The TIC Council Supports a robust Cybersecurity Framework for Industrial Control Systems

A robust framework will provide beneficial policies to ensure the continued reliable operation of industrial systems.

The TIC Council supports the incorporation of IEC 62443 cyber security standards and associated assessment and compliance program, or parts thereof, into a framework for Industrial Control System (ICS) cyber security programs. The IEC 62443 standard is globally recognized and provides a robust application to ICS that aligns with of the NIST National Framework for Improving Critical Infrastructure Cyber security 1.1.

Industrial control systems have historically been stand-alone systems, disconnected from other IT infrastructure. However, with the proliferation of the Internet of Things (IoT) functional devices, ICSs have increasingly been incorporated into integrated managed systems. Making them vulnerable to cybersecurity threats and possibly impact critical safety functions.

Cyberattacks of Industrial Control Systems are especially damaging to industry and government due to the critical role played in maintaining key systems. Cyber intrusions and attacks on such systems have the potential to result in lost revenue, seized data, disruptions in the supply chain, harm living beings or the environment, and more. Successful intrusions and attacks eventually trickle down to consumers slowing or disrupting our economy and further reducing public confidence.

While use of the NIST National Framework for Improving Critical Infrastructure Cyber security 1.1 is critical in ensuring the security of federally managed ICS applications, the incorporation of IEC 62443 standards into an overall, risk-based Cybersecurity Framework and compliance program for Industrial Control System (ICS) would help ensure global cyber security adoption for ICSs used by industries around the world.

This framework, supported by conformity assessment, is a reasonable and responsible model for addressing the challenges of providing and improving cyber security resilience throughout the product and production system lifecycle. Trusted independent third-party conformity assessment is a cost-effective policy solution as it provides the highest level of confidence and helps government leverage private-sector resources. The IEC 62443 standards compliance program may be adopted by these trusted third-party assessors, for immediate action, ensuring a continuous and congruent approach to cybersecurity in this area. For highly decentralized systems, e.g., in railway systems, additional requirements beyond IEC 62443 may apply.

Additionally, the TIC Council would appreciate the availability of a risk classification guidance for manufacturers.

Contact person: Karin Athanas, kathanas@tic-council.org

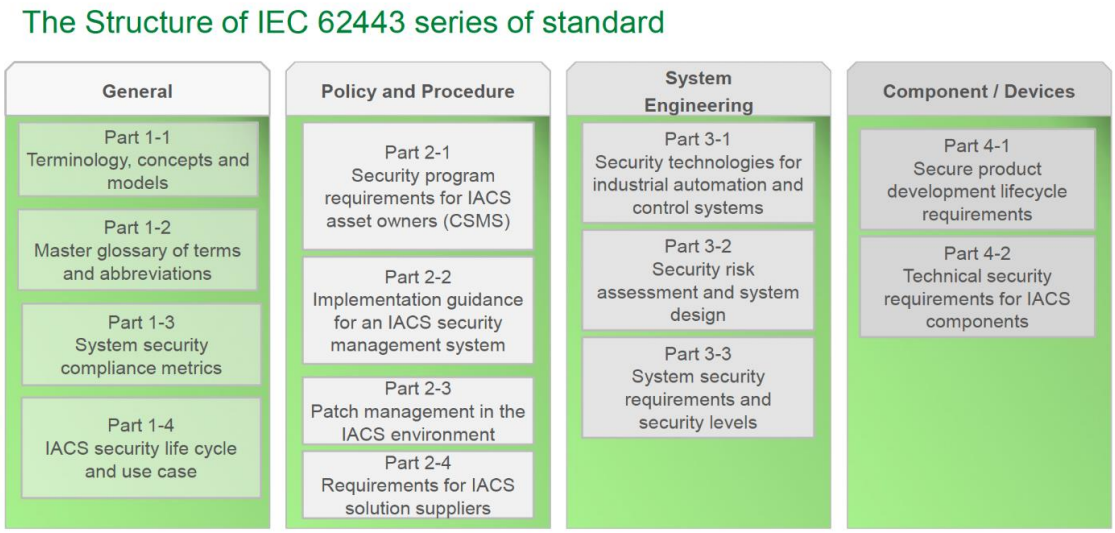
TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification and verification organizations. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion

Appenix 1 – Overview of IEC 62443 and ICS applications

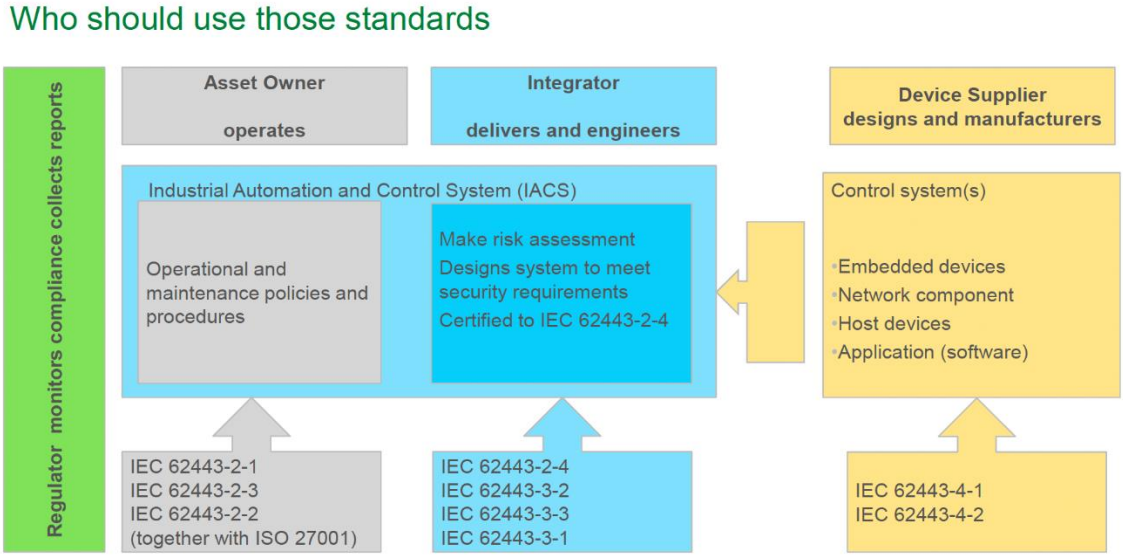
Adoption of IEC 62443 cyber security standards, or parts thereof, into a framework for ICS Cyber Security regulations United States.

The presidential Executive Order 13800 from May 2017 (amending executive order 13636 Feb. 2013) calls for strengthening the cyber security of Federal Networks and Critical Infrastructure. While the second version of the NIST National Framework for Improving Critical Infrastructure Cyber security 1.1, which has been release on April 2018, maps security requirements to various available national and international standards (incl. e.g., IEC 62443).

The concept of the 62443 standards consider Process Management, People Management and Technology Management. It is structured in a series that begin with a general certification and advances though a structured process of more advanced certificates of cyber security.



The industry can easily adopt the IEC 62443 standards along with ISO 27001, to help define and certify processes throughout our cyber development and market entry process.



The IECEE System, is the right passport to facilitate trade as it has been adopted globally. The IEC has 60 full members and 23 associate members. IEC runs an affiliate country program for newly industrializing countries around the world today where they have 87 countries participating in IEC affiliate country program and 170 countries accepting reports on the basis of IEC standards. The IECEE is the IEC conformity assessment program for those countries wishing to have a national certification and could be a great springboard for USA cyber security standards.

OD 2061 is a standardized assessment service intended to provide a framework for assessments in accordance with the IEC 62443 Security for industrial automation and control systems series of standards resulting in an IECEE Certificate of Conformity. The IEC 62443 series of standards specify requirements for security capabilities. As mentioned earlier, these capabilities may be technical capabilities (security mechanisms) or process capabilities (human procedures). The IECEE Industrial Cyber Security Program is operated following the same basic rules of the CB Scheme as specified in IECEE 02 Part I and its related Operational Documents (ODs) and Administrative Documents (ADs) with the following additional considerations. Test Results relate to the assessment of supporting evidence for security capabilities required by IEC 62443 and the application of those capabilities.

In a breakout session we can delve deeper in to the 62443 standards and assessments currently implemented, as well as the scope of the ODs e.g., OD 2061 and OD 2037.

There is a correlation of the adopted European Union “EU” regulation EU 2019/881, commonly called the Cyber Security Act and the need for the items below:

- Establishing an EU cybersecurity certification framework for information and communication technology (ICT) products, services, and processes
- Defining elements of European cybersecurity certification schemes
- Defining conformity assessment bodies
- Defining assurance levels for EU certification schemes, e.g., basic, substantial, and high
- Defining security objectives for certification schemes

The European directive calls for operators of essential services to deliver appropriate technical and organizational security measures preventing and minimizing the impact of incidents affecting the security of the network and information systems used for delivering the essential services.

Along these lines the United States reported the adoption of the “Internet of Things Cybersecurity Improvement Act of 2020”. While the act directly focuses on US governmental agencies and the suppliers to these agencies, it is expected that this law may have a far-reaching impact to the IoT industry since many products that are used by governmental agencies will have a shared purpose and be used by consumers, other industry/ public sectors alike. For example, the same connected thermostat that may be deployed by a government agency is likely to be used in commercial buildings and possibly in private homes.

For additional clarification, IoT devices are defined as devices which have at least one transducer (sensor or actuator) for interacting directly with the physical world; have at least one network interface and can function on their own and are not only able to function when acting as a component of another device, such as a processor. (This is assuming conventional Information Technology devices, such as smartphones and laptops are excluded). As the security of a systems often depends on the weakest part, the TIC Council would be in favor of including such devices in the scope of the legislation.

Along with the law, NIST has already published draft guidance documents, for the United States federal government and manufacturers supplying IoT device for US government entities/ agencies. The NIST documents itself are not deemed regulatory but describe the minimum-security capabilities an IoT device may deliver, so it may be integrated into federal information systems. These same NIST draft guidance documents provide information on the minimum non-technical capabilities a manufacturer should deliver in support and during the manufacturing of the product.

As a reference, the draft NIST documents are published as SP-800-213, NISTIR 8259B, NISTR 8259C and NISTIR 8259D. The referenced NIST documents complement the already earlier published NISTIR 8259 and NISTIR 8259A – IoT Device Cybersecurity Capability – Core Baseline.

Security Objectives

It is important to understand the security objectives of the regulations. The EU Cybersecurity Act specifies a more comprehensive list of objectives for EU certification schemes; however, the following is a subset of the list of objectives which may be considered important to the adoption for a set of security standards.

a) to protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;
b) to protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
c) that authorized persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
d) to identify and document known dependencies and vulnerabilities;
e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
i) that ICT products, ICT services and ICT processes are secure by default and by design;
j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.

And in comparison; the recently passed US Bill H.R. 1668 identifies, as most relevant security objectives. This is to help provide guidance to obtain the obligation for vulnerability disclosure and resolutions of governmental agency suppliers/ contractors. The items below reference NISTIR recommendations 8259.

a) Secure development
b) Identity management
c) Patching
d) Configuration management

Compliance

The EU Cybersecurity Act currently defines conformity assessment for three levels of assurance.

1) Basic - Basic assurance level shall provide assurance that the ICT products, ICT services, and ICT processes meet minimum security requirements, including security functionalities, and that they have been evaluated at a level intended to minimize the known basic risks of incidents and cyberattacks. The conformity assessment carried out shall include at least a review of technical documentation.

   While Basic is not further elaborated we assume "basic assurance" to be equivalent to casual and coincidental respectively lax application of security. A good example is the home router. Newer home routers have improved in security by requiring a new password while setting up. Most of the home routers sold up until 2018 did have preconfigured usernames "admin" and password "admin" which many consumers did not bother to change, possibly creating a security vulnerability.

2) Substantial - Substantial assurance level shall provide assurance that the ICT products, ICT services, and ICT processes meet security requirements, including security functionalities, and that they have been evaluated at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.

3) High - High assurance level shall provide assurance that the ICT products, ICT services and ICT processes meet security requirements, including security functionalities, and that they have been evaluated at a level intended to minimize the risk of state-of the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing.

As an added comment to Basic compliance mentioned, the EU Cybersecurity Act does foresee self-assessment for ICT products, ICT services and ICT processes,

which may present a low risk of vulnerability, corresponding to assurance level Basic.

Mapping security objectives to IEC 62443 requirements

The following table provides a mapping of the security objectives of the EU cyber security act and the recently published US IoT Cyber Security Improvement Act. The mapping shows that all security objectives are appropriately addressed by IEC 62443 by either the secure product development standard IEC 62443-4-1 and or by the product security requirement standard IEC 62443-4-2.

Security Objective EU Cybersecurity act	**IoT Cybersecurity Improvement Act and NISTIR 8259A**	**IEC 62443-4-1**	**IEC 62443-4-2**
	Secure development	All requirements	
	Identity management		CR 1.4
	Patching	Practice 7 – Security update management	
	Configuration management		CR 7.6
Protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing, access or disclosure during the entire life cycle	Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification		CR.4.1, 4.2, 4.3
Protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire life cycle	Logical access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only		CR 1.1, CR 1.2, CR 1.5, CR 1.7, CR 1.11, CR 2.1, CR 2.2, CR 2.13, CR 7.7
Authorized persons, programs or machines are able only to access the data, services or functions to which their access rights refer	Device Identification: The IoT device can be uniquely identified logically and physically		CR 1.1, CR 1.2
Identify and document known dependencies and vulnerabilities		Practice 1 – Security management SM-11, Practice 6 – Management security related issues	
Record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom	Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only		CR 2.8, CR 2.12
Make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom	Logical access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only		CR 2.8, CR 2.9, CR 2.10, CR 2.11, CR 2.12

Verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities		Practices 5 Security validation and verification testing SVV-1 to SVV-5	
Restore the availability and access to data, services, and functions in a timely manner in the event of a physical or technical incident	Device Configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only		CR 7.4, CR 7.6
Provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates	Software Update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	Practice 7 Security update management SUM 1 to SUM 5 Practices 5 Security validation and verification testing SVV-1 to SVV-5	CR 3.4, CR 3.10
CR x.x indicate the component requirement as per IEC 62443-4-2			

In Summary using IEC 62443 standards for addressing the recent regulatory requirements allows products to be designed and manufactured with global market access in mind. The largest global conformity assessment scheme – the IECEE CB scheme – operates the IEC 62443 cyber security certification program, to test and certify cyber security of electrotechnical products and systems in the electrotechnical sphere, based on applicable IEC Standards. The program can be applied to any sector with operational technology, including medical and automotive.

The IECCE CB scheme is based on mutual recognition of test results to obtain certification or approval at national levels around the world. What this means is; one test, one certification, recognized internationally. The number of certified companies and products has significantly increased in 2020.

TIC Council members were some of the first IECEE recognized testing labs (CBTL) and certification bodies (CB) for IEC 62443.
Sources:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
https://eur-lex.europa.eu/eli/reg/2019/881/oj
https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity
https://www.congress.gov/bill/116th-congress/house-bill/1668
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327