

Technical Requirements for Electrical Equipment Title General Technical Requirements on Cybersecurity	Document TBE 100:2
	Issue 5
	Date 2022-11-17
	Supersedes 4

Contents

1	General	2
2	Definitions	2
3	General Product Requirements	3
3.1	Basic Requirements	3
3.2	Standardization	3
4	Nuclear Specific Requirements	4
4.1	Design, Manufacturing, Verification and Validation	4
4.2	Installation and Commissioning	4
4.3	Phase out	4
4.4	Change Management/Spare Parts	4
5	Agreements between Manufacturer/Supplier and Purchaser	5

Document	Issue	Date	Supersedes
TBE 100:2	5	2022-11-17	4

1 General

These Technical Requirements state the general technical requirements on cybersecurity for electrical equipment intended for use in nuclear power stations.

For each acquisition there is a Technical Specification (TS). The TS compiles all requirements of the product and indicates applicable TBE and KBE.

Additional to this document, plant specific requirements regarding cybersecurity shall apply.

2 Definitions

Assets

Everything that is valuable for the organization (ISO/IEC 27002:2005).

Access Control

Means to ensure that access to assets is authorized and restricted based on business and information requirements.

Authorization

Function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular(IEC 62645:2019).

Cybersecurity

Set of activities and measures the objective of which is to prevent, detect, and react to:

– Malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation

– Malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

– Malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation

(IEC 62645:2019)

Information Security

Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved (ISO/IEC 27002:2005)

(This definition is only for information and comparison with cybersecurity)

Information Management System Program

Part of Manufacturer/Supplier management system that implement information-security issues

Management System

Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives. (ISO 9000:2015)

(This definition is only for information and comparison with Information management System program)

3 General Product Requirements

3.1 Basic Requirements

The Information Management System program shall be applied on the product during the whole life cycle. The Supplier/Manufacturer shall state among others how:

- integrity against unintended or irregular access to software or data have been maintained
- unintended or unauthorized changes or destruction of software and data have been prevented
- above stated measures shall be maintained by the Purchaser.

This shall be stated by computerized, physical measures or other suitable protective actions. Communication (internal/external), networks, tools, storage media, authentication etc. shall also be included.

The product shall be designed and manufactured in a way that the cybersecurity aspects has no negative impact on the product functionality (performance, safety functions and reliability).

3.2 Standardization

The Manufacturer/Supplier shall have an Information Management System Program that follow requirements in ISO 27001 as a part of Manufacturer/Supplier management system.

Design, manufacturing, verification and validation of the product shall follow requirements according to section 5 & 6 in IEC 62645 or other equivalent standards prior to Purchasers approval.

The Manufacturer/Supplier shall state in the tender which cybersecurity requirements the product fulfil or can maintain.

4 Nuclear Specific Requirements

Reactor safety requirements are superior to cybersecurity requirements.

Unused software features shall be defined and shall be blocked or deleted, to the extent it is possible.

Life-cycle activities below shall follow the requirements according to section 6 in IEC 62645.

4.1 Design, Manufacturing, Verification and Validation

The Manufacturer/Supplier shall state in the tender how the cybersecurity requirements are maintained during design, manufacturing, verification and validation.

4.2 Installation and Commissioning

The Manufacturer/Supplier shall state in the tender how the cybersecurity requirements are maintained during installation and commissioning.

4.3 Phase out

The Manufacturer/Supplier shall state in the tender how the cybersecurity requirements are maintained during and after the phase out of the product.

4.4 Change Management/Spare Parts

Changes in software design, components on circuit boards and manufacturing methods that can affect the cybersecurity shall be reported to the Purchaser.

5 Agreements between Manufacturer/Supplier and Purchaser

This checklist should be used as a base between Manufacturer/Supplier and Purchaser when discussing tenders or orders.

1	Acceptance of Technical Specification, TS and deviations, if any.	
2	Application of guidelines/standard.	
3	Continuously information from Manufacturer/Supplier to the Purchaser concerning identified Cybersecurity weaknesses in the product.	
4	<p>Remote access from not approved networks.</p> <p>Access by wireless and mobile networks or external media.</p> <p>Barriers between zones.</p> <p>Different types of identification and authentication control and the possibility to backtrack different events (event log).</p> <p>Access to event logs: access control, request errors, operating system events, and system events, backup and restore events, configuration changes.</p> <p>Back up available for restart of attacked system.</p> <p>Protect, detect and log installation of harmful/unauthorized code.</p> <p>Storage capacity of event logs.</p> <p>Time synchronisation.</p>	
5	<p>Example of areas that should be defined, verified, and documented before delivery.</p> <ul style="list-style-type: none"> • Used software features • User Authentication • Network Security • System Security (parameter setting etc.) • Users and Groups Management • Intrusion resistance • USB Removing/Blocking • Removing/Blocking of unnecessary SW features. 	