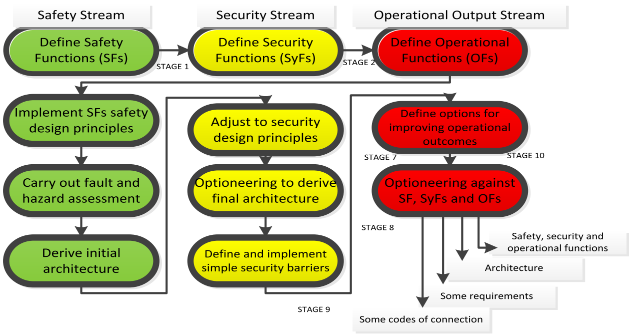

Safety Stream
Security Stream
Operational Output Stream
Define Safety Functions (SFs)
STAGE 1
Define Security Functions (SyFs)
STAGE 2
Define Operational Functions (OFs)
Implement SFs safety design principles
Adjust to security design principles
Define options for improving operational outcomes
STAGE 7
STAGE 10
Carry out fault and hazard assessment
Optioneering to derive final architecture
Optioneering against SF, SyFs and OFs
STAGE 8
Safety, security and operational functions
Derive initial architecture
Define and implement simple security barriers
Architecture
Some requirements
STAGE 9
Some codes of connection

FIGURE 6. Safety, security and operational output Stream [14].

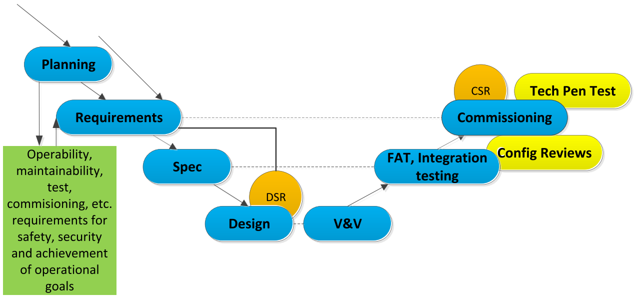

Planning
Requirements
Operability, maintainability, test, commisioning, etc. requirements for safety, security and achievement of operational goals
Spec
DSR
Design
V&V
FAT, Integration testing
Config Reviews
Commissioning
CSR
Tech Pen Test

FIGURE 7. V-model Lifecycle [10].

logical and structured approach through continual consideration of the effect of decisions on pre-determined and prioritized safety, security and operational functions throughout the design and implementation lifecycle. It proposes some techniques that can be employed in whole or part, are scalable and are suitable for further investigation, and potentially development by one of the groups currently looking at ICS security.

Figure 6 shows the interconnection among activities involved in defining safety, security and operational functions. It is important that each activity stream (Safety, Security and Operational output) must be performed by specialists on their field and then collaboration among them is crucial to the success of the activities.

Several stages need to be conducted to define safety, security and operational functions, define ICS architecture, and once an architecture has been decided, this can be inputted into a design lifecycle. The design lifecycle is based on a V-model as shown in Figure 7.

C. SAFETY AND SECURITY AWARE FRAMEWORK FOR THE DEVELOPMENT OF FEEDBACK CONTROL SYSTEMS [15]

This study [15] is for the military drive-by-wire land systems and civilian vehicles. The fundamental part of the study is to proposed a framework consists of a Simulink model for the development of feedback control system as shown in Figure 8.

The structure of the framework was presented in a manner that aligns safety and security within the design stage in a modular concept. These systems often include network enabled capability (NEC) allowing the use of electronics architectures to integrate different sub-systems. However, like ICSS, this increased complexity of integration capability is accompanied with augmented safety and cybersecurity risks. The study analyzes how the process of developing feedback control system for military land systems could benefit from the use of a framework that addresses safety and security issues at the system modelling level. Figure 9 shows each of the modules except the Control Input Unit Modules (CIUMs) and the Control Output Unit Modules (COUMs) is made of the sub-modules.

D. ANALYSIS OF THESE METHODS

The presented methods in integrating safety and security were good theoretical approach, however, they lack economic justification and/or practicality. FACT graph method showing merging of ISA 84 (IEC 61511) and ISA 99 (IEC 62443) lifecycles did not demonstrate economic viability. Likewise, safety, security and operational output stream did not expound the practical aspect of the said approach. Similarly, the development of feedback system utilizing safety and security framework did not present practical quantifiable benefits.

VII. OUR PROPOSAL – OVERVIEW

Our core proposal is a seamless integration of cybersecurity framework by the National Institute of Standards and Technology (NIST) [9] with safety and security standards ISA 84 (IEC 61511) [10] and ISA 99 (IEC 62443) [110], and the novel Funnel Risk Graph Method (FRGM) as shown in Figure 4. Economic benefits and practicality are presented.

The Functions [9] can be conducted in parallel and constantly to address the changing cybersecurity and safety risk. Except Risk Assessment and FRGM, functions below are not envisioned to form a sequential path or come to a final complete state, rather it is dynamic.

- Identify – The activities in this function are the building block for operative use of the NIST and FRGM framework. This includes development of the organizational understanding to manage cybersecurity and safety risk to systems, assets, data, and capabilities. Expected outcome categories within this function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy as shown in Figure 10.
- Risk Assessment – This can serve as risk assessment for cybersecurity and for safety. The organization's risk management process can be utilized to analyze the operational environment to distinguish the likelihood and impact of a cybersecurity event. For safety, the organization can utilize FRGM [6]:
- FRGM [6] – Use FRGM instead of using traditional standard methods such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and semi-quantitative method Layers of Protection Analysis (LOPA).

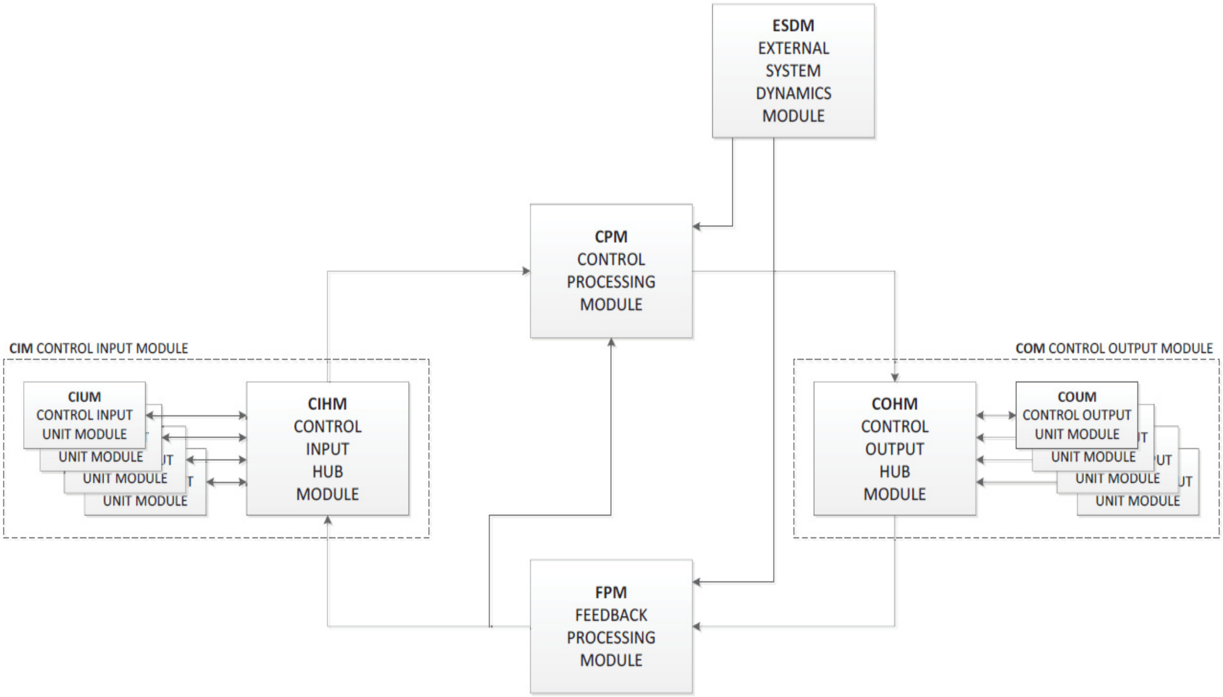


FIGURE 8. Top level architecture of the Simulink model of the framework [15].

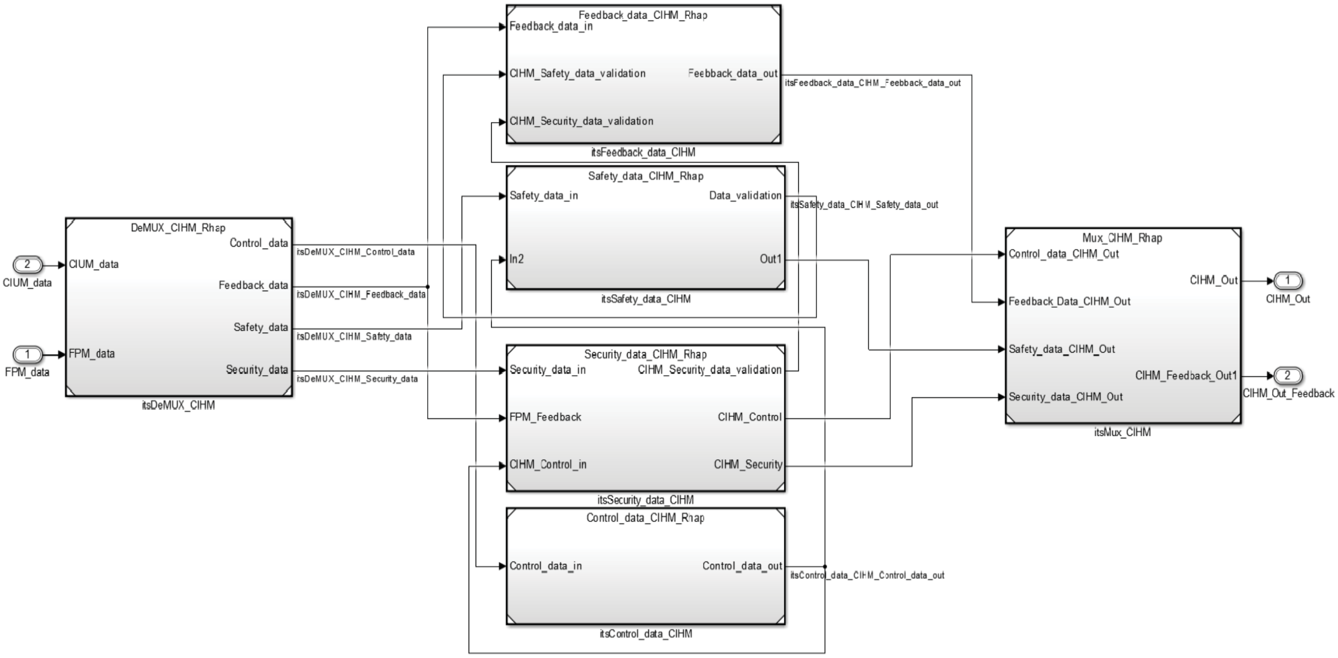


FIGURE 9. Processing segmentation inside the main modules of the framework [15].

- Protect – The Protect function supports the ability to constraint or exclude the impact of a potential cybersecurity incident by development of appropriate measures. Expected outcome categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- Detect – The Detect function facilitates suitable detection of cybersecurity incidents through development of appropriate activities. Expected outcome categories within this function includes: Anomalies and

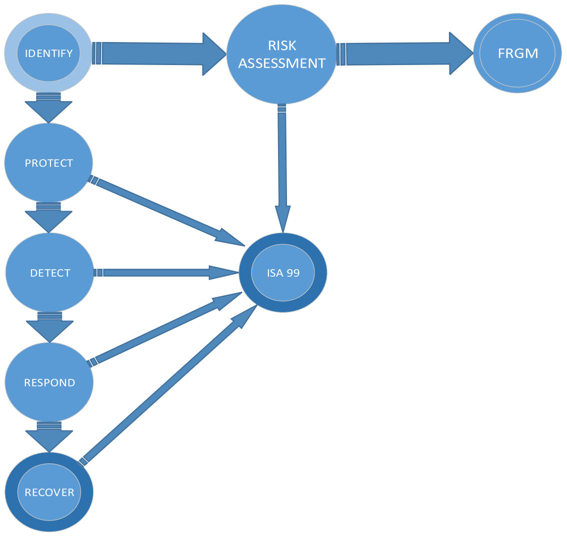


FIGURE 10. Overview of the alignment framework.

Events; Security Continuous Monitoring; and Detection Processes.

- Respond – Mitigative action regarding an identified cybersecurity incident.
- ISA 99 (IEC 62443) – NIST framework is inherently referenced with ISA 99.
- Recover - The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

VIII. OUR DETAILED PROPOSAL: ALIGNMENT OF THE NIST FRAMEWORK [9] WITH THE FRGM [6]

A. ALIGNMENT OF THE NIST FRAMEWORK WITH THE FRGM

Figure 11 shows our detailed proposed framework for the alignment of NIST with FRGM. The framework can be used to create a new cybersecurity and safety program or improve an existing program. These steps are iterative process until appropriate stage has been reached. This can be achieved using the following steps.

Step 1 (NIST – Identify, Scope and Prioritize): At a high-level, the organization identifies its business/mission objectives. With this information, the organization makes strategic decisions regarding cybersecurity and safety implementations and determines the scope of systems and assets that support the selected business line or process. Scoping includes identification and inventory of all assets involved. Using the NIST framework as show in Figure 11, the *Identify* step is performed. The activities in the Identify Function provides groundwork for are foundational for valuable use of NIST. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The activities in the Identify stage are shown in Figure 11 that includes, Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy.

Step 1.1 (NIST + FRGM - Perform a Risk Assessment (ID.RA)): The organization's risk management process can be utilise to analyse the operational environment to distinguish the likelihood and impact of a cybersecurity (using ISA 99) event and safety (using ISA 84). This is where the proposed integration of NIST and FRGM takes place. Highlighted boxes in Figure 11 are the path towards FRGM. The combined safety lifecycle process on *Phase 5: Safety Requirements Allocation* using the FRGM was based on [10] in reference to the general scheme described in [16] but characterized as a "*funnel*" approach. Typically, a medium-sized plant is comprised of thousands of SIF. Instead of subjecting all SIF one-by-one to a much complex (semi-quantitative or quantitative) assessment process, the FRGM (qualitative) is aimed to use as a funnel or an "*initial pass*". If the assessed safety-related systems received SIL allocation of greater than SIL2 during the "*initial pass*" then a semi-quantitative or a quantitative method as a "*final pass*" should be conducted, or the multi-disciplinary assessment team reached an agreement to justify the "second pass", or pose a high EUC risk.

The three (3) steps to the FRGM approach are as follows:

Step 1: Select one parameter (say Consequence C2 parameter) from Figure 4;

Step 2: Chosen parameters are then linked to other parameters (Exposure, Probability, Demand W);

Step 3: Resolve the SIL allocated to the SIF.

For example, Consequence C2, Frequency F1, Probability P1 with demand W3 would yield a SIL1. But if the Probability changes to P2 with the same condition, then SIL2 is allocated.

The FRGM approach can also be utilized to enable assessment of SIS where the potential consequences include severe environmental impact or property loss.

Step 2 (NIST - Protect): This step involves development and implementation of the required appropriate defenses deployed to critical infrastructure services. The expected result of this step includes Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance and Protective Technology as shown in Figure 11. This is part of the preventative measures of the Framework.

Step 3 (NIST - Detect): This step involves development and implementation of applicable activities to identify the occurrence of a cybersecurity event. This function enables timely discovery of cybersecurity events. Some of the examples of result include Anomalies and Events, Security Continuous Monitoring and Detection Processes. This function is critical such that detection process must be effective to determine real threats and vulnerabilities.

Step 4 (NIST - Respond): This step involves development and implementation of applicable activities to take action regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential

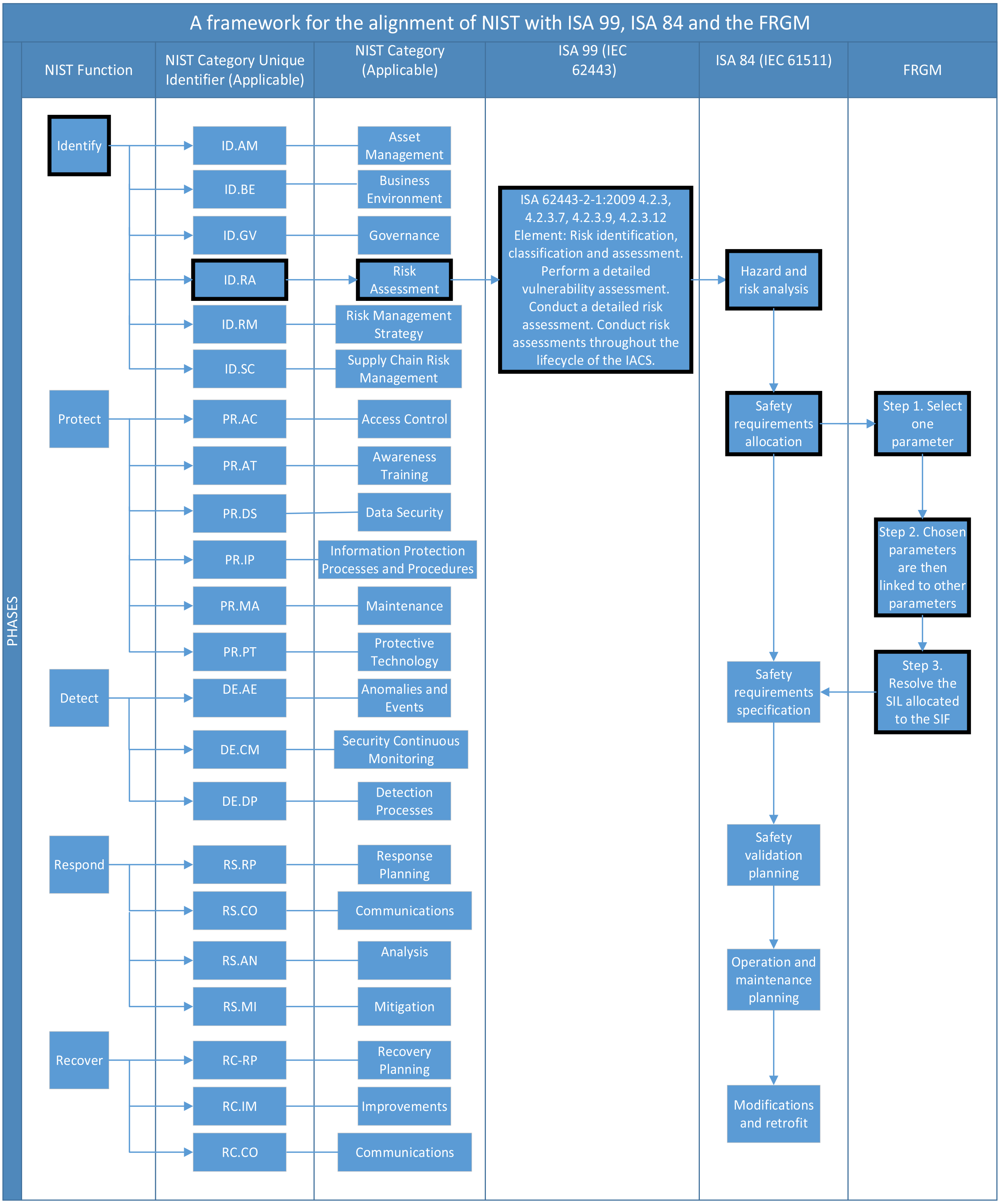

A framework for the alignment of NIST with ISA 99, ISA 84 and the FRGM
PHASES
NIST Function
NIST Category Unique Identifier (Applicable)
NIST Category (Applicable)
ISA 99 (IEC 62443)
ISA 84 (IEC 61511)
FRGM
Identify
ID.AM
Asset Management
ID.BE
Business Environment
ID.GV
Governance
ID.RA
Risk Assessment
ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 Element: Risk identification, classification and assessment. Perform a detailed vulnerability assessment. Conduct a detailed risk assessment. Conduct risk assessments throughout the lifecycle of the IACS.
Hazard and risk analysis
ID.RM
Risk Management Strategy
ID.SC
Supply Chain Risk Management
Protect
PR.AC
Access Control
Safety requirements allocation
Step 1. Select one parameter
PR.AT
Awareness Training
PR.DS
Data Security
Step 2. Chosen parameters are then linked to other parameters
PR.IP
Information Protection Processes and Procedures
PR.MA
Maintenance
PR.PT
Protective Technology
Step 3. Resolve the SIL allocated to the SIF
Detect
DE.AE
Anomalies and Events
Safety requirements specification
DE.CM
Security Continuous Monitoring
DE.DP
Detection Processes
Safety validation planning
Respond
RS.RP
Response Planning
RS.CO
Communications
RS.AN
Analysis
Operation and maintenance planning
RS.MI
Mitigation
Recover
RC-RP
Recovery Planning
Modifications and retrofit
RC.IM
Improvements
RC.CO
Communications

FIGURE 11. Detailed framework for the alignment of NIST and FRGM.

cybersecurity event. Examples of outcome categories within this function include Response Planning, Communications, Analysis, Mitigation and Improvements.

Step 5 (NIST - Recover): This step involves development and implementation of applicable activities to maintain plans for resilience and to restore any capabilities or services that were affected due to a cybersecurity event. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this function include Recovery Planning, Improvements and Communications. Restoration test activities are important to this step.

B. ADVANTAGE OF THIS PROPOSAL

Alignment of safety and security has many advantages. Both of them can utilise the same systems and assets that support the selected business line or process. Evaluating them against cybersecurity threats and safety risks using the integrated NIST and FRGM framework in one approach could eliminate or minimize loss to an organization thus entail economic advantage. For safety risk assessment, given the complexity of process industries, SIL and PL allocation should be performed via a quantitative or semi-quantitative methodology. However, it may be impracticable to apply a semi-quantitative or quantitative approach due to the substantial amount of time and resources involved, thus FRGM [6] approach is proposed as part of Step 4 above. The main difference with this proposed technique is that, instead of jumping in to costly and time-consuming methods (semi-quantitative or quantitative), all SIF will first undergo FRGM (qualitative), which usually takes only a few minutes for each SIF to collaborate with a multi-disciplinary team assuming that calibration process has been completed. Only those SIF which falls under the following category, which typically around 5% of the total SIF, will undergo a quantitative or semi-quantitative method:

- SIF with SIL allocation of more than SIL2 during the FRGM "*initial pass*".
- Did not achieve a satisfactory level of consensus within the multi-disciplinary team during the "*initial pass*".
- Pose a high EUC risk.

In order to show the simplicity and effectiveness of the FRGM, a block diagram of a conveyor safety system with three SIF is presented in Figure 12.

C. SIF#1, SIF#2 AND SIF#3 ANALYSES

The process involves transporting and handling of solids through a conveyor belt. All SIF is designed to disable any movement of the conveyor belt and its associated equipment during emergency or metal detection. SIF#1 safety switches activation is done via pulling the trip cable or from a broken trip cable i.e., total loss of tension on it. The two Normally-Close (NC) switches are connected in series; opening of the contacts of any of the two switches will activate the SILBUS/PILZ relay system and trips the conveyor. A beacon light is also connected to indicate switch activation. SIF#2 metal detector is used to sense any unwanted presence of metal in the conveyor and eventually disable conveyor movement. SIF#3 operator lanyard safety switches have similar function to SIF#1. However, the risk is located near to the operator station, where permanent exposure or almost permanent exposure is evident. The collaborative risk assessment [16] was conducted by a team of multi-disciplinary personnel which was composed of process control engineer, process specialist, safety specialist, control room and field operators with combined work experience of over 100 years.

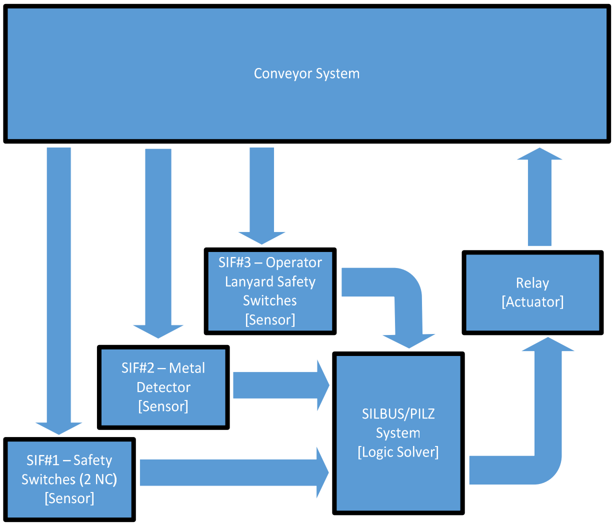

Conveyor System
SIF#3 – Operator Lanyard Safety Switches [Sensor]
Relay [Actuator]
SIF#2 – Metal Detector [Sensor]
SILBUS/PILZ System [Logic Solver]
SIF#1 – Safety Switches (2 NC) [Sensor]

FIGURE 12. Block diagram of conveyor safety system.

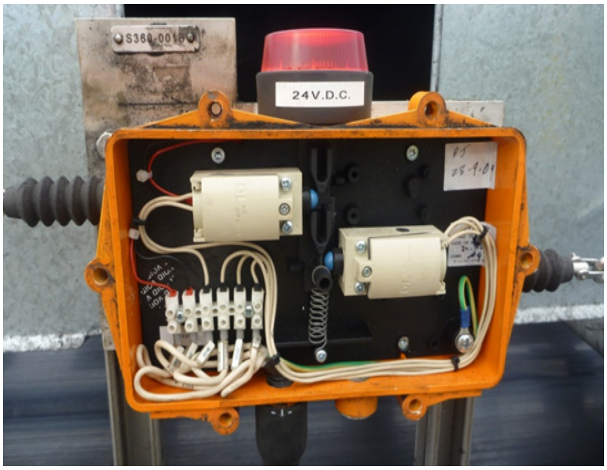


FIGURE 13. SIF#1 – A100 - safety switch.

Figure 13 shows the safety switch - SIF#1 – A100 and was evaluated using the proposed FRGM. The FRGM serves as an "*initial pass*" before going into a much complex assessment process, if required. Using the FRGM steps mentioned in Section VIII, Step 1.1:

Step 1: Select one parameter (Consequence C3 parameter was selected). C3 – Permanent disability or fatality;

Step 2: Chosen parameters are then linked to other parameters (Exposure F1, Probability P1, and Demand W3). F1 – rare to frequent exposure, P1 – avoidance is possible under certain conditions, W3 – function is demanded more than once per year;

Step 3: Resolve the SIL allocated to the SIF.

In this case, it was easily evaluated that the SIL for SIF#1 – A100 is SIL 2 as shown in Figure 14. Since this is only

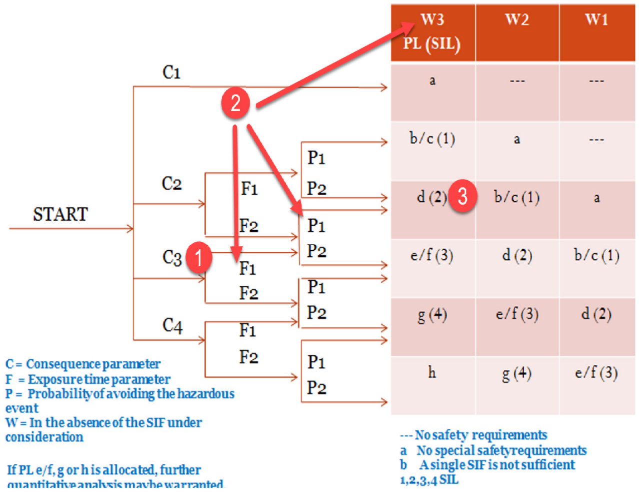

W3
PL (SIL)
W2
W1
C1
C2
C3
C4
START
F1
F2
P1
P2
1
2
3
a
---
b/c (1)
d (2)
e/f (3)
g (4)
h
C = Consequence parameter
F = Exposure time parameter
P = Probability of avoiding the hazardous event
W = In the absence of the SIF under consideration
If PL e/f, g or h is allocated, further quantitative analysis maybe warranted
--- No safety requirements
a No special safety requirements
b A single SIF is not sufficient
1,2,3,4 SIL

FIGURE 14. Result of SIF#1 using FRGM.

TABLE 1. Calibration of risk graph.

C (Consequence) Parameter	Description
C1	Minor injury (non-permanent)
C2	Serious injury (non-permanent)
C3	Permanent disability or fatality
C4	Multiple fatalities
F (Exposure) Parameter	**Description**
F1	Rare to frequent exposure
F2	Permanent exposure or almost permanent exposure
P (Avoidance) Parameter	**Description**
P1	Avoidance is possible under certain conditions (e.g., independent facilities are provided to alert exposed persons, independent facilities are provided to shutdown the plant, danger is easily recognised and there is sufficient time for persons to escape the hazard, or actual safety experience indicates that avoidance is possible)
P2	Avoidance is not possible or is almost impossible
W (Demand) Parameter	**Description**
W3	Function is demanded more than once per year
W2	Function is demanded less than once per year but more than once per 10 years
W1	Function is demanded less than once per 10 years.

TABLE 2. Summary of risk assessment and allocations using FRGM for SIF#1, SIF#2 and SIF#3.

SIF Identifier	SIF Description & Function	Allocations (C, F, P, W)				SIL	PL	CAT
SIF#1 – A100	C100 Conveyor Belt Gate Interlock Safety Switches	C3	F1	P1	W3	2	d	3
SIF#2 – M100	M100 Metal Detector	C2	F1	P1	W3	1	b/c	2
SIF#3 – A200	C200 Operator Lanyard Safety Switches	C3	F2	P1	W3	3	e/f	4

TABLE 3. Comparison between Standard Method and FRGM.

Criteria	Standard Methods (LOPA, FTA, ETA)	FRGM	Time Reduction	Cost Reduction ($150/hr. rate)
Time & Cost Reduction	Approximately 2.5 hours per SIF x 3,000 SIF = 7,500 hours	Approx. 20 minutes per SIF x 3,000 SIF = 990 hours	6,510 hours	$976,500
Steps Involved	13 steps for LOPA	3- step process		
Pros	More accurate assessment of risk.	Straight forward, resource-efficient		
Cons	Requires a lot of resources	Coarser or less accurate assessment of risk		

TABLE 4. Summary of risk assessment and allocations using LOPA – SIF#1 – A100.

#	1	2	3	4	5	6	7	8	9	10	11	12	13
	Impact event	Severity level	Initiating cause	Initiation likelihood	General process	BPCS	Alarms	Additional mitigation,	IPL additional	Intermediate likelihood	SIF integrity	Mitigated event	Notes
SIF#1 – A100	Permanent disability or fatality	Serious	Loss of tension	0.1	0.1	0.1	0.1	0.1	Machine guards	10^{-7}	**10^{-2} SIL2**	10^{-9}	Lanyard switch non-SIL rated
SIF#2 – M100	Serious injury (non-permanent)	Minor	Sensor failure	0.01	0.1	0.1	0.1	0.1	Machine guards	10^{-8}	**10^{-1} SIL1**	10^{-9}	Sensor requires regular cleaning
SIF#3 – A200	Permanent disability or fatality	Extensive	Loss of tension	0.1	0.1	0.1	0.1	0.5	Machine guards	5×10^{-7}	**10^{-3} SIL3**	5×10^{-10}	Lanyard switch non-SIL rated

SIL 2, it can be used as the assessed SIL. If the assessed safety-related system received SIL allocation of greater than SIL 2, during the "*initial pass*" then a semi-quantitative or a quantitative method as a "*final pass*" should be conducted. This is true in the case of SIF#3 – A200, which received a SIL 3. Since this SIF demands a higher safety function, it is justified that it will undergo a more complex process such as quantitative methodology.

At the discretion of the multi-disciplinary assessment team, they can come into an agreement to justify the "*final pass*" even though the outcome of FRGM is SIL 2 or less. Further justification for a final pass also includes those SIFs that are involved in preventing or mitigating high consequence events and which are the only risk control against a risk. Using the FRGM and corporate calibrated risk graph shown in Table 1, the result of safety risk assessment is shown in Table 2. SIL 2 is required for SIF#1 – A100, SIL 1 for SIF#2 –M100 and SIL 3 for SIF#3 – A200.

Table 3 shows the comparative differences between the standard quantitative methods such as FTA, ETA and semi-quantitative method LOPA, as compared to the proposed FRGM approach at 3,000 SIF. Cost reduction is realised by the number of hours spent by a multi-disciplinary team. Pros and cons using the proposed FRGM approach as compared to the standard approach are also shown in Table 3. The coarser or less accurate assessment of risk using the FRGM is not a concern as it is used as a funnel from a broad range of SIL 0 to SIL 2. Interestingly, the same safety function can be achieved using any of the methodology as shown in Table 4. A lot of resources can be saved using the simple FRGM.

IX. CONCLUSION

Safety and security are two key properties of ICSS. Safety focuses at protecting the systems from accidental faults, while security is aimed at protecting the systems from intentional attacks. Evaluating both safety and cybersecurity into an integrated framework is aimed at process optimisation and '*to leave no stone unturned*' using a single unified methodology. In this age of oil and gas economic downturn, an organisation should improve its processes and procedures to concentrate on its core objective. The safe and secure operation of critical oil and gas infrastructure is dependent on appropriate responses to safety, security and operational priorities into ICSS, at design stage and throughout the life of the system. The objective of this proposal is to come up with an integrated and optimised evaluation framework of ICSS and related subsystems considering cybersecurity and safety. This can be achieved by the alignment of the NIST cybersecurity framework with safety and security standards ISA 84 (IEC 61511) and ISA 99 (IEC 62443), and the FRGM.

REFERENCES

[1] BBC News. (May 15, 2017). *WannaCry Ransomware Cyber-Attacks Slow But Fears Remain*, accessed on May 18, 2017. [Online]. Available: http://www.bbc.com/news/technology-39920141#_=_

[2] (Jun. 2014). Oil and Gas Cyber Security Conference. Oslo, Norway. accessed on Jul. 6, 2017. [Online]. Available: http://www.Smi-online.co.uk/energy/europe/conference/Oil-and-Gas-Cyber-Security-Nordics?utm_source=E-046&utm_medium=oilandgas-cybersecurity7.asp&utm_campaign=GOTO&o=login&dl=br&p1=4515#tab_overview

[3] L. Piètre-Cambacèdés and M. Bouissou, "Cross-fertilization between safety and security engineering," *Rel. Eng. Syst. Safety*, vol. 110, pp. 110–126, Feb. 2013.

[4] *Application of Safety Instrumented Systems for the Process Industries*, Doc. ANSI/ISA 84.00.01-2004, Instrum., Syst., Autom. Soc., Research Triangle Park, NC, USA, 2004.

[5] *Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models*. Doc. ANSI/ISA-99-00-01-2007, Instrum., Syst., Autom. Soc., Research Triangle Park, NC, USA, 2007.

[6] A. Gabriel, "Design and evaluation of safety instrumented systems: A simplified and enhanced approach," *IEEE Access*, vol. 5, pp. 3813–3823, Mar. 2017, doi: 10.1109/ACCESS.2017.2679023.

[7] G. Stoneburner, "Toward a unified security-safety model," *Computer*, vol. 39, no. 8, p. 96, Aug. 2006.

[8] *ISA 99 Work Group 7—Safety and Security (Joint with ISA84 Committee)*, accessed on Apr. 11, 2014. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/WG7.aspx

[9] *Framework for Improving Critical Infrastructure Cybersecurity*, Doc. 20899, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Feb. 2014.

[10] *Functional Safety-Safety Instrumented Systems for the Process Industry Sector, Parts 1–3*, IEC61511, International Electrotechnical Commission, Geneva, Switzerland, 2003.

[11] *Industrial Communications Networks-Network and System Security-790 Part 2–1: Establishing An Industrial Automation and Control System 791 Security Program, Edition 1.0*, IEC62443-2-1, International 792 Electrotechnical Commission, Geneva, Switzerland, 2011.

[12] M. Punch, *Functional Safety for the Mining and Machinery-Based Industries*, 2nd ed. Tenambit, Australia: Marcus Punch Pty Ltd., 2013.

[13] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Proc. 1st Asia–Pacific Conf. Complex Syst. Design Manage. (CSD M Asia)*, 2014, pp. 41–53, doi: 10.1007/978-3-319-12544-2_4

[14] A. Ellis, "Integrating industrial control system (ICS) safety and security—A potential approach," in *Proc. 10th IET Syst. Safety Cyber-Secur. Conf.*, 2015, pp. 1–7, doi: 10.1049/cp.2015.0294.

[15] J. P. Lobo, P. Charchalakis, and E. Stipidis, "Safety and security aware framework for the development of feedback control systems," in *Proc. 10th IET Syst. Safety Cyber-Secur. Conf.*, 2015, pp. 1–5, doi: 10.1049/cp.2015.0280.

[16] *Electric/Electronic/Programmable Electronic Safety Related Systems, Parts 1–7*, IEC61508, International Electrotechnical Commission, Geneva, Switzerland, 2010.

ANGELITO GABRIEL (M'17) received the Instrumentation Technology degree (with most outstanding distinction) from the Don Bosco Technical College, the B.S. degree in computer engineering from the ICS, Pennsylvania, USA, the B.S. degree in mechanical engineering from the Polytechnic University of the Philippines, and the M.B.A. degree (Hons. with distinction) from the Ateneo Graduate Schools of Business, Philippines, in 2003. He is currently pursuing the Ph.D. degree at the University of Western Australia and Victoria University.

He is currently a Process Control Network Support Specialist with Chevron Australia. His research interests include control systems, safety instrumented systems, cybersecurity, and process control networks. He is a Fellow and a Chartered Professional Engineer of the Institution of Engineers Australia, TUV Functional Safety Engineer from Rheinland, Germany, and a Senior Member of ISA.

JUAN SHI (M'91) received the B.E. degree (Hons.) in electrical engineering from Northwest University, China, in 1988, and the Ph.D. degree in electrical engineering from Victoria University (VU), Melbourne, Australia, in 1995. She received the Graduate Certificate in Tertiary Education from VU in 2003.

She joined VU as a Lecturer in 1994, where she is currently an Associate Professor with the College of Engineering and Science. Her current research interests include automatic control and applications, power system stability, intelligent control and applications to smart energy systems, system identification, and engineering education.

CAGIL OZANSOY received the B.Eng. degree (Hons.) in electrical and electronic engineering and the Ph.D. degree in power system communications from Victoria University, Melbourne, Australia, in 2002 and 2006, respectively. He is currently a Senior Lecturer and a Researcher with the College of Engineering and Science, Victoria University. His major teaching and research focus is on electrical engineering, renewable energy technologies, power systems protection and communications, energy from waste, and distributed generation. He has over 50 publications detailing his work and contributions to these areas.