CHEMICAL ENGINEERING TRANSACTIONS

VOL. 77, 2019

A publication of AIDIC

The Italian Association of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216

DOI: 10.3303/CET1977105

Integration of Automation Lifecycles: Leveraging Functional Safety, Cybersecurity, and Alarm Management Work Processes

Kate M. Hildenbrandt*, Iwan J.W.R.J. van Beurden

exida, 80 N. Main St., Sellersville PA, 18960, USA
khildenbrandt@exida.com

Functional Safety standards have addressed how hazards and their risks are to be analyzed and protected against, as well as how the effectiveness of the protection must be evaluated and maintained. With the use of PLC based systems, the ease of generating alarms has increased significantly and alarm floods are common in most plants. Alarm management standards are addressing concepts of rationalization and prioritization. With advancements in automation the threats of cyber-attacks and cybersecurity incidents has presented itself. Cyber security standards are being written to address these issues both from a manufacturer as well as a user perspective. The most effective method for developing a streamlined work process is the creation of a cohesive lifecycle that addresses all automation requirements. This pulls from the functional safety, cyber security and alarm management lifecycles to create one unified approach to safety and security. This presentation will address a combined lifecycle approach while using common automation examples to enhance the importance of the integration of the respective automation needs.

1. Introduction

Risk management of a manufacturing process requires a deep dive into the Functional Safety, Cybersecurity and Alarm Management lifecycles. Each of these lifecycles is dictated by a different standard, and traditionally carried out by different teams within an organization. With little communication between the groups, it is a challenge to account for all risks and create a comprehensive event response plan during plant operation.
By integrating the three automation lifecycles it is possible to ensure awareness of all potential hazards and required risk reduction, improve efficiency and communication, and achieve a complete plant and enterprise view of risk management in an organization.

2. Overview of Automation Lifecycles

The international functional safety standard IEC 61511 provides the safety lifecycle as a steadfast guideline to assess and mitigate risk for manufacturing processes including refineries, chemical, petrochemical, pulp and paper, and power plants. Over time, the tasks of the functional safety lifecycle have been adopted internationally by the top companies in the process industry, creating a well-defined, streamlined work process meant to address process hazards. Traditionally, this work is carried out by the engineering team and is essential to implement a functionally safe system.
However, to properly manage risk at a facility, and companywide, careful consideration of cyber-attacks is required as well as process hazards. Indeed, the new revision of IEC 61511, initially released in 2016, highlights the need for a Cyber Risk Assessment, emphasizing the responsibility of the owner/operating company to identify the threat, likelihood and consequences of cybersecurity events. They must also determine requirements for additional risk reduction and implement measures to reduce or remove threats.
It is no longer adequate for plant operators, engineers, design and support personnel to only be aware of process hazards and risk. Cyber-attacks not only impact business from a financial perspective but can also initiate process safety incidents. IEC 62443 has presented a Cybersecurity lifecycle. The scope includes

Paper Received: 20 October 2018; Revised: 30 May 2019; Accepted: 9 July 2019

Please cite this article as: Hildenbrandt K., van Beurden I., 2019, Integration of Automation Lifecycles: Leveraging Functional Safety, Cybersecurity, and Alarm Management Work Processes, Chemical Engineering Transactions, 77, 625-630 DOI:10.3303/CET1977105

assessment of a system for inherent risk and subsequent design, implementation and maintenance of countermeasures against cyber threats. Traditionally, this work is carried out by Operation Technology (OT), with help from Information Technology (IT) teams within an organization.

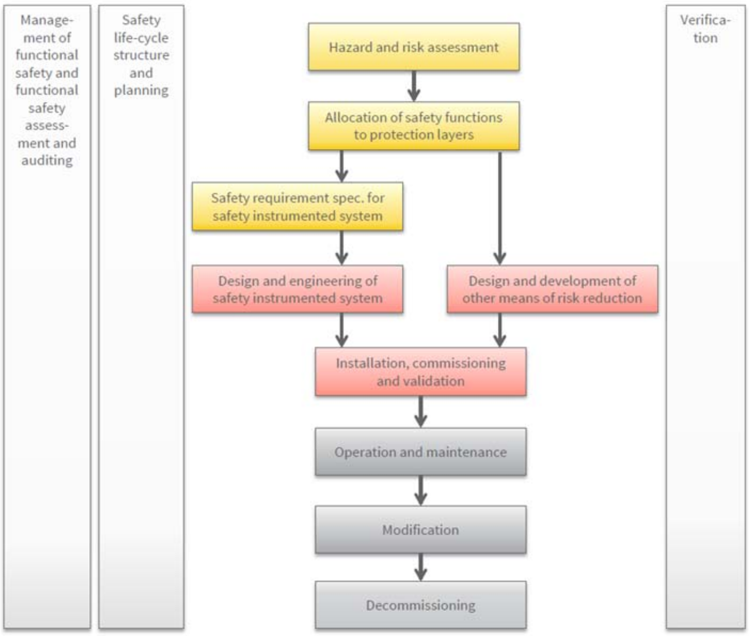

Figure 1: Functional Safety Lifecycle as defined by IEC 61511

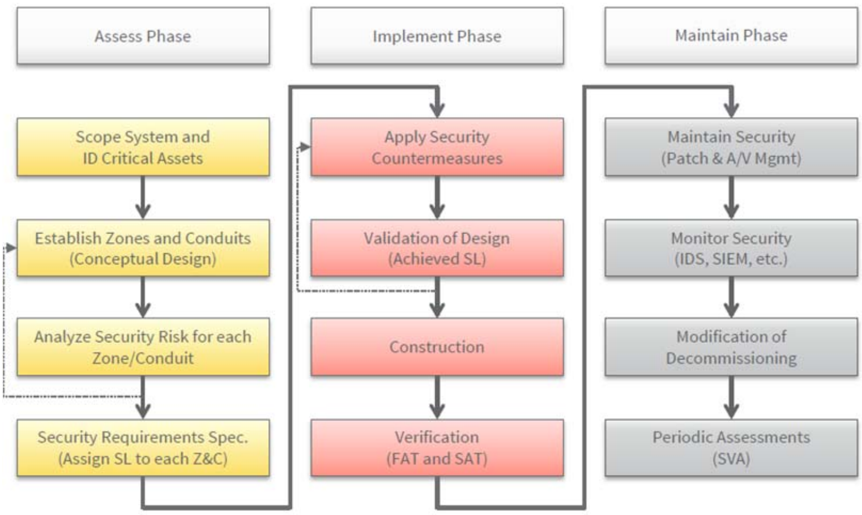

Figure 2: Cybersecurity Lifecycle as defined by IEC 62443

Both safety and cyber lifecycles include implementation of safeguards or countermeasures against a hazard scenario. In many cases, these include alarms. The identification and rationalization of alarms are addressed in the Alarm Management lifecycle as defined by ISA 18.2 and IEC 62682. The full scope of this lifecycle also includes design and implementation of alarms and operation, maintenance, monitoring and management of change of the master alarm database for a system. Traditionally, this is carried out by the Engineering and Operations teams within an organization.

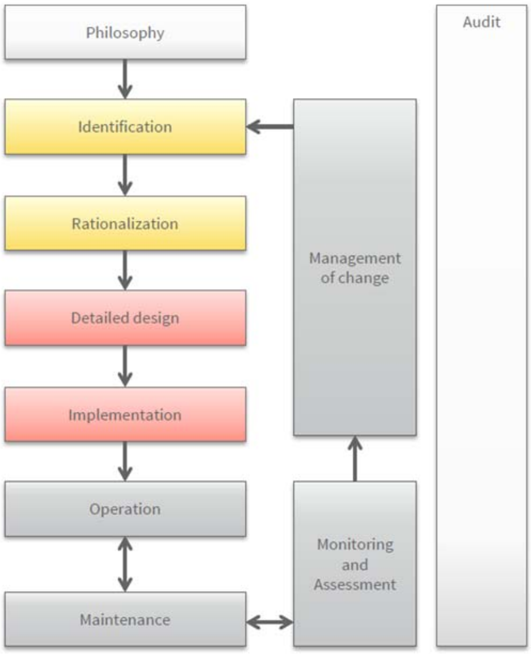

Figure 3: Alarm Management Lifecycle as defined by ISA 18.2

3. Integrated Functional Safety, Cybersecurity, and Alarm Management Lifecycles

Each of these lifecycles has a similar structure which includes analysis or assessment of the system for inherent risk, and subsequent design, implementation, and operation of safeguards or countermeasures against that risk. These similarities provide opportunities to leverage best practices to create one integrated work process the addresses functional safety, cybersecurity, and alarm management. Integrating the lifecycles, and opening the lines of communication between the Engineering, Operations, Operation Technology and Information Technology teams, results in awareness of all potential hazards and required risk reduction as well as a comprehensive event response plan.

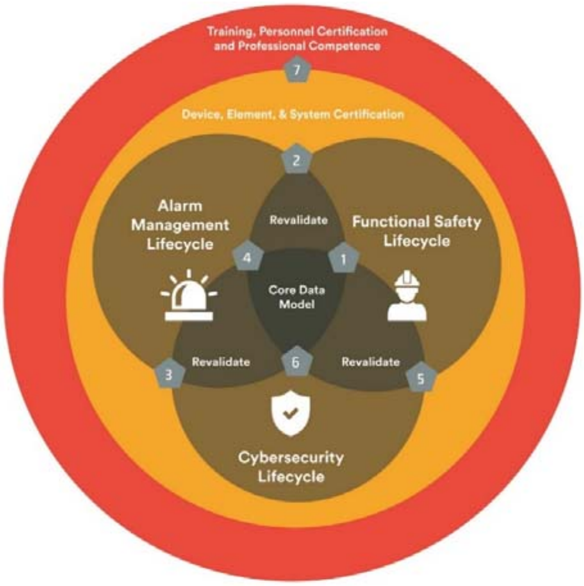

Figure 4: Areas of Overlap Between the Automation Lifecycles

The lifecycles overlap for each of the following tasks:

1. Hazard Identification
2. Process Hazard Data to Alarm Rationalization
3. Cyber Hazard Data to Alarm Rationalization
4. Alarm Rationalization Process
5. Process Hazard Data to Cyber Risk Assessment, SIL and SL Verification Process
6. Event Response Management

In the functional safety lifecycle, Process Hazard Analysis (PHA) is often done using the HAZOP methodology. Here the process is divided into smaller parts called units and nodes. Any challenge to the process is a deviation. The cause and consequence of that deviation are documented, and risk is determined by the frequency of the cause and the severity of the consequence. For high risk scenarios, safeguards are implemented to mitigate that risk. These safeguards may include alarms with operator intervention, pressure relief devices, and safety instrumented functions (SIFs) made up of a sensor, logic solver and final element, which is usually a remote actuated valve.

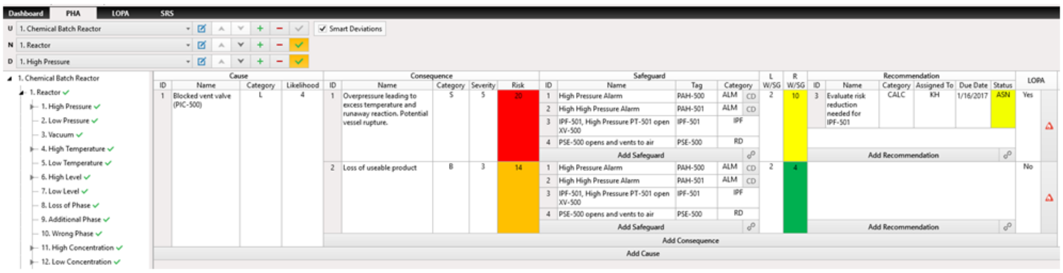

Figure 5: PHA Worksheet from exSILentia® PHAx™

The Cyber Risk Assessment is similar, with the system divided into smaller parts called cyber zones and cyber nodes. Any path that can be used to gain access is called a threat vector. The cause and consequence of the threat must be documented. Risk is determined by the likelihood of the threat and the severity of the consequence. For high risk scenarios, countermeasures can be implemented to mitigate the risk. These countermeasures may include alarms with operator intervention, network devices such as firewalls and switches with access controls, physical security of engineering work stations, among others. Best practices are leveraged here by using the same methodology for assessment and sharing findings and recommendations between the safety and cyber teams.

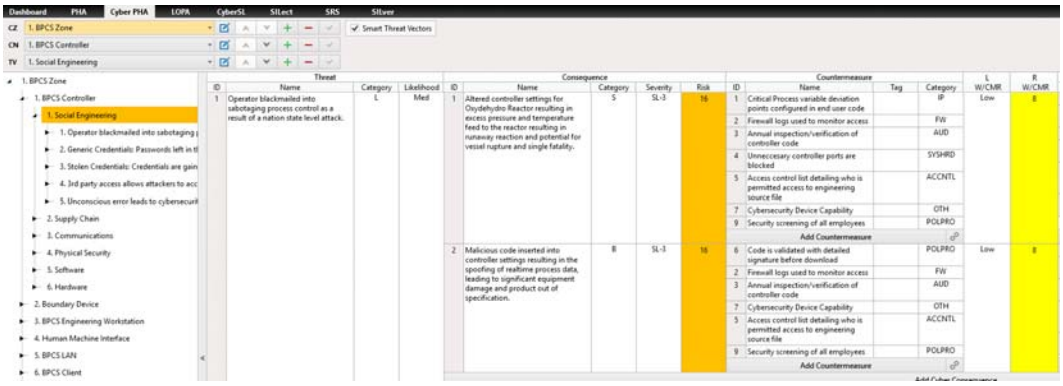

Figure 6: Cyber Risk Assessment Worksheet in exSILentia® CyberPHAx™

Each alarm safeguard or countermeasure accounted for in hazard identification must be included in the alarm rationalization process. The master alarm database design basis includes documentation of the cause, consequence, corrective action and time to respond for each alarm. Much of this information is already documented in the PHA or Cyber Risk Assessment. Cross referencing the alarm rationalization with Safety and Cyber Analysis tasks improves traceability and clearly communications design criteria.

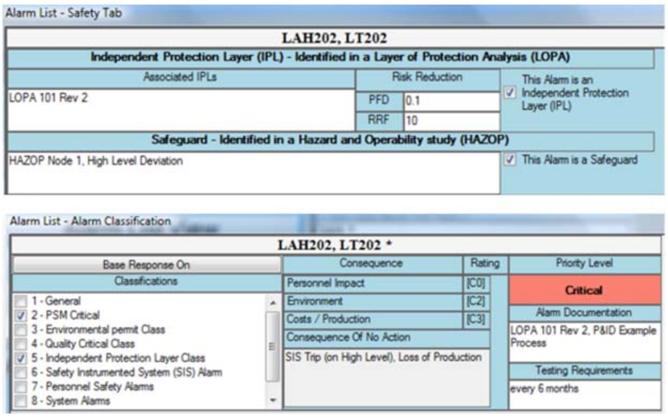

Figure 7: Alarm Classification in exSILentia® SILAlarm™

For safety and cyber, the next step includes using frequency based targeting the determine the design criteria for safeguards and countermeasures, respectively. For safety, a Layer of Protection Analysis (LOPA) is performed. In the LOPA, the frequency of each cause is multiplied by the probability of failure for each independent layer of protection, resulting in an actual frequency of the hazard scenario. This is compared to the tolerable frequency. If they are not equal, the result is the amount of risk reduction needed, and the Safety Integrity Level (SIL) required to design the Safety Instrumented System (SIS). SIL Verification calculations solidify the conceptual design by ensuring the Safety Instrumented Functions (SIFs) meet the target SIL.

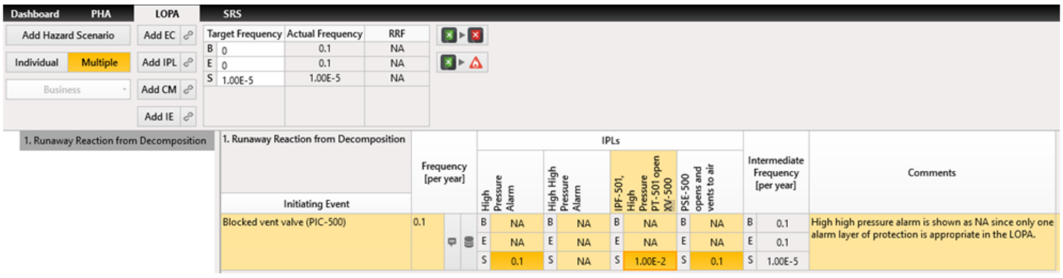

Figure 8: Layer of Protection Analysis Worksheet in exSILentia® LOPAx™

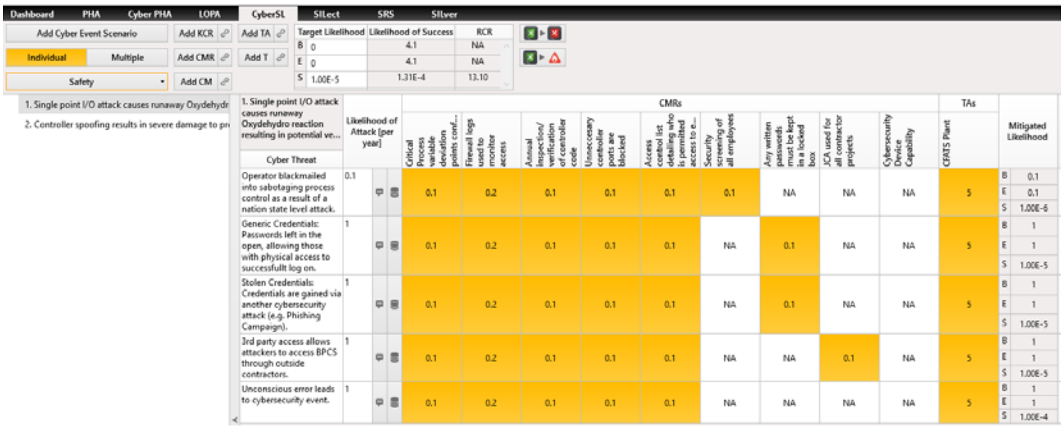

Figure 9: SL Verification Worksheet in exSILentia® CyberSL™

A similar method is used for SL Verification of your cyber countermeasures. In this case, the likelihood of each cyber threat is multiplied by the probability of failure of each countermeasure, resulting in the mitigated likelihood of the cyber event scenario. The intention is to close the gap between the actual likelihood and the target likelihood. This methodology is meant to ensure the countermeasures implemented can provide the

required amount of risk reduction. By utilizing a similar method as the LOPA, this becomes a straightforward, efficient way to verify the countermeasures meet the target security level.
Each lifecycle requires testing of safeguards, countermeasures, and alarms prior to start-up. The Factory Acceptance Test (FAT) involves testing of equipment prior to field installation and includes verification that the application program for SIF logic solvers and alarms, and cyber security countermeasures are implemented correctly. The Site Acceptance Test (SAT) involves testing of equipment after installation in the field and includes verification that all safeguards and countermeasures are implemented correctly, as well as alarm triggers and notification in HMI, and means for successful operator response. It is more efficient to do this testing together, saving engineering hours while assuring all safeguards and countermeasures work.
Operation and maintenance of safeguards, countermeasures, and alarms all include monitoring during operation, routine maintenance and testing, periodic assessment and potential for modification. In all cases to demonstrate compliance with safety standard it is a requirement that data is collected during the life of the plant to validate the conceptual design. Storing all data in one centralized database will streamline evaluation of safeguard and countermeasure health, and validation of the design. Finally, during operation of the plant the operator must have a comprehensive event response plan. Their duty includes keeping the plant online, physical security of the site and engineering station, process hazards (including any demands on the process, proof testing, device failures), and cyber hazards (cyber alarms, active and passive diagnostics). Integration of the lifecycles and communication between groups will give a full picture of the operator’s responsibilities ensuring they are manageable. Since operator response is key to alarm layers of protection, this is of utmost importance.

4. Conclusions

With an integrated automation lifecycle each area of overlap represents an opportunity to leverage best practices from established work processes to improve efficiency and drive communication between different teams. This method guarantees awareness of all potential hazards and required risk reduction, increases project velocity, and reduces project cost and schedule. Operational benefits include increased availability, reduced operation and maintenance cost and a comprehensive event response plan.

References

ANSI/ISA-18.2-2016, 2016, Management of Alarm Systems for the Process Industries, International Society of Automation, Research Triangle Park, NC, USA.

Hildenbrandt K.M., van Beurden I.J.W.R.J., 2017, Integration of Automation Lifecycles; How Functional Safety, Cybersecurity, and Alarm Management Work Together, presented at ISA Process Control and Safety Symposium, November 8, 2017, Houston, TX, USA.

IEC 61511 (2.1 edition), 2017, Functional Safety: Safety Instrumented Systems for the process industry sector, International Electrotechnical Commission, Geneva, Switzerland.

IEC 62443, 2018, Security for industrial automation and control systems, International Electrotechnical Commission, Geneva, Switzerland.