CYBERSECURITY FOR BUILDING CONTROL SYSTEMS

The importance of ISA 62443 certification

ALL CONNECTED SYSTEMS CAN FACE CYBER THREATS

Cyber threats continue to evolve and escalate, and there are no indications to show that this trend will slow in the years to come. It's no longer only computers or IT networks that are at risk.Operational technologies (OT) and OT networks, such as building controls, are increasingly at risk – in part because they may provide easier access to an organization's full IT network.

At times, it may seem that no system or data of any kind is safe from would-be attackers – whether it's the "script kiddie" who just wants to show what they can do or bad actors seeking to extort financial gain from their next cyber attack. Nation-state attackers can be particularly insidious and have multiple objectives: stealing intellectual property to benefit their own economy; disrupting sensitive infrastructure such as the energy sector; or pursuing other political and military objectives by causing disruption.

From mobile devices to building automation, we all depend on the digital products and connected systems that we use and take for granted, but how can we be sure whether they're resilient to cyber-attacks? For instance, how do system engineers and building integrators know which products are better protected when designing a new hospital or upgrading critical infrastructure such as a power plant?

History shows that no system can ever be absolutely secure – yet some protections and methodologies are safer than others. The challenge is to identify the better options.

DEFENDING AGAINST CYBER THREATS

When planning a new building system or infrastructure project, how do you identify the secure technology options?

It starts with the selection of components that the project requires, which is where an essential question that needs to be asked: Was this technology designed with cybersecurity in mind from the start? Or were cyber concerns simply an afterthought, tacked on just as the product was about to be marketed?

Greater transparency is required to make this selection process more fact based and meaningful – rather than leaving integrators and customers to interpret clever sales phrasing that cannot always be qualified or justified.

Cybersecurity is a fundamental necessity for all technology development. It needs to start from the beginning of the design process, and it should be incorporated into all aspects of the product's functionality and purpose.

Yet this design process is usually hidden from the person seeking to select the key elements for their system plans.

This is why it is essential to have an objective standard for measuring and verifying the maturity and security of a product's development lifecycle. When a secure development lifecycle is verified to follow best practices and established standards, customers can have confidence that those products have passed rigorous security review and testing.

This in turn builds trust with customers and users, by confirming that the product developer has:

- Identified security weaknesses and vulnerabilities early in the design.
- Managed product risk, using thoughtful analysis to identify risks, and then prioritize and remediate these risks.
- Complied with the latest versions of numerous evolving security standards and regulations.
- Measured their progress against secure-development standards and used those metrics to advance the security maturity of their development lifecycle.

ISA/IEC 62443 STANDARDS		
GENERAL	**ISA-62443-1-1**	Concept and models
	ISA-TR62443-1-2	Master glossary of terms and abbreviations
	ISA- 62443-1-3	System security conformance metrics
	ISA- TR62443-1-4	IACS security life-cycle and use-cases
POLICIES AND PROCEDURES	**ISA-62443-2-1**	Requirements for an IACS security management system
	ISA-TR62443-2-2	Implementation guidance for an IACS security management systems
	ISA-TR62443-2-3	Patch management in the IACS environment
	ISA-TR62443-2-4	Requirements for IACS solutions suppliers
SYSTEM	**ISA- TR62443-3-1**	Security technologies for IACS
	ISA-62443-3-2	Security risk assessment and system design
	ISA-62443-3-3	System security requirements and securty levels
COMPONENT	**ISA-62443-4-1**	Product development requirements
	ISA-62443-4-2	Technical security requirements for IACS components

SECURE DEVELOPMENT STANDARDS: ISA/IEC 62443

The design process is essential to every product's cybersecurity success – or failure. So what does a "good" design process look like?

This is a question that the technology industry itself has asked continually, which prompted the International Society of Automation (ISA) to form a team of security experts who could propose official criteria for "what good looks like" in automation technologies and control systems. The standards they created have been adopted internationally by the International Electrotechnical Commission (IEC) and are recognized by a growing number of governments worldwide.

This set of standards – known as ISA/IEC 62443 – covers the whole product lifecycle for operational technology used in automation and control systems. It has rapidly become the leading standard for establishing a product's cybersecurity within the automation and industrial sectors, and beyond.

Among the documents that make up the complete family of ISA/IEC 62443 standards (Figure 2), one focuses on the product-development process, defining how that process should account for cybersecurity in order to create a full "secure-lifecycle process" for product development. This standard is known as ISA/IEC 62443-4-1.

SECURE DEVELOPMENT LIFECYCLE PROCESS

Honeywell has relied on the ISA 62443-4-1 standard for many years as well as applicable companion standards to securely develop our building technology products.

For example, Honeywell building products also use ISA/IEC 62443-4-2 as the baseline for technical security requirements within components, and we use ISA/IEC 62443-3-3 for complete systems.

So for the integrators and customers selecting building technologies, Honeywell's adherence to the family of ISA/IEC 62443 standards can provide a high level of confidence that our products don't just claim to be cyber resilient – they've been designed, tested and validated for cyber resilience from the start.

But this raises another question: When a developer such as Honeywell claims to follow a secure development lifecycle, how can customers know whether that's true, and whether it's done effectively? We'll answer this question in the next section.

SECURE DEVELOPMENT LIFECYCLE: PROCESS CERTIFICATION

The next step in building transparency and trust is to provide evidence that companies who claim to follow a recognized process are indeed doing so.

To fulfill this need, a certification process has been defined in conjunction with U.S. and international standards bodies, including the ISA and IEC. Several independent assessment companies have been established under these auspices to independently vet companies that purport to follow the ISA/IEC 62443 processes.

The starting point is the secure development lifecycle itself, so the first certification milestone is the ISA/IEC 62443-4-1 Process Certification.

To achieve this certification, an independent assessor audits the secure development lifecycle of the company seeking the certification. The assessor conducts a deep dive into the company's defined processes and compares them against the expectations of the ISA/IEC 62443 standard. Projects are picked at random, then inspected to gather evidence that proves that appropriate processes are indeed being followed correctly. This is no short exercise – certification can take months.

If successful, ISA/IEC 62443 Process Certification is awarded, indicating that the standard is being followed to maintain a secure development lifecycle. This certification is then published on the ISASecure website to make it publicly accessible.

The Honeywell Building Technologies (HBT) division recently completed the ISA 62443-4-1 Certification process and was awarded a certificate in January 2023. The certificate can be found here.

This certification means that Honeywell customers can be assured that our products are developed in accordance with industry and international standards for cyber resilience, and that this has been confirmed by an approved independent third party.

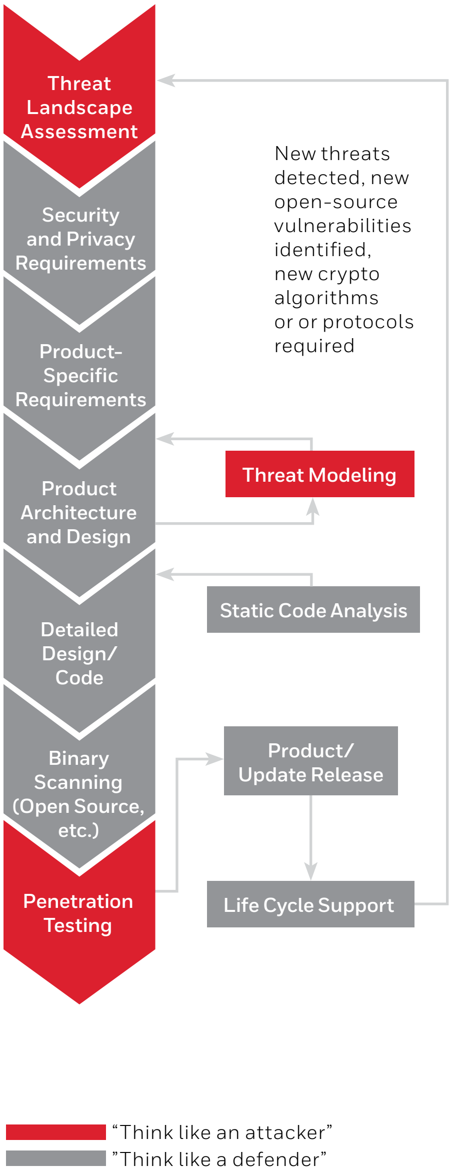
Threat Landscape Assessment
Security and Privacy Requirements
Product-Specific Requirements
Product Architecture and Design
Detailed Design/ Code
Binary Scanning (Open Source, etc.)
Penetration Testing
New threats detected, new open-source vulnerabilities identified, new crypto algorithms or or protocols required
Threat Modeling
Static Code Analysis
Product/ Update Release
Life Cycle Support
🟥 "Think like an attacker"
▬ "Think like a defender"

Figure 3: Example of a Secure Development Lifecycle based on international standards such as ISA/IEC 62443

Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308
buildings.honeywell.com

© 2023 Honeywell International Inc.

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell