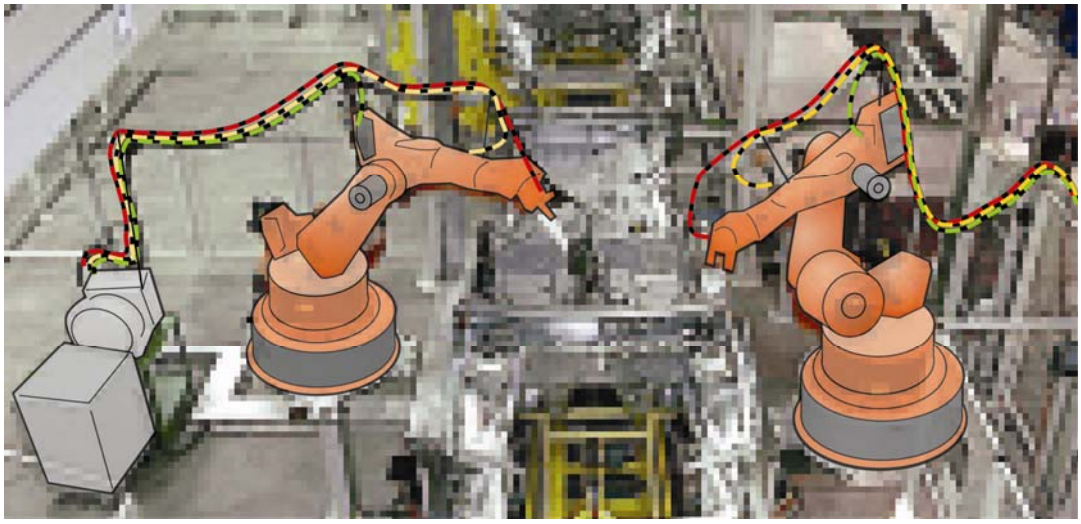
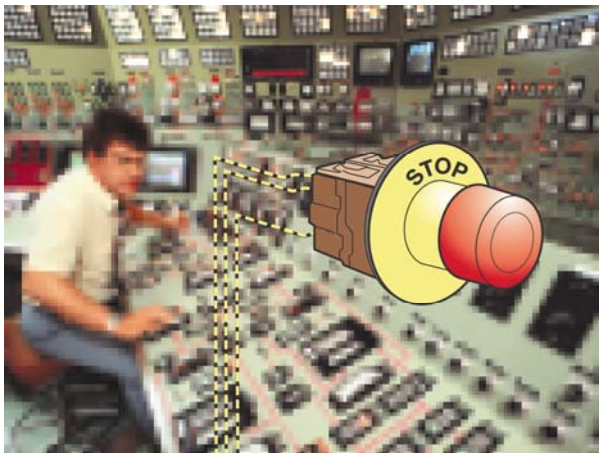
Säkerhetskritiska styrsystem i maskiner

Johan Hedberg
Henrik Eriksson
Jan Jacobson
Jan Tegehall

SP Sveriges Tekniska Forskningsinstitut





Elektronik

SP Rapport 2009:03

Säkerhetskritiska styrsystem i maskiner

Johan Hedberg
Henrik Eriksson
Jan Jacobson
Jan Tegehall

Abstract

Safety critical control systems in machinery

This report gives a short introduction to new requirements concerning safety of machinery. During the last years, a number of different functional safety standards have been developed (for instance IEC 61508:2002, ISO 13849-1:2006 and IEC 62061:2005). These new standards place more extensive requirements than earlier standards did.

The beginning of the report describes the basis of functional safety and describes the meaning of functional safety, e.g. what it means to work in accordance with a safety life cycle and the meaning of a safety function.

The following part of the report gives guidance on when respective standard is applicable. This part is important because to some degree these new standards cover the same technical area and thus create a certain level of confusion when to use or not to use a certain standard.

When you have found the applicable standard for a certain product, the rest of the report is helpful since it describes how each of these standards is built up. The fundamental requirements of these standards are basically the same but they differ when it comes to extent and direction.

The first part which is described in the report is the hazard and risk analysis, where the safety functions and the corresponding requirements on risk reduction shall be identified. In this part of the report, terms like SIL (Safety Integrity Level) and PL (Performance Level) are also described.

After this the report briefly explains how to continue and more in detail describes the requirements placed on the safety functions.

When the specification of the safety requirements is completed it is possible to continue with the hardware and software design.

During the hardware design it is important to handle systematic hardware failures. The report describes in a tabular form how these requirements differ between the different standards.

For the hardware it is also necessary to show that the probability of dangerous hardware failures is low enough. The report describes how these requirements differ depending on if you are a component supplier or if you are designing a complete safety function.

Finally the report describes the requirements placed on the software, described separately for embedded software and application software.

The aim of this report is to give a short introduction to which functional safety requirements that are put on machine control systems from different standards, and consequently it is necessary to read the underlying standards to get the full picture and all the details.

These standards are possible to buy via SIS, Swedish Standards Institute (www.sis.se)

This report is partly based on an earlier SP report named SP report 2008:08 but the focus of this report is safety of machinery in general and SP report 2008:08 was focusing on

functional safety of heavy vehicles. The earlier report SP report 2008:08 was the result of a study within the VINNOVA (The Swedish Governmental Agency for Innovation Systems) financed project RobustIQ, For more information, see www.robustiq.se.

Key words: IEC 61508, IEC 62061, ISO 13849-1, SIL, PL, safety function, functional safety, control system.

SP Sveriges Tekniska Forskningsinstitut
SP Technical Research Institute of Sweden

SP Rapport 2009:03
ISBN 978-91-85829-74-3
ISSN 0284-5172
Borås 2009

Innehållsförteckning

Figurförteckning

Tabellförteckning

Förord

Den här rapporten är en vidareutveckling av tidigare SP-rapport 2008:08 vilken fokuserade på funktionssäkerhet för tunga fordon medan denna rapport gäller generellt för alla typer av maskinstyrningar. Den tidigare rapporten SP-rapport 2008:08 var resultatet av en studie inom det VINNOVA-finansierade projektet RobustIQ. [1]

Målet har varit att sammanställa tekniker och metoder för utveckling av säkerhetssystem för maskiner. Flera standarder har studerats under arbetets gång: SS-EN 61508:2002, SS-EN ISO 13849-1:2008 och SS-EN 62061:2005. Skillnader och likheter mellan de olika standarderna har pekats ut och det har också belysts hur de olika standarderna hänger ihop. Nedan följer en kort översikt av rapportens olika delar.

De första avsnitten i rapporten definierar en terminologi samt innehåller en del som diskuterar allmänt kring funktionssäkerhet. Därefter följer en genomgång av tillämpliga funktionssäkerhetsstandarder för maskiner.

Sedan följer beskrivningar på hur de olika standarderna ser på hur en riskanalys ska genomföras och hur en säkerhetskravspecifikation skall utformas. Vidare följer hur man undviker samt hanterar systematiska hårdvarufel.

Därefter beskrivs hur man beräknar tillförlitlighetsvärden på hårdvara och hur man utvecklar säkerhetskritisk programvara.

I slutet av rapporten finns två appendix som översiktligt beskriver och, ur tillämpningsperspektiv, jämför de olika standarderna.

Syftet med denna rapport är enbart att ge en introduktion till vilka funktionssäkerhetskrav som ställs på maskinstyrningar. Det är viktigt att gå vidare och läsa underliggande standarder eftersom dessa i detalj beskriver vilka krav som måste uppfyllas.

Standarderna finns att köpa via SIS, Swedish Standards Institute (www.sis.se)

[1] RobustIQ är ett initiativ som fokuserar på produktutveckling och nya affärsmöjligheter där robust elektronik, dvs. inbyggd elektronik i svåra miljöer, står i centrum. Det är ett samarbete mellan Tekniska Högskolan i Jönköping tillsammans med Acreo, SP Sveriges Tekniska Forskningsinstitut, klusterinitiativet Tunga fordon, Science Park Jönköping, näringslivet samt offentliga aktörer.

Sammanfattning

Denna rapport ger en kort introduktion till vilka krav som ställs vid utveckling av säkerhetssystem för maskiner. Under de senaste åren har det utvecklats ett antal nya funktionssäkerhetsstandarder (bland annat SS-EN 61508:2002, SS-EN ISO 13849-1:2008 samt SS-EN 62061:2005) som ställer nya mer omfattande krav jämfört med tidigare standarder.

Inledningsvis går rapporten igenom grunderna i funktionssäkerhet och förklarar bland annat vad som menas med funktionssäkerhet, vad det innebär att arbeta enligt en så kallad safety life cycle (säkerhetslivscykel) samt förklarar vad ovanstående standarder menar med begreppet säkerhetskritisk funktion.

Därefter innehåller rapporten en vägledning som ger stöd kring när respektive standard är tillämpbar. Denna del är viktig eftersom ovanstående nya funktionssäkerhetsstandarder till viss del täcker samma teknikområden och därigenom skapar viss förvirring kring när respektive standard är tillämpbar eller ej.

När man väl fått klart för sig vilken standard som gäller för en viss produkt så beskriver resterande delar av rapporten hur var och en av ovanstående standarder är upplagd. Grundkraven i dessa olika standarder är desamma däremot skiljer de sig åt gällande omfattning och inriktning.

Den första delen som beskrivs i rapporten är riskanalysen där man skall identifiera de så kallade säkerhetskritiska funktionerna samt bestämma krav på riskreduktion. Här förklaras bland annat begrepp som SIL (Safety Integrity Level) och PL (Performance Level).

Därefter går rapporten kort igenom hur man skall gå vidare och mer i detalj beskriva vilka krav som ställs på de säkerhetskritiska funktionerna.

När kravspecifikationen för de säkerhetskritiska funktionerna är färdigställd, påbörjas arbetet med hård- och mjukvarukonstruktionerna.

I samband med hårdvarukonstruktionen är det viktigt att kunna hantera systematiska hårdvarufel. Rapporten beskriver i en jämförande tabell hur dessa krav skiljer sig åt mellan ovanstående standarder.

För hårdvaran ingår även att kunna visa att tillförlitligheten, det vill säga sannolikheten för slumpmässiga hårdvarufel, är tillräcklig låg. Rapporten går igenom hur dessa krav skiljer sig åt beroende på om man är komponentleverantör eller om man bygger ihop en komplett säkerhetskritisk funktion.

Avslutningsvis går rapporten igenom vilka krav som ställs på programvaran och här skiljer sig kraven åt beroende på om det är så kallad inbyggd programvara eller så kallad applikationsprogramvara.

Syftet med denna rapport är enbart att ge en kort introduktion till vilka funktions-säkerhetskrav som ställs på maskinstyrningar. Därför är det viktigt att gå vidare och läsa underliggande standarder eftersom dessa i detalj beskriver vilka krav som måste uppfyllas.

Ovanstående standarder finns att köpa via SIS, Swedish Standards Institute (www.sis.se)

Den här rapporten är en vidareutveckling av tidigare SP-rapport 2008:08 som fokuserade på funktionssäkerhet för tunga fordon medan denna rapport gäller generellt för alla typer av maskinstyrningar. Den tidigare rapporten SP-rapport 2008:08 var resultatet av en studie inom det Vinnova-finansierade projektet RobustIQ.

Terminologi och förkortningar

Tabell 1: Jämförelse av terminologi mellan standarderna

SS-EN 61508:2002	SS-EN 62061:2005	SS-EN ISO 13849-1:2008	Svensk översättning
safety function	safety function	safety function	säkerhetskritisk funktion / skyddsfunktion
electrical/electronic/ programmable electronic system	safety related electronic control system	combined safety-related part of a control system	E/E/PE-baserad säkerhetsarkitektur
hazard	hazard	hazard	riskkälla
hazardous situation	hazardous situation	hazardous situation	riskfylld situation
harm	-	harm	skada
common cause failure	common cause failure	common cause failure	fel av samma orsak
electrical/electronic/ programmable electronic safety function	safety-related control function	programmable electronic system safety function	elektriskt/elektroniskt/ programmerbart elektronisk baserad säkerhetskritisk funktion / skyddsfunktion
diagnostic coverage	diagnostic coverage	diagnostic coverage	feldetekterings-förmåga
safety integrity level	safety integrity level	safety integrity level	säkerhetsnivå
-	-	performance level	prestandanivå
subsystem	subsystem	safety-related part of a control system	delsystem som ingår som en del av en E/E/PE-baserad säkerhetskritisk funktion / skyddsfunktion
Equipment Under Control			styrd utrustning
architectural constraints	architectural constraints	-	begränsningar i vald hårdvaruarkitektur
-	functional block	-	funktionsblock
functional block element			funktionsblocks-element
safety life cycle			säkerhetslivscykel

Tabell 2: Förkortningar

B_{10}	The expected time at which 10% of the population will fail
C	Duty cycle
DC	Diagnostic Coverage
DC_{avg}	Diagnostic Coverage Average
E/E/PES	electrical/electronic/programmable electronic system
EUC	Equipment Under Control
FIT	Failures In Time (10^{-9} fel/timma)
FVL	full variability language
HFT	Hardware Fault Tolerance
HW	hardware
L	Logic
LVL	limited variability language
MTBF	Mean Time Between Failure
MTTF	MeanTime To Failure
MTTR	Mean Time To Restoration
PES	programmable electronic system
PFH_D	Probability of Dangerous Failure per Hour
PL	performance level
P_{TE}	Probability of Transmission Error
RBD	reliability block diagram
SFF	Safe Failure Fraction
SIL	safety integrity level
SRASW	safety-related application software
SRCF	safety-related control function
SRECS	safety related electronic control system
SRESW	safety-related embedded software
SRP/CS	safety-related part of a control system
SRS	safety requirements specification
SVP	safety validation plan
SW	software
SWSRS	software safety requirements specification
TE	Test Equiment

1 Allmänt om funktionssäkerhet

Det finns många olika riskkällor i tekniska system; mekaniska, kemiska, elektriska, explosiva etc. När ett system, en apparat eller en maskin betecknas som "säker" menas att alla dessa risker är tillräckligt låga. Säkerhet innebär alltså att det inte finns oacceptabla risker för fysiska skador eller skador på hälsa, både direkt eller indirekt som ett resultat av skador på egendom eller på miljön. I [IEC 61508-4] kan man hitta följande definition av säkerhet:

”Safety is freedom from unacceptable risk”

Funktionssäkerhet däremot är den del av den totala säkerheten som beror på om ett system eller en komponent fungerar korrekt med de insignaler som ges. Funktionssäkerhet ska inte förväxlas med elsäkerhet som innebär skydd mot elchock och brand orsakade av elektricitet. I [IEC 61508-4] kan man hitta följande definition av funktionssäkerhet:

”Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs”

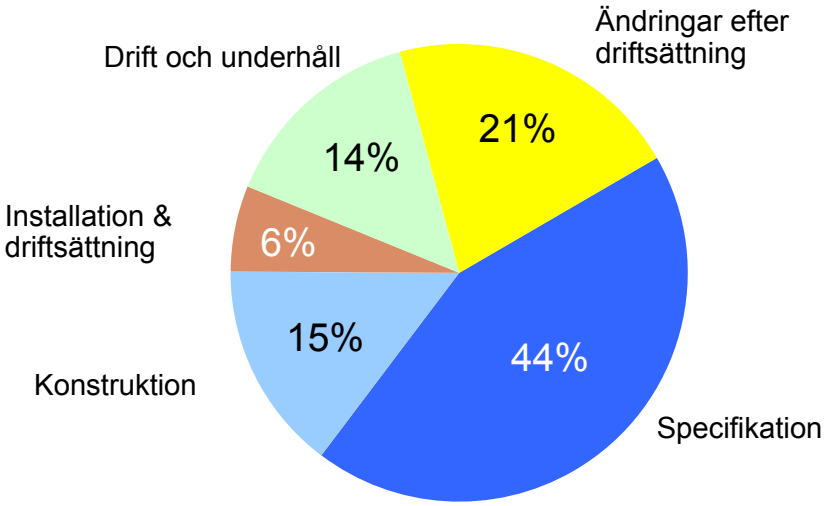
Ett exempel på funktionssäkerhet är en varvtalsvakt som förhindrar en slipskiva att rotera för snabbt och därmed löper risk att sprängas. Däremot är mekaniska skydd mot att skadas av den roterande slipskivan inte en aspekt av funktionssäkerhet. Inte heller bullerdämpare avsedda att minska risken för hörselskador har med funktionssäkerhet att göra. Däremot är alla åtgärderna viktiga för att slipmaskinen i sin helhet ska anses tillräckligt säker.

1.1 Säkerhetslivscykel

Moderna funktionssäkerhetsstandarder inkluderar en så kallad säkerhetslivscykel. Detta innebär att man tar ett helhetsgrepp när det gäller funktionssäkerhet och ställer krav på alla delar i utvecklingsarbetet, hela vägen från det inledande konceptstadiet till dess att produkten avvecklas/skrotas.

Detta ställer hårdare krav på företag som utvecklar säkerhetskritiska komponenter/system eftersom man redan från början måste tänka säkerhet. Det är alltså inte möjligt att i efterhand bygga in säkerhet i komponenten/systemet.

Bakgrunden till varför man valde att använda en säkerhetslivscykel bygger på en studie som HSE, Health and Safety Executive (den engelska motsvarigheten till Arbetsmiljöverket), genomförde i början av 1990 talet. I denna studie gick man igenom cirka 200 allvarliga olyckstillbud som hade skett inom maskinindustrin och undersökte varför de hade skett. Resultatet var intressant på så sätt att bara en liten andel av olyckorna berodde på fel under konstruktionsfasen och en betydligt större andel av felen berodde på fel som uppstått innan man påbörjat konstruktionen (till exempel ofullständig riskanalys, felaktiga kravspecifikationer) och efter att man konstruerat färdigt systemet (till exempel under drift, vid modifieringar).



Figur 1: Relation mellan allvarliga olyckstillbud och olika livscykelfaser

1.2 Säkerhetskritisk funktion

I [IEC 61508-4] kan man hitta följande definition av säkerhetskritisk funktion:

”*Function to be implemented by an E/E/PE safety-related system, other technology safety related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event*”

Som framgår av ovanstående definition kan en säkerhetskritisk funktion vara realiserad både med hjälp av:

- *E/E/PE safety-related system*: detta är en säkerhetskritisk funktion som är implementerad med hjälp av ett elektriskt/elektroniskt eller programmerbar elektroniskt system
- *other technology safety-related system*: detta kan vara en rent mekanisk säkerhetskritisk funktion
- *external risk reduction facilities*: detta kan vara att man har välutbildade operatörer som är väl medvetna om de risker som finns eller varningstext på maskiner

Om man går vidare och studerar en E/E/PE-baserad säkerhetskritisk funktion så beskrivs det i IEC 61508 att denna alltid är uppbyggd av en sensor, logik samt aktuator (Figur 2).

Figur 2: Uppbyggnad av säkerhetskritisk funktion

Vissa företag konstruerar enbart ett delsystem (som till exempel är E/E/PE-baserat eller rent mekaniskt) som är tänkt att ingå i en E/E/PE-baserad säkerhetskritisk funktion medan andra företag är ansvariga för att konstruera den kompletta säkerhetskritiska funktionen utgående från de individuella delsystemen.

1.3 EUs maskindirektiv och styrsystem

Alla maskiner som används inom EU och EES-området skall uppfylla EUs maskindirektiv. Gemensamma regler i de olika länderna gör det enklare att veta vilka grundläggande hälso- och säkerhetskrav som gäller. Maskindirektivet omarbetas och gäller i sin nya version från den 29 december 2009. I Sverige har Arbetsmiljöverket infört direktivet i Arbetsmiljöverkets föreskrifter AFS 2008:3.

Styrsystems säkerhet och tillförlitlighet beskrivs i punkt 1.2.1 av bilaga 1 till maskindirektivet:

Ett styrsystem skall vara konstruerat och tillverkat så att riskfyllda situationer inte skall kunna uppstå. Framför allt skall det vara konstruerat och tillverkat så att
— det kan tåla avsedda påfrestningar under drift och yttre påverkan,
— fel i styrsystemets maskinvara eller programvara inte leder till riskfyllda situationer,
— fel i styrsystemets logik inte leder till riskfyllda situationer,
— rimligen förutsebara mänskliga misstag under handhavandet inte leder till riskfyllda situationer

Särskild uppmärksamhet skall ägnas följande punkter:
— Maskinen får inte starta oväntat.
— Maskinens parametrar får inte ändras på ett okontrollerat sätt; om en ändring kan ge upphov till riskfyllda situationer.
— Maskinen får inte hindras från att stanna om stoppkommandot redan har givits.
— Ingen rörlig del av maskinen eller del som hålls av maskinen får falla eller kastas ut.
— Automatiskt eller manuellt stopp av rörliga delar av vilket slag som helst skall kunna göras obehindrat.
— Skyddsanordningarna skall fortsätta att vara effektiva fullt ut eller utlösa stoppkommando.
— De säkerhetsrelaterade delarna av styrsystemet skall fungera på ett sammanhängande sätt för en hel grupp av maskiner och/eller delvis fullbordade maskiner.
För trådlös styrning skall ett automatiskt stopp göras när korrekta styrsignaler inte går fram, inklusive kommunikationsbortfall.

Det omarbetade maskindirektiv som gäller från den 29 december 2009 har i stort sett samma krav som tidigare version av maskindirektivet. Nya krav har kommit på

- att förutse mänskliga misstag. Avsikten är att genom ergonomiska principer i styrningen minska risken för handhavandefel.
- att maskinens parametrar inte får ändras på ett okontrollerat sätt. Ett exempel på detta kan vara om maskinens bearbetningshastighet ställs om via fjärrstyrning utan att meddela operatören.
- att de säkerhetsrelaterade delarna ska fungera på ett sammanhängande sätt.
- att automatiskt stopp ska ges om korrekta styrsignaler inte når fram vid trådlös styrning. Kommunikationsbortfall eller störda meddelanden får inte orsaka farliga situationer.

Dessa regler har tillämpats redan tidigare i de flesta maskinstyrningar, men nu specificeras kraven i maskindirektivet.

För vissa typer av maskiner och logikenheter föreskrivs speciella förfaranden för CE-märkning. Om man har maskiner eller säkerhetskomponenter som omnämns i bilaga 4 och 5 gäller speciella regler för bedömning av överensstämmelse med direktivets krav. Man kan bli tvungen att anlita ett s.k. ”anmält organ”. Bilaga 4 och 5 har ändrats i det nya maskindirektivet. Den som arbetar med säkerhetskomponenter bör vara vaksam på ändringarna.

Kraven i direktivet är avsiktligt skrivna på ett sätt som möjliggör olika tekniska lösningar. Direktivet vill inte riskera att föreskriva detaljlösningar som snabbt kan bli föråldrade. Om man vill har ytterligare råd om hur styrsystem ska konstrueras får man gå vidare och läsa i standarder.

EUs maskindirektiv (EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2006/42/EG av den 17 maj 2006 om maskiner och om ändring av direktiv 95/16/EG) kan laddas ner från:
http://eurlex.europa.eu/LexUriServ/site/sv/oj/2006/l_157/l_15720060609sv00240086.pdf
Man kan också hitta direktivet bland Arbetsmiljöverkets föreskrifter (www.av.se). På Arbetsmiljöverkets hemsida finns även råd om maskinsäkerhet och CE-märkning.

1.4 Fel i styrsystem

Även i styrsystem av god kvalitet uppkommer förr eller senare fel. Felen i styrsystemet kan leda till att viktiga säkerhetskritiska funktioner inte utförs på avsett sätt. Orsaken till fel kan vara olika; programvara, hårdvara, miljöstörningar eller användarfel. Vissa fel är systematiska, dvs. de är resultatet av ett misstag i konstruktionsarbetet och finns i styrsystemet från början. Andra fel uppträder slumpmässigt, t.ex. beroende på åldring eller slitage. Misstag vid underhåll och ombyggnation kan leda till att nya fel byggs in i systemet.

Sannolikheten att ett säkerhetskritiskt system ska utföra en säkerhetskritisk funktion på avsett sätt kallas säkerhetsintegritet (eng. safety integrity). Helst ska säkerhetsintegriteten kunna kvantifieras med ett numeriskt värde. I ett felfritt system är sannolikheten för korrekt säkerhetskritisk funktion =1, och sannolikheten för fel = 0. Verkliga styrsystem är aldrig felfria. Därför finns det även i de mest avancerade styrsystemen en viss sannolikhet för felfunktion.

Det är möjligt att beräkna sannolikheten för den del av säkerhetsintegriteten som beror på hårdvara (eng. hardware safety integrity). Sannolikheten för fel i hårdvarukomponenter finns beskrivna i databaser. Därigenom blir det möjligt att beräkna sannolikheten för fel i hårdvarukonstruktioner om man tar hänsyn till styrsystemets arkitektur. Det är på sin plats att vara noggrann med vilka felsannolikhetsvärden beräkningarna baseras på. Felaktiga antaganden om felsannolikhet hos enskilda komponenter kan leda till grovt felaktiga slutsatser om felsannolikheter för systemet.

Den del av säkerhetsintegriteten som beror på systematiska fel (eng. systematic safety integrity) kan normalt inte kvantifieras med ett exakt siffervärde. Sannolikheten för konstruktionsfel i hårdvara eller programvara kan inte mätas eller beräknas exakt.

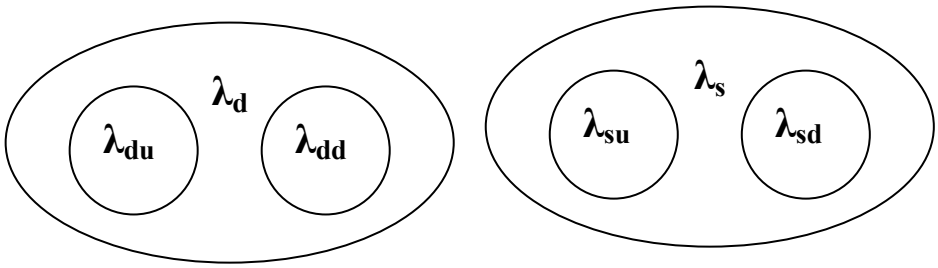
1.5 Fel med olika inverkan

Ett fel i hårdvara eller logik kan inverka på en funktion på olika sätt. I värsta fall orsakar felet en felfunktion som inte upptäcks och försätter systemet i ett farligt läge. Ett exempel på ett sådant fel är om en utgångstransistor går sönder så att den inte förmår bryta utgångsströmmen vid larmgräns.

I bästa fall påverkar felet inte den säkerhetskritiska funktionen och upptäcks dessutom av interna självtester. Exempel på ett sådant "säkert fel" är om minnesceller för display-texter förändras men upptäcks av interna kontrollsumma-beräkningar av minnesinnehållet.

Det blir nödvändigt att dela in felen i olika grupper beroende på hur de påverkar den säkerhetskritiska funktionen och om de kan upptäckas av självtester:
- fel som är farliga och oupptäckta (eng. dangerous undetected)
- fel som är farliga men upptäcks (eng. dangerous detected)
- fel som är "säkra" och oupptäckta (eng. safe undetected)
- fel som är "säkra" men upptäcks (eng. safe detected)

Ett styrsystem kan beskrivas med siffervärden för felintensitet. Felintensiteten räknas i antal fel per timma och betecknas med bokstaven λ (lambda). I normala fall är felintensiteten ett mycket litet tal. Ofta används enheten FIT (eng. failures in time) som betyder $1 * 10^{-9}$. Felintensiteten för de olika felen blir
- λ_{du} (eng. dangerous undetected)
- λ_{dd} (eng. dangerous detected)
- λ_{su} (eng. safe undetected)
- λ_{sd} (eng. safe detected)



Figur 3: Olika typer av felintensitet

De olika felintensiteterna anges av tillverkarna för givare, ställdon, styrsystem etc. När man sedan bygger ihop en säkerhetskritisk funktion av flera delkomponenter kan systembyggaren räkna ut felintensiteten för den säkerhetskritiska funktionen baserat på delkomponenternas värden.

Tid mellan fel används ibland istället för felintensitet. Eftersom man inte kan beräkna denna tid med exakthet brukar man tala om medeltid. Begreppet MTTF (eng. Mean Time To Failure) beskriver förväntad medeltid mellan fel. Begreppet MTTR (eng. Mean Time To Restoration) beskriver hur mycket tid som förväntas för reparationer m.m. innan systemet kan återställas efter ett upptäckt fel. Ibland använder man också begreppet MTBF (eng. Mean Time Between Failures) som beskriver hur lång tid det går mellan felen.

$$MTBF = MTTF + MTTR \qquad [h]$$

eftersom MTTF >> MTTR (vanligtvis) kan man oftast säga att

$$MTBF \approx MTTF$$

När beräkningarna avser faliga fel används ofta begreppet $MTTF_d$ (eng. Mean Time To Dangerous Failure). Värdet beskriver medeltiden mellan farliga fel i ett delsystem av styrsystemet.

Eftersom både felintensiteten λ och MTTF beskriver tid mellan fel kan man skriva

$$\text{felintensitet } \lambda = \frac{1}{MTTF} \text{ [fel/h]}$$

Eftersom MTTF >> MTTR (vanligtvis) kan man oftast säga att

$$\text{felintensitet } \lambda = \frac{1}{MTBF} = \frac{1}{MTBF + MTTR} \approx \frac{1}{MTBF} \text{ [fel/h]}$$

När ett fel inträffar i en säkerhetskritisk funktion önskar man att det inte ska orsaka ett farligt tillstånd. För att kunna jämför olika konstruktioner behövs ett mätetal för andelen säkra fel, SFF (eng. safe failure fraction).

SFF = (säkra fel + farliga upptäckta fel) / (farliga fel + säkra fel)

$$\text{SFF} = \frac{\lambda_s + \lambda_{dd}}{\lambda_d + \lambda_s} \text{ [\%]}$$

I ett idealt system är SFF=100%, dvs. alla fel är antingen "säkra" eller upptäcks i de automatiska självtesterna. Ett sådant system finns inte i verkligheten, men strävan är alltid att så stor del av felen som möjligt inte ska orsaka felfunktioner.

1.6 Självövervakning för att hitta fel

En stor fördel med programmerbara elektroniska system är att det går förhållandevis enkelt att bygga in automatiska självtester. Styrsystemen kan övervaka insignaler, minne, utsignaler, spänningsmatning och många andra delar av systemet. Förhoppningsvis kan systemet hitta en trasig komponent eller en orimlig signal innan felet orsakat en felaktig funktion.

Självtester byggs in i system och arbetar automatiskt utan att användaren märker dem. Först när ett fel upptäcks märker användaren att styrsystemet reagerar. Larmet från den inbyggda automatiska självtestet gör användaren uppmärksam på att ett fel finns i systemet. Kanske försätts styrsystemet i säkert läge.

Som ett mått på kvaliteten i självtesterna används begreppet feldetekteringsförmåga (eng. diagnostic coverage). Feldetekteringsförmåga beskriver hur stor del av de möjliga felen som förväntas kunnas hittas med en viss testmetod. Feldetekteringsförmåga kan gälla antingen ett helt styrsystem eller delar av systemet t.ex. fel i ställdon.

$$\text{Feldetekteringsförmåga (eng. diagnostic coverage), DC} = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \text{ [\%]}$$

där λ_{DD} är sannolikheten för upptäckta farliga fel och λ_{Dtotal} är totala sannolikheten för att farliga fel uppkommer. Om DC t.ex. anges till 91% innebär det att självtesten förmår upptäcka 91% av de farliga fel som kan uppkomma.

För vissa testmetoder kan man teoretiskt beräkna feldetekteringsförmågan. För andra testmetoder kan man inte exakt beräkna feldetekteringsförmågan. Måttet blir då mera ett kvalitativt begrepp som t.ex. låg, måttlig eller hög förmåga att upptäcka fel. Även ett sådant kvalitativt begrepp kan användas för att jämföra olika självtester.

1.7 Proof test

Det är önskvärt att testa de säkerhetskritiska funktionerna så komplett och så realistiskt som möjligt. Men vissa säkerhetskritiska funktioner går inte att testa fullständigt under normal drift. Testet i sig skulle innebära att åtgärder vidtas som allvarligt stör driften. Ett exempel på detta är test av brandlarm. Genom att utsätta en värmedetektor för hög temperatur kan man förvisso kontrollera att den fungerar, men olägenheterna när sprinklersystemet börjar arbeta kommer att störa driften.

Begränsade tester kan göras även om systemet är i drift. Dessa tester blir dock aldrig helt realistiska och kan inte täcka alla aspekter av den säkerhetskritiska funktionen. Om man aldrig testar hela systemet under anläggningens livstid, vet man inte säkert om den säkerhetskritiska funktionen kommer att fungera när den behövs. Det är möjligt att fel som inte upptäcks av självtester under drift ändå kan slå ut den säkerhetskritiska funktionen.

Ett s.k. ”proof test” är ett test som utförs med manuella ingrepp och vid ett visst specificerat intervall. Alla detektorer för ett brandlarm kan t.ex. testas vid en årlig översyn. På det sättet får man ett bevis på att den säkerhetskritiska funktionen ”brandlarm” fungerar minst en gång om året. Vid översynen kan man acceptera att vattnet till sprinklersystemet stängs av, och under en begränsad tid har man inte detta skydd mot brand. Syftet med en ”proof test” är att upptäcka alla fel, och därefter kunna åtgärda felen och återställa systemet till ursprungligt skick.

Mellan två ”proof test” tillfällen finns det en risk för att fel uppkommer som slår ut den säkerhetskritiska funktionen. Därför önskar man så korta ”proof test interval” som möjligt. Detta måste avvägas mot att ”proof test interval” ska vara långa för att inte i onödan orsaka driftstopp.

Genom att välja lämpligt ”proof test interval” kan man minska sannolikheten för fel i den säkerhetskritiska funktionen.

1.8 Styrsystemets arkitektur

1.8.1 En-kanaligt styrsystem

Styrsystem byggs enligt en viss arkitektur. Det enklaste fallet är en arkitektur som är "en-kanalig" d.v.s. det finns ingen dubblering eller övertalighet för någon del av systemet.

Den säkerhetskritiska funktionen beror på att denna enda kanal fungerar som avsett, s.k. "one-out-of-one" (1oo1). Om det blir fel någonstans kan det direkt slå igenom som en felfunktion. Det finns ingen tolerans mot hårdvarufel.

Denna arkitektur kan ändå användas för vissa säkerhetskritiska funktioner om man kan visa att en klart övervägande del av de tänkbara felen inte kommer att leda till farlig

funktion. En viktig förutsättning för detta är att det finns automatiska självtester som förmår att upptäcka många fel.

1.8.2 Redundant system

Genom att dubblera styrsystemet kan man skapa tålighet mot vissa fel. Den säkerhetskritiska funktionen styrs av två parallellt arbetande delsystem. Om ett fel uppträder i ena delsystemet fungerar förhoppningsvis ändå det andra delsystemet enligt avsikt. Det finns en tolerans mot hårdvarufel.

I de fall styrsystemet konstruerats för att båda delsystemen måste vara överens talar man om "two-out-of-two" (2oo2). När ett delsystem reagerar felaktigt kommer det att upptäckas då delsystemens utsignaler jämförs. Delsystemens gemensamma utsignal kommer att styra processen mot säkert läge.

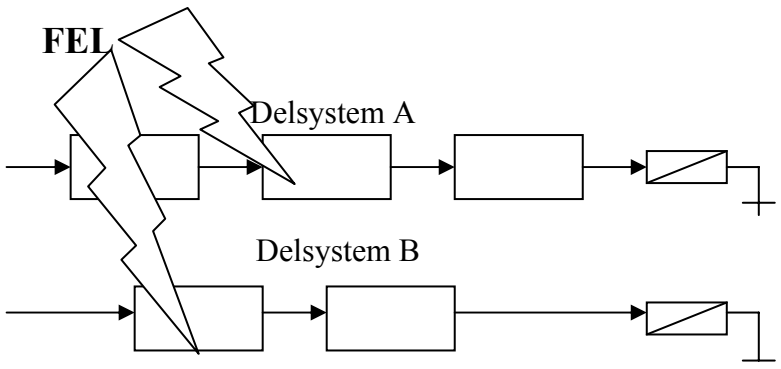
Ibland finns inget säkert läge där styrningen kan avbrytas. Styrsystemet måste i största möjliga mån förmås att hålla den säkerhetskritiska funktionen aktiv. Genom att dubblera styrsystemet försöker man öka tillgängligheten. Den säkerhetskritiskafunktionen styrs av två parallellt arbetande delsystem. Om ett fel uppträder i ena delsystemet fungerar förhoppningsvis ändå det andra delsystemet enligt avsikt.

I de fall redundansen tillförts för att öka tillgängligheten talar man om "one-out-of-two" (1oo2). När ett delsystem reagerar felaktigt tas styrningen över av det andra delsystemet. På detta sätt ökas tillgängligheten i styrsystemet.

1.9 Fel med gemensam orsak

Arkitekturer med två eller flera delsystem är inte effektiva om fel med gemensam orsak (eng. common cause failure) kan slå ut fler än ett delsystem. Det finns en risk att redundansen kan sättas ur spel.

Bland tänkbara fel med gemensam orsak finns:
- fel i gemensam spänningsmatning påverkar flera delsystem.
- miljöstörningar påverkar flera delsystem samtidigt.
- konstruktionsfel har gjorts på samma sätt i flera delsystem.



Figur 4: Fel med gemensam orsak i redundant system styrsystem

2 Använda versioner av standarder

Nedan listas vilka versioner av standarderna som använts i denna rapport.

SS-EN 62061:2005 *”Maskinsäkerhet – Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska styrsystem” ”*+ Corrigendum 1 & 2 [62061]

SS-EN ISO 13849-1:2008 *” Maskinsäkerhet - Säkerhetsrelaterade delar av styrsystem - Del 1: Allmänna konstruktionsprinciper ”* [13849-1]

SS-EN ISO 13849-2:2003 *“Maskinsäkerhet – Styrsystem – Säkerhetsrelaterade delar i styrsystem – Del 2: Validering*” [13849-2]

SS-EN 61508-1:2002 ”*Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 1Allmänna fodringar*” [61508-1]

SS-EN 61508-2:2002 ”*Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 2 Fodringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system* ” [61508-2]

SS-EN 61508-3:2002 ”*Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 3 Fodringar på programvara*” [61508-3]

SS-EN 61508-4:2002 ”*Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 4 Definitioner och förkortningar*” [61508-4]

SS-EN 61508-7:2002 ”*Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 7 Översikt över metoder och åtgärder*” [61508-7]

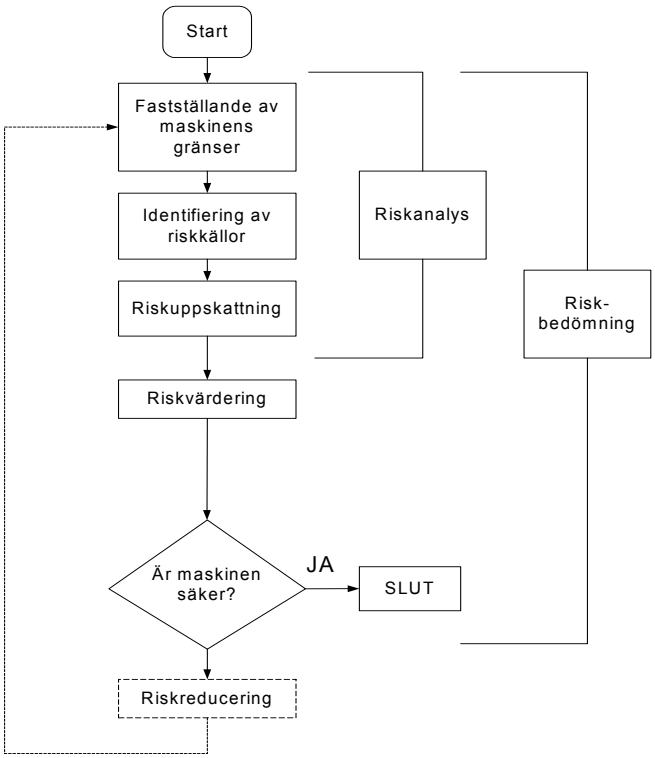
3 Riskanalys

Riskanalysen genomförs av tillverkaren av det kompletta systemet eftersom det är tillverkaren som har kunskap om vilka risker som användning av systemet kan innebära samt i vilken miljö systemet kommer att användas.

Syftet med denna övergripande riskbedömning är att:

- identifiera riskkällor
- identifiera vilka riskfyllda händelser som hänger ihop med varje enskild riskkälla
- avgöra om det krävs någon typ av riskreduktion
- bestämma sig för hur man skall åstadkomma krävd riskreduktion
  - bestämning av den säkerhetskritiska funktionen
  - bestämning av riskreduktion

Nedanstående flödesschema beskriver arbetssättet vid riskanalys:



Figur 5: Flödesschema vid riskbedömning, EN ISO 14121-1

Standarden EN ISO 14121-1:2007 *”Maskinsäkerhet – Riskbedömning - Del 1: Principer”* ger vägledning och vilken information som behövs för att kunna utföra en riskbedömning av maskiner. Som ett komplement finns en teknisk rapport ISO/TR 14121-2:2007 *”Maskinsäkerhet – Riskbedömning – Del 2: Praktisk vägledning och exempel på metoder”*. Rapporten ger praktisk vägledning gällande risk reducering och val av lämpliga skyddsåtgärder för att uppnå lämplig säkerhets nivå.

För de säkerhetskritiska funktioner som identifierats genom riskanalysen och baseras på styrsystemet (E/E/PES) tas lämplig nivå av riskreducering fram med hjälp av [13849-1](PLr) eller [62061] (SIL).

3.1 Riskanalys enligt SS-EN ISO 13849-1:2008

Kapitel 4.1, 4.2 och 4.3 i [13849-1] beskriver i detalj vilka krav som ställs på riskanalysen. När man identifierat riskkällor samt tillhörande riskfyllda händelser är nästa steg att bestämma sig för vilka säkerhetskritiska funktioner man behöver införa och tillhörande krav på riskreduktion.

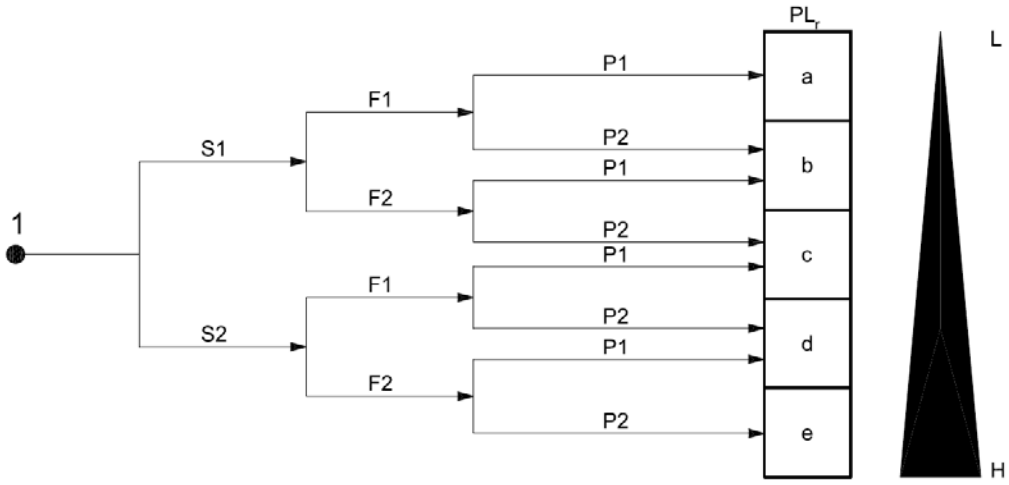
I [13849-1] finns definierat fem olika riskreduceringsnivåer (eng. Performance Level) från PL a till PL e där PL a ger minst riskreduktion och PL e ger mest riskreduktion, enligt tabell 3 i [13849-1] (Figur 6).

Table 3 — Performance levels (PL)

PL	Average probability of dangerous failure per hour 1/h
a	$\geqslant 10^{-5}$ to $< 10^{-4}$
b	$\geqslant 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geqslant 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geqslant 10^{-7}$ to $< 10^{-6}$
e	$\geqslant 10^{-8}$ to $< 10^{-7}$
NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.	

Figur 6: ISO 13849-1 Table 3 – PLs

Med hjälp av Figur 7 (Figure A.1 i [13849-1]) kan man komma fram till lämplig risk-reduktionsnivå för de säkerhetskritiska funktionerna



Key

1 starting point for evaluation of safety function's contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
PL_r required performance level

Risk parameters:

S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

Figure A.1 — Risk graph for determining required PL_r for safety function

Figur 7: ISO 13849-1 Figure A.1– Risk graph

3.2 Riskanalys enligt SS-EN 62061:2005

Kapitel 5.2 i [62061] beskriver i detalj vilka krav som ställs på riskanalysen. När man identifierat riskkällor samt tillhörande riskfyllda händelser är nästa steg att bestämma sig för vilka säkerhetskritiska funktioner man behöver införa och tillhörande krav på riskreduktion.

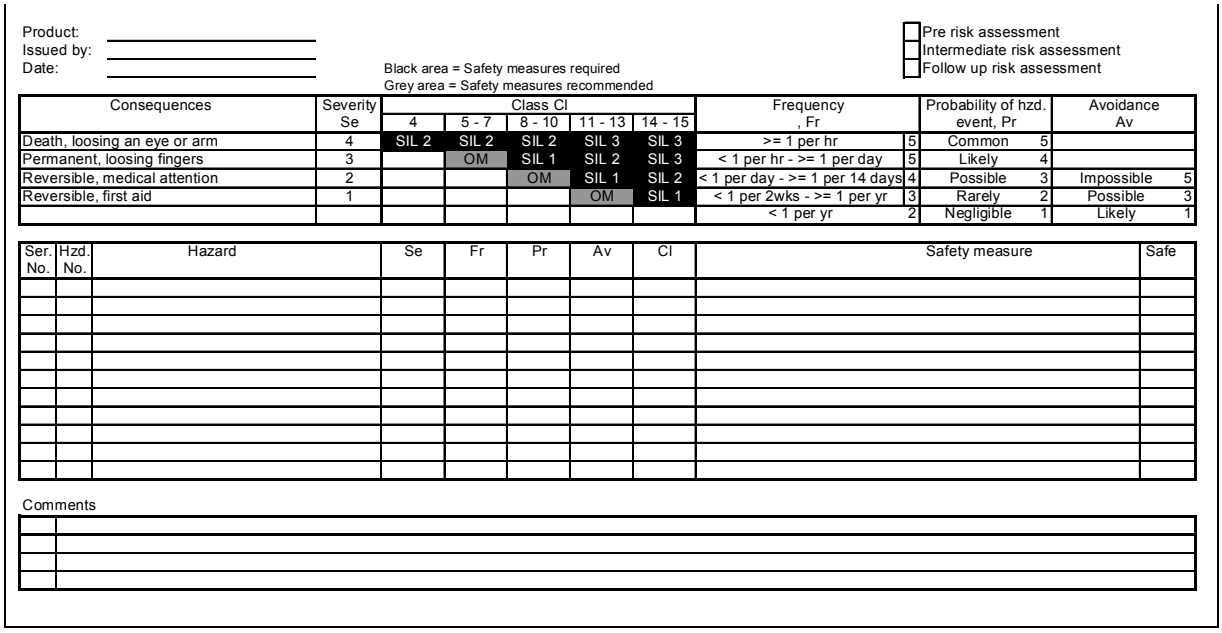
I [62061] finns definierat tre olika riskreduceringsnivåer (eng. Safety Integrity Level) från SIL 1 upp till SIL 3 där SIL 1 ger minst riskreduktion och SIL 3 ger mest riskreduktion, se Figur 8 (Table 3 i [62061]).

Table 3 – Safety integrity levels: target failure values for SRCFs

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Figur 8: IEC 62061 Table 3 – SILs

Med hjälp av Figur 9 (Figure A.3 i [62061]) kan man komma fram till lämplig risk-reduktionsnivå för de säkerhetskritiska funktionerna



Product: _____
Issued by: _____
Date: _____

Black area = Safety measures required
Grey area = Safety measures recommended

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Consequences	Severity Se	Class Cl 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency, Fr		Probability of hzd. event, Pr		Avoidance Av	
Death, loosing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	>= 1 per hr	5	Common	5		
Permanent, loosing fingers	3		OM	SIL 1	SIL 2	SIL 3	< 1 per hr - >= 1 per day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	< 1 per day - >= 1 per 14 days	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	< 1 per 2wks - >= 1 per yr	3	Rarely	2	Possible	3
							< 1 per yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

Figur 9: IEC 62061 Figure A.3 – Risk assessment

4 Specifikation av säkerhetskrav

Efter att man har identifierat de säkerhetskritiska funktionerna samt deras tillhörande SIL/PL måste man gå vidare och ta fram en separat kravspecifikation för de olika säkerhetskritiska funktionerna.

Syftet med denna säkerhetskravspecifikation är att mer detaljerat beskriva hur den säkerhetskritiska funktionen är tänkt att fungera. Denna kravspecifikation är väldigt viktig för att kunna gå vidare och konstruera de säkerhetskritiska funktionerna och dessutom är det detta dokument man utgår ifrån när man skall validera konstruktionen.

I kapitel 5 i [62061] beskrivs generellt hur säkerhetskravspecifikationen skall utformas.

I kapitel 5 i [13849-1] beskrivs generellt hur säkerhetskravspecifikationen skall utformas. Dessutom finns det lite mer detaljerad information om vanliga säkerhetskritiska funktioner som till exempel säkerhetsrelaterade stopfunktioner, manuella återställningsfunktioner samt start-/återstartsfunktioner.

5 Beräkning av hårdvarutillförlitlighet för den kompletta säkerhetskritiska funktionen

Både [62061] och [13849-1] ställer krav på beräkning av hårdvarutillförlitlighet. Tillvägagångssättet skiljer sig ganska mycket mellan dessa två standarder och därför kommer dessa beräkningar att beskrivas separat.

5.1 Krav enligt SS-EN 62061:2005 för den kompletta säkerhetskritiska funktionen

Som tidigare påpekats är [62061] tänkt att användas vid konstruktion av E/E/PE-baserade säkerhetskritiska funktioner och inte vid konstruktion av de ingående delsystemen. På grund av detta handlar tillförlitlighetsdelarna i [62061] mycket om att man skall ställa rätt krav på delsystemtillverkarna. När man fått rätt information från komponent-leverantörerna är det enkelt att summera ihop tillförlitligheten för hela den säkerhets-kritiska funktionen.

Utgående från vald hårdvarulösning skall man, genom beräkningar, kunna visa att man uppfyller de SIL-krav som identifierades i samband med den övergripande riskanalysen.

Innan man börjar fundera på vilka krav som ställs på de ingående komponenterna är det viktigt att få klart för sig gränserna för den säkerhetskritiska funktionen. I [62061] bygger man upp en säkerhetskritisk funktion (SRCF) med hjälp av funktionsblock. Funktions-block definieras på följande sätt i [62061]:

"the smallest element of a SRCF whose failure can result in a failure of the safety function"

Varje sådant funktionsblock kan även delas upp i så kallade funktionsblockselement. Funktionsblockselement definieras på följande sätt i [62061]:

"part of a function block"

Utgående från den logiska bilden av den säkerhetskritiska funktionen som beskrivs av funktionsblocken behöver man gå vidare och fundera på vilka delsystem som behövs för att realisera de olika funktionsblocken. Delsystem definieras på följande sätt i [62061]:

"entity of the top-level architectural design of the SRECS where a failure of any subsystem will result in a failure of a safety-related control function"

Denna definition innebär att en säkerhetskritisk funktion på översta nivå endast består av ett antal seriekopplade delsystem.

På samma sätt som för funktionsblock kan man dela upp delsystem i så kallade delsystemelement. Delsystemelement definieras på följande sätt i [62061]:

"part of a subsystem, comprising a single component or any group of components"

Hårdvarutillförlitlighetskraven i [62061] är uppdelade i följande delar:

- Begränsningar i vald hårdvaruarkitektur för ingående delsystem
- Sannolikhet för farliga slumpmässiga hårdvarufel (PFH_d)

Begränsningar i vald hårdvaruarkitektur för ingående delsystem

Kravet i [62061] gällande begränsningar i vald hårdvaruarkitektur för ingående delsystem handlar om att man skall kunna visa att alla ingående delsystem i en säkerhetskritisk funktion har en hårdvaruarkitektur som uppfyller kraven för en viss SIL.

Enligt tidigare definition av delsystem innebär detta att arkitekturen individuellt hos varje ingående delsystem måste uppfylla den SIL som gäller för hela den säkerhetskritiska funktionen.

Sannolikheten för farliga slumpmässiga hårdvarufel (PFH_d)

Det totala PFH_D värdet för den kompletta säkerhetskritiska funktionen erhålles genom att summera ihop PFH_D värden för de ingående delsystemen:

$$PFH_D = PFH_{D1} + ... + PFH_{Dn} + P_{TE}$$

PFH_D	Den totala sannolikheten för farligt fel per timma för den kompletta säkerhetskritiska funktionen
PFH_{D1}	Sannolikheten för farligt fel per timma för delsystem 1
PFH_{Dn}	Sannolikheten för farligt fel per timma för delsystem n
P_{TE}	Sannolikheten för farliga sändningsfel (vid digital kommunikation)

Den totala sannolikheten för farligt fel per timma för den kompletta säkerhetskritiska funktionen måste vara tillräckligt lågt för att uppfylla kraven för viss SIL enligt nedanstående tabell:

Tabell 3: SIL vs. sannolikhet för fel per timma

SIL	PFH_D(Probability of Dangerous Failure per Hour)
3	$\geq 10^{-8}$ till $< 10^{-7}$
2	$\geq 10^{-7}$ till $< 10^{-6}$
1	$\geq 10^{-6}$ till $< 10^{-5}$

Hårdvarutillförlitlighetskraven i [62061] för den kompletta säkerhetskritiska funktionen skiljer sig något åt beroende på typ av delsystem.

[62061] tar upp följande tre typer av delsystem:

- Komplexa programmerbara elektroniska delsystem
- Lågkomplexa delsystem konstruerade enligt ISO 13849-1:1999 och validera enligt ISO 13849-2:2003
- Lågkomplexa delsystem

5.1.1 Komplexa programmerbara elektroniska delsystem

Följande text finns att läsa under NOTE 2 i [62061]:

"In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS."

I [62061] definieras komplex komponent på följande sätt:

component in which
. the failure modes are not well-defined; or
. the behaviour under fault conditions cannot be completely defined

Tillverkaren av SIL-klassade komplexa programmerbara elektroniska delsystem skall kunna garantera att de uppfyller relevanta krav i IEC 61508 (till exempel genom att kunna tillhandahålla ett certifikat från en oberoende tredje part)

Dessa tillverkare skall kunna tillhandahålla följande information:

- Vilken SIL-nivå hårdvaruarkitekturen motsvarar
- λ_{De} antalet farliga fel per timma i en komponent
- Diagnostisk täckningsgrad (DC – Diagnostic Coverage)
- Diagnostiskt testintervall
- Proof-test intervall alternativt komponentens totala livslängd

5.1.1.1 Begränsningar i vald hårdvaruarkitektur för komplexa programmerbara elektroniska delsystem

Innan man kan gå in på vilka arkitekturkrav som gäller för komplexa programmerbara delsystem behöver man först förklara följande begrepp:

- Safe failure fraction (förkortas SFF)
- Hardware fault tolerance (förkortas HFT)

Följande definition av Safe failure fraction finns i [62061]:

"fraction of the overall failure rate of a subsystem that does not result in a dangerous failure"

Den matematiska definitionen av Safe failure fraction är:

$$\text{SFF} = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda_d + \sum \lambda_s} \quad [\%]$$

där

λ_S felintensiteten för säkra fel

λ_{DD} den andelen av de farliga felen som upptäcks med hjälp av diagnostiska funktioner

$\sum \lambda_s + \sum \lambda_d$ totala felfrekvensen

Följande definition av Hardware fault tolerance finns i NOTE 1 i Tabell 5 i [62061]:

"A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function"

Figur 10 (Table 5 i [62061]) beskriver hur maximal hävdad arkitektur-SIL för ett visst delsystem beror på hur man kombinerar ihop Safe failure fraction och Hardware fault tolerance.

Table 5 – Architectural constraints on subsystems. Maximum SIL that can be claimed for a SRCF using this subsystem			
Safe failure fraction	**Hardware fault tolerance (see Note 1)**		
	0	1	2
< 60 %	Not allowed (for exeptions seeNote3)	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL3 (see Note 2)
≥ 99%	SIL3	SIL3 (see Note 2)	SIL3 (see Note 2)
NOTE 1 A hardware fault tolerance of *N* means that *N+1* faults could cause a loss of the safety-related control function NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1 NOTE 3 See 6.7.6.4 or for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see 6.7.77.			

Figur 10: IEC 62061 Table 5 – Architectural constraints

Om man skall använda en inköpt komponent som redan uppfyller arkitekturkraven för en viss SIL behöver man inte ta hänsyn till Table 5 i [62061] i detalj utan i detta fall beskriver Table 5 vilka valmöjligheter tillverkaren har för att kunna nå upp till en viss SIL (alltså hur man kan kombinera SFF och HFT).

Sannolikheten för farliga slumpmässiga hårdvarufel i komplexa programmerbara delsystem

Kapitel 6.7.8.2 i [62061] ger ett antal olika exempel på hur delsystem kan kopplas samt tillhörande beräkningsformler för att bestämma PFH_D:

- Zero fault tolerance without a diagnostic function
- Single fault tolerance without a diagnostic function

- Zero fault tolerance with a diagnostic function
- Single fault tolerance with a diagnostic function

För att kunna genomföra dessa beräkningar är det viktigt att man får rätt data från komponentleverantörerna.

Då man inför redundans (single fault tolerance) är det även viktigt att ta hänsyn till gemensamma fel som ”slår” på båda kanalerna (eng. common cause failure). Kapitel 6.7.8.3 och Annex F i [62061] ger rekommendationer kring hur man skall skatta dessa gemensamma fel genom att bestämma en så kallad β-factor.

5.1.2 Lågkomplexa delsystem konstruerade enligt ISO 13849-1:1999 och validerade enligt ISO 13849-2:2003

I [62061] finns det en möjlighet att använda komponenter som tidigare konstruerats enligt ISO 1384-1:1999 (EN 954-1) och validerats enligt ISO 13849-2:2003 (prEN 954-2). Detta är dock endast möjligt för så kallade lågkomplexa komponenter.

Följande definition av lågkomplex komponent finns beskriven i [62061]:

component in which
. the failure modes are well-defined; and
. the behaviour under fault conditions can be completely defined

Tillverkaren av lågkomplexa komponenter konstruerade enligt ISO 13849-1:1999 och validerade enligt ISO 13849-2:2003 skall kunna visa att de uppfyller alla relevanta krav i denna standard.

En tillverkare skall kunna tillhandahålla följande information:

- Uppfylld kategori enligt ISO 13849-1:1999 och ISO 13849-2:2003
- Hårdvarufeltålighet (HFT)
- Safe failure fraction (SFF)
- Diagnostisk täckningsgrad (DC – Diagnostic Coverage)
- MTTF (Mean TimeTo Failure) värde
- Vilken SIL-nivå hårdvaruarkitekturen motsvarar
- PFH_D threshold value
- Test/check cycle time

Figur 11 (Table 6 i [62061]) beskriver arkitekturkraven för en lågkomplex komponent konstruerad enligt ISO 13849-1:1999 och validerad enligt ISO 13849-2:2003:

Table 6 – Architectural constraints: SILCL relating to categories			
Category	**Hardware fault tolerance**	**SFF**	**Maximum SIL claim limit according to architectural constraints**
	It is assumed that subsystems with the stated category have the characteristics given below.		
1	0	< 60 %	See Note 1
2	0	60 % - 90 %	SIL 1 (see Note 2)
3	1	< 60 %	SIL1
	1	60 % - 90 %	SIL2
4	>1	60 % - 90 %	SIL3 (see Note 3)
	1	> 90 %	SIL3 (see Note 4
Note 1 Subsystems that have a SFF of <60 % but are designed in accordance with Category 1 of ISO 13849-1:1999 and validated in accordance with ISO 13849-2:2003 are assumed to achieve a SILCL of SIL1. **Note 2** The case for Category 2 where SFF is > 90 % is assumed not to be achieved by the design requirements of ISO 13849-1:1999 **Note 3** The diagnostic coverage is assumed to be less than 90 % for Category 4 subsystems where greater than single hardware fault tolerance (i.e. accumulated faults) is considered. **Note 4** Category 4 requires a SFF of more than 90 % but less than 99 % when single hardware fault tolerance is considered. **Note 5** Category B in accordance with ISO 13849-1:1999 is not considered sufficient to achieve SIL 1.			

Figur 11: IEC 62061 Table 6 – Architectural constraints

Följande information finns beskriven i kapitel 6.7.8.1.6 I [62061]:

”Where a low complexity subsystem is designed according to ISO 13849-1 and validated according to ISO 13849-2 and also meets the requirements for architectural constraints (see chapter 6.7.6 in 62061) and systematic safety integrity (see chapter 6.7.9 in 62061), the threshold values of probability of dangerous failure (PFH_D) given in Table 7 can be used to estimate the hardware safety integrity (see chapter 6.6.3.2 in 62061).”

Table 7 – Probability of dangerous failure

Category	**Hardware fault tolerance**	**DC**	**PFH_D threshold values (per hour) that can be claimed for the subsystem PFH_D ($MTTF_{subsystem}$, T_{test}, DC)(See Note 1)**
	It is assumed that subsystems with the stated category have the characteristics given below.		
1	0	0 %	To be provided by supplier or use generic data (see annex D)
2	0	60 % - 90 %	$\geq 10^{-6}$
3	1	60 % - 90 %	$\geq 2 * 10^{-7}$
4	>1	60 % - 90 %	$\geq 3 * 10^{-8}$
	1	> 90 %	$\geq 3 * 10^{-8}$
NOTE 1 The PFH_D threshold value is a function of the subsystem MTTF (to be derived by the subsystem manufacturer or from relevant component data handbooks), test/check cycle time as specified in the safety requirements specification (this information is also required for subsystem validation in accordance with ISO 13849-2:2003, 3.5) and the diagnostic coverage as shown in this table (these values are based on the requirements of the categories described in ISO 13849-1:1999). NOTE 2 Category B in accordance with ISO 13849-1:1999 cannot be considered sufficient to achieve SIL 1.			

Figur 12: IEC 62061 Table 7 – Probability of dangerous failure

Figur 11 och Figur 12 (Table 6 och Table 7 i [62061]) gör det alltså möjligt att använda befintliga lågkomplexa komponenter och lyfta in dessa som ett delsystem i den kompletta säkerhetskritiska funktionen.

5.1.3 Lågkomplexa delsystem

Följande definition av Low complexity component finns beskriven i [62061]:

component in which
- *the failure modes are well-defined; and*
- *the behaviour under fault conditions can be completely defined*

En tillverkare skall kunna tillhandahålla följande information:

- Vilken SIL-nivå hårdvaruarkitekturen motsvarar
- λ_{De} antalet farliga fel per timma i en komponent
- Proof test interval/lifetime
- B10 value (endast för elektromekaniska delsystem)

5.1.3.1 Begränsningar i vald hårdvaruarkitektur för lågkomplexa delsystem

Table 5 i [62061] (Figur 13) är även tillämpbar för lågkomplexa delsystem och beskriver hur uppnådd arkitektur-SIL för ett visst delsystem beror på hur man kombinerar Safe failure fraction och Hardware fault tolerance.

Table 5 – Architectural constraints on subsystems. Maximum SIL that can be claimed for a SRCF using this subsystem

Safe failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60 %	Not allowed (see Note 3)	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL3 (see Note 2)
≥ 99%	SIL3	SIL3 (see Note 2)	SIL3 (see Note 2)

NOTE 1 A hardware fault tolerance of *N* means that *N+1* faults could cause a loss of the safety function
NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1
NOTE 3 Exception, see 6.7.7 in [1].

Figur 13: IEC 62061 Table 5 – Architectural constraints

Om man skall använda en inköpt lågkomplex komponent som redan uppfyller arkitekturkraven för en viss SIL behöver man inte ta hänsyn till Tabell 5 i [62061] i detalj utan i detta fall beskriver Tabell 5 vilka valmöjligheter tillverkaren har för att kunna nå upp till en viss SIL (alltså hur man kan kombinera SFF och HFT)

Sannolikheten för farliga slumpmässiga hårdvarufel i lågkomplexa delsystem

Kapitel 6.7.8.2 i [62061] ger ett antal olika exempel på hur delsystem kan kopplas samt tillhörande beräkningsformler för att bestämma PFH_D:

- Zero fault tolerance without a diagnostic function
- Single fault tolerance without a diagnostic function
- Zero fault tolerance with a diagnostic function
- Single fault tolerance with a diagnostic function

För att kunna genomföra dessa beräkningar är det viktigt att man får rätt data från komponentleverantörerna.

Då man inför redundans (single fault tolerance) är det även viktigt att ta hänsyn till gemensamma fel som ”slår” på båda kanalerna (eng. common cause failure). Kapitel 6.7.8.3 och Annex F i [62061] ger rekommendationer kring hur man skall skatta dessa gemensamma fel genom att bestämma en så kallad β-factor.

Även elektromekaniska delsystem definieras som lågkomplexa komponenter. Följande information om lågkomplexa komponenter finns beskrivet i kapitel 6.7.4.4.2 och 6.7.8.2.1 i [62061]:

For electromechanical subsystems the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle of the application (see 5.2.3). This information should be based upon a B10 value (i.e. the expected time at which 10% of the population will fail). See also IEC 61810-2.

For electromechanical devices the failure rate has to be determined using the B_{10} value and the duty cycle C of the application as specified (see 5.2.3 in 62061).

- $\lambda = 0.1*C/B_{10}$

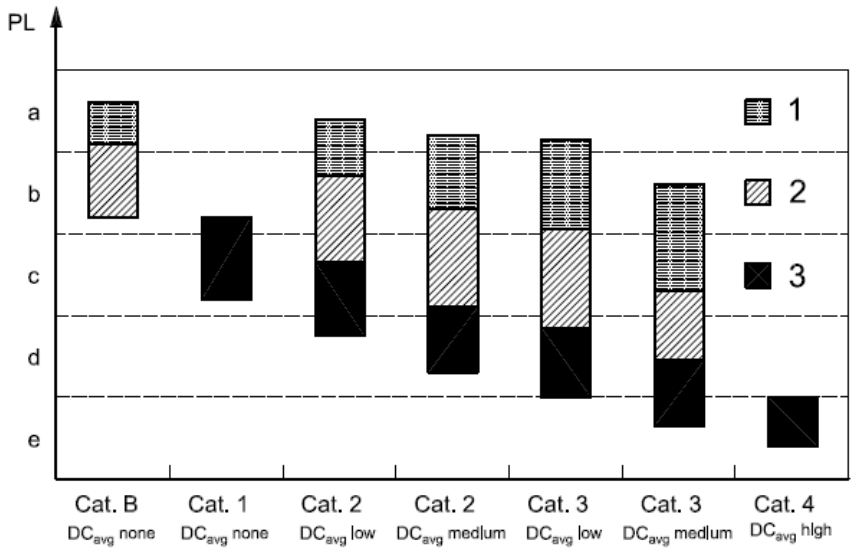
5.2 Hårdvarutillförlitlighetskrav enligt SS-EN ISO 13849-1:2008 för den kompletta säkerhetskritiska funktionen

Innan man påbörjar tillförlitlighetsberäkningarna är det viktigt att man har klart för sig gränserna för den säkerhetskritiska funktionen. Följande NOTE 1 finns att läsa i kapitel 3.1.1 i [13849-1]:

“The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).”

Utgående från riskanalysen har man kommit fram till en viss PL_r (PL required). Syftet med tillförlitlighetsberäkningarna enligt [13849-1] är att visa att den PL man når efter att man kopplat samman alla ingående komponenter överensstämmer med PL_r.

Beroende på vilken PL_r man kommit fram till i riskanalysen finns det flera olika möjligheter att uppfylla detta krav. Figur 14 (Figure 5 i [13849-1]) visar dessa olika möjligheter.



Key

PL performance level

1 $MTTF_d$ of each channel = low

2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_d$ of each channel and PL

Figur 14: ISO 13849-1 Figure 5 – Relationship between Cat, DC, MTTF, and PL

Som framgår i Figur 14 är standarden flexibel på så sätt att det går att tillämpa olika kategorier för att nå upp till en viss PL och dessutom kommer erhållen PL även att påverkas av parametrarna $MTTF_d$ samt DC_{avg}.

I Figur 14 framgår inte de exakta PL-gränserna för respektive kombination av kategori, $MTTF_d$ samt DC_{avg}. Annex K i [13849-1] innehåller de exakta numeriska gränserna för respektive kombination.

För att man skall kunna använda Figur 5 i [13849-1] för att bestämma erhållen PL för hela säkerhetskritiska funktionen måste man kunna visa att den arkitektur man valt överensstämmer med vissa fördefinierade arkitekturer (motsvarande kategorierna B,1, 2, 3 & 4 i EN 954-1) enligt kapitel 6.2 i [13849-1]:

"It is important that the PL shown in Figure 5, depending on the category, MTTFd of each channel and DCavg, is based on the designated architectures. If Figure 5 is used to estimate the PL the architecture of the SRP/CS should be demonstrated to be equivalent to the designated architecture of the claimed category."

Dessutom måste följande krav vara uppfyllda för att kunna tillämpa Figur 5 vid bestämning av PL enligt kapitel 4.5.4 i [13849-1].

- mission time, 20 years (see Clause 10);
- constant failure rates within the mission time;
- for category 2, demand rate u 1/100 test rate;
- for category 2, MTTFd,TE larger than half of MTTFd,L.

Det första man gör är att bestämma $MTTF_d$ värdet för en viss vald arkitektur/kategori. För kategori B, 1 & 2 får man fram det totala $MTTF_d$ helt enkel genom att summera ihop bidraget från de ingående komponenterna ($MTTF_d$ värdet för de ingående komponenterna erhålles från komponentleverantören).

För kategori 3 & 4 är det litet mer komplicerat eftersom man i detta fall har två olika kanaler. I detta fall skall man räkna fram ett separat $MTTF_d$ värde för varje enskild kanal ($MTTF_d$-värdet för de ingående komponenterna erhålls från komponentleverantören) och sedan räkna fram ett sammanvägt $MTTF_d$ värde med hjälp av ekvation D.2 i [13849-1] (Figur 15).

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right] \quad (D.2)$$

Figur 15: ISO 13849-1 Equation D.2 – MTTF

Det är detta sammanvägda $MTTF_d$ värde som man sedan använder i Figur 14.

I Figur 14 finns enbart angivet tre olika $MTTF_d$ -spann (Low, Medium, High). Dessa finns definierade i Table 5 i [13849-1] (Figur 16).

Table 5 — Mean time to dangerous failure of each channel ($MTTF_d$)

$MTTF_d$	
Denotation of each channel	**Range of each channel**
Low	3 years $\leqslant MTTF_d <$ 10 years
Medium	10 years $\leqslant MTTF_d <$ 30 years
High	30 years $\leqslant MTTF_d \leqslant$ 100 years

NOTE 1 The choice of the $MTTF_d$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $MTTF_d$ value of each channel less than three years is not expected to be found for real SRP/CS since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $MTTF_d$ value of each channel greater than 100 years is not acceptable because SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_d$ of each channel values to a maximum of 100 years refers to the single channel of the SRP/CS which carries out the safety function. Higher $MTTF_d$ values can be used for single components (see Table D.1).

NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.

Figur 16: ISO 13849-1 Table 5 – MTTF

Vad man får göra är helt enkelt att kontrollera inom vilket spann det uträknade $MTTF_d$-värdet ligger.

Därefter går man vidare och bestämmer ett sammanvägt DC_{avg}-värde för hela den säkerhetskritiska funktionen med hjälp av ekvation E.1 (Figur 17).

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

Figur 17: ISO 13849-1 Equation E.1 – Average DC

Det är detta sammanvägda DC_{avg} värde som man sedan använder i Figur 14.

I Figur 5 i [13849-1] finns det enbart angivet fyra olika DC_{avg}-värden (None, Low, Medium, High). Dessa finns definierade i Tabell 6 i [13849-1] (Figur 18).

Table 6 — Diagnostic coverage (DC)

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ⩽ DC < 90 %
Medium	90 % ⩽ DC < 99 %
High	99 % ⩽ DC

NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g. IEC 61508) dealing with diagnostic coverage of tests. Investigations show that (1 - DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 - DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called "none". A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.

Figur 18: ISO 13849-1 Table 6 – Diagnostic coverage

Vad man får göra är helt enkelt att kontrollera inom vilket spann det uträknade DC_{avg}-värdet ligger.

För kategori 2, 3 och 4 måste man även ta hänsyn till gemensamma fel och kunna visa att man som minst når 65 poäng när man går igenom Annex F i [13849-1].

Efter att man valt en viss kategori och räknat ut $MTTF_d$, DC_{avg} samt vid behov kontrollerat att gemensamma fel hanteras på ett riktigt sätt kan man gå tillbaka och se om man uppfyller de ursprungliga kraven som definierades av PL_r.

Om man inte lyckas uppfylla den PL_r som krävdes så får man göra om tillförlitlighetsberäkningarna och i samband med detta finns det flera olika möjligheter:

- Välja en annan kategori enligt EN 954-1, till exempel gå över ifrån kategori 2 till kategori 3
- Byta ut ingående komponenter så att man får ett bättre $MTTF_d$-värde, till exempel att man går från $MTTF_d$ = Medium till $MTTF_d$ = High
- Förbättra den inbyggda diagnostiken för vissa komponenter, till exempel så att man kan hävda DC = High istället för DC = Low

6 Beräkning av hårdvarutillförlitlighet för enskilda komponenter

Även då det gäller tillförlitlighetsberäkningar på enskilda komponenter skiljer sig dessa standarder ganska mycket.

När det gäller [62061] är den i första hand tänkt att användas för den kompletta säkerhetskritiska funktionen och när det gäller hårdvarutillförlitlighetskrav på elektriska, elektroniska och programmerbara elektroniska komponenter så refererar man till IEC 61508. Däremot finns det beskrivet i [62061] hur man bestämmer hårdvarutillförlitlighet för elektromekaniska komponenter.

[13849-1] är däremot tillämpbar både vid hårdvarutillförlitlighetsberäkningar på enskilda komponenter samt för hela den säkerhetskritiska funktionen.

6.1 Hårdvarutillförlitlighetskrav enligt SS-EN 62061:2005 för de ingående komponenterna

I kapitel 6.7.8.2.1 i [62061] finns beskrivet hur man går till väga för att bestämma hårdvarutillförlitlighet för elektromekaniska komponenter. För E/E/PE-baserade komponenter refererar [62061] till [61508].

For electromechanical devices the failure rate has to be determined using the B10 value and the duty cycle C of the application as specified (see 5.2.3 in 62061).

- $\lambda = 0{,}1 \times C/B10$

NOTE 1 For electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle (see 5.2.3 in 62061). This information should be based upon a B10 value (i.e. the expected time at which 10% of the population will fail). See also IEC 61810-22.

6.2 Hårdvarutillförlitlighetskrav enligt SS-EN ISO 13849-1:2008 för de ingående komponenterna

Annex C i [13849-1] beskriver hur man bestämmer $MTTF_d$ för följande typ av komponenter:

- Hydraulik
- Pneumatik
- Mekanik
- Elektromekanik
- El
- Elektronik
- Programmerbar elektronik

Förutom att bestämma $MTTF_d$ för komponenten så är det även viktigt, där det är applicerbart, att även kontrollera vilka diagnostiska funktioner som finns inbyggda i komponenterna. Vilka diagnostiska krav man måste uppfylla styrs av vilken DC man vill kunna hävda för komponenten (None, Low, Medium, High). Appendix E i [13849-1] innehåller mer detaljerad information om olika typer av diagnostiska funktioner.

6.3 Hårdvarutillförlitlighetskrav enligt SS-EN 61508:2002 för de ingående komponenterna

Hårdvarutillförlitlighetskraven i [61508-2] är uppdelade på följande delar:

- Bestämning av SFF (Safe Failure Fraction)
- Bestämning av PFH_d (Probability of Dangerous Failure per Hour)

Båda dessa delar måste vara uppfyllda för en viss SIL.

6.3.1 Bestämning av SFF (Safe Failure Fraction) med hjälp av FMEDA (Failure Mode Effects and Diagnostics Analysis)

Följande steg måste genomföras för varje identifierad säkerhetskritisk funktion:

1. Bestämma driftsmod (low demand or continuous/high demand)
2. Bestämma SIL nivå för hårdvaran (hårdvaru SIL=SIL framtagen i samband med riskanlys)
3. Dela upp den säkerhetskritiska funktionen i ett antal subsystem. Ett subsystem kan bestå av en enskild komponent eller en grupp av komponenter. Eventuellt är det lämpligt att genomföra en funktionsblocksbeskrivning av den säkerhetskritiska funktionen innan man delar upp den säkerhetskritiska funktionen i subsystem.

    - *För varje identifierat subsystem så är det viktigt att enbart inkludera de komponenter som är direkt relaterade till den säkerhetskritiska funktionen. Om till exempel en 8-kanals A/D omvandlare är definierad som ett subsystem och den säkerhetskritiska funktionen enbart utnyttjar två av dessa kanaler då skall enbart dessa två kanaler inkluderas i beräkningarna av Safe Failure Fraction (SFF) annars finns det risk att man felaktigt hävdar ett för högt SFF värde.*
4. För varje identifierat subsystem måste följande delar genomföras:
    - Bestämma vilken hårdvarufeltolerans som skall användas för subsystemet (d.v.s är subsystemet en-kanaligt eller fler-kanaligt)
5. När hårdvarufeltoleransen är bestämd kan tabell 2 & 3 i [61508-2] användas för att få reda på kraven angående SFF för varje subsystem.
6. Genomföra en FMEDA analys för varje subsystem. Följande aspekter skall beaktas:
    a. Felfrekvens hos enskilda komponenter
        - SN 29500 Siemens standard
        - IEC TR 62380 Reliability Data Handbook Universal model for reliability prediction of electronic components, PCBs and equipment
        - MIL-HDBK-217F Reliability prediction of electronic equipment

    b. Felfall som skall upptäckas beroende på vilken SFF nivå man vill hävda (se tabell A.1 i [61508-2])
    c. Bestäm procentuella fördelningen mellan olika felfall hos viss komponent
    d. Dela upp i felfallen för varje komponent i följande typer: safe detected (λ_{SD}), safe undetected (λ_{SU}), dangerous detected (λ_{DD}), dangerous undetected (λ_{DU})
    e. Ta hänsyn till inbyggd diagnostik (kan ändra λ_{du} till λ_{dd}

f. Eventuellt tillgodoräkna sig att fel i en viss del av systemet kan upptäckas av en annan del, till exempel är det möjligt för en säkerhets-PLC att upptäcka fel i en sensor.
För att kunna tillgodoräkna sig detta måste dessa antaganden tydligt framgå i sensorns säkerhetsspecifikationen.

7. Genomföra en beräkning av safe failure fraction (SFF) för varje subsystem!

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

Safe Failure Fraction (SFF) definieras på följande sätt i IEC 61508:

"fraction of the overall failure rate of a subsystem that does not result in a dangerous failure"

8. Är kraven på safe failure fraction (SFF) från punkt 5 uppfyllda för subsystemet? Om inte finns följande möjligheter:

   a. Behålla samma komponenter i subsystemet men utöka den inbyggda diagnostiken för att upptäcka fler farliga fel. Detta kommer att höja värdet på SFF
   b. Använda mer exakta felfrekvenser för ingående komponenter. Det möjligt att felfrekvensen minskar om generella data byts ut mot komponentspecifika
   c. Öka hårdvarufeltoleransen. Detta kommer att ställa lägre krav på SFF
   d. Byt ut existerande komponenter mot andra "bättre" komponenter som har lägre felfrekvens. Detta kommer att höja värdet på SFF
   e. Eventuellt tillgodoräkna sig att fel i en viss del av systemet kan upptäckas av en annan del (se 6 f)
   f. Minska det individuella SIL-kravet för varje subsystem och istället koppla två eller fler sådana subsystem parallellt för att nå det ursprungliga SIL-kravet (se punkt 9). Denna åtgärd kan eventuellt både sänka kraven på SFF och hårdvarufeltoleransen hos ingående subsystem.

9. Undersöka SIL-begränsningen hos den valda arkitekturen (d.v.s. hur de olika subsystemen är ihopkopplade)

   a. Om den säkerhetskritiska funktionen är uppbyggd av ett antal subsystem som ligger i serie så kommer den maximala SIL-nivån att bestämmas av den svagaste länken
   b. Om den säkerhetskritiska funktionen är uppbyggd av parallella kanaler kan dessa parallella kanaler tillsammans nå en högre SIL-nivå än de individuella subsystemen i varje enskild kanal

6.3.2 Bestämning av PFH_d (Probability of Dangerous Failure per Hour)

Följande ska beaktas då sannolikhet för farligt slumpmässigt hårdvarufel per timma i säkerhetskritiska funktionen uppskattas:

- Systemarkitektur (dvs serie/parallell konfiguration)
- Felfrekvensen hos varje delsystem som skulle orsaka farlig situation men som upptäcks av diagnostiska funktioner
- Felfrekvensen hos varje delsystem som orsakar farlig situation och som inte upptäcks av diagnostiska funktioner
- Benägenheten hos systemet att drabbas av "common cause"-fel (Beta-faktorn)

- ”*Diagnostic coverage*” samt ”*diagnostic test interval*”
- ”Proof test interval” (Mission time)
- Reparationstid för detekterade fel (om relevant)
- Sannolikhet för oupptäckta fel i kommunikation

För att bestämma PFH_d värdet kan man använda ett antal olika tekniker

- Felträdsanalys
- Reliability Block Diagrams (RBD)
- Markov-analys

7 Tekniker för att hantera och undvika systematiska hårdvarufel

Misstag kan aldrig helt undvikas utan fel kommer introduceras under utveckling och konstruktion av hårdvaran. Vid användning av systemet kommer fel också uppstå både orsakade av omgivande miljö och operatörer. Därför är det viktigt att använda tekniker som:

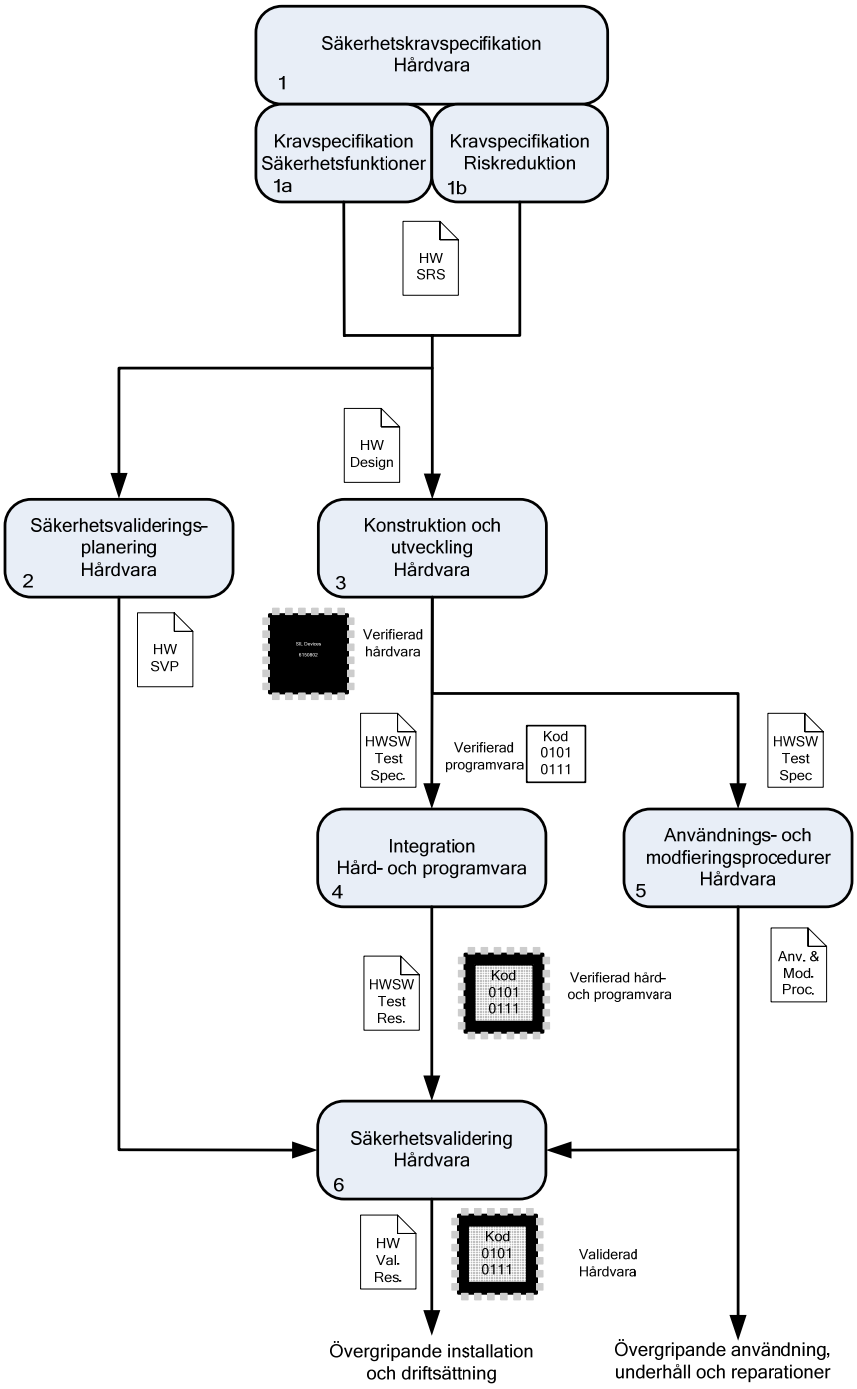
- kan minimera antalet introducerade konstruktionsfel
- får systemet att tolerera och hantera fel som uppkommer under användning

Dessa två klasser av tekniker är i fokus i detta kapitel.

7.1 Livscykel för hårdvaran

Figur 19 visar [61508-2] livscykeln för att uppnå säkerhet i hårdvaran. Utlämnat från figuren är interaktionen med livscykeln för programvaran. [61508-2] är den enda av standarderna som uttryckligen kräver att man upprättar en livscykel för hårdvaran.

För varje steg, eller fas, i livscykeln behövs erfordrad information. Det kan vara konstruktionsdokument, källkodsfiler, hårdvarukomponenter eller en kombination av dessa. Aktiviteterna i en viss fas resulterar i nya dokument samt eventuella programvaru- och hårdvarukomponenter. För varje fas ska man även verifiera att man uppnått rätt resultat.



Figur 19: Exempel på livscykel för hårdvara (IEC 61508)

7.2 Tekniker för att hantera systematiska hårdvarufel

Detta delkapitel ger exempel på tekniker som standarderna finner lämpliga för att hantera de fel som oundvikligen kommer att uppstå när systemet är i drift. Bland teknikerna finns olika former av redundans, olika typer av skydd mot fysisk påverkan samt användar-vänlighet.

För varje kategori av tekniker presenteras en tabell där de tekniker som rekommenderas av en viss standard för en viss riskreduceringsnivå presenteras. När det gäller tekniker rekommenderade av 61508 så har både ”Highly Recommended”- och ”Recommended”-tekniker tagits med. Läsaren bör alltså vara observant på att det finns ytterligare en nivåskillnad mellan teknikerna som inte helt framkommer i tabellerna.

7.2.1 Tekniker för att hantera fel som uppstår under designfasen

Här handlar teknikerna om att övervaka systemet och att lägga till redundans för att kunna detektera och rätta fel. Vidare kan man använda återhämtningstekniker och begränsade driftsmoder ”graceful degradation”.

En jämförelse mellan kraven från de olika standarderna finns i Tabell 4.Tom ruta betyder att inget krav finns. I 13849 kolumnen betyder kursiv stil att kravet kommer från [13849-1] och icke-kursiv stil att kravet kommer ifrån 13849-2.

Tabell 4: Jämförelse av tekniker för att hantera fel p.g.a. hård- och programvarudesign

Krav	61508	62061	13849
Övervakning av programflöde	SIL1-3		*PL a-e*
- Feldetektering genom on-line-övervakning	SIL1-3	SIL1-3	*PL a-e*
- Test m.h.a. redundant hårdvara	SIL1-3	SIL1-3	*PL a-e*
- Test accessport och boundary scan	SIL1-3		
- Tids- och/eller informationsredundans i dataflöde	SIL1-3		
- Diversifierad hårdvara	SIL3	SIL1-3	*PL a-e*
- Feldetektering och diagnos	SIL2-3		
- Felupptäckande och felrättande koder	SIL1-3		
- Failure assertion-programmering	SIL1-3		
- Safety bag-tekniker	SIL2-3		
- Diversifierad programmering	SIL1-3		
- Återhämtningstekniker	SIL1-3		
- Graceful degradation	SIL1-3		

7.2.2 Tekniker för att hantera fel som orsakas av miljöpåverkan

Här handlar teknikerna om att övervaka matningsspänningen, att använda filter och skydd mot miljöpåverkan och att helt enkelt bygga ihop systemet på ett bra sätt med ett lämpligt val av komponenter. Redundans kan också skydda mot vissa typer av fel från miljöpåverkan.

Tabell 5: Jämförelse av tekniker för att hantera fel p.g.a. miljöpåverkan

Krav	61508	62061	13849
Åtgärder mot för stor, för liten, varierande och ingen matningsspänning	SIL1-3	SIL1-3	*PL a-e*
Separation mellan data- och matningsspänningsledare	SIL1-3		
Filtrering och skärmning för att minska påverkan från interferens och skydda mot kortslutningar	SIL1-3		
Skydd mot miljöpåverkan (temperatur, fukt, damm, vibrationer, korrosion)	SIL1-3	SIL1-3	PL a-e
Spatial separering av bussledare	SIL1-3		
Säkert tillstånd vid energiförlust (pneumatisk, hydraulisk, el)		SIL1-3	PL a-e
Åtgärder för att hantera fel i datakommunikation		SIL1-3	*PL a-e*
Mekaniskt länkade kontakter		SIL1-3	PL a-e
Överdimensionering		SIL1-3	PL a-e
Lämpligt materialval och tillverkning		SIL1-3	PL a-e
Korrekt dimensionering och utformning		SIL1-3	PL a-e
Lämplig sammansättning och installation av system och komponenter		SIL1-3	PL a-e
Korrekt inkoppling av skyddsjord			PL a-e
Övervakning av jordfel			PL a-e
Transientskydd			PL a-e
Reduktion av responstid			PL a-e
Användning av kompatibla komponenter		SIL1-3	PL a-e
Säker fastsättning av givare och brytare			PL a-e
Skydd mot oväntad start			PL a-e
Skydd av kontrollkretsen			PL a-e
Sekventiella omslag av seriekontakter			PL a-e
Separationsavstånd			PL a-e
Energibegränsning			PL a-e
Begränsning av storlek hos elektriska parametrar (V, A, J)			PL a-e
Inga odefinierade tillstånd		SIL1-3	PL a-e
Positiv verkan		SIL1-3	PL a-e
Failure mode orientation			PL a-e
Oriented failure mode		SIL1-3	PL a-e
- Feldetektering genom on-line-övervakning	SIL1-3	SIL1-3	*PL a-e*
- Test m.h.a. redundant hårdvara	SIL1-3	SIL1-3	*PL a-e*
- Tids- och/eller informationsredundans i dataflöde	SIL1-3		
- Komplementär signalering	SIL1-3		
- Feldetektering och diagnos	SIL2-3		
- Felupptäckande och felrättande koder	SIL1-3		
- Failure assertion-programmering	SIL1-3		
- Safety bag-tekniker	SIL2-3		
- Diversifierad programmering	SIL1-3		
- Återhämtningstekniker	SIL1-3		
- Graceful degradation	SIL1-3		

7.2.3 Tekniker för att hantera fel som uppstår under användning

Här handlar teknikerna om att skydda ifrån modifiering och att övervaka och kontrollera rimligheten i operatörskommandon.

Tabell 6: Jämförelse av tekniker för att hantera fel p.g.a. användning

Krav	61508	62061	13849
Skydd mot modifiering	SIL1-3	SIL1-3	
- Feldetektering genom on-line-övervakning	SIL1-3		
- Kontroll av inmatning av operatörskommandon	SIL1-3		
- Failure assertion-programmering	SIL1-3		

7.3 Tekniker för att undvika systematiska hårdvarufel

Detta delkapitel ger exempel på tekniker som standarderna finner lämpliga för att undvika att fel introduceras under design av systemet. Teknikerna handlar om hur man konstruerar, till exempel modulbaserat, men även om att man projektleder och dokumenterar på ett bra sätt. Vidare föreslås ett antal verifieringstekniker som till exempel granskning och testning.

7.3.1 Tekniker för att undvika fel under specifikation av hårdvarusäkerhetskrav

Kraven skall härledas från kraven på det programmerbara systemet. Kraven skall vara strukturerade och uttryckta på sådant sätt att de är: tydliga, verifierbara, lätta att underhålla, passande för riskreduceringsnivå, spårbara och otvetydiga. Krav skall exempelvis tas fram på säkerhetsrelaterade funktioner som rör:

- realtidsegenskaper
- gränssnitt mot icke-säkerhetskritiska delar och gränssnitt mellan hård- och programvara
- möjliggör att applikationen kan nå eller behålla ett säkert tillstånd
- driftsmoder

Dessutom ska nödvändig riskreduceringsnivå anges för alla ovanstående funktioner där det är lämpligt. Där det passar bör semiformella metoder som till exempel funktions-blocks-, sekvens-, tillstånds- och dataflödesdiagram användas.

Kravspecifikationen ska dokumenteras och granskas.

Tabell 7: Jämförelse av tekniker för att undvika fel under kravspecifikation

Krav	61508	62061	13849
Projektledning	SIL1-3		
Dokumentation	SIL1-3	SIL1-3	
Strukturerad specifikation	SIL1-3	SIL1-3	
Separering av icke- och säkerhetskritiska delar	SIL1-3		PL a-e
- Granskning av specifikationen	SIL1-3		
- Semiformella metoder	SIL1-3		
- Checklistor	SIL1-3		
- Datorstödda specifikationsverktyg	SIL2-3		
- Formella metoder	SIL3		
Balans mellan komplexitet och enkelhet			PL a-e

7.3.2 Tekniker för att undvika fel under system och modulkonstruktion

Hårdvaran bör vara modulbaserad, lätt att testa och modifiera på ett säkert sätt. Arkitekturen skall vara uppdelad i större delsystem. Man skall även deklarera om delsystemen ska nyutvecklas eller är befintliga, om de har verifierats tidigare, om de är säkerhetsrelaterade och vilken riskreduktionsnivå de har.

Tillräckligt oberoende mellan kritisk och icke-kritisk hårdvara måste visas annars skall den icke-kritiska utvecklas på samma rigorösa sätt som den kritiska.

Där det passar bör semiformella metoder som till exempel funktionsblocks-, sekvens-, tillstånds- och dataflödesdiagram användas.

Ett systemspecifikationsdokument tas fram och granskas och parallellt tas ett testdokument fram för integrationstesterna. Därefter tas modulspecifikationsdokument fram och granskas. Parallellt tas även testdokument för modultestfasen fram.

Tabell 8: Jämförelse av tekniker för att undvika fel under konstruktion och utveckling

Krav	61508	62061	13849
Beaktande av riktlinjer och standarder	SIL1-3		
Projektledning	SIL1-3		
Dokumentation	SIL1-3	SIL1-3	
Strukturerad design	SIL1-3		
Modulbaserad design	SIL1-3		
- Användning av välbeprövade komponenter	SIL1-3		
- Semiformella metoder	SIL1-3		
- Checklistor	SIL2-3		
- Datorstödd utvecklingsmiljö	SIL2-3	SIL1-3	*PL a-e*
- Simulering	SIL2-3	SIL1-3	*PL a-e*
- Granskning av hårdvaran	SIL2-3	SIL1-3	*PL a-e*
- Formella metoder	SIL3		

7.3.3 Tekniker för att undvika fel under modul och systemtest

Modulerna och systemet skall testas så som specificerades i testspecifikationerna under modul- och systemkonstruktionsfaserna. Testerna ska visa att modulerna och systemet

enbart gör det de är avsedda att göra och ingenting annat. Testresultaten skall dokumenteras.

Tabell 9: Jämförelse av tekniker för att undvika fel under integration

Krav	61508	62061	13849
Funktionsprov	SIL1-3	SIL1-3	*PL a-e*
Projektledning	SIL1-3		*PL a-e*
Dokumentation	SIL1-3	SIL1-3	*PL a-e*
- Black-box-testning	SIL1-3		*PL a-e*
- Användarerfarenhet (field experience)	SIL1-3		
- Statistisk testning	SIL3		
Dynamiska tester		SIL1-3	

7.3.4 Tekniker för att undvika fel under validering

Syftet med valideringen är att säkerställa att hårdvaran uppfyller alla krav på säkerhet som ställts i specifikationen och att man når upp till erfordrad riskreduceringsnivå. Det är viktigt att man följer den framtagna valideringsplanen. Resultaten från valideringen skall dokumenteras och åtgärdsplaner vid upptäckta felaktigheter specificeras.

I [13849] är det del 2 som handlar om validering.

Testning, analyser och felinjicering skall vara de huvudsakliga valideringsmetoderna. Verktyg som används under valideringen skall vara kvalificerade eller på andra sätt vara erkända att vara passande för aktiviteten.

Tabell 10: Jämförelse av tekniker för att undvika fel under validering av säkerhet

Krav	61508	62061	13849
Funktionsprov	SIL1-3	SIL1-3	PL a-e
Funktionsprov under miljöpåverkan	SIL1-3	SIL1-3	PL a-e
Immunitetsprov	SIL1-3	SIL1-3	PL a-e
Felinjicering (om krävd DC > 90%)	SIL1-3		
Felinjicering (om krävd SFF > 90%)		SIL1-3	
Projektledning	SIL1-3		
Dokumentation	SIL1-3		
- Statisk, dynamisk och failure-analys	SIL2-3	SIL2-3	
- Simulering och failure-analys	SIL2-3	SIL1-2	
- ”Värsta fallet”, dynamisk och failure-analys	SIL3		
- Statisk och failure-analys	SIL1-2	SIL1-2	
- Utökat funktionsprov	SIL2-3		
- Black-box-testning	SIL1-3	SIL1-3	
- Felinjicering (om krävd DC < 90%)	SIL1-3		
- Felinjicering (om krävd SSF < 90%)		SIL1-3	
- Statistisk testning	SIL3		
- ”Värsta fallet”-testning	SIL3	SIL1-3	
- Användarerfarenhet	SIL1-3	SIL1-3	
- Failure-analys:			
- Fault-tree analysis (FTA)			PL a-e
- Event-tree analysis (ETA)			PL a-e
- Failure Modes and Effects Analysis (FMEA)			PL a-e
- Failure Modes, Effects and Criticality Analysis (FMECA)			PL a-e
Felinjicering (i simulering eller i riktig hårdvara eller protoyp) för att validera category			PL a-e

7.3.5 Tekniker för att undvika fel under användning och underhåll

När det gäller användning och underhåll är det egentligen bara [61508-2] som ställer krav relaterade till dessa. Skälet är att dessa livscykelfaser inte omfattas i [13849-1] och [62061]. Trots detta finns det enskilda krav som rör användarvänlighet och manualer i dessa två standarder.

Tabell 11: Jämförelse av tekniker för att undvika fel under användning och underhåll

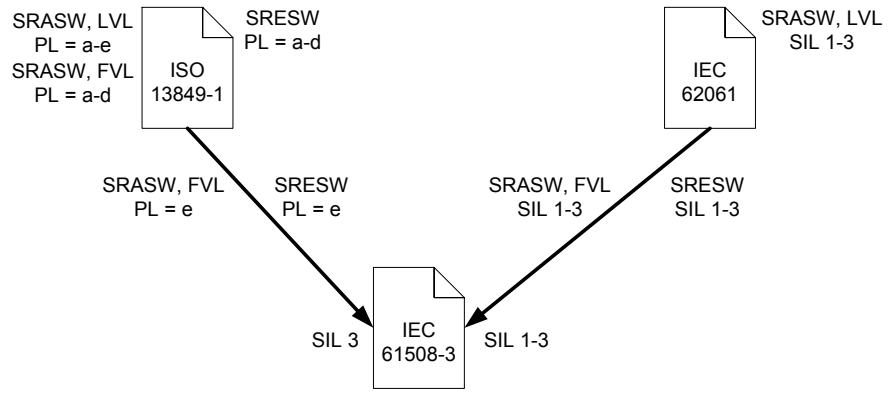
Krav	61508	62061	13849
Användnings- och underhållsmanualer	SIL1-3		PL a-e
Användarvänlighet	SIL1-3	SIL1-3	
Lätt att underhålla	SIL1-3		
Projektledning	SIL1-3		
Dokumentation	SIL1-3		
- Begränsade användningsfall	SIL2-3		
- Skydd mot användarmisstag	SIL2-3		
- Användning av utbildade operatörer	SIL2-3		

8 Säkerhetskritisk programvara

I [61508-3] kan man läsa att säkerhetskritisk programvara förutom applikationsprogramvara även inkluderar operativsystem, systemprogramvara, programvara i kommunikationsnätverk, funktioner för användargränssnitt, supportverktyg samt firmware. Liksom för hela det säkerhetskritiska systemet finns en livscykel för att uppnå säkerhet i programvaran.

I både [62061] och [13849-1] skiljer man på inbyggd (embedded) programvara (firmware) och applikationsprogramvara. Båda standarderna kräver att det finns en livscykel för att uppnå säkerhet i programvaran. I dessa två standarder delar man vidare upp applikationsprogramvaran i två kategorier: FVL[2] och LVL[3]. I [62061] hänvisas man till [61508-3] för FVL. För LVL finns ingen tydlig skillnad mellan SIL-nivåer men vid högre SIL skall tekniker och metoder appliceras och genomföras på ett mer rigoröst sätt. I [13849-1] är det lite mer komplicerarat. För embedded med PL e och FVL applikationsprogramvara med PL e skall [61508-3] SIL3 användas. I alla andra fall kan [13849-1] användas.

Hur de olika standarderna hänger ihop beskrivs i Figur 20.



Figur 20: Relation mellan standarder för utveckling av säkerhetskritisk programvara

[2] FVL (Full Variability Language): assembler, C, ADA, etc.
[3] LVL (Limited Variability Language): ladderdiagram, funktionsblocksdiagram

8.1 Kvalitetsstyrning

Förutom de med den övergripande livscykeln gemensamma kraven på bland annat dokumentation, oberoende granskning med mera, så ställs det specifika krav på versions- och konfigurationshantering. Analys- och kravdokument, specifikations- och konstruktionsdokument, källkodsfiler och bibliotek, testplaner och resultat samt verktyg och utvecklingsmiljöer som används för att skapa, testa eller på andra sätt påverka den säkerhetskritiska programvaran skall vara unikt identifierbara. För att förhindra obehöriga ändringar ska det även finnas procedurer för ändringskontroll.

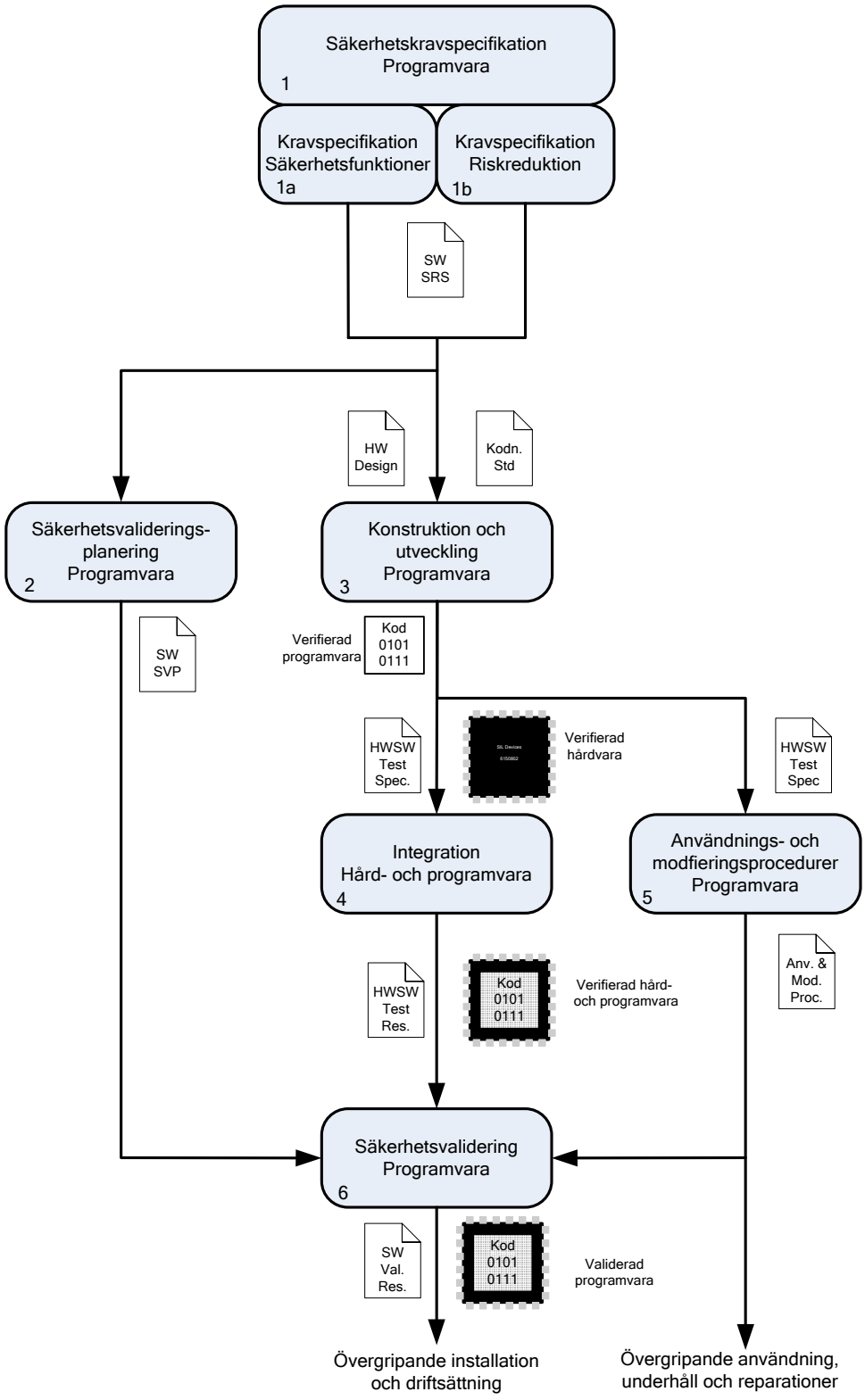
8.2 Livscykel för programvaran

Figur 21 visar [61508-3] livscykeln för att uppnå säkerhet i programvaran. Utlämnat från figuren är interaktionen med livscykeln för hårdvaran. Oavsett vald standard krävs det att man upprättar en livscykel för programvaran.

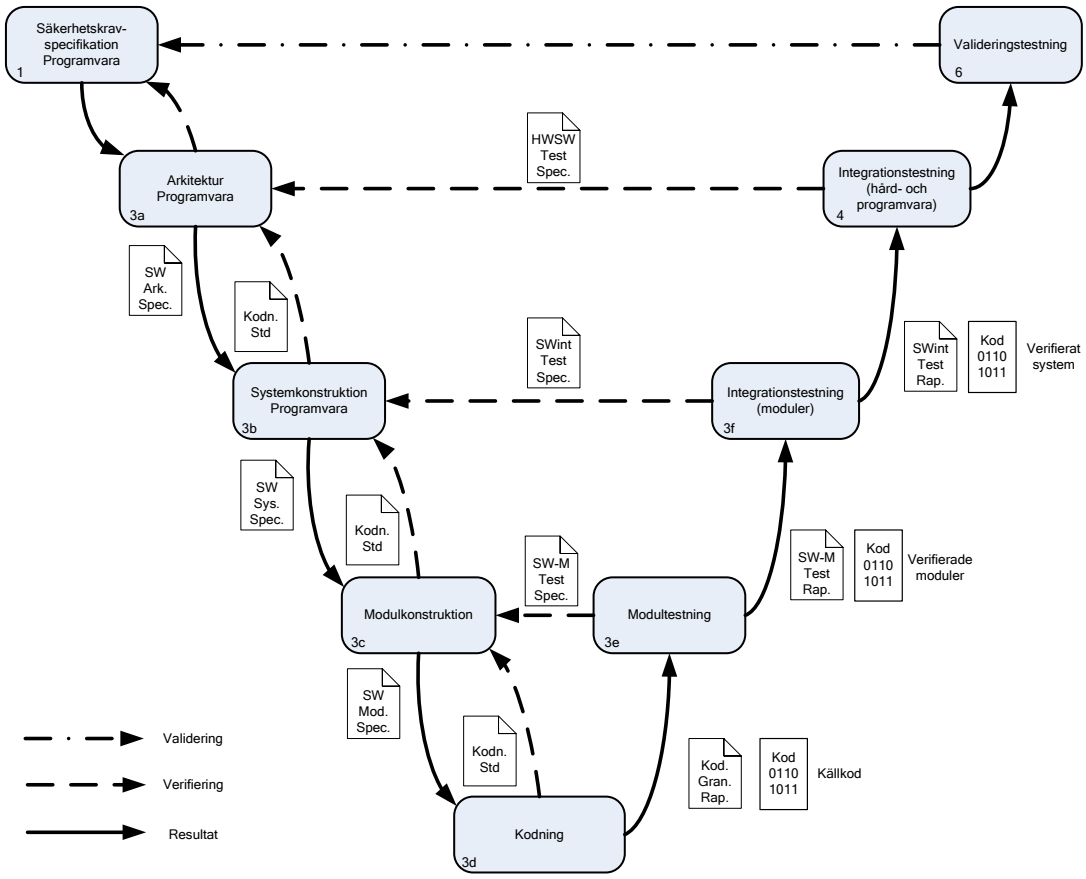
För varje steg, eller fas, i livscykeln behövs erfordrad information. Det kan vara konstruktionsdokument, källkodsfiler, hårdvarukomponenter eller en kombination av dessa. Aktiviteterna i en viss fas resulterar i nya dokument samt eventuella programvaru- och hårdvarukomponenter. För varje fas ska man även verifiera att man uppnått rätt resultat.

I Figur 22 visas ett exempel på en utvecklingsprocess (V-modellen) för programvara tagen från [61508-3]. Figur 22 motsvarar innehållet i box 1, 3, 4 och 6 i Figur 21. Utvecklingsprocessen i Figur 22 liknar den livscykel för programvaran som föreslås i [13849-1] med den skillnaden att i [13849-1] har Arkitektur- och Systemkonstruktionsfasen (steg 3a och 3b) slagits samman till en fas och på motsvarande sätt de två integrationsfaserna. I [62061] ges ingen detaljerad bild av något exempel på en livscykel men eftersom den refererar till [61508-3] så gäller dess livscykel.

Här följer nu en kortfattad och övergripande genomgång av vilka aktiviteter man förväntas genomföra i de olika faserna i livscykeln. Faserna följer uppdelningen enligt [13849-1] och visar på vilka typer av krav de olika standarderna ställer i de olika faserna. Verifikationsaktiviteter som genomförs i samband med alla faser behandlas separat. För Performance Level e i [13849-1] gäller att man följer SIL 3 i 61508 för alla livscykelfaser.



Figur 21: Exempel på livscykel för programvara (IEC 61508)



Figur 22: Exempel på utvecklingsprocess för programvara (V-modellen).

8.3 Specifikation av mjukvarusäkerhetskrav

Kraven skall härledas från kraven på det programmerbara systemet samt kraven på hårdvaran. Kraven skall vara strukturerade och uttryckta på sådant sätt att de är: tydliga, verifierbara, lätta att underhålla, passande för riskreduceringsnivå, spårbara och otvetydiga. Krav ska tas fram på säkerhetsrelaterade funktioner som rör:

- detektering och hantering av fel i givare, logikenheter, ställdon, och i själva programvaran (självdiagnos).
- realtidsegenskaper
- arkitektur
- on- och off-linetester av säkerhetskritiska funktioner
- gränssnitt mot icke-säkerhetskritiska delar och gränssnitt mellan hård- och programvara
- att applikationen kan nå eller behålla ett säkert tillstånd
- driftsmoder
- periodiska och diagnostiska tester
- dataformat och gränsvärden

Dessutom ska nödvändig riskreduceringsnivå anges för alla ovanstående funktioner där det är lämpligt. Där det passar bör semiformella metoder som till exempel funktionsblocks-, sekvens-, tillstånds- och dataflödesdiagram användas.

Kravspecifikationen ska dokumenteras och granskas.

För varje kategori av tekniker presenteras en tabell där de tekniker som rekommenderas av en viss standard för en viss riskreduceringsnivå presenteras. När det gäller tekniker rekommenderade av 61508 så har både ”Highly Recommended”- och ”Recommended”-tekniker tagits med. Läsaren bör alltså vara observant på att det finns ytterligare en nivåskillnad mellan teknikerna som inte helt framkommer i tabellerna.

En jämförelse mellan kraven från de olika standarderna finns i Tabell 12. Kraven beror på riskreduktionsnivå samt om det är applikations- eller embedded-programvara. Applikationsprogramvaran delas även upp i LVL och FVL. Tom ruta betyder att inget krav finns.

8.4 System- och modulkonstruktion

Programvaran bör vara modulbaserad, lätt att testa och modifiera på ett säkert sätt. Arkitekturen ska vara uppdelad i större delsystem, exempelvis:

- operativsystem
- databaser
- I/O
- kommunikation
- applikationsprogramvara

Varje delsystem delas upp i ett antal moduler där det är möjligt. Man skall även deklarera om delsystemen ska nyutvecklas eller är befintliga, om de har verifierats tidigare, om de är säkerhetsrelaterade och vilken riskreduktionsnivå de har. Vidare skall man välja tekniker för att skydda säkerhetsrelaterat data samt olika felhanteringstekniker som till exempel defensiv och diversifierad programmering samt återhämtningsmekanismer.

Tillräckligt oberoende mellan kritisk och icke-kritisk programvara måste visas annars skall den icke-kritiska utvecklas på samma rigorösa sätt som den kritiska. Den säkerhetskritiska delen av programvaran skall göras så liten som är praktiskt möjligt.

Vidare ska rimlighets- och integritetskontroller göras på data från sensorer eller kommunikationsdata. Där det är möjligt skall välbeprövade funktioner och bibliotek användas.

Där det passar bör semiformella metoder som till exempel funktionsblocks-, sekvens-, tillstånds- och dataflödesdiagram användas.

Ett systemspecifikationsdokument tas fram och granskas och parallellt tas ett testdokument fram för integrationstesterna. Därefter tas modulspecifikationsdokument fram och granskas och parallellt dess testdokument för modultestfasen.

En jämförelse mellan kraven från de olika standarderna finns i Tabell 13.

Tabell 12: Jämförelse av tekniker för att undvika fel under kravspecifikation

Krav	61508 SRESW	62061			13849		
		SRASW		SRESW	SRASW		SRESW
		LVL	FVL		LVL	FVL	
Kravdokument	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
Baserad på Syst. SRS	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Baserad på HW SRS	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Krav ska vara:							
- tydliga	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- verifierbara	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- testbara	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- underhållsbara	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- passande för riskreduktionsnivå	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- spårbara	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- otvetydiga	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Specifikation av:							
- säkerhetskritiska funktioner och deras riskreduktionsnivåer	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- konfigurationer	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- arkitektur	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- realtidskrav	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- gränssnitt	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- driftsmoder	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- diagnostiktester		SIL1-3					
- säkert tillstånd	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- felhantering	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- dataformat och gränsvärden		SIL1-3			PL c-e		
- periodiska tester	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- skydd mot modifiering	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- oberoende mellan icke- och säkerhets-kritiska delar	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
Användning av semiformella metoder i kravspecifikation	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- logikdiagram	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- blockdiagram	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- sekvensdiagram	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- dataflödesdiagram	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- tillståndsmaskiner	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- sanningstabeller	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Granskning av kravspecifikation	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
Användning av datorstödda specifikationsverktyg	SIL1-3		SIL1-3	SIL1-3		PL e	PL e

Tabell 13: Jämförelse av tekniker för att undvika fel under modul- och systemkonstruktion

Krav	61508 SRESW	62061			13849		
		SRASW		SRESW	SRASW		SRESW
		LVL	FVL		LVL	FVL	
Specifikations-dokument	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
Testdokument	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
Användning av semiformella metoder i kravspecifikation	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- logikdiagram	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- blockdiagram	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- sekvensdiagram	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- dataflödesdiagram	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- tillståndsmaskiner	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- sanningstabeller	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Separation mellan icke- och säkerhetskritiska delar	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL c-e	PL c-e
Minimering av säkerhetskritiska delar	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Strukturerad design	SIL1-3		SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
Modulbaserad design	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
- Begränsad modulstorlek	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Abstraktion	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- Begränsat antal parametrar	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- Endast en anrops-punkt och en returpunkt	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Fullt specificerade gränssnitt	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Testbarhet	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Möjlighet till säker modifiering	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Diagnostiktester	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Datorstödd specifikationsverktyg	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Datorstödd utvecklingsmiljö	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Tekniker för att skydda kritiskt data	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
Övervakning av kontrollflöde	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Övervakning av dataflöde	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Felrättande och -upp-täckande koder	SIL1-3		SIL1-3			PL e	PL e
Återhämtnings-mekanismer	SIL1-3		SIL1-3			PL e	PL e
Diversifierad programmering	SIL1-3		SIL1-3			PL e	PL e
Formella metoder	SIL2-3		SIL2-3			PL e	PL e
Granskning av spec.	SIL1-3		SIL1-3			PL e	PL e

8.5 Kodning

Koden skall vara läsbar, lätt att förstå samt testbar. Man skall använda kodningsstandarder och utvecklingsverktyg samt programvarukomponenter och moduler som har testats tidigare. Pekare, avbrott samt rekursion skall användas sparsamt. Koden bör vara modulbaserad och strukturerad. Storleken på moduler bör vara begränsad och det bör bara finnas en anropspunkt och en returpunkt i funktioner. Vidare ska säkerhetskritisk programvara separeras från icke-säkerhetskritisk.

Vid utveckling av applikationsprogramvara rekommenderas att man använder grafiska programmeringsspråk som funktionsblocksdiagram och ladder diagram. Man trycker på att använda symboliska variabler istället för explicita minnesadresser. Rimlighets- och integritetskontroller bör göras i applikationsprogramvaran.

Alla säkerhetskritiska källkodsmoduler ska granskas.

En jämförelse mellan kraven från de olika standarderna finns i Tabell 14.

8.6 Modul- och systemtest

Modulerna och systemet skall testas så som specificerades i testspecifikationerna under modul- och systemkonstruktionsfaserna. Testerna ska visa att modulerna och systemet enbart gör det de är avsedda att göra och ingenting annat. Testresultaten skall dokumenteras. Testfallen kan baseras på ekvivalensklasser eller programstrukturen för att minska antalet testfall. Man kan även använda prototyping, simulering och probabilistiska testmetoder.

En jämförelse mellan kraven från de olika standarderna finns i Tabell 15.

8.7 Validering

Syftet med valideringen är att säkerställa att mjukvaran uppfyller alla krav på säkerhet som ställts i specifikationen och att man når upp till krävd riskreduceringsnivå. Det är viktigt att man följer den framtagna valideringsplanen. Resultaten från valideringen skall dokumenteras och åtgärdsplaner vid upptäckta felaktigheter specificeras.

Testning skall vara den huvudsakliga valideringsmetoden. Mjukvaran skall testas med både förväntade data från normal drift så väl som med data som kräver åtgärder från systemet.

Verktyg som används under valideringen skall vara kvalificerade eller på annat sätt vara erkända passande för aktiviteten.

Tabell 14: Jämförelse av tekniker för att undvika fel under kodning

Krav	61508 SRESW	62061			13849		
		SRASW		SRESW	SRASW		SRESW
		LVL	FVL		LVL	FVL	
Kommentering av kod:							
- Ansvarig	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Beskrivning	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Spårbarhet till krav		SIL1-3					
- Spårbarhet till bibl.		SIL1-3					
- In- och utdata	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- Konfiguration	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Läsbar	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
Lätt att förstå	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
Testbar	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
Strukturerad design	SIL1-3		SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
Modulbaserad design	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
- Begränsad modulstorlek	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Abstraktion	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- Begränsat antal parametrar	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- Endast en anropspunkt och en returpunkt	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Fullt specificerade gränssnitt	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Defensiv programmering	SIL2-3		SIL2-3	SIL2-3	PL c-e	PL e	PL e
Kodningsstandard:	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- Inga dynamiska objekt	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- Inga dynamiska variabler	SIL2-3		SIL2-3	SIL2-3		PL e	PL e
- Begränsad användning av avbrott	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- Begränsad användning av pekare	SIL2-3		SIL2-3	SIL2-3		PL e	PL e
- Begränsad användning av rekursion	SIL2-3		SIL2-3	SIL2-3		PL e	PL e
Inga ovillkorliga hopp i högnivåspråk	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Kodgranskning	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Kontrollflödesanalys	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Dataflödesanalys	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Formell verifiering	SIL2-3	SIL2-3	SIL2-3	SIL2-3		PL e	PL e

Tabell 15: Jämförelse av tekniker för att undvika fel under modul- och systemtest

Krav	61508 SRESW	62061			13849		
		SRASW		SRESW	SRASW		SRESW
		LVL	FVL		LVL	FVL	
Testrapport	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL c-e	PL c-e
Funktionstest	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL a-e	PL a-e	PL a-e
- struktur	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- gränsvärden	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- sekvenser		SIL1-3					
- ekvivalensklasser	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Strukturtestning	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Test på gränssnitt	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Prestandatest	SIL1-3		SIL1-3	SIL1-3		PL c-e	PL c-e
Probabilistisk testning	SIL2-3		SIL2-3	SIL2-3		PL e	PL e
Simulering	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL c-e	PL c-e
Symbolisk exekvering	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Prototyping	SIL3		SIL3	SIL3		PL e	PL e
Dataflödesanalys	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Kontrollflödesanalys	SIL1-3		SIL1-3	SIL1-3		PL c-e	PL c-e
Felgissning	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Granskning	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL c-e	PL c-e

8.8 Verifikationsaktiviteter

Enligt 61508 skall verifieringsaktiviteter genomföras efter varje livscykelfas. I de tidiga livscykelfaserna (vänstra benet i v:et) är metoderna statiska som till exempel olika typer av granskning, formell verifiering, data- och kontrollflödesanalys samt symbolisk exekvering. I de senare faserna när kod finns tillgänglig övergår metoderna till dynamiska som till exempel olika typer av testning. Testfall innefattar gränsvärden och ekvivalensklasser.

Alla verifikationsaktiviteter skall dokumenteras och åtgärdsplaner vid upptäckta fel specificeras.

Istället för att upprepa informationen i tidigare tabeller har verifikationsaktiviteter fetstilmarkerats i dessa.

8.9 Verktyg, bibliotek och programspråk

En lämplig uppsättning verktyg innehållande: programspråk, kompilator, versionshanteringsverktyg och eventuellt automatiska testverktyg skall väljas så att man uppnår tillräcklig riskreduceringsnivå.

Programspråket skall ha en kompilator som är certifierad eller vara bedömd som passande för önskad riskreduktionsnivå. Vidare skall språket vara helt och otvetydigt specificerat och passa för applikationen. Språket skall också innehålla stöd för att detektera programmeringsmisstag och dessutom skall det passa för konstruktionsmetodiken.

För detaljer rörande kodningsstandard se Tabell 14.

Tabell 16: Jämförelse av tekniker för att undvika fel p.g.a. verktyg, bibliotek och programspråk

Krav	61508 SRESW	62061			13849		
		SRASW		SRESW	SRASW		SRESW
		LVL	FVL		LVL	FVL	
Programspråk							
- betrott	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e
- passande för applik.	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
- betrodd kompilator	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
- subset	SIL1-3	SIL1-3	SIL1-3	SIL1-3	PL c-e	PL e	PL e
- starkt typat	SIL1-3		SIL1-3	SIL1-3		PL e	PL e
Bibliotek							
- betrodda	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL c-e	PL c-e
Verktyg							
- betrodda	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL c-e	PL c-e
- passande för applik.	SIL1-3	SIL1-3	SIL1-3	SIL1-3		PL e	PL e
Kodningsstandard	SIL1-3		SIL1-3	SIL1-3	PL c-e	PL e	PL e

9 Resultat

Appendix A & B i rapporten förklarar när respektive standard är tillämpbar.

I [13849-1] används begreppet PL för att beskriva kvalitén på de införda säkerhetskritiska funktionerna medan man i [62061] och 61508 använder begreppet SIL. Detta skapar förvirring för företag som kommer i kontakt med både PL och SIL begreppet.

Specifikationen av säkerhetskraven skiljer sig inte så mycket mellan de olika standarderna.

Hårdvarutillförlitlighetsberäkningarna skiljer sig väldigt mycket mellan [62061] och [13849-1], där [62061] tar upp begreppet PFH_d medan [13849-1] tar upp begreppet $MTTF_d$. [62061] bygger huvudsakligen på att man har tillgång till individuella tillförlitlighetsvärden för alla ingående komponenter medan [13849-1] istället huvudsakligen bygger på att alla ingående komponenter skall uppfylla samma säkerhetskategori.

Inte helt oväntat visar tabellerna i kapitel 7 att 61508 ställer fler uttryckliga krav på tekniker som ska användas för att undvika och hantera systematiska hårdvarufel. När det gäller tekniker för att hantera fel från miljöpåverkan syns det tydligt att 13849 och [62061] är mer applikationsnära i och med att de båda pekar ut ett antal tekniker om hur maskiner skall konstrueras, till exempel att maskinerna skall ha positiv verkan.

Som synes i tabellerna i kapitel 8 ställer 61508 flest uttryckliga krav och ISO 13849 minst när det gäller säkerhetskritisk programvara. Om man skall utveckla egna komponenter (SRESW) hamnar man snabbt i IEC 61508 om man inte följer ISO 13849 och har PL a till d. Utvecklar man applikationsprogramvara i ett FVL-språk så räknas det som SRESW. För PL a och b ställs i 13849 väldigt få uttryckliga krav på mjukvaran.

Appendix A: Jämförelse av maskinsäkerhetsstandarder tillämpbara vid konstruktion av den kompletta E/E/PE-baserade säkerhetskritiska funktionen (SS-EN ISO 13849-1:2008 samt SS-EN 62061:2005)

Både [13849-1] och [62061] kan användas vid konstruktion av den kompletta säkerhetskritiska funktionen. Nedan finns ett antal frågeställningar. Svaren på dessa frågeställningar är tänkta att fungera som en hjälp vid val av vilken standard som är lämpligast för olika specifika tillämpningar.

A. Vad ställer köparen av den kompletta maskinen för säkerhetskrav på de ingående säkerhetskritiska funktionerna?
Om man tillverkar en komplett maskin som ska säljas vidare är det viktigt att undersöka vilka krav köparen kan komma att ställa. Kunskapsnivån hos köparen kommer förmodligen att variera. Följande situationer kan uppstå:

- Köparen känner varken till vad PL eller SIL innebär. I detta fall kan man som tillverkare själv avgöra vilken säkerhetsstandard man vill tillämpa.
- Köparen kräver att de säkerhetskritiska funktionerna skall uppfylla en viss PL . I detta fall innebär det att man måste tillämpa [13849-1]
- Köparen kräver att säkerhetskritiska funktionen skall uppfylla en viss SIL. I detta fall innebär det att man måste tillämpa [62061]

B. Är både maskinsäkerhets- och processäkerhetsrisker förknippade med användning av den kompletta maskinen?
Om användning av den kompletta maskinen omfattas av både maskinsäkerhets- och processäkerhetsrisker kan det vara en fördel att tillämpa [62061] istället för [13849-1] när det gäller maskinsäkerhetsriskerna. Detta beror på att för processäkerhetsriskerna finns enbart en funktionssäkerhetsstandard som är tillämpbar, nämligen IEC 61511, och denna standard är väldigt lik [62061] i upplägg (till exempel bygger båda dessa standarder på SIL begreppet).

C. Vilken av standarderna kommer man att referera till i produktstandarder?
Eftersom [13849-1] och [62061] är relativt nya har man ännu inte hunnit införa dessa fullt ut i de olika produktstandarderna. Absolut senast november 2009 måste detta vara genomfört eftersom EN 954-1 utgår då. Båda standardiseringskommittéerna som har arbetat fram [13849-1] och [62061] anser att författarna av produktstandarderna skall möjliggöra användning av båda dessa standarder. Om detta önskemål kommer att tillgodoses i framtida produktstandarder är svårt att bedöma i dagsläget.

D. Vilken typ av system omfattas av de båda olika standarderna?
[62061] omfattar enbart elektromekaniska, elektriska, elektroniska samt programmerbara elektroniska system. [13849-1] omfattar både elektromekaniska, elektriska, elektroniska och programmerbara elektroniska samt även hydraulik, pneumatik och mekaniska system. Då den säkerhetskritiska funktionen i den kompletta maskinen är uppbyggd av en kombination av E/E/PE-system och hydraulik/pneumatik/mekanik kan det vara en fördel att tillämpa [13849-1] eftersom denna standard täcker in alla dessa typer av system. Dock bör poängteras att det givetvis även är möjligt att tillämpa [62061] i detta fall för den

kompletta säkerhetskritiska funktionen. För de delar av systemet som bygger på hydraulik/pneumatik/mekanik är man dock hänvisad till [13849-1].

E. Vilken grad av riskreducering skall man uppnå med säkerhetskritiska funktionen?
I [13849-1] finns definierat 5 olika riskreduceringsnivåer från PL a som ger minst riskreduktion upp till PL e som ger högst riskreduktion. I [13849-1] finns en begränsning som säger att denna standard inte är tillämpbar för säkerhetskritiska funktioner innehållande ”complex electronics” som dessutom skall uppfylla PL e. I detta fall är man hänvisad till att tillämpa [62061].

F. Vad har dessa standarder för koppling till EN 954-1?
[13849-1] har starkast koppling till EN 954-1 eftersom denna standard bygger vidare på kategorierna som finns definierade i EN 954-1 (B, 1, 2, 3 & 4). Om man tidigare har arbetat med EN 954-1 kan det upplevas som en fördel att tillämpa [13849-1] eftersom man känner igen sig med de gamla kategorierna. [62061] har ingen sådan stark koppling till EN 954-1. Däremot finns det en möjlighet att ”lyfta in” komponenter av låg komplexitet utvecklade enligt kraven i ISO 13849-1:1999 (EN 954-1) och ISO 13849-2:2003 (prEN 954-2) som en del av säkerhetskritiska funktionen (för mer information se kapitel 6.7.6.4 & 6.7.8.1.6 i [62061]).

G. Hur påverkar antalet ingående komponenter vilken PL eller SIL man kan uppnå?
Grundtanken i [13849-1] är att man skall kunna identifiera att hela den säkerhetskritiska funktionen skall kunna tilldelas en viss kategori (B, 1, 2, 3, 4) enligt EN 954-1 och när man väl gjort detta kan man räkna sig fram till vilken PL man når genom att bland annat ta hänsyn till parametrar som $MTTF_d$, DC (Diagnostic Coverage) samt CCF (Common Cause Failure). I vissa situationer är det dock inte möjligt att tilldela hela säkerhetskritiska funktionen en viss kategori, till exempel då någon av de ingående komponenterna är inköpta och man enbart vet vilken PL denna komponent uppfyller. I detta fall hänvisas man till tabell 11 i [13849-1]. Nackdelen med denna tabell är att den är något konservativ, till exempel om man har tre ingående komponenter som uppfyller PL c så säger denna tabell att totala PL för hela säkerhetskritiska funktionen enbart uppfyller PL b.

När det gäller [62061] har man inte samma problem eftersom denna standard bygger på att man kopplar samman olika komponenter (som inte nödvändigtvis behöver vara uppbyggda av samma arkitektur, till exempel kategorierna enligt EN 954-1) och där man känner till dess individuella tillförlitlighetsvärdena, PFH_d (Probability of Dangerous Failure per Hour). Skillnaden jämfört med [13849-1] är alltså att det inte finns någon bestämd övre gräns på antal komponenter som styr vilken SIL man kan uppnå. Erhållen SIL styrs istället av det totala sammanlagda PFH_d värdet för alla ingående komponenter.

H. Kan man lyfta in en E/E/PE-komponent som uppfyller en viss PL enligt 13849-1 som en komponent i 62061?
Nej, när [62061] publicerades 2005 visste man inte om att den dåvarande preliminära utgåvan av 13849-1 skulle komma att bli publicerad och därför kunde man inte referera till [13849-1] överhuvudtaget. Däremot är det möjligt att för komponenter med låg komplexitet, utvecklade utgående från kraven i ISO 13849-1:1999 (EN 954-1) och ISO 13849-2:2003 (prEN 954-1), ”lyfta in” dessa som en del av den säkerhetskritiska funktionen om kraven under punkt F ovan är uppfyllda.

I. Kan man lyfta in en E/E/PE-komponent som uppfyller en viss SIL enligt IEC 61508 som en komponent i 13849-1?
Ja, däremot framgår det inte tydligt var i standarden man hittar denna koppling

J. Vad gäller vid inköp av E/E/PE-komponenter? Är det vanligast att dessa komponenter är klassade mot en viss SIL enligt IEC 61508 eller en viss PL enligt 13849-1?
Hittills har det varit vanligast att komponenter är klassade enligt IEC 61508 beroende på att denna standard har varit publicerad ända sedan 1998 medan [13849-1] publicerades först i år. Fler och fler tillverkare väljer dock att bli certifierade mot båda standarderna.

K. Hur omfattande är kraven i respektive standard?
Omfattningen av [13849-1] respektive [62061] är jämförbar, d.v.s det finns ingen direkt anledning att välja en specifik standard av dessa enbart för att den skulle vara enklare.

Appendix B: Jämförelse av funktionssäkerhets-standarder tillämpbara vid konstruktion av individuella E/E/PE-baserade delsystem (SS-EN 61508:2002 och SS-EN ISO 13849-1:2008)

Både [13849-1] och 61508 kan användas vid konstruktion av individuella delsystem baserade på E/E/PE. Svaren på frågeställningarna nedan är tänkta att fungera som en hjälp vid val av vilken standard som är lämpligast för olika specifika tillämpningar.

A. Vad ställer köparen av er komponent för krav?
Om man tillverkar en individuell komponent är det viktigt att undersöka vilka krav köparen kan komma att ställa. Kunskapsnivån hos köparen kommer förmodligen att variera. Följande situationer kan uppstå:

- Köparen känner varken till vad PL eller SIL innebär. I detta fall kan man som tillverkare själv avgöra vilken säkerhetsstandard man vill tillämpa.
- Köparen kräver att komponenten skall uppfylla en viss PL . I detta fall kan man tillämpa både [13849-1] och 61508.
- Köparen kräver att komponenten skall kunna ingå i en säkerhetskritisk funktion upptill en viss SIL. I detta fall innebär det att man måste tillämpa 61508.

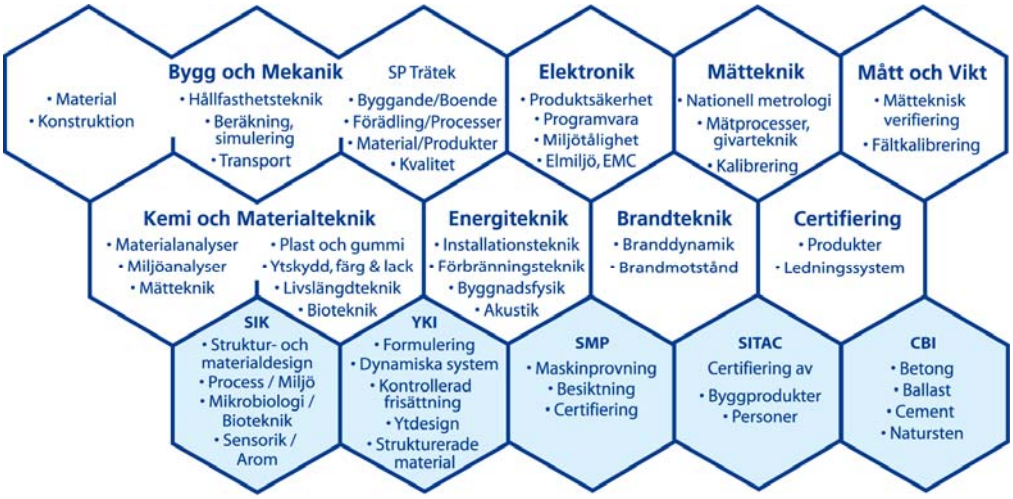
B. Vilken av standarderna kommer man att referera till i produktstandarder?
Eftersom funktionssäkerhetsstandarderna är relativt nya har man ännu inte hunnit införa dessa fullt ut i de olika produktstandarderna. Absolut senast november 2009 måste detta vara genomfört eftersom EN 954-1 utgår då. Båda standardiseringskommittéerna som har arbetat fram [13849-1] och [62061] (vilken refererar vidare till 61508 för konstruktion av enskilda E/E/PE-komponenter) anser att författarna av produktstandarderna skall möjliggöra användning av båda dessa standarder. Om detta önskemål kommer att tillgodoses i framtida produktstandarder är svårt att bedöma i dagsläget.

C. Vilken grad av riskreducering ställs på den enskilda komponenten?
I [13849-1] finns definierat 5 olika riskreduceringsnivåer från PL a som ger minst riskreduktion upp till PL e som ger högst riskreduktion. I [13849-1] finns det en begränsning som säger att denna standard inte är tillämpbar för konstruktion av komponenter baserade på *complex electronics* och som dessutom skall uppfylla PL e. I detta fall är man hänvisad till att tillämpa IEC 61508.

D. Vad har dessa standarder för koppling till EN 954-1?
[13849-1] har starkast koppling till EN 954-1 eftersom denna standard bygger vidare på kategorierna som finns definierade i EN 954-1 (B, 1, 2, 3 & 4). Om man tidigare har arbetat med EN 954-1 kan det upplevas som en fördel att tillämpa [13849-1] eftersom man känner igen sig med de gamla kategorierna. 61508 har ingen som helst koppling till EN 954-1.

E. Hur omfattande är kraven i respektive standard?
61508 är en mer omfattande standard som ställer hårdare krav vid konstruktion av E/E/PE-komponenter jämfört med [13849-1]. Vid konstruktion av en PE komponent som skall uppfylla PL e så refererar dock [13849-1] helt och hållet till [61508-3] då det gäller krav på mjukvarukonstruktionen.

SP Sveriges Tekniska Forskningsinstitut utvecklar och förmedlar teknik för näringslivets utveckling och konkurrenskraft och för säkerhet, hållbar tillväxt och god miljö i samhället. Vi har Sveriges bredaste och mest kvalificerade resurser för teknisk utvärdering, mätteknik, forskning och utveckling. Vår forskning sker i nära samverkan med högskola, universitet och internationella kolleger. Vi är ca 870 medarbetare som bygger våra tjänster på kompetens, effektivitet, opartiskhet och internationell acceptans.



SP är organiserat i åtta tekniska enheter och fem dotterbolag.

SP Sveriges Tekniska Forskningsinstitut
Box 857, 501 15 BORÅS
Telefon: 010-516 50 00, Telefax: 033-13 55 02
E-post: info@sp.se, Internet: www.sp.se
www.sp.se

Elektronik
SP Rapport 2009:03
ISBN 978-91-85829-74-3
ISSN 0284-5172