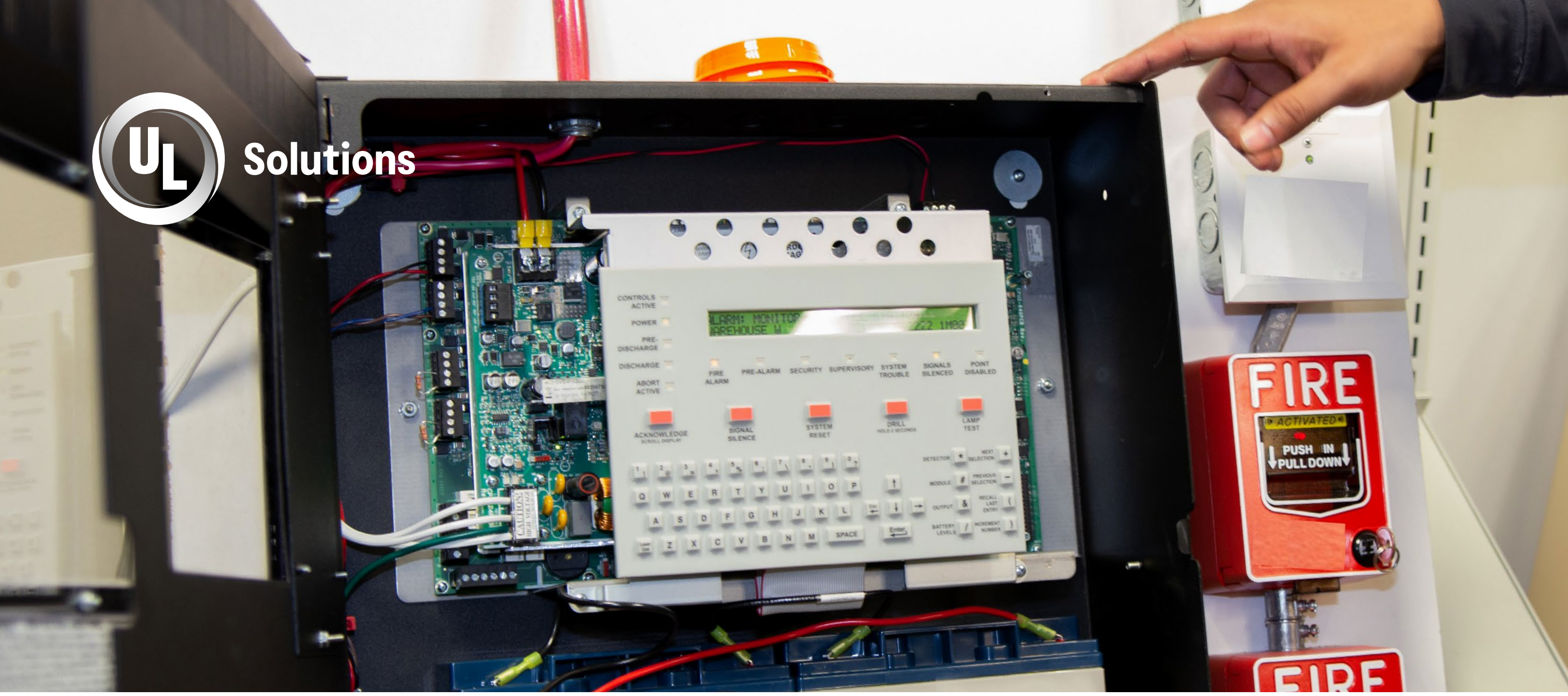


Cybersecurity for Security and Life Safety Signaling Systems

In today's interconnected world, the importance of cybersecurity cannot be overstated, especially for manufacturers of security and life safety signaling systems. These systems play a critical role in safeguarding people's lives and protecting valuable assets. However, as technology advances and these systems become more sophisticated, they also become vulnerable to cyber threats.

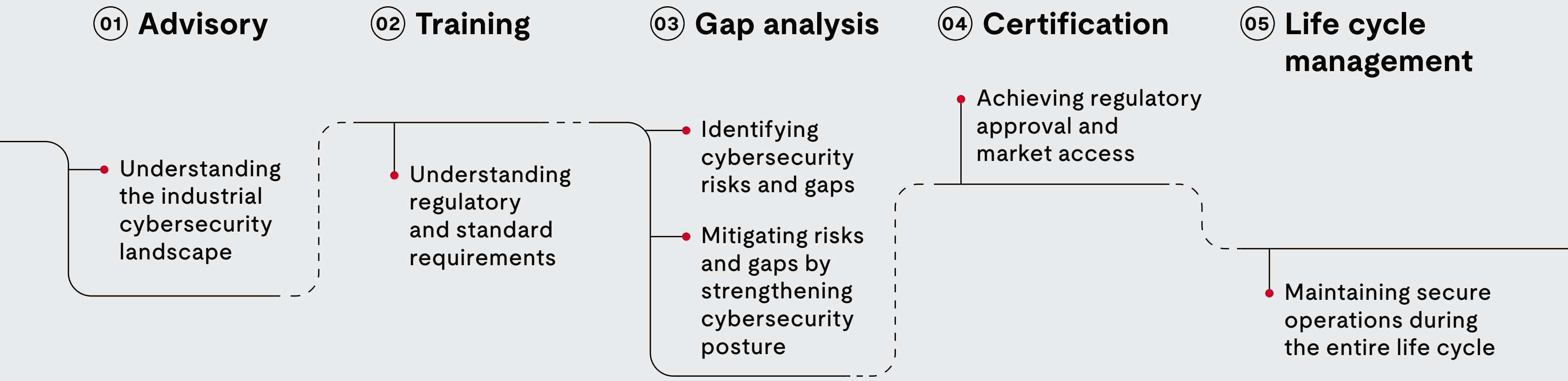
Manufacturers have a responsibility to demonstrate the integrity and reliability of their products. By implementing robust cybersecurity measures, they can minimize the risk of unauthorized access, data breaches, and system disruptions. These measures include implementing strong authentication protocols, encryption techniques, and regular software updates to address any identified vulnerabilities.

The consequences of a cybersecurity breach in this industry can be severe. A compromised security or life safety signaling system can result in devastating consequences, such as unauthorized access to secure areas, false alarms, or even malfunctions and disruptions in communication to or from the central station that compromise the safety of individuals. Therefore, manufacturers must prioritize cybersecurity to protect not only their reputation and business interests but also the lives and well-being of those who rely on these systems for their safety and security.

Code authorities, national codes, manufacturers and end users are becoming increasingly aware of the importance of cybersecurity protection for Internet of Things (IoT) connected security and life safety equipment and systems. Like consumer products, professional-grade security and signaling products and systems are susceptible to cyber threats that can have a significant impact on their ability to protect, signal and function as intended. UL Solutions offers several services that can help mitigate cybersecurity threats through assessment and testing.

Collaborate with UL Solutions

Your cybersecurity journey along the product development life cycle



01 Advisory

- Understanding the industrial cybersecurity landscape

02 Training

- Understanding regulatory and standard requirements

03 Gap analysis

- Identifying cybersecurity risks and gaps
- Mitigating risks and gaps by strengthening cybersecurity posture

04 Certification

- Achieving regulatory approval and market access

05 Life cycle management

- Maintaining secure operations during the entire life cycle

UL Standard for life safety and signaling systems

To help improve the security of critically connected electronic physical security systems, UL 2900-2-3, the Standard for Software Cybersecurity for Network-Connectable Products: Particular Requirements for Security and Life Safety Signaling Systems, developed with industry input, provides a foundational set of cybersecurity performance and evaluation requirements that manufacturers of network connectable products can use to establish a baseline of cyber protection against known vulnerabilities, weaknesses and malware.

UL Solutions can test and evaluate a product's software for the presence of malware, vulnerabilities and weaknesses, and certify the product's software architecture and design to the specifications enumerated in the Standard.

Electronic physical security infrastructures and life safety signaling systems include emergency communications systems, fire alarm systems, burglar alarm and intrusion detection systems, alarm receiving systems, automated teller machine systems, access control systems, surveillance cameras, DVRs, NVRs and the like.

For UL 2900-2-3, a three-tiered security approach was developed, with an increasing level of security for each tier. Tests include malformed input testing, known vulnerability detection, code and binary analysis, risk control analysis, structured penetration testing and security risk controls assessment.

Level 1 (L1) includes foundational cybersecurity testing requirements for security risk assessment of software in products covered in this standard. Provides assessment of general security capabilities of a product with limited knowledge of the internal security controls of the product. L1 does not require the submission of source code. This level is closest to "black box" testing. L1 is recommended as a minimum level of assessment.

Level 2 (L2) includes L1 assessment and testing requirements and additional requirements for security risks assessment of software in products. Source code is tested at this level. Provides assessment of security capabilities of a product with knowledge of internal security controls of the product. Because specific protections for sensitive data are included at L2, this is the lowest level recommended for products sending, receiving or processing sensitive data.

Level 3 (L3) includes L1 and L2 assessment and testing requirements and additional requirements of the vendor process and management. Provides assessment of security capabilities of a product with knowledge of internal security controls of the product and knowledge of the business practices of the vendor to support the lifecycle of the product.

In today's connected world, the variety of devices available offers numerous points of entry for cyberattacks. UL 2900-2-3 certification is recognized by the life safety and signaling industry as a valuable demonstration of a product's cybersecurity posture.[1]

[1] NFPA (n.d.). *NFPA 72 National Fire Alarm and Signaling Code*. www.nfpa.org/. Retrieved December 19, 2023, from https://www.nfpa.org/codes-and-standards/7/2/nfpa-72

ISA/IEC 62443 family of standards

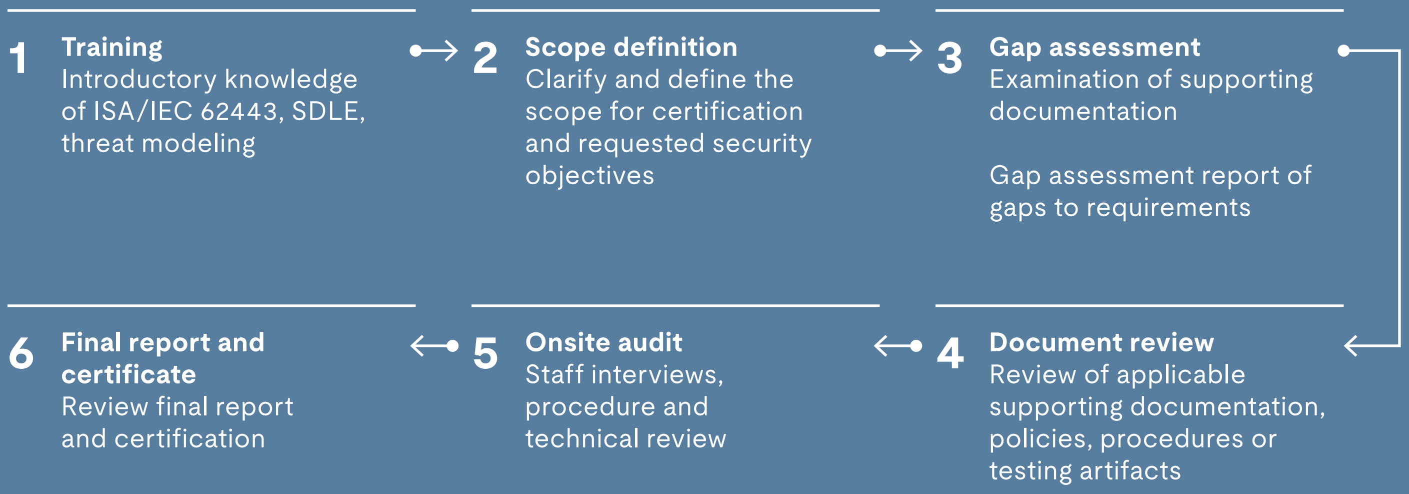
Digital technologies have successfully penetrated the manufacturing sector and continue to do so at an ever-increasing rate. This merging of the cyber and physical worlds means improved efficiency, but also results in an increased exposure of your critical manufacturing infrastructure to cyber risk.

ISA/IEC 62443 activities are part of a strategy based on an all-comprehensive engagement in the development of the ISA/IEC 62443 standards framework, related services, and conformity assessments.

We have a suite of cybersecurity testing and certification services for ISA/IEC 62443 designed to fit your needs. The ISA/IEC 62443 family of standards has cybersecurity requirements for industrial automation control systems that a manufacturer or system integrator needs to instill cybersecurity rigor into their processes. Certification to these standards is an easy way to demonstrate to customers that your organization has done the due diligence of building cybersecurity into your processes and practices with a trusted third party. Our portfolio of cybersecurity services for ISA/IEC 62443 incorporates cybersecurity testing, including relevant tests required for a strong secure development lifecycle (SDLC) process, certification to the published requirements of ISA/IEC 62443, risk assessment, documentation review and training.

UL Solutions offers certification services to the following four ISA/IEC 62443 standards:

- ISA/IEC 62443-2-4 – Installation and maintenance requirements for suppliers
- ISA/IEC 62443-3-3 – System security requirements and security levels
- ISA/IEC 62443-4-1 – Product development requirements
- ISA/IEC 62443-4-2 – Technical security requirements for components



1 **Training**
Introductory knowledge of ISA/IEC 62443, SDLE, threat modeling

2 **Scope definition**
Clarify and define the scope for certification and requested security objectives

3 **Gap assessment**
Examination of supporting documentation

Gap assessment report of gaps to requirements

4 **Document review**
Review of applicable supporting documentation, policies, procedures or testing artifacts

5 **Onsite audit**
Staff interviews, procedure and technical review

6 **Final report and certificate**
Review final report and certification

NISTIR 8259 series of reports

The NISTIR 8259 series of reports offers manufacturers and their third-party partners guidance for incorporating cybersecurity capabilities, which may be included in a holistic system approach based on risk and use case.[2]

NISTIR 8259 series is made up of three documents: NISTIR 8259, NISTIR 8259A, and NISTIR 8259B. NISTIR 8259 outlines a series of steps that IoT manufacturers should adhere to during the development and maintenance of IoT devices:

Pre-market activities:

- Identify expected customers and users and define expected use cases.
- Research customer cybersecurity needs and goals.
- Determine how to address customer needs and goals.
- Plan for adequate support of customer needs and goals.

Post-market activities:

- Define approaches for communicating to customers.
- Decide what to communicate to customers and how to communicate it.

NISTIRs 8259A and 8259B expand upon the guidelines provided in NISTIR 8259 by introducing distinct technical functionalities (Table 1) and non-technical supporting actions (Table 2) that manufacturers should consider incorporating into their product designs and support strategies. These additions may be crucial for effectively meeting the cybersecurity requirements and objectives of IoT customers.

- NISTIR 8259 serves as the fundamental guidance for expected requirements of the new U.S. Cyber Trust Mark framework described in NISTIR 8425.
- The IoT Cybersecurity Improvement Act requires government agencies to only acquire and utilize IoT devices that include cybersecurity capabilities mandated by each agency head.

UL Solutions provides assessment, advisory and gap analysis services based on NISTIR 8259.

NISTIR 8259A (May 2020)
Technical Baseline

- Device Identification
- Logical Access to Interfaces
- Device Configuration
- Software Update
- Data Protection
- Cybersecurity State Awareness

NISTIR 8259B (Aug 2021)
Non-Technical Baseline

- Documentation
- Educate and Awareness
- Information and Query Reception
- Information Dissemination

Source: https://www.nist.gov/itl/applied-cybersecurity/nistcybersecurity-iot-program/nistir-8259-series

[2] NIST (2021, November 9). NISTIR 8259 Series. https://nist.gov/. Retrieved December 19, 2023, from https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series

Why UL Solutions for cybersecurity?

- Independent, trusted third party
- Full life cycle solutions
- Hardware- and software-based security evaluations
- Assessment of security development practices
- Cybersecurity expertise
- Industry knowledge
- Cybersecurity and safety
- Global teams and local support

Cybersecurity foundation

- Expertise in global standards and frameworks
- Extensive knowledge of best practices
- Growing list of Internet of Things (IoT) security solutions

Learn more and speak to one of our experts today at **UL.com/cybersecurity**.