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
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
What is IEC SC45A? (1)

- Participating members (22)
- Observer members (5)

<table>
<thead>
<tr>
<th>P-Members</th>
<th>O-Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>Korea (Rep. of)</td>
</tr>
<tr>
<td>Belgium</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Canada</td>
<td>Norway</td>
</tr>
<tr>
<td>China</td>
<td>Romania</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Russian Fed.</td>
</tr>
<tr>
<td>Egypt</td>
<td>South Africa</td>
</tr>
<tr>
<td>Finland</td>
<td>Sweden</td>
</tr>
<tr>
<td>France</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Germany</td>
<td>U.S.A.</td>
</tr>
<tr>
<td>Italy</td>
<td>Ukraine</td>
</tr>
<tr>
<td>Japan</td>
<td>United Kingdom</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Belarus</td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
</tr>
</tbody>
</table>
Standardization Context (1)

• 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-Categorization
  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 2\textsuperscript{nd} 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

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 1

Edition 2
IEC 62859 – Overview

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

  - Reinforcement
  - Antagonism
  - Dependancy
  - Independance

Need for a normative framework to master these interdependencies in I&C system nuclear environments.
IEC 62859 – Timeline

2012
• New Work Proposal (NWIP)

2014
• Draft CD1

2016
• FDIS and issued

2018
• CENELEC decision: IEC 62859 should become EN

2019
• Creation of an amendment
• CDV + FDIS + issued

2020
• Start of work on EN

Edition 1
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 point of time they act**
  • **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 nature**
  • **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

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

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 62645

ISO/IEC 27001

ISO/IEC 27005

ISO/IEC 27006

IEC 62859

IEC 63096

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

IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts (ICONS2020), 10th to 14th of February 2020, Vienna
IEC 63096 structure (1)

1 Scope
2 References
3 Terms and definitions & Abbreviations

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

4.3 Security controls catalogue

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

- Standard IEC structure
- Audience
- Source for security controls
- Structure for security controls description
- Process of applying security controls (consistent with IEC 62645, Ed 2)
- Crediting/inheritance of existing programs
- Legacy topics
The security controls catalogue …
• represents the statement of applicability (SOA) for the nuclear I&C domain.
• contains technical, physical and administrative security controls.

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
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**
  - D → I&C Platform Development

- **Project Engineering for plant specific I&C system**
  - 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_p → Project Engineering activities “Installation” and “Commissioning”
      - E → Sub-activity “Installation (on-site Integration and Acceptance Testing)”
      - E_c → Sub-activity “Commissioning (Commissioning and Acceptance Testing)”

- **Operation & Maintenance of I&C system**
  - 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**

<table>
<thead>
<tr>
<th>Implementation guidance</th>
<th>Implementation</th>
<th>BR</th>
<th>S3</th>
<th>S2</th>
<th>S1</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) For I&amp;C: All communication services that are not used by the I&amp;C should be either</td>
<td></td>
<td>(E\text{\textsubscript{physic}}/O)</td>
<td>(E\text{\textsubscript{\text{physic}}}/O)</td>
<td>E\text{\textsubscript{\text{physic}}}</td>
<td>E\text{\textsubscript{\text{physic}}}</td>
</tr>
<tr>
<td>• removed from the operating system, or if not possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• be disabled.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tools: Not identified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legacy: Not identified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Security Degrees

- **BR**: To handled in all Engineering phases before installation and commissioning
- **S3**: To be in place and tested in the I&C system during Integration and Validation; in place during shipping
- **S2**: 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

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

**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**

**Activity letters show applicability:**

- **E\text{\textsubscript{P}}**: To handled in all Engineering phases before installation and commissioning
- **E\text{\textsubscript{Vs}}**: To be in place and tested in the I&C system during Integration and Validation; in place during shipping
- **E\text{\textsubscript{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

**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

**Letters are italic**

- New security control compared to ISO/IEC 27002
Simplified process overview for applying security controls

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 | 5 | 5.1 Management direction for cybersecurity | 5.1.1 Policies for cybersecurity | 5.1.1 (A) At the highest level, organizations should define an “cybersecurity … | 5.1.1 (B) The set of policies for cybersecurity during development, should … | 5.1.1 (C) The set of policies for cybersecurity during engineering, should … | 5.1.1 (D) The set of policies for cybersecurity during operation, should … | 5.1.2 Review of the policies for cybersecurity | 5.1.2 (A) According to 5.1.1 each policy should have an owner … |
|--------|----------------------|---|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| 6      | Organization of cybersecurity | Internal organization | 6.1 Internal organization | 6.1.1 Cybersecurity roles and responsibilities | 6.1.1.1 Responsibilities for the protection of individual assets | 6.1.1.1.1 (A) Responsibilities for the protection of individual assets | 6.1.1.1.1 (B) Responsibilities for the protection of individual assets | 6.1.1.1.1 (C) An I&C system security programme | 6.1.1.1.1.2 NU. - Responsible entities and authorization levels for each asset or cybersecurity process should be defined and documented | 6.1.1.2 (A) All organizations involved in any phase of the I&C … | 6.1.1.2 (B) I&C system security oversight should be assigned to a … | 6.1.1.2 (C) Security responsibilities should be addressed prior to employment in … | 6.1.1.2 (D) Employees, contractors and authorized third parties should sign agreements … | 6.1.1.2.1 a) To be able to fulfill responsibilities in the cybersecurity area, the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments |

### Security Controls by Security Degrees

| Clause | Security Control Name | 5 | 5.1 Management direction for cybersecurity | 5.1.1 Policies for cybersecurity | 5.1.1 (A) At the highest level, organizations should define an “cybersecurity … | 5.1.1 (B) The set of policies for cybersecurity during development, should … | 5.1.1 (C) The set of policies for cybersecurity during engineering, should … | 5.1.1 (D) The set of policies for cybersecurity during operation, should … | 5.1.2 Review of the policies for cybersecurity | 5.1.2 (A) According to 5.1.1 each policy should have an owner … |
|--------|----------------------|---|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| 6      | Organization of cybersecurity | Internal organization | 6.1 Internal organization | 6.1.1 Cybersecurity roles and responsibilities | 6.1.1.1 Responsibilities for the protection of individual assets | 6.1.1.1.1 (A) Responsibilities for the protection of individual assets | 6.1.1.1.1 (B) Responsibilities for the protection of individual assets | 6.1.1.1.1 (C) An I&C system security programme | 6.1.1.1.1.2 NU. - Responsible entities and authorization levels for each asset or cybersecurity process should be defined and documented | 6.1.1.2 (A) All organizations involved in any phase of the I&C … | 6.1.1.2 (B) I&C system security oversight should be assigned to a … | 6.1.1.2 (C) Security responsibilities should be addressed prior to employment in … | 6.1.1.2 (D) Employees, contractors and authorized third parties should sign agreements … | 6.1.1.2.1 a) To be able to fulfill responsibilities in the cybersecurity area, the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments |

### Filtering available

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

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

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

### XLSX and CSV

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

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

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

XLSX and CSV
**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