USE CASE

Background

Challenge: Increased process industry safety risks due to digitization and electrification exposes even the most secure systems to cyber threats.

Approach: Prioritize hazard and resilience assessments and audits. Learn and implement proper safety and cybersecurity standards.

Results:

1. Identification of plant safety gaps
2. Adaptation of new digital operations to a hybrid safety approach (combining cybersecurity and functional safety)
3. Monitoring of safety on an ongoing basis in an automated fashion
4. Greater peace of mind and lower threat of harmful cyber attacks

UL Solutions

Process plants: Why functional safety and cybersecurity are emerging as resilience-critical success factors

Adhering to standards and identifying hazards are important first steps in protection

Most global manufacturers now embrace digitization and electrification to streamline operations, reduce carbon emissions and increase production output while maintaining product quality. New connected, digitized products and services are radically shortening business turnaround cycles. In many cases, new productivity and efficiency levels that were not affordable or technically feasible in the past are now both possible and cost less.

A typical example would be a company that creates specialty materials of incredibly high purity in high-temperature environments. Workers operate electrified furnaces that run at several thousand degrees. Workers' safety and equipment integrity emerge as top management priorities in such plants.

Whether the task is creating silicon carbide wafers for semiconductor applications or synthetic sapphire and diamond for industrial applications, thousands of people work across the company's 10,000+-square-foot factory floor running critical equipment such as digitally controlled lasers, compressed air-driven devices, and thousands of distributed valves, pumps and motors.

As companies add tools and devices meant to transform operations and improve functional safety, they face the increased risk of cyber threats targeting the very tools that help deliver employee and workplace safety. For example, companies can transform their operations by adding networks of sensors, consolidating data from those sensors and analyzing that data to execute operational decisions more rapidly. When these technological transformations occur, the issue of human and asset safety takes on a new dimension. In many cases, adding safety functions related to information acquisition, monitoring and processing, and automated machine stoppage becomes mandatory to comply with published safety standards.

Challenges

However, implementing advanced safety measures to protect digitized plant operations can be complex, especially when the company's core competency lies in manufacturing goods and not in implementing safety science. Beyond functional safety, which has long been addressed in industry standards and practice, cybersecurity-related safety concerns now emerge. The Industrial Internet of Things (IIoT) and the overall increase of connected devices contribute to enlarging the potential attack surface for external hackers and internal bad actors.

The growing number of physical and digital interfaces, including interconnected devices controlled by intelligent dashboards, introduces a new set of cybersecurity vulnerabilities, risks and liability issues. Therefore, safety assessments and safety function deployments must take on a more integrated approach to demonstrate that plant assets are well protected.

If hackers have established a presence within an operations technology (OT) endpoint, they can take over the systems responsible for control operations. At that point, the hacker could issue commands that turn off and on systems — in essence, crippling plant operations.

According to a SecurityScorecard report released in early 2023 at the World Economic Forum, almost half of all critical manufacturing across the globe faces a significant risk of a data breach[1]. The report also asserts that "48% of critical manufacturing providers in key sectors, as designated by the U.S. government, were rated C or below for cyber resilience, making them more vulnerable to malicious activity."

These cybersecurity risks can also lead to problems with safety regulations, which can lead to lost production, penalties, negative corporate image and legal damages resulting from physical injury.

> Almost half of all critical manufacturing across the globe faces a significant risk of a data breach.
>
> **SecurityScorecard**

UL Solutions

UL Solutions

Approach

Organizations like UL Solutions can help process industries understand how to plan and deploy advanced security services to protect plant operations. Several approaches can help to reduce process industry cybersecurity and safety risks, including:

- **Resilience reviews –** Industrial organizations must better protect their IIoT-driven expanded cyberattack surface. Reviewing the resilience of power and industrial control systems is a logical place to start. However, even IIoT devices that do not perform control functions but furnish data from which control decisions are made should be accounted for. Stakeholders must monitor what is happening to make sure that configurations are not being altered.
- **Hazard analysis –** Process hazard analysis (PHA) exercises play an essential role in manufacturing system design approaches across industrial plants. PHA identifies potential hazards and implements changes to reduce hazard risks. New cyber PHA approaches can now be incorporated to address exposures and gaps in areas where information technology (IT) and OT systems converge. Both methods can be combined to bolster the overall design process with periodic health checks whenever new systems are integrated into the process operation.
- **Implementation of the proper standards –** Several industrial standards play critical roles in helping to improve process industry safety and cybersecurity. IEC 61508, for example, provides guidance surrounding the design, deployment and maintenance of safety and automatic protection systems. IEC 61511 is another international standard that defines the requirements for safety instrumented systems in the process industry. This standard addresses the concerns of process system specification, design, installation, operation and maintenance. It is most applicable for designers, integrators and process system users.

How UL Solutions can help

By highlighting common safety scenarios and the use cases, UL Solutions helps process industry technical design leaders understand and adopt more secure approaches for deploying plant digitized power and automation upgrades.

To learn more about how functional safety is applied in the process industry, read our **Benefits of Functional Safety Certification in Hazardous Locations (HazLoc)** article.

On the cybersecurity side, ISA/IEC 62443 has emerged and helps to incorporate and govern cyber PHA. This standard provides guidance for securing industrial control systems (ICS) and OT networks by adapting traditional functional safety guidelines to cybersecurity and cyber safety. ISA/IEC 62443 certification demonstrates an organization's compliance to established cybersecurity requirements to better protect the organization from device hijacking, data siphoning, device theft, device spoofing and data breach threats.

Within this standard, ISA/IEC 62443-3-2 outlines procedures for conducting a control system and cybersecurity assessments, while ISA/IEC 62443-2-4 addresses the integration and maintenance of industrial automation and control systems (IACS).

For more information on how to address OT security, visit our industrial cybersecurity page that explores **ISA/IEC 62443 services.**

Conclusion

Safety is a top priority across process industries, due to humans' proximity to powerful machines, high-intensity furnaces and environments often involving flammable and toxic materials. The industry adopts a layered safety approach that relies on plant designs that carefully integrate technologies, people and processes to comply with safety regulations. In such environments, functional safety and cyber protection mechanisms act as the automation control systems' last lines of defense.

As a global leader in applied safety science, UL Solutions helps companies understand how to demonstrate safety, enhance sustainability, strengthen security, improve quality, manage risk and achieve regulatory compliance through standards implementations. Visit us at **UL.com/functionalsafety** to learn more about our process industry safety certification, verification and testing services. To learn more about our wide range of cybersecurity services visit us at **UL.com/cybersecurity.**

LEARN MORE

End note:

[1] Cybersecurity Dive. Dive brief: Almost half of critical manufacturing organizations face significant risk of data breach. Jan. 23, 2023. **https://www.cybersecuritydive.com/news/critical-manufacturing-cyber-risk/640951/**