Tekniska bestämmelser för elektrisk utrustning	Beteckning/Document TBE 106:1-1
	Utgåva/Issue 2 (S)
Rubrik/Title Programmerbar Elektronik (PE) med programmerbar applikation	Datum/Date 2017-05-22
	Ersätter/Supersedes 1 (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 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 funktions-moduler/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.

CCF, Common Cause Failure

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

Diversifiering

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

Driftparametrar

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

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)

PROM

Programmable Read-Only Memory

RAM

Random Access Memory

Read/write memory - not permanent.

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)

ROM

Read-Only Memory

Read memory – permanent

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 ofta 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

Framtagningsmetodiken av produkten ska ha skett enligt en utvecklingsmodell som följer kraven enligt IEC 60987 för maskinvara, IEC 60880 för programvara och IEC 61513 för gemensamma systemkrav för maskinvara och programvara.

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, IEC 60987 och IEC 61513.

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 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 basprogramvara och applikationsprogramvara.

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

Generell kontrollplan framgår av KBE IP-106:1-1 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.

Batteriernas kapacitet ska övervakas. Vid larm om låg laddning ska det finnas en reservkapacitet om minst 2 månader.

3.2.2 Lagringsmedia

Lagringsmedia och utrustning för backup av programvaran (bas-, applikation-, databaser m.m.) ska anges av Tillverkaren/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. Tillverkaren/Leverantören ska redovisa hur utrustningen beter sig vid omstart som t.ex. hantering av data, aktivering av utgångar, påverkan på andra systemdelar etc.

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

Ändring ska märkas med tid och ID-kod för den som utfört ändringen.

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.

3.3.3 Programutformning

Standardprogram ska vara strikt uppdelade i moduler eller subrutiner med så få beroenden som möjligt dem emellan. Modulerna ska vara väl avgränsade till funktion och innehåll med väl definierade in- och utgångar till andra moduler.

Programmoduler i basprogramvaran får inte modifieras i samband med applikationsprogrammeringen utan beställarens godkännande.

3.3.4 Oanvänd programvara

Programvara eller programdelar som inte används ska i första hand avlägsnas. I annat fall ska Tillverkaren/Leverantören visa hur det är säkrat att exekvering av icke använd programvara inte kan ske eller kan påverka använd programvara.

3.4 Gemensamma utrustningskrav (maskin- och programvara)

3.4.1 Utbyggbarhet av funktionalitet

Tillverkaren/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

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).

3.4.5 Hjälpmedel

Hjälpmedel som används för programmering, bildbyggande, 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.

3.4.6 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 Tillverkaren/Leverantören. Uppgifter om MTBF och MTTR värden ska anges. Leverantören/Tillverkaren ska beskriva använda beräkningsmetoder och bedömningsgrunder. Uppgifterna ska redovisas på utrustningsnivå eller på den konfiguration som gäller för aktuellt system.

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

3.4.8 Prestanda

Tillverkaren/Leverantören ska ange bitupplösning, och svarstid. Allmänna krav på mätområde, inställningsvärde, 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

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

Även maskinvarans status ska vara övervakad. t.ex. ”watch-dog”' med tidsövervakning av processorns arbete. Vid onormala förhållanden ska utrustningen gå till ett förutbestämt säkert läge och ge larm.

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

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.

<u>Loggning av felhändelser</u>

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

Kontroll av minnesinnehåll

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

3.4.10 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.

3.4.11 Kapacitet

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

Tillverkaren/Leverantören ska ange metod för bestämning av belastningen. Värdet ska verifieras vid test.

CPU-lasten ska kunna beräknas enligt en deterministisk metod som anvisas av Tillverkaren/Leverantören. Momentant värde och historik ska kunna visas vid anrop. Motsvarande gäller även för nätverkslast.

3.4.12 Kommunikationsgränssnitt

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

Om specifikt kommunikationsgränssnitt krävs anges detta i Teknisk Specifikation.

3.4.13 Redundanta funktioner

Redundanta processorfunktioner i samma utrustning ska behandlas i olika processorer utan kommunikation dem emellan. Fel i en processor får inte påverka den andra redundanta processorn.

3.4.14 Övriga krav

Tillverkaren/Leverantören ska ha ett system för aktivt inhämtande 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.

Tillverkaren/Leverantören ska löpande informera beställaren om upptäckta fel och brister som kan påverka funktionen i den applikation som beställaren har.

Tillverkaren/Leverantören ska kunna leverera identisk programvara och maskinvara av systemet i minst 10 år från det att systemet 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.

Test av systemet ska normalt kunna ske utan att hela eller delar av systemet tas ur drift och därmed får negativ påverkan på processfunktionerna i anläggningen.

Om systemet av något skäl kopplats bort eller tagits ur drift ska detta uppmärksammas via larmfunktion.

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.

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 versions-/revisionsnummer och tillhörande hårdvaruversion ska anges.

Standardprogram - Modulbeskrivning
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 ska 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.

Applikationsprogrammet kod ska vara utskrivet i läsbart format.

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

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

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

I samband med leverans av hela systemfunktioner kan annan information krävas. Detta specificeras i samband med beställning. Tillverkaren/Leverantören ska på begäran kunna redovisa det underlag som krävs. 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	Redovisning av ej använd programvara	
11	Jämföra befintlig programversion i utrustningen och lagrade kopior	
12	Redovisa möjligheter och omfattning på utbyggbarhet	
13	Behörighet för olika nivåer	
14	Testbarhet efter ett utbyte eller i samband med återkommande provning	
15	Hjälpmedel utvärderade och godkända	
16	Utrustningens tillförlitlighet Uppgifter + referenser	
17	Prestanda Kapacitet, med marginaler Svarstider + verifiering vid test Mätområden, noggrannheter, felvisning, bitupplösning Tidsupplösning	
18	Egenövervakning	
19	Kontroll av minnesinnehåll	
20	Loggning av felhändelser	
21	Säkert läge	
22	Metod för bestämning av CPU-belastning Belastning verifieras vid belastningsprov	
23	Kommunikationsgränssnitt	
24	Inhämtande av erfarenheter och sprida detta till användare Upptäckta fel som kan påverka applikationen	
25	Produktunderhåll Support och service efter leverantörens/tillverkarens utfasning av produkten Leverans av samma programvara i 10 år Kompatibilitet avseende utrustning/programvara	
26	Redovisning av dokumentstruktur och var informationen enligt beskrivningen finns beskriven	
27	Produktdokumentation	
28	Konstruktionsdokumentation	

29	Underhållsdokumentation	
30	Driftdokumentation	
31	Kontrolldokumentation	
32	Analyser	
33	Gränssnitt/interface mot anläggningens övriga system	
34	Strukturella krav	
35	Kommunikationskrav inkl. krav på funktionell separation	
36	Operatörskommunikation	
37	Underhållsmässighet, krav på vissa åtgärder under drift (t.ex. kort- och batteribyte)	
38	Krav på maskinvaran Lagringsmedia, miljökrav, fysiska dimensioner, elektriska krav	
39	Enkelfel, redundans, fysisk separation	
40	Grad av och metod för diversifiering	
41	Analys av riskfaktorer	
42	Övervakning, självtest	
43	Datatrafikflöde i kommunikationsgränssnitt	
44	IT-säkerhet	
45	Leverans av källkod	
46	Spänningsmatning	