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

Contents

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.

The Requirement 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 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:

<table>
<tr><td>1. Microprograms</td><td rowspan="3">System software</td><td rowspan="4">Basic essential software</td></tr>
<tr><td>2. Compiler</td></tr>
<tr><td>3. Operating system</td></tr>
<tr><td colspan="2">4. Standard software</td></tr>
<tr><td colspan="3">5. Application software</td></tr>
<tr><td colspan="3">6. Default position parameters (defined operating mode, limit value, etc.)</td></tr>
<tr><td colspan="3">7. Operating parameters (operating mode, set point, etc.)</td></tr>
</table>

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.

CCF, Common Cause Failure

Faults which have the same origin, e.g. faulty specification or software fault in identical redundant channels.

Diversification

Existence of different means of performing a required function (e.g. other physical principles, other ways of solving the same task) (IEC 60880)

Operating parameters

The changes in apparatus positions, set points etc. that are included in normal actions during operation.

FMEA

Failure Mode and Effect Analysis

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)

RAM

Random Access Memory

Read/write memory - not permanent.

Redundancy

Provision of alternate (identical or diverse) elements or systems so that any one can perform the required function regardless of the state of operation or failure of any other. (IAEA 50-SG-D8)

Standard software

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

ROM

Read-Only Memory, Read memory – permanent

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 IEC 60987 for hardware, IEC 60880 for software and IEC 61513 for common system requirements for hardware and software requirements.

If other than the above mentioned development processes have been used, the Manufacturer/Supplier shall compare and specify to what extent the invoked standard or development process satisfies the requirements set out in IEC 60880, IEC 60987 and IEC 61513.

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 lifecycle 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 present 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-106:1-1 with associated examination procedures.

3.2 Hardware requirements

3.2.1 Battery backup

If battery backup is included, the life of the batteries shall be stated by the Manufacturer/Supplier. The batteries shall have a service life of at least five years.

The capacity of the batteries shall be monitored. In the event of a low charge alarm there shall be a running remaining capacity of at least two months.

3.2.2 Storage media

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

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

In the event of a change, the system or the tool shall be able to compare new and old versions of the software and to report differences.

Changes shall be marked with time and the id code of the person who made the change.

3.3.2 Upgrading base software

When upgraded base 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.

3.3.3 Software design

Standard software shall be strictly divided into modules or subroutines with as few interdependencies as possible. The modules shall be well delimited as regards function and content, with well-defined inputs and outputs to other modules. Program modules in the basic essential software shall normally not be modified during application programming, without the Purchasers approval.

3.3.4 Unused software

Unused software or parts of software should preferably be removed. If this is not done, the Manufacturer/Supplier shall demonstrate how execution of unused software is prevented not affecting the software that is used.

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)
- 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 have been evaluated and approved by the Manufacturer/Supplier.

The Manufacturer/Supplier shall show if it is considered suitable to connect tools with the equipment in operation and how this is done, e.g. analysis of the equipment, reading of parameters etc. In the documentation it shall be described which limitations there are for allowing such a connection and how it affects the equipment.

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 manoeuvres 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 Supplier/Manufacturer shall describe the calculation methods used and the bases for assessment. The pieces of information shall be shown at the equipment level or for the configuration which applies for the system.

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 keypress 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.

The 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. The Manufacturer/Supplier shall specify what monitoring functions there are. Such monitoring functions shall not affect safety functions that may be invoked by the equipment.

The status of the hardware shall also be monitored, e.g. a ”watchdog” with time monitoring of the work of the processor. In abnormal conditions, the equipment shall go to a predetermined safe state and give an alarm.

Every incorrect or implausible entry of data or instructions shall be prevented and give a warning/help.

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.

Check of memory content

Base and application software shall not be affected during execution. Memory areas where such software is stored should therefore be checked automatically or periodically in normal operation with a checksum or similar. Where base software and parameters are read on start up, e.g. from ROM to RAM, with which the processor subsequently works, the RAM shall periodically be checked against the ROM in the same way.

3.4.10 Safe state

In the event of a fault such that the equipment cannot perform its safety functions, the equipment shall put all outputs in a safe state and give an alarm. This also applies to the loss of power supply voltage. Safe state may mean start, stop, open, close or continued operation of a number of functions and is defined in the Technical Specification.

3.4.11 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.

The Manufacturer/Supplier shall state the method for determining the load. The value shall be verified by testing.

It shall be possible to calculate the CPU load according to a deterministic method specified by the Manufacturer/Supplier. It shall be possible to display the present value and history on request. This is also applicable for network load.

3.4.12 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.

3.4.13 Redundant functions

Redundant process functions in the same equipment shall be treated in different processors without communication between them. A fault in the processor may not influence the other redundant processor.

3.4.14 Other requirements

The Manufacturer/Supplier shall have a system for actively gathering experiences and disseminating information to owners of the equipment in question. This requires checking of the versions of hardware, software and tools supplied at different times.

The Manufacturer/Supplier shall continuously inform the Purchaser of discovered faults and shortcomings that may affect the function in the application that the Purchaser has.

The Manufacturer/Supplier shall be able to supply identical software and hardware of the system for at least 10 years from the start date of operation of the system by the Purchaser. The Manufacturer/Supplier shall be able to promise service and customer support for at least the same period.

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.

Testing the system shall normally be possible without that the complete or part of the system needs to be taken out of operation and by this may negatively affect the process functions of the plant.

Attention shall be called for via the alarm function if the system is disconnected or taken out of operation for any reason.

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 deliver the executed type tests and routine tests according to the agreed inspection plan.

If a complete system/process function is delivered complementary documentation may be required. This is specified in the order/contract. The Manufacturer/Supplier shall upon request present the requested documentation.

See also KBE 100.

4.7 Analyses

The following shall be described in the form of reports:

- Reliability studies
- FMEA
- CCF

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 Changes shall be marked	
10	Statement of unused software	
11	Compare the software version currently in the equipment and stored copies.	
12	State the scope and possibilities of expandability	
13	Authorisation for different levels of access	
14	Testability after a replacement or in connection with recurring testing	
15	Tools evaluated and approved	
16	The reliability of the equipment Information + references	
17	Performance Capacity, including margins Response times + verification at test Measuring ranges, accuracies, fault display, bit resolution Time resolution	
18	Self-monitoring	
19	Check of memory content	
20	Logging of fault events	
21	Safe state	
22	Method for determining CPU load The load is verified in load tests	
23	Communication interface	
24	Gathering of experiences and disseminating these to users. Discovered faults that may affect the application	
25	Product maintenance Support and service after phasing-out of the product by the supplier/manufacturer Supply of the same software for 10 years Compatibility with respect to equipment/software	
26	Statement of document structure and where the information according to the description can be found.	
27	Product documentation	
28	Design documentation	

29	Maintenance documentation	
30	Operating documentation	
31	Inspection documentation	
32	Analyses	
33	Interfaces to other systems in the plant	
34	Architectural/Structural requirements	
35	Communication requirements, including requirements for functional separation	
36	Operator communication	
37	Maintainability, requirements regarding certain actions in service (e.g. card and battery replacement)	
38	Requirements to be met by hardware Storage media, environmental requirements, physical dimensions, electrical requirements	
39	Single failure, redundancy, physical separation	
40	Degree and method of diversification	
41	Analysis of risk factors	
42	Monitoring, self-testing	
43	Data flow in the communication interface	
44	Cyber Security	
45	Delivery of source code	
46	Power Supply	