



Cybersecurity for Industrial Operations

Danish Standards Cyberday 2026

SIEMENS

The Intention behind the legislation

NIS2



CRA



MR



Understanding the EU Cybersecurity Trifecta



NIS2 –
Accountability



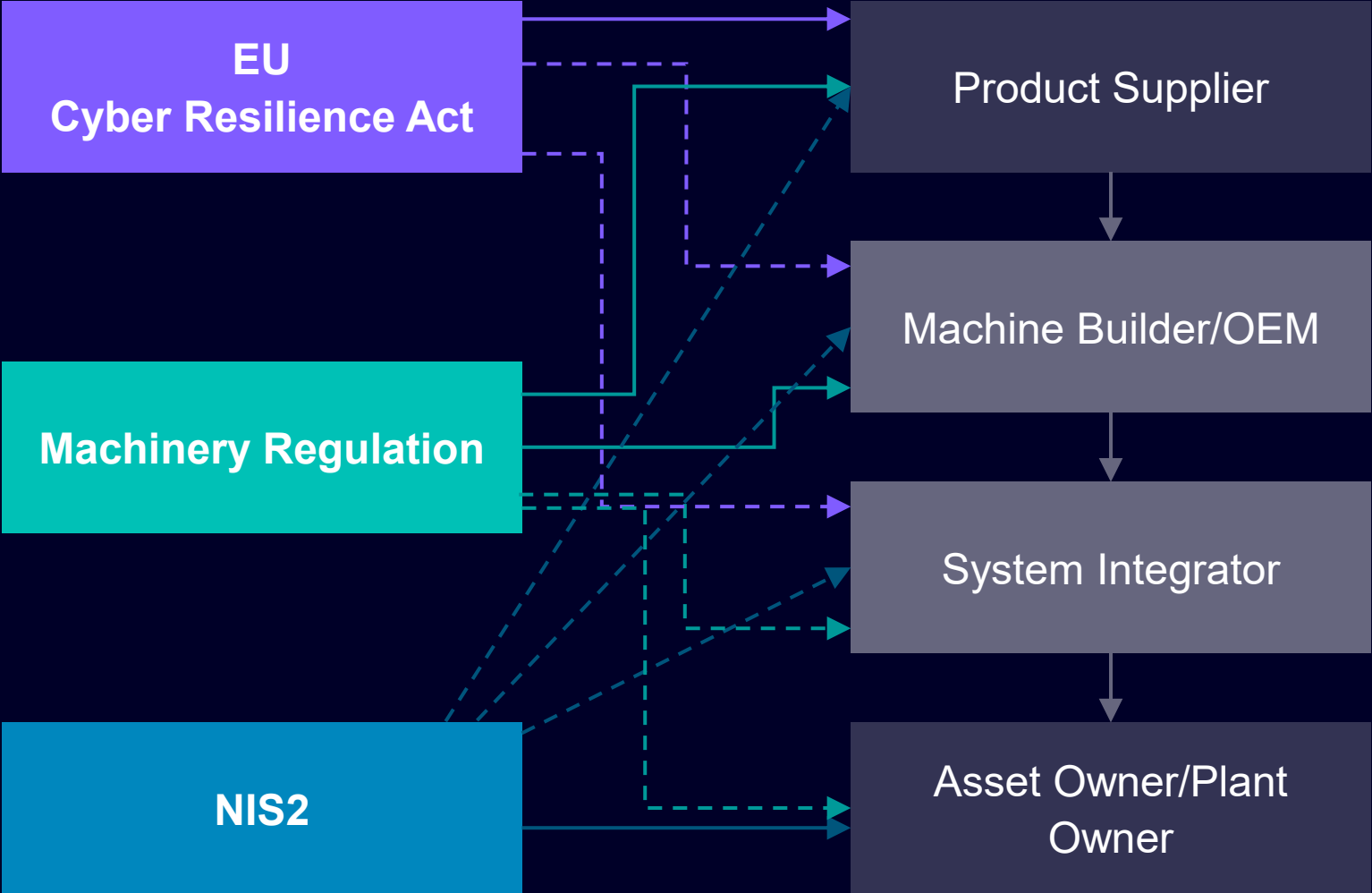
CRA –
Compromise?



Machine
Regulation –
Real Danger



The New Normal in OT cybersecurity



Mapping of IEC 62443 series to the EU Cybersecurity Trifecta

The EU Cybersecurity Trifecta



Machine Regulation
Security requirements

EN 50742
App. B



Cyber Resilience Act
For Operational Technology



NIS2
Security measures for Operational Technology

SAMSIK

no 1:1 match – more requirements in CRA!

IEC 62443-3-3

IEC 62443-4-2

EN IEC 62443-3-3

EN IEC 62443-4-1

EN IEC 62443-4-2

IEC 62443-2-1

IEC 62443-3-3

CRA Obligations

Security Capabilities

- Secure by default
- Protect from unauthorized access
- Data integrity and confidentiality
- Resilience against DDoS
- Limit attack surface
- Mechanisms to securely update ...

Lifecycle Process

- Cybersecurity risk assessment
- Provisioning of updates
- Defined support periods ...

Vulnerability Handling

- Regular testing
- Publicly disclose vulnerability info
- Provide contact address ...

Documentation

- Internal technical documentation (compliance, test results,...)
- Info and **instructions to users** (intended purpose, environment, secure configuration...)

Reporting

- ...of actively exploited vulnerabilities
- ...of **severe** incidents having impact on the security of the product

Conformity Assessment

- Depending on product classification: **self-declaration** alone or inclusion of **notified body**



Evaluate product portfolio: Due-Diligence



Based on Windows Embedded CE

Customer questions about: Due-Diligence?

During the transition period before the CRA applies, manufacturers will not be able to check whether third-party components are compliant with the CRA. This does not prevent manufacturers from integrating such components, and they should exercise **due diligence through** other means (see also entry 4.4.2 What is the appropriate level of due diligence?).

If I buy 50 panels before CRA applies and keep using them in my product with digital elements, am I breaking the law?

Source: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions>

IEC 62443-4-2

Part 4-2: Technical security requirements for IACS components

Entry type: Manual Entry ID: 109977121, Entry date: 11/27/2024

Configuration of SCALANCE products to cover the functional range of IEC 62443-4-2

SCALANCE XR-500

4.1 Security architecture

Entry
Edition

FR = Foundational Requirement

Product
Document

The "Integration" column
C: The requirement is covered by the product
S: The requirement is covered by the product and a technical feature of the product

Display
PDF

Security
In order to continue

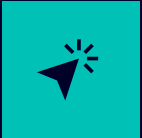
Number	
Identification and authentication	
CR 1.1	Human user identification and authentication
CR 1.1 RE1	Unique identification and authentication

Configuration of SCALANCE products to cover the functional range of IEC 62443-4-2

4.2 FR 1 – Identification and authentication control (IAC)

4.2.1 CR 1.1 – Human user identification and Authentication

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.1	By default, the product requires authentication via password for every human user interface (SSH, HTTPS or console port) each time a user logs on. All other interfaces are deactivated by default. The password for the user can be configured at: Security >> Users >> Passwords (CM WBM: 6.7.3 / CM CLI: 12.1.2) Security >> Users >> Passwords (CM WBM: 6.7.3 / CM CLI: 12.1.2)
Reaching SL 2 – 4	CR 1.1 RE1	Additionally required: To reach SL 2, the SCALANCE X device must additionally use an external RADIUS server for unique identification and authentication



IEC 62443-4-1

Part 4-1: Secure Product Development Lifecycle Requirements

ZERTIFIKAT ♦ CERTIFICATE ♦ CERTIFICADO ♦ CERTIFICAT



Product Service

CERTIFICATE
No. IITS2 128627 0001 Rev. 00

Holder of Certificate: **Siemens AG**
DI FA
Gleiwitzer Straße 555
90475 Nürnberg
GERMANY

Certification Mark:


Product Type: Industrial IT Security

Model(s): **SIMATIC S7-1500 Controller Family**
(Applicable from Firmware Version 3.1 and later)
Software Controller
(Applicable from Firmware Version 30.1 and later)

Tested according to:
IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003C:2024 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 713318447-04
Valid until: 2027-10-23

Date, 2024-10-28


(Stefan Würth)

Page 1 of 1
TUV SUD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany



ZERTIFIKAT ♦ CERTIFICATE ♦ CERTIFICADO ♦ CERTIFICAT



Product Service

CERTIFICATE
No. IITS2 059855 0004 Rev. 00

Holder of Certificate: **Siemens AG**
DI PA DCP
Gleiwitzer Straße 555
90475 Nürnberg
GERMANY

Certification Mark:


Product Type: Industrial IT Security

Model(s): Industrial Security Appliance SCALANCE SC-600
(SC 622, SC 626, SC 632, SC 636, SC 642 and SC 646)

Tested according to:
IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 713300122-04
Valid until: 2026-11-22

Date, 2023-12-07


(Michael Hermes)

Page 1 of 1
TUV SUD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany



Page 9

SIEMENS

Contact



Marc Nirari Kako Brændstrup

Siemens A/S Lokation: Runevej 2A
8210 Aarhus, Danmark

E-mail marc.braendstrup@siemens.com