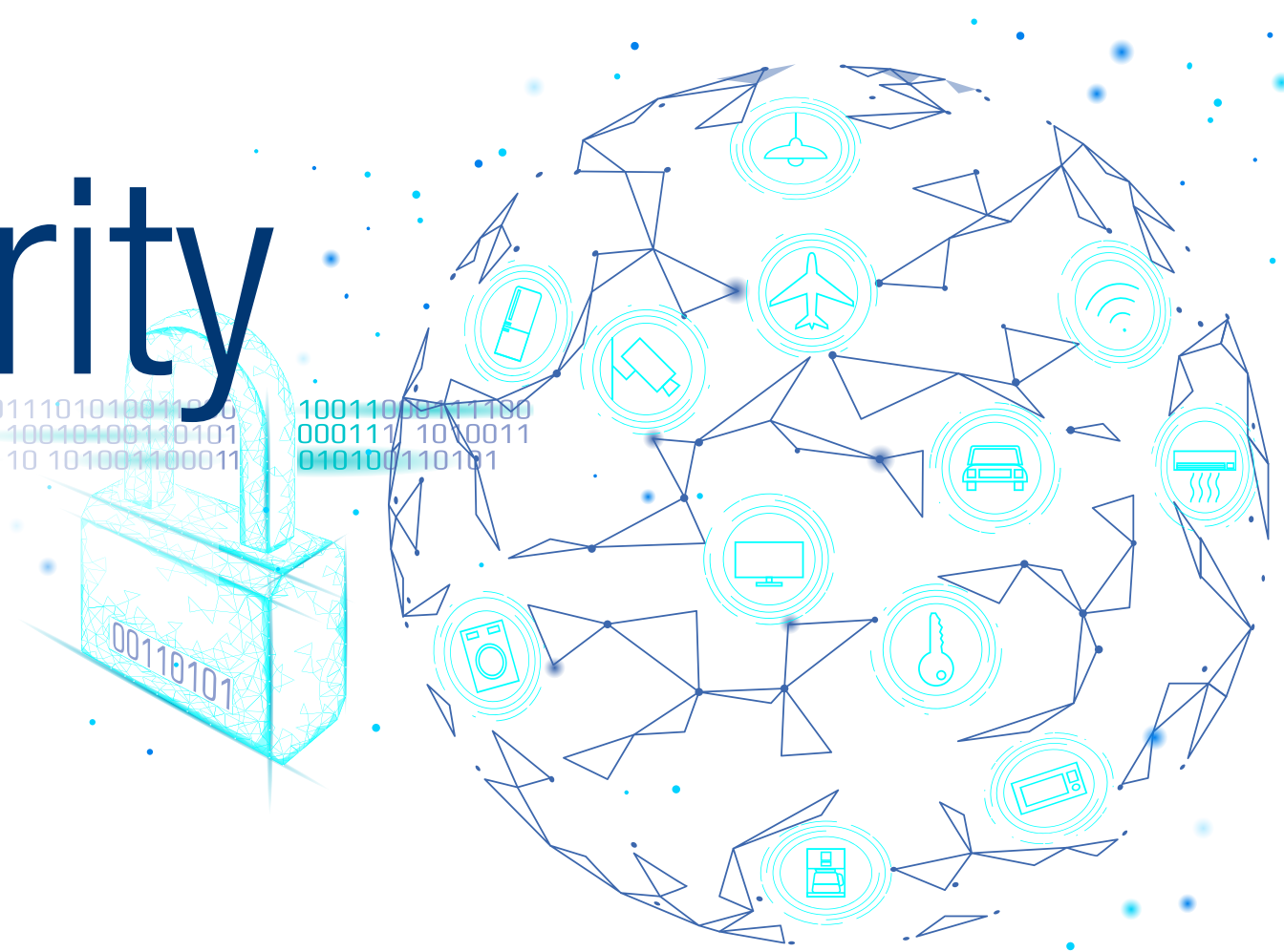


Enhanced Cybersecurity for the IIoT



Sponsored by 



**Meet Infineon Technologies at Hannover Messe,
April 1–5, 2019**

Amazon Web Services (AWS) Booth F46, Hall 6
Infineon will be demonstrating secured cloud connectivity in a smart factory
with OPTIGA™ TPM in industrial grade

Enhanced Cybersecurity for the IIoT

INSIDE

3

10 Steps to IIoT Security

By Steve Hanna, senior principal, *Infineon Technologies*

8

Why Hardware Security is the Preferred Choice for IIoT

By Nitin Dahad, European correspondent, *EE Times*

13

Real-Life Industrial IoT Cyberattack Scenarios

By Ann R. Thryft, Industrial Control & Automation Designline Editor, *EE Times*, and Nitin Dahad, European correspondent, *EE Times*

22

Designer's Guide to IIoT Security

By Nitin Dahad, European correspondent, *EE Times*

29

Embedding Security at the Edge

By Nitin Dahad, European correspondent, *EE Times*

35

Protecting communication within the smart factory and to the cloud: Infineon presents the world's first TPM 2.0 for Industry 4.0

Sponsored content

37

Maximizing Security with OPTIGA™ TPM SLM 9670

Sponsored content

10 Steps to IIoT Security

By Steve Hanna, *senior principal, Infineon Technologies*

The urgency of industrial internet of things (IIoT) security is becoming more and more apparent. It's clear that security has come to the top of the agenda as a result of many high-profile cyberattacks, such as that on the [Ukraine power grid](#), a [German steel mill](#), and [Iran's nuclear program](#). Despite the heightened awareness, the hardest part for developers of electronics systems in industrial control systems is how to implement that security.

In this article, we present 10 steps to help un-

derstand how to design in IIoT security.

Start with an industrial standard

Before we get into the list, it's worth understanding the foundation for these 10 steps, based on an international standard already available. The IEC 62443 is a series of standards and technical reports providing authoritative guidance on securing industrial automation and control systems (IACS). More details can be found in the breakout box — The Basics of IEC 62443.



The 10 steps

1 Educate yourself on this topic.

Implementing security is the hardest part of developing the technology for an industrial control system using IoT. With the convergence of operational technology (OT) and information technology (IT), new security paradigms need to be understood as the attack surface of an OT system is increased by the connectivity, yet the legacy IT systems that are often at the enterprise management layer of the industrial system may not have safety and security as an integral part of its fabric.

2 Identify the system under consideration.

Consider what it is you are trying to secure. Map out the system from the sensors and controllers at the factory or plant level to the management systems at enterprise level. Ensure that you

understand how and where everything is connected in the network.

3 Conduct initial high-level risk analysis.

This should involve clearly spelling out the risks if the systems should be compromised and the level of those risks. For example, in a gas pipeline, the potential for a gas leak and explosion presents a high level of risk.

4 Divide assets into security zones.

All of the assets should be grouped into zones that can then be identified and isolated. In the event of a failure or compromise of one zone, the security policy and process can then be designed to ensure that the breach is restricted to that zone and doesn't affect the others. In a typical industrial scenario, the zones might be segregated into a control station zone including the device level, supervisory zone

for the SCADA workstation, and enterprise zone for the business management systems and external internet connection.

5 Assign target security levels to zones.

From the five security level classifications (SL 0 to SL 4, as described earlier), assign the appropriate level of protection required for each zone based on the risk analysis in Step 3. This is defined as the target security level required for that zone based on the risk level for that zone if it is compromised.

6 Determine security requirements for systems and components based on the specified target security level (SL).

This involves deciding which security requirements apply to the systems and components based on the security level targets determined in Step 5. For ex-

ample, for a target security level of SL 4, a security requirement could be fulfilled in the supervisory zone by implementing multi-factor authentication for humans accessing the system through any network — using both passwords and biometric information. For SL 4, another requirement calls for hardware security for all devices and processes.

7 Evaluate systems and component capabilities in context of countermeasures.

Now that you have an understanding of the risks and the security protection levels needed to address those threats, it is then necessary to evaluate what the capabilities of the systems and components actually are in countering those threats and if there is a shortfall in the capability. Put differently, you know what you want to achieve in terms of security level requirements, but are the

components capable of achieving them?

8 If residual risk is too high, improve capabilities or apply countermeasures.

If your target security level is higher than the system components are actually capable of, then appropriate countermeasures need to be taken. For example, if your target security level at a factory floor level is SL 3, but your actual capability based on Step 7 is only SL 1, you need to figure out if you are able to upgrade the system or component to achieve SL 3 or whether something needs to be added (such as a new secure gateway) to enable the security level target to be achieved.

9 Develop a cybersecurity management system (policies and procedures).

Once all of the above steps have been

taken, you are now ready to put in place a set of policies and procedures at the system level to enable cybersecurity. For example, this might include things like “network segmentation must not be bypassed” and “users must not share passwords or tokens”; plus, there may be policies on password length.

10 Secure operations according to the policies developed.

It’s one thing to develop policies and procedures, but security is a never-ending process, so these need to be constantly in force and be updated as part of secure operations; otherwise, the security policies become pointless.

What we’ve established in this article is that IEC 62443 is an important industrial security standard, which is organized into four different layers from a general policies and procedures level down to the system

and component level, with five security level classifications based on the risk levels of an attack.

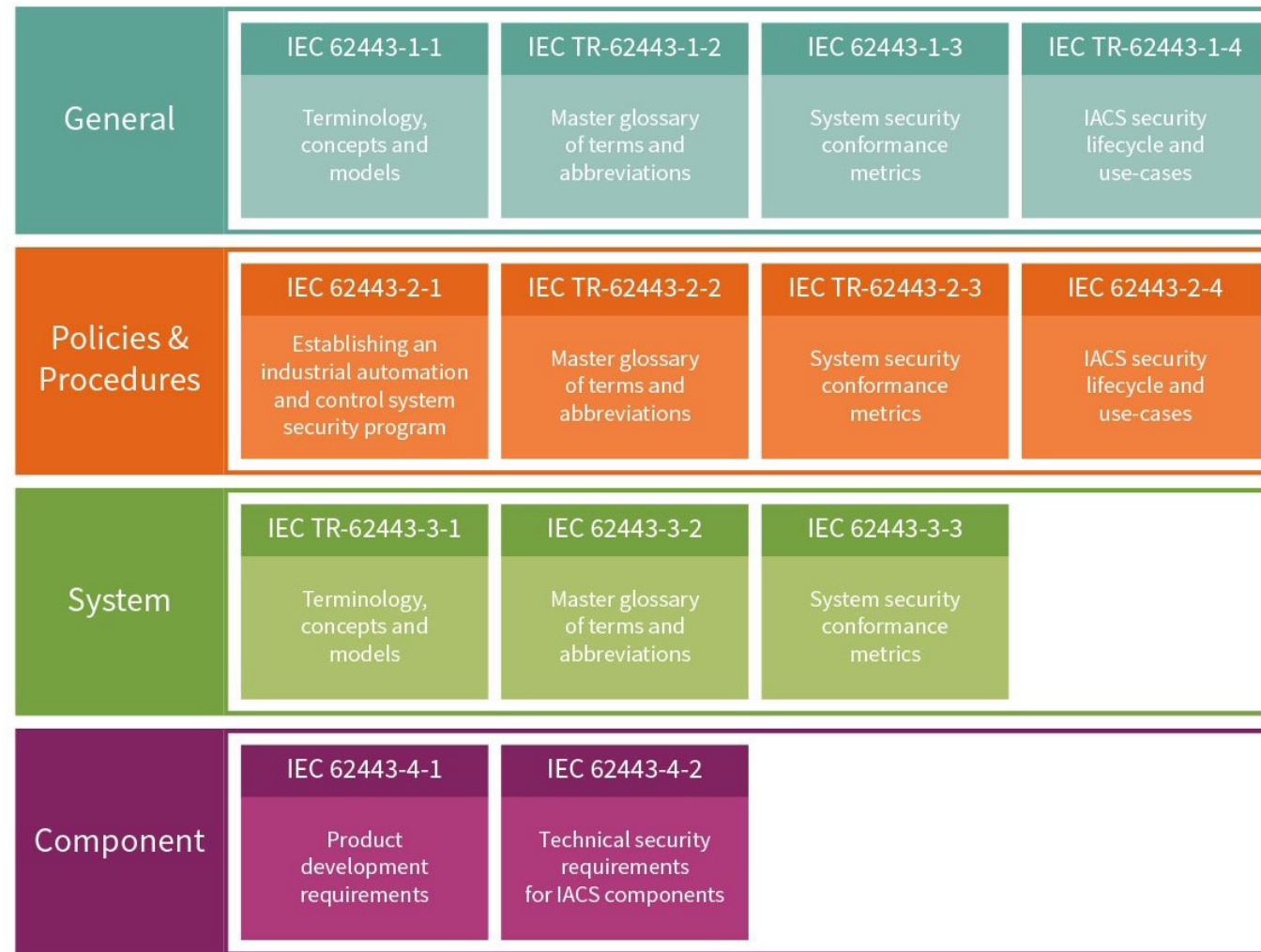
This helps in developing a 10-step approach to designing security into IIoT or industrial automation and control systems. In these 10 steps, we start with a high level of system mapping and risk-level analysis and then drill down to the capability of the system and components in countering the cyber-threats and what measures need to be taken to improve or update legacy systems to meet those needs. It then continues in operations throughout the life of the system in order to maintain security as long as the system is in commission.

For more information, follow these links:

[Introduction to IEC 62443](#)

[ISA Security Compliance Institute](#) (for IEC 62443 conformance guidance on the cybersecurity of industrial automation control systems)

The many parts of IEC 62443



The IEC 62443 standard is organized into four categories: **General, Policies & Procedures, System, and Component.** (Image: Infineon Technologies)

The basics of IEC 62443

IEC 62443 enables a systematic approach to provide a thorough set of recommendations for defending industrial networks

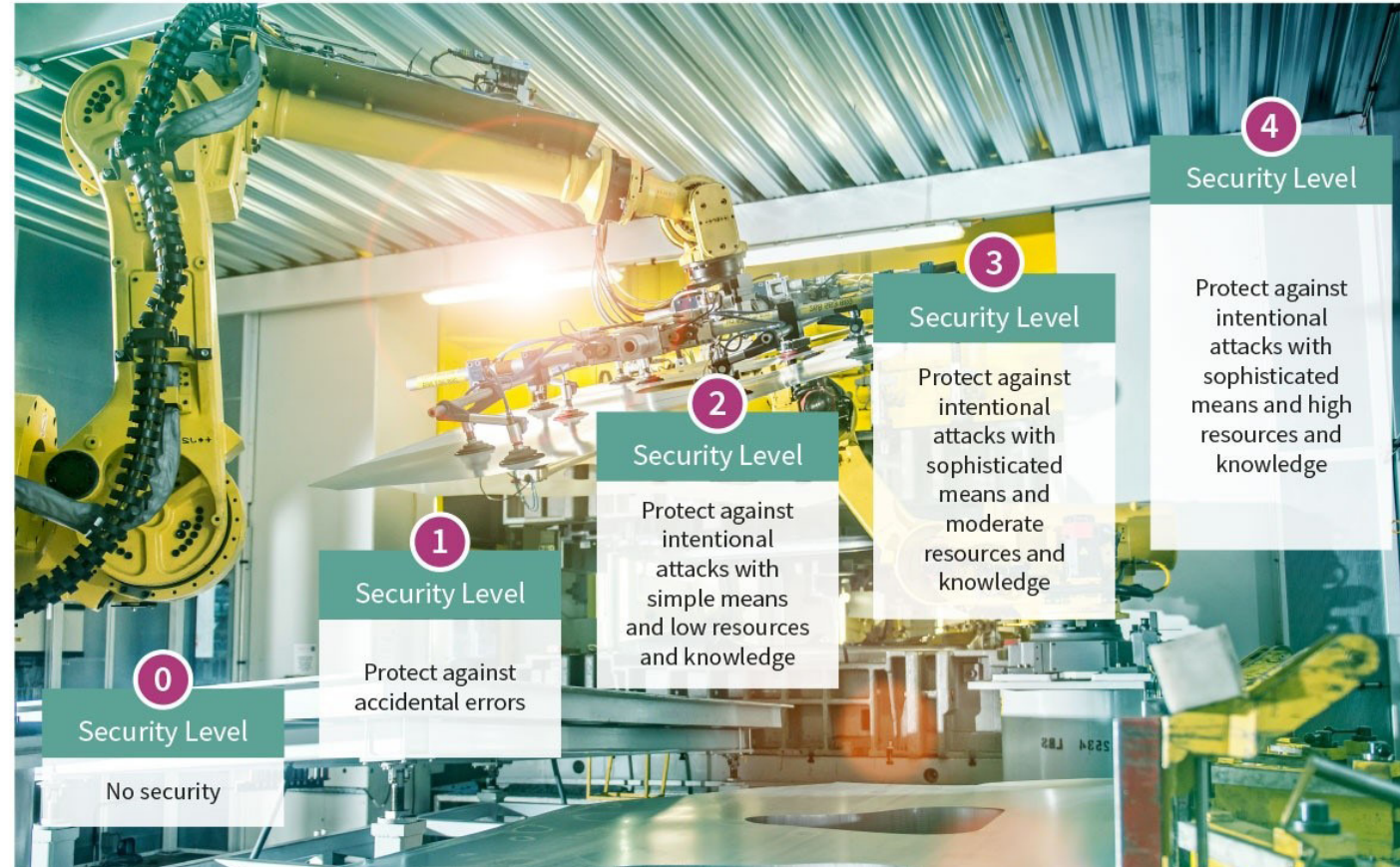
against cybersecurity threats, covering every stage and aspect of protecting systems from cyberattack from risk assessment through operations. The standard describes tech-

Security Levels (SL)

niques enabling industrial stakeholders to assess the cybersecurity risks to each system and to set out policies and procedures to decide how to address those risks.

In order to understand the context for the 10 steps to IIoT security, it's a good idea to understand how IEC 62443 is organized into four categories and five security levels.

- The “general” documents provide an overview of the industrial security process and introduce essential concepts.
- The documents on “policies & procedures” highlight the importance of policies, which are often neglected but are critical to establishing industrial systems security; even the best security is useless if people are not trained and committed to supporting it.
- The “system” documents recognize that even if you have the right parts, the sys-



The five security levels defined in IEC 62443. (Image: Infineon Technologies)

tem cannot be secured unless you use them in the right way and treat them as part of an integrated system.

- The “component” documents describe the requirements that must be met for secured industrial components.

In order to classify how much security protection is needed and recognizing that one size of security doesn't fit all, IEC 62443 defines five security levels, from SL 0 (no security) to SL 4 (resistant against nation-state attacks). Each level is characterized based on what they can protect against.

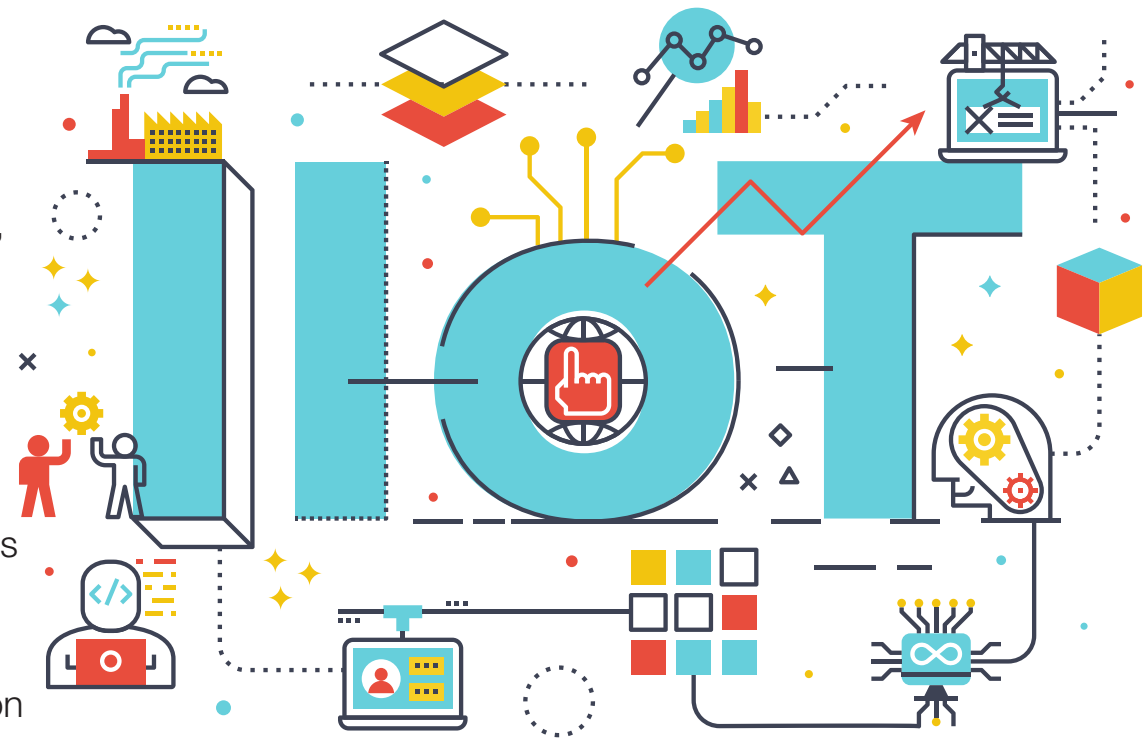
Why Hardware Security is the Preferred Choice for IIoT

By Nitin Dahad, *European correspondent, EE Times*

Industrial automation will be one of the biggest areas of spending in the internet of things (IoT) in 2019, according to the latest industry forecast. The questions are, how can the devices connecting the systems to the network be trusted, and what's the best way to ensure that their industrial IoT (IIoT) systems are secure — software or hardware? In this article, we look at the case for hardware-based security as the preferred choice for IIoT and its benefits beyond just security, such as time to market, scalability, and performance and manufacturing flexibility.

Industrial to drive IoT in 2019

An industry forecast published by International Data Corporation (IDC) highlights manufacturing, transportation, and utilities as the leading sectors expected to spend on IoT solutions in 2019 — these are the sectors typically addressed with IIoT systems. With total global spend this year expected to reach \$745 billion, industries that will spend the most are discrete manufacturing (\$119 billion), process manufacturing (\$78 billion), transportation (\$71 billion), and utilities (\$61 billion). Among



manufacturers, this will largely be focused on solutions that support manufacturing operations and production asset management. In transportation, more than half of IoT spending will go toward freight monitoring, followed by fleet management. IoT spending in the utilities industry will be dominated by smart grids for electricity, gas, and water.

Hardware spending will be about \$250 billion, led by more than \$200 billion in module/sensor purchases. Given this growth, the potential risk from cyberattacks will also increase significantly. System developers will be looking to rapidly deploy security technology, with both hardware and software solutions available on the market. A key factor determining which route to go is essentially around vulnerability.

Software is arguably much more vulnerable because it can more easily be analyzed by attackers to undermine security. On the other hand, hardware security chips are more likely to be tamper-resistant and have additional

features that can efficiently prevent attacks. This includes protected processing and storage of software, code, and data — enabled through encrypted memory and processing, fault and manipulation detection, and secure code and data storage. Hence, the software running on the secured hardware can also then be protected from reading, copying, and cloning and from being analyzed, understood, and sabotaged.

What the standards say

International industry standards like IEC 62443 require hardware security for the highest levels of security, as do the National Institute of Standards and Technology (NIST) and the Industrial Internet Consortium (IIC). The NIST “Platform Firmware Resiliency Guidelines” talk about the functions of the roots of trust (RoTs) and the chains of trust (CoTs) needing to be resistant to tampering attempted by any software running under, or as part of, the operating system on the host

processor. It explicitly states that information transferred from the software on the host processor to the platform firmware should be treated as untrusted.

The RoT is the foundation of security and resiliency in an industrial control system and serves as an anchor in a CoT. Generally, successive elements are cooperative in maintaining the chain of trust started by the RoT. Components in a chain of trust have the privileges not available to less trusted software to perform security-critical functions like carrying out device updates. RoTs and CoTs may have mechanisms to relinquish these privileges once the security function is complete or if it is determined that the security function is not required. A CoT may also relinquish privileges before passing control to a non-cooperative element.

Because RoTs are essential to providing critical security functions, they need to be secure by design. Major considerations for determining confidence in RoTs are an analy-

sis of the attack surface of an RoT and an evaluation of the mitigations used to protect that attack surface. The responsibility of ensuring the trustworthiness of an RoT is on the vendor that provides the root of trust. Vendors typically protect RoTs by either making them immutable or by ensuring that the integrity and authenticity of any changes to RoTs are verified prior to performing such updates. Often, RoTs run in isolated environments, run at a greater privilege level than anything that could modify it, or complete their function before anything can modify it to ensure that devices cannot compromise their behavior during operation.

Offering more than just security

Steve Hanna, senior principal at Infineon Technologies, highlights why hardware-based security is the most secure and how it provides more than just the security aspect. He commented, “Hardware-based security not only implies tamper-resistance,

but it also enables benefits in terms of time to market, scalability, and performance. It also plays a part in protecting against theft and counterfeiting through the logistics supply chain. A dedicated security chip, which is evaluated by independent security testing laboratories and certified by international institutions, can be used as a building block to carry out cryptography and reduce the overall complexity of your design. This can reduce time for security implementation to just weeks rather than months.”

Haydn Povey, a board member on the IoT Security Foundation and CEO and founder of Secure Thingz, added, “You need to be able to build a root of trust, and hardware is better placed to enable an immutable boot path. You have more control with the hardware root of trust, and it provides an audit path. Hardware enables the secure enclave, can run fundamental boot services like the secure boot manager, and can bring the device into a known good state should it be required.”

He said that from a “secrets” perspective, a trusted ecosystem is essential. A silicon vendor is well-placed to provision the secure elements of a device, or the keys can be injected by an OEM. For volume quantities, the chip company can provision these at wafer level, but for lower quantities, part of the trusted ecosystem would include distributors such as Arrow, who can then provide the programming of the secure elements.

Infineon’s Hanna is keen to emphasize the time-to-market aspect of utilizing hardware-based security. The argument is that there are building blocks already available from some silicon vendors, and these hardware security chips are often evaluated by independent security testing laboratories and then security-certified. Certification can prove the highest barriers to attackers looking to penetrate a chip’s defenses.

By deploying these independently tested chips, the ready-made solutions can help a designer quickly add functions like hard-

Meeting the toughest Security Requirements of IEC 62443



ware protection for device authenticators or protecting supplier keys and data as roots of trust (see chart). This is particularly appropriate because it's often the case that IIoT security requires a huge learning curve, so by using devices already available, this can take a lot of the pressure and time off of the development work.

Scalability, performance, and manufacturing flexibility

With the growth in IIoT highlighted for 2019 at the beginning of this article, in addition to time to market, scalability is also a key requirement. Hardware-based security devices lend themselves well to scaling for different performance levels, different security levels, and different platforms. In order to protect the integrity, authentication, confidentiality, and availability of products and data being handled by the system, the same discrete security controller could be deployed across an entire product

		OPTIGA™ Trust B	OPTIGA™ Trust E	OPTIGA™ Trust X	OPTIGA™ TPM
SR & CR 1.5 RE 1:	Hardware protection for device authenticators	✓	✓	✓	✓
SR & CR 1.9 RE 1:	Protect private keys with hardware	✓	✓	✓	✓
CR 1.14 RE 1:	Protect critical symmetric keys with hardware			✓	✓
EDR, HDR, & NDR 3.11:	Provide tamper resistance and detection	✓	✓	✓	✓
EDR, HDR, & NDR 3.12:	Protect supplier keys and data as ROTs			✓	✓
EDR, HDR, & NDR 3.13:	Protect owner keys and data as ROTs			✓	✓

IEC 62443 defines many specific security requirements and requirement enhancements. Depending on their scope and applicability, these are known as System Requirements (SR), Component Requirements (CR), Embedded Device Requirements (EDR), Network Device Requirements (NDR), or Host Device Requirements (HDR). As the Security Level (SL) increases, the set of requirements increases also. For example, Security Levels 3 and 4 require that devices and users must authenticate each other and use hardware security to protect their credentials and Root of Trust (ROT).

Infineon's OPTIGA™ product family provides a range of security chips for authentication and other functions. (Image: Infineon Technologies)

portfolio. This has the benefit of providing assurance of the same level of security implementation across a number of products.

Performance can be a real concern when adding security to a device. This is where the hardware approach can provide signifi-

cant advantages over software-based solutions for functions such as secure storage and calculations. An example might be in securely hiding the calculation carried out by a cryptographic key: A dedicated tamper-resistant chip will complete the

calculation in one pass because it's happening in a protected environment, but getting the same level of security with a software solution could require multiple "cover-up" operations to hide the key during calculation — thus impacting both performance and power consumption.

Manufacturing supply chain logistics can present a significant challenge for IoT device manufacturers because devices and their private keys could be susceptible to theft and counterfeiting. The security concept in most IoT devices is based on injecting a key pair, one public and one private, providing a unique identity to be assigned to a device that, in turn, enables it to be authenticated within a network and allocated access according to its privileges. But the way that many manufacturing operations are set up as

part of global supply chains, it is possible that if private keys are intercepted or stolen along their route, then it's possible for someone outside the system to manufacture counterfeit devices, resulting in a potential threat to system security. This is where hardware-based security can offer secured tracking on a value chain and offer manufacturing flexibility being that the chip can be interrogated at appropriate points to verify authenticity.

Ultimately, Hanna commented, hardware-based security offers significant benefits for connected devices and systems in IIoT. "Even if an attacker did get in, they can't easily decipher what's happening in the chip. Our security technology can make it extremely difficult for an attacker to find or probe those vulnerabilities."



Implementing IEC 62443 — How to Meet the Challenges

Learn how to achieve strong industrial security with the IEC 62443 standard. This whitepaper gives a short introduction to this needed standard, which was developed to prevent equipment damage, downtime, and safety issues in industrial environments.

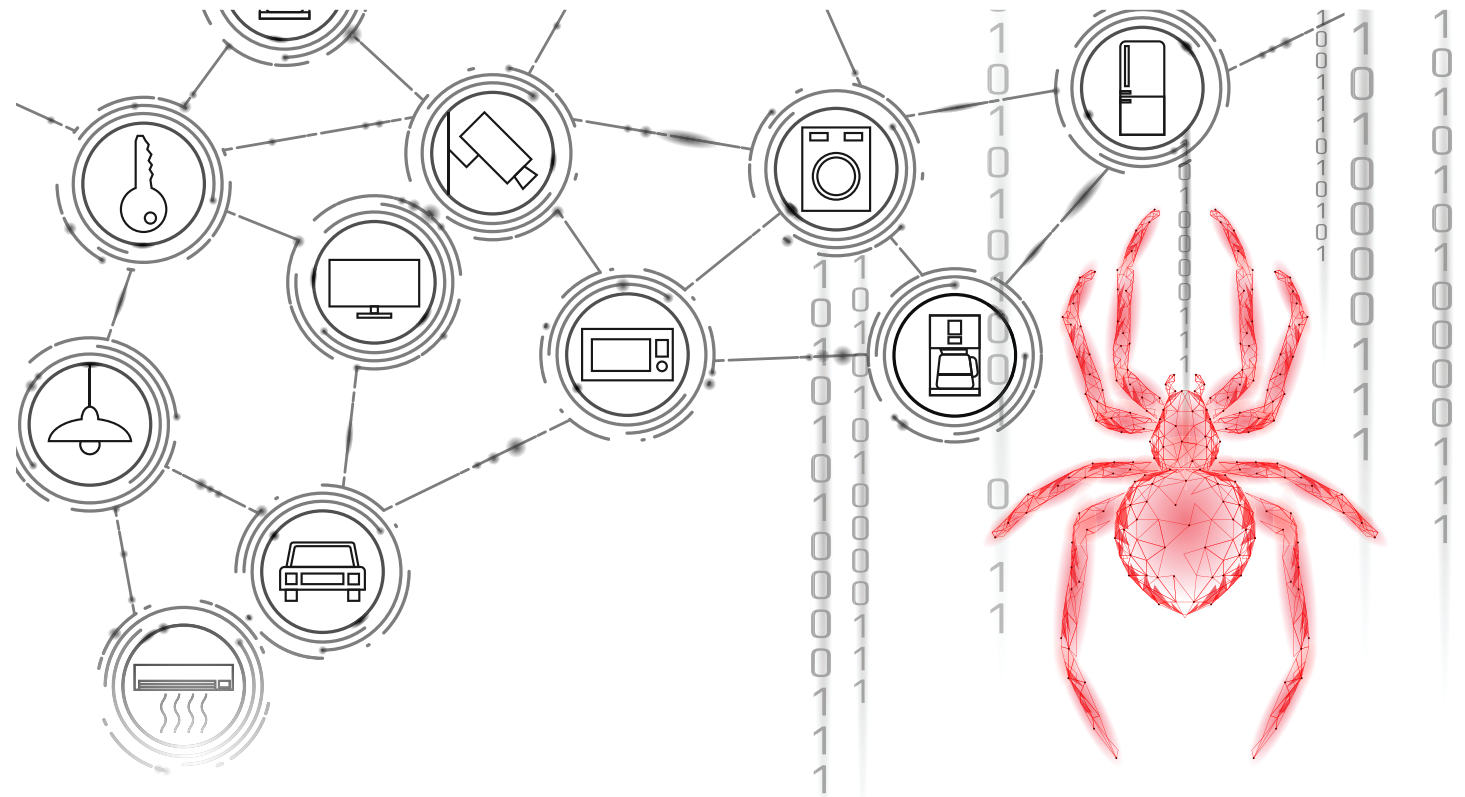
[DOWNLOAD WHITEPAPER](#)

Real-Life Industrial IoT Cyberattack Scenarios

By **Ann R. Thryft**, *Industrial Control & Automation Designline Editor, EE Times*,
and **Nitin Dahad**, *European correspondent, EE Times*

What are the worst-case possibilities if your company gets hacked? Imagine these scenarios:

- The world's largest pure-play semiconductor company shuts down some of its fabs after a WannaCry malware variant spreads through the production network.
- After being fired, an engineer who still has access to a water and sewage company's SCADA system opens up the valves so that the system dumps sewage everywhere.
- Hackers take control of production management software and then the industrial control system at a steel mill, causing massive physical damage.



- Unknown attackers change process parameters in the recipe for a food and beverage product by altering process controller code, increasing the quantity of salt to three times what it should be. The change goes undetected until customers complain.
- Hackers take control of an entire network of wind turbines at a U.S. wind farm using a Raspberry Pi-based card with a cellular module for remote access to programmable automation controllers.
- Competitors of an electronics company rewrite the code on the robots used in its manufacturing process, which begins introducing subtle defects that reduce yields and cause product recalls.

The first four have already happened, and the first one happened to Taiwan Semiconductor Manufacturing Co. (TSMC) last summer.

The wind farm hack was an experiment to show just how easy it was to do. The manufacturing robot hack hasn't happened yet — as far as we know — but the ease of intruders gaining control of industrial robot systems has been demonstrated by several industry groups.

The hacking of the IIoT

What do these all have in common? The systems that got hacked and/or compromised were industrial control systems (ICS), a central part of operational technology (OT) networks that form, along with IT networks, the industrial internet of things (IIoT).

As more and more devices get connected to IIoT networks, many of the increasingly sophisticated cyberthreats originally directed at IT environments are now entering OT environments, including ICS.

These threats pose very different and potentially larger, more hazardous risks as they migrate to OT environments. Targets

may include critical infrastructure such as power grids, dams, oil rigs, chemical processing plants, manufacturing plant equipment, and production lines.

Inside jobs

Although the typical image of a cyberattacker is an outside hacker (usually wearing a hoodie), note that not all of the attackers in the list above were outsiders: Some of these events were inside jobs, which many companies see as their greatest threat.

Potential internal attackers could include disgruntled ex-employees who may still have access to the control system, said Chris Sistrunk, principal consultant for industrial control systems at FireEye's Mandiant cybersecurity service.

Sistrunk told us about the Australian water and sewage company's attack and, more recently, a Louisiana case wherein an engineer who was let go still had remote access from home and shut down a paper mill.

Although a production shutdown could be very costly, it's not the biggest concern that could result from your IIoT being hacked, said Joe Slowik, adversary hunter for industrial cybersecurity firm Dragos. "Not counting the money lost by a day or so of a shutdown — at least with that, you know what happened, and things [might be] stopped before something more pernicious could take root."

Slowik told us about the possibility of hackers attacking production robots and affecting quality control, which could be much worse. "This causes a dramatic increase in your defect rate in a way that's hard to troubleshoot. So then your production doesn't meet standards and you suffer a reputation loss among your customers and vendors."

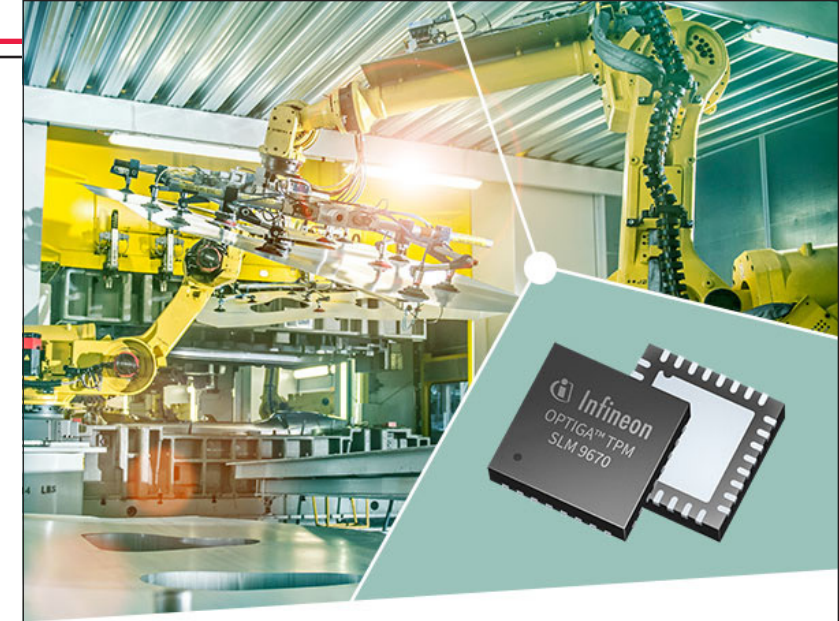
Third-party breaches

Other attacks have been executed by presumably trustworthy third parties. For example, a fake official pretending to do a fire

inspection could easily introduce a piece of malware to enable an attack by inserting a USB stick into a computer attached to an internal network, including those located at a remote facility and connected to the internet.

Another example of third-party breaches is one event among the additional Russian hacks of U.S. power grids and other critical infrastructure revealed last year by the U.S. Department of Homeland Security (DHS). Attackers got access via spear-phishing emails sent to equipment maintenance staff, who have legitimate remote access, to steal their login credentials, said Phil Neray, vice president of industrial cybersecurity for OT cybersecurity firm CyberX.

Even with some of the best physical security in place, that's not enough to protect physical assets in a cyberattack, said Andrea Carcano, chief product officer and co-founder of Nozomi Networks, who told us about the food and beverage product hack. That



Smart factories and Industry 4.0 call for robust security:

OPTIGA™ TPM industrial grade

- › Extended temperature range
- › Extended lifetime
- › Industrial-grade quality
- › Standardized and certified security chip

Learn more:

www.infineon.com/industrial-TPM

company still doesn't know if the change to its process code was introduced by external malware or someone inside the plant.

“So you may have physical protection, but changing process parameters could cause a much more dangerous effect than too much salt,” said Carcano. “If altered program code inside a process controller changes the way a product is created, without cybersecurity protection, you won't know why or even that it's happened. All of the pharmaceutical and chemical manufacturing companies are concerned about this possibility of changing the recipes and the processes.”

Data breaches & cyberattacks now No. 1 concern

In factories and other industrial settings, the IIoT is often heralded as the answer to many challenges. The connectivity assists in productivity, efficiency, and profitability. For utilities, it also helps manage demand. In public infrastructure, it assists governments to

deliver better services more effectively and economically, including public safety.

- But the IIoT and [microprocessors](#) are emerging battlegrounds for cyberattacks, according to the global 2018 [SonicWall Cyber Threat Report](#). Both areas are also often overlooked and unsecured.
- In 2017, there were 9.32 billion malware attacks and more than 12,500 new common vulnerabilities and exposures worldwide. Data breaches and cyberattacks overall are seen by executives as the No. 1 business, operations, and financial risk, to the extent that Lloyd's of London considers them a greater threat than catastrophic natural disasters, says the report.
- That perception is echoed in the 2018 [World Economic Forum Global Risks Report](#) (Cyberattacks are the risk of greatest concern to business leaders in advanced economies) as well as the

2018 [21st CEO Report](#) from PricewaterhouseCoopers (PwC) (North American executives said that cyberthreats are the chief threat).

- In just the last couple of years, a perfect storm of conditions and trends has led to a huge jump in the number of cybersecurity events targeting the OT side of the IIoT. We detail the elements of that perfect storm in a companion article in this special report, “[What Makes IIoT Systems So Vulnerable to Cyberattacks?](#)” This jump includes discoveries of vulnerabilities in industrial control or related hardware and software, cyberattack incidents, and actual breaches.
- As defined by the [Verizon 2018 Data Breach Investigation Report](#), in cybersecurity-speak, an incident is commonly understood as “a security event that compromises the integrity, confidentiality, or availability of an information asset” (Translation: The barn door is open, but

Malware Attacks, Vulnerabilities, and Other Cybersecurity Events Affecting Industrial Control Systems/Operational Technology

2007...2017

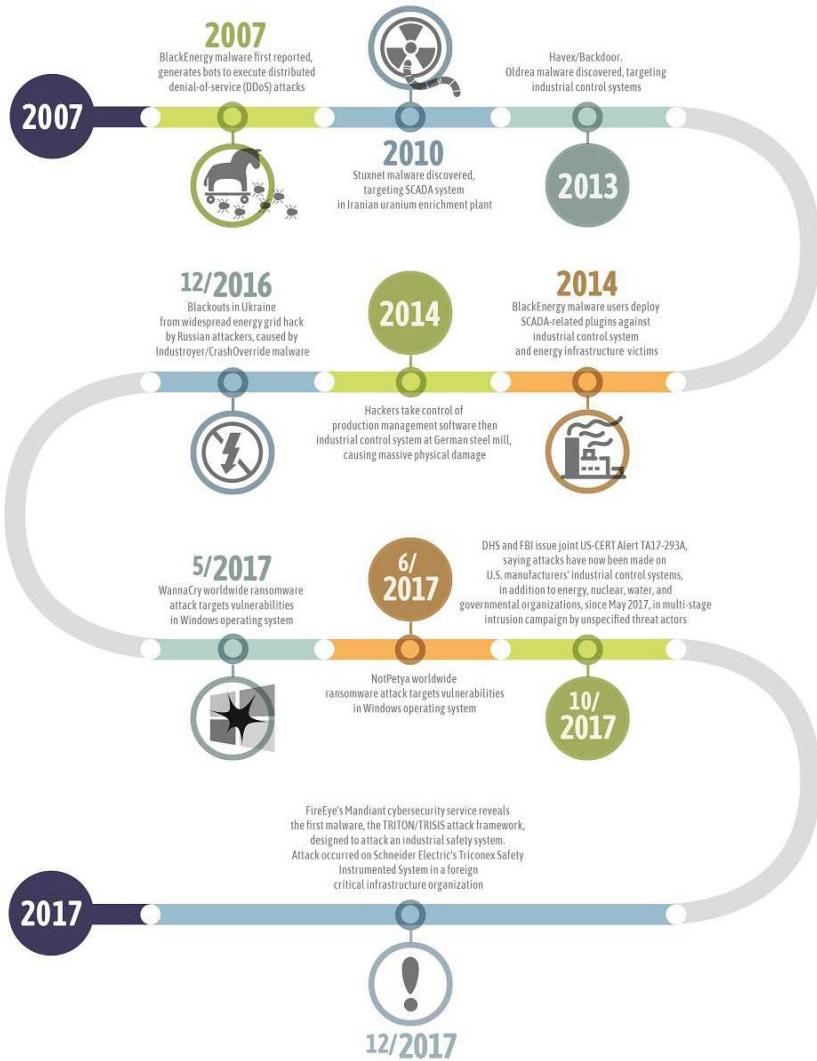


Image: EE Times

the cows haven't left), while a breach is "an incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party" (Translation: The cows have now gotten out). This report identified more than 53,000 overall cybersecurity incidents and 2,216 breaches around the world in multiple industries during the previous 12 months.

2007 to 2017: ICS cyber events increase

"Attacks on control systems have been occurring since the late 1990s, but they didn't become mainstream until 2010, when Stuxnet malware was discovered and reported on — that changed everything," said Mandiant's Sistrunk. FireEye's Mandiant cybersecurity service discovered the TRITON/TRISIS malware designed to attack ICS-connected safety instrumented systems (SIS). "After that, we started seeing a lot of

interest in security for control systems. At that time, security features were not being built into industrial control system equipment."

The increase in ICS-related events can be appreciated by looking at a sampling of events in 2018 contrasted with a sampling of those between 2007 and 2014.

Between 2007 and 2014, the first three malware types targeting ICS were developed: the Stuxnet worm, the Havex/Backdoor.Oldrea remote access Trojan (RAT), and the SCADA-targeting version of BlackEnergy. In December 2016, cyberattackers began ratcheting up their efforts against industrial systems with release of the fourth, the Industroyer/Crashoverride malware framework that shut down large parts of the Ukraine energy grid.

During 2017, both industrial and more broadly targeted cyberattacks escalated. While the WannaCry and NotPetya ransomware attacks were capturing world attention

by revealing Windows vulnerabilities, DHS warnings to manufacturers and infrastructure owners about ICS vulnerabilities jumped.

In October 2017, those warnings became reality when the DHS and the FBI issued a [joint technical alert](#) stating that attacks were now targeting the ICS of U.S. manufacturers and the previously known energy, nuclear, and water organizations. The alert also revealed that all of those attacks comprised an ongoing, long-term campaign by unnamed actors targeting small and low-security networks as vectors for gaining access to larger, high-value networks in the energy sector.

In December 2017, a new type of malware targeting industrial processes struck an unnamed foreign critical infrastructure facility. The [TRITON/TRISIS malware framework](#) was the first designed to attack an industrial plant's safety systems connected to ICS, making this a watershed event. It also targeted a specific hardware model.

2018: ICS cyberevents escalate

Security events multiplied in 2018:

- The Meltdown and Spectre microprocessor vulnerabilities that started out the year
- The DHS/FBI identification of Russia as the source of the years-long attack on U.S. critical infrastructure and manufacturing
- Hacks of oil pipeline EDI systems, causing their temporary shutdown
- Vulnerabilities detected in multiple types of industrial hardware and software, including some PLCs, security cameras, routers, bridges/access points, and network management software
- A revised version of TRITON/TRISIS that now attacks many more brands of safety system hardware and has breached U.S. firms
- Revelations that the China-based “Thrip” group has infiltrated satellite communication, telecom, geospatial im-

Malware Attacks, Vulnerabilities, and Other Cybersecurity Events Affecting Industrial Control Systems/Operational Technology

During 2018



aging, and defense organizations in the U.S. and Southeast Asia

Cyberthreat activity within the industrial environment is definitely increasing, said Dragos's Slowik. His firm extensively analyzed the TRITON/TRISIS attack and identified the malware's inventors.

"Is that because we're looking harder, or is this truly a new trend?" he said. "My answer is that it's both greater awareness and greater capability to do the analysis versus five years ago, when it was difficult or not even sensible to say, 'This is definitely a malware event.' That said, the threat landscape for both commodity non-targeted and professional targeted instances seems to be increasing. By 'commodity,' we mean criminal, often publicly available infections such as repurposed WannaCry, and by 'professional,' we mean a dedicated, almost exclusively state-sponsored activity without a primary motivation for monetizing events."

- According to the Pwne Express 2018

[Internet of Evil Things report](#), 85% of security professionals believe that cybersecurity threats will lead to an attack on major critical infrastructure over the next five years, and that opinion was echoed by many of the cybersecurity experts to whom we spoke in preparing this special report.

- The annual Kaspersky Lab survey of global OT/ICS cybersecurity practitioners at industrial organizations, [The State of Industrial Cybersecurity 2018](#), found that more than half view the increased risks associated with connectivity and integrating IoT ecosystems, in addition to the management of these risks, as a major OT/ICS cybersecurity-related challenge.
- That report also cited new challenges from a growing percentage of organizations that are deploying both IIoT systems and cloud solutions for SCADA systems. More than three-quarters of respondents

believe that their company will likely be the target of a cybersecurity incident affecting their industrial control networks.

It's not only industry executives and cybersecurity professionals who are concerned about cyberattacks and vulnerabilities.

More than half of critical infrastructure operators in the energy, utilities, and manufacturing sectors said that they weren't confident that either their own organizations or other infrastructure companies are protected from security threats to their OT environments, according to a [poll](#) released last spring by industrial cybersecurity firm Indegy.

Protection often lacking for ICS/OT networks

As has been noted in [previous studies of ICS/OT cybersecurity readiness](#), both awareness of and budgets for ICS/OT security have been increasing, yet protection levels are low.

- According to a study conducted in 2017

by CyberX, the [Global ICS and IIoT Risk Report](#), one-third of OT networks with ICS-controlled processes are exposed to the public internet. Of more concern is how few are protected against that exposure. More than half use easily hackable plain-text passwords in control networks, and half lack anti-virus protection. More than 75% run obsolete Windows systems like XP and 2000 unsupported with security patches, while 82% run well-known remote access management protocols, making it easier to access and manipulate network equipment. Twenty percent have wireless access points, which can be compromised in multiple ways.

- In 2017, information security researcher Jason Staggs from the University of Tulsa, Oklahoma, [demonstrated how](#) he could take control of entire networks of wind turbines at U.S. wind farms using just a Raspberry Pi-based card with

a cellular or Wi-Fi module for remote access to programmable automation controllers. Staggs and his colleagues would have been able to cause significant damage or loss if they'd been real attackers.

- In a [report in Wired](#) on his research, Staggs reportedly said, "They don't take into consideration that someone can just pick a lock and plug in a Raspberry Pi." The turbines that his team broke into were protected only by easily picked standard five-pin locks or by padlocks that took seconds to remove with a pair of bolt cutters.

But regardless of how cyberattackers get into an insufficiently protected OT network, once they're in, they can move around the network and compromise or control industrial devices relatively easily. The types of cyberattacks that can be made, and the types of effects that threat actors are after, vary widely.

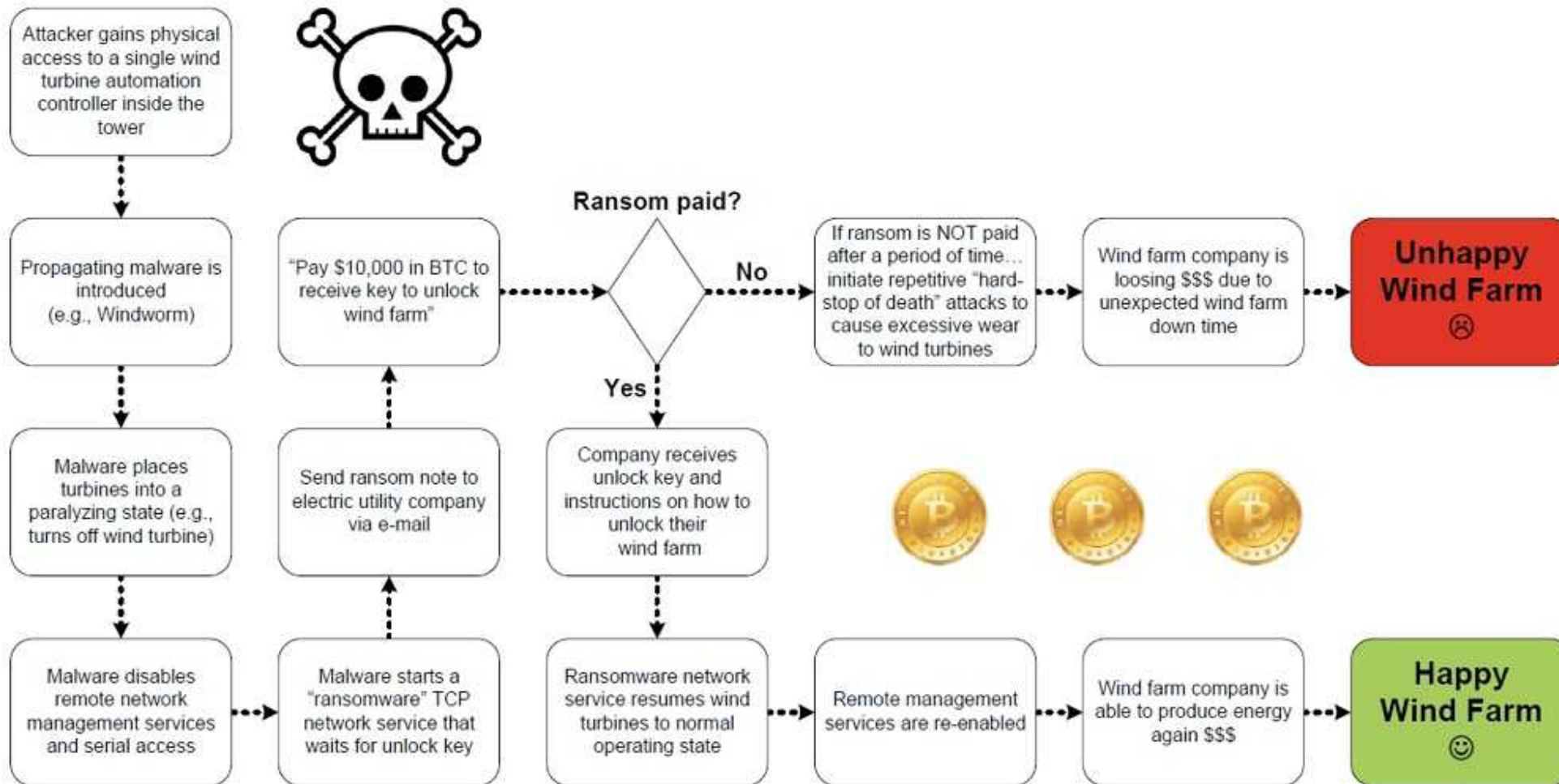
Kinds of threats

In the ICS/OT environment, cyberthreats are potentially larger and much more damaging than threats made to the IT environment. They can include:

- ransomware demands backed by shutdown threats
- altering production process code that can change industrial robot safety levels, affect product contents and manufacturing yields, or even cause massive damage, as in the steel mill attack
- industrial espionage

Several cybersecurity experts pointed out the importance of possibly unintentional effects of attacks originating either inside or outside the company. In giving examples of commodity non-targeted versus professional targeted instances, Dragos's Slowik identified the recent TSMC fab shutdowns as an opportunistic, non-targeted event.

"It looks like it was caused ultimately by the WannaCry virus, yet after all that time,



Example scenario of the potential consequences of a wind farm ransomware attack, as demonstrated by information security researcher Jason Staggs at a talk given at Black Hat USA 2017. (Image: Jason Staggs/Black Hat USA 2017)

[the virus] was still effective in spreading by hitting production,” he said.

“WannaCry is a ‘dumb weapon’ in that it spreads indiscriminately through infected networks based on what network nodes are vulnerable to the Windows MS17-010

vulnerability. So while the exploit is fairly sophisticated, its implementation is not. Thus, in cases such as TSMC, a relatively unsophisticated, untargeted threat can rapidly spread, causing an impact in the victim environment without any intention on the

part of the original author. It’s very possible that such an event was not even foreseen by the MS17-010 author, given the difficulty of monetizing ICS intrusions — at least without attracting significant law enforcement attention.”

Designer's Guide to IloT Security

How to fit all the security puzzles together

By Nitin Dahad, *European correspondent, EE Times*

We've all heard of the internet of things (IoT) and the industrial internet of things (IIoT). We know that the two are different because IoT is commonly used for consumer usages and IIoT is used for industrial purposes.

But how does a professional group like the Industrial Internet Consortium (IIC) actually define the IIoT?

The group sees IIoT as a system that connects and integrates operational technology (OT) environments, including industrial control systems (ICS), with enterprise



systems, business processes, and analytics.

These IIoT systems differ from ICS and OT because they are connected extensively to other systems and people. And they differ from IT systems in that they use sensors and actuators that interact with the physical world, where uncontrolled change can lead to hazardous conditions.

The benefits of IIoT are the ability of sensors or connected devices, as part of a closed-loop system, to collect and analyze data and then do something based on what the data reveals. The very connectivity, however, also grows the risk of attack — and increasingly cyberattacks — by those who may want to bring down the system.

One of the [many](#) projects under a Department of Energy (DoE) program to reduce cyber-incidents is being driven by Intel, looking at enhanced security for the power system edge.

Because grid edge devices communicate with each other directly and through the cloud, the research is developing security enhancements to emphasize interoperability and

provide for real-time situational awareness.

First this needs to be done in the form of a secure gateway for brownfield, or legacy, power system devices, then as an internal field-programmable gate array (FPGA) upgrade designed as part of greenfield, or present-day, devices.

The goal is to reduce the cyberattack surface in a way that doesn't impede the normal functioning of the critical energy delivery functions.

Sven Schrecker, chief architect of IoT security solutions at Intel and co-chair of the security working group at the IIC, said that security should not be the sole consideration when designing and deploying devices for IIoT systems, but developers should be thinking more broadly about five overall key factors:

- safety
- reliability
- security
- privacy
- resilience

Resources

IEC 62443 — How to achieve strong industrial security

**IEC 62443 on-demand webinar
How to Achieve the Highest Levels of Industrial Security**

Get your free whitepaper: “Strong industrial security with the IEC 62443 standard”

Smart factories call for robust security: OPTIGA™ TPM in industrial grade

Security for smart factories — learn more

While design engineers might have to implement security elements into a chip, software, or platform, they may not necessarily be aware of how their work fits into their company's bigger-picture security policies. "The security policy must be authored by both the IT team and the OT team together so that everyone knows what device is allowed to talk to what," Schrecker said.

Building a chain of trust

A common theme is to establish a security policy and chain of trust from the outset and then ensure that it is maintained through design, development, production, and the entire life cycle of a device. Trust must be built into the device, the network, and the entire supply chain.

Haydn Povey, a board member of the IoT Security Foundation and CEO and founder of Secure Thingz, said that security needs to be addressed at four levels:

- CxO level
- security architect
- development engineer
- operations manager

The development or design engineers are the ones that need to take the company's security policy. They may also define factors such as how to identify and verify that a product is theirs and how to securely provide software and hardware updates and implement this in chips or software.

The fourth part of the chain is where OEMs are involved in manufacturing products for IIoT networks or in deployment of those products. Here, the production or operations manager needs to ensure that every electronic component has its own unique identity and can be securely authenticated at every point in the supply chain.

In discussing the lack of a chain of trust in hardware and software, Robert Martin, senior principal engineer at the MITRE Corpo-

ration and a steering committee member of the IIC, said, "Connected industrial systems have so many different tech stacks."

In fact, he cautioned, "A small change in a microprocessor can have an unintended impact on the software running on it. If we recompile the software, run it on a different OS, it will work differently, but no one will be accountable for software failures resulting from the changes."

He added, "Compare this to the building trade, where you would be penalized for making changes that affected safety — there's regulation, certification. But we just don't have the same regime in software-based technologies."

Design considerations for IIoT security

So where does one start with designing security for the IIoT, and what design considerations must be looked at?

Various industry guidelines exist, such as the [IIC's IoT Security Framework](#), together

with its [manufacturing profile](#) providing details for implementing the Framework in the plant, or the [National Institute of Standards and Technology Cybersecurity Framework](#).

The main task for the design engineer is determining how to translate a security policy or security framework into the design and life cycle management of a device that forms all, or part of, an IIoT endpoint.

The considerations range from enabling devices with unique identities to being able to protect the device, identify an attack, recover from it, remediate it, and patch the device.

“The process is no different from safeguarding other systems,” said Chet Babla, vice president of solutions for IoT devices at Arm. “We need to think about security from the ground up.”

He explained, “The first part is the analysis — what are the threat vectors and what are you trying to protect?”

Arm introduced its own platform security

architecture (PSA) last year to support developers of IoT devices. Babla says that the PSA is device-agnostic, as the company is trying to encourage the industry to think about security.

Analyze, architect, implement

The PSA framework comprises three stages — analyze, architect, and implement. “Analysis is the core part of what we are trying to stress,” said Babla.

This means, for example, conducting a threat model analysis, and Arm has introduced three analysis documents for common use cases in asset trackers, water meters, and network cameras. This analysis is essential and echoed by others.

MITRE Corp.’s Martin commented, “We need to start talking about what the potential weaknesses in the hardware are and be able to emulate attack patterns and make test cases.”

Design engineers need to think about the

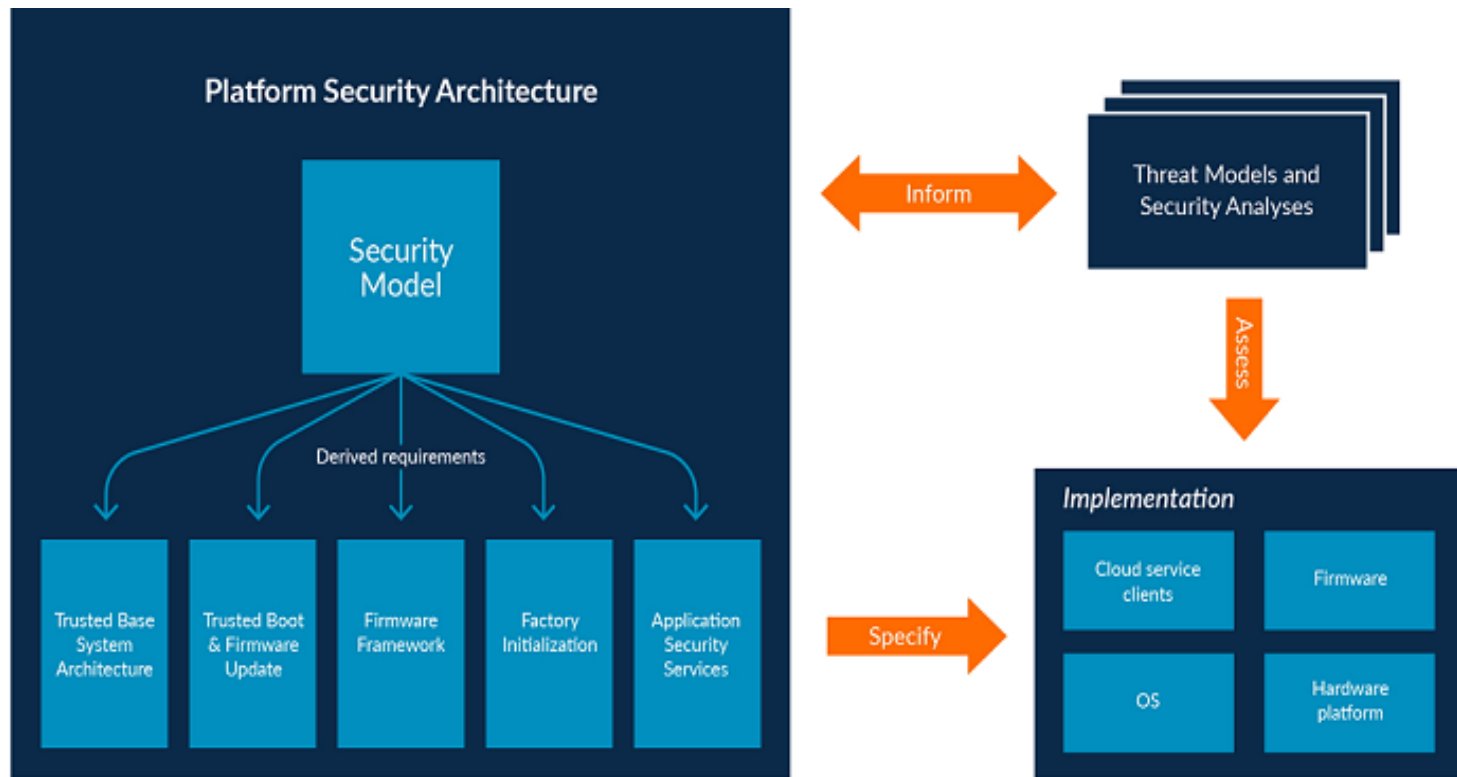
whole ecosystem, from chip to cloud, in terms of implementing a system that comprises an immutable device or one with a non-changeable identity; enabling trusted boot; and ensuring that over-the-air (OTA) updates and authentication can be carried out securely. “Then you can think about mitigation in silicon, the access points, and the cloud,” said Babla.

Life cycle management

An important consideration that some say differentiates IIoT security from traditional IoT security concerns is the life cycle management (LCM).

Secure Thingz’s Povey said that LCM has an impact on when software updates or configuration changes are deployed to IIoT devices. In IIoT environments, the connected devices, sensors, and control systems will typically not, or should not, be connected to the open internet.

Therefore, some type of device LCM con-



Arm's platform security architecture (PSA) framework encourages designers to first consider the threats and then look at design and implementation. (Image: Arm)

control layer needs to be part of IIoT devices. This can be complex software for the reporting, configuration, and management of devices.

But security needs vary in an IIoT network depending on the endpoints in the system

because it may comprise both an offline internal network of non-IP-based smart controllers and some type of protection or isolation from the external internet, and there will also be wireless devices and sensors that may or may not be IP-based.

All of the endpoint devices need to be managed and controlled in an industrial system as part of the LCM function.

This allows the industrial factory to control the introduction, configuration, and management of endpoint devices/products that are added to the internal factory network.

Some high-level objectives of a security solution for IIoT are:

- Product endpoint authentication (device, sensor, control system): Is the endpoint product authentic and not a clone? Provides traceability back to product manufacturer, manufacturing date, and any other pertinent information.
- Product endpoint configuration and usage control: secure management and configuration control of the endpoint with various rights and usage models controlled or limited
- Secure control of the endpoint control state

- Maintenance of the endpoint: This includes secure software updates.
- Secure communications between control systems and the endpoints and secure storage of control system data.
- Advanced security protection: intrusion detection and security monitoring

Fundamental to enabling this endpoint product security at a lower level are the following requirements for the endpoint device:

- Immutable device identity: The device has to have a non-changeable/protected identity, which must be verifiable by cryptographic means. This allows a product to identify itself and authenticate who made it, pertinent dates, and other information.
- Immutable root of trust (RoT): Besides the device identity, there also are RoTs provisioned into the product. These include low-level secure boot loaders, certificates, and asymmetric key pairs

that allow the device to support bilateral authentication and enable secure software updates. Some parts of the RoT require that keys and other items are protected in some type of secure storage area so that they cannot easily be extracted from the product.

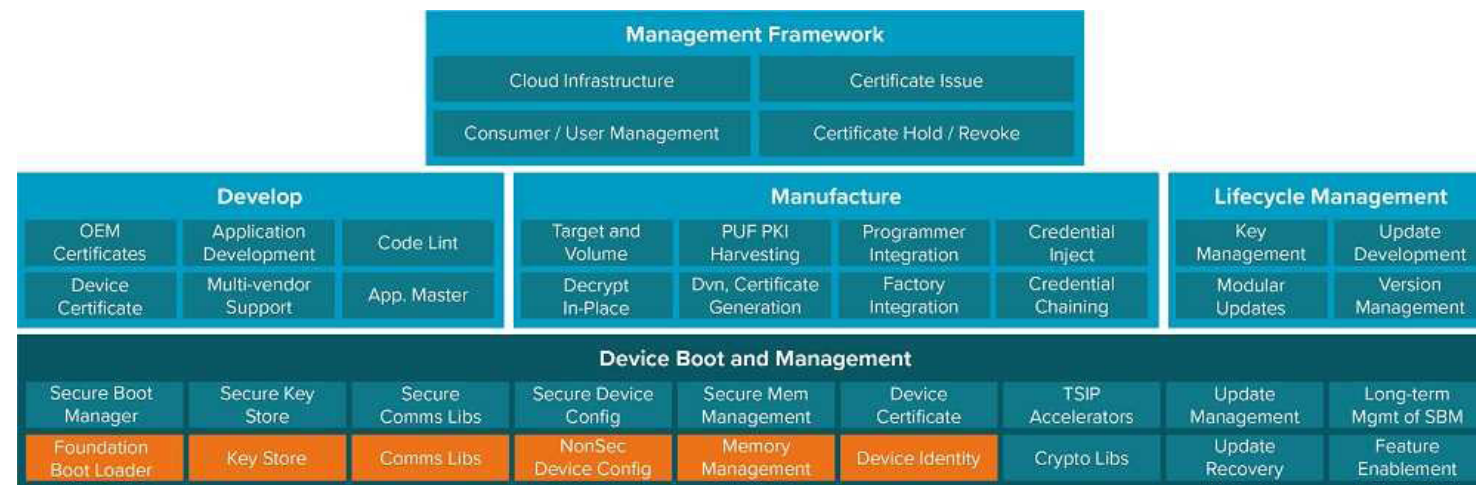
- Immutable secure boot loader: Some type of low-level secure boot manager that verifies all firmware and configuration updates to the device/product before they are applied. Only the secure boot manager can install and apply low-

level configuration updates to the endpoint device/product.

- LCM software/services: Some type of low-level LCM control services that enables management of the endpoint product, including software updates and configuration changes

Security enclaves

Secure Thingz's Povey said, "Device procurement is influenced by factors like enabling standard mechanisms to push out updates, how the update will be stored on



Considerations when designing for security at the device level as well throughout the life cycle of an IoT device.

(Image: Secure Thingz)

an edge device, and the device and memory resource impacts.”

He added, “You need to think about the security enclaves, where to hide the secrets and the base keys, how to watermark the device.” Engineers should consider a development environment that allows these factors to be considered independently from silicon vendor and architecture.

The general industry consensus is that the secure elements really need to be in hardware to ensure embedded trust because chip-level encryption can be enforced and protected.

Rich Carpenter, general manager for control and edge platforms for GE Power, Automation, and Controls, said, “We try

to establish the root of trust that starts at the hardware level. Our ‘defense-in-depth’ approach requires that if a compromise occurs, it won’t propagate through the system.”

He says that GE uses off-the-shelf trusted platform modules (TPMs) and is working with Intel and AMD processors.

Expectedly, Intel is focused on the hardware approach. Schrecker said, “Having a hardware root of trust is vital. Hardware-based identity is burned into the system and having identity at the chip level means it can be tracked. But the key is to be able to ensure that the chips are genuine, to be able to authenticate, and for updateability.”

He adds that hardware-based security

doesn’t replace software security; it just augments it.

In summary, the key considerations when designing for security in IIoT devices are making the devices immutable, being able to provide trusted and secure boot, and managing device security over the entire life cycle, which includes OTA software updates and patches.

In case of an attack, there needs to be a way of accurately identifying the device, reinstating it to a previous known good state, and then being able to resolve the issue at the point of attack as appropriate. Taking these principles into account is a good start for going to the next step — hardware implementation.

Embedding Security at the Edge

Lay of the land for IIoT security solutions

By Nitin Dahad, *European correspondent, EE Times*

As safety and reliability have become critical in IIoT systems, embedding the highest levels of trust is now essential.

So while the PC connected to the network might have traditionally been the point at which security was enabled, the trust anchors now need to be located down at the hardware level, in silicon, and as close to the edge as possible — even in the sensors.

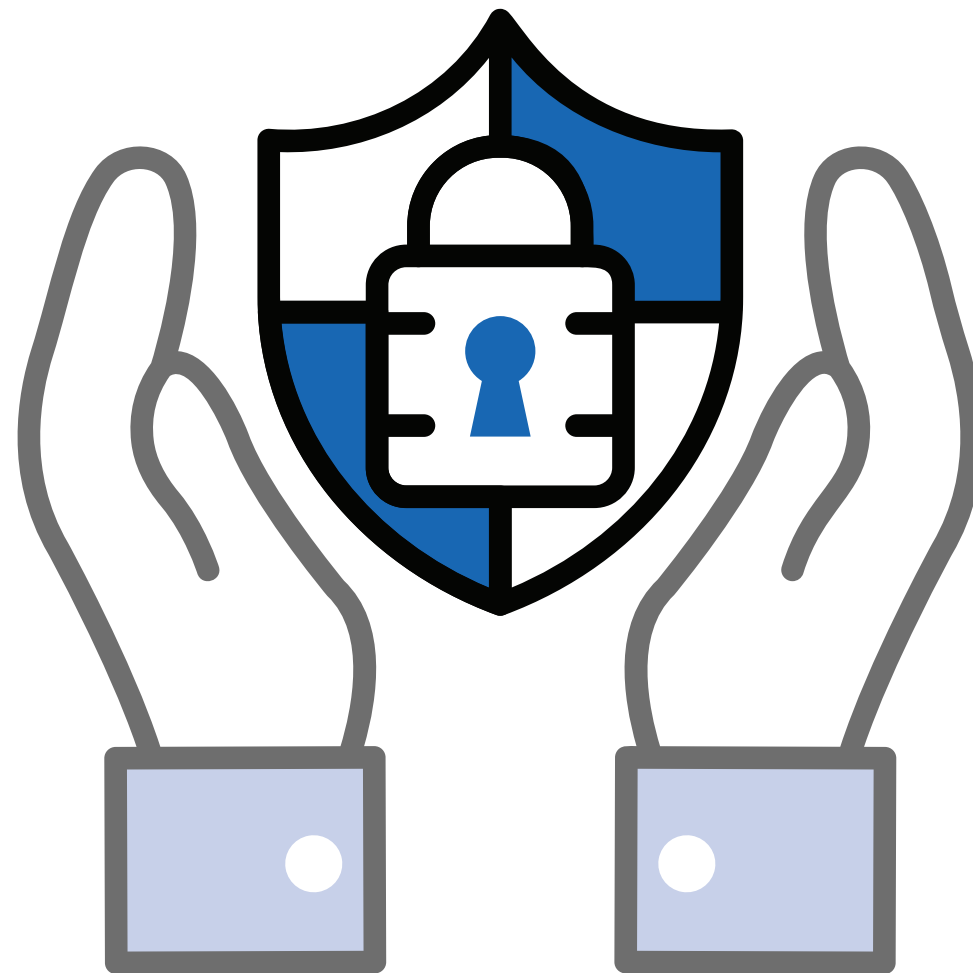
In the following pages, we will offer you the lay of the land for IIoT security so-

lutions. First, we start with the chip level, where there are several options.

Infineon

Infineon provides the OPTIGA™ family of hardware security controllers with software containing the cryptographic keys and certificates, plus the drivers and software libraries. It enables engineers to integrate security into their systems.

For simple authentication, the Trust B product is used for IoT edge devices and “dumb” sensors that simply supply



information; the device supports smaller cryptographic key sizes that might be used for authenticating a spare part or a battery, for example.

Trust E addresses the security requirements of devices that are more feature-rich and need a higher level of security; it is a turnkey solution with OS, Applet, and complete host-side integration support and up to 3-kB memory.

The company's main solution for high-end security for industrial automation is the [OPTIGA™ Trust X](#). It's a discrete hardware security module built on elliptic curve cryptography (ECC) with 256-bit, AES128, and secure hash algorithms (SHA)-256 encryption.

It enables functions like mutual authentication, secured communication, data store protection, life cycle management, secured updates, and platform integrity protection and has up to 10-kB user memory.

Steve Hanna, senior principal at Infineon,

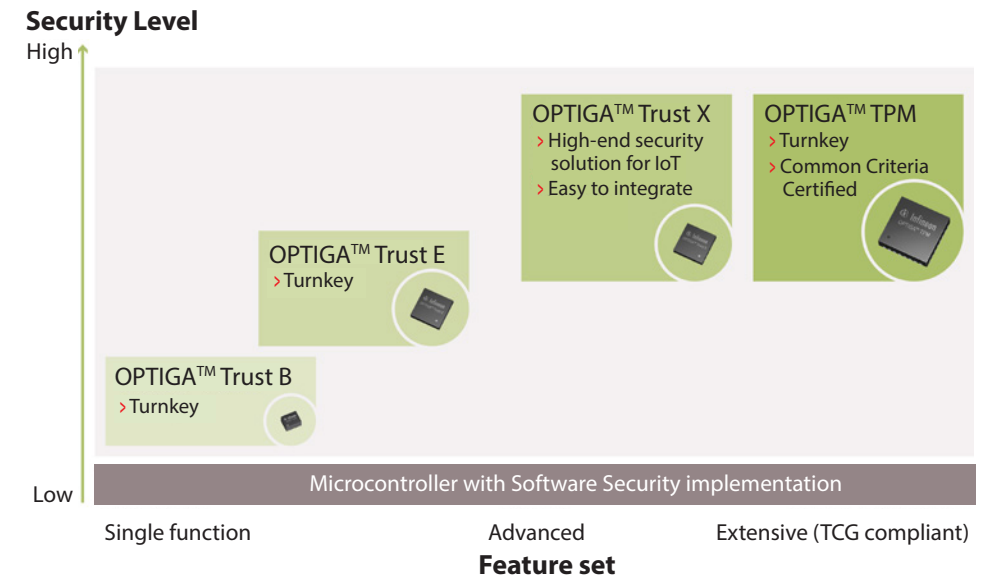
says that Trust X is designed for environments in which the main CPU may not have full-fledged power, and asymmetric and symmetric cryptography must be offloaded from the main CPU.

Two of the world's largest industrial equipment manufacturers use Infineon's security chips at the IIoT gateway and the endpoints. "Industrial IoT is very much a complete system, so you need to look at the endpoint, the gateway, and the cloud," he said.

"Our chips are designed to be easily integrated into the system as well as cloud-based architectures. The gateway is an ideal choke point to implement security without touching the edge, so our customers are integrating security chips into [both] gateways and endpoints."

NXP

NXP introduced its [A71CH](#) secure element embedded solution for IoT devices, edge



Infineon OPTIGA™ family of security controllers. (Image: Infineon Technologies)

nodes, and gateways earlier this year.

Designed to secure peer-to-peer or cloud connections, the chip comes with the required credentials pre-injected for autonomous cloud onboarding and peer-to-peer authentication.

It provides a root-of-trust (RoT) solution at the silicon level with security functionalities such as encrypted key storage, key generation, and derivation to protect private information and credentials for mutual authentication.

The A71CH is designed for use in indus-

trial applications, including sensor networks, gateways, and IP cameras.

Like many solutions on the market, it claims a “plug-and-trust” approach supporting easy integration of security and cloud onboarding — for example, through host libraries and a development kit compatible with different NXP microcontroller and microprocessor (MCU and MPU) platforms such as Kinetis and i.MX.

It also collaborates with data I/O for high-volume personalization capabilities for any quantities beyond the capacity of NXP’s trust provisioning service.

Sami Nassar, vice president of cybersecurity solutions at NXP, said that the industry has moved on from software-based security and traditional methods of securing an industrial environment, such as isolation of the network.

“In the past, protection was through isolation, private networks rather than public, and an isolated command center,” said Nassar.

“That’s not enough anymore — software ends up being on the inside of these networks, so isolating the network is no good. Hardened protection introduced at the chip level enables strong authentication at the gateway, and as time passes, we’ll see more security at the endpoint, too.”

Asked about regional differences in the implementation of IIoT security based on NXP’s experience, Nassar noted, “The smart grid and smart metering market is the most serious about security and embedding security. In public utilities, it depends on government influence and the different political systems.”

He added, “The U.S. was first to think about it, but China has been the first to implement, with millions already using the embedded security functions. However, in Europe, where you have more standards, much of the security aspects are just guidance; therefore, adoption is slower.”

Microsoft TCPS

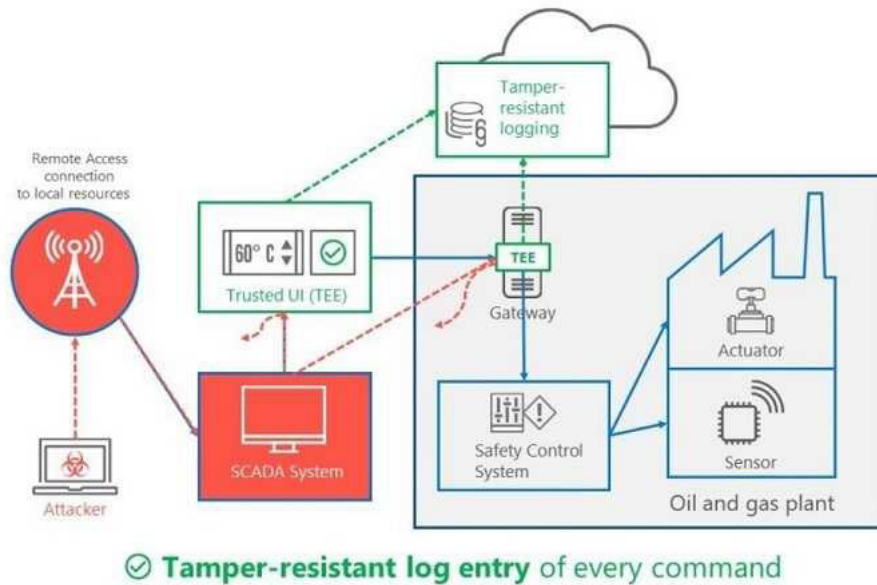
Most vendors addressing security for the IIoT emphasize the need to take a holistic approach across the development flow and life cycle of a device.

Microsoft added its flavor in this with the announcement earlier this year of its [trusted cyber-physical systems](#) (TCPS) solution to protect critical infrastructure. Microsoft says that its TCPS creates a security pattern to process critical data throughout distributed systems.

Data in execution must be protected by trusted execution environments (TEEs) such as Intel SGX, Arm TrustZone, and SecureElements. Components must not only use secure protocols and protect keys and data at rest; they must also perform all critical operations in a TEE that is protected from public cloud hosts and OS vendors.

The overarching security principle for TCPS is that the solution owner/opera-

Microsoft's trusted cyber-physical systems (TCPS) solution to protect critical infrastructure, shown here applied in a typical industrial environment. (Image: Microsoft)



tor must not lose control over their critical systems.

Microsoft likens the TCPS approach of preventing unauthorized access and control of connected devices to the transition in the credit card industry that is embedding a secure element (SE) in the cards instead of magnetic strips.

The SE-based solution establishes an end-to-end trusted connection between the

content on the credit card and the credit card's processing center, preventing any other system in the path from accessing confidential information, cloning a card, or replaying messages.

Secure Thingz

Establishing an RoT as the foundation for a secure supply chain is another way of presenting the case for building security into

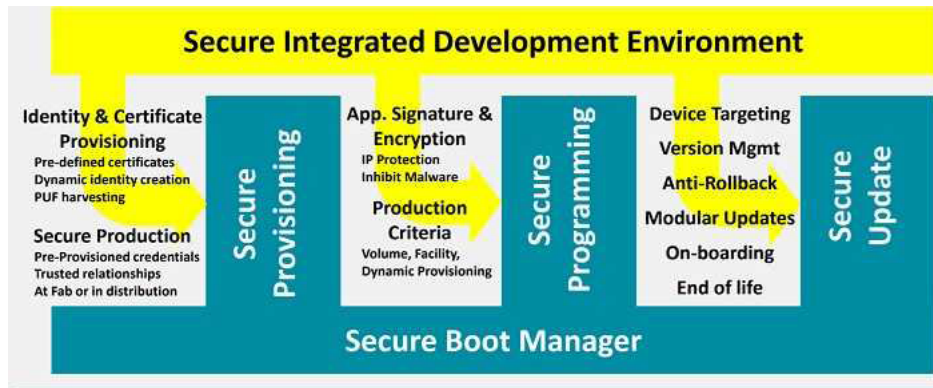
the IIoT environment.

Secure Thingz says that a secure development flow needs to start with the correct security frameworks and a secure boot manager (SBM), which is injected into MCUs at “birth” alongside the provisioning of secure keys and certificates that provide a robust RoT.

Its key product is the Secure Deploy Architecture, a high-security framework ensuring simple management of critical intellectual property within the development process. It also offers secure key management targeted for development, manufacturing, and applications.

The architecture can be integrated into Tier 1 programming and manufacturing systems, thus eliminating overproduction and counterfeiting through constrained device programming.

It includes firmware that is integrated with the core cryptographic hardware to ensure that credentials — keys and certificates

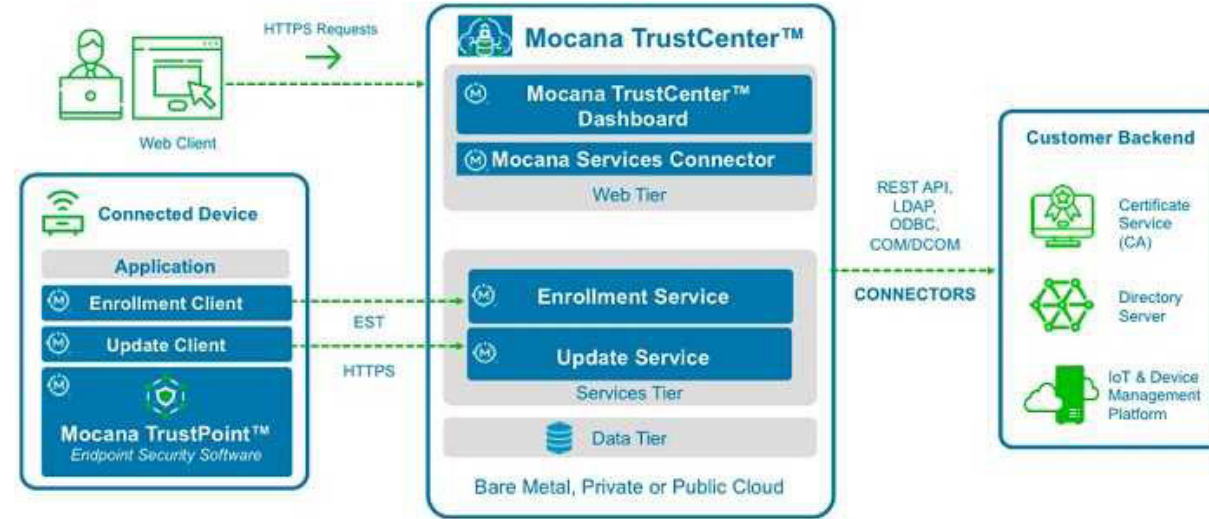


Secure Thingz's secure integrated development environment. (Image: Secure Thingz)

— can be managed and stored correctly across the critical phases of factory provisioning, operational startup, and patching and remediation cycles.

Earlier this year, the company introduced its Embedded Trust security development environment. It integrates security into the workflow by defining identity, thus simplifying security development, streamlining secure manufacturing, and enabling the management of devices across their life cycles.

The Embedded Trust solution includes a scalable SBM that leverages secure device hardware to provide low-level secure services and foundation update management.



Mocana's TrustCenter platform for managing security across the life cycle of IIoT and industrial control devices includes its own TrustPoint endpoint protection software. (Image: Mocana)

Mocana

Providing device-level security with over 70 chipsets, Mocana has its own endpoint protection software: TrustPoint. It is part of its TrustCenter platform to manage security across the life cycle of IIoT and industrial control devices.

The company recently announced support for Trusted Platform Module (TPM) 2.0 features on IIoT devices.

TPM is an international standard for a secure crypto-processor, a dedicated microcontroller designed to secure hardware

through integrated cryptographic keys.

TPM was conceived by the Trusted Computing Group, a computer industry consortium, and was later standardized by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2009 as ISO/IEC 11889.

Some key features of Mocana's support for TPM 2.0 are support for advanced ciphers, including ECC and 256- and 512-bit SHA 2, and multiple ownership of keys, separating owners for the TPM endorse-

ment key for signing/attestation from the storage root key with support for endorsement hierarchies and storage hierarchies.

It also offers better seeding for entropy — seeding and reseeding of a non-deterministic pseudorandom number generator with an entropy source internal to the TPM’s cryptographic boundary to ensure a high degree of randomness for key generation.

GE Automation: a user perspective on IIoT security

One of the prominent companies involved in providing industrial automation systems is GE Power Automation and Controls. So what are the factors that they are focused on with some of their key customers?

Rich Carpenter, general manager for control and edge platforms for GE Power Automation and Controls, said, “We try and establish a root of trust that starts at the hardware. We are working with Intel and AMD to get that at the chip level.”

Earlier this year, the company introduced its PACSystems “outcome-optimizing” [RX3i CPx400 series of controllers](#), which provides near-real-time dynamic adjustment of industrial controls based on the data that they have collected in connected industrial systems.

These currently use 1.2-GHz AMD G Series quad-core processors and standard TPMs along with secure, trusted, and measured boot.

Carpenter said that they are looking to move to eight- and then 16-core processors. The controllers are designed to perform in a range of applications including water, metro, industrial steam, and chemical.

For existing installations and for collecting data securely, it uses [Mini Field Agent technology](#) based on an 800-MHz Arm Cortex-A8 processor.

Carpenter emphasized the need for a defense-in-depth approach to apply cyber-defense capabilities at every level.

The hardware RoT should form the foun-

dation of the security constructs in the control system.

Hence, GE features TPM technology in all of its controllers, which stores the private keys for all GE-signed boot firmware, ensuring that only GE-authenticated firmware will run on the hardware. “We believe a connected device is more secure than a non-connected device because we can easily identify if there is a problem,” he said.

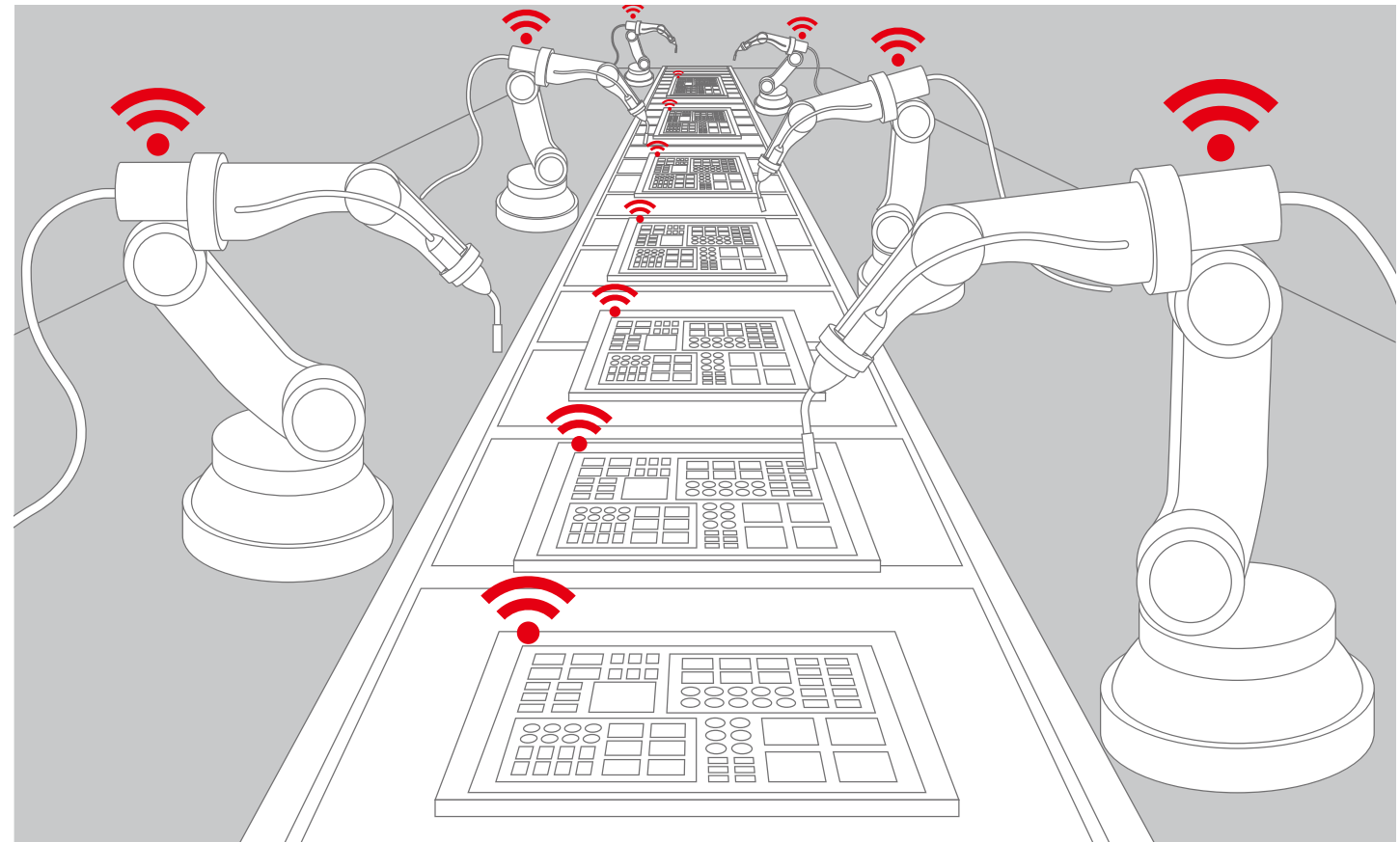
GE’s mini field agent for secure industrial internet connectivity. (Image: GE)



Protecting communication within the smart factory and to the cloud: Infineon presents the world's first TPM 2.0 for Industry 4.0

MUNICH, Germany — Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY) presents the world's first Trusted Platform Module (TPM) specifically for industrial applications at this year's Hannover Messe (Hannover, Germany, April 1–5, 2019). The OPTIGA™ TPM SLM 9670 protects the integrity and identity of industrial PCs, servers, industrial controllers, or edge gateways. It controls access to sensitive data in key positions in a connected, automated factory as well as at the interface to the cloud.

The TPM acts as a vault for sensitive data in connected devices and lowers the risk of data and production losses due to cyberattacks. Users' benefit is not limited to security only, as TPMs also help to shorten time to market and reduce costs for industrial applications. Through the use of Infineon's audited and certified TPMs, manufacturers of industrial devices can achieve higher security levels



of the IEC 62443* standard and accelerate their certification processes. Furthermore, they can cut costs for maintenance of the devices through secured remote software updates.

The OPTIGA™ TPM SLM 9670 fully meets the TPM 2.0 standard of the Trusted Computing Group and is certified by an independent test lab in accordance with Common Criteria.** With a service life of 20 years and the ability to update the firmware on the chip, the TPM is able to cope with long-term security risks that may be encountered in an industrial environment. The chip boasts an extended temperature range of -40°C to 105°C and meets the stringent requirements of

industry in terms of robustness and quality as it is qualified according to the industrial JEDEC JESD47 standard.

Availability

The OPTIGA™ TPM SLM 9670 is manufactured at Infineon's security-certified facilities in Germany and will be available in large volumes from the second half of 2019. For more information, please go to www.infineon.com/industrial-tpm.

Infineon at the Hannover Messe

The internet of things is increasing the fields of application for the TPM. With its extensive OPTIGA™ TPM product family, Infineon offers application-specific solutions for

business PCs and routers, connected vehicles, or cloud applications.

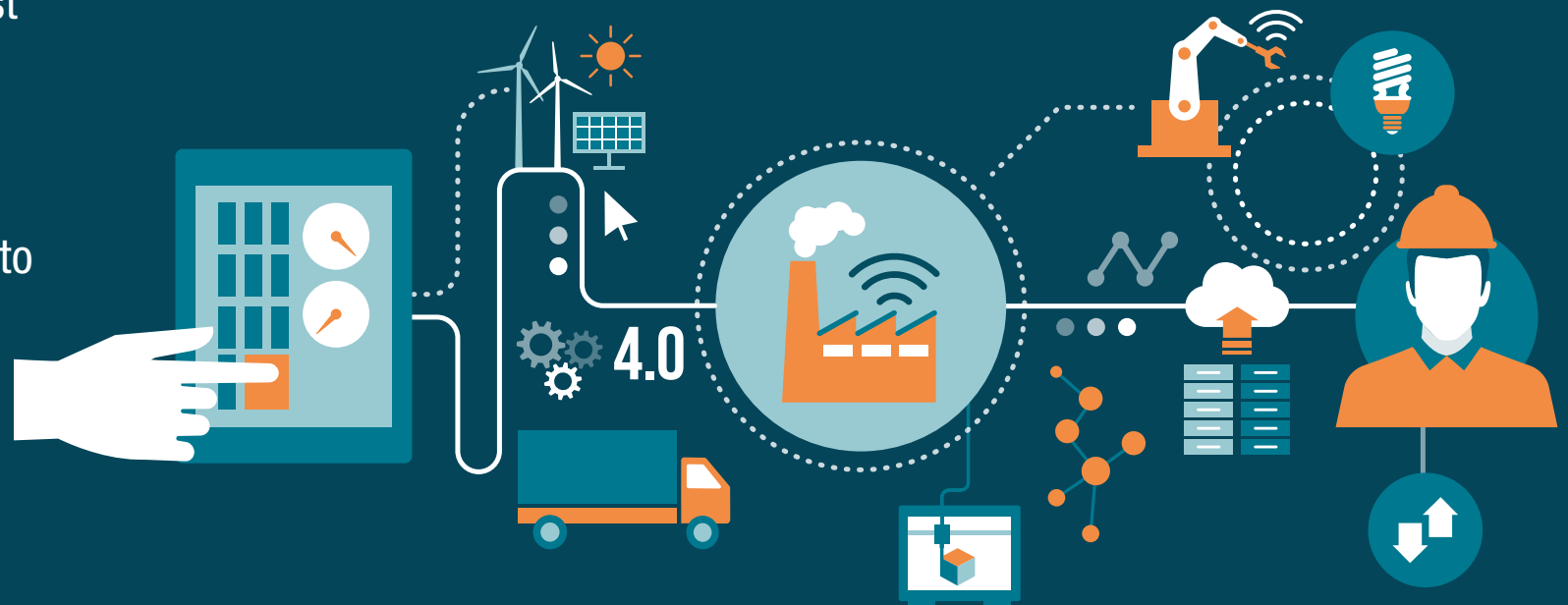
The OPTIGA™ TPM SLM 9670 will be presented for the first time at this year's Hannover Messe, the world's leading industrial show. Infineon will show various products and a demonstrator for energy-efficient and secured smart factories at the Amazon Web Services stand (Hall 6, Stand F46). This demo also includes an edge gateway, which is a perfect place for the strong security of the OPTIGA™ TPM SLM 9670 because of the gateway's central and security-critical function in industrial networks.

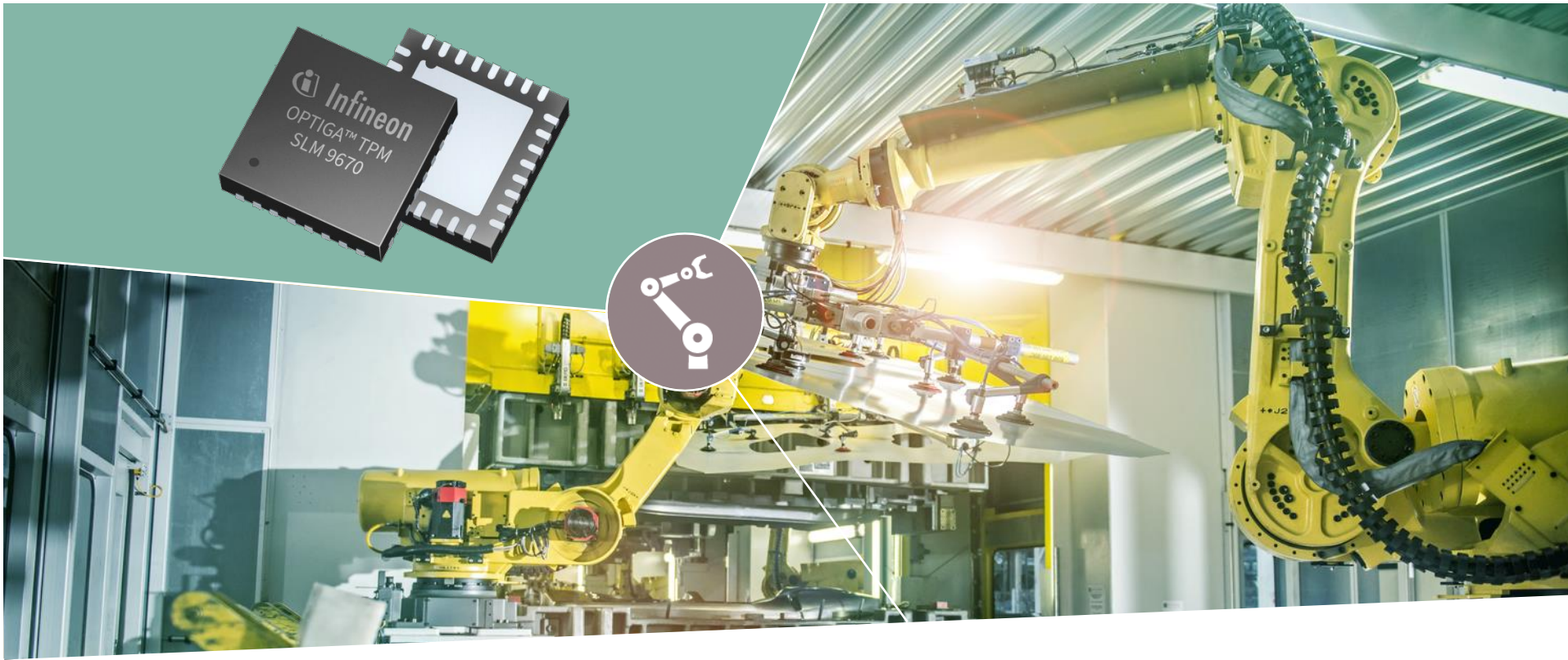
*[IEC 62443](#) is an international series of standards that defines the IT security requirements for industrial communication networks.

**Common Criteria is an international standard for computer security certification.

Maximizing Security with OPTIGA™ TPM SLM 9670

- Industrial IoT and Industry 4.0 bring many opportunities and many risks.
- To maximize the opportunities, you must understand how to minimize the risks.
- The following slides explain the most common security industrial use cases, how and when they are used, and how to implement them.







OPTIGA™ TPM SLM 9670 for Industrial Use Cases

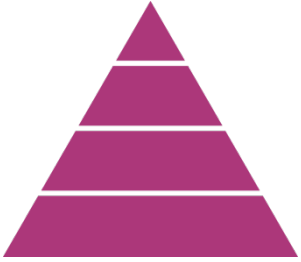
www.infineon.com/industrial-TPM

Industrial Use Cases are enabled by hardware-based security in OPTIGA™ family

	Industrial use cases enabled by hardware-based security
<p>Supervisory and Control Levels (e.g. PLC, RTU, HMI, IPC)</p> 	<ul style="list-style-type: none"> › Predictive maintenance › Remote diagnosis & service (Remote maintenance) › Counterfeit detection › Equipment-as-a-service › Cloud analysis and optimization › After-market revenues <ul style="list-style-type: none"> – Feature upgrades – Services (e.g., security) › Protecting proprietary IP 	<p>OPTIGA™ TPM SLM 9670 Tamper-resistant certified and standardized security chip enabling ...</p> <ul style="list-style-type: none"> › Digital Device ID, including Mutual authentication › Device Integrity & Secured Boot › Remote Software and Firmware updates › Secured communication › Secured storage of data and keys
<p>Field Level (e.g. Sensor, Actuator, Controller Board)</p> 	<ul style="list-style-type: none"> › Predictive maintenance › Remote diagnosis & service (Remote maintenance) › Counterfeit detection › Equipment-as-a-service › Asset tracking & inventory management › Protecting proprietary IP 	<p>OPTIGA™ Trust X</p> <ul style="list-style-type: none"> › Tamper-resistant security chip enabling: <ul style="list-style-type: none"> – Mutual authentication – Secured communications – Secured storage – Remote SW & FW updates – Integrity verification › Streamlined offering

Secured Communication

Industrial Level



Description

- › Protection of communications with the cloud and within the industrial networks
- › Mutual authentication and confidential data exchange with integrity & replay protections
- › Critical keys securely stored in secured Hardware
- › Needed to secure many customer use cases: predictive maintenance, remote maintenance, equipment-as-a-service, cloud analysis and optimization, after-market revenues, feature upgrades, and protecting proprietary IP

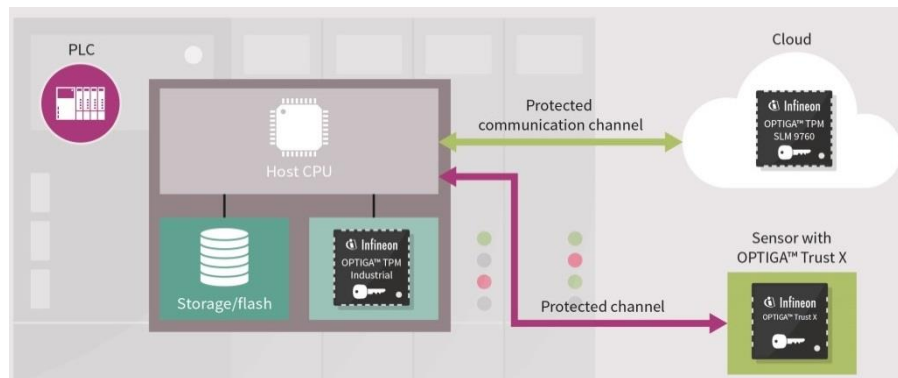
Addressed Threats

- › Malicious access or control by unauthorized parties
- › Loss of keys and ability of authentication (clones, false data, invalid access)
- › Extraction of proprietary IP

Customer Benefits

- › Increase safety and reliability
- › Enable new online business models
- › Contribute to company reputation and image

Solution Approach



- › Secured communication library adapted to use keys in secured OPTIGA™ Hardware for first authentication phase
- › Subsequent data transfer and bulk encryption use performant session keys derived from the authentication key

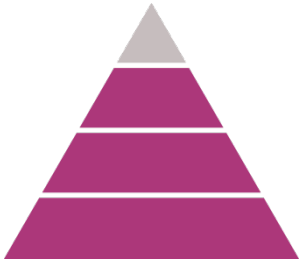
Solution Benefits of OPTIGA™

- › Tamper resistant key storage
- › Turn-key solution
- › Security certified (TPM only)
- › Industrial temperature range
- › Extended lifetime

- › Long-term authentication keys are kept in the secured OPTIGA™ Hardware

Remote Software & Firmware Updates

Industrial Level



Description

- › Secured update of SW or FW in supervisory, control, and field devices
- › Remote feature activation & deactivation
- › Enabling safe fixes for bugs and vulnerabilities
- › Updates signed by OEM, verified by device
- › Detect and recover from improper updates
- › Distribute updates via networks, USB, etc.
- › Needed to secure many customer use cases: remote maintenance, equipment-as-a-service, after-market revenues, and feature upgrades

Addressed Threats

- › Malicious or manipulated updates
- › Reverse engineering of updates
- › Rollback attacks
- › Unauthorized feature access

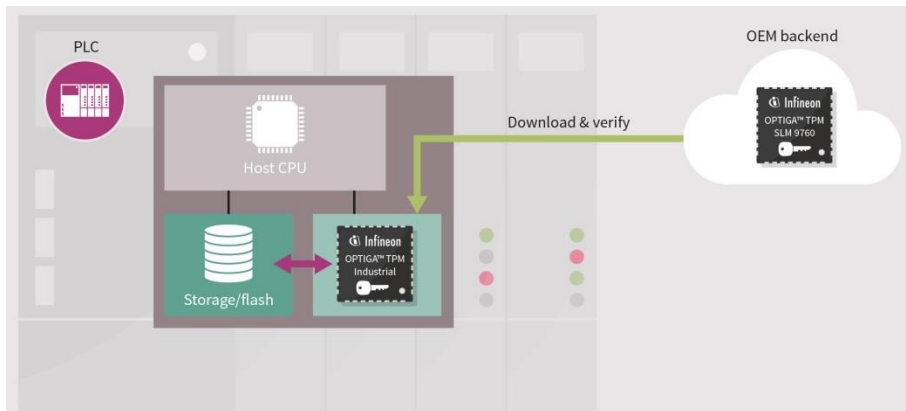
Customer Benefits

- › Reduce update costs
- › Enable new business models
- › Contribute to company reputation and image
- › Ease Software improvements
- › Increase safety and reliability

Solution Benefits of OPTIGA™

- › Tamper resistant key storage
- › Turn-key solution
- › Security certified (TPM only)
- › Industrial temperature range
- › Extended lifetime

Solution Approach

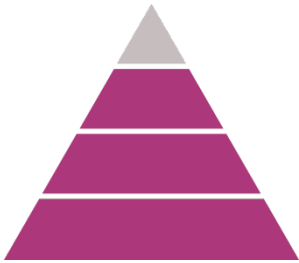


- › Updates and feature licenses are loaded into the device

- › Long-term keys are kept in the OPTIGA™ Hardware and used to verify and/or decrypt updates and feature licenses
- › Proper installation of updates and feature licenses can be verified locally and remotely via policies and attestation

Device Identity

Industrial Level



Description

- › Providing a strong, unique digital device identity
- › Enabling one-way or mutual authentication
- › Fundamental Requirement of IEC 62443 for all devices (supervisory, control, field, etc.)
- › Basis for most other security use cases such as secured communications
- › Needed to secure many customer use cases: remote maintenance, equipment-as-a-service, counterfeit detection, after-market revenues, asset tracking and inventory management

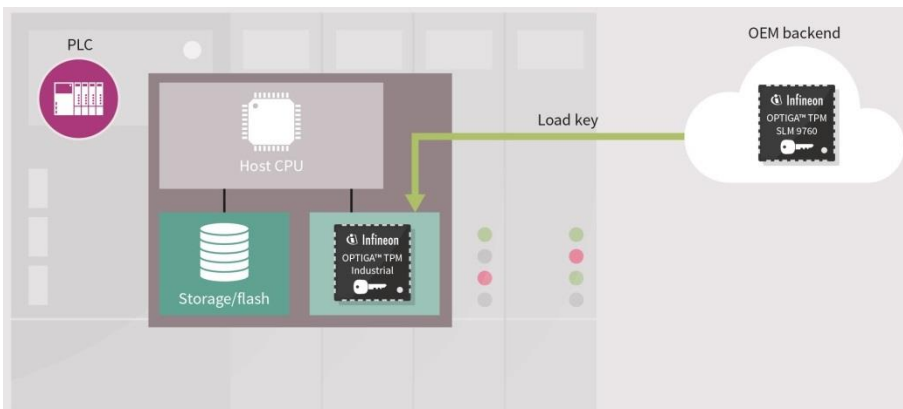
Addressed Threats

- › Unauthorized access and control
- › Impersonation and forgery
- › False data, improper commands
- › Cloning and counterfeiting
- › Unauthorized access to IP & data

Customer Benefits

- › Reduce update costs
- › Enable new business models
- › Contribute to company reputation and image
- › Ease Software improvements
- › Increase safety and reliability

Solution Approach



- › More keys and certificates may be added securely later
- › Device identity keys and certs are used to authenticate the device and establish secured communications

Solution Benefits of OPTIGA™

- › Tamper resistant key storage
- › Turn-key solution
- › Security certified (TPM only)
- › Industrial temperature range
- › Extended lifetime
- › Supports X.509 & other standards

- › Device identity keys and certs are loaded into the OPTIGA™ Hardware during Infineon manufacturing