



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

## WHY WE'RE HERE: THE EVERYDAY IMPACTS OF OUR WORK



### FEATURED STORIES



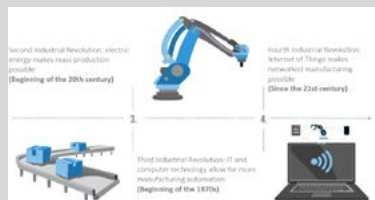
Using Standards to Help Ensure Product Safety



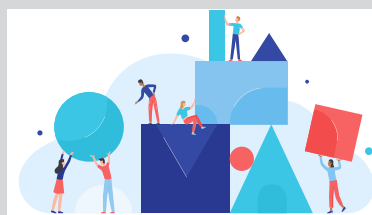
Why Standards? Outcomes Matter



Cybersecurity Standards and Guidelines to Assist Small and Medium-Sized Manufacturers



Leveraging Standards for Manufacturing Digital Transformation



Strategic Standardization



USNC Launches New Professional Mentoring Program

### IN THIS ISSUE

**3** Decision Depot

**15** Call for Action and Participation

## Using Standards to Help Ensure Product Safety: Testing and Certification Insights

By: Joan Sterling, Vice President, Public and Government Affairs, Intertek and USNC VP-Conformity Assessment



Ensuring the overall safety of electrical products, keeping people and property safe and secure are critical. These are the very reason standards exist. Once standard

development organizations (SDOs) draft requirements and guidelines for product safety and performance, they often become requirements for the industry. Additionally, manufacturers may voluntarily elect to have products assessed to standards that are not legally required.

Whether mandatory or voluntary, standards—and the assessments they include—form the root of the testing and certification process. When considering the implications of product standards, it is important to understand how products and equipment are tested and certified, as well as how this process can impact getting products to market.

### Approved Labs

In the United States, testing and certification for products used in the workplace is done by accredited, independent third-party testing organizations called Nationally Recognized Testing Laboratories (NRTLs). The Occupational Safety and Health Administration (OSHA) approves NRTLs to evaluate, test, and certify electrically operated or gas- and oil-fired products. Labs conducting testing must be accredited under ISO/IEC 17025, whereas certification bodies (CBs) are accredited to ISO/IEC 17065. If an agency functions as both a testing lab and certification body, as



required of NRTLs, it must have both accreditations.

### Testing

Testing may be a measure of a product, used for purposes such as R&D, benchmarking, or assuring quality, performance, or general safety. It can also be used as a precursor to product certification. Regardless of the outcome of the testing, the process always begins with a standard. Standards provide requirements specific to the product, including conditions, guidelines, and/or characteristics that will help ensure products are appropriate and safe for their intended use and the setting where they will be operated. Because they play such an important role in testing and subsequently getting products to market, it is important to know and understand the standards

and their requirements before the testing process begins.

To begin the process, the testing lab identifies applicable standard(s), prepares a test plan, and then conducts the safety and performance testing and assessments outlined in the standard(s). Typically, manufacturers provide the lab with samples representative of normal product or component manufacture—those that use the materials, composition, and processes that will be used when manufacturing the product in the future. It is understood that the product will continue to be manufactured in the same manner as these samples, thus meeting—or failing—the standard, just as the samples did.

The lab evaluates the provided samples to the required standard(s), assessing things like overall safety, function, performance, and/or

adherence to codes such as the National Electric Code. Following these evaluations, the lab produces a test report outlining testing methods, data, and findings. The more specific the information, the better. Given these contents, the test report illustrates compliance or non-compliance to standards. Next steps will depend on the type of product and the assessments being made.

While the testing process is closely associated with certification, not all products require certification and not all standards result in certification as their endpoint. In cases where certification is not required, the testing report is the final deliverable in the process and products can then be placed on the market. For products requiring certification however, testing is simply the first step. The next step is undergoing the certification process.


## Certification

Certification is an independent third party's attestation of a product's compliance with a safety standard that is generally necessary for market entry.

Certification demonstrates compliance to a safety standard required for market entry. The National Electrical Code (NEC) mandates certification (listing, in NFPA parlance) of electrical wiring and many types of equipment. Certified products bear a certification mark from an accredited certification body. Certification marks demonstrate that product samples have been appropriately evaluated and found to meet applicable certification requirements. Some of the more common safety marks used on electrical products in North America include ETL, CSA, FM, and UL.

Upon completion of testing, all data and quality documents are compiled and sent for technical review. A certification review follows a satisfactory technical review. Finally, there will be a mark/label review. When all three levels of review are finished, most CBs will issue certification and list the product in a relevant directory. Follow-up inspections and certification maintenance will continue throughout the product's certification lifecycle.

Manufacturers can then apply to mark to the product, packaging and/or product manuals, following marking guidance from the CB. It is important to note that a listing mark indicates a product complied with applicable standards at the time it left the manufacturing location. Any changes, alterations or reconditioning will invalidate the certification. Equipment that has been modified or changed after leaving the factory should be evaluated and certified by a third-party.

Some manufacturers may consider testing and certification a hurdle to overcome before going to market; others consider it an important way to reduce risk of liability or to illustrate compliance. But for many parties, including inspectors, distributors, retailers and end users, certification provides peace of mind. It all starts with standards, but it ends with products whose safety, quality, and performance are better assured, benefitting the manufacturer, consumers, and everyone in between. 

## 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 the decision at SMB 7260 and CB 1173 held virtually on February 22-23, 2021 and January 27, 2021 respectively.

[SMB/7260/DL](#)

[CB/1173/DL](#)

## Why Standards? Outcomes Matter

by Joe Musso, Standards Program Manager, Underwriters Laboratories & USNC TMC Member and TAG Secretary, IEC/TC 72; and Grace Roh, International Standards Specialist, Underwriters Laboratories & USNC Communications Committee Member and TAG Assistant Secretary, IEC/TC 61, IEC/TC 108



Consumers depend on a number of products throughout the day, from the phone alarms they use to wake up and the electric toothbrushes they use to get ready, to the coffee makers that provide them with much-needed caffeine and the myriad of other products they use for daily tasks. One may venture to guess that most consumers do not give much thought as to whether these products could pose any threat to the safety of their families. It's possible that the average consumer is even more unaware of the thousands of standards professionals across the United States—and the world—who work in different capacities to promote the safety of products with designs that help to guard against injury.

Standards are an unsung hero, setting requirements that help to protect consumers, largely without their knowledge. Ask the average consumer why a gas oven stove knob must first be pushed in and then turned in order to start the flame on the stovetop. Few may realize that the design is a safety measure and not part of the mechanics required to turn the stovetop on.

One of the most commonly used items in the kitchen is the microwave oven. \$345.3 million U.S. dollars of retail microwave ovens were sold



in the U.S. in 2019 alone.<sup>1</sup> When baby-proofing a household, parents typically do not include the microwave on the list of items to safeguard against, as they do with outlet plugs. These appliances, however, can present a serious danger to small children—one which standards professionals have been working to mitigate.

### Working Behind the Scenes

Imagine a busy family with a young toddler. The family comes home after running some errands and plans to reheat last night's dinner of chicken noodle soup. Upon hearing the microwave tone alerting the family

that the soup has been reheated, the anxious and hungry toddler opens the door. The child is completely unaware that removing the bowl—something he has seen his parents do many times before—actually requires careful thought. Before a parent can get to the microwave, the child has already opened the door and pulled out the steaming bowl of soup. Accidents of this nature can happen in the blink of an eye. Standards provide a way to not only bolster product safety, they also help to guard the users of the product from accidents.

Unfortunately, the above microwave example is a reality, and a common cause of burn injury to young children. Underwriters Laboratories was approached by a team of pediatric doctors and burn specialists who had seen these injuries first-hand and were passionate about doing something

<sup>1</sup> Retail sales of microwave cookware in the United States from 2019 to 2019 (in million U.S. dollars)\*," Statista, accessed February 10, 2021

<https://www.statista.com/statistics/515137/us-retail-sales-of-microwave-cookware/>

to help prevent them. This group of medical professionals compiled data to support what they were seeing in their burn units, and also shared heart-breaking anecdotal stories that put faces to the statistics. But even with all this information in front of them, they were still unsure about how to address the problem.

The team had worked with various consumer safety organizations, including Kids in Danger and the Consumer Product Safety Commission (CPSC), which eventually helped guide them toward the Safety Standard for Microwave Cooking Appliances, UL 923. Once they became educated about standards development, and specifically how they could engage directly in the process to influence the requirements, they began to see a path toward a potential solution.

The previous efforts of this team of doctors, including their research on potential technical solutions, led to a proposal to revise UL 923. The original proposal did not reach consensus with the standards committee and resulted in additional work to refine the proposed changes to the standard. The additional work required a partnership, or working group, between the team of doctors, data and human factors specialists, key industry members and technical staff. This work was led by the Association of Home Appliance Manufacturers (AHAM), who eventually submitted the refined proposal on behalf of the working group. The second proposal successfully achieved consensus and the new requirements were published in UL 923 in 2018.

The new requirements consist of a dual approach. First, to open the microwave oven door, two distinct actions will be required. This approach is consistent with product standards

applicable to other consumer products, including hot water dispensers, battery compartments, heating appliances, highchairs and cribs, which require dual-action mechanisms to reduce potential hazards to children. The second approach is to require an on-product label that warns against young children using the microwaves and calls out the potential hazard of burns from heated contents. The use and care instructions for these products will also be updated to align with this warning label wording.


### Why We Do It

If there is a lack of understanding by the general public on the work of standards, it should not be interpreted as a correlation to the importance of standards development. Rather, one can make the case that this lack of understanding is actually because standards work so well in ensuring safety, allowing the average consumer to go about their day unaware of how much could go wrong with the very phone, electric toothbrush, coffee machine, or microwave oven that they use routinely. Basically, if standards are effective in mitigating hazards, they are doing their job—no news is good news!

In this particular case, young children and their families might actually feel the impact. Parents may not have realized the need for the two simultaneous but dissimilar actions that will be required on microwave oven doors, but the standard can help them rest assured, knowing that their young children will be hindered from opening microwaves and removing hot items without their knowledge. Medical workers may likewise see a reduction in cases of scalding, which will allow them to focus on other medical cases. Producers of these

products might also find confidence that their products will not mistakenly cause harm.

Standards workers share a common experience in explaining to others what it is that we do. Even then, we are a community that understands the amount of work it takes to write and revise standards. It is easy to look at a standard document, count the votes and consider the comments submitted, but we should remember that the lives and well-being of those impacted by our work are our families, our friends and our communities. Standards have real implications on the lives of consumers. Standards can help protect the most vulnerable among us. As technology evolves and we are more informed on accidents and injuries, it is crucial that our standards are living documents that get revised and updated.

Many will never understand or fully appreciate the work we do. Our reward is not in the acknowledgment, but quite possibly in the affirmation that people continue to enjoy their lives using products throughout the day without a second thought to their safety. Standards outcomes matter—it is WHY we do what we do. 

## Cybersecurity Standards and Guidelines to Assist Small and Medium-Sized Manufacturers

by Timothy Zimmerman, CheeYee Tang, Michael Pease, National Institute of Standards and Technology (NIST) and Keith Stouffer, NIST and TAG Member, IEC/TC 65



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, isolated collections of hardware and software. With no external network connections, security focus was primarily on physical threats to the equipment rather than network or cyber threats. Today, network connectivity, commercial software applications, Internet-enabled devices including Internet of Things (IoT), Industrial IoT (IIoT), and other information technology (IT) are being integrated into many ICS to allow operations data to support real-time business decisions. While this connectivity has delivered many benefits, it also increases the vulnerability of these systems to malicious attacks and other cyber threats.

Cybersecurity standards establish controls to protect the confidentiality, integrity, and availability for data and systems. Many IT cybersecurity standards were established with an emphasis on data confidentiality and privacy. However, ICS, especially those considered critical infrastructure, must maintain a higher level of data and system integrity, availability, and operational resilience for many reasons including economic, environmental, human safety, and national security.

For many ICS, it is unacceptable to degrade performance even for the sake of security. As a result, many organizations such as small and medium-size manufacturers (SMMs) may have difficulty with understanding how to implement cybersecurity standards in ICS environments. A concern of many SMMs is that cybersecurity implementations could have a negative impact on the operation of their manufacturing systems.

The National Institute of Standards and Technology (NIST) has recently released two publications to assist SMMs with developing and deploying cybersecurity programs for their manufacturing systems, NISTIR 8183 Rev. 1, *Cybersecurity Framework Version 1.1 Manufacturing Profile* and NISTIR 8183A (3 volumes), *Cybersecurity Framework*

*Manufacturing Profile Low Impact Level Example Implementations Guide*.

### **NISTIR 8183 Rev. 1, Cybersecurity Framework Version 1.1 Manufacturing Profile**

NISTIR 8183 Rev. 1 provides a manufacturing implementation, or Profile, of the Cybersecurity Framework (CSF) Version 1.1, to help manufacturers reduce cybersecurity risks while maintaining alignment with manufacturing sector goals and industry best practices. The Profile incorporates several informative references including ISA/IEC 62443, Industrial Automation and Control Systems (IACS) Security, NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, and Control Objectives for Information and Related Technologies (COBIT) 5.

The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. It is meant to enhance, not replace, current cybersecurity standards and industry guidelines that the manufacturer is following. The Profile provides customized CSF subcategory language relevant to the manufacturing domain with a focus on desired cybersecurity outcomes and can be used to identify opportunities for improving the current cybersecurity posture of a manufacturing system.

NISTIR 8183A (3 volumes), *Cybersecurity Framework Manufacturing Profile Low Impact*

## Level Example Implementations Guide (Volume 1, Volume 2, Volume 3)

The 730-page, 3-Volume NISTIR 8183A is the first detailed cybersecurity implementation guide to be developed specifically for manufacturers. The Implementation Guide drives the CSF Manufacturing Profile to practice and enables manufacturers to efficiently select and deploy cybersecurity tools and techniques that best fit their needs. Making cybersecurity no longer a “black art,” the Implementation Guide assures manufacturers that impacts on demanding system operational performance, reliability, and safety requirements of manufacturing systems will not outweigh the great benefits of more secure systems.

Volume 1 provides manufacturers with a process to determine the appropriate level of cybersecurity required for their company. Volumes 2 and 3 consist of 44 cybersecurity product installation and configuration examples for process control manufacturing environments and discrete manufacturing environments. These easy-to-understand, step-by-step example solutions help users easily follow the examples relevant to their operations and demonstrate how available open-source and commercial off-the-shelf cybersecurity products can be deployed to secure manufacturing environments.

The examples provided in the Implementation Guide detail over 80 measured network, device, and operational performance impacts observed after each installation in the [NIST ICS Cybersecurity Testbed](#). Over 125 GB of publicly-available performance impact measurement data support these findings. This benchmark data allows manufacturers to know what to expect when they select cybersecurity solutions, then allows them to minimize any potential performance impacts on the operation



of the manufacturing system when deploying those cybersecurity tools and techniques.

The intent of the Implementation Guide is to provide example implementations and is not intended as a one-size-fits-all approach. Each individual manufacturer must make their own determinations regarding the cybersecurity solutions they implement. Some important factors to consider include the size of the company, cybersecurity expertise, risk tolerance, the threat landscape, and technologies used in their manufacturing processes.

Along with the two publications discussed, NIST has several other resources to assist SMMs with developing and deploying cybersecurity programs for their manufacturing systems.

### **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.


### **NIST's National Cybersecurity Center of Excellence (NCCoE)**

NCCoE cybersecurity experts are working with manufacturing sector stakeholders and technology vendors to develop practical example solutions to some of the sector's most pressing cybersecurity challenges.

### **The NIST Manufacturing Extension Partnership (MEP)**

MEP is a public-private partnership with Centers in all 50 states and Puerto Rico dedicated to enhancing the productivity and technological performance of U.S. manufacturing.

### **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 the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose. 

## Leveraging Standards for Manufacturing Digital Transformation

by Jacob Chapman, Grantek Systems Integration and TAG Member, IEC/TC 65



### Introduction

Manufacturers today are in the grips of the Fourth Industrial Revolution, adopting technologies to improve real-time

visibility and optimization of their business. Digital Transformation is a very challenging pursuit, and many organizations struggle not only with technology, but also how to affect change within the organization, justify the costs, and maintain momentum against a shared vision. Technical standards play a critical role in that effort.

### The Challenge Manufacturers Face

Industrial manufacturing today is not what it was 20 years ago, and systems at that time were very different from 40 years ago. For example, the 1970s marked the start of Third Industrial Revolution, when IT computer technology allowed for automating complex systems, and manufacturers raced to adopt the

technology in order to speed up their manufacturing processes, increase their output, reduce their prices and maintain their competitive edge. But it only took a few decades to transition from the third Industrial Revolution to the fourth, which indicated a record-breaking pace for manufacturing innovations globally. As we've seen in many areas of our daily lives, the introduction of computer technology has changed the rules of the manufacturing game so rapidly, it's hard to keep track of what the rules are at any given time.

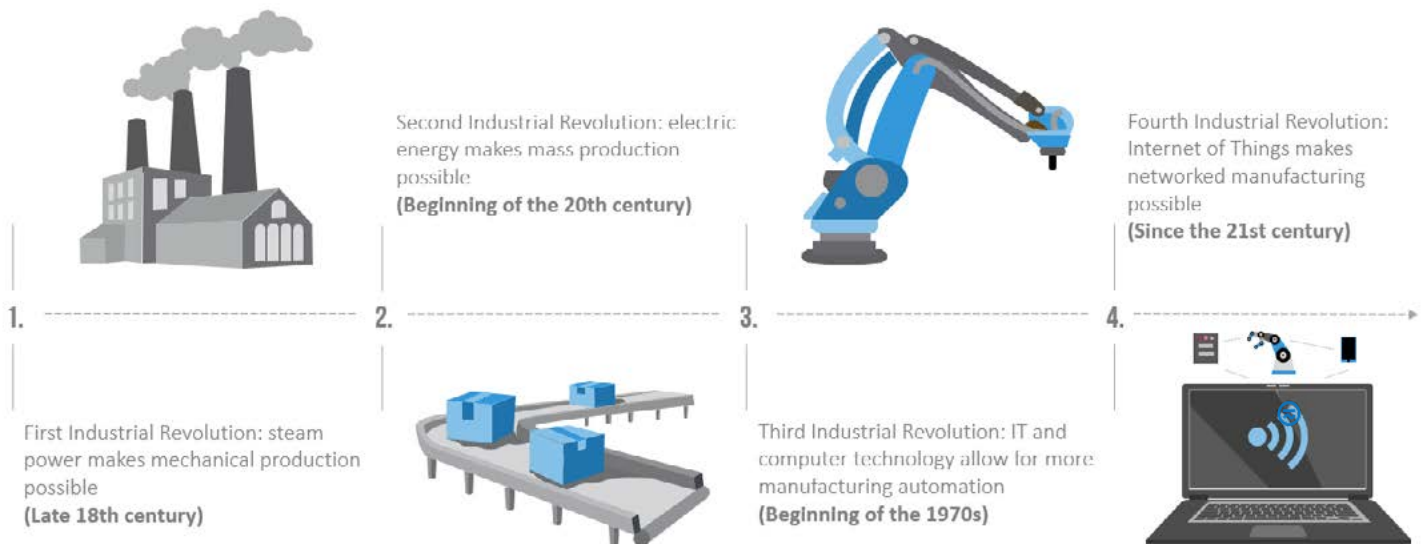
To win the game 20 years ago, a manufacturer needed to increase output and efficiency through automation. But now that's just a basic requirement to play. Since the 21<sup>st</sup> century the name of the game has become real-time optimization throughout the entire supply chain by having systems that report real-time logistics and production data to business-level systems in order for the business to make strategic and operational decisions based on

real-time conditions. These systems come in the form of OEE, SPC, MES, Sensor-to-Cloud (IoT), and other systems. That is what the fourth Industrial Revolution is about, that is what Digital Transformation describes, and it's the biggest challenge that manufacturers face today.

### Connectivity Limits Progress

Acatech—a working academy based in Germany which provides information and advice to politicians and the public on technical subjects—developed and published a study in 2017 titled Industrie 4.0 Maturity Index which received attention globally and has most recently been updated with a 2020 edition. That study described stages of Digital Transformation maturity, which started with a “Computerization” stage and ended in an “Adaptability” stage of maturity. A subsequent study of manufactures was then performed by the Industrie 4.0 Maturity Center and found that 80% of participants measured within the second “Connectivity” stage of maturity.

Figure 1 – Timeline for the 4th Industrial Revolution





The index and results demonstrate that connectivity is a requirement for Digital Transformation, manufacturers generally have achieved that at a fundamental level, but are struggling to advance beyond that.

Fundamentally, it is easy to understand that systems that facilitate Digital Transformation require deep and secure connectivity. But that concept becomes complicated when you dive into the details, and it becomes apparent why manufacturers struggle to advance further. I'd propose that the underlying Industrial IT Infrastructure upon which Smart Factory systems run is the primary limiter preventing more rapid progress.

## The Role of Industrial IT Infrastructure

Industrial IT infrastructure—which is the networking, PCs and servers, and the cybersecurity systems for the industrial systems—is analogous to civil infrastructure like highways, which enable you to get where you want to go through the use of a car. Highways are incredibly costly to build and maintain and they are critically important but in spite of that, most drivers don't appreciate the highway itself; the car they drive and the good time they make on their commute is what they appreciate.

Within manufacturing, the Industrial IT infrastructure is the highway, and Smart Factory technologies are the car that get an organization towards Digital Transformation. Like highways, the Industrial IT infrastructure is costly to develop and maintain, and in spite of that businesses don't value the infrastructure as much as they do the Smart Factory technologies that give them real-time visibility and optimization.

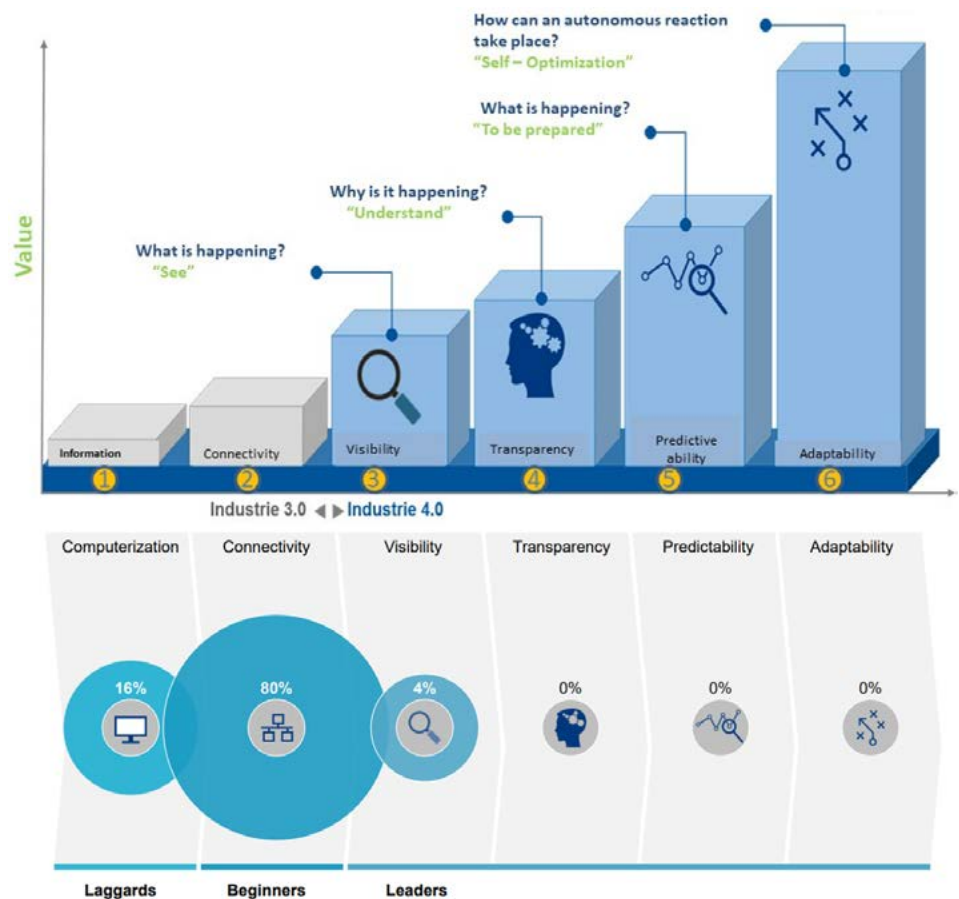


Figure 2 – Acatech Industrie 4.0 Maturity Index and Study Results

## The Industrial IT Problem

The problem that most manufacturers find themselves in is that the industrial IT infrastructure was not built to support Smart Factory technologies. Usually, the Industrial IT infrastructure is built and deployed to support individual control systems. There is a very significant difference between the two.

For example, for a small control system to run, a low-cost unmanaged switch that simply passes network traffic through is sufficient, and an independent physical server located in an IT closet can host the application. But as these systems and servers add

up and are interconnected—as they have been to perform plant-wide data collection and remote access—the low-cost switches can't handle the increasing traffic load, there are too many independent physical servers to maintain properly, and even worse, the entire infrastructure is extremely insecure.

In many cases the only way to properly correct the infrastructure is to design and deploy a new plant-wide infrastructure which some organizations do, but most find too difficult. Infrastructure is notoriously difficult to demonstrate an ROI through traditional methods, it is

disruptive to the organization, it is laborious and complex, and the long-term value is not understood broadly.

## Tie Infrastructure Investment to Digital Transformation and Security

The solution to the Industrial IT problem will never be solved at the facility-level, because operational teams' priorities focus on efficiency and productivity. Project ROI requirements are a strong example of this: including the (expensive) costs of a proper infrastructure within a typical engineering project bloats the costs of the project, throws off the ROI, and ultimately does not get approved. The costs of re-architecting a network, consolidating servers, or deploying security management tools must be justified against the value they provide, which is the strategic value that digital transformation brings and the risk reduction that security brings to the organization.

Strategy and business risk is managed at the corporate and executive level, which is where the costs of solving the Industrial IT problem can be justified against the strategic and business risk reduction value it brings. That business justification step itself is a challenging one, but it's dwarfed by the subsequent labor needed to effectively

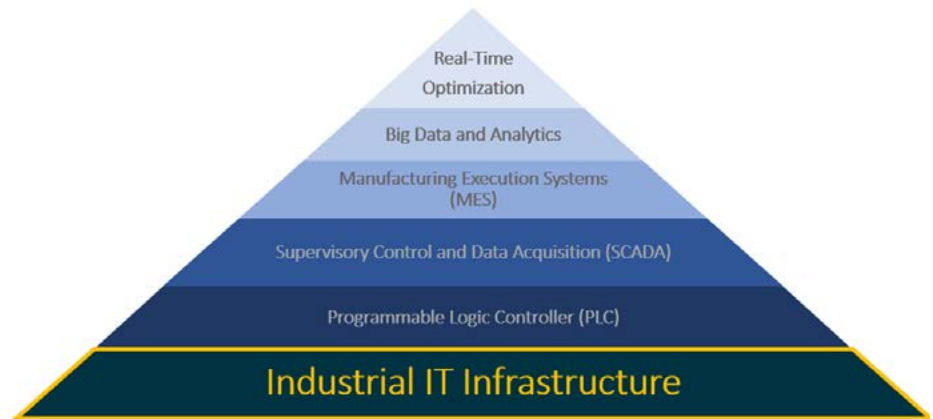


Figure 3 – Industrial IT Infrastructure Foundation

implement change throughout the organization and actually solve the problem.

## Use IEC-62443 to Achieve Digital Transformation

I put forward that the IEC-62443 is the best framework for manufacturers to lean on in order to solve the Industrial IT problem, develop an operational environment that is able to adopt Smart Technology platforms, and thus achieve digital transformation. That may sound like a reach considering that IEC-62443 is an ICS cybersecurity standard, but there are more reasons than not that it is the tool to solve the problem.

First, we have learned through recent decades of innovation that for a device or system to be secure, it must be built from the ground up with the appropriate security requirements and controls in mind. Developing any device or system first and then securing it later simply does not work; there are too many layers within the system for it to be secured later. **This is why IEC-62443 security approaches should be incorporated even before organizations begin designing and deploying new Industrial IT components during Digital Transformation.**

Second, the depth of connectivity and security the organization needs varies throughout the industrial environment. One particular facility may be of strategic importance to the business, and thus deserves enhanced connectivity, monitoring and optimization to improve the business' position in the market. Another system in a separate facility may pose the greatest operational risk to the business should a security incident occur. A challenge that the organization will face while solving the Industrial IT problem and pursuing digital transformation is to identify the varying requirements and distribute investments where they are

Figure 4 –Simplified ICS Cybersecurity Risk Management Cycle



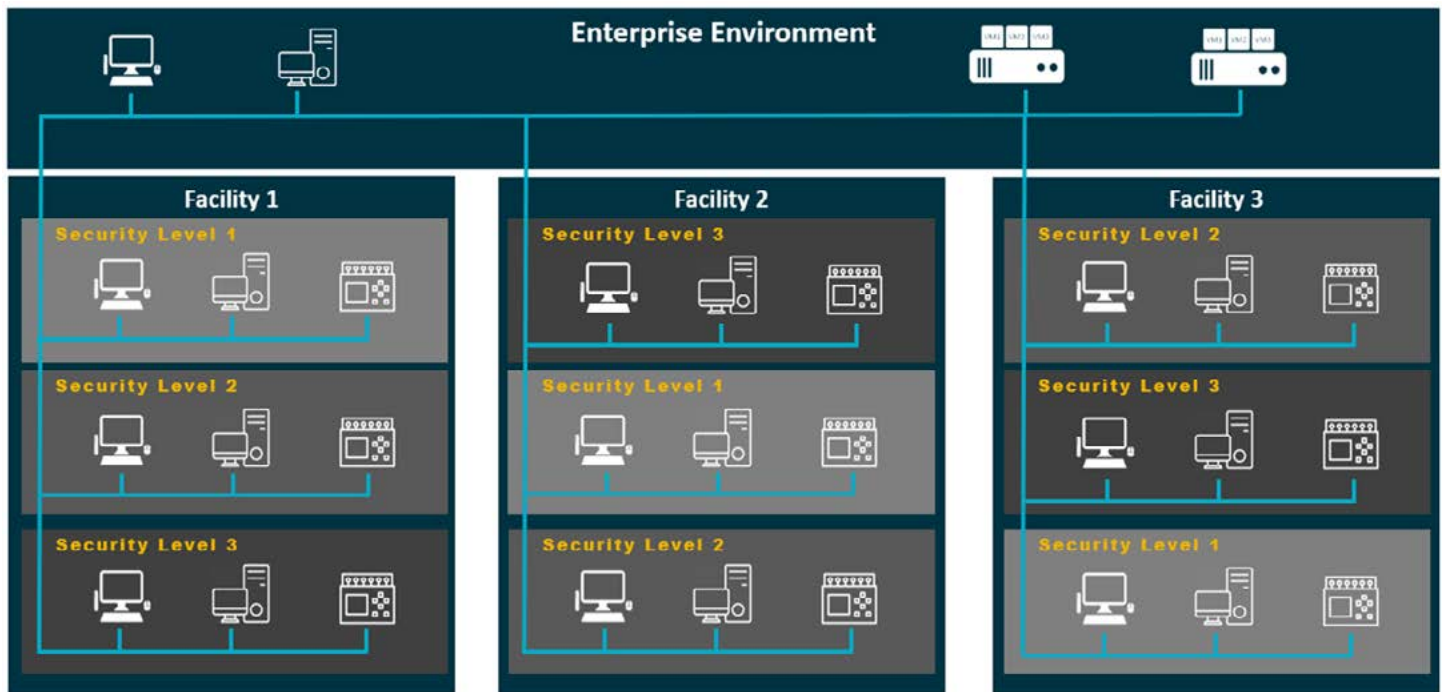



Figure 5 –Graphical Depiction of Security and Connectivity Investment Distribution

needed throughout the organization. This, too, is a consideration that is built into the IEC-62443 series of standards and achieved by first quantifying the amount of security risk reduction required for a system before identifying the security controls which should be implemented on that system. This approach can be leveraged and harmonized

with the strategic value of digital transformation to appropriately distribute and justify investment. Finally, a critical component for success in any multi-year, multi-facility initiative is to be able to monitor, re-evaluate and adjust on a continuous basis to adjust to changing conditions. A function for doing this is built into the IEC-62443 series of

standards and that process can be leveraged to not only monitor and adapt the organization’s security program in response to changing security risks, but also harmonize course corrections with changing strategic priorities and goals around digital transformation the Smart Factory technologies that the organization is prioritizing. 

## IS STANDARDS CONNECT A GOOD FIT FOR MY ORGANIZATION?



Standards can be accessed in a variety of ways. One such solution is Standards Connect from ANSI. Standards Connect is a cost-saving, fully-customizable solution for companies that:

- » Spend more than \$2,000 a year on standards and want to translate that spend into an annual subscription model
- » Want an online standards-management solution that simplifies access, search, monitoring, and collaboration
- » Need centralized access to up-to-date standards for multiple users at one or more locations

[Try Standards Connect free or request a quote.](#)

## Strategic Standardization

by Muhammad Ali, CStd – Sr. Standards Strategy and Policy Lead, AMS – HP, Inc. & USNC YEP Committee Member



Standardization can be defined as the process of formulating, issuing, and implementing standards. Strategic Standardization is more than a technical tool that can be

used for planning the development and use of standards to achieve specific objectives. It is about creating a robust standards strategy and implementing it to meet both technical and business goals. Standards are often viewed as offensive weapons and defensive shields. An offensive (proactive) approach requires pushing a specific position or a standard to gain competitive advantage while a defensive (reactive) approach requires to influence the work already in progress, protecting company's interests to avoid a competitive disadvantage.

A strategic approach to standardization requires knowledge about the standards ecosystem. The following are the key pillars for a company utilizing strategic standardization:

- » Standards Policy: Utilizing industry associations to influence regional standards strategies, laws, regulations, and trade policy
- » Standards Development: Managing the standards development participation in SDOs, industry consortia, forums etc. while protecting company IP
- » Standards Advocacy: Driving awareness on strategic standardization internally and externally

For the Standards Policy pillar, it is important to educate policy makers on the benefit attaching to the use of international standards as a tool for



achieving public policy and regulatory initiatives. This helps to avoid technical barriers to trade, promote interoperability, and build trust. Standards strategies, trade policy documents, and regulations need to have proper language regarding standards. This initiative can best be accomplished by collaborating with relevant internal groups and by participating effectively in relevant industry associations.

For the Standards Development pillar, a company needs to determine where, how, and at what level to participate effectively. It is helpful to have tools to assess the impact of a specific standard before participation as that would help in the decision on how to participate. There could be several modes of participation depending on the required outcome such as proposing and driving a new standard, engaging to influence content or to ensure progression, or simply to monitor the development. It is also important to have a method for evaluating the participation requests to protect company IP.

For the Standards Advocacy pillar, the subject matter experts participating in standards development need to be mentored and have access to training materials so they can participate actively. There also needs to be efforts to continuously provide the value of participating in international standards at the leadership level. This can be accomplished by having an internal community of experts for knowledge-sharing and having a forum to discuss issues arising. The subject matter experts need to be able to demonstrate the value coming out from standardization work. This requires them to have a breadth (cross-discipline competence such as knowledge on the intersection of standards and trade, IPR and SEP, and digital literacy) and depth (standards development expertise) of this discipline.

A successful standards strategic framework can be accomplished by participating in relevant standards development activities, connecting those activities with business outcomes, and then collaborating internally with other departments

(Govt Relations, Global Trade, R&D etc.) for better alignment at all levels.

## Why International Standards?


The primary goal of international standardization is to define requirements that products and services should meet to be acceptable in global markets. Open, industry-led international technical standards development work is a key component of trade facilitation as it enables interoperability, safety, and quality of products and services across markets. As an example, think about how interoperability and communications standards such as USB, Bluetooth, and Wi-Fi have revolutionized the way PCs can connect with peripherals and communicate seamlessly globally.

It is also important to have a diverse and inclusive standard system that is

consistent with the principles of the World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT) and the WTO TBT Committee Decision on international standards. This role that standards play in facilitating global trade is recognized as being important enough for the WTO to operate its non-tariff related TBT program to ensure that all UN member states sign up to a 60 day notification period where other countries have the right to comment on and object to the introduction of a national standard—having a material impact on global trade—where a global one exists.

Countries should bring their contributions to international standards bodies where U.S. companies and other stakeholders can influence the direction of the

standards, and avoid creating their own country specific unique national standards (often made compulsory through adoption in law or regulation) which can become de-facto market access barriers and affect the interoperability of products and services globally.

It should also be noted that success in international standards development is not by number of experts in a working group, number of delegates to plenary meetings, number of new work item proposals or number of publications by a specific TC/SC but rather by standard's adoption in the marketplace due to effectiveness in responding to a market need or its ability to open new markets and opportunities. 

## USNC LINKEDIN



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)).



**Looking for standards? Check out ANSI's webstore!**

**ANSI webstore purchases and standards subscriptions support USNC activities.**

[webstore.ansi.org](http://webstore.ansi.org)

## USNC Launches New Professional Mentoring Program

by USNC staff

Through the dedicated work of the USNC Communications Committee, the USNC launched a professional mentoring pilot program in January 2021. This new program provides emerging standards and conformity assessment professionals an opportunity to enter into a one-on-one relationship with a more experienced member of the USNC community for the purpose of retention, development and overall success.

Whereas training is typically a significant volume of information passed from one to many, mentoring is a partnership in which two individuals set their own agenda, and the mentor provides guidance to the protégé in order to assist in achieving the latter's goals. A mentoring program would foster the growth of emerging standards and conformity assessment professionals and enable them to be successful in their endeavors, whether their goals are to take on leadership roles in US or International programs, or to be successful contributing experts or delegates. The USNC Professional Mentoring Program can be seen as a way to retain new standards and conformity assessment professionals and as a means of filling the pipeline for future leaders in the USNC.



The 2021 pilot program accepted an inaugural cohort of 22 participants and is scheduled to conclude at the end of June. The USNC plans to review the program participant experience and feedback, make any beneficial modifications, and re-open applications for a new cohort beginning fall 2021.

The currently running pilot program spans a six-month period. Program participants are asked to hold monthly calls with their mentor or protégé. Two formal check-ins with program administrators are built into the

program, one around the mid-point and one as the pilot wraps-up.

Time commitments for the program beginning in fall 2021 will be similar, however the program is expected to run the full academic year, rather than the shortened six-month period.

Interested in joining the next USNC Professional Mentoring Program cohort? You can find the program application [here](#). Please contact Megan Pahl at [mpahl@ansi.org](mailto:mpahl@ansi.org) with any questions. 

## UPCOMING EVENTS

Due to the ongoing health crisis, many upcoming events have been postponed or are being held remotely. Please check the website of the individual organization for up-to-date information.

## Call for Action and Participation in Standards!

### USNC Virtual Technical Advisory Group (VTAG) for Strategic Group (SG) 12: Digital Transformation and Systems Approach – USNC Participants Needed

Following the recommendations made by ahG 86 Future of Digital Transformation including system approaches in its final report, SMB approved to reconstruct SG 12 as Digital Transformation and Systems Approach and revise its scope. For more detailed information on the new SG 12, please see attached.

Anyone who is interested in participating in the USNC VTAG for SG 12 is invited to contact Ade Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org) as soon as possible.

Please see the revised scope for SG 12 below.

#### Scope

- » Define the aspects of Digital Transformation that are relevant to the IEC and its standardization activities.
- » Develop a Digital Transformation methodology for international standardization.
- » Act as Digital Transformation and Systems Approach competence centres within the IEC and provide associated expertise and advisory services to all IEC Committees.

- » Identify emerging trends, technologies and practices needed for the development, delivery and use of IEC's work.
- » Provide a platform for relevant discussion and collaboration with internal and external participation.
- » Coordinate IEC's activities with those of external entities (e.g. ISO, ITU).

### CALL FOR MEMBERS – USNC TAG to IEC/SyC Smart Manufacturing

The USNC Technical Management Committee would like to grow the membership of the USNC Technical Advisory Group (TAG) to IEC/SyC Smart Manufacturing (SM). The current USNC TAG Officers are Technical Advisor Kirk Anderson (NEMA) and Secretary David Richmond (NEMA). Individuals who are interested in joining the USNC TAG to IEC/SyC SM are invited to contact Ade Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org).

Please see the scope for IEC/SyC SM below:

#### Scope

To provide coordination and advice in the domain of Smart Manufacturing to harmonize and advance Smart Manufacturing activities in the IEC, other SDOs and Consortia according to clause 2 in AC/22/2017 superseded by the AC/17/2018.

### USNC TAG Administrator – Organization Needed

ASME is relinquishing its role as the USNC TAG Administrator for the USNC TAG to IEC/TC 5: Steam turbines. 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 an organization is interested in the position of USNC TAG Administrator for the USNC TAG to IEC/TC 5, they are invited to contact Ade Gladstein at [agladstein@ansi.org](mailto:agladstein@ansi.org).

Please see the scope for the IEC/TC 5 below.

#### Scope

Preparation of specifications and standards for the rating and testing of steam turbines.



## Save the date!

IEC 2022 General Meeting, Host City: San Francisco

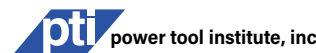
Sponsor the IEC 2022 General Meeting, hosted by the USNC

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 10-day event.

For more information, see the [IEC 2022 Sponsorship Brochure](#) or contact Adelana Gladstein at: [agladstein@ansi.org](mailto:agladstein@ansi.org) or 212-642-4965.



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



## 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).