Technical Requirements for Electrical Equipment Rubrik/Title Programmable electronics with fixed application	Beteckning/Document TBE 106:2-1
	Utgåva/Issue 2 (E)
	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 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, transmitters and protection relays.

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 a 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 classification1E- 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.

CCF (Common Cause Failure)

Failures that have the same origin, e.g. incorrect specification or software faults in identical redundant channels.

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
- micro-controllers
- 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)

RAM

Random Access Memory.

Read/write memory - not permanent.

ROM

Read-Only Memory.

Read memory – 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).

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 follows the requirements according to IEC 60987 for hardware and IEC 60880 for software.

A development process according to IEC 61508 with SIL 2 supplemented with operating experiences may be accepted following an assessment and approval by the Purchaser.

If SIL 3 is required lower SIL classification of the component (SIL 2) may be approved if it is configured according to the requirements in IEC 61508 to fulfil SIL 3.

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 fulfils the requirements according to IEC 60880 and IEC 60987.

Documented and traceable operating experiences may to a certain extent compensate deficiencies in the production 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 different stages of completion 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-106:2-1 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.

In the event of a low charge alarm there shall be a battery reserve of at least two months.

3.2.2 Storage media

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

3.2.3 Power supply

The Manufacturer/Supplier shall present how the equipment behaves during disturbances in the power supply out of the specified range. An alarm shall be given when the supply deviates from the permitted value.

3.3 Software requirement

3.3.1 Check of software versions

It shall be possible to read 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. The connection of the change and its influence on other parts of the software shall be presented.

3.4 Common equipment requirements (hardware and software)

3.4.1 Cyber Security

Requirements on Cyber Security 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, a 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.

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.

3.4.4 Reliability

The Manufacturer/Supplier shall state the reliability of the equipment. MTBF and MTTR figures shall be stated. The Manufacturer/Supplier shall describe the calculation methods used and the bases for assessment.

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

There shall be the requisite amount of monitoring of information flows during execution. The Manufacturer/Supplier shall specify what checking functions there are. Such checking 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” for time monitoring the work of the processor. In abnormal conditions, the equipment shall enter into a defined state and give an alarm.

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

Logging of fault events

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

Check of memory content

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 software and parameters are read on start up e.g. from ROM to RAM, to which the processor works, the RAM shall be periodically be checked to the ROM in the same way.

3.4.7 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 can mean start, stop, open, close or continued operation of a number of functions and is defined in the Technical Specification.

3.4.8 Communication interface

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

3.4.9 Authorisation control

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

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

– Change of parameters such as alarm and limit values for activation.

3.4.10 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 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 equipment/component type and complexity and is specified in the Technical Specification.

The Manufacturer/Supplier shall be able to supply identical software and hardware of the system for at least ten 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.

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 shall be stated

There shall be a description of function, way of working, inputs and outputs, parameters and other data of interest.

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

A main document which gives a complete picture of the entire function of the system including communication.

The scope of the description is governed by the size and complexity of the system.

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 particular properties.

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.

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.

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 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	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	Self-monitoring	
17	Check of memory content	
18	Logging of fault events	
19	Safe state	
20	Communication interface	
21	Gathering of experiences and disseminating these to users. Discovered faults that may affect the application	
22	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	
23	Statement of document structure and where the information according to the description can be found.	
24	Product documentation	
25	Design documentation	
26	Maintenance documentation	
27	Operating documentation	
28	Inspection documentation	

29	Analyses	
30	Interfaces to other systems in the plant	
31	Requirements to be met by hardware Storage media, environmental requirements, physical dimensions, electrical requirements	
32	Monitoring, self-testing	
33	Cyber Security	
34	Power supply	