|  |  |
| --- | --- |
| cetlogo ***CHEMICAL ENGINEERING TRANSACTIONS***  ***VOL., 2025*** | A publication of  aidiclogo_grande |
| The Italian Association  of Chemical Engineering  Online at www.cetjournal.it |
| Guest Editors:  Copyright © 2025, AIDIC Servizi S.r.l. **ISBN**; **ISSN** | |

Effective Cybersecurity Risk Assessment Approach for Integrating in Process Safety Management

Masayuki Tanabea,b,\*, Atsumi Miyakeb

aStrategic PSM Initiative Group LLC [23-17-408, Sakuragaoka-Cho, Shibuya 150-0031, Japan]

bYokohama National University [79-1, Hodogaya-ku, Yokohama, 240-8501, Japan]

tanabe.masayuki@strategic-psm.com

Cyberattacks targeting the process industry have become increasingly prevalent in recent years. The ISA TR84.00.09 standard and the CCPS guidelines propose methodologies for conducting process risk assessments against cyberattacks on process facilities, such as attacks on the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS), to ensure robust functional requirement management throughout the plant lifecycle. However, hazard identification and risk assessment techniques addressing process incidents triggered by cyberattacks remain largely unstandardized. Contemporary cybersecurity (CS) risk assessments predominantly focus on general Information Technology (IT) risks within business contexts. A notable contributing factor is the persistent misalignment between IT and Operational Technology (OT), including Process Safety (PS). OT professionals often regard CS as the responsibility of IT personnel, while IT teams typically lack familiarity with OT systems. Consequently, integrated IT-OT risk assessments are not widely implemented. This study explores an effective framework and methodology for conducting CS risk assessments specific to process incidents. The research utilizes a typical LNG plant model as the basis for a detailed CS risk assessment. The findings reveal several potential pathways for cyberattacks that could lead to major process incidents, underscoring the criticality of inherent safety measures and effective coordination between CS and PS disciplines. The CS risk assessment framework and procedural guidance detailed in this study are anticipated to significantly enhance the effectiveness of CS risk evaluations and the precise definition of functional requirements to mitigate cybersecurity risks.

* 1. Introduction

The past several years have witnessed several cybersecurity incidents targeting process industries and other hazardous sectors. In response to the escalating frequency of such cyberattacks, the concept of risk-based cybersecurity (CS) management, underpinned by CS risk assessment methodologies, was introduced (CCPS, 2022; ISA, 2017). The Yokohama National University (YNU) Strategic PSM Initiative Group (SPSM) proposed a comprehensive framework in 2020 to facilitate the effective implementation of risk-based process safety (RBPS) management systems within existing plant organizations (YNU SPSM, 2022). Given the adaptability of the proposed Process Safety Management (PSM) framework to other Management System (MS) elements, SPSM initiated research to extend the framework to encompass CS management through the application of CS risk assessment methodologies. This paper examines the CS risk assessment methodology for addressing cyberattacks targeting process incidents and identifies the challenges associated with integrating this methodology into PSM, as revealed through case studies conducted using model LNG plant data.

* 1. Strategic PSM concept

The SPSM outlines the design flow for a Management System (MS) as illustrated in Figure 1. This process comprises several stages: "Collect Baseline Information," "PSM Gap Analysis," which evaluates the discrepancies between the current state and the desired goals of the MS, "Design Management System," where the essential requirements to bridge these gaps are defined, "Management Plan (New Baseline)," and "Conduct of PSM."

If the necessary requirements for cybersecurity (CS) can be identified and defined through CS risk assessment methodologies, CS risk management can be seamlessly integrated into PSM by incorporating CS functional requirements within the same MS framework. Notably, this integration is centered on the management of cyberattacks specifically targeting process incidents, excluding broader cyberattacks on business systems, similar to how PSM is focused on addressing process incidents caused by hazardous material leaks from process facilities.



Figure 1: SPSM Concept for Designing PSM with CS Functional Requirements

* 1. Overview of cybersecurity risk assessment programme

Various cybersecurity (CS) risk assessment methods are available for addressing cyberattacks targeting process incidents, including CS-PHA (Preliminary Hazard Analysis), CS-HAZOP (Hazard and Operability Study), and CS-LOPA (Layer of Protection Analysis). However, international guidelines (CCPS, 2022; ISA, 2017) emphasize not merely the application of individual methods but the adoption of a combined approach. This strategy involves employing the appropriate methods in sequence, aligned with specific phases of the facility design lifecycle (e.g., the design phase of the plant lifecycle). Figure 2 illustrates the implementation flow of a CS risk assessment. The process begins with collecting Baseline Information related to the facilities under assessment, such as process flow diagrams, site layout plans, and network configuration diagrams. Subsequently, the network configuration is segmented into "Systems Under Consideration" (SUCs), analogous to "nodes" in conventional HAZOP for process safety. The CS-PHA method is then utilized to evaluate and identify worst-case scenarios for each SUC, including scenarios where hackers gain control over plant operations or disable Safety Instrumented Systems (SIS), potentially leading to significant hazards, including personnel injuries, environmental damage, or business losses. In this study, the CS-HAZID (Hazard Identification) method is employed as one of the tools under CS-PHA. For SUCs identified as higher risk, the CS-HAZOP method provides a more detailed analysis of cyberattack paths leading to worst-case scenarios identified during the CS-PHA stage. The CS-LOPA method subsequently quantifies the risks associated with identified cyberattack scenarios and assesses whether adequate Process Safety (PS) and CS protection layers are in place to mitigate these risks to an acceptable level. The LOPA methodology mirrors the process used in PS-LOPA. Where residual risk gaps to acceptable levels are identified, they are categorized under Security Level (SL), a concept akin to Safety Integrity Level (SIL). The CS risks and their corresponding protection layers are systematically identified and evaluated through this series of assessments. Figure 3 highlights the roles of CS-HAZID, CS-HAZOP, and CS-LOPA in addressing specific aspects of a bow-tie diagram representing process safety. Functional requirements, such as reliability metrics and inspection frequencies, are assigned to each protection layer to ensure effective operation and maintenance controls.



Figure 2: Cybersecurity Risk Assessment Flow Chart



Figure 3: Cybersecurity Risk Assessment Coverage in Bowtie Chart

* 1. Case Study

Although international guidelines outline a framework for cybersecurity (CS) risk management, they provide limited information on the detailed methodologies for conducting CS risk assessments. To address this gap, a case study was undertaken to examine the CS risk assessment process and identify opportunities for further improvement in practical implementation. In particular, the functional requirements for CS risk management must be derived from CS risk assessments and seamlessly integrated into Process Safety Management (PSM) to ensure robust process safety against cyberattacks during the operation and maintenance (O&M) of process plants.

* + 1. Plant Data used in the Case Study

In this case study, a typical configuration of an LNG liquefaction process plant was utilized as a model (Figure 4). The process flow and operating conditions were based on published data (Tanabe and Miyake, 2012). The plant's layout was logically arranged to align the process units with the LNG process flow within a rectangular plot. The network configuration assumed a baseline level of cybersecurity measures, including properly defined and segregated zones and conduits enforced by firewalls (e.g., between business systems, BPCS, and SIS) or Modbus TCP/IP protocols (e.g., between BPCS and SIS). Additionally, advanced operational optimization systems, such as AI-based tools, were assumed to be located outside the plant's network security zone.

The CS-HAZID, CS-HAZOP, and CS-LOPA methodologies were applied to this model plant to identify vulnerable cyberattack scenarios and define the functional requirements necessary for integrating CS risk management into PSM.



Figure 4: A Typical LNG Liquefaction Process Plant Data used in the Case Study

* + 1. Definition of SUC

The guidelines recommend defining SUCs (Systems Under Consideration) based on specific systems; in this case study, SUCs were further subdivided by physical location. This approach was adopted to address vulnerabilities to cyberattacks that may arise during turnaround periods when numerous subcontractors are present onsite, increasing the risk of man-in-the-middle cyberattacks.

Table 1 provides an example of SUC definitions, highlighting their classification by both system and physical location, along with additional remarks to identify specific vulnerabilities, such as increased exposure to cyberattacks during maintenance activities or turnaround events.

Table 1: Example of SUC Definition

|  |  |  |  |
| --- | --- | --- | --- |
| SUC No. | SUC | Physical Location | Remarks |
| 1 | Advanced systems for operation optimization (e.g., AI) | Outside of plant network security zone | Possible to change DCS parameters if attacked by hackers |
| 2.1 | BPCS | PLC (Programmable Logic Controller) and engineering workstation in central control room |  |
| 2.2 |  | PLC in local instrumented building in process unit …. | Vulnerable to man-in-the-middle cyberattacks in turn around |
| 3.1 | SIS | PLC and engineering workstation in central control room |  |
| 3.2 |  | PLC in local instrumented building in process unit …. | Vulnerable to man-in-the-middle cyberattacks in turn around |

* + 1. Cybersecurity HAZID

There is comparatively limited information available on conducting CS-PHA compared to CS-HAZOP and CS-LOPA. This study proposes the use of CS-HAZID, a brainstorming technique analogous to HAZOP, but specifically adapted to cybersecurity. By effectively applying the guidewords outlined in Table 2, CS-HAZID facilitates the systematic identification of worst-case scenarios arising from cyberattacks.

Table 2: CS-HAZID Guidewords used in the Case Study

|  |  |
| --- | --- |
| Heading1 | Guidewords |
| Process hazards | Process releases unignited, Process releases ignited, Process releases, Flaring, Venting, Draining, Sampling |
| Cyber security hazards | Deviation from safe operating envelope, Damage to critical equipment, Safety system/devices disabled, Loss of functionality, Significant LOC (Loss of Containment), Spurious shutdown, Domino events, Fatality, Environmental damage, Economical damage |

* + 1. Cybersecurity HAZOP

As CS-HAZOP is focused on identifying detailed pathways to realize the worst-case scenarios identified in CS-HAZID, the guidewords employed are specifically linked to various cyberattack mechanisms. In this case study, the guidewords presented in Table 3 were utilized, with reference to the guidelines outlined in the guideline(CCPS, 2022).

Table 3: CS-HAZOP Guidewords used in the Case Study 2)

|  |  |
| --- | --- |
| Category | Guidewords |
| Cyberattack mechanism | Social Engineering (e.g., phishing, spear phishing) |
|  | Communications (e.g., denial of service, man‐in‐the‐middle) |
|  | Supply Chain (e.g., compromise of service provider) |
|  | Physical Access (e.g., logging onto on unguarded workstation) |
|  | Software (e.g., exploiting a known software vulnerability) |
|  | Hardware (e.g., connecting a USB to an unsecured port) |

* + 1. Cybersecurity LOPA

The CS-LOPA adopts a similar approach to the traditional PS-LOPA. In this case study, residual risk is evaluated as the Risk Reduction Factor (RRF), as represented in Equation (1) below.

|  |  |
| --- | --- |
|  | (1) |

Incident likelihood is calculated as the product of TL (Threat Likelihood), PFD (Probability of Failure on Demand) for both Process Safety (PS) and Cybersecurity (CS), and VF (Vulnerability Factors) related to ignition and personnel presence. The Risk Reduction Factor (RRF) is then derived by dividing the incident likelihood by the TMEL (Target Mitigated Event Likelihood). If the PFD for CS is not accounted for, the remaining RRF can be allocated as the SL (Security Level). Each user must determine their TMEL based on their specific risk matrix, with parameter references available in international guidelines (CCPS, 2001; CCPS, 2022).

The key distinctions between CS-LOPA and traditional PS-LOPA include the introduction of TL as the frequency of cyberattacks and the incorporation of PFDs for cybersecurity protection layers.

* 1. Results

The CS risk assessment process evaluates the worst-case scenarios, potential cyberattack pathways leading to these scenarios, and the protection layers required to mitigate CS risks. The output images from the case study are presented in Figure 5. The results indicate that safety equipment relying on mechanical devices, such as pressure relief valves and other inherently safer measures, is more effective in reducing cyberattack risks compared to functional safety devices. Conversely, when process safety equipment is safeguarded by computer-based systems such as DCS and SIS, the significance of the IT protection layer—such as IT access monitoring and regular scanning of DCS PLCs—becomes paramount.

Given the increasing reliance on BPCS and SIS in modern plant safety design, functional requirements, including reliability and inspection frequency, must be explicitly defined and managed within operational control systems under PSM. Accordingly, a comprehensive SUC functional register should be established.

The allocated Risk Reduction Factor (RRF) for each Protection Layer (PL) and the associated functional requirements to ensure their effectiveness must be clearly documented in a register. For this case study, a simplified format of the SUC Functional Requirements Register (Table 4) was employed, balancing practicality with the complexities involved in preparing detailed registers.



Figure 5: Output images from CS risk assessment in the Case Study

Table 4: Example of SUC Functional Requirements Register

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SUC | Cyberattack scenarios | Risk allocation | Residual RRF | Functional Requirements |
| 1.Advanced systems for operation optimization (e.g., AI) | Location: Outside of plant security zone  Threat: Phishing by advanced hackers to leak administrator rights to an external PC for driver assistance and model prediction. Entrapment of the ability to rewrite to BPCS from the system.  Consequence: Tampering with the BPCS control value to cause a CS-PHA scenario.  Exceeding the normal operating range of the process, and in the worst-case scenario, exceeding the safe operating range, resulting in leakage, ignition, fire, and possible explosion. | PS-PLs   * PSV: 0.01 * SIS: 0.1 * Access Control: -   CS-PLs   * Unauthorized access prevention measures x Unauthorized tampering prevention measures: ***0.01*** * IT access management and periodic PLC inspections: ***0.2*** | 0.2 | * Management of the PS system independent protection layer shall follow the management requirements in the PSM. * Unauthorized access and tampering prevention measures should be updated regularly (white list). * Monitoring of IT access for unauthorized logins should be performed at all times, and the method of coordination with the PSM shall be clearly defined. * PLC inspections shall be performed at least once a month. |
| … |  |  |  |  |

* 1. Challenges to integrate into PSM

The case study demonstrates that the definition of CS risk management requirements can be effectively achieved using the CS risk assessment process, with certain improvements proposed in this paper. Figure 6 illustrates the integration of CS within PSM.

Beyond the straightforward management of CS-critical elements such as BPCS and SIS, Operations and Maintenance (O&M) PSM elements—such as Permit to Work (PTW)—must also incorporate CS risk management considerations. For example, the physical accessibility of PLC devices introduces the potential for man-in-the-middle attacks, such as virus uploads via USB drives. Therefore, PTW approvals should account for the risk of cyberattacks involving contractors’ personnel.

Additionally, the CS perspective must be extended to other PSM elements, such as the Management of Change (MoC) for networks and associated devices, to ensure the integrity and reliability of IT infrastructure.

Since CS risk management aspects are not typically included in conventional PSM elements, organizational adjustments are necessary on the OT side to enhance CS integration within the PS team. This may involve educating PS team members on CS principles and including CS specialists within the PS team to ensure effective implementation and oversight.



Figure 6: Example of CS Integrated risk-based PSMS

* 1. Conclusions

The case study highlights the potential for integrating CS risk management into PSM, provided that CS functional requirements are clearly defined through CS risk assessment methodologies from a technical perspective. However, the integration of CS and PS management systems presents significant challenges, despite leveraging the same risk-based framework.

For instance, PS engineers are required to address cybersecurity concerns in addition to the extensive technical demands of process safety. While involving CS specialists in PS teams can provide valuable expertise, effective integration necessitates seamless communication and mutual understanding between PS and CS professionals to establish a cohesive management system.

Given the increasing adoption of smart technologies, the role of PS engineers is expanding, necessitating broader expertise. This challenging transition underscores the need for a well-structured education system that incorporates both PS and CS elements. To address this, the SPSM Initiative Group LLC supports process plant organizations in acquiring the necessary knowledge through e-learning platforms that facilitate effective learning in both process safety and cybersecurity.

References

CCPS, 2001, Layer of Protection Analysis, AIChE, USA

CCPS, 2022, Managing Cybersecurity in the Process Industries, Wiley, USA.

ISA, 2017, TR84.00.09 Cybersecurity Related to the Functional Safety Lifecycle, USA.

Tanabe, M., Miyake, A., 2012, Approach enhancing inherent safety application in onshore LNG plant design, Journal of Loss Prevention in the Process Industries, 25, 809-819.1.2011

Yokohama National University (YNU) Strategic PSM Initiative Group (SPSM), 2022, Guidelines for Strategically Implement PSM in Organization <www.anshin.ynu.ac.jp/pdf/SPSM01guide.pdf> accessed 23.09.2024