

<b>Technical Requirements for Electrical Equipment</b>  Rubrik/Title <b>Programmable Electronics (PE) with programmable application</b>	Beteckning/Document TBE 106:1-2
	Utgåva/Issue 5 (E)
	Datum/Date 2017-05-22
	Ersätter / Supersedes 4 (E)

## Contents

1	Introduction	2
2	Definitions	2
3	Product Requirements	4
3.1	Standardisation	4
3.2	Hardware requirements	5
3.3	Software requirements	5
3.4	Common equipment requirements (hardware and software)	6
4	Documentation	8
4.1	General	8
4.2	Product documentation	8
4.3	Design documentation	9
4.4	Maintenance documentation	9
4.5	Operating documentation	10
4.6	Inspection documentation	10
4.7	Analyses	10
5	Agreement between Manufacturer/Supplier and Purchaser	11

Document	Issue	Date	Supersedes
TBE 106:1-2	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 programmable application (PE = programmable electronics).

In its basic version, the equipment consists of a general system in which a unique application can be programmed – or configured – by combining different standardised but product specific function modules/blocks/elements. The programming of the various function modules is seldom accessible. Usually it is delivered in a library of modules. After a running-in period, the application software can be locked by burning it into a PROM.

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.

These requirements specify 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 classified as 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.

## Application software, base software, etc.

The software can be divided into the following levels:

1. Microprograms	System software	Basic essential software
2. Compiler		
3. Operating system		
4. Standard software		
5. Application software		
6. Default position parameters (defined operating mode, limit value, etc.)		
7. Operating parameters (operating mode, set point, etc.)		

## Application software

*A computer program that performs a task related to the process being controlled rather than to the function of the computer itself (IEC 60880).*

The part of the software that is linked to the function of the controlled process

## Default position parameters

These define the position of the equipment involved in a controlled process in certain defined operating modes, such as start up, safe state, etc. In addition, they describe settings of parameters for signal, activation, regulating characteristics, etc.

## Basic essential software

System software and standard software together. These define a general PE system without application software

## 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)

## **PROM**

Programmable Read-Only Memory

## **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.*

## **Standard software**

The specific software with modules (function blocks, “building blocks”) that characterise the particular system as produced by the Supplier/Manufacturer of a given PE system. Usually delivered as a software library

## **System software**

*Software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs, for example, operating systems, compilers, utilities. System software is usually composed of operational system software and support software. (IEC 60880)*

# **3 Product Requirements**

## **3.1 Standardisation**

The method used to produce the product shall conform to a development process which follows the requirements according to IEC61508 SIL2, IEC 62138 or requirement according to ISO 9001 and ISO 90003.

Documented and traceable operating experiences may to some extent compensate the shortcomings of the method used to produce the software.

Regarding requirements to be met by quality systems 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 being 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 the base software and application 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-106:1-2 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 by the Manufacturer/Supplier.

### **3.2.2 Storage media**

Storage media and equipment for backing up the software (basic essential, application, databases, etc.) shall be stated by the Supplier/Manufacturer.

### **3.2.3 Image presentation**

Image presentations shall be chosen considering the relatively bright lighting which normally prevails in the control room.

### **3.2.4 Maintenance requirements**

It shall be possible to change cards without shutting down the whole equipment/system. Restarting the replaced part is acceptable. The Manufacturer/Supplier shall present the equipment behaviour during the start-up process e.g. data handling, output settings, influence on other system parts etc.

### **3.2.5 Power supply**

The Manufacturer/Supplier shall present how the equipment behaves during disturbances in the power supply out of the specified range. An alarm is necessary when the voltage level diverges from the specified value.

## **3.3 Software requirements**

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

The system or the tool shall be able to compare new and old versions of the software and to report differences.

### **3.3.2 Upgrading base software**

When upgraded basic essential software is offered, the changes made between the software versions shall be specified. The connection to and influence on other parts of the software shall be shown.

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

### **3.4.1 Expandability of functionality**

The Manufacturer/Supplier shall state the scope and possibilities to expand the functionality and performance of the equipment.

### **3.4.2 Authorisation control**

It shall be possible to control authorisation for at least the following:

- *change in application software*
- *change of parameters such as alarm and limit values for activation, (base position parameters)*
- *normal operator management.*

Changes in authorisation protected areas shall automatically be marked with time and authorisation signature.

### **3.4.3 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.

### **3.4.4 Testability**

The Manufacturer/Supplier shall state how the equipment is to be verified after a replacement of 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

### **3.4.5 Tools**

Tools used for programming, image generation, testing, documentation, etc., shall be evaluated and approved by the Manufacturer/Supplier.

### **3.4.6 Man-machine interface**

The Purchaser shall be able to choose colours for different functions.

Alarm texts and other texts shall be writeable with Swedish letters.

The above is also applicable for programming tools, tools for parameter setting, tests, maintenance etc.

Surveillance and manoeuvre shall occur in a manner which is easy, unambiguous and well arranged for the operator.

### **3.4.7 Reliability**

The Manufacturer/Supplier shall state the reliability of the equipment. MTBF and MTTR figures shall be stated. The pieces of information shall be shown at the equipment level or for the configuration which applies for the system in question.

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

### **3.4.8 Performance**

The Manufacturer/Supplier shall state bit resolution and response time.

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.). First response of a pressed button/keyboard 0.1 s.

Response time for static display, i.e. from pressing a button/keyboard to presentation of entire display: 0.5 s. Response time for entire display, with 50 dynamic points, i.e. from press of a button/keyboard to presentation of entire display is maximum 2 s.

Corresponding response times for trend displays is maximum 4.0 s.

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

### **3.4.9 Self-monitoring**

There shall be a requisite amount of monitoring of information flows during execution. This shall be specified by the Manufacturer/Supplier.

Implausible signals from the process shall give an alarm and lead to a safe state.

For defined Cyber Security Attacks the system shall give an alarm and if possible enter into a defined or safe state.

#### Logging of fault events

All faults that occur on the equipment in service shall be recorded and be printable on paper.

### **3.4.10 Capacity**

The load of the central unit (processor) shall not be higher than that the function with the lowest priority, with a margin, can be guaranteed to be executed within the prescribed response time.

### **3.4.11 Communication interface**

The equipment shall be capable of communicating with other computer systems by standardised protocols.

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

### **3.4.12 Other requirements**

For new versions of software, hardware and tools, the Manufacturer/Supplier shall guarantee compatibility with old systems. The Manufacturer/Supplier shall show how the Purchaser will be able to maintain the system for a longer period of time than ten years.

The system should be self-documenting, so that, in addition to application 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.

## **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 Manufacturer/Supplier 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 shall be designed in a specific way, the Purchaser shall specify this.

### **4.2 Product documentation**

As well as describing the equipment, 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.

#### Standard software – Module description

Each module shall be well described with regard to function, way of working, inputs and outputs, parameters and other data of interest.

The programming instruction shall describe the procedure for programming and database configuration and give instructions for image generation. Examples of typical cases shall be given.

The legal rules that apply to use of the software, copying of the software, and issues regarding software license, 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*
- *Card type*
- *Card position*
- *Signal names*
- *Unambiguous references to the function diagram*
- *Rules for handling/storage*

A main document which, together with the circuit diagram and the signal address list, gives a complete picture of the entire function of the system. In most systems there is a facility for automatically generating the function diagram.

Descriptions shall be provided of program function, database and graphical presentation of configuration the system, including communication.

There shall be a graphical overview diagram of software and software modules.

It shall be possible to follow signals by means of unambiguous references in the function diagram and to the circuit diagram, within the system and to other connected systems.

The logic diagram and the control block diagram give an overall description of the function 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 in normal operation.

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 particular properties.

## 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)*
- *Changing parameters*
- *Equipment for performing the above*

- *Linking between version/revision numbers for:*
  - \* *hardware*
  - \* *software*
  - \* *tools*
- *Rules for handling/storage of the software*

## **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 and review the Manufacturer/Supplier 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.

## **4.7 Analyses**

Reliability studies (method and results) shall be documented.

## 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. Support	
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 Applies also on tools	
9	Compare new and old versions of the software and report differences	
10	Compare the software version currently in the equipment and stored copies	
11	State the scope and possibilities of expandability	
12	Authorisation for different levels of access	
13	Testability after a replacement or in connection with recurring testing.	
14	Tools evaluated and approved	
15	The reliability of the equipment Information + references	
16	Performance Capacity, including margins Response times + verification at test Measuring ranges, accuracies, fault display, bit resolution Time resolution	
17	Statement of document structure and where the information according to the description can be found	
18	Product documentation	
19	Design documentation	
20	Maintenance documentation	
21	Operating documentation	
22	Inspection documentation	
23	Analyses	
24	Interfaces to other systems in the plant	
25	Architectural/Structural requirements	
26	Communication requirements, including requirements for functional separation	
27	Operator communication	
28	Maintainability, requirements regarding certain actions in service (e.g. card and battery replacement)	

29	Requirements to be met by hardware Storage media, environmental requirements, physical dimensions, electrical requirements	
30	Cyber Security	
31	Defined state when fail/error occur	
32	Delivery of source code	
33	Power Supply	