IEC STANDARD-FAMILY ON CYBERSECURITY FOR NUCLEAR POWER PLANTS

Thomas WALTER

IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts (ICONS2020), 10th to 14th of February 2020, Vienna

International
Electrotechnical
Commission

Content

- What is IEC and Cybersecurity Standards
- IEC 62645 overview
- IEC 62859 overview
- IEC 63096
  - IEC 63096 scope and What is a security control?
  - IEC 63096 structure
  - Structure of each security control
  - Security controls overview list in IEC 63096, Annex A
  - IEC 63096 development timeline

What is IEC? (1)

Leading global organization that prepares and publishes standards for:

- Electrical and electronic products
- Related technologies
  - Electricity, electronics, magnetics, electro-magnetics, electro-acoustics, multimedia, telecommunication, energy production and distribution, electromagnetic compatibility, measurement and performance, dependability, safety, environmental aspects

Membership is by National Committees

What is IEC? (2)

Organized in Technical Committees (TC) and Subcommittees (SC)

- 104 TC
- 99 SC

TC45 for Nuclear instrumentation

- SC45A for instrumentation, control and electrical systems of nuclear facilities
- SC45B for radiation protection instrumentation

What is IEC SC45A? (1)

SC 45A: Instrumentation and Control of Nuclear Facilities

WG 2	Sensors and measurement techniques
WG 3	ICS: architecture and system specific aspects
WG 5	Special process measurement and radiation monitoring
WG 7	Functional and safety fundamentals of instrumentation, control and electrical power systems
WG 8	Control rooms
WG 9	System performance and robustness toward external stress
WG 10	Ageing management of instrumentation, control and electrical power systems in NPP
WG 11	Electrical power systems: architecture and system specific aspects

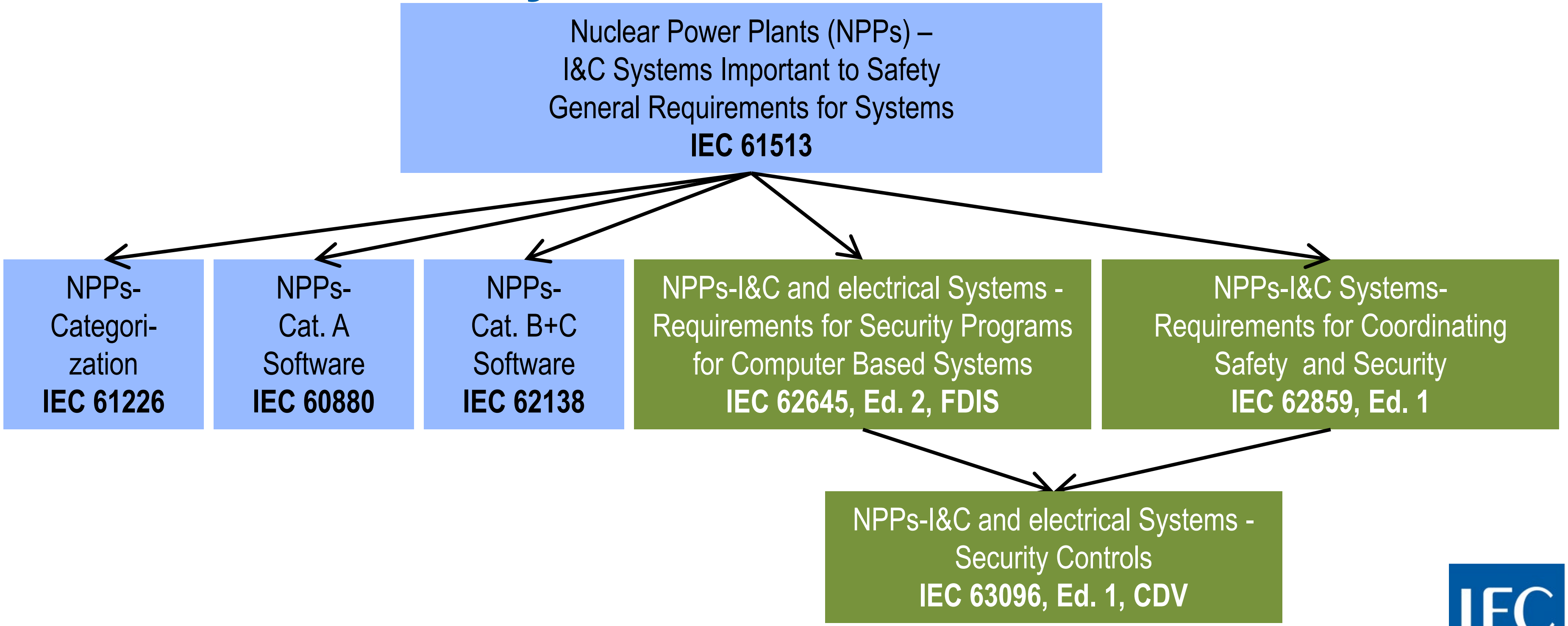
P-Members		O-Members
• Argentina	• Korea (Rep. of)	• Belarus
• Belgium	• Netherlands	• Greece
• Canada	• Norway	• Pakistan
• China	• Romania	• Portugal
• Czech Republic	• Russian Fed.	• Spain
• Egypt	• South Africa	
• Finland	• Sweden	
• France	• Switzerland	
• Germany	• U.S.A.	
• Italy	• Ukraine	
• Japan	• United Kingdom	

Standardization Context (1)

- IEC 61513 Ed 2.0 2011 – Nuclear Power Plants – I&C for Systems Important to Safety – General Requirements for Systems (Similar to IEEE-603-1998)
- IEC 60880 Ed 2.0 (2006) – Nuclear Power Plants – I&C Systems Important to Safety Software Aspects for Computer-Based systems performing Category A Functions (Similar to IEEE 7- 4.3.2-2003)

Standardization Context (2) SC45A

Standard Hierarchy



Nuclear Power Plants (NPPs) –
I&C Systems Important to Safety
General Requirements for Systems
IEC 61513

NPPs-
Categori-
zation
IEC 61226

NPPs-
Cat. A
Software
IEC 60880

NPPs-
Cat. B+C
Software
IEC 62138

NPPs-I&C and electrical Systems -
Requirements for Security Programs
for Computer Based Systems
IEC 62645, Ed. 2, FDIS

NPPs-I&C Systems-
Requirements for Coordinating
Safety and Security
IEC 62859, Ed. 1

NPPs-I&C and electrical Systems -
Security Controls
IEC 63096, Ed. 1, CDV

IEC 62645 – Scope

- Cybersecurity requirements and guidance for development and management of effective computer-based I&C systems, possibly integrating HPD with HDL (Hardware Description Language)
- limited only to I&C programmable digital systems systems
- inherent to these requirements and guidance the power plant’s security programme should comply with the applicable country’s I&C CB&HPD security requirements.
- Human errors, natural events are excluded

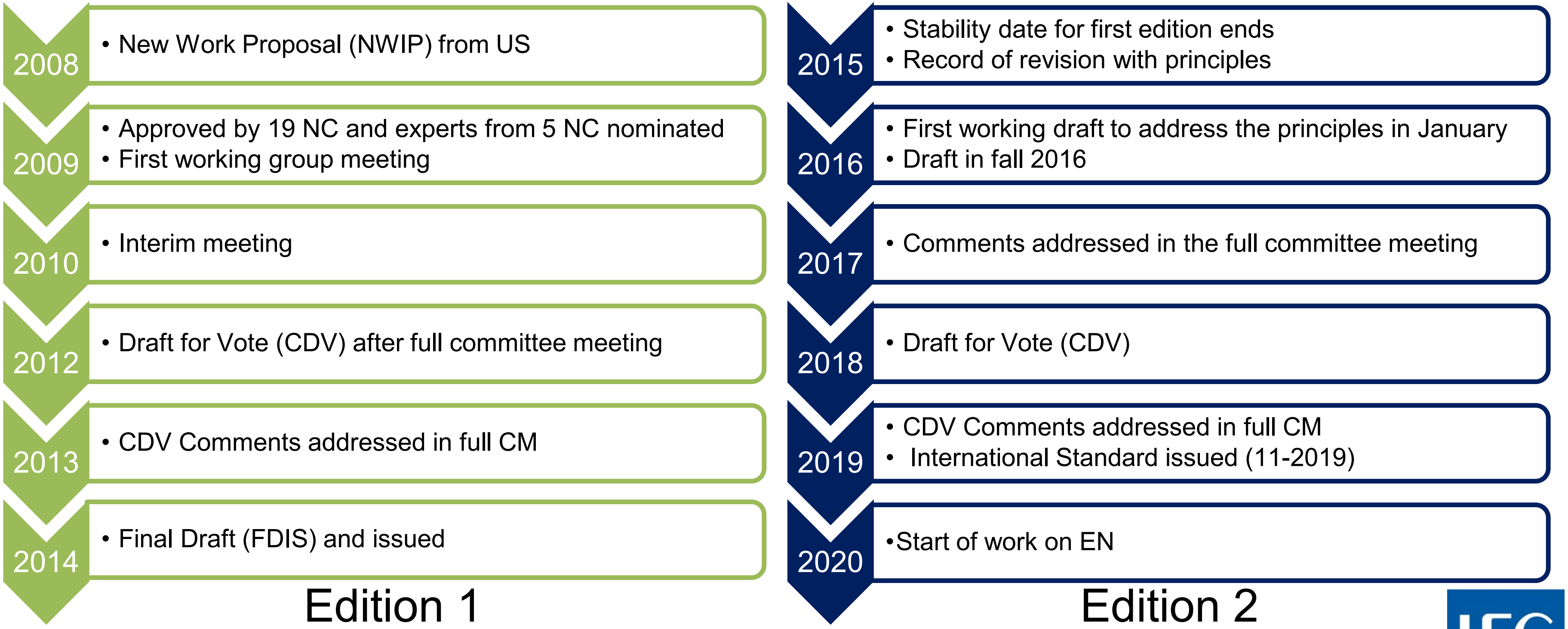
IEC 62645 – Second Edition

- adapt the 2013 editions structure and high-level principles of ISO/IEC 27001 and ISO/IEC 27002.
- consistency with IAEA principles and concepts (NSS17)
- consistency with IEC 62443 series, when relevant
- consistency and articulation with IEC 61513
- coordination with IEC 62138, IEC 60880, and all SC45A standards mentioning computer security
- Rearrangement of the structure to take into account the future second level documents

IEC 62645 – Modification 2nd Ed.

- concept of security degrees and their associated criteria:
  - possibility of further security degrees for non-I&C systems (NSS17).
- Confidentiality issues should be addressed
- Consideration of (smart) electrical systems
- Specific guidance, on legacy systems
- Guidance, recommendations or requirements about cybersecurity audits and risk assessment
- High-level security requirements and/or recommendations to wireless technologies.

IEC 62645 – Timeline



2008
- New Work Proposal (NWIP) from US

2009
- Approved by 19 NC and experts from 5 NC nominated
- First working group meeting

2010
- Interim meeting

2012
- Draft for Vote (CDV) after full committee meeting

2013
- CDV Comments addressed in full CM

2014
- Final Draft (FDIS) and issued

Edition 1

2015
- Stability date for first edition ends
- Record of revision with principles

2016
- First working draft to address the principles in January
- Draft in fall 2016

2017
- Comments addressed in the full committee meeting

2018
- Draft for Vote (CDV)

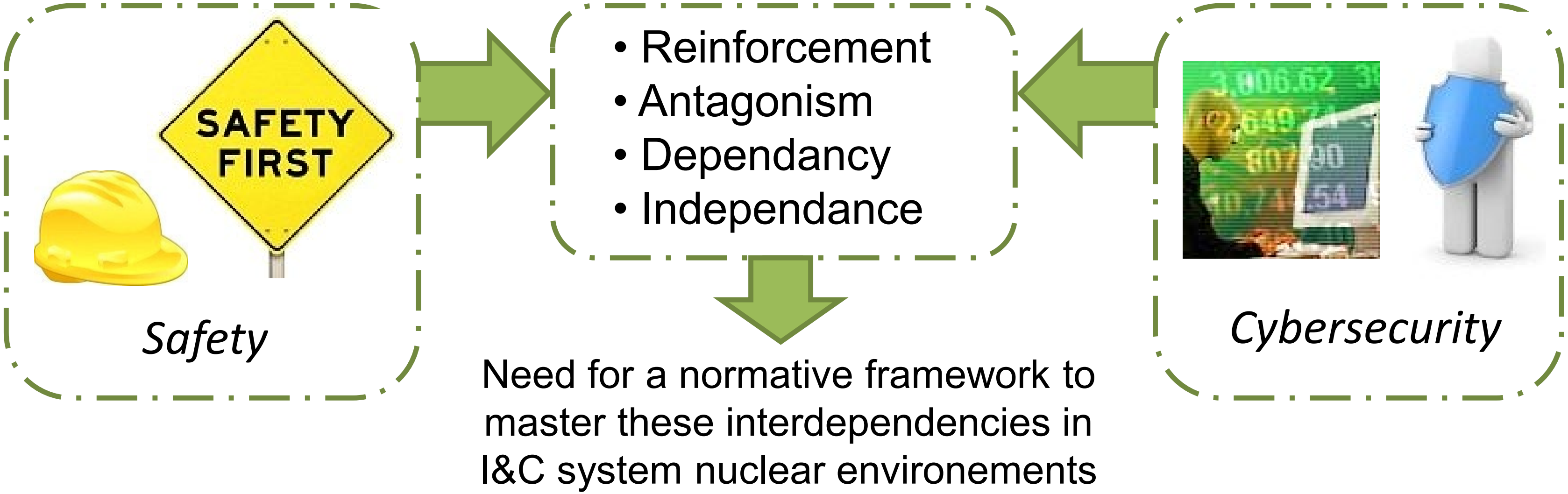
2019
- CDV Comments addressed in full CM
- International Standard issued (11-2019)

2020
- Start of work on EN

Edition 2

IEC 62859 – Overview

- Title: Requirements for coordinating cybersecurity and safety
- Scope:



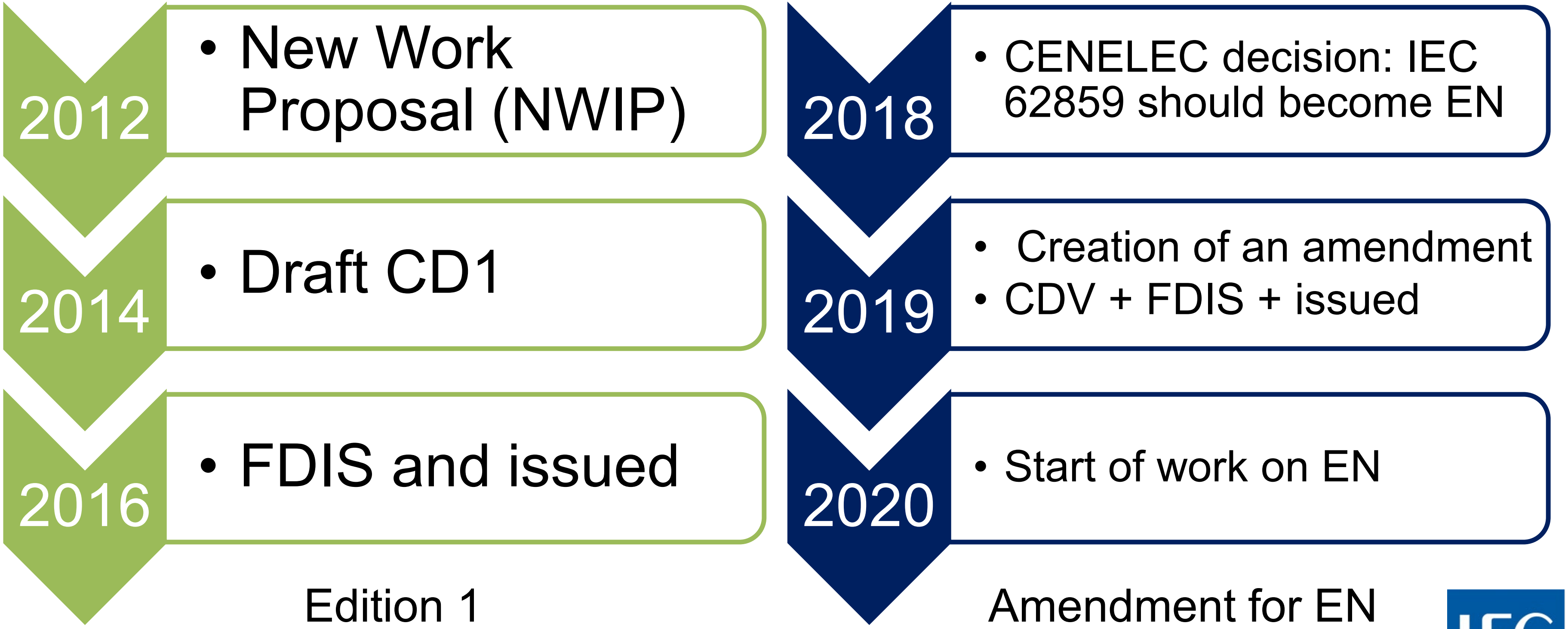
Safety

- Reinforcement
- Antagonism
- Dependancy
- Independance

Cybersecurity

Need for a normative framework to master these interdependencies in I&C system nuclear environements

IEC 62859 – Timeline



2012

- New Work Proposal (NWIP)

2014

- Draft CD1

2016

- FDIS and issued

Edition 1

2018

- CENELEC decision: IEC 62859 should become EN

2019

- Creation of an amendment
- CDV + FDIS + issued

2020

- Start of work on EN

Amendment for EN

IEC 63096 – Scope

- **Security controls for I&C and electrical systems in NPPs**
  - Security controls catalogue based on ISO/ IEC 27002
    → Definition of highly recommended and optional security controls
    → Depending on grading (security degree)
  - Details on the process of applying security controls in line with the IEC 62645 requirements
  - To prevent, detect and correct cyber security attacks

- **For …**
  - new NPPs
  - modernization of I&C in existing NPPs

- **Crediting/ inheritance of existing programs**
- **Legacy I&C systems**

What is a Security Control?

- **Explanation of the term security control**
  - **Security controls** are measures/ countermeasures/ provisions to **avoid**, **detect**, **counteract**, or **minimize cybersecurity risks**

- **Classification of security controls according to <u>point of time they act</u>**
  - **Before the event: Preventive** security controls are intended to prevent an incident from occurring (e.g. by requiring an authentication during login, firewalls)
  - **During the event: Detective** security controls are intended to identify an incident (e.g. sending an alarm if somebody has pulled a network cable);
  - **After the event: Corrective** security controls are intended to limit the extent of any damage caused by the incident (e.g. by restoring an attacked component, analyzing security event logs in order to analyze what has happened)

- **Classification of security controls according to their <u>nature</u>**
  - **Technical** security controls (e.g. Integrity monitoring, firewalls, data diode)
  - **Physical** security controls (e.g. locked cabinet doors, locked electronic rooms)
  - **Administrative** controls (e.g. incident response processes, security awareness training)

IEC 63096 consistent with IEC 62645

- **Graded Approach (Security Degrees)**
  - Security degree S1, highest level, safety class 1 I&C programmable digital systems
  - S2 as minimum for safety class 2 I&C programmable digital systems
  - S3 as minimum for safety class 3 I&C programmable digital systems
  - Baseline requirement

  Security degree also dependent on the consequences on the plant when the I&C is attacked

- **Process of applying security controls**
  - Is in line with IEC 62645, Ed. 2, CDV
  - Process has been detailed together with the IEC 62645 Project Lead

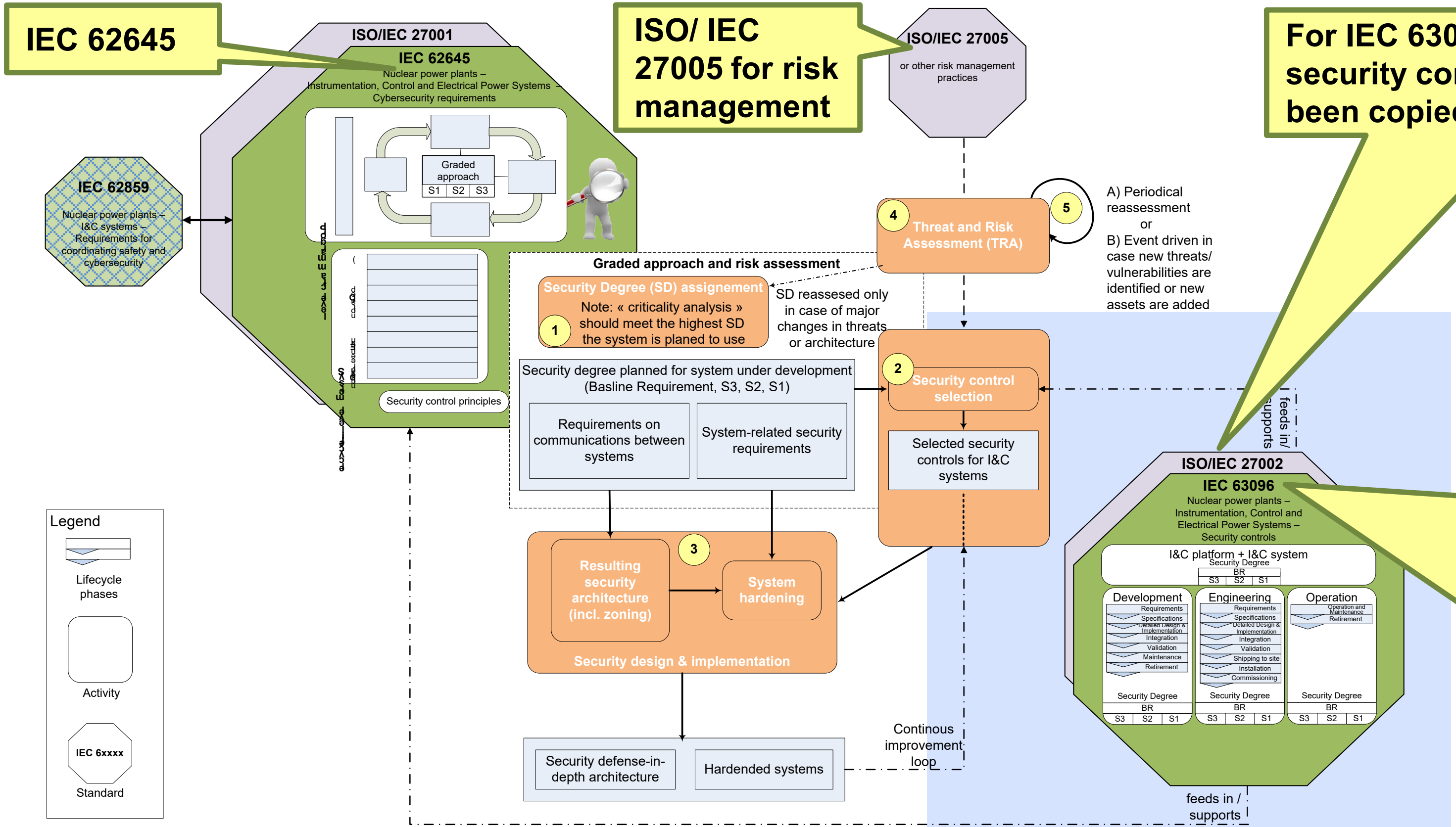
- **IEC 63096 details the security controls topic that is described in IEC 62645 on a high level**

Connection to IEC 62645 and ISO/IEC 27002

IEC 62645

ISO/ IEC 27005 for risk management

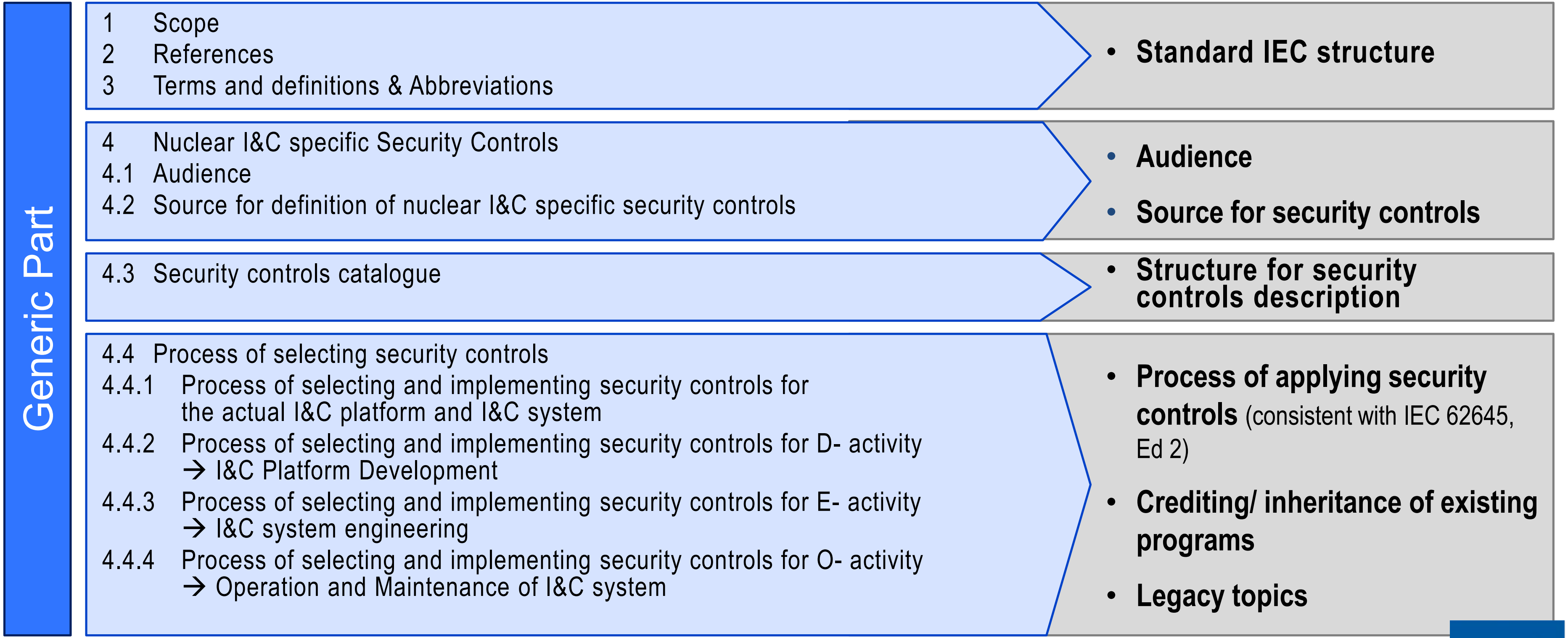
For IEC 63096 the ISO/IEC 27002 security controls catalogue has been copied, modified and extended


ISO/IEC 27001
IEC 62645
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements
Graded approach
S1
S2
S3
Security control principles
IEC 62859
Nuclear power plants – I&C systems – Requirements for coordinating safety and cybersecurity
ISO/IEC 27005
or other risk management practices
4
Threat and Risk Assessment (TRA)
5
A) Periodical reassessment
or
B) Event driven in case new threats/ vulnerabilities are identified or new assets are added
Graded approach and risk assessment
Security Degree (SD) assignement
1
Note: « criticality analysis » should meet the highest SD the system is planed to use
SD reassesed only in case of major changes in threats or architecture
Security degree planned for system under development (Basline Requirement, S3, S2, S1)
Requirements on communications between systems
System-related security requirements
2
Security control selection
Selected security controls for I&C systems
feeds in/ supports
3
Resulting security architecture (incl. zoning)
System hardening
Security design & implementation
Security defense-in-depth architecture
Hardended systems
Continous improvement loop
ISO/IEC 27002
IEC 63096
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Security controls
I&C platform + I&C system
Security Degree
BR
S3
S2
S1
Development
Requirements
Specifications
Detailed Design & Implementation
Integration
Validation
Maintenance
Retirement
Engineering
Requirements
Specifications
Detailed Design & Implementation
Integration
Validation
Shipping to site
Installation
Commissioning
Operation
Operation and Maintenance
Retirement
Security Degree
BR
S3
S2
S1
feeds in / supports
Legend
Lifecycle phases
Activity
IEC 6xxxx
Standard

IEC 63096: Security controls for:

1. I&C platform and I&C system (typically technical and physical security controls)
2. Development environment
3. Engineering environment
4. Operation & Maintenance Environment

IEC 63096 structure (1)



Generic Part

1 Scope
2 References
3 Terms and definitions & Abbreviations

- **Standard IEC structure**

4 Nuclear I&C specific Security Controls
4.1 Audience
4.2 Source for definition of nuclear I&C specific security controls

- **Audience**
- **Source for security controls**

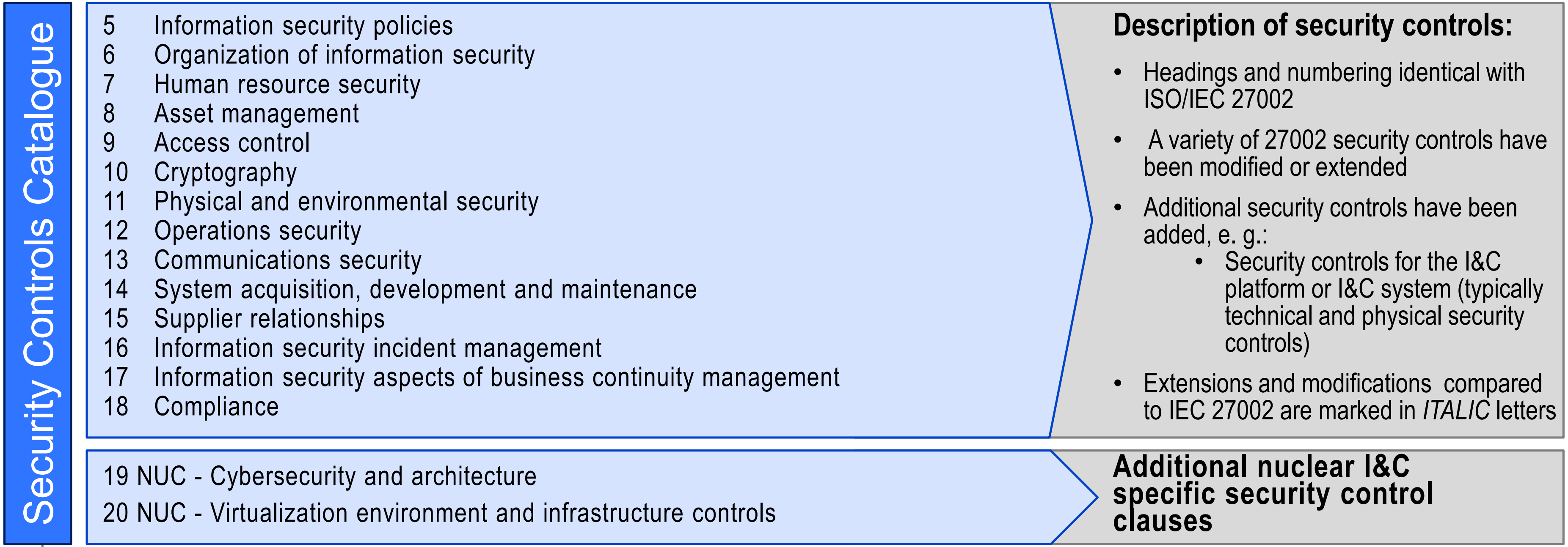
4.3 Security controls catalogue

- **Structure for security controls description**

4.4 Process of selecting security controls
4.4.1 Process of selecting and implementing security controls for the actual I&C platform and I&C system
4.4.2 Process of selecting and implementing security controls for D- activity → I&C Platform Development
4.4.3 Process of selecting and implementing security controls for E- activity → I&C system engineering
4.4.4 Process of selecting and implementing security controls for O- activity → Operation and Maintenance of I&C system

- **Process of applying security controls** (consistent with IEC 62645, Ed 2)
- **Crediting/ inheritance of existing programs**
- **Legacy topics**

IEC 63096 structure (2)



Security Controls Catalogue

5 Information security policies
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance

Description of security controls:

- Headings and numbering identical with ISO/IEC 27002
- A variety of 27002 security controls have been modified or extended
- Additional security controls have been added, e. g.:
    - Security controls for the I&C platform or I&C system (typically technical and physical security controls)
- Extensions and modifications compared to IEC 27002 are marked in *ITALIC* letters

19 NUC - Cybersecurity and architecture
20 NUC - Virtualization environment and infrastructure controls

Additional nuclear I&C specific security control clauses

The security controls catalogue …

- represents the **statement of applicability (SOA) for the nuclear I&C domain**.
- contains **technical**, **physical** and **administrative** security controls.

Structure of each security control (1)

- **Control**

  This subclause contains a short description of the specific security control. If there is no modification the original ISO/ IEC 27002 text has been taken over.

- **Preservation of**

  Description of the objective of the security control in terms of Confidentiality, Integrity and Availability (CIA):

  - C → Confidentiality
  - I → Integrity
  - A → Availability

- **Control focus**

  This subclause contains the description of the focus of the security control in terms of prevention, detection and correction

  - p → Prevention
  - d → Detection
  - c → Correction

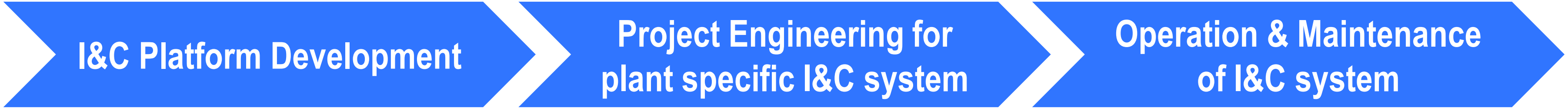
Structure of each security control (2)

- **Implementation guidance (1)**
  - The implementation guidance is described in a standardized table format.
  - The implementation guidance depends on the security degree (as defined in IEC 62645) that is assigned to the individual I&C system.
  - If no security degree is assigned the implementation guidance of the security baseline “Baseline Requirement” applies.
  - For the security baseline and the security degrees following column headings are defined:
    - BR → Baseline Requirement
    - S3 → Security degree 3
    - S2 → Security degree 2
    - S1 → Security degree 1

Structure of each security control (3)

Implementation guidance (2)

- The applicability of the implementation guidance also depends on one or several of the following activities, shown by the following activity letters in columns BR, S3, S2, S1:


I&C Platform Development
Project Engineering for plant specific I&C system
Operation & Maintenance of I&C system

D → I&C Platform Development

D → activity letter

E → Project Engineering for plant specific I&C system

- E_b → Project Engineering before "Installation" and "Commissioning"
- E_d → Sub- activities "Requirements", "Specifications" and "Detailed design and implementation"
- E_g → Sub- activity "Integration (offsite integration)"
- E_v → Sub- activity "Validation (factory acceptance testing)"
- E_s → Sub- activity "Shipping to site"

E_{ic} Project Engineering activities "Installation" and "Commissioning"

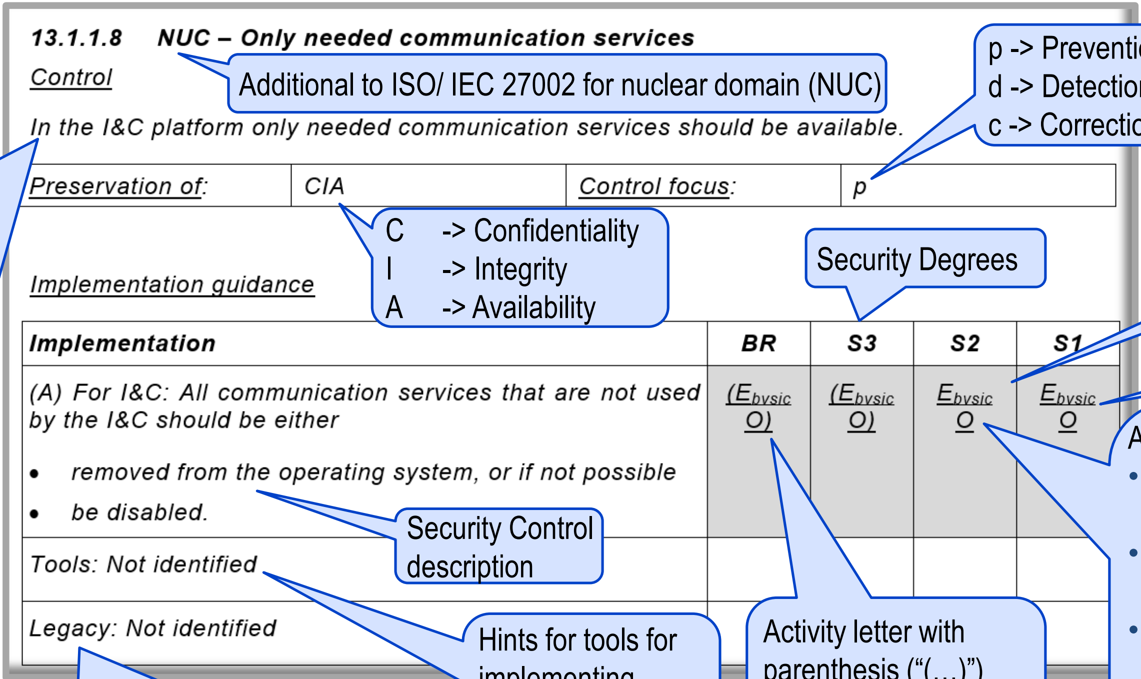
- E_i → Sub- activity "Installation (onsite Integration and Acceptance Testing)"
- E_c → Sub- activity "Commissioning (Commissioning and Acceptance Testing)"

O → Operation and Maintenance of I&C system

- O_o → Sub- activity "Operation"
- O_m → Sub- activity "Maintenance"
- O_r → Sub- activity "Retirement"

Security controls description

Security Controls example for I&C platform or system



13.1.1.8 NUC – Only needed communication services

Control

In the I&C platform only needed communication services should be available.

Preservation of:	*CIA*	*Control focus:*	*p*

Implementation guidance

Implementation	***BR***	***S3***	***S2***	***S1***
(A) For I&C: All communication services that are not used by the I&C should be either • *removed from the operating system, or if not possible* • *be disabled.*	(E_{bvsic} O)	(E_{bvsic} O)	E_{bvsic} O	E_{bvsic} O
Tools: Not identified				
Legacy: Not identified				

Letters are *italic*→ new security control compared to ISO/ IEC 27002

Additional to ISO/ IEC 27002 for nuclear domain (NUC)

p -> Prevention
d -> Detection
c -> Correction

C -> Confidentiality
I -> Integrity
A -> Availability

Security Degrees

Gray shading and activity letters underlined:
→ Security control for I&C platform or I&C system

Activity letter without parenthesis (no “(…)”)
→ Security control is highly recommended

Activity letters show applicability:

- **E_b:** To handled in all Engineering phases before installation and commissioning
- **E_{vs}:** To be in place and tested in the I&C system during Integration and Validation; in place during shipping
- **E_{ic}:** To be in place in the I&C system during Installation and Commissioning
- **O:** To be in place in the I&C system in all phases of Operation and Maintenance

Security Control description

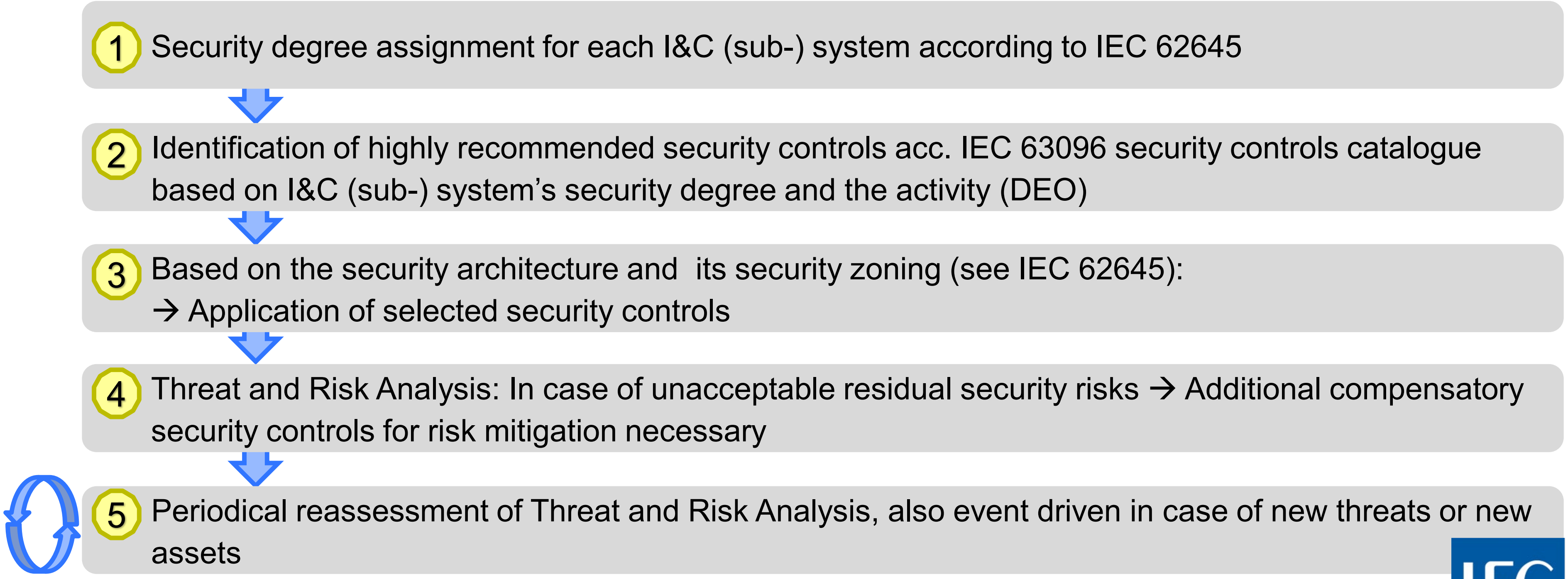
Hints for tools for implementing security control (in this case no hint)

How Legacy could be handled (In this case no recommendation)

Activity letter with parenthesis (“(…)”)
→ Security control is optional

Simplified process overview for applying security controls

x from slide 18



1 Security degree assignment for each I&C (sub-) system according to IEC 62645

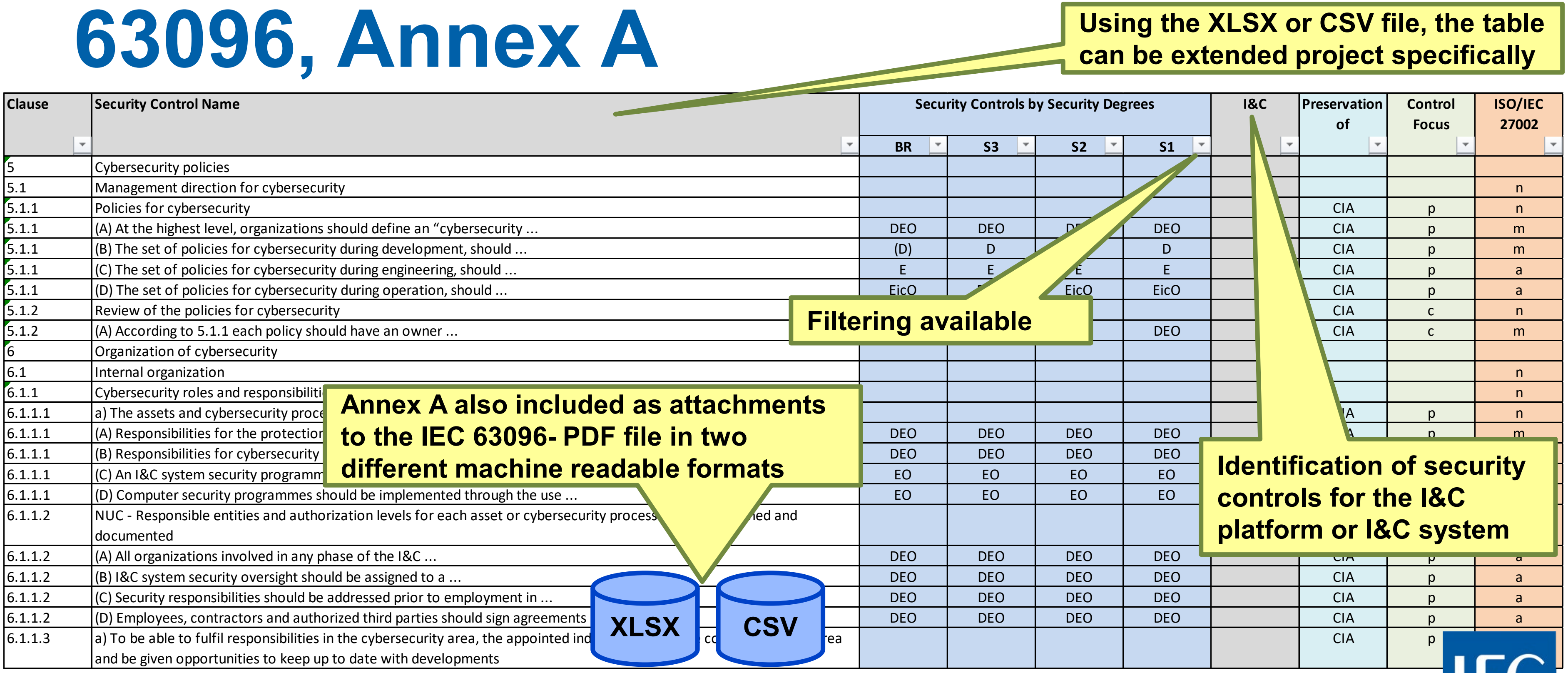
2 Identification of highly recommended security controls acc. IEC 63096 security controls catalogue based on I&C (sub-) system’s security degree and the activity (DEO)

3 Based on the security architecture and its security zoning (see IEC 62645):
→ Application of selected security controls

4 Threat and Risk Analysis: In case of unacceptable residual security risks → Additional compensatory security controls for risk mitigation necessary

5 Periodical reassessment of Threat and Risk Analysis, also event driven in case of new threats or new assets

Security controls overview list in IEC 63096, Annex A



Clause	Security Control Name	Security Controls by Security Degrees				I&C	Preservation of	Control Focus	ISO/IEC 27002
		BR	S3	S2	S1				
5	Cybersecurity policies								
5.1	Management direction for cybersecurity								n
5.1.1	Policies for cybersecurity						CIA	p	n
5.1.1	(A) At the highest level, organizations should define an “cybersecurity ...	DEO	DEO	DE	DEO		CIA	p	m
5.1.1	(B) The set of policies for cybersecurity during development, should ...	(D)	D		D		CIA	p	m
5.1.1	(C) The set of policies for cybersecurity during engineering, should ...	E	E	E	E		CIA	p	a
5.1.1	(D) The set of policies for cybersecurity during operation, should ...	EicO	E	EicO	EicO		CIA	p	a
5.1.2	Review of the policies for cybersecurity						CIA	c	n
5.1.2	(A) According to 5.1.1 each policy should have an owner ...				DEO		CIA	c	m
6	Organization of cybersecurity								
6.1	Internal organization								n
6.1.1	Cybersecurity roles and responsibiliti								n
6.1.1.1	a) The assets and cybersecurity proce						IA	p	n
6.1.1.1	(A) Responsibilities for the protection	DEO	DEO	DEO	DEO		A	p	m
6.1.1.1	(B) Responsibilities for cybersecurity	DEO	DEO	DEO	DEO				
6.1.1.1	(C) An I&C system security programm	EO	EO	EO	EO				
6.1.1.1	(D) Computer security programmes should be implemented through the use ...	EO	EO	EO	EO				
6.1.1.2	NUC - Responsible entities and authorization levels for each asset or cybersecurity process ned and documented								
6.1.1.2	(A) All organizations involved in any phase of the I&C ...	DEO	DEO	DEO	DEO		CIA	p	a
6.1.1.2	(B) I&C system security oversight should be assigned to a ...	DEO	DEO	DEO	DEO		CIA	p	a
6.1.1.2	(C) Security responsibilities should be addressed prior to employment in ...	DEO	DEO	DEO	DEO		CIA	p	a
6.1.1.2	(D) Employees, contractors and authorized third parties should sign agreements	DEO	DEO	DEO	DEO		CIA	p	a
6.1.1.3	a) To be able to fulfil responsibilities in the cybersecurity area, the appointed ind co rea and be given opportunities to keep up to date with developments						CIA	p	

Using the XLSX or CSV file, the table can be extended project specifically

Filtering available

Annex A also included as attachments to the IEC 63096- PDF file in two different machine readable formats

Identification of security controls for the I&C platform or I&C system

IEC 63096 - timeline

08/2016
- Approval of NWIP
- New Work Item Proposal (NWIP) idea from the US

03/2017
- First WD (working draft)
- Review at IEC TC45A WGA9 Intermediate meeting

06/2017
- CD (committee draft) proposal ready for WGA9 review

08/2017
- CD proposal review by WGA9

10/2017
- IEC TC45A conference in Shanghai

02/2018
- CD1 issued for IEC review

12/2018
- CD2 issued for IEC review

04/2019
- IEC TC45A conference in Paris

07/2019
- CDV (committee draft for vote) handed over to TC45A secretary for IEC review preparation

01/2020
- CDV IEC review results expected to be available

02/2020
- IEC TC45A WGA9 Intermediate meeting in Erlangen, Germany, scheduled

12/2020
- Planned FDIS (Final Draft International Standard) hand over to IEC

Completion of IEC 63096 FDIS planned for end of 2020

Thank you!

Thomas WALTER
PreussenElektra GmbH
thomas.walter1@preussenelektra.de

in Cooperation with
E. L. Quinn, Technology Resource Inc., USA
L. Pietre-Cambacedes, EdF, France
J. E. Bochtler, Siemens AG, Germany