

# USNC CURRENT

Vol. 19, No. 1 - Winter 2024

## CYBERSECURITY



United States  
National Committee  
of the IEC

Published by the U.S. National  
Committee of the IEC, a  
committee of the American  
National Standards Institute



## CYBERSECURITY

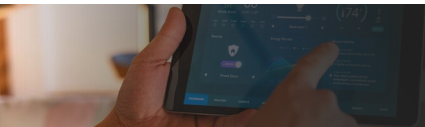
### FEATURED STORIES

3



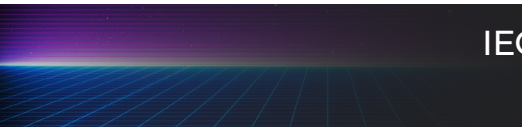
THE SCOPE AND SUCCESS OF IEC  
62443 SECURITY STANDARDS

7



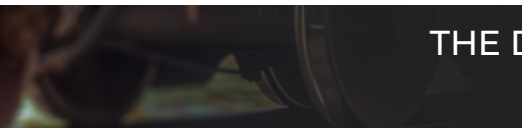
THE HOME ELECTRONIC SYSTEM (HES)  
FAMILY OF STANDARDS

13



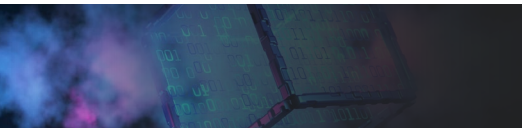
IEC HORIZONTAL STATUS WIDENS IMPACT OF  
INDUSTRIAL CYBERSECURITY STANDARDS

15



THE DUALISM BETWEEN SAFETY AND SECURITY  
IN RAIL AND TRANSIT SYSTEMS

20



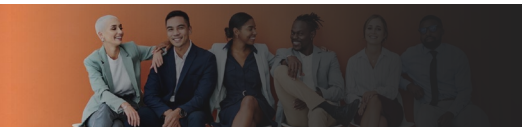
PRIVACY BY DESIGN STANDARDS

23



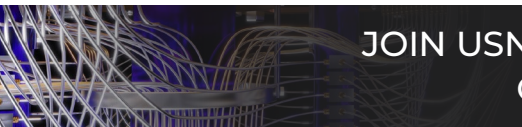
FOOD AND DRUG OMNIBUS REFORM ACT OF 2022  
(FDORA) AND MEDICAL DEVICE CYBERSECURITY

26



REFLECTIONS ON THE IEC YOUNG  
PROFESSIONALS PROGRAMME

29



JOIN USNC TAG FOR NEW IEC/ISO JOINT TECHNICAL  
COMMITTEE ON QUANTUM TECHNOLOGIES

### IN THIS ISSUE

14 Decision Depot

28 Just Published

31 Don Heirman Award Program

22 USNC/IEC Training and Education

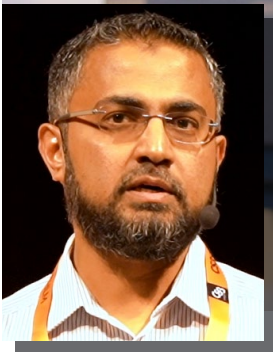
30 Call for Standards Action and Participation





## THE SCOPE AND SUCCESS OF IEC 62443 SECURITY STANDARDS

*Khalid Ansari – Principal Engineer for Cybersecurity at FM Approvals  
ISA Certified Automation Professional; ISA Certified 62443 Expert; Member of IEC/ISA JT-62443-4-1,  
JT-62443-3-2, and ISA99 WG4-TG2 (62443-4-2) sub-committees*



The IEC 62443 series of standards for security of industrial automation and control systems plays an important role in managing the cybersecurity risk of entities that make up nations' critical infrastructure. This article discusses the scope of IEC 62443 standards and their applicability to the various stakeholders, with an emphasis on product manufacturers. Overviews of IEC 62443-based product certification and secure product development lifecycle will be covered. Growing acceptance of IEC 62443 by other standards and codes developers, and its potential inclusion in international regulations, will also be presented.

### INTRODUCTION

The invention of the Programmable Logic Controllers (PLC) in the late 1960s transformed assembly lines and manufacturing plants by replacing hardwired relays with control logic that could be programmed. PLCs, and later Distributed Control Systems (DCS), were designed to operate on the production floor and in process plants, with reliability and safety as their key goals. It is not uncommon to hear a PLC running for

several years without interruption or requiring downtime. These systems operated in isolation and kept chugging along. However, with the push for further optimization, the convergence between information technology (IT) and operational technology (OT), and digital transformation, capabilities to facilitate network connectivity and remote access to these industrial automation and control systems (IACS) were added. Consumer-grade operating systems and commercial-off-the-shelf (COTS) network equipment proliferated the IACS ecosystem, which is now termed OT to distinguish it from the traditional IT. Cybersecurity was not a consideration for IACS and OT as it was not a threat—until everything changed with Stuxnet in 2010. Stuxnet was a highly sophisticated malware that targeted a specific make and model of PLC and clandestinely changed the logic running in the PLCs to gradually manipulate the rotor speed and eventually destroy hundreds of centrifuges at the Natanz nuclear enrichment facility in Iran.

There has been an increasing number of attacks on IACS and OT ever since. Many of the disruptions are



collateral damage of attacks on the IT or enterprise side of a business, like the ransomware attack on Colonial Pipeline in the U.S. Other attackers are opportunistic and go after exploits of COTS components found in the OT environment, such as Windows-based human-machine interfaces (HMI) and software applications. The most dangerous, though, are those that specifically target IACS systems and components to exploit their inherent weaknesses. As odd as it may sound, seemingly unflawed and fully operational features and functions are abused by adversaries due to the insecure-by-design nature of most IACS protocols and components.

## IEC 62443 STANDARDS

To address this lack of cybersecurity in IACS systems, industry has come together and created security standards, foremost of which is the IEC 62443 series of standards. The IEC, together with the International Society of Automation (ISA), develops and maintains these standards jointly. These standards are commonly referred to as “ISA/IEC 62443”; however, we will use “IEC 62443” here. This set of standards and technical reports addresses overall security of IACS systems, including policies and procedures, security programs, risk management, zones-and-conduits based architecture, and security levels, among many other important topics.

The audience and stakeholders of the IEC 62443 standards include asset owners, systems integrators, maintenance, and service providers, as well as product suppliers. Asset owners are organizations that own and operate IACS in a variety of industries, such as oil and gas, power generation, chemical manufacturing, and transportation. They have the ultimate responsibility for ensuring the cybersecurity of their systems and are accountable for any security breaches that occur. Asset owners often outsource the design, implementation, and maintenance of their systems to systems integrators.

Systems integrators are organizations that design, implement, and maintain industrial control systems on behalf of asset owners. They must ensure that the systems they deliver meet the cybersecurity requirements defined by the asset owners. In the context of the IEC 62443 standards, systems integrators must ensure that the systems they deploy and configure are compliant with the security requirements defined by the standards.

Product vendors develop and sell the hardware and software components used in IACS. They must ensure that their products comply with security controls addressed in parts 3-3 (System security requirements and security levels), 4-2 (Technical security requirements for IACS components), and 4-1 (Product development requirements) of the standards.

All of these stakeholders must work together to ensure the cybersecurity of IACS. Specifying certified products with certain security level capabilities immensely simplifies the procurement process. It also aids in subsequent risk assessments of the facility.

## PRODUCT CERTIFICATION

ISASecure® is a third-party conformity assessment scheme based on the IEC 62443 series of standards. A third-party conformity assessment scheme is also known as a certification scheme, and provides guidelines on conformance testing and verification of requirements specified in the standards. In addition to the rigorous testing of the IACS system as per part 3-3, and component per part 4-2, the certification schemes mandate a thorough assessment and audits of product manufacturers' processes, promoting the security development lifecycle best practices, based on part 4-1.

The security development lifecycle certification ensures product manufacturers consistently practice security-by-design methodology, have processes for incident response and communication of security incidents, and provide security guidelines to the end users. Adherence to these requirements enables manufacturers to meet



their obligation to mitigate any new vulnerabilities and support the security of their product throughout its lifecycle.

A critical piece to the effectiveness of the IEC 62443 series of standards is the certification of equipment. As a highly specialized and internationally recognized ISASecure® Certification Body, FM Approvals is one of the CBs that tests and certifies the conformance of industrial control systems, connected systems, and related components to the IEC 62443 standards.

The FM Approvals Cybersecurity Laboratory is operated by cybersecurity experts with hosted servers and specially designed test stations configured to efficiently evaluate multiple products simultaneously for compliance with IEC 62443. Products tested and certified by FM Approvals for cybersecurity have designed-in security, have passed vulnerability identification testing, and are robust against cybersecurity attacks at the designated security level.

## SUCCESS AND ADOPTION OF IEC 62443 STANDARDS

The adoption and success of the IEC 62443 standards has been steadily increasing over the years. A primary reason for the success of the IEC 62443 standards is the collaboration between industry stakeholders, including asset owners, system integrators, and product vendors. The standards were developed by a global team of cybersecurity experts from industry, academia, and government, ensuring that they are relevant, practical, and effective. The IEC 62443 standards have been designated as horizontal standards because they are applicable to IACS in multiple industries and sectors. This horizontality allows for a consistent and standardized approach to cybersecurity, regardless of the industry or sector.

Following are some of the adoptions and successes of the IEC 62443 standards:

American Petroleum Institute's standard, API-1164, *Pipeline Control Systems Cybersecurity*, utilizes many

fundamental concepts from the IEC 62443 standards, such as the risk-based approach, zones, and conduits, etc., and has informative references to them.

The National Fire Alarm and Signaling Code, NFPA 72, published by the National Fire Protection Association, in its current edition (2022) recommends in Annex J, that “systems should be designed, installed, and maintained in accordance” with the IEC 62443 standards, among others.<sup>1</sup>

The American Society of Mechanical Engineers' code, ASME A17.1-2022, *Safety Code for Elevators and Escalators*, explicitly requires the manufacturers to “have a listed/certified secure product development life cycle process conforming to the relevant requirements of IEC 62443-4-1” and conformance to other “relevant parts of the IEC standards.”<sup>2</sup>

Due to its popularity, requirements from IEC 62443 standards have also been mapped to other cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework<sup>3</sup> and the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals.<sup>4</sup>

Common Weakness Enumeration (CWE) is a list of common software and hardware weakness types that have security ramifications. These are referenced in security advisories, including those that are maintained in the National Vulnerabilities Database. Recently, a mapping of IEC 62443 requirements was done for the most commonly encountered CWEs. With this in

1 NFPA 72 - National Fire Alarm and Signaling Code® 2022 Edition; Annex J - Guidelines for Cybersecurity: <https://www.nfpa.org/codes-and-standards/7/2/72>

2 ASME A17.1-2022/CSA B44:22; Section 8.14 - Cybersecurity: <https://www.asme.org/codes-standards/find-codes-standards/a17-1-csa-b44-handbook-safety-code-elevators-escalators>

3 NIST CSF-62443 Mapping: <https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=101#/>

4 CISA CPG-62443 Mapping: <https://www.cisa.gov/resources-tools/resources/complete-cpgs-matrixspreadsheet>






place, one could drill down an IACS advisory and look up the IEC 62443 requirement that would mitigate the vulnerability, and may have potentially prevented the vulnerability from manifesting itself in the first place.

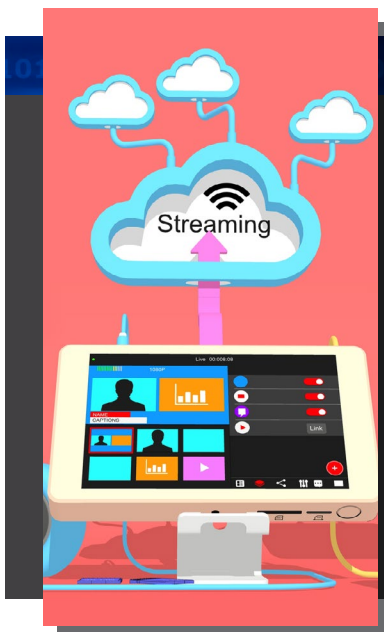
While many countries and regions are working hard to combat all forms of cybercrime, the European Union (EU) has been at the forefront of these efforts. In the past few years, the EU has developed and enacted multiple measures to help secure personal data and harden various industries against cyberattacks. In September 2022, the European Commission published a draft of the Cyber Resilience Act (CRA), which proposes to create conditions for the development of secure products by: ensuring that hardware and software products are placed on the market with fewer vulnerabilities; ensuring that manufacturers take security seriously throughout a product's life cycle; and creating conditions that allow users to take cybersecurity into account when selecting and using products with digital elements.

Although it is unclear at this point as to what standards the CRA may adopt for conformance testing of IACS, industry experts have posited IEC 62443 to be a good candidate.<sup>5</sup>

Malaysia, Qatar, Brazil, India, and Singapore have also adopted IEC 62443 standards to varying degrees for the protection of their critical infrastructure.<sup>6</sup>

In closing, the IEC 62443 standards have been very successful in their adoption across sectors and geographical regions. Several IEC-ISA joint committees are actively working to keep these standards updated and relevant in the face of changing threats. Consider volunteering your time by joining a committee and participating in the protection of critical infrastructure. 

- 5 What cybersecurity standards will products in the EU soon have to meet?: <https://fluchsfriktion.medium.com/what-cybersecurity-standards-will-products-in-the-eu-soon-have-to-meet-590854ba3c8c>
- 6 ISAGCA - Adoption Status of Laws, Regulations, and Standards: <https://isagca.org/advocacy-adoption>



## ANSI MEMBERSHIP WEBINARS

Membership in ANSI is the key to unlocking the benefits and opportunities that standardization can provide. Standardization and conformity assessment activities lead to lower costs by reducing redundancy, minimizing errors, and reducing time to market, resulting in enhanced profitability.

These interactive 30-minute webinars—held on the first Friday of each month and free of charge—are hosted live and provide an overview of ANSI's activities, as well as information on how to take full advantage of ANSI membership. A Q&A session encourages active dialogue between all participants.

For more details, visit our [website!](#)

## THE HOME ELECTRONIC SYSTEM (HES) FAMILY OF STANDARDS

*Dr. Kenneth Wacks – Deputy Technical Advisor; ISO/IEC JTC1/SC25/WG1 TAG Convener, ISO/IEC JTC1/SC25/WG1*



The international standards working group ISO/IEC JTC 1/SC 25/WG 1, responsible for the Home Electronic System (HES), develops IoT-related (Internet of Things) standards for communication networks and interfaces. These standards enable the interconnection of electrical and electronic equipment and products for homes and small buildings. The primary markets for WG 1 standards are creators, manufacturers, and installers of these products and related services.

The HES comprises a family of standards that enable home and building occupants to:

- » live more comfortably at home,
- » be more protected and feel safe at home,
- » work productively in smart buildings, and
- » live and work more economically with minimal environmental impact by reducing energy consumption and/or producing and storing or selling excess energy.

Applications of products and services based on HES standards include entertainment, lighting, comfort

control, life safety, health, and energy management. Energy management has become important with the evolution of distributed energy resources (DER: solar panels, wind turbines, and storage batteries) for installation at homes and buildings, possibly interconnected with smart grids to access public power. Energy efficiency, reliability, resiliency, and reduction of greenhouse gases to mitigate climate change are topics of global interest. SC 25/WG 1 develops standards supporting energy management for appliances and electric vehicle chargers within homes and small buildings.

### THE HES GATEWAY

A communications interface between a wide area network (WAN), such the Internet, and a local area network (LAN), used in homes and buildings, is called a gateway. A LAN in a house is often called a HAN: Home Area Network. This term is used in the ISO/IEC 15045 HES gateway series and in this article. The ISO/IEC 15045 series of international standards specifying the HES gateway extends the conventional



communications gateway with some unique features. All the HES gateway standards were proposed and managed by the U.S.

## HES GATEWAY FEATURES

The HES gateway links a WAN outside the home or building with a HAN to provide traditional gateway communication services, plus much more. The HES gateway provides these additional services:

- » Support for multiple HANs
- » Support for cybersecurity protection
- » Support for applications
- » Support for interconnected gateways
- » Support for interoperability among competing products

As home automation evolved from a hobby to an industry, there were attempts nationally and internationally to create standards for a uniform

communications infrastructure to interconnect devices such as sensors, actuators, controllers, and user interfaces. These standards were completed and were technically sound; however, they were not adopted. Instead the market fragmented into specialized networks, such as KNX, LonTalk, Wi-Fi, Zigbee, Z-Wave, etc. With this reality, HES focuses on enabling interoperability among disparate HANs and devices using these HANs.

## THE HES GATEWAY STRUCTURE

Figure 1 shows the functional components of a generic HES gateway.<sup>1</sup> The various interface cards are specialized for each WAN and HAN to translate messages

<sup>1</sup> ISO/IEC 15045-1, *Information Technology – Home Electronic System (HES) Gateway – Part 1 A Residential gateway model for HES*  
 ISO/IEC 15045-2, *Information Technology – Home Electronic System (HES) Gateway – Part 2: Modularity and protocol*  
 ISO/IEC 15045 Parts 1 and 2 are published; the other parts cited are in development.

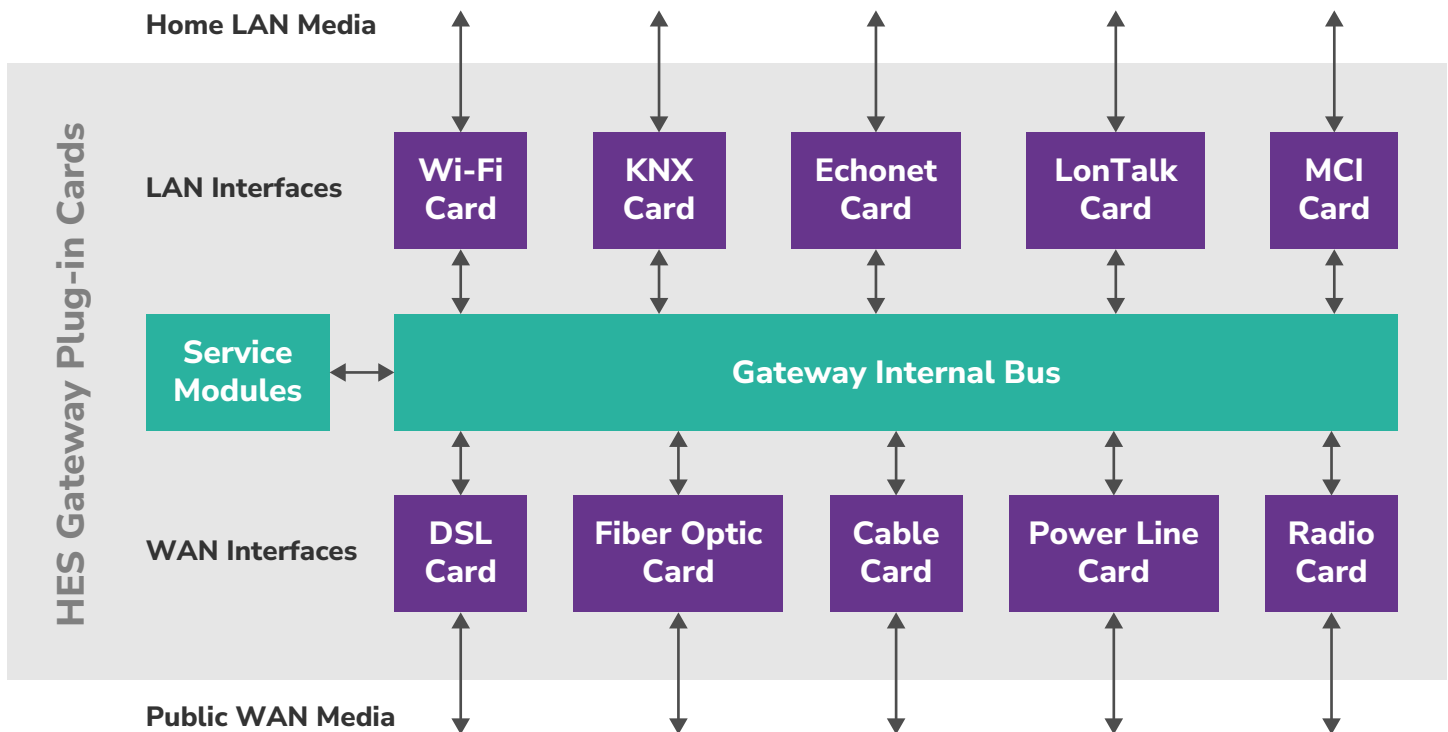


Figure 1: HES Gateway structure





using an HES gateway feature called the Interworking Function. The core functionality of the HES gateway is embodied in service modules. A service module contains instructions for processing service data to implement protocol translation, cybersecurity protections, applications, and any other responsibilities assigned to the HES gateway.

Standards are developed to provide specifications for models, architectures, interfaces, and communication protocols while offering flexibility for manufacturers to create significant product differences. Manufacturers can differentiate their HES gateway offerings from competitors by choosing, for example:

- » Which HES gateway functions to include from among the options in the standards
- » Whether to package the HES gateway with other consumer electronics
- » The user interface for the consumer or installer to configure the HES gateway

These standards encourage a diverse market for HES gateway products. ISO/IEC 15045-4-1<sup>2</sup> and subsequent parts<sup>3</sup> specify classes of HES gateway configurations that range in capabilities and complexity.

The primary function of the gateway is a communications interface. Some commercial home automation systems are being developed around a platform

---

2 ISO/IEC 15045-4-1, *Information Technology – Home Electronic System (HES) Gateway – Part 4-1: HES gateway structural class and module requirements*

3 ISO/IEC 15045-4-2, *Information Technology – Home Electronic System (HES) Gateway – Part 4-2: Simple HES gateway*  
ISO/IEC 15045-4-3, *Information Technology – Home Electronic System (HES) Gateway – Part 4-3: Complex integral HES gateway*

ISO/IEC 15045-4-4, *Information Technology – Home Electronic System (HES) Gateway – Part 4-4: Complex modular HES gateway*

ISO/IEC 15045-4-5, *Information Technology – Home Electronic System (HES) Gateway – Part 4-5: Interconnected HES gateways*

that acts as a communications hub and a host for controlling applications. The HES gateway includes the option for embedding Service Modules that support applications, so the HES gateway can be configured as a platform both for communications and for applications. Applications such as energy management could be hosted by the HES gateway, as specified in ISO/IEC 15045-5-1<sup>4</sup> and ISO/IEC 15045-5-2.<sup>5</sup>

## HES GATEWAY CYBERSECURITY

The ISO/IEC 15045-3 series specifies features for an HES gateway to provide cybersecurity services for homes and buildings. These services are intended to protect user data, privacy, and safety. Data protection is a growing challenge as devices are designed with access to Internet services. Such access makes these devices targets for data theft, reprogramming to create mayhem, and launching platforms for malware bots (Internet robots) that attack other devices.

## THE HES DEVICE REGISTRY

With the proliferation of non-wired networks such as radio, infrared (typically used in remote control units), and power-line carrier, it is easy to insert rogue devices into a home network. Therefore, the HES gateway can include a registry of legitimate devices. The gateway validates cybersecurity certificates presented by attached devices to determine if the device belongs on this network. A certificate is a digital message to verify that a device was provided by a known company and operates according to agreed rules. It is analogous to a driver's license issued by the government attesting that the holder has demonstrated driving competency.

After the device certificate is validated, the gateway can then establish a secure link with the device and an

---

4 ISO/IEC 15045-5-1, *Information Technology – Home Electronic System (HES) – HES gateway, Application services, Part 5-1: Overview, foundation, and requirements*

5 ISO/IEC 15045-5-2, *Information Technology – Home Electronic System (HES) – HES gateway, Application services, Part 5-2: Energy management and measuring application (EMMA)*



application controller by distributing encryption keys. Since the device certificate registry is maintained in the HES gateway, a loss of external communications would not impact cybersecurity, as would a cloud-based security service.

## HES MESSAGE SERVER SCREENING

The HES gateway has the option of examining message headers to determine if local devices are communicating with the intended cloud-based servers. To accomplish this, the HES gateway maintains a list of servers with which each local application could be communicating for accessing remote services. Users would be warned of attempts to reach unauthorized servers.

## HES PRIVACY AND SAFETY PROTECTION

The HES gateway supports an optional feature that screens data traffic for compliance with policies intended to protect consumer privacy. Also, appliance control messages impacting safety might be screened and blocked by the same mechanism.

Figure 2 illustrates the elements in the gateway for protection of Premises and Personally Identifiable Information (PPII, explained in the next section) and safety. The “CS, PP11 & Safety Controller” block in Figure 2 contains the rules about which data flows are allowed and which are blocked. The “CS, PP11 & Safety Processor” block enforces these rules by filtering the data to allow or block transmission.

For example, using a smart phone app when away from home to start a burner on a cooktop could be dangerous unless someone is at home to check that the appropriate pot with food is in place and nothing flammable is nearby. The HES gateway safety service modules could be programmed to screen remote control commands sent to such appliances. The functions of screening and filtering data extend the mission of the gateway to provide “data sentry” services for cybersecurity protections of customer data, privacy, and safety.

Privacy policies have focused on protecting PII such as name, address, government-issued identification

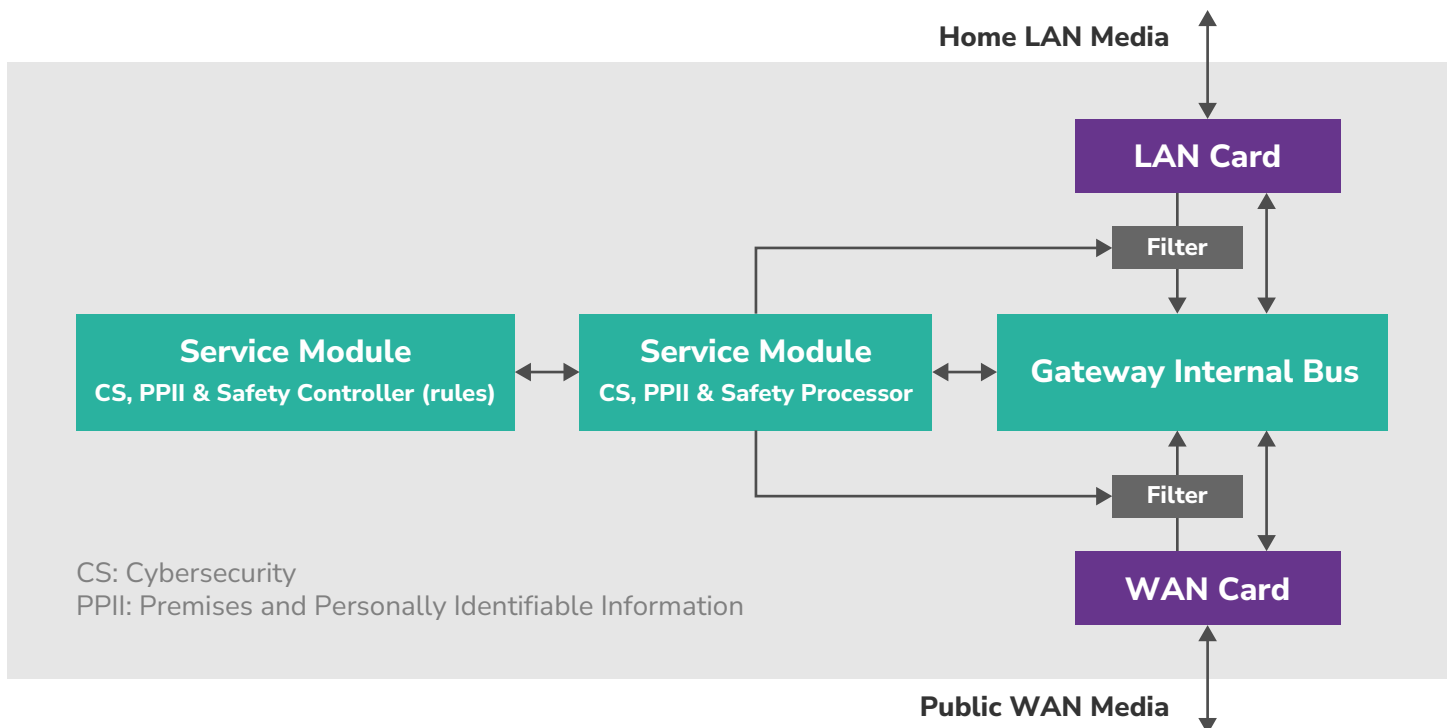


Figure 2: Gateway Service Modules



numbers, facial photos, etc. ISO/IEC 29100<sup>6</sup> specifies a privacy framework for enterprise-level information technology (IT). This framework defines common privacy terminology, the elements that control and process PII, considerations for safeguarding privacy, and references to privacy principles that apply to IT. The scope of ISO/IEC 29100 states that these PII standards apply “to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.”

The HES gateway ISO/IEC 15045-3<sup>7</sup> series extends the enterprise privacy framework from persons to devices by introducing the term PPII to incorporate devices and persons. The data sentry screening functions are intended to:

- » Prevent active inbound attacks and unsafe commands.
- » Discover and classify outbound traffic.
- » Mediate network traffic within homes and buildings.
- » Manage mechanisms for privacy and security.
- » Develop a dashboard for reporting gateway activities and status to a non-technical end user.

## HES GATEWAY DATA SCREENING

For the gateway technology to enforce privacy and safety provisions, all messages to and from devices must be checked by the gateway for compliance with

6 ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

7 ISO/IEC 15045-3-1, *Information Technology – Home Electronic System (HES) gateway – Part 3-1: Introduction to privacy, security, and safety*

ISO/IEC 15045-3-2, *Information Technology – Home Electronic System (HES) gateway – Part 3-2: Privacy framework*

the provisions of the privacy contract. The gateway scans and filters messages in real-time as the messages pass through the gateway.

For data not needed in real time, the gateway might function as a repository where these data are buffered. For example, a thermostat could register with the gateway and be allocated storage of a specified number of readings. The remote user with appropriate permission to access this repository would then retrieve these temperature readings from the gateway.

A gateway hardened against unintended data flows is effective if the gateway is the sole data pipe into the home. However, mobile (cellular) operators are planning communication protocols to transport IoT (Internet of Things) data. As mobile data transmission becomes cheaper, it is possible that manufacturers might install mobile phone data transceivers inside appliances and IoT devices to report on usage and performance without informing the customer. For HES compliance, messages to be sent via such a mobile interface are pre-screened by the HES gateway to enable customer cybersecurity protection.

## CYBERSECURITY PROTECTION MANDATES AND PREFERENCES

The HES gateway cybersecurity services can provide protection for customer’s data, privacy, and safety. This is important for energy data and applications since energy consumption patterns can reveal who is home, when they are home, and what they are doing.

We may be at a confluence of social, political, and technical events that make standards and technology specifications for privacy timely. Consumers are becoming aware that personal data can be misused. In May 2018, the European Union (EU) General Data Protection Regulation (GDPR) became law. It protects the personal data, such as names, addresses, photos, and voice recordings, of all EU residents, regardless of where the data are processed. Explicit consent is required before processing personal data for one or more specific purposes.





Market studies have shown that privacy concerns are impacting the sale of connected home products. Parks Associates, a market research firm that tracks home systems, surveys 10,000 broadband households periodically for "Smart Home Device Inhibitors." Privacy concerns have consistently ranked third after device costs and benefits for 2020 through 2022. More than 30% of those surveyed agreed, "I have data privacy and security concerns about having smart devices in my home." [These survey results were provided courtesy of Parks Associates by president and chief marketing officer Elizabeth Parks in 2023.]

Privacy is no longer just an abstract concept, but can be enabled with appropriate policies, technology, and products. Consumers need products with technology that can protect privacy. The HES gateway ISO/IEC 15045-3 series specifies technology that allows consumers and service providers to choose and enforce privacy options. It is now up to designers and manufacturers to incorporate privacy technology into products and service providers to offer privacy choices with opt-in provisions. Building in privacy protection during product design is less costly for manufacturers than fixing problems later and compensating customers for cybersecurity breaches. 





## IEC HORIZONTAL STATUS WIDENS IMPACT OF INDUSTRIAL CYBERSECURITY STANDARDS

Charley Robinson – FSES, Director, ISA Standards

Member of USNC TMC; USNC TAG Member of IEC TC 65, SC 65A, SC 65E, and SyC Smart Manufacturing



The IEC defines horizontal standards as those that are widely applicable and are to be used by all relevant committees to ensure consistency and coherence in IEC standards development. The status is granted following an enhanced review process and approval by the IEC Standardization Management Board.

The ISA/IEC 62443 standards, *Industrial Automation and Control Systems Security*, were designated as a horizontal series in late 2021, establishing primacy across the wide range of IEC standards projects on matters related to cybersecurity in industrial, critical infrastructure, and related applications.

The ISA/IEC 62443 standards are developed primarily by the ISA99 committee of the International Society of Automation, with simultaneous review and approval by the IEC—along with approval by ANSI as American National Standards. ISA99 draws on the input of cybersecurity experts across the globe in developing consensus standards that are applicable to all industry sectors and critical infrastructure, providing a flexible

and comprehensive framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS).

IEC horizontal status is among several notable recognitions in the ongoing development and global application of the ISA/IEC 62443 series. These include:

- » A decision by the United Nations Economic Commission for Europe to integrate the standards into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe.
- » An agreement at the request of the NATO Energy Security Center for Excellence to establish official collaboration and exchange of information.

IEC horizontal designation reflects the comprehensive application range of standards in the series, which include:

- » ISA/IEC 62443-3-2, *Security Risk Assessment for System Design*, defines engineering measures to guide organizations through the essential process






of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels. The standard can be applied across all industry segments and critical infrastructure sectors.

- » ISA/IEC 62443-4-1, *Secure Product Development Lifecycle Requirements*, specifies process requirements for the secure development of products used in an IACS and defines a secure development lifecycle for developing and maintaining secure products.
- » ISA/IEC 62443-4-2, *Technical Security Requirements for IACS Components*, provides the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications.
- » ISA/IEC 62443-2-1, *Establishing an Industrial Automation and Control Systems Security Program*, describes the elements in a cybersecurity management system for use in the IACS environment and provides guidance on how to meet the requirements for each element.

A newly established ISA/IEC working group will extend the work by identifying, defining, and describing the competencies required of a specialized IACS cybersecurity workforce across primary (organizational) roles and professional (personnel) roles during all IACS security lifecycle phases. The work will focus on specifying the competencies and training necessary for a workforce to reliably and safely design, develop, operate, maintain, and decommission IACS security technology and security management programs as defined in the ISA/IEC 62443 series.

Additional standards in the ISA/IEC 62443 series cover terminology, concepts, and models; patch management; and system security requirements and security levels. All may be accessed at [www.isa.org/findstandards](http://www.isa.org/findstandards), where information on related training resources may also be found.

For more information on ISA99 and the ISA/IEC 62443 series of standards, contact Charley Robinson, ISA Standards, [crobinson@isa.org](mailto:crobinson@isa.org). 



## DECISION DEPOT

This column provides easy access to recent decisions that have been made regarding IEC and USNC policies and procedures that directly affect our members. Click the link below to access the recent decisions.

See the Decision List below for decisions made at the following meeting: IEC Board meeting held in Switzerland on 2024-02-20/21.

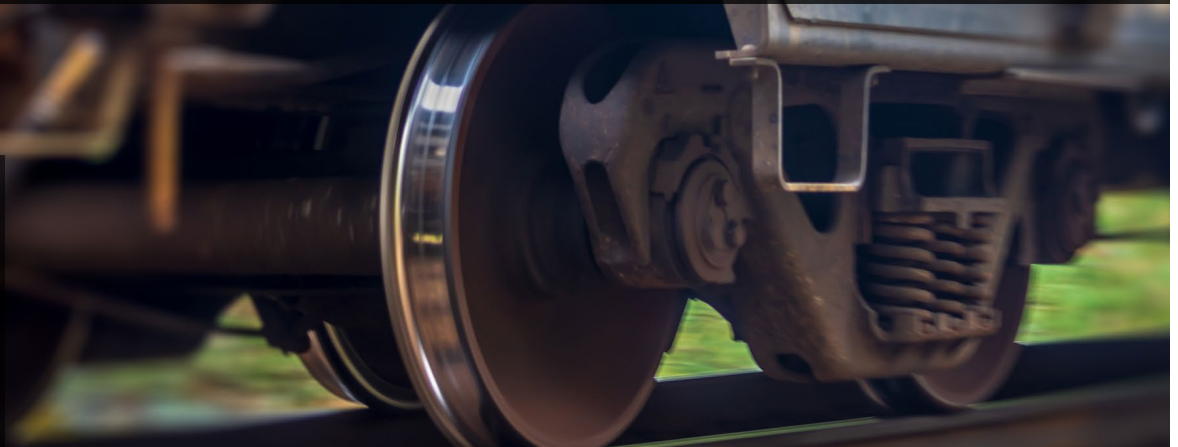
### IEC BOARD





## THE DUALISM BETWEEN SAFETY AND SECURITY IN RAIL AND TRANSIT SYSTEMS

Dr. Hadi Meshgi – Transit Comms/Systems Engineering Lead at VHB; USNC TAG Member of IEC TC 9



Rail and transit systems are deemed as safety-critical, given their failure can lead to human fatalities or catastrophic incidents. The design for such systems primarily prioritizes safety, which necessitates each subsystem to attain a set minimum Safety Integrity Level (SIL).<sup>1,2</sup> Also, all systems in charge of vital functions require safety certification. However, the safety standards employed for railway infrastructure do not consider cybersecurity and simply suggest that a cybersecurity approach should be designed for use with the standard.<sup>3</sup> For instance, IEC 61508—which is a general standard for the safety of electronic and electric devices—doesn't handle security concerns.

1 CENELEC EN 50126, *Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, European Committee for Electrotechnical Standardization, 2018.

2 IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, International Electrotechnical Commission, Apr. 2010

3 K. Hansen, "Security attack analysis of safety systems," in *Emerging Technologies & Factory Automation (ETFA)*, pp. 1–4, IEEE, 2009.

Another Railway safety standard is CENELEC EN 50159,<sup>4</sup> which provides requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system. It addresses topics like message authenticity and integrity, but doesn't cater to broader cybersecurity issues, such as preventing overloading transmission systems or ensuring the confidentiality of safety-related information. Both standards only suggest the need to factor in deliberate malicious human actions and propose the ISA/IEC 62443<sup>5</sup> standard, which provides four degrees of safety hazards and four security levels.

4 CENELEC EN 50129, "EN 50129, *Railway applications - Communication, signalling and processing systems - Safety-related electronic systems for signalling*, European Committee for Electrotechnical Standardization, Nov. 2018.

5 ISA/IEC 62443, *Security for Industrial Automation and Control Systems* series of standards, International Society of Automation & International Electrotechnical Commission, Jul. 2009.



## CHALLENGES OF INCLUDING CYBERSECURITY IN RAIL AND TRANSIT-CRITICAL SYSTEMS

The overlooking of cybersecurity in safety-related standards signifies a grave concern in the rail and transit industry. Presently, railway systems heavily depend on industrial control systems (ICS) to keep them moving. The key components of these ICSs include programmable logic controllers (PLCs), data communication systems (DCSs), and supervisory control and data acquisition (SCADA). Communication between these components is facilitated through a transport network operated by a central operation control center (OCC), where numerous operational tasks are consolidated. The cybersecurity aspects of Industrial Control Systems (ICS) can be examined within the scope of Operational Technology (OT) cybersecurity, which refers to the strategies and measures taken to protect the systems that monitor or manipulate physical devices, events, or processes.

The absence of a standard design approach that includes cybersecurity considerations is leading to the development of critical railway systems that may not comply with necessary regulations. Currently, the implementation of security in railway systems usually adopts one of the following approaches:

- » General norms or security guideline, such as APTA SS-CC-03-15, *Securing Control and Communications Systems in Rail Transit Environments*.<sup>6</sup>
- » IEC Standard 62443<sup>5</sup>, which is the global standard for network security of industrial control systems (ICSs).

The primary challenge associated with these approaches is that these standards are not developed with that specific railway system in mind, resulting in conflicts or gaps. Another problem is that solutions derived from generic standards are not flexible, meaning that it proves challenging to employ the same solution in different modules.

In addition to issues regarding security standards, another problem in the railway context is that safety always supersedes security. Railways are considered as safety-critical systems, emphasizing safety in their very definition. Often, professionals responsible for designing railway safety modules are not aware of potential security risks. Consequently, if any security measures are integrated, they are likely added post-development of the system or module. On the other side, most of security experts overlook safety considerations

6 J. Thompson, T. Ellis, J. Moore, et al. (2010). *Securing control and communications systems in rail transit environments*. American Public Transportation Association, Washington, D.C. [Online]. Available: <https://www.apta.com/resources/standards/Documents/APTA%20SS-CCS-RP-004-16.pdf>



## LOOKING FOR STANDARDS?

ANSI's online store provides access to over half a million active and historic standards from more than 130 publishers. Choose from individual standards, bundles, or custom subscription services.

[WEBSTORE.ANSI.ORG](https://www.ansi.org/webstore)



as well. This mutual lack of comprehension between safety and security professionals creates complications in security implementation.

Moreover, even if a manufacturer considers security during the development of a safety module, there are still technical challenges. Firstly, the hardware or software performing critical functions requires safety certification. If security modules are added, achieving this certification is much more difficult, as these modules are not designed in line with safety standards. Secondly, even in scenarios where safety certification is attained with included security systems, the problem is not entirely resolved. Cyber threats evolve daily, calling for regular updates to security modules to guarantee protection. However, any modifications made to a safety-certified system necessitate its re-certification. As a result, it is almost impossible to re-certify the system each time a security module is updated.

## COMMON NORMS AND STANDARDS FOR OT CYBERSECURITY

As has been stressed so far, the concept of safety in the railway industry is more prevalent than security and it is not unexpected that some organizations might be unaware of security issues and the significance of enhancements in this domain. The bottom line is that, considering the inherent risks linked to the extensive usage of communications in critical systems, it's crucial to include cybersecurity considerations to mitigate potential risks. In this section we provide several cybersecurity-related best practices and norms that are commonly used in rail and transit industry:

- » APTA guidelines in “Securing Control and Communications Systems in Rail Transit Environments” (Parts I–IIIb).<sup>6</sup>
- » The *Common Criteria for Information Technology Security Evaluation* (CC), or ISO/IEC 15408.<sup>7</sup> This

standard presents security specifications, the method of implementing them, and the evaluation processes customized for the intended environment.

- » the ISO/IEC 27001<sup>8</sup> standard that outlines the necessary requirements for the development, implementation, and maintaining of information security management systems.
- » the Cybersecurity Framework (CSF)<sup>9</sup>, a set of standards, guidelines, and best practices related to managing cybersecurity risks. It also facilitates effective communication of cybersecurity expectations and awareness within and between organizations through a unified language.
- » the NIST Special Publications Series 800, specifically NIST SP 800-53<sup>10</sup>, which incorporates the NIST CSF security controls, and NIST SP 800-82<sup>11</sup>, which addresses ICS security controls.

---

*and general model*, International Organization for Standardization & International Electrotechnical Commission, Dec. 2009.

- 8 ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*, International Organization for Standardization, Oct. 2013.
- 9 M. Barrett, “Framework for improving critical infrastructure cybersecurity,” NIST Cybersecurity Framework, National Institute of Standards and Technology, Apr. 2018. ver. 1.1.
- 10 NIST Joint Task Force, “Security and privacy controls for information systems and organizations,” NIST Special Publication 800-53, National Institute of Standards and Technology, Sep. 2020. Rev. 5.
- 11 K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to industrial control systems (ICS) security,” NIST Special Publication 800-82, National Institute of Standards and Technology, May 2015. Rev. 2.

---

<sup>7</sup> ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction*





» The Open Source Security Testing Methodology Manual (OSSTMM),<sup>12</sup> which has been universally accepted as the standard guideline for performing vulnerability assessments. It incorporates an auditing methodology designed to fulfill both regulatory and industry requirements.

The mentioned standards and guidelines, however, are fairly general and are not specifically designed for rail and transit systems. Additionally, they primarily serve as recommendations for implementing security measures. It can be an initial stage, but is insufficient as each manufacturer can choose to either adhere to or disregard these suggestions.

## COEXISTENCE OF CYBERSECURITY AND SAFETY IN TRANSIT AND RAIL SYSTEMS

This section provides several technical recommendations and reviews the ongoing work in the railway industry to improve the coexistence of safety and security.

### TECHNICAL SHORT-TERM SOLUTION

The optimal resolution to the problems of safety and security would be to establish a common standard addressing both domains and ensure its adherence by all manufacturers. However, this appears to take time. Thus, it becomes crucial to discover an interim remedy utilizing existing norms. To illustrate how safety and security can coexist, here is an example of a Network Intrusion Detection System (NIDS) in a safety tool.<sup>13</sup>

The NIDS must be regularly updated because it identifies intrusions based on network patterns, and these patterns can change at any moment. Therefore, the security module must bypass the safety certification

process. This can be achieved by physically separating the NIDS security module from the safety modules, thereby the device cannot execute any safety-critical tasks.

To access the communication network for intrusion detection without affecting the safety certification, the system employs the black channel principle, which allows the transmission of safe and non-safe process data over the same network or bus line.<sup>14</sup> According to EN 50129, adding a layer with built-in safety mechanisms to the communication protocol allows safety-certified and non-certified devices to share the same network.

These types of technical solutions and recommendations toward the integration of safety and security should be considered case by case and cannot be generalized. A more comprehensive effort for standardization of cybersecurity in rail and transit is being developed in different technical committees and will be discussed in the next section.

### CYBERSECURITY STANDARDS FOR RAILWAY

In recent years, governments, security, and manufacturer companies have been working together to develop a common cybersecurity framework for railways around the world. Several projects have also tried to address rail sector cybersecurity challenges under the Shift2Rail<sup>15</sup> initiative, a European public-private joint undertaking for rail research.

Among those projects, CENELEC TS 50701, *Railway Applications - Cybersecurity*<sup>16</sup> is one of the first attempts

12 P. Herzog, "The open-source security testing methodology manual," tech. rep., Institute for Security and Open Methodologies (ISECOM), Dec. 2010.

13 L. J. Valdivia, I. Adin, S. Arrizabalaga, J. Añorga, and J. Mendizabal, "Cybersecurity – the forgotten issue in railways: security can be woven into safety designs," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 48–55, 2018.

14 A. Elia, L. Ferrarini and C. Veber, "Analysis of Ethernet-based safe automation networks according to IEC 61508," in Proc. IEEE Conf. Emerging Technologies and Factory Automation, 2006. doi: 10.1109/ETFA.2006.355419

15 E. Masson and C. Gransart, "Cyber security for railways – a huge challenge – Shift2Rail perspective," in International workshop on communication technologies for vehicles (Nets4Cars / Nets4Trains / Nets4Aircraft), pp. 97–104, Springer, 2017.

16 CENELEC CLC/TS 50701:2021, *Railway applications – Cybersecurity*, European Committee for Electrotechnical



at addressing the integration issue between safety and security. This technical specification is built on ISA/IEC 62443, and it offers a solution for the railway industry encompassing rolling stock, signaling, and infrastructure. The idea is to apply a system engineering approach to include cybersecurity into the development life cycle of a product or system. This includes the phases of design, implementation, verification and validation, and finally testing and commissioning. It is required to establish synchronization points between different stakeholders, as well as between safety and security, during these stages.


Another example for developing cybersecurity standards for railway systems is under the U.S. National Committee (USNC) of the International Electrotechnical Commission (IEC) Technical Committee 9, PT 63452. The goal of this project is to establish an International Standard (IS) for handling cybersecurity for the whole railway sector based on existing industrial cybersecurity security standards (i.e. IEC 62443 and TS 50701). This technical committee serves as a forum for collaboration with industry leaders and government agencies to stay abreast of evolving best practices to improve railway's security posture in the following areas:

- » Railway asset model
- » Risk assessment: improving parts related to threat intelligence and threat landscape, optimization of Initial Risk assessment (IRA), and Detailed Risk Assessment (DRA)
- » Overall cybersecurity management, such as the OT Cybersecurity Program, supply chain management, and cybersecurity training

- » Interface definition with other disciplines (e.g. V&V, Safety, etc.)
- » Operational, maintenance, and disposal requirements

## CONCLUSION

This article provides an evaluation of cybersecurity in the rail and transit industry. Cyber threats have the potential to affect every component of railway infrastructure, with attacks ranging from accessing CCTV camera feeds, to modifying a train's speed. We can assert that security has a direct impact on safety functions and hence, should be considered equally as significant as safety.

In the realm of cybersecurity, there are mostly general norms and recommendations available, leaving the manufacturers with the discretion to choose whether or not to follow these standards. Reaching an acceptable cybersecurity maturity level (as per APTA SS-CCS-RP-006-23)<sup>17</sup> is a significant challenge, given that these guidelines often suggest different things, making it extremely difficult to achieve a satisfactory level of security. We've provided examples of the several undergoing projects aiming at creating cybersecurity standards specific for railway industry which are very promising. 

---

<sup>17</sup> "Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview". American Public Transportation Association, Washington, D.C. Publication date: 05/23/2023 [Online]. Available: <https://www.apta.com/wp-content/uploads/APTA-SS-CCS-RP-006-23.pdf>



## PRIVACY BY DESIGN STANDARDS

Aaron Weller – Global Privacy Engineering CoE Leader



Standards play a key role in expanding market access and promoting successful deployment of new technologies and products by ensuring interoperability, safety, and reliability. In addition, standards can accelerate the speed at which innovations become more than ideas. ISO/IEC JTC 1 SC 27<sup>1</sup> on Cybersecurity and Privacy is an international standards committee that develops standards on Information security, cybersecurity, and privacy protection. ISO/IEC JTC 1/SC 27/WG 1 standards (the ISO/IEC 27000 family of standards on ISMS) play a vital role for privacy by design. ISO/IEC JTC 1/SC 27/WG 5 standards such as ISO/IEC 29100, ISO/IEC 29134, and ISO/IEC 29151 are essential in defining the standardization requirements for consumer privacy by design.

### WHAT IS PRIVACY BY DESIGN?

Privacy by Design is an idea that has been around for many years, but came to prominence when the EU General Data Protection Regulation (GDPR) included

<sup>1</sup> <https://www.iso.org/committee/45306.html>

legally binding requirements<sup>2</sup> to implement processes to achieve “Privacy by Design and Default.” The fundamental idea behind Privacy by Design is that because fundamental privacy concepts such as transparency and control over usage of collected data permeate the way that systems work, considering them during the earliest stages of development leads to better outcomes that are both more effective in protecting privacy as well as more efficient in terms of the level of effort required to achieve them. This is similar to the related concept in information security that effective controls need to be “built in, rather than bolted on”<sup>3</sup> to systems, applications, and processes.

### WHAT IS THE NIST PRIVACY FRAMEWORK?

The U.S. National Institute of Standards and Technology (NIST) has a role to promote innovation through development and promulgation of standards across

<sup>2</sup> <https://gdpr-info.eu/art-25-gdpr/>

<sup>3</sup> <https://resources.infosecinstitute.com/topics/application-security/why-you-should-build-security-into-your-system-rather-than-bolt-it-on/>





a wide range of disciplines, including security and privacy. Building on its widely adopted Cybersecurity Framework, NIST released the first version of their Privacy Framework in 2020.<sup>4</sup> One of the key features of the Framework, as opposed to other standards, is its structure. Incorporating core control areas, supplemented by implementation tiers, the Framework explicitly rejects the concept of 'one-size-fits-all' in favor of a flexible approach allowing organizations to implement a framework appropriate to their needs and risks.

## ISO 31700: PRIVACY BY DESIGN FOR CONSUMER GOODS AND SERVICES

A pair of ISO standards related to Privacy by Design were published in early 2023. ISO 31700-1 includes high level privacy requirements and its companion; ISO 31700-2 covers how 31700-1 could be implemented across a variety of use cases. I was involved in the U.S. Technical Advisory group that contributed to the development of these standards and am very proud of the final product. One of the factors that we looked closely at when developing 31700 was to ensure that the entire product (and supporting services) lifecycle was considered. The standard extends Privacy by Design far beyond launch, into training those responsible for selling the product, providing easy ways to remove personal data prior to sale on the secondary market and controls around eventual disposal of devices.

One drawback of ISO 31700 is that, unlike ISO 27001 and some other ISO standards, it is not possible to certify an organization against the requirements of ISO 31700, although that capability may be developed through future standards. This was a conscious decision during development of the standard to accelerate the release of an initial version.

Many of the requirements in ISO 31700-1 also map over to the NIST Privacy Framework.

<sup>4</sup> <https://www.nist.gov/privacy-framework/privacy-framework>

## PERSONAL INFORMATION LIFECYCLE

There are several published versions of a Personal Information Lifecycle, which is one of the fundamental models used by organizations to help develop their privacy program. Privacy professionals need to be thinking about personal information before it is even collected, considering the principles of data minimization and transparency among others. Many privacy laws have a requirement to minimize the amount of personal data collected to that which is necessary for a set of pre-defined purposes. Clearly this understanding needs to be developed early in the development of a product or service, as it could have fundamental implications on downstream activities. After data has been collected, consideration should be given to controls related to storage, access, sharing, retention, and eventually deletion or destruction. This personal information lifecycle is a useful framing for Privacy by Design as it helps to avoid missing important controls later in the data lifecycle that may not be front of mind during development.

## RISK MANAGEMENT

Let us consider a risk as an event with a cause that has the potential to harm, and can be defined in terms of its significance and likelihood. Events happen all the time and many are benign. We really only want to expend effort to manage risks where the combination of significance and likelihood hits some threshold value, often referred to as a "risk appetite," where action should be taken to reduce the risk back to an acceptable level.

Privacy by Design is one way of managing privacy risks by thinking about what causes would trigger what events that would present a high enough harm, and taking action before they occur to mitigate or manage them.


I tend to frame risk management as a resource allocation problem. We never have the resources to address every potential harm, so we need to make choices.



Being able to quantify and rank risks allows us to prioritize in a quantitative way that gives us a defensible position if something goes wrong.

Standards are an important part of risk management for a couple of key reasons. Primarily, no matter how much experience you have in a particular topic area, the experts that are assembled to create a standard will have collectively orders of magnitude more experience and can provide peer review to incorporate a range of perspectives and considerations. This leads directly to the second key benefit of standards—that they are standardized (bear with me). What I mean is that a standard is broadly understood by a range of stakeholders, including auditors, privacy professionals,

and regulators. This provides a range of benefits, from tooling that has been designed to meet certain requirements expressed in a standard, to the ability to hire resources who are already familiar with a standard even if they aren't familiar with your specific implementation of it, resulting in a shorter period of time to get up to speed.

As someone who has both worked with, audited against, and, more recently, contributed to a range of standards, the privacy community has and will continue to greatly benefit as more standards are developed that turn “it depends” into a more generally understood approach to achieve a specific risk management goal. 



## USNC/IEC TRAINING & EDUCATION

New to USNC? The USNC provides education and training resources for electrotechnical standardization and conformity assessment.

We encourage you to take advantage of our training opportunities available now on the [USNC webpage!](#)

- » USNC Constituency Training Modules
- » USNC Effective IEC Participation Webinar (2023 Webinar now available!)
- » USNC & IEC Conformity Assessment 101
- » Why IEC Standards Work Is Important to My Company
- » Benefits of Standards Work for Emerging Professionals

Looking for more? IEC Academy & Capacity Building hosts frequent webinars. You can access past webinar recordings and register for upcoming webinars [here](#).



## FOOD AND DRUG OMNIBUS REFORM ACT OF 2022 (FDORA) AND MEDICAL DEVICE CYBERSECURITY

Ken Zalevsky – CEO at Vigilant Ops



On December 29, 2022, the president of the United States signed into law the Food and Drug Omnibus Reform Act of 2022 (FDORA) as part of the Consolidated Appropriations Act, 2023. This law introduces various provisions aimed at improving medical device cybersecurity, which will have considerable effects on medical device manufacturers and their consumers. Through FDORA, the United States Food and Drug Administration (FDA) was granted the legislative authority to require cybersecurity documentation from medical device manufacturers.

In the medical device industry, this recently-executed legislation represents a dramatic shift in the regulatory landscape. While FDA has authored numerous guidance documents, with various recommendations for medical device manufacturers, this legislative authority is a whole new ball game.

### WHAT THIS MEANS TO MEDICAL DEVICE MANUFACTURERS

We'll start by taking a look at the scope of the legislation and the description of the medical devices covered. According to the document, the legislation applies to

all **cyber devices**, which are defined as any device that has the **ability to connect to the internet** and **contains technological characteristics that could be vulnerable to cybersecurity threats**. In other words, this legislation is applicable to most medical devices. While there are undoubtedly devices that are standalone with no ability to communicate and others that have no technological characteristics (a tongue depressor comes to mind), for most medical device manufacturers, this law applies to some device or multiple devices in their portfolio. And, to add urgency to the matter, this law is actually enforceable at this very moment.

### NON-COMPLIANCE RESULTS IN PENALTIES SOONER RATHER THAN LATER

According to the legislation, these cybersecurity requirements went into effect 90 days after the date of the Act, on March 29, 2023. While manufacturers were given until October 31, 2023, to begin submitting the appropriate documentation, compliance with these legislative requirements is now expected.





The legislation spells out the consequences of non-compliance by adding this phrase to the Federal Food, Drug, and Cosmetic Act (FD&C): “The failure to comply with any requirement under section 524B(b)(2) relating to ensuring device cybersecurity” to the Prohibited Acts and Penalties of the FD&C. This chapter of the FD&C covers, in great detail, those activities which will incur penalties and begins with, “The following acts and the causing thereof are hereby prohibited.” In other words, failure to comply with cybersecurity requirements is prohibited by law and is now considered alongside prohibited acts such as mislabeling and misbranding.

## VULNERABILITY PLAN

For medical device manufacturers, the cybersecurity requirements begin at the top of page 3538 in section (b), describing how manufacturers should handle vulnerabilities. The requirement is to “submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket vulnerabilities and exploits...”

While it may seem contradictory to require a post-market plan in a premarket submission, the message conveyed to manufacturers is that cybersecurity cannot be an afterthought. The cybersecurity of the device should be considered as far upstream in the development lifecycle as possible. Requirement (2) under section (b) contains various references to the development lifecycle of devices, beginning with the recommendation for secure processes from development all the way through to the availability of postmarket updates and patches to address cybersecurity vulnerabilities. In addition, the ability to respond to vulnerabilities in “a reasonable time” implies frequent, if not continuous, vulnerability monitoring. This is another key consideration for medical device manufacturers as they build or adapt processes to support compliance.

## SOFTWARE BILL OF MATERIALS

Requirement (3) under section (b) requires manufacturers to provide a software bill of materials, “including

commercial, open-source, and off-the-shelf software components.” As a list of software components in a device, the SBOM makes sense and is easy to understand. As always, however, the danger lies in the details. Knowing what an SBOM is and consistently, reliably generating and maintaining an SBOM for each device are two different stories. Then there is the sharing dilemma.

Some device manufacturers are debating the question of sharing SBOMs, due to some very real concerns about exposing vulnerable components to bad actors. While sharing SBOMs with FDA is a must-have, some are still looking at sharing with consumers as a nice-to-have. This view will need to adapt to the seemingly eventual demand for SBOMs from consumers.

Fortunately, there are many SBOM resources available to help manufacturers, from minimum SBOM requirement documentation to open-source and commercial tools available to assist in automating the SBOM process, depending on where the manufacturer is in their SBOM journey. Given the breadth of the SBOM topic and the lack of homogeneous adoption, we won't attempt to cover the topic here; however, we have included a Resources section at the end of this article with SBOM and other references.

## SUMMARY

In this article, we highlighted FDORA content with specific impact on medical devices and the resulting requirements for medical device manufacturers. While medical device cybersecurity continues to evolve, manufacturers need to evolve, as well. By prioritizing cybersecurity and the development of supporting processes and procedures, they will be well on their way toward compliance, now and in the future.

## RESOURCES


This article detailed the cybersecurity requirements found in the Consolidated Appropriations Act, H.R. 2617, which is available at <https://www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf>



For additional details from FDA on the application of the reviewed legislation to medical devices, please refer to the following guidance documents from FDA:

- » FDA Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions>
- » FDA Postmarket Management of Cybersecurity in Medical Devices <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices>

For help with the software bill of materials (SBOM), please refer to the following:

- » The Cybersecurity & Infrastructure Security Agency (CISA) Software Bill of Materials <https://www.cisa.gov/sbom>
- » International Medical Device Regulators Forum (IMDRF) – “Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity” <https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity>
- » Achieve SBOM Compliance with the InSight Platform from Vigilant Ops <https://www.vigilant-ops.com/> 







## REFLECTIONS ON THE IEC YOUNG PROFESSIONALS PROGRAMME

*Mariah Dixon – Senior Standards Engineer at UL Standards & Engagement; 2023 USNC/IEC Young Professional*



I am truly grateful for the opportunity to attend this virtual conference in 2023. Being selected by the U.S. National Committee (USNC) to represent the U.S. in the IEC Young Professionals Programme was a great honor. Despite the unforeseen circumstances that led to the conversion of the events to a virtual setting due to the conflict between Israel and Palestine, I am thankful for the chance to participate in the IEC Young Professionals (YP) Workshop and the 87<sup>th</sup> Annual IEC General Body Meeting.

One of the aspects I appreciated most about the virtual workshop was the ability to connect and network with professionals from around the world. Although the virtual format limited the number of people I could meet, I had the pleasure of collaborating with exceptional individuals who were not only great to work with but also a source of valuable knowledge. The workshop itself was highly informative, offering insights into various areas of focus within the IEC.

Among the activities, the IEC Serious Game stood out as particularly intriguing. It demonstrated the power

of collaboration and learning from others with diverse backgrounds and experiences. The game provided a creative and engaging way to explore IEC standards and conformity assessments. Erdun Lai, a fellow YP from Australia and now a YP Leader, played a pivotal role in fostering connections among the participants by tapping into our shared passion for video games. We realized that by developing a compelling storyline, we could effectively educate people about the importance and relevance of IEC standards and conformity assessments.

Another notable session was the Online Standards Development (OSD) presentation, which showcased how technology is enhancing the standards development process. The OSD platform facilitates collaborative work, transparency, and harmonization within the IEC and ISO community. It streamlines the writing, reviewing, and commenting processes, allowing for flexibility and improved coordination. This investment in technology sets a strong foundation for future products and services provided by the IEC, and I believe






it will yield significant dividends as the standards development process continues to evolve in this technology-driven era.

The program also emphasized the critical role that standards play in ensuring the safety, interoperability, and quality of products, systems, and services. I gained a deeper understanding of how standards impact various industries and how they contribute to global trade, innovation, and sustainability. The discussions on emerging technologies, such as artificial intelligence, Internet of Things (IoT), and renewable energy, highlighted how standards are evolving to address the challenges and opportunities presented by these advancements.

Despite the challenging time difference between Chicago, IL, and Cairo, Egypt, which meant early

mornings without the sun's warmth, I consider myself privileged to have participated in this once-in-a-lifetime opportunity. This experience has broadened my perspective on the world of standardization. I eagerly look forward to engaging with the IEC in future opportunities as I continue to grow in my career. I highly recommend this program to young professionals aspiring to make their mark in the field of standardization.

I would like to express my heartfelt gratitude to the U.S. National Committee for providing me with this incredible opportunity. I am also grateful to all those who have supported me along the way. Thank you for believing in me and helping me reach this milestone in my career journey. 

---

## TMC MEETING

Derrick Martin (UL Standards & Engagement), Secretary to USNC TAG TC 85 and TC 129, provided a report on each TAG's activities to the USNC Technical Management Committee (TMC) at their January 24, 2024 meeting held in San Francisco, CA





## JUST PUBLISHED

Check out the latest and greatest recently published standards by the IEC. A complete list of recently published documents can be found [here](#). Here's just one (of many!) we think you'll find interesting:

### **ISO/IEC 42001:2023 INFORMATION TECHNOLOGY – ARTIFICIAL INTELLIGENCE – MANAGEMENT SYSTEM**

ISO/IEC 42001:2023 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. It is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems.

ISO/IEC 42001 is the world's first AI management system standard, providing valuable guidance for this rapidly changing field of technology. It addresses the unique challenges AI poses, such as ethical considerations, transparency, and continuous learning. For organizations, it sets out a structured way to manage risks and opportunities associated with AI, balancing innovation with governance.

Benefits:

- Framework for managing risk and opportunities
- Demonstrate responsible use of AI
- Traceability, transparency, and reliability
- Cost savings and efficiency gains

Developed by ISO/IEC JTC 1/SC 42, *Artificial Intelligence*



## MAKE AN IMPACT ON QUANTUM TECHNOLOGIES: JOIN USNC TAG FOR NEW IEC/ISO JOINT TECHNICAL COMMITTEE ON QUANTUM TECHNOLOGIES



Calling all U.S. stakeholders: [The American National Standards Institute](#) (ANSI) encourages interested experts to participate in the USNC Technical Advisory Group (TAG) for the newly formed International Electrotechnical Commission (IEC)/International Organization for Standardization (ISO) Joint Technical Committee (JTC) 3, *Quantum Technologies*.

In January, the USNC Technical Management Committee approved the National Institute of Standards and Technology (NIST)—which has released two documents on Quantum Readiness [open for public comment](#)—as the USNC TAG Administrator for JTC 3.

### ABOUT JTC 3 ON QUANTUM TECHNOLOGIES

Following the approval of a proposal from the British Standards Institution (BSI) for IEC and ISO to form a JTC, in November 2023, the IEC Standardization Management Board (IEC/SMB) and the ISO Technical Management Board (ISO/TMB) announced the scope of the JTC 3:

- » Standardization in the field of quantum technologies.
- » The scope includes standardization in the field of quantum technologies, including quantum information technologies (quantum computing and quantum simulation), quantum metrology, quantum sources, quantum detectors, quantum

communications, and fundamental quantum technologies. The JTC will coordinate the results of these efforts with relevant committees and subcommittees that have within their scopes the development of specific sector-based applications of quantum technologies.

- » Excluded: Specific sector-based applications and standardization in the fields of information technology (JTC 1 and its subcommittees), nanotechnology (IEC TC 113 and ISO TC 229), fibre optics (IEC TC 86), cryogenic vessels (ISO TC 220), and semiconductors (IEC TC 47).
- » Liaisons: JTC 1 and its appropriate subcommittees, IEC TC 46, IEC TC 47, IEC TC 62, IEC TC 86, IEC TC 90, IEC TC 113, ISO TC 172, ISO TC 201, ISO TC 206, ISO TC 220, ISO TC 229, ITU-T, ETSI, CEN & CENELEC JTC 22.

The new JTC will operate under the IEC Directives Supplement and IEC IT system, and ANSI staff assigned to the USNC/IEC will facilitate and coordinate related activities; the ANSI internal oversight of the USNC TAG for the new JTC is under the USNC Technical Management Committee (USNC/TMC).

### HOW TO GET INVOLVED

Stakeholders interested in becoming a member of the USNC TAG to JTC 3 should email Tony Zertuche ([tzertuche@ansi.org](mailto:tzertuche@ansi.org)) or Ade Gladstein ([agladstein@ansi.org](mailto:agladstein@ansi.org)).





## CALL FOR STANDARDS ACTION AND PARTICIPATION



### IEC MARKET STRATEGY BOARD (MSB) – US REPRESENTATIVE NEEDED

Michael Regelski's final term on the IEC Market Strategy Board (MSB) ends on May 31, 2024. Individuals interested in serving as a U.S. representative to the IEC MSB are invited to **contact Ade Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org) by Friday, March 8, 2024.**

#### IEC MSB SCOPE

The IEC Board delegates to the Market Strategy Board (MSB) the identification and investigation of principle technological trends and market needs in the Commission's fields of activity.

The MSB collaborates with the CAB and the SMB, and with other relevant bodies reporting to the IEC Board.

It may establish Special Working Groups (SWGs) to investigate certain subjects in-depth or to develop a specialized document.

### USNC PARTICIPANTS NEEDED

IEC approved one (1) new Committee: IEC Project Committee (PC) 131, *Rotating electrical machines for the traction of road vehicles.*

NEMA was recently approved as the USNC TAG Administrator to PC 131. Individuals who are interested in becoming a USNC Technical Advisory Group (TAG) member for the USNC TAG to PC 131, *Rotating electrical machines for the traction of road vehicles*, are invited to **contact Ade Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org) as soon as possible.**

#### PC 131 SCOPE

Standardization of rotating electrical machines for the traction of road vehicles without limitations of voltage below <1000/1500 AC/DC, output (power, torque, and speed) or dimensions, with the exception of the following:

- » Traction motors within the scope of TC 9, *Electric railway equipment – including traction motors for trolleybuses*;
- » Motors and generators within the scope of TC 2, *Rotating machinery*;
- » Motors and generators for use in aeronautics or space applications;
- » Motors and generators for road vehicles which are not intended for the traction of them;
- » Road vehicles with pantographs.



## CALL FOR MEMBERS – USNC TAG TO IEC SC 23K ELECTRICAL ENERGY EFFICIENCY PRODUCTS

The USNC Technical Advisory Group (TAG) to IEC SC 23K, *Electrical Energy Efficiency products*, would like to grow its membership. Individuals who are interested in joining the USNC TAG to IEC SC 23K as members are invited to **contact Adelana Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org) as soon as possible.**

### IEC SC 23K ELECTRICAL ENERGY EFFICIENCY PRODUCTS SCOPE

Standardization in the field of energy efficiency products, systems, and solutions, to be used in existing and new electrical installations, for monitoring, measuring, controlling, managing, and optimizing the overall efficient use of A/C and D/C electrical energy for household and similar.

## USNC TAG ADMINISTRATOR – ORGANIZATION NEEDED


CSA Group is relinquishing its role as the USNC TAG Administrator for the USNC TAG to IEC/TC 57, *Power systems management and associated information exchange*. The USNC is looking for a new organization to take on this USNC TAG Administratorship.

Please note that according to the rules and procedures of the USNC, a USNC TAG cannot exist without a USNC

TAG Administrator. If we cannot find a new USNC TAG Administrator, the USNC will have to withdraw from international participation and register with the IEC as a Non-Member of this Committee.

If any organizations are interested in the position of USNC TAG Administrator for the USNC TAG to IEC/57, they are invited to **contact Adelana Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org) by March 1, 2024.**

### TC 57 POWER SYSTEMS MANAGEMENT SCOPE

To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, tele-protection, and associated information exchange for real-time and non-real-time information, used in the planning, operation, and maintenance of power systems. Power systems management comprises control within control centres, substations, and individual pieces of primary equipment including tele-control and interfaces to equipment, systems, and databases, which may be outside the scope of TC 57. The special conditions in a high voltage environment have to be taken into consideration. 

## DON HEIRMAN AWARD PROGRAM: APPLICATION DEADLINE APPROACHING!

Did you know the USNC launched the new [Don Heirman Award Program](#) on electromagnetic compatibility (EMC)?

This new program gives students and young professionals the opportunity to compete in an annual paper competition on the topic of electromagnetic compatibility (EMC) for a **\$1,000 cash prize**. Submissions are due by 5 p.m. ET on **Friday, June 7, 2024**, to [mpahl@ansi.org](mailto:mpahl@ansi.org).

For more details, including how to apply, please see the [program flyer](#).

The USNC would like to thank our generous donor, Mr. Bill Radasky, for making this award program possible.





United States  
National Committee  
of the IEC



## JOIN THE USNC LINKEDIN GROUP

Would you like to stay updated with the news and events of the USNC? [Join our LinkedIn Group](#) to learn about and provide input on all issues electrotechnical that can affect your life, from your own home to the other side of the globe! If you have any information to share on LinkedIn, please contact Megan Pahl ([mpahl@ansi.org](mailto:mpahl@ansi.org)).



## ABOUT THIS PUBLICATION

The USNC Current newsletter is distributed to the constituency of the U.S. National Committee (USNC) of the International Electrotechnical Commission (IEC). It provides updates on technical activities and other information of interest to members of the electrotechnical community. Some articles are reprinted with permission from the IEC News log.

### DISCLAIMER

The opinions expressed by the authors are theirs alone and do not necessarily reflect the opinions of the USNC or ANSI.

### HOW TO CONTRIBUTE

Contributions are gladly accepted for review and possible publication, subject to revision by the editors. Submit proposed news items to: Megan Pahl, [mpahl@ansi.org](mailto:mpahl@ansi.org).