IEC/IEEE 60802 brainstorming: Simplified Standardization Workflows, ISA/IEC 62443 Security for industrial automation and control systems and Mapping of Standards to 62443

Dieter Proell (Siemens AG)

Introduction – simplified Workflow – IEC/European/National Standardization

Standardization - IEC Level → IEC <project number>
IEC (International Electrotechnical Commission, https://www.iec.ch/)

Standardization – European Level → EN
CEN/CENELEC (https://www.cencenelec.eu/)

EN IEC harmonized standards → hEN
Details see https://boss.cenelec.eu/fadel/pages/eniec/eniecforojeu/

Publish at Official Journal of the European Union (OJEU)
https://eur-lex.europa.eu/

NC – National Committee comments and votes on Standardization projects. I.e. IEC/IEEE 60802.

Standardization - National Level → DIN or VDE
Example: German National Committee https://www.dke.de/en

"Under the Frankfurt Agreement, the standards are developed by IEC under parallel procedure with CENELEC (unless exempted from parallel procedures through a BT decision)."
(https://boss.cenelec.eu/fadel/pages/eniec/eniecforojeu/)

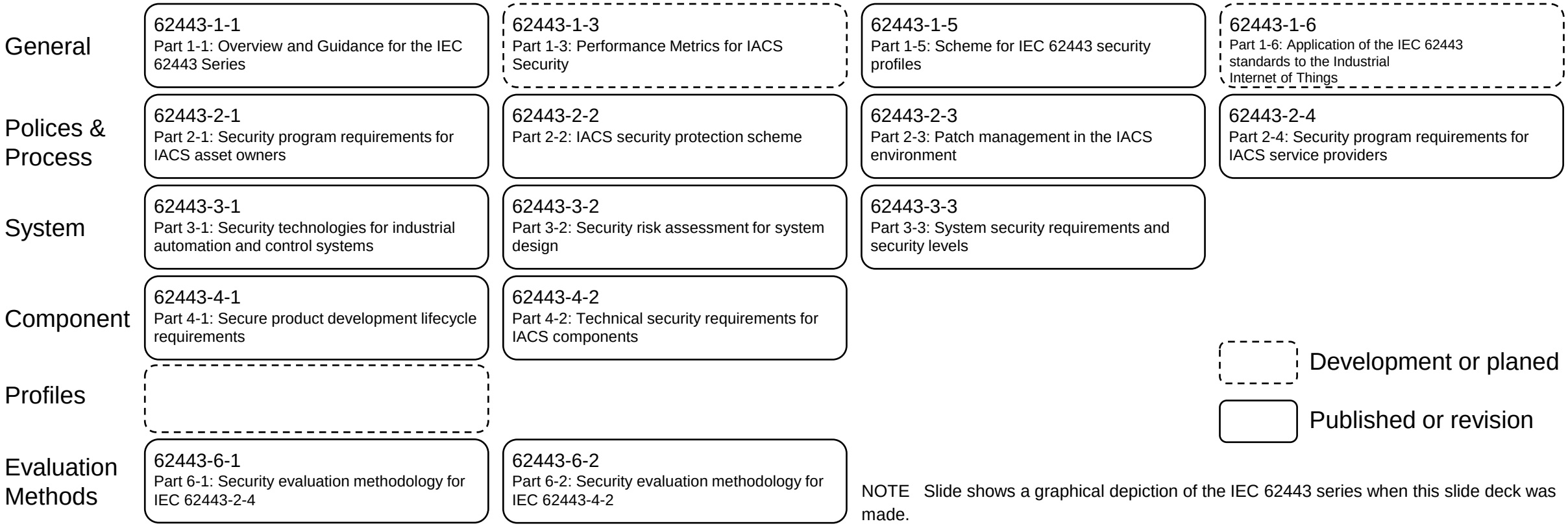
"Regulation (EU) No 1025/2012 on European standardization defines a harmonized standard as a European standard adopted on the basis of a request made by the Commission for the application of Union harmonization legislation."
(https://boss.cenelec.eu/fadel/pages/eniec/eniecforojeu/)

Introduction – ISA/IEC 62443 Security for industrial automation and control systems (IACS)

“IEC 62443 is a series of standards that address security for operational technology in automation and control systems. The series is divided into different sections and describes both technical and process-related aspects of automation and control systems security.” (https://en.wikipedia.org/wiki/IEC_62443).

Standardization in a cooperation between IEC (International Electrotechnical Commission, https://www.iec.ch/) and ISA (International Society of Automation, https://www.isa.org/) ongoing since 2010.

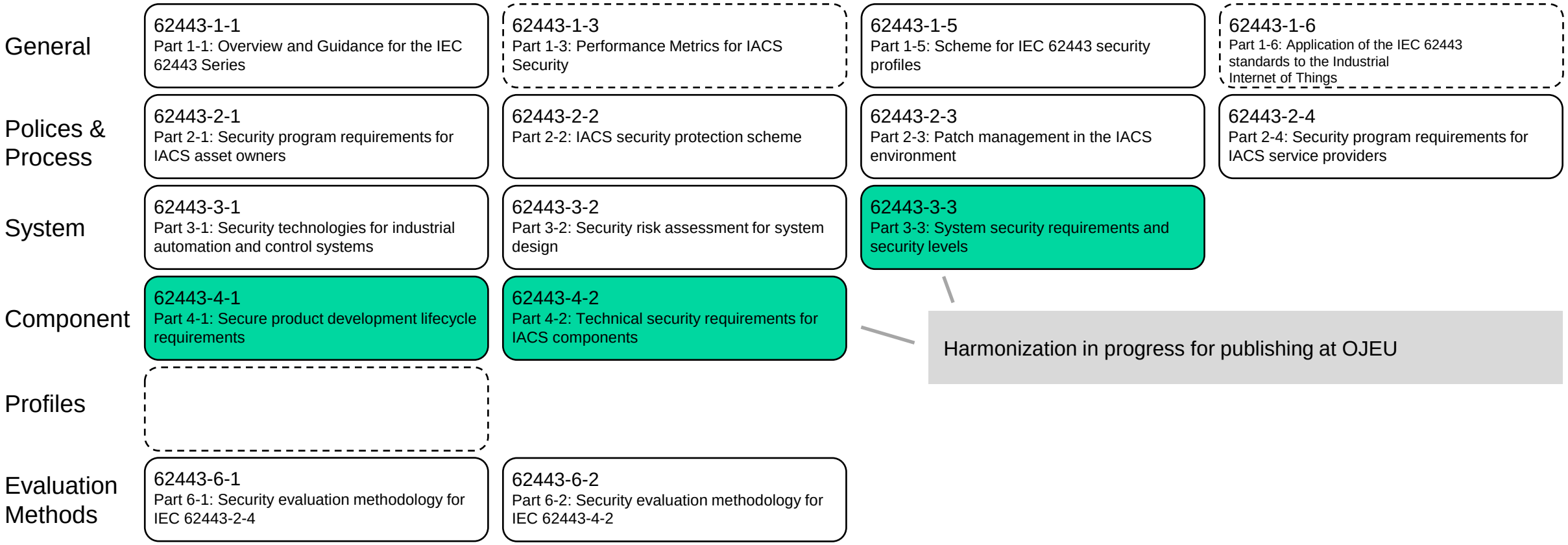
- More information and History at Wikipedia https://en.wikipedia.org/wiki/IEC_62443
- ISA/IEC 62443 Series of Standards https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- Dashboard IEC TC65 WG10 https://www.iec.ch/dyn/www/f?p=103:30:7126358780844:::FSP_ORG_ID,FSP_LANG_ID:1250,25



NOTE Slide shows a graphical depiction of the IEC 62443 series when this slide deck was made.

IEC 62443 Security for industrial automation and control systems (IACS)

EN IEC harmonized standards to publish at OJEU (Official Journal of the European Union)



The planed harmonization (→hEN) for publishing at OJEU (Official Journal of the European Union), support the CRA (Cyber Resilience Act). For more details about CRA follow the webinar https://www.cencenelec.eu/news-and-events/events/2025/2025-03-10_webinar_cyber-resilience-act/.

Brainstorming 60802

There is no need to harmonize each cybersecurity standard to support CRA. The 62443 series offers a mapping of CRs (component requirement) and REs (requirement enhancement) to FR (foundational requirement) SL (security level) levels 1-4 (shown at IEC 62443-4-2, Annex B).

Example with public link to “OPC 10000-2: UA Part 2: Security” (https://reference.opcfoundation.org/Core/Part2/v105/docs/) in Annex A Mapping to ISA/IEC 62443.

Table A.7 – ISA/IEC 62443 Mapping FR 7 Resource availability

ISA-62443-4-2 CRs and REs	Related to				Applies to OPC UA	OPC UA Part #	Keyword text or comment
	SL1	SL2	SL3	SL4			
CR 7.1: Denial of service protection	√	√	√	√	Y	OPC 10000-2	Application Crashes, Fuzz Testing, Certification
						OPC 10000-4	CreateSession, OpenSecureChannel, AuthenticationToken
						OPC 10000-7	Session Services Facets, Standard UA Client 2017 Profile, Base Server Behavior Facet

NOTE Screenshot from OPC 10000-2: UA Part 2: Security, Annex A, Table A.7 with link https://reference.opcfoundation.org/Core/Part2/v105/docs/A#_Ref169293497.

Requirements are clustered as foundational requirements.
Component requirement and requirement enhancement indicate details.
Check box indicates fulfillment of a security level.

Security Level from Wikipedia (https://en.wikipedia.org/wiki/IEC_62443#Security_Level). “The levels are:
Security Level 0: No special requirement or protection required. [SL0 is not used in the example]
Security Level 1: Protection against unintentional or accidental misuse.
Security Level 2: Protection against intentional misuse by simple means with few resources, general skills and low motivation.
Security Level 3: Protection against intentional misuse by sophisticated means with moderate resources, automation-specific knowledge and moderate motivation.
Security Level 4: Protection against intentional misuse using sophisticated means with extensive resources, automation-specific knowledge and high motivation.”

➔ Starting point of Discussion: Develop an Annex “Mapping to ISA/IEC 62443” in Edition 2 of IEC/IEEE 60802.