Security Frameworks

For Industrial Applications – Brief Overview

weLOTec
a byte smarter

IEC 62443

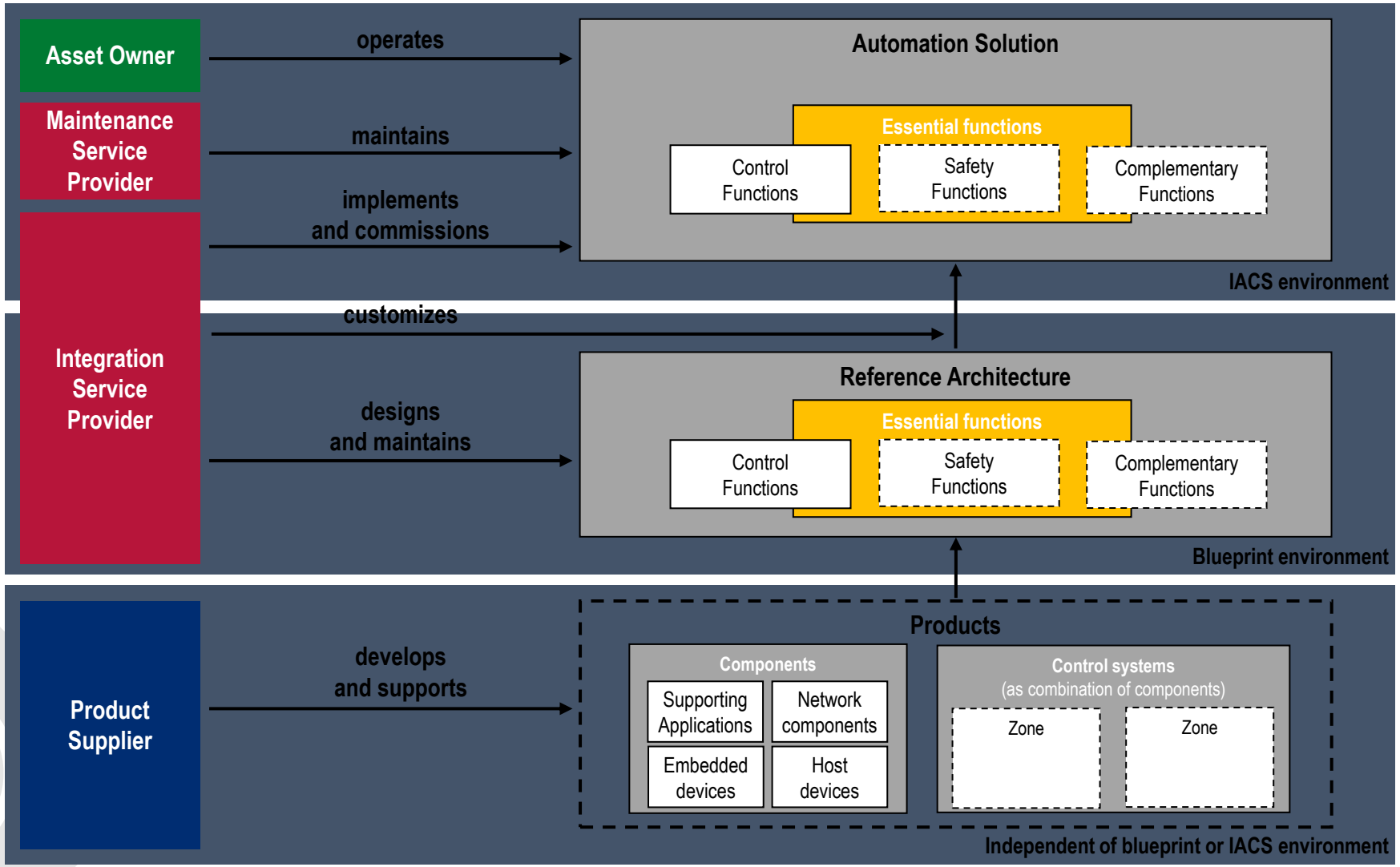
Parts related to roles

IEC 62443
Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidan-ce for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owner		

- Asset Owner
- Service Provider
- Product Supplier

IEC 62443



Applicable Standards

- IEC 62443-2-1 Edition 2
- ISMS (e.g. ISO/IEC 27001, NIST CSF)

Applicable Standards

- IEC 62443-2-4
- IEC 62443-3-3

Applicable Standards

- IEC 62443-4-1
- IEC 62443-4-2
- IEC 62443-3-3

Examples from the IEC 62443-4-2 (Product)

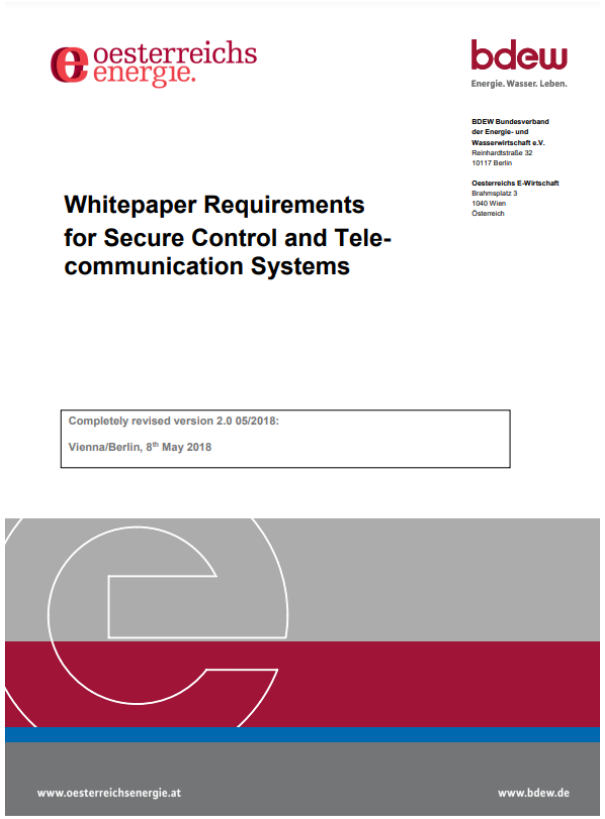
13.9 EDR 3.14 - Boot Process Integrity

- Embedded devices must verify the integrity of the firmware, software, and configuration data required for the boot process before applying them at boot.

7.10 CR 3.8 Session integrity.

- Components shall provide mechanisms to protect the integrity of communication sessions including:
  (a) The ability to override the validity of session identifiers after user logout or other type of session termination (including browser sessions).

Additional Cyber Security Frameworks perspective



https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/

The European Cybersecurity Act (Regulation (EU) 2019/881) entered into force on 27 June 2019. The core elements of this Regulation include a permanent mandate for the European Union Agency for Cybersecurity (ENISA), accompanied by the introduction of a uniform European certification framework for ICT products, services and processes. These are to be certified according to various criteria and assigned the predefined security levels of 'low', 'medium' and 'high'.

Following the publication of the proposed Regulation in September 2017, the Federal Office for Information Security (BSI) contributed in-depth support to the negotiations and consultations conducted in the drafting committees. These contributions helped ensure that successful existing certification frameworks were transposed into the new Regulation. The EU Member States also continue to play a key role in certification for high-security applications.

The certification framework set out in Article III of the Regulation also significantly changes the procedure for developing certification schemes and issuing certificates within the European Union. As a member of bodies such as the European Cybersecurity Certification Group (ECCG), the BSI is making significant contributions to the new processes created by the Regulation. As before, the BSI also continues to work closely with European partners in the field of cyber security certification.

https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/Cyber-Security-Act/cyber-security-act_node.html

Example from the BDEW Whitepaper

BDEW Whitepaper - 4.3.4 - Virtualization

- e) The failure of virtualization servers or other components of the virtualization infrastructure shall not have a negative impact on the defined availability requirements. Faults and failures of the virtualization environment must also be taken into account in the emergency concept and restart planning (see 4.8.2)".

ISO/IEC 27002:2013 / 27019:2017: 12.1.3, 12.3.1, 12.6.1, 13.1.3, 17.2.1

BDEW Whitepaper - 4.5.6 - Logging

- d) The log file shall be protected from subsequent modification.

ISO/IEC 27002:2013 / 27019:2017: 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3

Example from the BSI

TR-02102-2 - Recommendations and Key Lengths for TLS

3.3.3 Signature algorithms

In TLS 1.2, the client can use the extension "signature_algorithms" (see [RFC5246]) to inform the server about the signature algorithms he wants to use for key agreement and certificates. In case of mutual authentication, the server informs the client about the signature algorithms it accepts with the CertificateRequest message. In both cases, the algorithms have to be specified as combination of signature algorithm and hash function.

The use of the extension "signature_algorithms" is recommended.

The use of the following signature algorithms is recommended:

Signature algorithm	IANA no.	Specified in	Use up to
rsa	1	[RFC5246]	2025
dsa	2	[RFC5246]	2029+
ecdsa	3	[RFC5246]	2029+

Table 5: Recommended signature algorithms for TLS 1.2

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=5