

<b>Technical Requirements for Electrical Equipment</b>  Rubrik/Title <b>Programmable electronics with fixed application</b>	Beteckning/ ocument TBE 106:2-2
	Utgåva/Issue 5 (E)
	Datum/Date 2017-05-22
	Ersätter/Supersedes 4 (E)

## Contents

1	Introduction	2
2	Definitions	2
3	Product requirements	3
3.1	Standardisation	3
3.2	Hardware requirements	4
3.3	Software requirements	4
3.4	Common equipment requirements (hardware and software)	4
4	Documentation	6
4.1	General	6
4.2	Product documentation	6
4.3	Design documentation	7
4.4	Maintenance documentation	7
4.5	Operating documentation	7
4.6	Inspection documentation	8
5	Agreement between Manufacturer/Supplier and Purchaser	9

Document	Issue	Date	Supersedes
TBE 106:2-2	5 (E)	2017-05-22	4 (E)

# 1 Introduction

These Technical Requirements set out the requirements to be met by programmable electronics intended for use in nuclear power plants. The Technical Requirements comprise only requirements for technical systems. Administrative computer systems are not covered by these Requirements. The requirements shall be met by the Manufacturer/Supplier in order to achieve the safety and reliability goals of the Swedish nuclear power plant owners.

The purpose of this document is to set out general requirements to be met by programmable electronics and by the process of developing the software.

Overall requirements to be met by the programmable equipment, as well as other instructions for the Manufacturer/Supplier, are stated in other Requirements in accordance with the Technical Specification.

In addition to the Requirements in this document, the relevant parts of the requirements of TBE 100:1, General Technical Requirements and explanations, apply.

PE with a fixed application (PE = programmable electronics). Like PE with a programmable application, this can perform system functions, but the software function is not accessible to the user to change. You can only perform configurations in the application by setting certain parameters, usually with buttons and knobs on the front. As an alternative, in some cases, parameters can be set with a plugged-in tool. Examples of equipment are UPSs, switchboards/circuit-breakers frequency converters and transmitters.

These Requirements shall be applied to all components and equipment whose function is realised with software for gathering data, converting data, and controlling or regulating other equipment.

The Requirements specifies the technical requirements which are necessary in order to attain the sufficient safety when implementing the protective functions with the PE-equipment.

TBE 106 is divided into two requirement levels on the basis of functional requirements and other for the plant specific considerations. The requirement levels cannot be translated directly to the plants' classification principles with regard to electrical function class; instead an assessment shall be made in each individual case when the requirement level is chosen.

The requirement levels are designated TBE 106: X-1 and TBE 106: X-2, where level -1 is the highest requirement level.

For equipment belonging to electrical functional classification 1E-according to IEEE or category A equipment according to IEC 61226, TBE 106: X-1 shall always be applied.

# 2 Definitions

In cases where definitions are taken from an established standard, the original text is quoted in italic type and the source is given. Other definitions have been written specifically for this document.

## Hardware

*Physical equipment used in data processing, as opposed to computer programs, Procedures, rules, and associated documentation (IEEE, ISO).*

## Module

*A logically delimited software section or a subroutine with a defined function and with well defined interfaces*

*In a PE system this usually means a function block e.g. a logic gate or regulator, which is configured by application programming and which is combined with other modules to form a system function*

## MTBF

Mean Time Between Failure

## MTTR

Mean Time To Repair

## Programmable electronics (PE)

*Based on computer technology which may be comprised of hardware, software and of input and/or output units*

*NOTE – This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.*

*Example: The following are all programmable electronic devices:*

- microprocessors
- microcontrollers
- programmable controllers
- application specific integrated circuits (ASICs)
- programmable logic controllers (PLCs)
- other computer based devices (for example smart sensors, transmitters, actuators) (IEC 61508-4)

**Software** *A set of ordered instructions and data that specify operations in a form suitable for execution by a digital computer (IEC 60880).*

## Safety integrity level (SIL)

*Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest*

*NOTE – The target failure measures (see 3.5.13) for the four safety integrity levels are specified in tables 2 and 3 of IEC 61508-1.*

# 3 Product requirements

## 3.1 Standardisation

The method used to produce the product shall conform to a development process which at least follows the requirements according to IEC 61508 SIL 2 or another documented and reviewable

development process at the equivalent level e.g. ISO 9001 and ISO 90003. The Manufacturer/Supplier shall describe the development process used at the development of the product.

Documented and traceable operating experiences may to a certain extent replace deficiencies in the development methodology.

Regarding requirements on quality system please refer to KBE 100.

The method used to produce the product shall describe a life-cycle approach from product idea through to phasing out of the product. This also includes describing how the product can be replaced with other compatible equipment and how support works after the product is no longer commercially available.

It is especially important that the Manufacturer/Supplier can produce a configuration management plan which provides a basis for defining, controlling and tracing requirements at the completion of different stages during the design process including documentation and versions of software.

In the Quotation, the Manufacturer/Supplier shall state how the Requirements and applicable product standards are met.

A general inspection plan is set out in KBE IP-106:2-2 with associated examination procedures.

## **3.2 Hardware requirements**

### **3.2.1 Battery backup**

If battery backup is included, the service life of the batteries shall be stated.

### **3.2.2 Storage media**

Storage media and equipment for backing up the parameter settings shall be stated by the Manufacturer/Supplier.

## **3.3 Software requirements**

### **3.3.1 Check of software versions**

It shall be possible to verify the current software version in the equipment.

### **3.3.2 Upgrading software**

When upgraded software is offered, the changes made between the software versions shall be specified.

## **3.4 Common equipment requirements (hardware and software)**

### **3.4.1 Cyber Security**

Requirements on Cyber Security are specified in TBE 100:2.

The documentation shall also comprise communication connections (internal/external), network, tools, storage media, access control etc.

### **3.4.2 Testability**

The Manufacturer/Supplier shall state how the equipment is to be verified after a replacement of a component, change/upgrade of software or in connection with recurring testing.

It shall be possible to verify (simulate) important functions which needs periodically testing and are specified in the Technical Specification.

### **3.4.3 Tools**

Tools used for testing, documentation, etc., shall have been evaluated and approved by the Manufacturer/Supplier.

### **3.4.4 Reliability**

The Manufacturer/Supplier shall state the reliability of the equipment. MTBF- and MTTR-figures shall be stated.

The Manufacturer/Supplier shall also submit references to previously supplied equipment of equivalent size or complexity.

### **3.4.5 Performance**

General requirements regarding measuring range, setting value and maximum error indication, accuracy, etc., are stated in the Technical Specification.

Unless the Technical Specification stipulates otherwise, the response time for measuring and operating functions shall not exceed 1 s and for safety functions 0.1 s. (These times do not include the running times of apparatus.)

The Manufacturer/Supplier shall state the response times for different functions. Response times shall be verified by testing.

### **3.4.6 Self-monitoring**

Internal monitoring and self-supervision shall exist to the necessary extent and be specified by the Manufacturer/Supplier.

### **3.4.7 Communication interface**

If a specific communication interface is required this is stated in the Technical Specifications.

### **3.4.8 Authorisation control**

It shall be possible to control authorisation for e.g. operators, maintenance personnel and modifications/changes.

### **3.4.9 Other requirements**

The system should be self-documenting, so that, in addition to software in the form of code, all information about the current configuration can be printed out on paper in a format that is clear and easy-to-read. Such a printout should consist of logic or function diagrams in graphical form, as well as parameter lists and signal address lists.

The applicability of the requirements is governed by the type of equipment/component and the complexity and is specified in the Technical Specifications.

For new versions of software, hardware and tools the Supplier/Manufacturer shall guarantee compatibility with old systems.

The Manufacturer/Supplier shall show how the Purchaser in a suitable manner will be able to maintain the system for a period of time longer than ten years.

## **4 Documentation**

### **4.1 General**

In addition to the documentation requirements according to TBE 100:1, the following requirements apply.

The information below shall be documented and supplied to the Purchaser.

The Manufacturers/Suppliers structure, content and designations for the documents may be different, but may also differ depending on the type of equipment.

The Manufacturer/Supplier shall describe their document structure and state in which documents the information below or the corresponding information is described.

If the documentation has to be designed in a particular way, the Purchaser shall specify this.

### **4.2 Product documentation**

As well as describing the component, including data sheets and specification, the technical description shall also describe the function of the software. The version/revision number of the software and hardware shall be stated.

The legal rules that apply to use of the software, copying of the software, and issues regarding software licence, shall be set out.

## 4.3 Design documentation

The design documentation describes how equipment and components are connected together electrically. Normally it includes:

- Internal and external connections
- Circuit diagram
- Terminal connections
- Component list
- Dimension details
- Installation instructions

Description of program function including communication

It shall be possible to follow signals by means of unambiguous references in the function diagram and to the circuit diagram and to other connected systems. The parameter list provides a list of timer circuits, counters and so on. There should be a list of the variables used. Where the parameters have particular properties, these shall be stated. Inputs and outputs are shown on the circuit diagram and need not be included in the parameter list unless they have specific properties.

The logic diagram and the control block diagram give an overall description of the working of the system. Generally it cannot be replaced by the function diagram, since this has such a high level of detail and information density that it becomes unsuitable for describing the function of the system for normal operation.

## 4.4 Maintenance documentation

The maintenance guide describes:

- Starting and restarting the system
- Backup procedure, restore procedure
- Interpretation of fault signals and fault printouts
- Fault localisation, troubleshooting
- Fault correction
- Preventive maintenance (checks, calibrations, cleaning, replacement of components with limited life in relation to the life of the system/component, etc.)
- Changing parameters
- Equipment for performing the above
- Linking between version/revision numbers for:
  - \* hardware
  - \* software
  - \* tools

## 4.5 Operating documentation

Documentation that is used for daily operation shall be written in Swedish.

## 4.6 Inspection documentation

The Manufacturer/Supplier shall show in writing that the development process invoked for the method used to produce the software is fulfilled on the basis of the chosen inspection plan. The Purchaser shall be given the opportunity to examine the Manufacturers/Suppliers method of production.

The Manufacturer/Supplier shall show the executed type tests and routine tests according to the agreed inspection plan.

See also KBE 100.

## 5 Agreement between Manufacturer/Supplier and Purchaser

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

1	Review and upgrading of Technical Specification.	
2	Description of development and design process	
3	Description of the life cycle of the product.	
4	Description of the configuration management plan	
5	Describe how the Requirements and applicable product standards are met.	
6	Battery backup and battery monitoring	
7	Storage media for software backup	
8	Human-machine interface Screens, colours, language Also applies on tools	
9	Compare new and old versions of the software and report differences.	
10	State the scope and possibilities of expandability.	
11	Authorisation for different levels of access	
12	Testability after a replacement or in connection with recurring testing.	
13	Tools evaluated and approved.	
14	The reliability of the equipment. Information + references	
15	Performance Capacity, including margins Response times + verification at test Measuring ranges, accuracies, fault display, bit resolution Time resolution	
16	Communication interface	
17	Product maintenance Support and service after phasing-out of the product by the supplier Supply of the same software for 15 years Compatibility with respect to equipment	
18	Statement of document structure and where the information according to the description can be found.	
19	Product documentation	
20	Design documentation	
21	Maintenance documentation	
22	Operating documentation	
23	Inspection documentation	
24	Analyses	
25	Interfaces to other systems in the plant	
26	Requirements to be met by hardware Storage media, environmental requirements, physical dimensions, electrical requirements	
27	Monitoring, self-testing	
28	Cyber Security	
29	Power supply	