Tekniska bestämmelser för elektrisk utrustning	Beteckning/Document TBE 106:2-1
	Utgåva/Issue 2 (S)
Rubrik/Title Programmerbar elektronik fast applikation	Datum/Date 2017-05-22
	Ersätter/Supersedes 2 (S)

Innehåll

1 Inledning

Dessa Tekniska Bestämmelser anger de krav som ställs på programmerbar elektronik avsedda för användning i kärnkraftverk. De Tekniska bestämmelserna omfattar endast krav för tekniska system. Administrativa datorsystem omfattas ej av dessa bestämmelser. Kraven ska uppfyllas av Tillverkaren/Leverantören för att uppnå de svenska kärnkraftverksägarnas målsättning avseende säkerhet och tillförlitlighet.

Syftet med denna handling är att ge allmänna krav på programmerbar elektronik samt på processen att utveckla programvaran.

Övergripande krav på den programmerbara utrustningen samt övriga anvisningar för Tillverkaren/Leverantören, framgår av andra bestämmelser enligt den Tekniska Specifikationen.

Utöver bestämmelserna i detta dokument, gäller kraven i TBE 100:1, Gemensamma Tekniska Bestämmelser och förklaringar, i tillämpliga delar.

PE med fast applikation (PE = programmerbar elektronik). Denna kan liksom PE med programmerbar applikation realisera systemfunktioner men programfunktionerna är inte tillgängliga för användaren att ändra. Tillämpningen kan bara konfigureras genom att sätta vissa parametrar vanligen med knappar och vred på fronten alternativt kan inställning med anslutningsbart hjälpmedel förekomma. Exempel på utrustning kan vara UPS, ställverk/brytare, frekvensomriktare, transmittrar och reläskydd.

Denna bestämmelse ska tillämpas på alla komponenter och utrustningar där funktionen realiseras med programvara för att samla in data, omvandla data, styra eller reglera en annan utrustning.

Bestämmelsen specificerar de tekniska krav som krävs för att uppnå tillräcklig säkerhet vid realiserandet av skyddsfunktioner med PE-utrustning.

Utifrån utrustningens funktionella krav och övriga för anläggningen specifika aspekter delas TBE 106 in i 2 kravnivåer. Kravnivåerna kan inte direkt översättas till anläggningarnas klassningsprinciper med avseende på elektrisk funktionsklass utan en bedömning måste göras i varje enskilt fall när kravnivån väljs.

Kravnivåerna benämns TBE 106: X-1 och TBE 106: X-2 där nivå -1 utgör den högsta kravnivån.

För utrustning tillhörande elektrisk funktionsklass 1E- enligt IEEE och kategori A-utrustning enligt IEC 61226 ska alltid TBE 106: X-1 tillämpas.

2 Definitioner

I de fall definitioner är hämtade från någon etablerad standard anges originaltexten oöversatt i kursiv stil med angivande av källan. Övriga definitioner är specifikt framtagna för denna handling.

CCF, Common Cause Failure

Fel som har samma ursprung, t.ex. felaktig specifikation eller programvarufel i identiska redundanta kanaler

FMEA

Failure Mode and Effect Analysis

Maskinvara

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

Modul

Ett logiskt avgränsat programavsnitt eller en subrutin som är definierad till sin funktion och med definierade gränssnitt mot omvärlden. Vanlig betydelse i ett PE system är ett funktionsblock t.ex. en logisk grind eller regulator, som via applikationsprogrammering konfigureras och sätts samman med andra moduler till en systemfunktion.

MTBF

Mean Time Between Failure

MTTR

Mean Time To Repair

Programmerbar elektronik (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)

Programvara

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.

Läs- och skriv-minne - ej beständigt

ROM

Read-only memory.

Läsminne , beständigt

Redundans

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 Produktkrav

3.1 Standardisering

Framtagningen av produkten ska ha skett enligt en utvecklingsmodell som följer kraven enligt IEC 60987 för maskinvara och IEC 60880 för programvara.

Utvecklingsmodell enligt IEC 61508 med SIL 2 kompletterad med drifterfarenheter kan accepteras efter utvärdering och godkännande av Beställaren.

Om högre krav (t.ex. SIL 3) krävs kan detta uppfyllas med komponenter uppfyllande SIL 2 om dessa komponenter sätts samman enligt beskrivning i IEC 61508 så att det uppfyller krav på SIL 3.

Om andra än ovanstående utvecklingsmodeller har använts ska Tillverkaren/Leverantören göra jämförelse och ange i vilken grad åberopad standard eller utvecklingsmodell uppfyller kraven enligt IEC 60880 och IEC 60987.

Dokumenterade och spårbara drifterfarenheter kan till viss del kompensera brister i framtagnings-metodiken.

Beträffande krav på kvalitetssystem hänvisas till KBE 100.

Framtagningsmetodiken för produkten ska beskriva ett livscykeltänkande från produktidé till avveckling av produkten. Detta innefattar även beskrivning av hur produkten kan ersättas med annan kompatibel utrustning och hur support fungerar efter det att produkten inte längre är kommersiellt tillgänglig.

Av speciell vikt är att Tillverkaren/Leverantören kan visa en konfigurationsstyrningsplan som ger underlag för att definiera, styra och spåra krav vid olika fasavslut under konstruktionsprocessen samt tillhörande dokumentation och versioner av programvara.

Tillverkaren/Leverantören ska i Anbudet redovisa hur föreskrifter och tillämpliga produkt-standarder uppfylls.

Generell kontrollplan framgår av KBE IP 106:2-1 med tillhörande kontrollmoment.

3.2 Krav på maskinvara

3.2.1 Batteribackup

Om batteribackup ingår ska batteriernas livslängd redovisas av Tillverkaren/Leverantören. Batterierna ska ha en livslängd om minst 5 år.

Vid larm om låg laddning ska det finnas en batterireserv om minst 2 månader.

3.2.2 Lagringsmedia

Lagringsmedia och utrustning för backup av parmeterinställningar ska anges av Tillverkaren/Leverantören.

3.2.3 Spänningsmatning

Tillverkaren/Leverantören ska redovisa hur utrustningen uppträder vid störningar i spänningsmatningen utanför specificerat intervall. Larm ska ges då spänningsnivån avviker från tillåtet värde.

3.3 Krav på programvara

3.3.1 Kontroll av programversioner

Det ska finnas möjlighet att utläsa befintlig programversion i utrustningen.

3.3.2 Uppgradering av program

Vid eventuellt erbjudande av uppgraderad programvara ska det framgå vilka ändringar som införts mellan de aktuella programversionerna. Ändringens koppling och påverkan på övriga delar i programvaran ska redovisas.

3.4 Gemensamma utrustningskrav (maskin- och programvara)

3.4.1 IT-säkerhet

Krav på IT-säkerhet anges i TBE 100:2

Redovisningen ska även omfatta kommunikationsanslutningar (interna/externa), nätverk, hjälpmedel, lagringsmedia, behörigheter m.m.

3.4.2 Testbarhet

Tillverkaren/Leverantören ska redovisa hur utrustningen ska verifieras efter ett utbyte av komponent, ändring/uppgradering av programvara eller i samband med återkommande provning.

Viktiga funktioner som kräver regelbunden provning specificeras i Teknisk Specifikation och ska kunna verifieras (simuleras).

3.4.3 Hjälpmedel

Hjälpmedel som används för test, dokumentation etc. ska vara utvärderade och godkända av Tillverkaren/Leverantören.

Tillverkaren/Leverantören ska redovisa om det kan anses vara lämpligt att ansluta hjälpmedel med utrustningen i drift samt hur detta görs, t.ex. analys av utrustningen, utläsning av parametrar m.m. Redovisning ska göras av vilka begränsningar som finns för att sådan anslutning ska få ske och vilken påverkan på utrustningen det medför.

3.4.4 Tillförlitlighet

Utrustningens tillförlitlighet ska anges av Tillverkaren/Leverantören. Uppgifter om MTBF och MTTR värden ska anges. Tillverkaren/Leverantören ska beskriva använda beräkningsmetoder och bedömningsgrunder.

Tillverkaren/Leverantören ska också lämna referenser till tidigare levererad utrustning av motsvarande storlek eller komplexitet.

3.4.5 Prestanda

Allmänna krav på mätområde, inställningsvärde och maximal felvisning, noggrannhet, etc. framgår av Teknisk Specifikation.

Om inget annat anges i Teknisk Specifikation får svarstid för mät- och manöverfunktioner inte överstiga 1 s och för skyddsfunktioner 0,1 s. (I dessa tider räknas inte apparaters gångtider).

Tillverkaren/Leverantören ska ange de aktuella svarstiderna för olika funktioner. Svarstider ska verifieras genom test.

3.4.6 Egenövervakning

Interna övervakningar av informationsflöden under exekvering ska finnas i erforderlig omfattning. Tillverkaren/Leverantören ska specificera vilka kontrollfunktioner som finns. Sådana kontrollfunktioner får inte påverka säkerhetsfunktioner som kan påkallas av utrustningen.

Även maskinvarans status ska vara övervakad. t.ex. ”watch-dog” för tidsövervakning av processorns arbete. Vid onormala förhållanden ska utrustningen gå till ett definierat läge och ge larm.

Varje felaktig eller orimlig inmatning av data eller instruktioner ska förhindras och ge varning/ hjälp.

<u>Loggning av felhändelser</u>

Alla fel som inträffar på utrustningen under drift ska registreras och kunna skrivas ut på papper.

<u>Kontroll av minnesinnehåll</u>

Program får inte påverkas under exekvering. Därför bör minnesareor där sådant lagras, kontrolleras automatiskt eller periodiskt under normal drift med checksumma eller liknande. Då program och parametrar vid uppstart läses t.ex. från ROM till RAM, vilket processorn arbetar mot, ska RAM periodiskt kontrolleras mot ROM på samma sätt.

3.4.7 Säkert läge

Utrustningen ska vid fel av sådan art, att den inte kan fullfölja sina säkerhetsfunktioner, sätta alla utgångar till säkert läge och ge larm. Detta gäller också bortfall av matningsspänning. Säkert läge kan innebära start, stopp, öppna, stänga eller fortsatt drift av ett antal funktioner och definieras i Teknisk Specifikation.

3.4.8 Kommunikationsgränssnitt

Om specifikt kommunikationsgränssnitt krävs anges detta i Teknisk Specifikation.

3.4.9 Behörighetsstyrning

Möjlighet att styra behörigheten för olika nivåer (t.ex. operatör, underhåll, ändringar) ska finnas.

Möjlighet att styra behörigheten ska finnas för följande:

– ändring av parametrar som larm- och gränsvärden för utlösning.

3.4.10 Övriga krav

Tillverkaren/Leverantören ska ha ett system för aktiv inhämtning av erfarenheter och spridande av information till innehavare av den aktuella utrustningen. Detta kräver kontroll av de versioner av maskinvara, programvara och hjälpmedel som levererats vid olika tillfällen.

Utrustning bör vara självdokumenterande så att all information om aktuell konfigurering kan fås utskrivet på papper i överskådlig och lättläst form. Sådan utskrift bör vara logik- eller funktionsscheman i grafisk form samt parameter- och signaladresslistor. Kravets tillämpbarhet styrs av utrustningstyp/komponenttyp och komplexitet och specificeras i Teknisk Specifikation.

Tillverkaren/Leverantören ska kunna leverera identisk programvara och maskinvara i minst 10 år från det att utrustningen tagits i drift av Beställaren. Tillverkaren/Leverantören ska kunna utlova service och kundstöd under minst samma tid.

För nya versioner av programvara, maskinvara och hjälpmedel ska Tillverkaren/Leverantören garantera kompatibilitet med gamla system.

Tillverkaren/Leverantören ska redovisa hur Beställaren på lämpligt sätt ska kunna vidmakthålla systemet under längre tid än 10 år.

4 Dokumentation

4.1 Allmänt

Utöver krav på dokumentation enligt TBE 100:1 gäller följande krav.

Nedanstående information ska vara dokumenterad och levereras till Beställare.

Tillverkaren/Leverantören struktur, innehåll och benämningar på dokumenten kan vara annorlunda men även skilja sig åt beroende på typ av utrustning.

Tillverkaren/Leverantören ska beskriva sin dokumentstruktur och ange i vilka dokument informationen enligt nedan eller motsvarande information finns beskriven.

Om dokumentationen ska utformas på ett speciellt sätt ska detta specificeras av Beställare.

4.2 Produktdokumentation

Teknisk beskrivning ska förutom beskrivning av utrustningen inklusive datablad och specifikation, även beskriva programvarans funktion.

Programvarans och hårdvarans versions-/revisionsnummer ska anges.

Beskrivning med avseende på funktion, arbetssätt, in- och utgångar, parametrar och övriga data av intresse ska finnas.

De juridiska reglerna som gäller för användande och kopiering samt licensfrågor ska framgå.

4.3 Konstruktionsdokumentation

Konstruktionsdokumentationen beskriver hur utrustningar och komponenter kopplas ihop elektriskt och innehåller normalt:

- Inre och yttre förbindningar
- Kretsschema
- Plintanslutningar
- Komponentförteckning
- Måttuppgifter
- Montageanvisning

Ett huvuddokument som ger en fullständig bild av systemets hela funktion inklusive kommunikation ska redovisas. Omfattningen av beskrivningen styrs av systemets storlek och komplexitet.

Beskrivning av programfunktion inklusive kommunikation.

Signalföljning ska kunna göras genom entydiga hänvisningar inom funktionsschemat och till kretsschema samt anslutning till andra system.

Parameterlistan ger en förteckning över tidkretsar, räknare och liknande. Lista på använda variabler bör finnas. I de fall parametrarna har speciella egenskaper ska dessa anges. In- och utgångar presenteras i kretsschema och behöver inte ingå i parameterlistan såvida de inte har speciella egenskaper.

Logikschemat och reglerblockschemat beskriver översiktligt systemets funktion. Det kan som regel inte ersättas av funktionsschemat då detta är utformat med så hög detaljeringsgrad och informationstäthet, att det blir olämpligt för att beskriva systemfunktionen för normal drift.

4.4 Underhållsdokumentation

Underhållshandledningen beskriver:

- Uppstart, omstart av systemet

- Backuphantering, återlagringsförfarande
- Tolkning av felsignaler och felutskrifter
- Fellokalisering
- Felavhjälpning
- Förebyggande underhåll (kontroller, kalibreringar, rengöring, utbyte av komponenter med begränsad livslängd i förhållande till systemets/komponentens livslängd mm)
- Ändring av parametrar
- Utrustning för att utföra ovanstående
- Koppling mellan versions-/revisionsnummer för:
  * maskinvara
  * programvara
  * hjälpmedel

4.5 Driftdokumentation

Dokumentation som används för dagligt handhavande ska vara skriven på svenska.

4.6 Kontrolldokumentation

Tillverkaren/Leverantören ska skriftligen visa att den åberopade utvecklingsmodellen för programvarans framtagningsmetodik uppfylls utifrån vald kontrollplan. Beställaren ska ges möjlighet att granska Tillverkaren/Leverantören framtagningsmetodik.

Tillverkaren/Leverantören ska redovisa genomförda typprov och allprov enligt överenskommen kontrollplan. Se även KBE 100.

4.7 Analyser

Följande ska redovisas i form av rapporter:

- Tillförlitlighetsstudier
- FMEA
- CCF

5 Överenskommelse mellan Tillverkare/Leverantör och Beställare

Nedanstående checklista bör tjäna som underlag för genomgång mellan Tillverkare/Leverantör och Beställare i samband med offert eller beställning.

1	Genomgång och komplettering av Teknisk Specifikation.	
2	Redovisning av utvecklings- och konstruktionsmodell	
3	Beskrivning av produktens livscykel	
4	Redovisning av konfigurationsstyrningsplan	
5	Redovisa hur föreskrifter och tillämpliga produktstandarder uppfylls	
6	Batteribackup och batteriövervakning	
7	Lagringsmedia för backup av programvaran	
8	Människa-maskin interface Skärmar, färger, språk Gäller även hjälpmedel	
9	Jämföra ny och gammal programversion och rapportera skillnader Ändringar ska vara märkta	
10	Redovisa möjligheter och omfattning på utbyggbarhet	
11	Behörighet för olika nivåer	
12	Testbarhet efter ett utbyte eller i samband med återkommande provning	
13	Hjälpmedel utvärderade och godkända	
14	Utrustningens tillförlitlighet Uppgifter + referenser	
15	Prestanda Kapacitet, med marginaler Svarstider + verifiering vid test Mätområden, noggrannheter, felvisning, bitupplösning Tidsupplösning	
16	Egenövervakning	
17	Kontroll av minnesinnehåll	
18	Loggning av felhändelser	
19	Säkert läge	
20	Kommunikationsgränssnitt	
21	Inhämtande av erfarenheter och sprida detta till användare Upptäckta fel som kan påverka applikationen	
22	Produktunderhåll Support och service efter leverantörens utfasning av produkten Leverans av samma programvara i 10 år Kompatibilitet avseende utrustning/programvara	
23	Redovisning av dokumentstruktur och var informationen enligt beskrivningen finns beskriven	
24	Produktdokumentation	
25	Konstruktionsdokumentation	
26	Underhållsdokumentation	
27	Driftdokumentation	
28	Kontrolldokumentation	
29	Analyser	

30	Gränssnitt/interface mot anläggningens övriga system	
31	Krav på maskinvaran Lagringsmedia, miljökrav, fysiska dimensioner, elektriska krav	
32	Övervakning, självtest	
33	IT-säkerhet	
34	Spänningsmatning	