IEC 62443-4-1 Supports NIST Cybersecurity Framework Based Programs

In freight rail, transit, mining, industrial or marine industries, the integration of advanced cybersecurity standards into product development processes is becoming increasingly important. This is particularly true as rail networks incorporate emerging technologies such as 5G, AI (Artificial Intelligence), and the Industrial Internet of Things (IIoT), which introduce complex security challenges. For vendors and operators serving critical infrastructure segments, the ability to align to common standards and frameworks reduces supply chain related cybersecurity risk.

Wabtec's product cybersecurity program supports operator cybersecurity programs in critical infrastructure. Spearheaded by our Chief Product Security Officer, Wabtec's product cybersecurity team is on a mission to develop products that support the resilience of the vital industries we serve. They establish secure design practices and provide tools that incorporate cybersecurity in each phase of product development and life cycle management in alignment to industry recognized practices. Wabtec's IEC 62443-4-1 certified product cybersecurity program provides well-defined benchmarks throughout the development lifecycle. This standards-driven approach enables a common cybersecurity baseline for Wabtec products.

The National Institute of Standards and Technology Cyber Security Framework (NIST CSF) is a voluntary set of guidelines, standards and best practices that help organizations improve their cybersecurity posture. Adoption of NIST CSF among critical infrastructure operators, enables those organizations to manage and reduce cybersecurity risks. NIST CSF is structured around six core functions: Identify, Protect, Detect, Respond, Recover and Govern. For companies leveraging NIST CSF, deploying products developed in compliance with IEC 62443-4-1 can complement the overarching goals of NIST CSF based security programs. This includes methodologies for managing and securing operational technology (OT) systems, monitoring potential threats, and implementing appropriate security controls based on established security levels.

Selecting vendors with IEC 63443-4-1 certification supports operators' internal cybersecurity programs tied to NIST CSF. The table below illustrates the alignment between the broader cybersecurity objectives of NIST CSF and the product security life cycle related practices and requirements outlined in IEC 62443-4-1:

NIST CSF 2.0 Function	IEC 62443-4-1:2018 Practice	IEC 62443-4-1:2018 Key Elements (Sections)	Summary of Key Elements
Identify	Practice 1	SM-6: File integrity (5.8) SM-8: Controls for private keys (5.10) SM-9: Security requirements for externally provided components (5.11) SM-10: Custom developed components from third-party suppliers (5.12) SM-11: Assessing and addressing security-related issues (5.13) SM-13: Continuous improvement (5.15)	Defining a security environment for products, guiding design decisions and configuration.
	Practice 2	SR-1: Product Security Context (6.2) SR-2: Threat model (6.3)	
Protect	Practice 1	SM-4: Security expertise (5.6) SM-7: Development environment security (5.9)	Incorporating secure design principles and a multi-layered security approach to protect against threats.
	Practice 2	SR-3: Product security requirements (6.4) SR-4: Product security requirements content (6.5) SR-5: Security requirements review (6.6)	
	Practice 3	SD-1: Secure Design Principles (7.2) SD-2: Defense in Depth Design (7.3) SD-4: Secure design best practices (7.5)	

NIST CSF 2.0 Function	IEC 62443-4-1:2018 Practice	IEC 62443-4-1:2018 Key Elements (Sections)	Summary of Key Elements
Detect	Practice 1	SM-11: Assessing and addressing security-related issues (5.13)	Providing well defined product security requirements and identifying potential vulnerabilities to enhance detection capabilities.
	Practice 3	SR-3: Product security requirements (6.4)	
	Practice 6	DM-1: Receiving notifications of security-related issues (10.2)	
	Practice 8	SG-3: Security hardening guidelines (12.4)	
Respond	Practice 6	DM-2: Reviewing security-related issues (10.3) DM-3: Assessing security-related issues (10.4) DM-4: Addressing security-related issues (10.5) DM-5: Disclosing security-related issues (10.6)	Developing protocols for managing and responding to security incidents, crucial for maintaining system integrity.
Recover	Practice 7	SUM-1: Security Update Qualification (11.2) SUM-4: Security update delivery (11.5) SUM-5: Timely delivery of security patches (11.6)	Furnishing relevant security updates and patches, critical for system recovery and ongoing protection post-incident.

NIST CSF 2.0 Function	IEC 62443-4-1:2018 Practice	IEC 62443-4-1:2018 Key Elements (Sections)	Summary of Key Elements
Govern	Practice 1	SM-2: Identification of responsibilities (5.4) SM-3: Identification of applicability (5.5) SM-5: Process scoping (5.7) SM-9: Security requirements for externally provided components (5.11) SM-10: Custom developed components from third-party suppliers (5.12)	Maintaining a governance framework that emphasizes strategic decision making and leadership involved in security, aligning with organizational risk management.

Operator efforts to secure critical infrastructure rely on supply chain security. Through selecting products developed in compliance with IEC 62443-4-1, customers are equipped with solutions that meet their required security levels and effectively address the core functions of the NIST CSF.

To learn more about product cybersecurity at Wabtec visit https://www.wabteccorp.com/product-cybersecurity.