Tekniska bestämmelser för elektrisk utrustning	Beteckning/Document TBE 106:1-2
	Utgåva/Issue 5 (S)
Rubrik/Title Programmerbar Elektronik (PE) med programmerbar applikation	Datum/Date 2017-05-22
	Ersätter/Supersedes 4 (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 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 Tillverkare/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 programmerbar applikation (PE = programmerbar elektronik). Utrustningen består i sitt basutförande av ett generellt system, där en unik applikation kan programmeras - eller snarare konfigureras genom kombination av olika standardiserade men produktspecifika funktionsmoduler/block/element. De olika funktionsmodulerna är sällan åtkomliga utan levereras som regel i någon form av programbibliotek. Applikationsprogrammet kan även efter en inkörningsperiod låsas via inbränning i PROM.

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 eller 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.

Applikationsprogram, basprogram etc.

Programvaran kan indelas i följande nivåer:

<table>
<tr><td>1. Mikroprogram</td><td rowspan="3">Systemprogram</td><td rowspan="4">Basprogram</td></tr>
<tr><td>2. Kompilator</td></tr>
<tr><td>3. Operativsystem</td></tr>
<tr><td colspan="2">4. Standardprogram</td></tr>
<tr><td colspan="3">5. Applikationsprogram</td></tr>
<tr><td colspan="3">6. Baslägesparametrar (definierat driftläge, gränsvärde etc.)</td></tr>
<tr><td colspan="3">7. Driftparametrar (driftläge, börvärde etc.)</td></tr>
</table>

Applikationsprogram

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

Den del av programvaran som är bunden till den styrda processens funktion.

Baslägesparametrar

Definierar läge hos de i en styrd process ingående apparater vid vissa definierade driftlägen, såsom uppstart, säkert läge etc. Dessutom inställningsvärden hos

parametrar för signal, utlösning, reglerkarakteristiker mm.

Basprogram

Systemprogram och Standardprogram tillsammans. Definierar ett generellt PE-system utan applikationsprogram.

Driftparametrar

De förändringar i apparatlägen, börvärden m.m. som ingår i normala åtgärder under drift.

Maskinvara

Hardware: *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 microelectronics 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

Software: *A set of ordered instructions and data that specify operations in a form suitable for execution by a digital computer (IEC60880)*

PROM

Programmable Read-Only Memory

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.

Standardprogram

De specifika program med moduler (funktionsblock, ”byggstenar”) som karaktäriserar det speciella system så som det är framtaget av Leverantören/Tillverkaren av ett visst PE-system. Levereras oftast i ett programbibliotek.

Systemprogram

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 Produktkrav

3.1 Standardisering

Framtagningen av PE-utrustningen (maskinvaran, bas- och applikationsprogramvaran) ska ha skett enligt en utvecklingsmodell som minst följer kraven enligt IEC 61508 SIL 2, IEC 62138 eller kraven enligt ISO 9001och ISO 90003.

Dokumenterade och spårbara drifterfarenheter kan till viss del kompensera brister i framtagningsmetodiken.

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 Tillverkare/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 basprogramvara och applikationsprogramvara.

Tillverkare/Leverantören ska i anbudet redovisa hur föreskrifter och tillämpliga produktstandarder uppfylls.

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

3.2 Krav på maskinvara

3.2.1 Batteribackup

Om batteribackup ingår ska batteriernas livslängd redovisas.

3.2.2 Lagringsmedia

Lagringsmedia för backup av programvaran (bas-, applikation-, databaser m.m.) ska anges av Tillverkare/Leverantören.

3.2.3 Bildpresentation

Bildpresentation ska väljas med hänsyn till den relativt starka belysningen som normalt förekommer i kontrollrum.

3.2.4 Underhållskrav

Kortbyte ska kunna utföras utan att hela utrustningen/systemet måste tas ur drift. Omstart av utbytt del accepteras. Leverantören/Tillverkaren ska redovisa hur utrustningen beter sig vid omstart som t.ex. hantering av data, aktivering av utgångar, påverkan på andra systemdelar.

3.2.5 Spänningsmatning

Tillverkare/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 med hjälp av systemet eller hjälpmedlet kunna jämföra ny och gammal programversion och rapportera skillnader.

3.3.2 Uppgradering av basprogram

Vid eventuellt erbjudande av uppgraderad basprogramvara 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 Utbyggbarhet av funktionalitet

Tillverkare/Leverantören ska redovisa möjligheter och omfattning på utbyggbarhet av utrustningens funktionalitet och prestanda.

3.4.2 Behörighetsstyrning

Möjlighet att styra behörigheten ska minst finnas för följande:

- ändring i applikationsprogram
- ändring av parametrar som larm- och gränsvärden för utlösning, (baslägesparametrar)
- normal operatörshantering

Ändringar i behörighetsskyddade områden ska automatiskt märkas med tidpunkt och behörighetssignatur.

3.4.3 IT-säkerhet

Krav på IT-säkerhet anges i TBE 100:2

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

3.4.4 Testbarhet

Tillverkare/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).

3.4.5 Hjälpmedel

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

3.4.6 Människa-maskin interface

Beställaren ska kunna välja färger för olika funktioner.

Larmtexter och andra texter ska kunna skrivas med svenska tecken.

Ovanstående gäller även programmeringshjälpmedel, hjälpmedel för parameterinställning, test, underhåll etc.

Övervakning och manöver ska ske på ett för operatören enkelt, entydigt och överskådligt sätt.

3.4.7 Tillförlitlighet

Utrustningens tillförlitlighet ska anges av Tillverkare/Leverantören. Uppgifter om MTBF och MTTR värden ska anges. Uppgifterna ska redovisas på utrustningsnivå eller på den konfiguration som gäller för aktuellt system.

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

3.4.8 Prestanda

Tillverkare/Leverantören ska ange bitupplösning, och svarstid.

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.) Första respons på tangenttryckning 0,1 s.

Svarstid för statisk bild, dvs. från tangenttryckning till att hela bilden presenteras 0,5 s. Svarstider för hel bild, med 50 dynamiska punkter, dvs. från tangenttryckning till att hela bilden presenteras max 2 s.

Motsvarande svarstider för trendbilder är max 4 s.

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

3.4.9 Egenövervakning

Intern övervakningar ska finnas i erforderlig omfattning och redovisas av Tillverkare/Leverantören.

Orimliga signaler från processen ska ge larm och systemet ska inta ett säkert läge.

För definierade IT-attacker ska systemet ge larm och om så är möjligt ska systemet inta ett definierat eller säkert läge.

Loggning av felhändelser

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

3.4.10 Kapacitet

Centralenheten (processorn) får inte vara mer belastad än att även den minst prioriterade funktionen med marginal garanteras bli exekverad inom föreskriven svarstid.

3.4.11 Kommunikationsgränssnitt

Utrustningen ska kunna kommunicera med andra datorsystem med hjälp av standardiserat protokoll.

Om specifikt kommunikationsgränssnitt krävs anges detta i Teknisk Specifikation.

3.4.12 Övriga krav

För nya versioner av programvara, maskinvara och hjälpmedel ska Tillverkare/Leverantören garantera kompatibilitet med gamla system. Tillverkare/Leverantören ska redovisa hur Beställaren på lämpligt sätt ska kunna vidmakthålla systemet under längre tid än 10 år.

Systemet bör vara självdokumenterande så att förutom applikationsprogram i kodform, 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.

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.

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

Tillverkare/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 versions-/revisionsnummer och tillhörande hårdvaruversion ska anges.

<u>Standardprogram - Modulbeskrivning</u>

Varje modul ska vara väl beskriven med avseende på funktion, arbetssätt, in- och utgångar, parametrar och övriga data av intresse.

Programmeringsanvisningen ska beskriva förfarande vid programmering, databaskonfigurering samt anvisningar för bildbyggande. Typfall ska exemplifieras.

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
- Korttyp
- Kortplats
- Signalnamn
- Entydiga hänvisningar till funktionsschema
- Regler för hantering/lagring

Ett huvuddokument som tillsammans med kretsschemat och signaladresslistan ger en fullständig bild av systemets hela funktion. Hos de flesta systemen finns möjlighet att automatiskt generera funktionsschemat.

Beskrivning av programfunktion, databas och grafisk presentation av konfigurering av systemet inklusive kommunikation ska redovisas.

Det bör finnas ett grafiskt översiktsschema över program och programmoduler.

Signalföljning ska kunna göras genom entydiga hänvisningar inom funktionsschemat och till kretsschema inom systemet samt till övriga anslutna system.

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.

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.

4.4 Underhållsdokumentation

Underhållshandledningen beskriver:

- Uppstart, omstart av systemet
- Backuphantering, återställningsförfarande
- 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
– Regler för hantering/lagring av programvaran

4.5 Driftdokumentation

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

4.6 Kontrolldokumentation

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

Tillverkare/Leverantören ska redovisa genomförda typprov och allprov enligt överenskommen kontrollplan.

Se även KBE 100.

4.7 Analyser

Tillförlitlighetsmetodik och resultat ska redovisas.

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 Support, ersättning med kompatibel utrustning efter utfasning	
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	
10	Jämföra befintlig programversion i utrustningen och lagrade kopior	
11	Redovisa möjligheter och omfattning på utbyggbarhet	
12	Behörighet för olika nivåer	
13	Testbarhet efter ett utbyte eller i samband med återkommande provning	
14	Hjälpmedel utvärderade och godkända	
15	Utrustningens tillförlitlighet Uppgifter + referenser	
16	Prestanda Kapacitet, med marginaler Svarstider + verifiering vid test Mätområden, noggrannheter, felvisning, bit-upplösning Tidsupplösning	
17	Redovisning av dokumentstruktur och var informationen enligt beskrivningen finns beskriven	
18	Produktdokumentation	
19	Konstruktionsdokumentation	
20	Underhållsdokumentation	
21	Driftdokumentation	
22	Kontrolldokumentation	
23	Analyser	
24	Gränssnitt mot anläggningens övriga system	
25	Strukturella krav	
26	Kommunikationskrav inklusive krav på funktionell separation	
27	Operatörskommunikation	
28	Underhållsmässighet, krav på vissa åtgärder under drift (t.ex. kort- och batteribyte)	
29	Krav på maskinvaran Lagringsmedia, miljökrav, fysiska dimensioner, elektriska krav	
30	IT-säkerhet	
31	Definierat läge vid inträffat fel	
32	Leverans av källkod	
33	Spänningsmatning	