Life Is On | Schneider Electric

Jon Boyens
Manager
Security Engineering & Risk Management Group
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

May 27, 2021

Mr. Boyens,

Schneider Electric welcomes the opportunity to contribute to the government's implementation of the recent Executive Order on Improving the Nation's Cybersecurity. The National Institute of Standards and Technology (NIST) plays a critical role in this implementation and we appreciate NIST's willingness to engage with industry on these important issues. Attached you will find our submission in response to the **Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security**. At Schneider Electric, we take the cybersecurity of our products, systems, and customers very seriously and we look forward to engaging with you on this topic in the future. For technical questions regarding our submission, please contact Gabriel Faifman, Global Cybersecurity Architect & Innovation Manager, at Gabriel.Faifman@se.com.

Our submission includes responses to each of the prompts stated below:

1. *Criteria for designating "critical software."*
2. *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.*
3. *Guidelines outlining security measures that shall be applied.*
4. *Initial minimum requirements for testing software source code.*
5. *Guidelines for software integrity chains and provenance.*

Our responses include direct references to the ISA/IEC 62443 suite of standards. Additionally, and in support as a founding member, Schneider Electric is supporting the International Society of Automation (ISA) Global Cybersecurity Alliance's response to this same request. Both responses align to our commitment to be an international steward of security practices as they pertain to Industrial Control Systems and Operational Technology. We believe that the ISA/IEC 62443 suite of standards significantly aids in the adoption and implementation of the security best practices referenced in the President's Executive Order on Improving the Nation's Cybersecurity.

Sincerely,

Patrick. M. Ford

Patrick M. Ford
Regional Chief Information Security Officer, Americas Region
Schneider Electric

1) ***Criteria for designating "critical software."***

The best practices for operational technology (OT) Service Providers, described by the **ISA/IEC 62443-2-4** standard, presents a set of security capabilities that an organization needs to have while designing a secure automation solution. Having the capability to translate a business, production, and safety risk into technical and procedural capabilities that a system needs is one of the basic principles referenced within (**ISA/IEC 62443-2-4-SP.03.01BR** referring in its Rationale to **ISA/IEC 62443-3-2**).

Performing the risk translation includes the capacity to identify and manage security vulnerabilities and associated threats for all the associated components of the automation solution and its authorized data storage points, data flows, and control actions by design (**ISA/IEC 62443-2-4-SP.03.09BR/10BR**) including its safeguarding requirements.

Then, those commands or essential functions (**ISA/IEC 62443-3-3-SR.5.2RE(2)/RE(3); ISA/IEC 62443-4-2-CR.2.10/CR.7.1**), parameters and associated data have to be properly protected either by built-in technical capabilities (**ISA/IEC 62443-4-2)**, integrated system capabilities (**ISA/IEC 62443-3-3**) and/or procedural/organizational capabilities(**ISA/IEC 62443-4-1; ISA/IEC 62443-2-4 and ISA/IEC 62443-2-1**).

2) Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.

The **ISA/IEC 62443-4-1** describes component or system development lifecycle requirements related to cybersecurity for those components or systems intended for use in an OT environment and provides guidance on how to meet the requirements described for each element. When a Product Supplier is using an **ISA/IEC 62443-4-1** compliant process, enables a Service Provider to follow the **ISA/IEC 62443-2-4** compliant practices to integrate, configure, validate, commission, and maintain an intended security posture by design.

3) Guidelines outlining security measures that shall be applied to the federal government's use of critical software.

ISA/IEC 62443-2-4 and **ISA/IEC 62443 3-3 together provide guidance to fulfill this section of the EO.** The **ISA/IEC 62443-2-4** provides compliant practices to integrate, configure, validate, commission, and maintain an intended security posture by design. The **ISA/IEC 62443 3-3** provides compliant practices for system integrity, data confidentiality, restricted data flow, network segmentation, and timely response to events.

4) Initial minimum requirements for testing software source code.

ISA/IEC 62443 4-1 outlines processes for security testing (automated and manual) as part of overall product lifecycle management, to include, security verification & validation, management of security relates issues and security update management. **ISA/IEC 62443 4-1** advocates using a risk-based approach to mitigating vulnerabilities, which can include patching as well as compensating controls, especially when patches cannot be made available.

5) Guidelines for software integrity chains and provenance.

The **ISA/IEC 62443-4-1-SM-9 Security Requirements for externally provided components** requires software development organizations to have a process to identify and manage security risks of all externally provided components used within the product. The rationale of that requirement provides the

guidance for compliance, referring to the Defense in Depth strategy, identifying all components as well as their security context, rigor applied to the component implementation, verification/validation, notifications, etc.
Examples of work items that would satisfy some elements of this requirement include:

- identifying known vulnerabilities in specific versions of open source software components and updating the version of the open source components to the version that fixes the vulnerability.
- evaluating the compliance of vendors of commercial off the shelf (COTS) components to this document or a similar SDL standard.
- employing compensating mechanisms for known vulnerabilities on COTS or open source components (such as static code analysis).
- It is recommended that there be an inventory of components from third party suppliers in order to facilitate defect management.

Additionally, Schneider Electric fully supports managing supply chain risk by ensuring integrity and authenticity. In regards to provenance, the definition and elements need to be clearly defined as it can range from simply country of origin of the manufacturer to many elements (e.g. developer location, coding standards, chain of custody) for all layers (third-party components including open source software and commercial components). The software development industry rarely captures this meta-data in the construction of a software or firmware package. For open-source, such as standard TCP/IP stacks, there are thousands of developers globally who contribute to the source and no provenance information has been captured. For commercial products that were previously built (whether legacy or active development), the provenance information would have to have been captured at the time of "code commit". It cannot be reconstructed some-time after the build. Depending on the definition of provenance, the entire documentation set could be hundreds of pages for a single release.

Schneider Electric recommends characterizing provenance as the "build country of origin" and to the primary vendor (one-layer / parent). Vendors cannot attest to the provenance of third-party components except when the information is declared by the commercial or third-party component. Except in the very rare cases where one-hundred percent of code is written in-house, we must assume that nearly every product globally has code written by developers from every country. The traceability and provenance for millions of lines of code is not achievable unless captured at the absolute beginning with no external components or libraries included.

Tables and Figures

Table 1: ISA/IEC 62443-4-1

Value	Req ID	# of Reqs
SM – Security Management	SM-xx	13
SR – Specification of security reqs	SR-xx	5
SD – Secure by design	SD-xx	4
SI – Secure Implementation	SI-xx	2
SVV – Security Verification & Validation	SVV-xx	5
DM – Mgmt of security related issues	DM-xx	6
SUM – Security update management	SUM-xx	5
SG – Security Guidelines	SG	7
SM – Security Management	SM-xx	13
SR – Specification of security reqs	SR-xx	5
SD – Secure by design	SD-xx	4

Source: Schneider Electric adaptation of IEC/ISA 62443 suite of standards.

Table 2: ISA/IEC 62443-2-4

Value	Req ID	# of Reqs
Solution staffing	SP.01.XX	11
Assurance	SP.02.XX	7
Architecture	SP.03.XX	24
Wireless	SP.04.XX	6
SIS	SP.05.XX	12
Configuration management	SP.06.XX	4
Remote access	SP.07.XX	5
Event management	SP.08.XX	8
Account management	SP.09.XX	17
Malware protection	SP.10.XX	8
Patch Management	SP.11.XX	12

Source: Schneider Electric adaptation of IEC/ISA 62443 suite of standards.

Table 3: ISA/IEC 62443-3-3

Value	Req ID	# of Reqs
FR 1 – Identification and authentication control	SR.01.XX	13
FR 2 – Use control	SR.02.XX	12
FR 3 – System integrity	SR.03.XX	9
FR 4 – Data confidentiality	SR.04.XX	3
FR 5 – Restricted data flow	SR.05.XX	4
FR 6 – Timely response to events	SR.06.XX	2
FR 7 – Resource availability	SR.07.XX	8

Source: Schneider Electric adaptation of IEC/ISA 62443 suite of standards.

Table 4: ISA/IEC 62443-4-2

Value	Req ID	# of Reqs
FR 1 – Identification and authentication control	CR.01.XX	14
FR 2 – Use control	CR.02.XX	13
FR 3 – System integrity	CR.03.XX	14
FR 4 – Data confidentiality	SR.04.XX	3
FR 5 – Restricted data flow	SR.05.XX	4
FR 6 – Timely response to events	SR.06.XX	2
FR 7 – Resource availability	SR.07.XX	8
SAR – Software application	SAR.X.X	2
EDR – Embedded device	EDR.XX.XX	8
HDR – Host device	HDR.XX.XX	8
NDR – Network device	NDR.XX.XX	12

Source: Schneider Electric adaptation of IEC/ISA 62443 suite of standards.

Table 5: Mapping of NIST Cybersecurity Framework to ISA/IEC 62443 and NERC CIP v5

Function Identifier	Function	Category Identifier	Category	IEC 62443	NERC CIP v5
ID	Identify	ID.AM	Asset Management	:2-4 – SP.06.02/SP.01.x	CIP-003-5
		ID.BE	Business Environment	:2-4 –SP.01.x	CIP-003-5 CIP-004-5
		ID.GV	Governance	:2-4 –SP.01.x :2-1 -ORG-02	CIP-003-5
		ID.RA	Risk Assessment	:2-4-SP.02.01	CIP-003-5
		ID.RM	Risk Management Strategy	:2-1/2-4/3-3/4-1	CIP-003-5
		ID.SC	Supply Chain Risk Management	IEC 62443-2-4	CIP-003-5 CIP-004-5
PR	Protect	PR.AC	Identity Management and Access Control	:3-3 –SR02.04/ SR.02.07/SR.03.08x :2-4 -SP.08.x	CIP-007-5
		PR.AT	Awareness and Training	:2-4 –SP.01.x	CIP-003-5 CIP-004-5
		PR.DS	Data Security	:2-1 –DATA01-04 /CRYPT-01-03 :2-4 – SP.05.09x/ SP.03.10x :3-3 – SR.03.01RE(1) /SR.04.03	CIP-011-1
		PR.IP	Information Protection Processes and Procedures	:2-1:ORG-02 /NET-12 :2-4: SP.03.08x :3-3- SR 7.6	CIP-003-5
		PR.MA	Maintenance	:2-4 (complete) :3-3 -SR.04.02	CIP-003-5 CIP-010-1
		PR.PT	Protective Technology	:2-4-SP.08.x :3-3-SR01.01 – SR.02.07	CIP-007-5
	Detect	DE.AE	Anomalies and Events	:2-4-SP.08.x	CIP-008-5
		DE.CM	Security Continuous Monitoring	:3-3-SR02.08-SR02.12 /SR03.09/SR.06.01/SR.06.02 :2-4- SP.08x	CIP-008-5
		DE.DP	Detection Processes	:2-4-SP.07.x/SP.06.x	CIP-008-5
RS	Respond	RS.RP	Response Planning	:2-4-SP.02.x/SP.12.x :2-1-ORG-08/10/02	CIP-009-5
		RS.CO	Communications	:2-4-SP.02.x/SP.12.x :2-1-ORG-x	CIP-009-5
		RS.AN	Analysis	:2-4-SP.02.x/SP.12.x :2-1-ORG-x	CIP-009-5
		RS.MI	Mitigation	:2-4-SP.02.x/SP.12.x :2-1-ORG-x	CIP-009-5
		RS.IM	Improvements	:2-4-SP.02.x/SP.12.x :2-1-ORG-x	CIP-009-5
RC	Recover	RC.RP	Recovery Planning	:2-4-SP.12.x :2-1-ORG-x	CIP-009-5
		RC.IM	Improvements	:2-4-SP.12.x :2-1-ORG-x	CIP-009-5

		RC.CO	Communications	:2-4-SP.12.x :2-1-ORG-x	CIP-009-5

Source: Schneider Electric mapping of the NIST Cybersecurity Framework, IEC/ISA 62443 suite of standards, and NERC CIP v5.