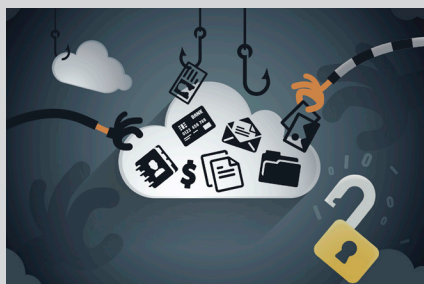


FOCUS ON: CYBERSECURITY AND STANDARDS

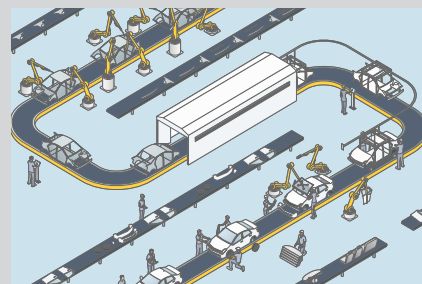
FEATURED STORIES



Cybersecurity and Standards: Where Are We Today?



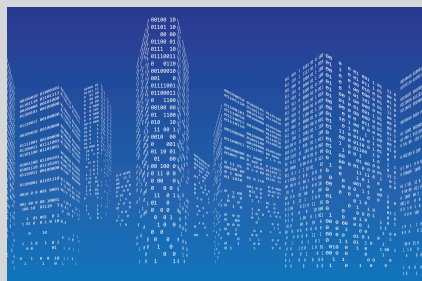
Standardization and Trade: Core Principles and Their Applicability to Digital Issues Including Cybersecurity



Industrial Control System Cybersecurity Standards and Guidelines



IEC Cybersecurity Standards and Guidelines for the Smart Grid



Process Sensor Cybersecurity and Safety Is Currently Not Addressed: What It Means to Standards



In Memoriam: Samuel "Keel" Kelly & Ron Peterson

IN THIS ISSUE

2 Featured Stories

7 Laugh Track

8 Decision Depot

18 News

19 Documents of Interest

19 Upcoming Events



United States
National Committee
of the IEC

Cybersecurity and Standards: Where Are We Today?

By Laura Lindsay, U.S. National Standards Officer, Corporate Standards Group, Microsoft



What is cybersecurity?

The term means different things depending on the industry that is using it. In reality, there is no single definition for Cybersecurity; it

is defined based on what industry you are talking with. One confusion is in "How do IT security/information security and cybersecurity relate to each other?" Some use the terms interchangeably, and there is some overlap between the two. IT security, also referred to as information security, is concerned with the confidentiality, integrity, and availability of information, which really means the protection of and prevention of unauthorized use of information/data. This includes protecting organizations and the devices/machines that organizations use. Cybersecurity is also concerned with the same concepts of ensuring confidentiality, integrity, and availability. Where these differ is that information security can cover anything including the paper copies kept in a file drawer, whereas cybersecurity is really only what is digitally connected. cybersecurity also draws on concerns around safety and resilience that are not considered in a pure information security environment.

In the U.S., we have what most refer to as the NIST Cybersecurity Framework, which is actually titled "Framework for Improving Critical Infrastructure Cybersecurity." In the Interagency Report on Strategic U.S. Government Engagement in International



Standardization to Achieve U.S. Objectives for Cybersecurity (NISTIR 8074), cybersecurity is defined as "the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability."¹

Standards Landscape

Much of the work that has been done over the last 50 years in the IT/information security area is applicable to cybersecurity and can be leveraged by non-IT organizations. These good practices are applicable to any digitally connected environment. To better understand the breadth of cybersecurity, we can take a look at NISTIR 8074 where it describes the core areas of cybersecurity to be:

- » Cryptographic techniques
- » Cyber incident management
- » Identity and access management
- » Information security management systems (ISMS)
- » IT systems security evaluation
- » Network security
- » Security automation and continuous monitoring
- » Software assurance
- » Supply chain risk management
- » System security engineering

Note the broad overlap with areas that have traditionally been considered IT, but are now considered in the broad context of cybersecurity.

To further explain that cybersecurity is more than just IT, look at the examples of some of the applications

1. U.S. Department of Homeland Security, Blueprint for a Secure Cyber Future: the Cybersecurity Strategy for the Homeland Security Enterprise, November 2011, p. D-2. Available at: <http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf> [accessed 11/20/2015].

of cybersecurity (again from NISTIR 8074):

- » Cloud computing
- » Emergency management
- » Industrial control systems
- » Health IT
- » Smart grid
- » Voting
- » Internet of things (IoT)

With this wide range of applications, you can imagine that there is a broad range of standards that already exist. In bringing these concepts together to create a strong cybersecurity program, we can start with the NIST Cybersecurity Framework. This document provides a framework for setting up, implementing, and maintaining a Cybersecurity program to help an organization manage increasing cybersecurity threats. The key to this framework is that an organization needs to understand what the risks are to the organization and do a risk analysis and assessment. This risk-based approach allows organizations to address what is relevant to their organization, business, and industry.

The NIST Cybersecurity Framework then provides a framework of five functions to help organizations determine what actions need to be taken to address and mitigate those risks. These functions include Identify, Protect, Detect, Respond, and Recover. Within each of these functions are categories and subcategories that describe actions that should be taken. One example is that the Identify function is used to develop the

organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. One category under Identify might be Business Environment: understanding an organization's objectives, stakeholders, and activities—ensuring they are understood and used to inform roles, responsibilities, and risk management decisions. Comprehensive security measures are necessary covering the company itself, its group companies, business partners of its supply chain, and IT system-control outsourcing companies.

To be able to implement this outcome or better understand how to implement, there are a number of existing standards that can help an organization. To understand the existing set of standards that are available in ISO and IEC, there is a Technical Report, ISO/IEC TR 27103, *Information technology—Security techniques—Cybersecurity and ISO and IEC Standards*, that builds on the concepts that are initially introduced in the NIST Cybersecurity Framework and addresses them across an international view mapping to existing ISO, IEC, and ISO/IEC standards. This technical report takes into account not just information security standards but also looks at applicable standards that exist in other verticals, such as industrial control systems, so that there is an understanding that the concepts are the same and a variety of existing standards can be used. Even though the standards that are mapped in this technical report do not have titles that include the word “cybersecurity,” these standards are applicable to protecting a cybersecurity environment.

To address a better understanding of cybersecurity, there are efforts underway in ISO/IEC Joint Technical Committee 1, Sub-committee 27 (JTC 1/SC 27) to draft an overview and concepts for cybersecurity to better address how cybersecurity relates to information security, privacy, safety, and resilience. To address harmonization around the many cybersecurity programs and frameworks that are popping up globally, ISO/IEC JTC 1/SC 27 has also initiated a standard for guidelines for a cybersecurity framework that will address the concepts needed to address in any cybersecurity program that an organization may want to create. Addressing resiliency standards are being worked in other ISO committees (such as ISO/TC 292), particularly around organizational resilience and supply chain security.

Governance is integral to addressing cybersecurity in the boardroom, and this is an area that is still a gap in the standards space. Tying the existing standards to organizational and business requirements in a way that can be understood at a high level but still addressed by those that need to implement that work is a work in progress.

Summary

Standards to address cybersecurity exist already, even though those standards may not say “cybersecurity” on them. There are some gaps in standards and those are starting to be addressed. As the gaps are addressed, standards will have a full way to address cybersecurity concerns.



Standardization and Trade: Core Principles and Their Applicability to Digital Issues Including Cybersecurity

By Renee Hancher, Lead, Standards Policy and Negotiations, Office of Standards and Investment Policy, Industry and Analysis, International Trade Administration (ITA)



Standards-related measures, which include standards, technical regulations, conformity assessment procedures, and accreditation, play a critical role in

shaping the flow of international trade. Standards are the building blocks for regulations and trade. They are essential to accelerating the widespread commercialization of new technologies and enabling goods to move easily between markets. Conformity assessment and accreditation provide confidence that traded goods will perform as specified. Simply put, standardization is the key that opens the door to global markets.

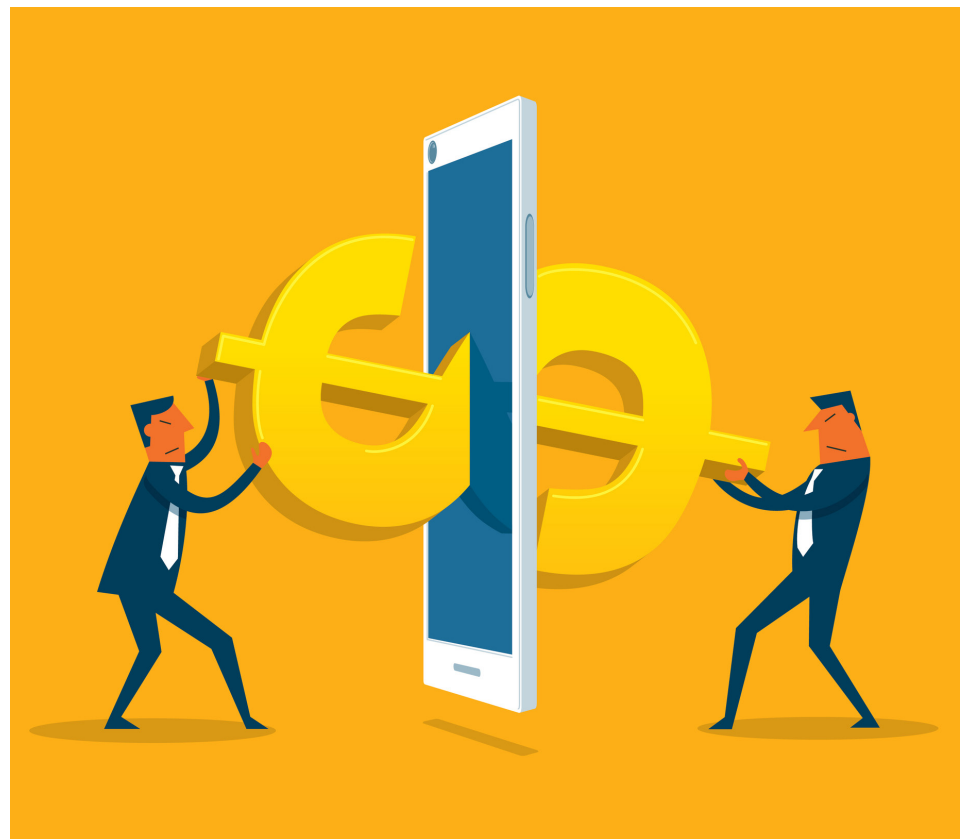
What is critical is how standards and conformity assessment measures are developed and applied. When standards are developed in an open, transparent, inclusive, and balanced manner, they can facilitate trade. If not, they can create trade barriers. When used by an economy as the basis for establishing a technical requirement in a regulation, voluntary standards can help harness relevant technology to achieve regulatory objectives in a cost-effective manner. If all relevant parties are not engaged, markets do not benefit from the best solutions and products may not be as safe, or serve the needs of consumers the way they should. If standards are not developed in the most open and transparent process possible, this can

also lead to less competition as the market is not allowed to find the most lucrative market-based solution.

A recent ITA study found that 92% of U.S. goods exports are affected by standards and technical regulations.² Standards-related non-tariff measures are the most common non-tariff barrier U.S. exporters encounter. Similarly, conformity assessment measures (e.g., testing or certification requirements) can have a trade impact when, for example, countries require unnecessary or duplicative

procedures, or in-country-only testing to sell in those markets.

The World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT Agreement) sets forth the multilateral rules governing standards-related measures to help ensure that such measures are transparent, are not discriminatory, and are not more trade restrictive than necessary to meet legitimate regulatory objectives. The WTO Agreement on Sanitary and Phytosanitary Measures (SPS Agreement) also establishes



2. <https://www.trade.gov/press/press-releases/2016/new-report-shows-92-percent-of-us-goods-exports-may-be-affected-by-foreign-technical-regulations-062916.asp>

disciplines for food safety and related areas, including the importance of science-based decision making. U.S. free trade agreements (FTAs) include both TBT and SPS provisions.

A few critical provisions of the TBT Agreement and subsequent WTO TBT Committee work have underscored the role of standards in trade. The TBT Agreement requires that each WTO member use relevant international standards as the basis for its technical regulations and conformity assessment procedures. The Agreement also makes clear that there can be more than one relevant standard. This increases consumer choice and facilitates global trade.

The TBT Agreement does not define an international standard as being developed by a specific body. Rather, a subsequent decision of the TBT Committee developed a set of principles for international standards development (including openness, transparency, impartiality, and consensus); any standard developed according to these principles should be considered an "international standard."³ When regulations and accompanying testing and certification procedures diverge from globally recognized standards, especially in ways that are unnecessarily trade-restrictive, they create powerful market access challenges for industry.

These core principles remain relevant in the digital economy space as well. Connectivity, interoperability, and cybersecurity depend upon the use of globally recognized standards, state of the art practices and policies, and approaches that are aligned across markets. Divergent or overly prescriptive measures can restrict trade and reduce flexibility needed to

keep up with the dynamic technology changes that are taking place.

The ITA at the U.S. Department of Commerce (DoC) recognizes the fundamental role standards play in trade and works to support U.S. industry in increasing its global market share, which in turn supports jobs and growth. ITA has a complete toolbox of standards resources to support U.S. industry. Standards issues can be raised in commercial dialogues organized with major trading partners like Brazil and India, in bilateral or Free Trade Agreement (FTA) meetings, or at the World Trade Organization. ITA can assist in resolving transactional issues via our network of offices around the United States and around the globe.

ITA also works to foster public-private partnerships to tackle standardization challenges, convenes U.S. and foreign regulators on specific sector issues, and highlights U.S. standardization solutions that underpin emerging technologies. Much of this work happens in regional fora such as the Asia Pacific Economic Cooperation forum (APEC) and with the Association of Southeast Asian Nations (ASEAN), among other regional groups.

ITA's standards work is increasingly focused on emerging technology areas where market rules, regulatory requirements, and standards are not yet set or may be evolving. ITA partners with standards development organizations, industry groups, and other parties to explain the U.S. approach to our trading partners with the aim of encouraging compatibility or flexibility in standards and regulatory requirements that will ensure U.S. goods and technology have market access. With regard to cybersecurity standardization, ITA tracks cyber regulatory requirements

in other markets and encourages comments on draft requirements. ITA works with other agencies, including the Department of Homeland Security (DHS) and the National Institute for Standards and Technology (NIST), another agency of the DoC, to exchange information with U.S. trading partners on approaches to the creation and implementation of a cybersecurity regulatory framework.

To export successfully, regardless of the product or technology, one needs to know how to navigate the global standards, testing, and regulatory landscape. Some useful ITA resources are available on Export.gov, including 125 Country Commercial Guides (www.export.gov/ccg) which have a standards and regulations section.

In addition, the Top Markets reports from ITA's Industry and Analysis unit (see trade.gov/topmarkets) include information on the global regulatory landscape for 27 different sectors. Another valuable resource is the free Notify U.S. service that is operated by NIST, where one can find out about proposed technical regulations and conformity assessment procedures—and send comments to trading partners before these rules become effective. Information can be customized by sector or country. See www.nist.gov/notifyus.

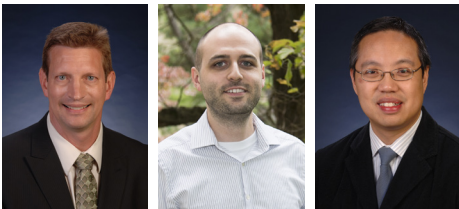
Standards and trade are as interconnected today as our digital world. They underpin the strength and innovative nature of the U.S. economy and provide a gateway to global commerce. As new opportunities open up globally in emerging areas, understanding the standards and technology involved, and how to navigate this new trade frontier, will be necessary for U.S. industry to remain at the forefront of innovation.



3. Decision on Principles for the Development of International Standards, Guides and Recommendations with Relation to Articles 2, 5 and Annex 3 of the WTO Agreement on Technical Barriers to Trade (2002).

Industrial Control System Cybersecurity Standards and Guidelines

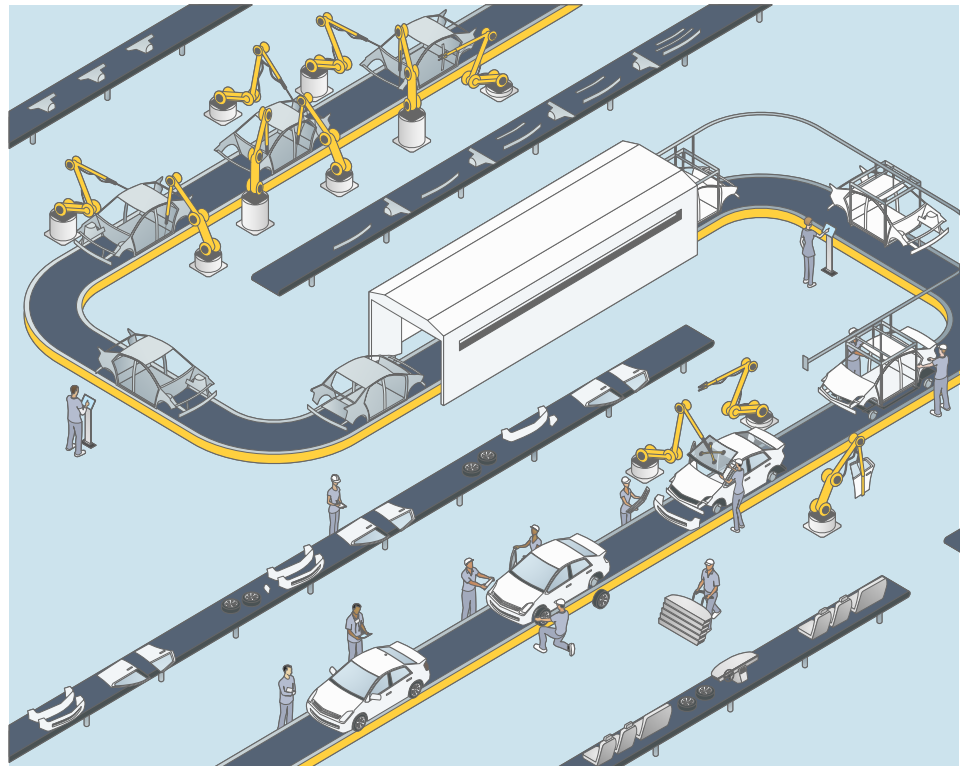
By Keith Stouffer, Timothy Zimmerman, and CheeYee Tang, National Institute of Standards and Technology (NIST)



Industrial control systems (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system devices such as programmable logic controllers (PLCs) often found in the industrial sectors and critical infrastructures. ICS control and monitor power generation and distribution systems, hydroelectric dams, water treatment plants, oil and gas distribution, nuclear power plants, and many varieties of manufacturing systems.

Many ICS began as proprietary, stand-alone collections of hardware and software that were disconnected from the rest of the world and therefore isolated from most external threats. Today, network connectivity, commercial software applications, Internet-enabled devices, and other information technology (IT) offerings have been integrated into many systems, and the data produced in ICS operations is used to support business decisions. This connectivity has delivered many benefits, but it also has increased the vulnerability of these systems to malicious attacks and other cyber threats.

Traditional IT cybersecurity policies focus primarily on confidentiality, with availability typically being the lower priority. In contrast, ICS, especially



those considered critical infrastructure, must maintain a high level of data and system integrity, data and system availability, and operational resilience for many reasons including economic, environmental, human safety, and national security. For many systems, it is unacceptable to degrade ICS performance for the sake of security.

ICS Cybersecurity Standards and Guidelines

Several voluntary cybersecurity standards and guidelines detailing best practices for protecting ICS have been produced by industry, trade groups, and government agencies. Due to their unique performance, reliability, and safety requirements,

securing ICS often requires adaptations and extensions to traditional IT cybersecurity standards and guidelines.

ISA/IEC 62443, Industrial Automation and Control Systems (IACS) Security

ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure industrial automation and control systems (IACS). This guidance applies to end-users, system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing IACS.

NIST SP800-82, Guide to Industrial Control Systems (ICS) Security

Downloaded more than 3 million times since its initial release in 2006, NIST SP 800-82 provides a comprehensive cybersecurity approach for securing ICS while addressing their unique system performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

NISTIR 8183, Cybersecurity Framework Manufacturing Profile

NISTIR 8183 provides a manufacturing implementation, or profile, of the Cybersecurity Framework (CSF) to help manufacturers reduce cybersecurity risks while maintaining alignment with manufacturing sector goals and industry best practices. This CSF Manufacturing "target" profile provides customized CSF subcategory language relevant to the manufacturing domain, and focuses on desired cybersecurity

outcomes and can be used to identify opportunities for improving the current cybersecurity posture of a manufacturing system. The CSF Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems.

ICS Cybersecurity Objectives

Several of the primary cybersecurity objectives defined within these voluntary standards and guidelines include:

- » Logical protection: Segregate the ICS and business network, restricting logical access to the ICS network and network activity. Implement a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer. Consider separate authentication mechanisms and credentials for users of the business and ICS networks.
- » Physical protection: Restrict physical access to the ICS network and devices using a combination of physical access controls such as locks, card readers, and/or guards. Unauthorized physical access to components could cause serious disruption of the ICS.
- » Asset protection: Protect individual ICS components from exploitation. Deploy security patches in as expeditious a manner as possible. Disable unused ports and services. Restrict ICS user privileges to only those that are required. Implement antivirus and file integrity checking software where feasible to prevent, deter, detect, and mitigate malware.
- » Continuous monitoring: Monitor risk and update security controls to mitigate vulnerabilities. Security is not a once and done exercise. Continuously monitor system boundaries, risk, and threats.

LAUGH TRACK



CartoonStock.com

NIST ICS Cybersecurity Testbed

As previously mentioned, several voluntary cybersecurity standards and guidelines detailing best practices for protecting ICS have been developed; however, guidance that describes how to balance those protections with potential negative impacts they may have on performance of the ICS is scarce.

To address that gap, NIST has developed an ICS Cybersecurity Testbed to measure the performance of ICS when instrumented with cybersecurity protections prescribed by the standards and guidelines mentioned in this article.

The testbed includes ICS scenarios for process control and discrete manufacturing. The Tennessee Eastman chemical process model was chosen for the process control scenario since it is a well-known model used in control systems research and the dynamics of the process is well understood. The Tennessee

Eastman process is controlled by industry-standard ICS hardware and software while the chemical reaction is simulated. A collaborative robotic assembly scenario was chosen to research the impacts of cybersecurity on a discrete manufacturing system with embedded control and dynamic operations. The testbed is intended to emulate a real-world industrial enterprise system as closely as possible without reproducing an entire system.


The testbed is intended to be reconfigurable such that different components may be interconnected in a variety of network configurations for testing. The testbed also includes a measurement system that captures network traffic and security events using tools like Syslog and Wireshark to analyze any network and operational performance impacts.

Research areas of interest for the testbed include: perimeter network security; host-based security; user and

device authentication; packet integrity and authentication; encryption; zone-based security; field bus (non-routable) protocol security; and robust/fault tolerant control.

Research outputs will be used to produce guidelines, test methods, metrics, and tools based on measurement science and standards to give industry the confidence it needs to effectively apply cybersecurity protections on their systems without negatively affecting their performance, safety, or reliability.

DISCLAIMER

Certain commercial equipment, instruments, or materials may be identified in this article in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose. 

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 links below to access the recent decisions.

[CAB/1759/DL](#)

CONFORMITY ASSESSMENT BOARD (CAB)
Meeting 43, Geneva, 2018-06-11

[CB/942/DL](#)

COUNCIL BOARD (CB)
At the 2017-10-11 meeting in Vladivostok and at the 2018-06-14 Council Board meeting in Geneva

[SMB/6460/DL](#)

STANDARDIZATION MANAGEMENT BOARD (SMB)
Meeting 162, Geneva, 2018-06-12

IEC Cybersecurity Standards and Guidelines for the Smart Grid

By Frances Cleveland, President, Xanthus Consulting International



Cybersecurity for the Smart Grid

Over the last few years, cybersecurity for the electric power industry has shifted from being viewed as mostly unnecessary to becoming a critical aspect of smart grid operations. This paradigm shift has occurred for many reasons, but the key drivers are:

- » Deliberate cyber attacks have been successful in causing major outages. The most visible was

the attack on the Ukrainian power system in December 2015.

- » The smart grid is becoming increasingly reliant on cyber assets, and increasingly uses commonly available information technologies (IT) for intelligent systems and communications rather than special proprietary technologies.
- » Distributed energy resources (DER) are becoming major sources of energy, but are not, for the most part, under the direct control of utilities, are located in unsecured

sites, and could be easily threatened for financial or political gain.

Recent Cyber Attacks against Power System

In the past it was considered unimaginable why anyone would want to attack the electric grid via cyber means, since well-placed bombs on transmission towers would be much easier for terrorists. However, cyber attacks against the “cyber-physical” power system are beginning to increase:

- » An attack on a few power plants around the world was able to continue for years because they only quietly monitored the plants for a few years. By being quiet, this attack avoided detection
- » A malware attacker (BlackEnergy) on the Ukrainian power system monitored operations for a few months, then in December 2015, initiated an attack which tripped substation breakers and then blocked the SCADA system from restoring the power grid. Ukraine only experienced a short blackout and was saved by field crews who hadn’t forgotten the manual methods for restoring power—a capability not shared by most other utilities.
- » A more powerful version of the malware, Industroyer/ CrashOverride, was “tested” in 2016 in the Ukraine, and has been detected in other SCADA systems. In these episodes, the attackers took screen shots of the SCADA displays to prove they had infiltrated the systems, but then did nothing more. This malware



contains four ICS-specific modules that can exploit the four most commonly used smart energy protocols: IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OPC DA, thus posing a very realistic threat to power system operations.

- » The very similar Dragonfly 2.0 malware has been detected by cybersecurity firms in utility systems, although no attacks are as yet known (publicly).
- » There will be more attacks—and more successful attacks—particularly if power system communications protocols fail to include cybersecurity protection.

Smart Grid Reliance on Cyber and Communications Technologies

Although most discussions of cybersecurity focus on the threat of intentional attacks by cyber attackers, the vulnerabilities of the smart grid are more likely due to increased inadvertent “attacks” caused by human mistakes, equipment failures, and natural disasters. From a power system operation perspective, it does not matter what caused the disruption. For this reason, cybersecurity approaches must include protection from both deliberate and inadvertent attacks, as well as coping strategies for handling successful attacks.

Smart grid systems are becoming more automated and increasingly dependent on cyber assets and communications. Utility control centers are increasing their use of digital technologies to monitor, analyze, and update field equipment to improve power system planning and operations, increasingly for medium- and even low-voltage power systems. Asset management is becoming more sophisticated with the use of digital technologies to collect asset information (QR codes, nameplate data) to manage

the updating, maintenance, and replacement of equipment, and to ensure the accuracy of the asset information as third parties add, upgrade, and remove equipment. Substations are being automated using digital technologies and international standards such as IEC 61850, while customer metering is being automated with advanced metering infrastructure technologies.

Distributed Energy Resources (DER) Communications

The increased interconnection to the grid of distributed energy resources (DERs) is causing a paradigm shift in grid structure and operations. Not only are these DERs (both renewable and non-renewable) dispersed throughout the distribution system, they are generally not owned or directly operated by the utilities. These DER are increasingly requiring communications, not necessarily directly with utilities, but often with third parties for management or market purposes. These third parties then provide aggregated or more tailored information on these DER to the utilities. The aggregators typically use the Internet and cellphone networks because these communication networks have been developed and implemented widely, thus reducing technology costs, as well as the costs for finding the appropriate communications expertise. This has made these “information technology (IT)” technologies very attractive for many of the DER communication requirements.

Utilities are finding that DERs can no longer be viewed as “passive negative loads,” but must be integrated as energy resources into power system operations. Renewable DER, which are generally intermittent, widely distributed, and ranging from very small residential DER to multiple megawatts DER plants, are forcing utilities to seek different methods for

maintain grid reliability and resilience. New DER technologies, such as energy storage, electric vehicles, and flexible load are potentially capable of providing grid support services but are still in their infancies in terms of their management.

“IT” and “OT” Cybersecurity in Smart Grid Operations

Smart Grid as Cyber-Physical Systems

As a result of these paradigm shifts in smart energy business drivers and communication technologies, particularly after the recent successful attacks on SCADA systems, there has been a recognition that cybersecurity is critical to meeting these new and evolving requirements. But, these smart grid cybersecurity requirements are both the same and different from typical IT cybersecurity requirements.

In particular, power systems must now be considered as cyber-physical systems. This means they are comprised of “intelligent” systems that are engineered as coordinated networks of physical and “computational” (cyber) components that must work together in a highly orchestrated manner and will result in physical (including electrical) actions. Cyber failures or misoperations can cause unwanted physical results, including electrical outages, equipment damage, and safety concerns.

Cybersecurity for Cyber-Physical Systems: Prevention, Notification, Coping, and Recovery

Despite all attempts to prevent cyber attacks, security will always be breached at some time—there is no perfect security solution. Therefore, it is important not only to try to prevent successful security attacks (whether deliberate or inadvertent), but to take steps to ameliorate the impacts of these successful attacks.

The basic security steps are:

- » Prevention: deterrence and delay
- » Detection of attacks
- » Assessment of attacks
- » Coping with attacks
- » Recovery from attacks

Confluence and Misconceptions of "IT" and "OT" Cybersecurity

IT cybersecurity provides an arsenal of tools for assessing risks, for developing security policies and procedures for organizations, and for deploying security technologies. These are, in general, very useful for protecting operational technology (OT) environments—so long as the special OT requirements and constraints are taken into account. It is this mixture of IT and OT that can be very challenging for smart grid systems.

There are, understandably, given the newness of cybersecurity for the smart energy domain, many misconceptions of what cybersecurity for the smart grid really means. Some of these misconceptions include:

» **Cybersecurity is just protection against hackers and terrorists.**

Actually the most dangerous deliberate attacker is the "disgruntled employee" who knows the system well, has access to sensitive information, and has the time and expertise to design a very effective attack. In addition, the large majority of "attacks" are inadvertent: the result of natural disasters, human mistakes, and equipment failures. But these can also affect the cyber assets needed to operate the power system and can have just as serious consequences as deliberate attacks.

» **Cybersecurity is synonymous with "encryption of data."**

Just encrypting data, although helpful in some instances, does not ensure security. For instance, an attacker can learn a password of a power system operator by pretending to be from the IT department. Or a USB memory stick can introduce malware that provides a "back door" to the SCADA system. Once inside the SCADA system, the attacker can trip off all power system breakers, then wipe out the SCADA computer system.¹ Or a maintenance person can mistakenly turn off a power system application that normally checks for contingencies, thus allowing the power system to potentially become unstable.²

» **Cybersecurity specialists from the IT environment know exactly what is needed for securing the OT environment.**

Although IT cybersecurity experts know a lot about security computer systems, they are generally not familiar with cyber-physical power systems, nor the special constraints and requirements that real-time management of physical assets entail. Power system operations require very different types of cyber protection than traditional IT domains. For instance, if an IT system is under attack, a typical solution is to turn it off. However, in power system operations, control systems can not be turned off since that may actually cause worse problems such as safety dangers and blackouts. In some situations, keeping the power on is more important than following strict cybersecurity rules.

» **Confidentiality is the most important requirement.**

Unlike most corporations where protecting their data from being seen is the most critical requirement, the voltage on a line or the power on a substation bus is not considered sensitive data in most situations. Encrypting data could actually be an obstacle to rapid monitoring and control actions. For OT systems, therefore, confidentiality of data is NOT the most important security requirement for power system operations.

» **Integrity of data is the next most important security requirement.**

The typical IT focus of this requirement is that data is not changed, but this is not the most critical requirement for OT systems, where authentication and authorization are as important as availability for many cyber-physical systems. The data being exchanged must be authenticated as coming from the expected source, must use the correct formatting, must not have been changed, and must only be accessed by authorized entities. Integrity of data is sometimes referred to as establishing "trust," in which entities must be able to trust that the sources of data are who they say they are, while access control must be in place to ensure that only authorized interactions take place. Data validation, system and network monitoring, non-repudiation, and security logs are required to support the even more secure "trust but verify" methodology.

1. Similar to the attack on the Ukrainian power system in 2015

2. One cause of the widespread blackout of Northeastern USA and Canada in 2003.

» **Availability is of least interest since cybersecurity technologies can have limited impact on availability.**

Actually availability of data is usually the most critical “security” requirement for OT systems. Power systems are “just-in-time” systems that involve millisecond responses for some interactions (e.g., protective relaying) and that rely on accurate data received in a timely manner for many other interactions (e.g., SCADA monitoring and control). Availability is often a combination of engineering (providing redundant equipment, designing failover of systems, and designing for peak data volumes) and cyber security (checking for and avoiding denial-of-service situations, such as coping with SYN flood and spoofing attacks).

For these reasons, IT and OT cybersecurity requirements may be similar in some areas but can be quite different in other areas. This is often expressed as IT focuses on “confidentiality, integrity, and availability (CIA),” while OT focuses on “availability, integrity, and confidentiality (AIC).”

ISO/IEC Cybersecurity Standards and Guidelines

The following section discusses the different ISO and IEC cybersecurity standards that address this challenge. ISO and IEC have developed many cybersecurity standards and guidelines, covering both organizational and procedural requirements (what) and technical requirements (how), as well as conformance and certification standards. These are illustrated in figure 1 below.

ISO/IEC 27000 Series (what)

The ISO/IEC 27000 series covers a wide range of cybersecurity requirements. These cybersecurity standards are focused on what cybersecurity policies and procedures should be put in place at the enterprise level.

For the Smart Grid, the most relevant are ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27019. These standards identify the high-level organizational and procedural requirements for cybersecurity, including risk assessment requirements, personnel security processes, and information security. ISO/IEC 27001 is general for all types of organizations, while

ISO/IEC 27002 covers industrial organizations. Additional requirements for energy organizations are included in ISO/IEC 27019. Conformance and certification procedures are also provided.

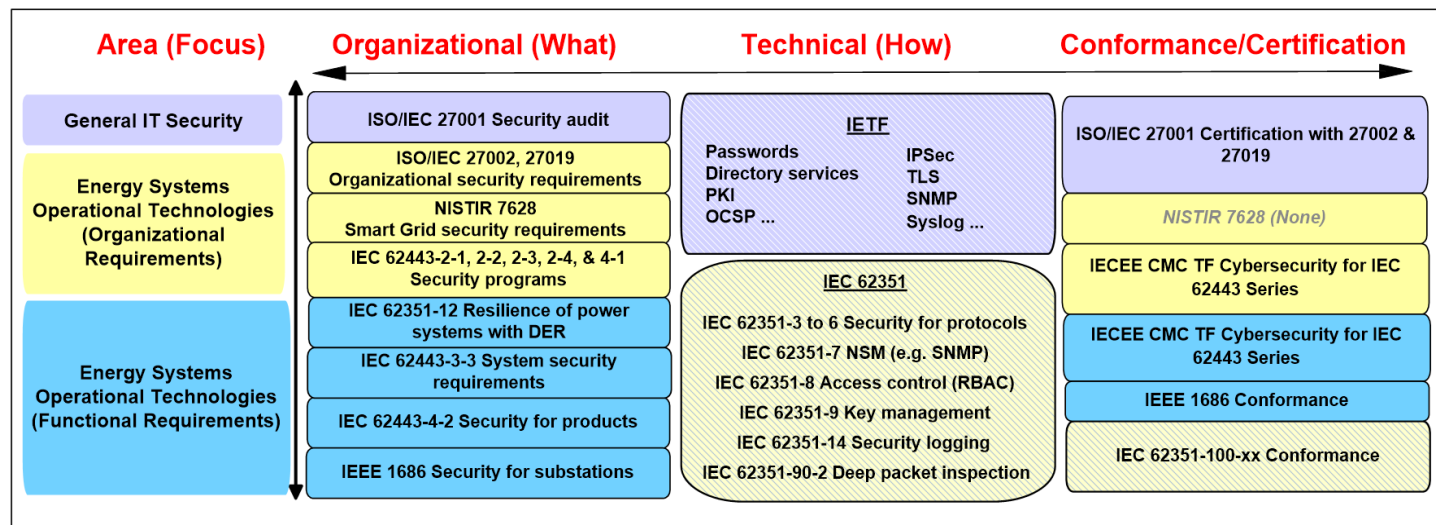
NISTIR 7628 Guidelines for Smart Grid Cybersecurity (what)

The NISTIR 7628 consists of guidelines intended primarily for addressing cybersecurity of smart grid systems and the constituent subsystems of hardware and software components. The NISTIR 7628 guidelines are very similar in scope to the ISO/IEC 27000 standards, except these guidelines focus exclusively on the smart grid sector. It defines approximately 300 high-level security requirements, based on similar security controls in other NIST documents.

IEC 62443 Series for Industrial Automation (what)

The IEC 62443 series for industrial automation was originally developed as the ISA 99 series. It takes the results of risk assessments and translates them into specific security requirements for field operations. Of particular pertinence to the smart grid are the organizational requirements,

Figure 1



IEC 62443-2-1, 2-2, 2-3, 2-4, and 4-1, and the more technical requirements covered in IEC 62443-3-3 and 4-2.

Although focused on industrial automation in general, most of the cybersecurity requirements also apply to the energy sector, and include more details on specific operational and field equipment requirements for cyber-physical systems than the ISO/IEC 27000 series.

NET Cybersecurity Standards (how)

The Internet Engineering Task Force (IETF) is an open standards organization that deals with Internet standards and cooperates with the IEC and the ISO on communication standards. IETF is responsible for the Internet TCP/IP standards and the IP suite, and has defined the associated security standards. These IETF standards can apply to many domains, including the smart grid.

IEC 62351 Series for the SmartGrid (how)

The IEC 62351 series of standards includes cybersecurity technologies for the communication protocols defined by the IEC technical committee (TC) 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. As shown in the diagram below, there is not a one-to-one correlation between the IEC TC57 communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers. Conformance testing for these standards are also part of the series as IEC 62351-100-xx.

Additional IEC 62351 standards cover broader security requirements, such as network and system management, role-based access control, key management, and cybersecurity event logging. Some technical reports address general topics such as deep

packet inspection and resilience of power systems with DERs (see figure 2 below).

Conclusions

Cybersecurity for the smart grid requires well-structured security policies (what), security procedures (what), and security technologies (how). These cybersecurity policies and procedures, based on detailed and thorough risk assessments, must cover not only "protection" against cyber attacks, but also the ability to detect possible attacks, cope with on-going attacks, and recover from those successful attacks. For the smart grid "cyber-physical" systems, authentication, authorization, availability, data integrity, and non-repudiation are more critical than confidentiality for most interactions.


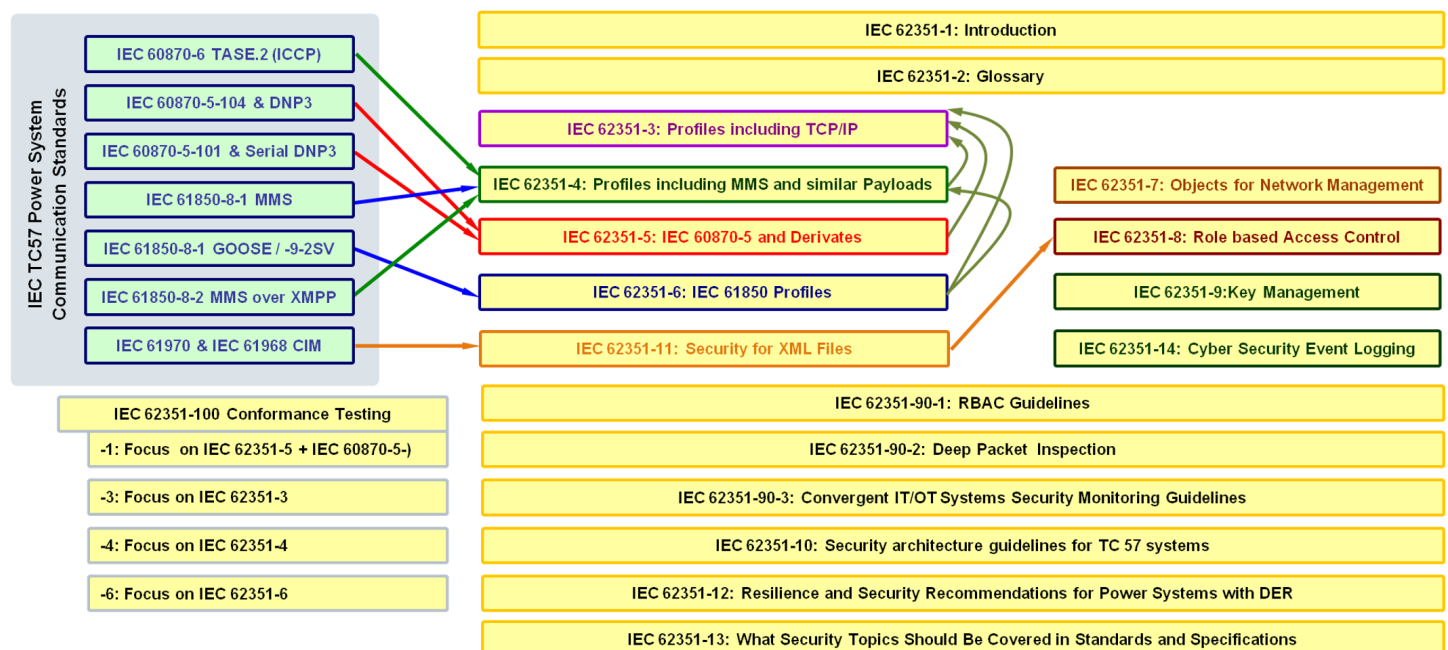
The ISO and IEC cybersecurity standards provide the framework for tackling these very complex security issues for the smart grid. 

Figure 2



Process Sensor Cybersecurity and Safety Is Currently Not Addressed: What It Means to Standards

By Joe Weiss, PE, CISM, CRISC, Applied Control Solutions, LLC



Cybersecurity for commercial, industrial, medical, automotive, and defense applications consist of traditional information technology (IT)

networks and what is referred to as operational technology (OT) networks. The IT networks are addressed by standards such as ANSI/IEC27000 while OT networks are addressed by standards such as ANSI/IEC62443. There is a significant amount of discussion of the differences between IT and OT and how to bridge the gap between the IT and OT organizations. OT is really the networking of control system equipment, not the actual control system equipment. Because OT is really about Ethernet packets, the distinction between IT and OT is blurring.

The Purdue Reference Model Level 0,1 devices (e.g., process sensors, actuators, and drives) are where the real physical processes occur. Level 0,1 communications start before they become Ethernet packets and they can be compromised before they become Ethernet packets. However, most discussions at standards meetings and cyber security conferences are of OT networks with very few, if any, discussions about Level 0,1 devices. What occurs physically before the Ethernet packet creation is where the systems' ground truth is to be found, and it's there that one finds the unaddressed security and safety issues. When discussing safety and security, the security discussions need to start with the Level 0,1 devices before the communications become Ethernet



packets. The need to address Level 0,1 devices is finally being addressed by a new task group within ISA99—ISA99 WG4 TG7—to address whether the existing IEC 62443 standards are adequate to address Level 0,1 devices. The consensus is that existing IEC 62443 standards do not adequately address Level 0,1 devices.

As mentioned, cybersecurity has effectively been confined to Internet Protocol (including Ethernet)-based networks. Process sensors, actuators, and drives have been considered to be engineering systems, so they have not been addressed from a cybersecurity perspective. As an analogy, if you are a doctor, you must be able trust your temperature and blood pressure readings to make a correct diagnosis. The equipment must be well maintained and procedures must be followed


to obtain the correct data need to care for the patient. The same theory applies to process sensors connected to control system networks, and like the doctor example, the results of incomplete or incorrect data could, and has been, disastrous and/or fatal. Yet the existing process sensors, actuators, and drives have no cybersecurity or authentication. Additionally, sensor protocols such as wired and wireless HART, Fieldbus, and Profibus have been demonstrated to be cyber vulnerable. As process sensors are the starting point for all process controls and safety applications, and actuators, motors, and drives are the final elements, the lack of security in these devices affect system security and safety.

There have been more than 1,000 actual control system cyber incidents to date worldwide in electric transmission and distribution; power

plants including fossil, hydro, and nuclear; water/wastewater; pipelines; oil/gas; manufacturing; transportation; building controls; and defense. A number of these incidents were process sensor-related. Impacts have ranged from trivial to equipment damage, to environmental releases, to wide-spread electric outages, to deaths. Most of these incidents were assumed to be unintentional. Because of the lack of ICS cyber forensics at the process-sensor level, it is not possible to determine whether

the incidents were malicious or unintentional. However, the impacts are the same.

The lack of security in Level 0,1 devices affects multiple American National Standards Institute (ANSI)-approved standards including those from ISA, IEEE, API, AICHE, NERC, and ASME, to name a few. There are a limited number of process sensor suppliers, and most are international serving multiple markets. Cybersecurity of process sensors affect standards dealing with alarm and

alerts, intelligent device management, process safety, control valves, drives, wired and wireless sensors, sensor protocols, electric substations, SCADA, DCS, PLCs, intelligent automation including manufacturing and transportation, and predictive maintenance. Process sensors are also the starting point for IOT, IIOT, and Industry4.0. Consequently, the lack of cybersecurity in these sensors impacts numerous standards and requires coordination among numerous international organizations. 

IN MEMORIAM

Samuel "Keel" Kelly

On June 20, a great loss to the standards committee and battery industry befell with the passing of Samuel "Keel" Kelly. Keel was a great professional who contributed so much to the U.S. national and international standards work, both as an individual contributor and work group (WG)/maintenance team (MT) leader. Much more importantly, he was a fine person and a true gentleman.

Keel was a detail oriented contributor to American National Standards Institute (ANSI) and IEC standards development for nearly 40 years. He brought his passion for quality assurance into the realm of battery standards. In the late 1990s, he guided the development of new standalone battery safety standards within ANSI and nurtured their status to new heights during his tenure as Subcommittee Chair of C18-5. As the

long time convener to IEC technical committee (TC) 35 MT16 on the safety of primary aqueous electrolyte batteries, he helped to enhance the global competitiveness of the U.S. battery industry through his standards activities and involvement. Keel appreciated how standards could be used to benefit both industry and consumers.

As a result of Keel's long time commitment and expertise, he received the IEC 1906 Award in 2004, recognizing his exceptional achievements in IEC TC 35 for primary cells and batteries.

Keel was gifted in so many ways. He was a quiet leader, incredibly efficient, and always able to see the workable compromise in almost any situation. This balance of civility, willingness to listen, and maintaining/defending his own position was truly a gift.



Ron Petersen

A longtime stalwart in the IEEE standards development process, Ron Petersen died on July 9, 2018. He was 81. Ron served on various IEEE committees and particularly SCC28, SCC34, and SCC39 (i.e., International Committee on Electromagnetic Safety-ICES) since the 1970s. He has been a dominant figure in this field ever since—so much so that he was named “the Czar of Electromagnetic Energy.” He worked on IEEE standards until his last days distributing upcoming meeting information for the ICES just a few days before his passing.

Ron Petersen received BSEE and MSEP (Electrophysics) degrees from the Polytechnic Institute of Brooklyn. He joined the Bell Labs Solid-State Device Development Laboratory in 1960 where he was involved with the development of low-noise travelling-wave maser amplifiers, broadband solid state amplifiers, and silicon diode array camera tubes. In 1970 he joined the Bell Labs Environmental Health and Safety Center and, until his retirement in 2001, managed the Bell Labs Wireless and Optical Technologies Safety Department (WOTS), which served as the AT&T and Lucent Technologies Inc. resource for all non-ionizing radiation safety issues and related standards.

He chaired IEEE Standards Coordinating Committee 34 (SCC-34) *Product Performance Standards Relative to the Safe use of Electromagnetic Energy*, SCC-28

Safety Standards with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, and most recently served as Executive Secretary/Treasurer of SCC-39, which was formed by merging SCC-28 with SCC-34. He was a member of the IEEE-SA Standards Board for several years and served on and chaired several Standards Board committees. He also chaired IEC Technical Committee 106 *Assessment of Exposure of Humans to Electric, Magnetic and Electromagnetic Fields, 0 to 300 GHz*. He served two six-year terms on the National Council on Radiation Protection and Measurements (NCRP) where he chaired Scientific Committee 89 *Non-Ionizing Radiation* and served as Scientific Vice-President of the Non-Ionizing Radiation Program Area. He also chaired the American National Standards Institute Accredited Standards Committee for the Safe use of Lasers (ANSI/ASC Z136) and chaired ANSI Z136.2 *Safety of Optical Fiber and Free Space Optical Telecommunications Systems*.

Ron received a number of awards including the IEEE SA Standards Medallion, the IEEE-SA International Award, IEEE SA Distinguished Service Award, the American National Standards Institute Finnegan Standards Medal, and the IEC Thomas A Edison Award. He was an IEEE Life Fellow and a Fellow of the Laser Institute of America.



A number of fellow committee members interacted with Ron over the years on the topic of radiofrequency safety through joint participation in meetings and hearings on the subject and collaboration on publications.

Ron's passing represents a great loss for IEEE, and especially for ICES. His constant attention to the workings of the committee and the development of standards documents formed the glue that insured the continued cohesiveness and success of ICES. He was a giant—and will be greatly missed. We will all miss Ron in our meetings. Ron lives forever in our memories.



JOIN US!

USNC INDUSTRY SYMPOSIUM

Protection of Critical Infrastructure through IEC Standards

Topics for discussion will include: **Critical Infrastructure, Cybersecurity, Industrial Control Systems (Manufacturing), Resiliency (Energy), Broadband Access, Transportation (Oil/Gas and Rail)**

WEDNESDAY, SEPTEMBER 12, 2018
NEWSEUM, WASHINGTON D.C.

For more information, please contact the USNC General Secretary, Tony Zertuche, at tzertuche@ansi.org

This roundtable event is designed to bring together some of the top experts and critical players in the fields of standards development and critical infrastructure to highlight the important role standards play in confronting and pre-empting challenges in an increasingly vulnerable sector. The USNC is dedicated to developing international standards that reinforce the cyber resiliency and cybersecurity aspects of critical infrastructure, particularly as it relates to IoT, Smart Manufacturing, and Smart Cities, while continuing to advance and protect U.S. interests in the standards development process. Interested stakeholders will be from business, government, emerging industry, academia, and the non-profit sectors.



A keynote address will be given by:

Jim Shannon, IEC President

Former President and CEO, National Fire Protection Association

Former Member, U.S. House of Representatives



United States
National Committee
of the IEC

NEWS

ISO, IEC, and ITU Publish Comprehensive Monthly Listings of April and May Work Items

In an effort to increase stakeholder engagement and collaboration and reduce duplicative work, the **International Organization for Standardization** (ISO), **International Electrotechnical Commission** (IEC), and **International Telecommunications Union** (ITU) have coordinated publication of a monthly document that lists all new work items from the three organizations, including updates on projects and timelines for the technical committees' work.

As the U.S. member body to ISO and (via the U.S. National Committee) the IEC, the **American National Standards Institute** (ANSI) encourages stakeholders to review the **April and May 2018 listings here**.

Those seeking more information about ISO new work items can visit <http://isotc.iso.org/pp/> (password required). Further details on IEC technical committees and subcommittees are available at <http://www.iec.ch>. See directions for accessing these documents [here](#).

Register for ANSI's Personnel Certification Accreditation Workshop

The **American National Standards Institute** (ANSI) invites all interested stakeholders to register for its two-day Personnel Certification Accreditation Workshop on September 10-11, 2018, from 9 a.m. to 5 p.m. at ANSI headquarters in Washington, D.C.

The workshop is designed to introduce interested stakeholders to the international standard ANSI/ISO/IEC 17024, *General requirements for bodies operating certification schemes for persons*, including revised and new requirements in the latest 2012 edition. Discussions will focus on building an understanding of the standard's requirements, its benefits, and why it has become the benchmark for personnel certification. The sessions are intended for all organizations considering accreditation by ANSI to ISO/IEC 17024, which is an international standard increasingly recognized by the U.S. government, the certification industry, and employers.

» **Register now** for the September course. For more information, visit www.ansi.org/17024

Registrants will participate in presentations, small group discussions, and exercises to get a better understanding of what ANSI expects organizations to provide as demonstration of compliance to each of the requirements. In addition, attendees will be able to self-assess their own operations, and identify areas needing improvement prior to applying for ANSI accreditation.

Relevant stakeholders include:

- » Personnel from corporations, organizations, government agencies, and others that operate certification programs, and that want to learn more about how accreditation can add value to their programs
- » Organizations that are considering developing a personnel certification programs
- » Organizations that are considering whether or not to pursue ANSI accreditation and want to understand the benefits and uses of accreditation
- » Organizations going through the ANSI accreditation process
- » Organizations that are currently accredited
- » Organizations that support certification programs through testing, marketing, IT, and other services

For more information on eligibility, class scheduling, or to register, click [here](#) or contact Dr. Vijay Krishna, ANSI director of personnel certification accreditation, at vkrishna@ansi.org.

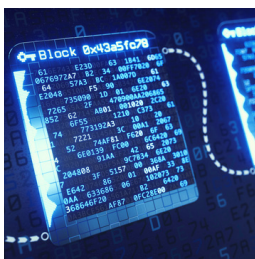
DOCUMENTS OF INTEREST



Women in a man's world

Women inventors and their influence on today's technologies

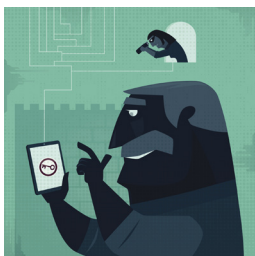
Women's contributions to science, technology, engineering, and mathematics (STEM) have often been overlooked and left out of history books. When asked to name inventors, people tend to cite Thomas Edison, Graham Bell, Benjamin Franklin, or Albert Einstein.... [Read more at IEC...](#)



Building blocks for cybersecurity

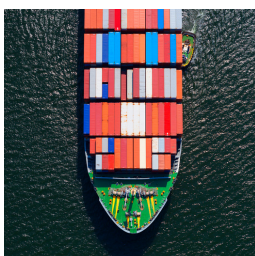
Blockchain opens up new possibilities for data protection

As we move towards more connected environments, cyber security threats are increasing. One technology that could help with data protection is blockchain, which is also starting to be used in some renewable energy projects..... [Read more at IEC...](#)



Why cybersecurity and privacy rely on international standards

Standards are essential for human civilization. Standards enable the global interoperability of technical solutions while ensuring that the technical progress can be applied smoothly..... [Read more on the IEC blog...](#)



Cyber pirates on the high seas

According to a new study commissioned by Inmarsat, the maritime industry has one of the most favourable attitudes towards the adoption of analytic, management and operational tools based on the internet of things (IoT). The report, to be published on 26 June and based on 750 interviews, provides a detailed account of attitudes towards IoT and digitalization... [Read more on the IEC blog...](#)

UPCOMING EVENTS

Sep
10-14

CAPCC/TMC/Council
Arlington, VA

Oct
10-12

FINCA Meetings
Mexico City, Mexico

Sep
12

Industry Event: Standards and the
Protection of Critical Infrastructure
Washington, DC

Oct
22-26

82nd IEC General Meeting
Busan, Republic of Korea

Save the date!

IEC 2022 General Meeting, Host City: San Francisco

Sponsor the IEC 2022 General Meeting, hosted by the USNC

For only the seventh time since 1904, the United States is gearing up to host the IEC General Meeting, 31 October – 4 November, 2022, in San Francisco. Organizations with a stake in all areas of electrotechnology are invited to demonstrate their commitment to international standardization and conformity assessment through sponsorship of the ten-day event.

For more information, see the [IEC 2022 Sponsorship Brochure](#) or contact Kendal Szulowski-Francis at: ksfrancis@ansi.org or 212-642-4965.



Thank you to the organizations already on board as IEC 2022 sponsors!





Looking for standards? Check out ANSI's webstore!

ANSI webstore purchases and standards subscriptions support USNC activities.

webstore.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/IEC nor of ANSI.

HOW TO CONTRIBUTE

Contributions are gladly accepted for review and possible publication, subject to revision by the editors. Submit proposed news items to:
Kendall Szulewski-Francis,

ksfrancis@ansi.org

UPCOMING ISSUES

Q III: Stakeholder Involvement

Q IV: Regional Partnerships (FINCA, COPANT, APCF, PASC, etc.)