SÄKERHET OCH TRANSPORT
ELEKTRIFIERING OCH PÅLITLIGHET

Guide gällande dokumentationskrav för EN ISO 13849

Kristian Flink, Andreas Söderberg, Johan Hedberg

RISE rapport 2020:12

Guide gällande dokumentationskrav för EN ISO 13849

Kristian Flink, Andreas Söderberg, Johan Hedberg

Abstract

Guide to documentation requirements for EN ISO 13849

The European Machinery directive gives the requirements for safe machinery, and safe machine control, within the European Union. The European standard EN ISO 13849-1 describes safety-related machine control. This report explains some of the documentation requirements, especially for safety-related machine control systems.

Key words: maskinsäkerhet, CE-märkning, maskinstyrningar, EN ISO 13849

RISE Research Institutes of Sweden AB

RISE rapport 2020:12
ISBN: 978-91-89049-92-5
Borås 2020

Innehåll

Förord

RISE Research Institutes of Sweden är anmält organ för Maskindirektivet. Vi utför tekniska utvärderingar och kan utfärda EG-typgodkännande av säkerhetskomponenter. RISE är också anmält organ för flera andra europeiska direktiv.

SMP Svensk Maskinprovning är en del av RISE. SMP är anmält organ för ett stort antal maskintyper.

Syftet med denna rapport är att vara en hjälp till små och medelstora företag som tillverkar produkter (maskiner och styrsystem) som omfattas av EN ISO 13849. Denna rapport är baserad på många års erfarenheter av projekt inom säkerhetsrelaterade delar av styrsystem. Rapporten ska läsas som vägledning och inte tolkas som krav. RISE tar inget ansvar för bedömningar gjorda utifrån denna rapport. Det är varje tillverkares eget ansvar att finna och tolka de krav som gäller för dennes produkt. Kraven finns i standarden EN ISO 13849.

Standarder skyddas av copyright och kan köpas från SIS (www.sis.se), från ISO (www.iso.org) eller från andra nationella standardiseringsorganisationer. För att förstå en standard behöver läsaren det kompletta dokumentet, och inte bara enstaka citat eller illustrationer som använts i denna rapport.

Sammanfattning

Denna rapport ger en rekommendation för vilka nödvändiga dokument som ska tillhandahållas enligt EN ISO 13849. Rapporten beskriver också ett antal viktiga aspekter som behöver mer detaljerade förklaringar:

- Produktspecifikation
- Projektstyrning, ledningssystem
- Riskanalys
- Teknisk tillverkningsdokumentation
- Specifikation av säkerhetsfunktioner
- Konstruktion av säkerhetsfunktioner
- Validering (inklusive verifiering)
- Användarinformation

1 Beskrivning av EN ISO 13849 för maskinstyrningar

EN ISO 13849–1:2015 och EN ISO 13849–2:2012

Det finns många europeiska standarder inom maskinsäkerhet. För maskiners styrsystem finns standard EN ISO 13849 Maskinsäkerhet – Säkerhetsrelaterade delar av styrsystem. Del 1 av standarden beskriver allmänna konstruktionsprinciper. Del 2 beskriver validering. EN ISO 13849 del 1 och del 2 är B-standarder enligt definitionen i EN ISO 12100. De är vanliga vid utveckling av säkerhetslösningar till maskiner. De kan användas till alla typer av styrsystem (elektriska, elektroniska, pneumatiska, hydrauliska samt mekaniska system) som ska realisera säkerhetsfunktioner.

Del 1: Allmänna konstruktionsprinciper
Syftet med Del 1 är att vara en vägledning till de som konstruerar och bygger säkerhetsrelaterade styrsystem eller säkerhetsfunktioner avsedda för maskiner.

Del 2: Validering
Syftet med Del 2 är att vara en vägledning vid validering av styrsystem eller säkerhetsfunktioner avsedda för maskiner.
Denna Del 2 specificerar vad som ska följas vid validering av SRP/CS genom analys och test av:

- den specificerade säkerhetsfunktionen
- vilken kategori som är uppnådd
- vilken PL nivå som är uppnådd

Det rekommenderas att valideringen utförs av en person som inte har deltagit i utvecklingsarbetet. Valideringen ska dokumenteras och ingå i den tekniska dokumentationen.

1.1 Begrepp som används i SS-EN ISO 13849

SRP/CS

(Safety Related Parts of a Control System) Säkerhetsrelaterad del i ett styrsystem, är de delar av ett styrsystem som ingår i säkerhetsfunktioner. Det kan vara ett komplett styrsystem eller delar av ett styrsystem samt kringutrustning i form av säkerhetskomponenter som ansluts till styrsystemet, för att tillsammans utgöra en komplett säkerhetsfunktion.

Det är utförandet av dessa SRP/CS delar som denna standard inriktar sig på och som om man följer, ger presumtion till de ”grundläggande hälso- och säkerhetskraven” gällande styrsystem i Maskindirektivet.

Erforderlig prestandanivå, PLr
För att kunna utveckla ett styrsystem som ska utgöra en säkerhetsfunktion för en viss riskkälla, så måste man veta vilka krav man ska ställa på styrsystemet, denna erforderliga prestandanivå kallas PLr (required Performance Level).

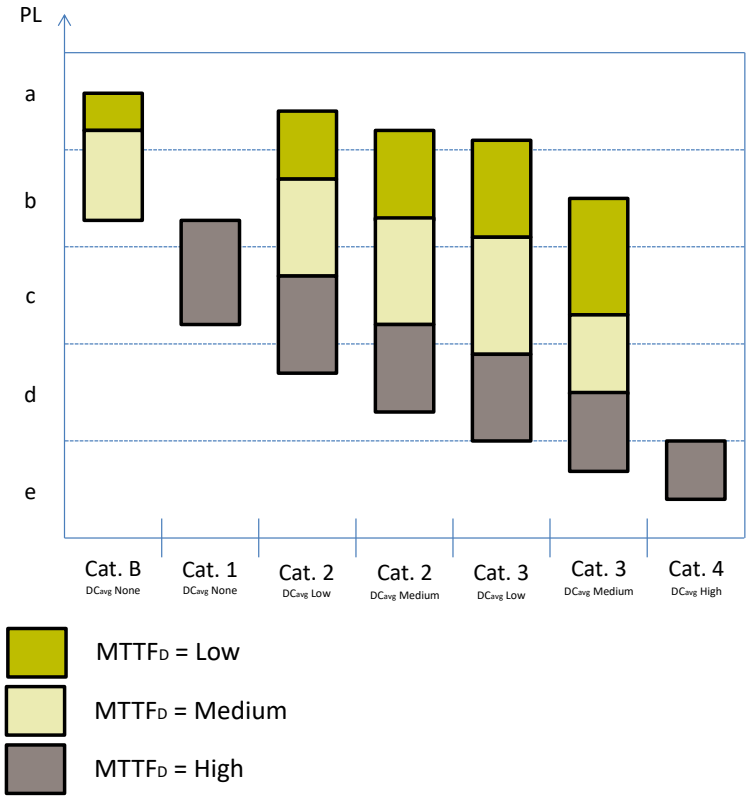
Det finns fem nivåer som beskriver tillförlitligheten på säkerhetsfunktionen. Den lägsta nivån är PL = a och den högsta PL = e.

Det finns olika sätt att fastställa PLr nivån. Det kanske säkraste sättet är att göra en riskbedömning av konstruktionen där man identifierar de riskkällor som maskinen medför och som man sedan gör en riskvärdering på och därigenom får fram en PLr nivå. Det är alltså den PLr nivån som talar om vilka tillförlitlighetskrav som ska ställas på säkerhetsfunktionen. Om man vet exakt vilken maskintyp som styrsystemet är avsett för, så kan det finnas C-standarder som är applicerbara, de kan då innehålla PLr nivåer för de olika säkerhetsfunktioner som är applicerbara. I det fallet så är PLr nivån förbestämd för de riskkällor som är identifierade i C-standarden.

Det kan dock påpekas att Maskindirektivet kräver att man gör en riskanalys även om det finns en C-standard, då det inte finns någon garanti för att en C-standard täcker alla riskkällor för alla varianter av maskiner som ingår i en viss maskintyp.

Prestandanivå, PL
Prestandanivån är ett samlingsbegrepp som i fem nivåer beskriver tillförlitligheten på säkerhetsfunktionen som styrsystemet ska utföra.

Det är flera faktorer inblandade som påverkar prestandanivån, det är hårdvarustrukturen, programvarustruktur, feldetekteringsförmågan (DC), medeltid till farlig felfunktion ($MTTF_D$), fel av samma orsak (CCF), driftsbelastning, miljöaspekter mm.



Figur 1 Prestandanivå från EN ISO 13849–1

Den lägsta nivån är PL = a och den högsta PL = e.

Prestandanivån (PL) är det värde som man beräknar på sin konstruktion för att jämföra med den erforderliga prestandanivån (PLr) för att verifiera att säkerhetsfunktionen är tillräckligt tillförlitlig.

Kategori
För att underlätta konstruktionsarbetet och bedömningen av erforderliga prestandanivå, så har man i denna standard infört begreppet kategori, vilket beskriver strukturen på de säkerhetsrelaterade delarna. Det är förutbestämda strukturer för Ingångssteg – Logik – Utgångssteg i ett styrsystem eller för en komplett säkerhetsfunktion. Dessa strukturer delas in i fem nivåer, som kallas kategori B, 1, 2, 3 och 4 där den lägsta och minst avancerade är kategori B (Basic) och den mest avancerade är kategori 4.

Medeltid till farlig felfunktion, $MTTF_D$ (*Mean Time To dangerous Failure*)
$MTTF_D$ är ett statistiskt värde som beskriver en förväntad medeltid till en farlig felfunktion uppstår.
Den ingår som en del i beräkningen av PL-nivån. För att fastställa $MTTF_D$ värden på de komponenter som ingår i en säkerhetsfunktion ska man i första hand välja komponentleverantörens data. Om detta inte är möjligt så kan man använda de generella värden

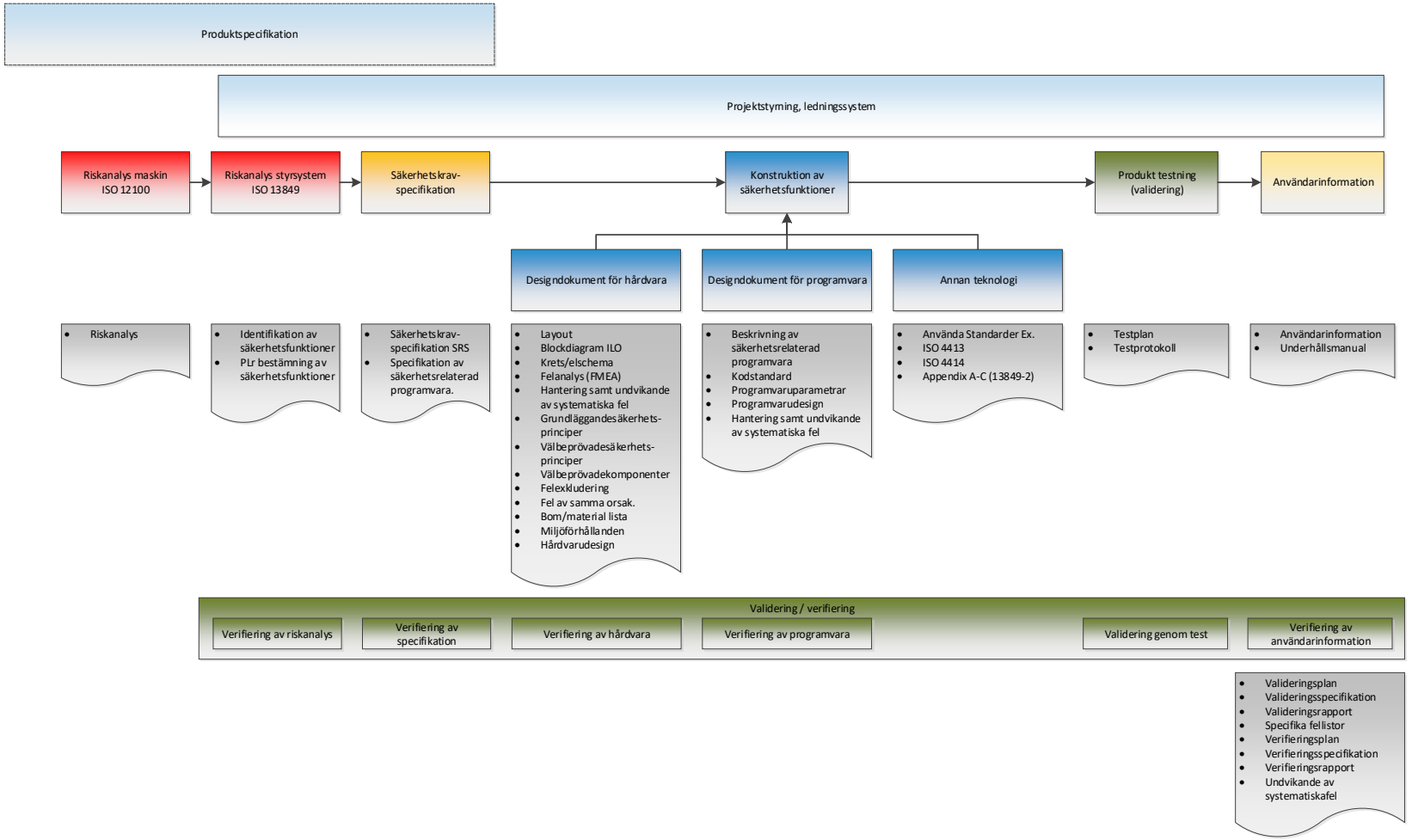
som ges i EN ISO 13849–1 för vissa komponenter, dessa är dock oftast mer konservativa än tillverkarens värden.
Det finns ytterligare metoder för fastställande av $MTTF_D$-värden som beskrivs i standarden.

Feldetekteringsförmåga, DC (*Diagnostic Coverage*)
Förmågan hos ett system att kunna övervaka sig själv och kunna detektera fel, kallas feldetekteringsförmåga. DC värdet anger ett mått på effektiviteten och bestäms som förhållandet mellan felfrekvensen för detekterade fel och felfrekvensen för totala antalet fel.

Fel av samma orsak, CCF (*Common Cause Failure*)
Fel av samma orsak, till exempel fel på gemensam spänningskälla eller miljöstörning
Detta fenomen kan påverka i system som har någon form av redundans, där ett enda fel har förmågan att sätta de redundanta kanalerna ur spel.

Systematiska fel
Ett systematiska fel är ett mänskligt fel eller misstag införd i design- eller tillverkningsprocessen, som endast kan elimineras genom ändring av konstruktionen, tillverkningsprocessen, dokumentationen eller andra relevanta faktorer som beror av mänskligt beteende.

2 Dokumentstruktur



Figur 2 Rekommenderad dokumentstruktur för nödvändiga dokument enligt EN ISO 13849

3 Produktspecifikation

En produktspecifikation är ett dokument som sammanfattar användarens krav på produkten som ska framställas, för att fastställa kvaliteten och att den överensstämmer med vad leverantören ska leverera. Det finns inga krav i EN ISO 13849 att det ska finnas en produktspecifikation, men ändå vill man veta att de säkerhetsfunktioner som konstrueras uppfyller användarens krav.

Maskindirektivet ställer krav på att det ska följa med en bruksanvisning med alla maskiner. Bland annat ska bruksanvisningen ge anvisningar för idrifttagande och användning av maskinen. En väl utförd produktspecifikation kommer att underlätta framtagandet av den bruksanvisning som behövs hos användaren av maskinen eller styrsystemet. EN ISO 13849 täcker inte in bruksanvisningen i sin helhet.

4 Projektstyrning, ledningssystem

4.1 Projektstyrning

Det finns inget krav på projektstyrning i EN ISO 13849, men för att undvika systematiska fel vid exempelvis specifikation, utveckling och integration av säkerhetsrelaterade delar i ett styrsystem (SRP/CS) bör någon typ av projektstyrning ingå. För ytterligare information finns andra funktionssäkerhetsstandarder som kan man titta i där det finns krav i för projektstyrning, till exempel:

- IEC 61508–1
- IEC 62061
- IEC 61511
- ISO 26262–2

4.2 Ledningssystem

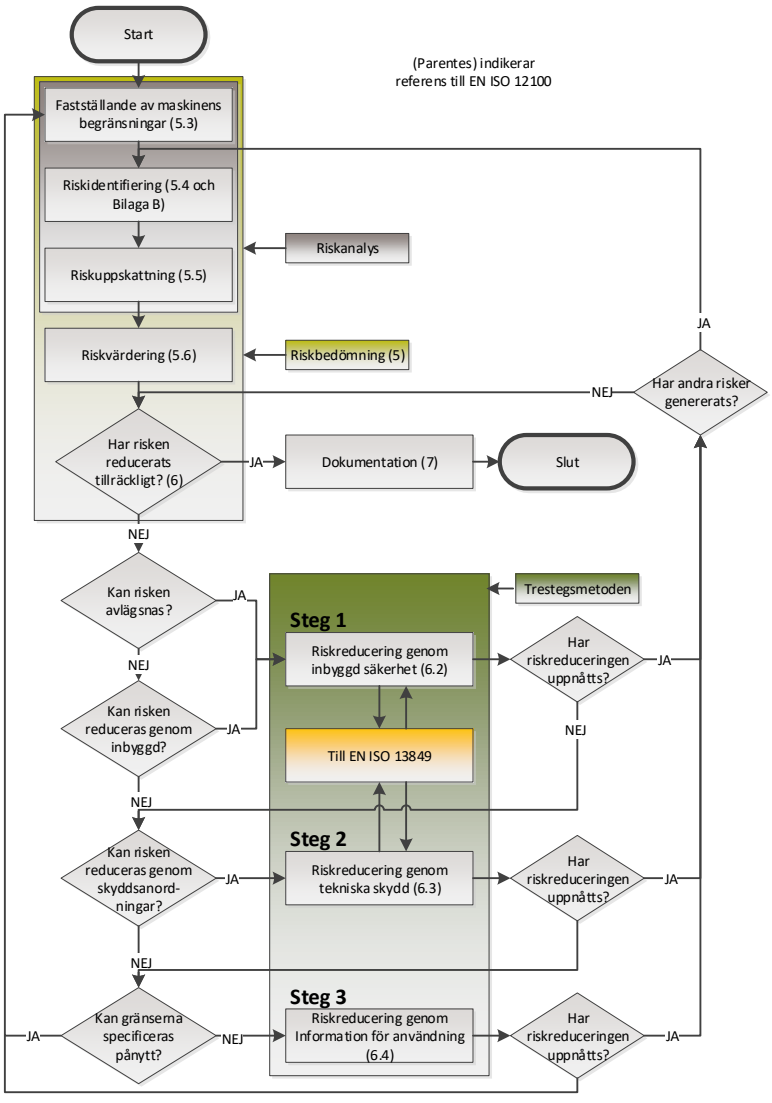
Det finns ett fåtal krav på ledningssystem i EN ISO 13849. Det finns till exempel krav på ledningssystem vid inbyggd programvara av en viss prestandanivå (PL). RISE anser att det blir svårt att tillverka en produkt utan ett bra ledningssystem, till exempel brist på revisionsstyrning (för spårbarhet av krav).

5 Riskanalys

5.1 Riskanalys maskin EN ISO 12100

EN ISO 12100:2010

När en produkt ska tillverkas behöver man identifiera alla eventuella riskkällor som produkten kan vara behäftad med. Detta sker genom att man genomför en riskanalys enligt med EN ISO 12100. Denna riskanalys bör itereras vid flera tillfällen under utvecklingsprocessen, och är alltså ett levande dokument. Riskanalys skall genomföras före konstruktionsstart för att identifiera riskkällor som kan konstrueras bort, och vid andra lämpliga tillfällen under utvecklingsfasen där vetskap om återstående och/eller tillkommande risker bidrar till en bra konstruktion.



Figur 3 Schematisk framställning av riskreduceringsmetod inklusive iterativ trestegsmetod

Information om riskanalys finns bland annat i följande dokument:

- 2006/42/EG Bilaga 1 kap.1
- EN ISO 12100:2010 Hela
- EN ISO 13849–1:2015 kap.4.1, 4.2, 4.3 Annex A
- ISO TR 14121–2:2012 Valda delar

Dokumentationen enligt EN ISO 12100 beskriver det förfarande som har följts, och de resultat som har uppnåtts. Detta omfattar, när så är tillämpligt, dokumentering av;

- den maskin för vilken bedömningen har gjorts (till exempel specifikationer, begränsningar, avsedd användning).
- alla relevanta antaganden som har gjorts (laster, hållfasthet, säkerhetsfaktorer etcetera).
- de riskkällor och riskfyllda situationer som har identifierats och de riskfyllda händelser som beaktats vid bedömningen.
- informationen som riskbedömningen grundar sig på (se EN ISO 12100 avsnitt 5.2).
    - de uppgifter och källor som använts (olyckshistorik, erfarenhet från riskreducering som tillämpats på liknande maskiner etcetera).
    - osäkerheten som finns i samband med de uppgifter som används och deras påverkan på riskbedömningen.
- riskreduceringsmålen, som ska uppnås genom skyddsåtgärder.
- de åtgärder som implementerats med inbyggd säkerhet för att eliminera de identifierade riskkällorna eller för att reducera sannolikheten för de riskfyllda händelserna.
- kvarvarande risker som förknippas med maskinen;
- resultatet av riskbedömningen.
- formulär som fyllts i vid riskbedömningen.

5.2 Riskanalys styrsystem EN ISO 13849

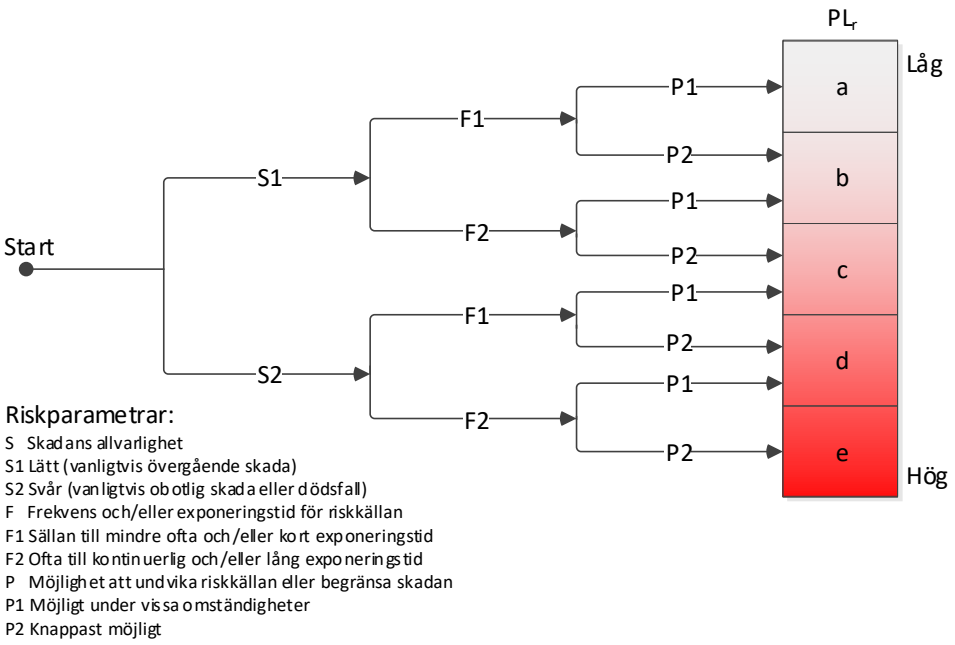
EN ISO 13849–1:2015 Annex A

Med utgångspunkt från att riskbedömningen av maskinen är genomförd enligt EN ISO 12100 (se 3.1), ska man besluta vilken typ och grad av riskreducering som måste uppnås av varje enskild säkerhetsfunktion. Bedömningen utgår från en situation innan den avsedda säkerhetsfunktionen har tillämpats. EN ISO 13849 behandlar den riskreducering som de säkerhetsrelaterade delarna i ett styrsystem bidrar till. I EN ISO 13849–1:2015 annex A hittar man en metod som ger en uppskattning av vilken riskreduceringen som krävs och är avsedd som vägledning för konstruktionen. Metoden har till uppgift att hjälpa till med bedömningen av erforderlig prestandanivå (PLr).

Figur 4 visar en metod som används för att bedöma erforderlig prestandanivå där a = lägsta nivån och e = högsta nivån av riskreducering. För att bedöma den erforderlig prestandanivå finns tre olika parameter. Dessa parametrar är:

- skadans allvarlighet (betecknad med S),
- frekvens och exponeringstid för riskkällan (F), och
- möjlighet att undvika riskkällan eller begränsa skadan (P).

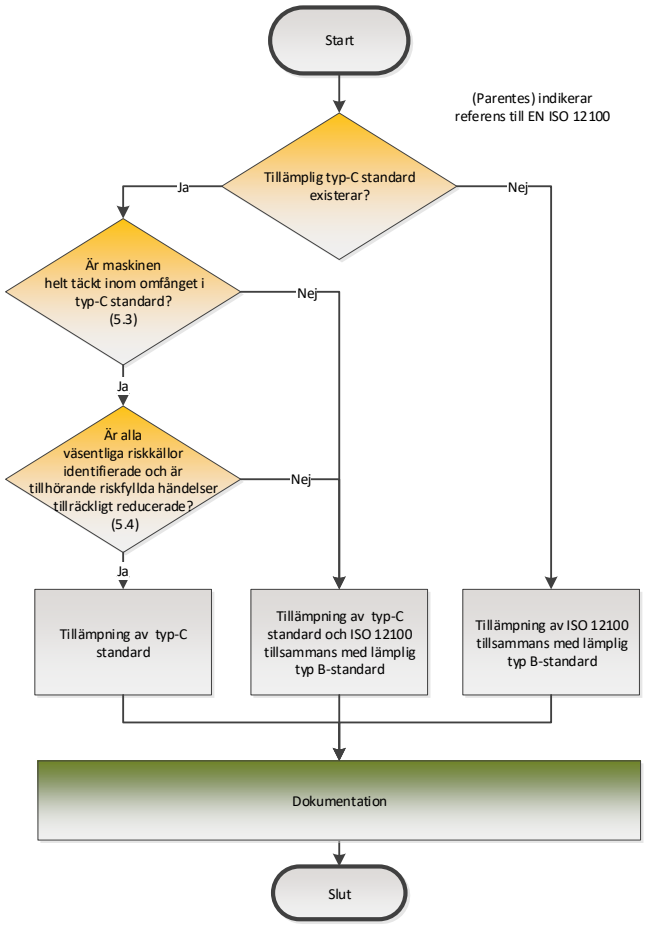
Resultatet av de identifierade säkerhetsfunktionerna och bedömningar av de olika parametrarna för prestandanivån ska dokumenteras.



Figur 4 Riskdiagram för fastställande av erforderlig PLr för säkerhetsfunktion

5.3 Riskanalys från produktstandard

Om en produkt omfattas av en produktstandard (C-standard) kan riskanalyser redan vara genomförd för kända riskkällor som produkten är behäftad med. I de fallen brukar erforderlig prestandanivå (PLr), redan vara bestämd. För dessa risker behöver man inte göra en egen riskanalys. Om eventuella tillkommande risker identifieras, ska man göra en kompletterande riskanalys, se figur 5. För vidare information angående typ-A, typ-B och typ-C standarder, se ISO TR 22100–1.



Figur 5 Praktisk användning av ISO 12100 och befintliga typ-B och typ-C standarder. ISO TR 22100–1

5.4 Verifiering

EN ISO 13849–2: 2012 kapitel 5.1, 7

Vid verifiering ska man utvärdera riskanalysen för att säkerställa korrektheten med avseende på de standarder och krav som tillhandahålls som input.

Verifieringen ska visa att:

– den erforderliga prestandanivån har bedömts på ett lämpligt sätt

Verifieringen bör planeras i en verifieringsplan, specificeras i en verifieringsspecifikation och rapporteras i en verifieringsrapport. Verifieringen bör utföras av personer som är oberoende av framställandet av riskanalysen.

6 Teknisk tillverkningsdokumentation

EN ISO 13849–1 :2015 kapitel 10

Den tekniska tillverkningsdokumentationen ska visa att maskinen överensstämmer med kraven i 2006/42/EG.

EN ISO 13849 täcker den tekniska tillverkningsdokumentationen som beskriver säkerhetsrelaterade delar i ett styrsystem (SRP/CS). När SRP/CS konstrueras ska konstruktören dokumentera minst följande information angående säkerhetsrelaterade delar:

- säkerhetsfunktion (er) som utförs av SRP / CS;
- varje enskild säkerhetsfunktions egenskaper;
- de exakta punkterna där säkerhetsrelaterad(e) del(ar) börjar och slutar;
- omgivningens miljöförhållanden;
- prestandanivån (PL);
- kategorin eller kategorierna som valts;
- parametrar som är relevanta för tillförlitligheten ($MTTF_D$, DC, CCF och livslängd);
- åtgärder mot systematiska fel;
- använd teknik eller teknologier;
- alla beaktade säkerhetsrelevanta feltillstånd;
- motivering till felexkluderingar (se EN ISO 13849–2);
- konstruktionsbeskrivning (till exempel beaktade feltillstånd, felexkluderingar);
- programvarudokumentation;
- åtgärder mot rimligen förutsebar felanvändning.

För information om ”teknisk tillverkningsdokumentation” för den kompletta maskinen se också:
- 2006/42/EG Bilaga 7

7 Specifikation av säkerhetsfunktion

Följande delar för den tekniska tillverkningsdokumentationen ska besvaras i kravdokumenten.

- säkerhetsfunktion (er) som utförs av SRP/CS;
- varje enskild säkerhetsfunktions egenskaper;
- de exakta punkterna där säkerhetsrelaterad(e) del(ar) börjar och slutar;
- omgivningens miljöförhållanden;
- prestandanivån (PL);

7.1 Säkerhetskravspecifikationen (SRS)

EN ISO 13849–1:2015 kapitel 4.2.2, 5

För varje säkerhetsfunktion skall egenskaperna (se avsnitt 5 i EN ISO 13849–1) och erforderlig prestandanivå specificeras och dokumenteras i säkerhetskravspecifikationen (safety requirements specification). Säkerhetskravsspecifikationen är mycket viktig för att undvika misstag vid övergången från riskbedömningen och riskreduceringsprocessen enligt ISO 12100 till SRP/CS design och valideringsprocessen enligt EN ISO 13849–1, speciellt om dessa två processer utförs av olika personer.

Säkerhetskravspecifikationen ska endast innehålla övergripande funktionella krav (med avseende på säkerhetsfunktioner) och inte implementationsdetaljer. Säkerhetskravspecifikationen bör innehålla följande information vilken är nödvändig för att uppnå de säkerhetsåtgärder som krävs av ett styrsystem för den specifika applikationen:

Allmän information om projektet:

- Version, datum, dokumentnamn.
- Termer och definitioner.
- Produktidentifikation.
- Versions- och ändringshistorik.
- Direktiv och/eller standarder som är relevanta.

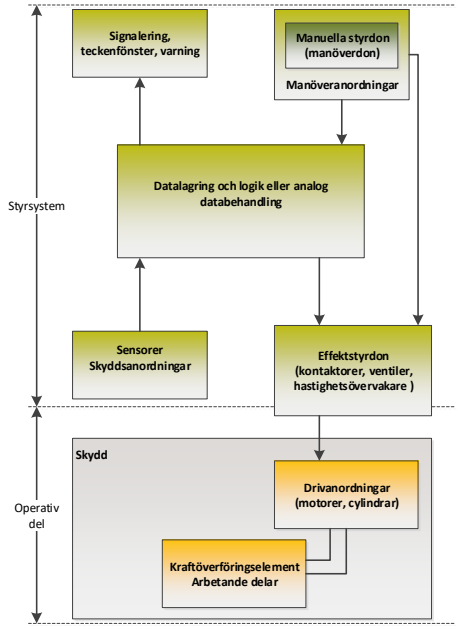
Allmän information om maskinen:

- Beskrivning avsedd användning av maskinen
- Resultat av riskbedömningen för varje enskild fara eller farlig situation, inklusive vilken del av maskinen som genererar fara.
- Rimligen förutsebar felanvändning.
- Maskinensdriftsätt (till exempel lokal drift, automatisk drift, drift av en zon eller del av maskinen.
- Villkor (till exempel driftsätt) för maskinen då säkerhetsfunktionen ska vara aktiv.
- Cykeltid.
- Reaktionstid tills säkert tillstånd (safe state) kan uppnås.
- Nöddrift (Se EN 60204–1 Bilaga E).
- Beskrivning av samverkan mellan olika arbetsprocesser och manuella ingrepp (reparation, inställning, rengöring, felsökning, etcetera).
- Maskinens beteende vid fel/avbrott i kraftförsörjningen.

Information om säkerhetsfunktioner

- Den erforderliga prestandanivån PLr för varje säkerhetsfunktion och källan till denna (riskanalys, C-standard, marknadskrav). Eventuellt även kategori om produkt-standarder anger detta som tilläggs-krav.
- Kort beskrivning / titel på varje säkerhetsfunktion och dess egenskaper implementerad i SRP/CS för att få en tydlig referens. Exempel på titel kan vara med några få ord i text ge en beskrivning av hur den är tänkt att fungera, till exempel om man har ett

inpasseringsskydd till en farlig maskin skulle formuleringen kunna vara: ”Stäng av kraftmatning till motor när dörren öppnas”.
- Unik identifikation (till exempel löpnummer) till varje säkerhetsfunktion/-krav för spårbarhet
- Maskinens beteende som en säkerhetsfunktion är avsedd att förhindra.
- Villkor för att maskinen ska återstarta.
- Initieringshändelsen som aktiverar säkerhetsfunktionen.
- Exakta avgränsningar där säkerhetsfunktionen börjar och slutar.
  Beskrivning: Kombinationen av säkerhetsrelaterade delar i ett styrsystem startar där de säkerhetsrelaterade insignalerna initieras (inklusive exempelvis nockskivan och positionsbrytarens rulle) och slutar vid styrdonens utsignaler (inklusive exempelvis huvudkontakterna på en kontaktor). Se också beskrivning av maskin i figur 6.



Figur 6 Beskrivning av maskin från figur A.1 i ISO 12100

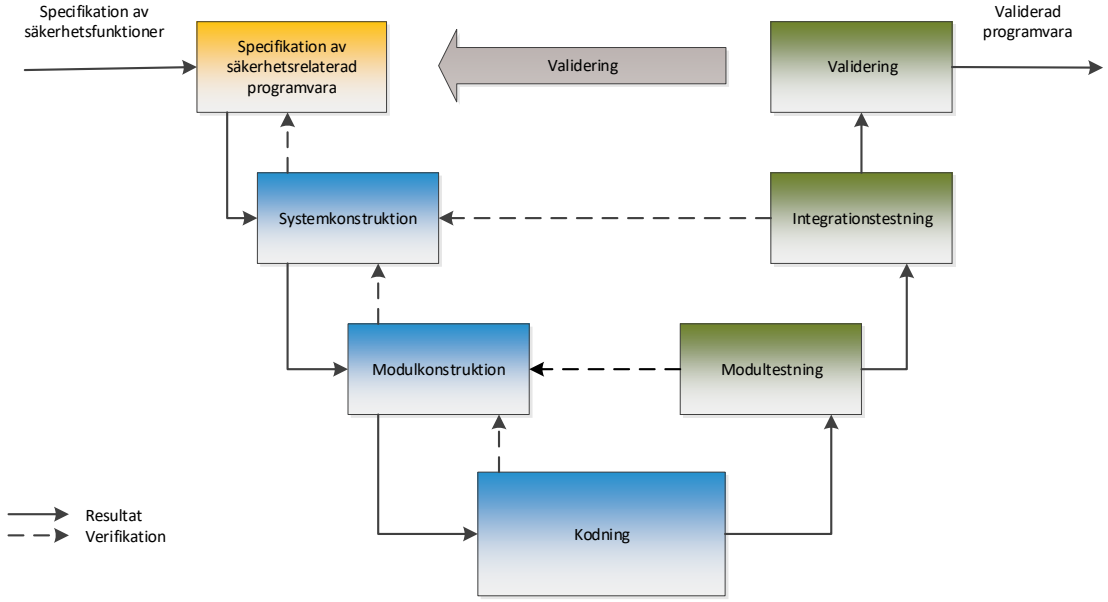
- Vilka delar som ingår som I, L resp. O i säkerhetsfunktionen.
- Reaktionstiden för maskinen att uppnå ett säkert tillstånd efter att initieringshändelsen aktiverat säkerhetsfunktionen, till exempel den totala stopptiden (reaktionstid plus stopptid). Om detta krävs enligt riskbedömningen.
- Behovssfrekvens (Demand rate) för varje säkerhetsfunktion; Se också typ av säkerhetsfunktion (”high demand” eller ”continuous mode) i EN ISO 13849–1:2015 3.1.38.
- Prioritering mellan olika säkerhetsfunktioner som samtidigt kan aktiveras och orsaka motverkande effekter. (till exempel kan flera säkerhetsfunktioner behöva påverka samma styrdon).
- Interface till icke-säkra delar av styrsystemet.
- Ergonomiska aspekter, exempel så att operatören inte är frestad att agera på ett farligt sätt.
- Beskrivning av driftsmiljön. Användningsgränser i förhållande till driftsmiljön (IP-klass, vibration, EMC, osv).
- Eventuella acceptkriterier för validering.

Ovanstående är en icke-uttömmande lista över detaljer för säkerhetsfunktioner som i nästa steg kan implementeras av SRP/CS. Ett SRP/CS kan också innefatta ett eller flera tidigare validerade delsystem. Specifikationen av säkerhetskraven bör verifieras innan konstruktionen påbörjas, eftersom alla andra aktiviteter är baserade på dessa krav. Kontrollen ska säkerställa att alla säkerhets-funktioner är angivna för att uppnå den avsedda riskreduktionen vid maskinen (EN ISO 13849–2 kapitel 7).

7.2 Specifikation av säkerhetsrelaterad programvara

EN ISO 13849–1:2015 kapitel 4.6

Alla livscykelaktiviteter som utförs av säkerhetsrelaterad inbyggd programvara eller applikationsprogramvara ska i förstahand undvika feltillstånd som uppstår under programmets livscykel (se figur 7). Det huvudsakliga målet med de följande kraven är att programvaran ska vara läsbar, begriplig, samt möjlig att testa och underhålla.



Figur 7 Förenklad V-modell av programvarans säkerhetslivscykel

Den första fasen i V-modellen som visas i figur 7 är att utveckla en specifikation av säkerhetsrelaterad programvara. I denna fas är det viktigt att se över säkerhetskravs-specifikationen för varje säkerhetsfunktion för att kontrollera vilka av dessa krav som påverkar eller behöver beskrivas närmare i specifikationen av säkerhetsrelaterad programvara.

Till hjälp finns andra funktionssäkerhetsstandarder för tolkning av kraven, till exempel:
- IEC 61508–2, 3, 7 (Funktionssäkerhet hos elektriska elektroniska och programmerbara elektroniska säkerhetskritiska system)
- ISO 26262–6, 8 (Vägfordon Funktionssäkerhet i el- och elektroniksystem)
- MISRA-C (Motor Industry Software Reliability Association, kodningsstandard för språket C)
- IEC 61131–3 (Programmerbara styrsystem – Programspråk (för applikationsprogramvara)

7.2.1 Specifikation för säkerhetsrelaterad inbyggd programvara (SRESW)

EN ISO 13849–1: 2015 kapitel 4.6.2

Specifikationen av säkerhetsrelaterad inbyggd programvara ska vara tillräckligt detaljerad för att kunna uppnå tillräcklig riskreducering för varje säkerhetsfunktion. Följande skall beaktas:

Information om säkerhetsfunktioner

- Säkerhetsfunktionerna och deras PLr nivåer.
- Eventuella krav i samband med periodisk testning av säkerhetsfunktionen.
- Funktioner som gör det möjligt för systemet att uppnå eller behålla ett säkert tillstånd (safe state).

Information om diagnostik

- Funktioner relaterade till detektering och hantering av fel i hårdvaran (sensorfel och ställdonsfel).
- Funktioner relaterade till detektering och hantering av fel i programvaran (självkontroll i logikdelen).
- Funktioner som gör att programvaran kan modifieras på ett säkert sätt.
- Prestandakriterier (till exempel reaktionstider för diagnostikfunktioner).

Information om gränssnitt

- Gränssnitt till icke-säkerhetsrelaterade funktioner.
- Säkerhetsrelaterad datakommunikation (se 7.4.11 i IEC 61508–2).
- Oberoende krav mellan funktioner.
- Farliga tillstånd som genereras av applikationsprogrammet identifieras och undviks.
- Operatörsgränssnitt och dess användbarhet.

Övrig information

- Säkerhetskrav som implementeras av konfigurationsdata.
- Beskrivning av logik med de ingående modulerna.
- Relevanta driftslägen för applikationen.
- Acceptkriterier för mjukvaruverifiering.
- Referenser till andra dokument.

7.2.2 Specifikation för säkerhetsrelaterad applikationsprogramvara (SRASW)

EN ISO 13849–1: 2015 kapitel 4.6.3

Specifikationen av säkerhetsrelaterad applikationsprogramvara ska vara tillräckligt detaljerad för att kunna uppnå tillräcklig riskreducering för varje säkerhetsfunktion. Följande skall beaktas:

Information om säkerhetsfunktioner

- Säkerhetsfunktionerna och deras PL nivåer.
- Eventuella krav i samband med periodisk testning av säkerhetsfunktionen.
- Funktioner som gör det möjligt för systemet att uppnå eller behålla ett säkert tillstånd (safe state).

Information om diagnostik

- Funktioner relaterade till detektering och hantering av fel i hårdvaran (sensorfel och ställdonsfel).
- Prestandakriterier, till exempel reaktionstider.

Information om gränssnitt

- Gränssnitt till icke-säkerhetsrelaterade funktioner.
- Farliga tillstånd som genereras av applikationsprogrammet identifieras och undviks.
- Operatörsgränssnitt och dess användbarhet.

Övrig information

- Beskrivning av logik med de ingående modulerna
- Relevanta driftslägen för applikationen.
- Acceptkriterier för mjukvaruverifiering.
- Referenser till andra dokument.

7.3 Verifiering

EN ISO 13849–2: 2012 kapitel 7

Vid verifiering ska man analysera specifikationerna för att säkerställa korrektheten med avseende på de standarder och krav som tillhandahålls som input. Specifikationerna bör analyseras innan designen påbörjas, eftersom alla andra aktiviteter är baserade på dessa krav. Verifieringen ska säkerställa att alla säkerhetsfunktioner är specificerade för att uppnå den avsedda riskreduceringen på maskinen.

Verifieringen ska visa att:

- krav för alla säkerhetsfunktioner i maskinens styrsystem är dokumenterade
- lämpliga åtgärder för att undvika systematiska fel genomförts

Verifieringen bör planeras i en verifieringsplan, specificeras i en verifieringsspecifikation och rapporteras i en verifieringsrapport. Verifieringen bör utföras av personer som är oberoende av framställandet av specifikationerna.

8 Konstruktion av säkerhetsfunktioner

Konstruktionen ska vara designad enligt säkerhetskravspecifikationen. Följande delar av den tekniska tillverkningsdokumentationen ska beskrivas i designdokumenten.

- kategorin eller kategorierna som valts;
- parametrar som är relevanta för tillförlitligheten ($MTTF_D$, DC, CCF och livslängd);
- åtgärder mot systematiska fel;
- använd teknik eller teknologier;
- alla relevanta feltillstånd;
- motivering till felexkluderingar (se EN ISO 13849–2);
- konstruktionsbeskrivning (till exempel beaktade feltillstånd, felexkluderingar);
- programvarudokumentation;
- åtgärder mot rimligen förutsebar felanvändning.

8.1 Designdokument för hårdvara.

Designdokument bör innehålla följande information som är nödvändig för att uppnå de säkerhetsåtgärder som krävs av ett styrsystem för den specifika applikationen och för varje säkerhetsfunktion:

Information om säkerhetsfunktioner

- Beskrivning av den övergripande säkerhetsfunktionen och eventuella delsystem inklusive blockscheman för I-, L, respektive O-delen.
- Definierade prestandanivån (PL).
- Kategorin eller kategorierna som valts enligt EN ISO 13849–1.
- Motivera att de krav som är relevanta för vald kategori är beaktade (se tabell 1 nedan).
- Ev. beskrivning av summering för PL>= PLr vid flera SRP/CS i samma säkerhetsfunktion.
- Beskrivning av reaktionstider för grundsäkerhetsfunktionen.
- Beskrivning av återställning och återstart.
- Vald teknik, (elektronik, pneumatik, hydraulik och/eller mekanik.).
- Åtgärder mot rimligen förutsebar felanvändning.
- Motivering till felexkludering (se EN ISO 13849–2)
- Beskrivning av uppfyllda miljöförhållanden.

Information om diagnostik för säkerhetsfunktionerna (kategori. 2/3/4).

- Beskrivning av diagnostiska funktioner och vald diagnostikteknik i I-, L, respektive O-delen av säkerhetsfunktionen.
- Reaktionstider och periodicitet för vald diagnostik.
- Definiera ett säkert tillstånd (safe state) då man upptäcker farliga fel vid diagnostiskt test. Här kan man behöva definiera att man eventuellt vill ”gå till” olika ”säkra tillstånd” om man upptäcker farliga fel i I-, L, respektive O-delen.

Information om komponenter

- Livslängd på valda komponenter, (EN ISO 13849–1 kap. 4.5.4 anger Mission time).
- Användningsfrekvens, (n_{op}).
- Komponentval, $MTTF_D$ värden.
- Källa till $MTTF_D$ /PFH värden.
- El-, elektronikscheman, komponentlistor.
- Motivering om komponenten anses väl beprövad

Övrig information

- Datablad samt EG-försäkran för inköpta säkerhetsklassade produkter som använts.
- Ev. felanalys (FMEA)
- En layout av maskinen.

Kravlista	Kategori för vilken dokumentation krävs				
	B	1	2	3	4
Grundläggande säkerhetsprinciper	x	x	x	x	x
De förväntade driftspåkänningarna	x	x	x	x	x
Påverkan av bearbetat material	x	x	x	x	x
Prestanda under annan relevant yttre påverkan	x	x	x	x	x
Väl beprövade komponenter	-	x	-	-	-
Väl beprövade säkerhetsprinciper	-	x	x	x	x
Medeltid till farlig felfunktion hos varje kanal ($MTTF_D$)	x	x	x	x	x
Säkerhetsfunktionernas kontrollprocedur(er)	-	-	x	-	-
Feldetekteringsåtgärder som genomförts, inklusive felrespons	-	-	x	x	x
Kontrollintervall, om sådana ar specificerade	-	-	x	x	x
Genomsnittlig feldetekteringsförmåga (DC_{avg})	-	-	x	x	x
Förutsägbara enstaka fel som beaktades i konstruktion en och tillämpad detekteringsmetod	-	-	x	x	x
Fel av samma orsak (CCF) identifierade och hur man kan förhindra dem	-	-	x	x	x
Förutsägbara enstaka fel som exkluderades	-	-	-	x	x
Fel som ska upptäckas	-	-	x	x	x
Hur säkerhetsfunktionen upprätthålls vid varje fel	-	-	-	x	x
Hur säkerhetsfunktionen upprätthålls för var och en av kombinationer av fel	-	-	-	-	x
Åtgärder mot systematiska fel	x	x	x	x	x
Åtgärder mot programvarufel	x	-	x	x	x
x dokumentation krävs - dokumentation krävs inte					

Tabell 1 Dokumentationskrav för kategorier med avseende på prestandanivåer enligt med Tabell 2 i EN ISO 13849–2:2012

Information om grundläggande- och väl beprövade säkerhetsprinciper

- Beskrivning av vidtagna åtgärder för uppfyllande av varje grundläggande- och/eller väl beprövade säkerhetsprincip.
- Motivering om vissa säkerhetsprinciper inte är tillämpningsbara.
- Ovanstående kan med fördel genomföras genom att lägga till en kolumn i den tabell som specificerar säkerhetsprinciperna enligt exemplet i Tabell 2 nedan.

Grundläggande säkerhetsprinciper	**Anmärkningar**	**Infomation** (tillkommande kolumn)
Användning av lämpliga material och adekvat tillverkningssätt	Val av material, tillverkningsmetoder och behandling i förhållande till exempelvis belastning, hållbarhet, elasticitet, friktion, slitage, korrosion, temperatur, ledningsförmåga, dielektrisk motståndskraft.	- Beskrivning av vidtagna åtgärder, eller - Referens till styrkande dokument, eller - Motivering till varför säkerhetsprincipen inte är tillämpningsbar
Korrekt dimensionering och formgivning	Beaktande av exempelvis belastning, töjning, utmattning, ytjämnhet, toleranser och tillverkningssätt.	- Beskrivning av vidtagna åtgärder, eller - Referens till styrkande dokument, eller - Motivering till varför säkerhetsprincipen inte är tillämpningsbar
O s v	O s v	O s v

Tabell 2 Exempel på dokumentation för grundläggande- och väl beprövade säkerhetsprinciper (i detta exempel är gråmarkerade kolumner kopierade från Tabell D.1 i ISO 13849-2:2012. Vitmarkerad kolumn är tillagd information)

Information om åtgärder mot systematiska fel

- Beskrivning av samtliga åtgärder som vidtagits för att hantera (införda-) samt undvika (att införa-) systematiska fel. ISO 13849-1:2016, Bilaga G listar strecksatser med olika aspekter som är lämpliga att ta hänsyn till med avseende på hantering/undvikande av systematiska fel.
- Ovanstående kan med fördel genomföras genom att skapa en tabell som specificerar vidtagna åtgärder för exempelvis aspekterna i ISO 13849-1, Bilaga G enligt exemplet i Tabell 3 nedan.

Bilaga	Åtgärder för att hantera systematiska fel	Vidtagna åtgärder
G.2	- Användning av energibortkopplingsprincipen (viloströmsprincipen) (se ISO 13849-2:2012)	- Beskrivning av vidtagna åtgärder, eller - Referens till styrkande dokument, eller - Motivering till varför åtgärden inte är tillämpningsbar - Motivering till varför annan åtgärd valts än rekommenderad åtgärd i ISO 13849-1:2016
G.2	- Åtgärder för att hantera effekterna av fel och andra konsekvenser som kan uppkomma från någon datakommunikationsprocess (se IEC 61508-2:2010, 7.4.11)	Notera att vissa aspekter kan kräva omfattande dokumentering!
O s v	- O s v	O s v
Bilaga	**Åtgärder för att undvika systematiska fel**	**Vidtagna åtgärder**
G.3	- Granskning av hårdvarans konstruktion (exempelvis genom inspektion eller genomgång)	- Beskrivning av vidtagna åtgärder, eller - Referens till styrkande dokument, eller - Motivering till varför åtgärden inte är tillämpningsbar - Motivering till varför annan åtgärd valts än rekommenderad åtgärd i ISO 13849-1:2016
O s v	- O s v	O s v

Tabell 3 Exempel på dokumentation för åtgärder mot systematiska fel (i detta exempel är gråmarkerade kolumner kopierade från Bilaga G i ISO 13849-1:2016. Vitmarkerad kolumn är tillagd information)

8.1.1 Verifiering

EN ISO 13849–2: 2012 kapitel 9

Vid verifiering ska man testa och utvärdera designen för hårdvara för att säkerställa korrektheten med avseende på de standarder och krav som tillhandahålls som input. I EN ISO 13849–2: 4.1 står det att analysen bör startas så tidigt som möjligt i och parallellt med designprocessen.

Verifieringen ska visa att:

- det finns en korrekt utvärdering av PL, baserat på kategorin, DC_{avg} och $MTTF_D$
- det finns en korrekt utvärdering av PL, baserat på PFH_D och PL / SIL av delsystem
- varje individuell säkerhetsfunktion ska prestandanivån (PL) som uppnåtts av SRP/CS visa att den uppfyller den erforderliga prestandanivån (PLr) enligt säkerhetskravs-specifikationen: PL ≥ PLr.

Verifieringen bör planeras i en verifieringsplan, specificeras i en verifieringsspecifikation och rapporteras i en verifieringsrapport. Verifieringen bör utföras av personer som är oberoende av framställandet av designen.

8.2 Designdokument för programvara (System och modul-konstruktion).

När specifikationen för säkerhetsrelaterad programvara är klar är det möjligt att fortsätta med system- och moduldesignen. Syftet med denna fas är att ge en högnivåbeskrivning av hur programvaran fungerar. Alla aktiviteter ska vara dokumenterade.

8.2.1 Säkerhetsrelaterad inbyggd programvara (SRESW)

EN ISO 13849–1: 2015 kapitel 4.6.2

För komponenter med PLr = a – d ska följande grundläggande åtgärder användas:

- Beskrivning av programvarurelaterad arkitektur
- Beskrivning av säkerhetsrelaterad programvara
- Beskrivning av utvecklingslivscykel (se figur 7).
- Beskrivning hur man styrker att man har modulär och strukturerad konstruktion och kodning.
- Beskrivning av hantering och undvikande av systematiska fel.
- Beskrivning av åtgärder för att ha kontroll över slumpmässiga hårdvarufel
- Beskrivning av programvarubaserade säkerhetsparametrar
- Beskrivning av kodningsstandard (till exempel MISRA-C)

För komponenter med PLr = c eller d ska dessutom följande extra åtgärder användas:

- Beskrivning av vald projektledning och kvalitetssäkringssystem (till exempel IEC 61508 eller ISO 9001)
- Beskrivning av alla relevanta aktiviteter under programvarans säkerhetslivscykel;
- Beskrivning av säkerhets- och konstruktionskraven;
- Beskrivning hur man styrker att man har lämpligt programmeringsspråk och datorbaserade verktyg som är väl beprövade;
- Beskrivning av konstruktions- och kodningsstandard (till exempel MISRA-C);

För komponenter med PLr = e

Komponenter med PLr = e ska överensstämma med IEC 61508–3:2010, kapitel 7, lämplig för SIL 3. När diversitet används i specifikation, konstruktion och kodning för de två kanalerna som används i SRP/CS med kategori 3 eller 4, kan PLr = e uppnås med de ovan nämnda åtgärderna för PLr c eller d.

8.2.2 Säkerhetsrelaterad applikations programvara (SRASW)

EN ISO 13849–1: 2015 kapitel 4.6.3

Kod skriven i programspråk med begränsat språkomfång (LVL), som uppfyller kraven nedan, kan uppnå PL a – e. Om den är skriven i programspråk som inte har begränsat språkomfång (FVL) ska kraven för inbyggd programvara tillämpas och PL a – e kan uppnås.

För komponenter med PLr a – e ska följande grundläggande åtgärder vidtas:

- Beskrivning av programvarurelaterad arkitektur
- Beskrivning av säkerhetsrelaterad programvara
- Beskrivning av utvecklingslivscykel (se figur 7)
- Beskrivning av programmeringsverktyg/programspråk
- Beskrivning hur man styrker att man har modulär och strukturerad programmering;

- Beskrivning av programvarubaserade säkerhetsparametrar

För komponenter med PLr från c – e

För komponenter med PLr från c – e krävs eller rekommenderas följande extra åtgärder med ökande effektivitet (lägre effektivitet för PLr = c, medelhög effektivitet för PLr = d, högre effektivitet för PLr = e).

- Beskrivning av val av verktyg, bibliotek, språk:
- Beskrivning av programvarukonstruktionen och den ska omfatta:
    1). semiformella metoder för att beskriva data och kontrollflöde, till exempel tillståndsdiagram eller programflödesschema,
    2). modulär och strukturerad programmering huvudsakligen realiserad genom funktionsblock från validerade säkerhetsrelaterade funktionsblocksbibliotek,
    3). funktionsblock med minimerad kodlängd,
    4). kodutförande inom funktionsblocken som bör ha en ingångs- och en utgångspunkt,
    5). arkitekturmodell i tre steg, ingångar> logik> utgångar,
    6). tilldelning av en säkerhetsutgång endast till en programdel, och
    7). användning av metoder för detektering av externa felfunktioner och för defensiv programmering inom ingångs-, logik- och utgångsblock som leder till ett säkert tillstånd.
- Beskrivning av programvarurealisering/kodning
- Beskrivning av valt LVL språk (Se IEC 61131-3)

8.2.3 Verifiering

Vid verifiering ska man testa och utvärdera programvaran för att säkerställa korrektheten med avseende på de standarder och krav som tillhandahålls som input.

Verifieringen ska visa att:

- verifiering av programvaruåtgärder är tillräckliga för den angivna PLr för de individuella säkerhetsfunktionerna
- det ska finnas åtgärder och aktiviteter vid programutveckling för att undvika systematiska programvarufel.
- Kodningsverifiering genomförts genom granskning, inspektion, genomgång eller andra lämpliga aktiviteter. Verifiering bör också genomföras genom kontroll och dataflödesanalys (för SRAFS endast på PL = d eller e).

Följande kompletterande verifieringsåtgärder ska användas för programvarubaserad parametrisering:
- verifiering av korrekta inställningar för varje säkerhetsrelaterad parameter (minimum, maximum och representativa värden);
- verifiering av att de säkerhetsrelaterade parametrarna har kontrollerats vara rimliga, till exempel genom inmatning av ogiltiga värden etc.;
- verifiering av att obehöriga ändringar av säkerhetsrelaterade parametrar är förhindrade;
- verifiering av att data/signaler för parametrisering har genererats och behandlats på ett sätt som gör att feltillstånd inte kan leda till förlust av säkerhetsfunktionen.

Verifieringen bör planeras i en verifieringsplan, specificeras i en verifieringsspecifikation och rapporteras i en verifieringsrapport. Verifieringen bör utföras av personer som är oberoende av framställandet av programvaran.

8.3 Annan teknologi

Vid konstruktion av säkerhetsfunktioner så kommer man eventuellt att använda andra standarder som i sin tur ska dokumenteras. Exempel på dessa kan vara:

- ISO 4413 Hydraulik – Allmänna regler och säkerhetskrav för system och deras komponenter
- ISO 4414 Pneumatik - Allmänna regler och säkerhetskrav för system och deras komponenter
- Se även ISO 13849–2 Bilaga A till C.

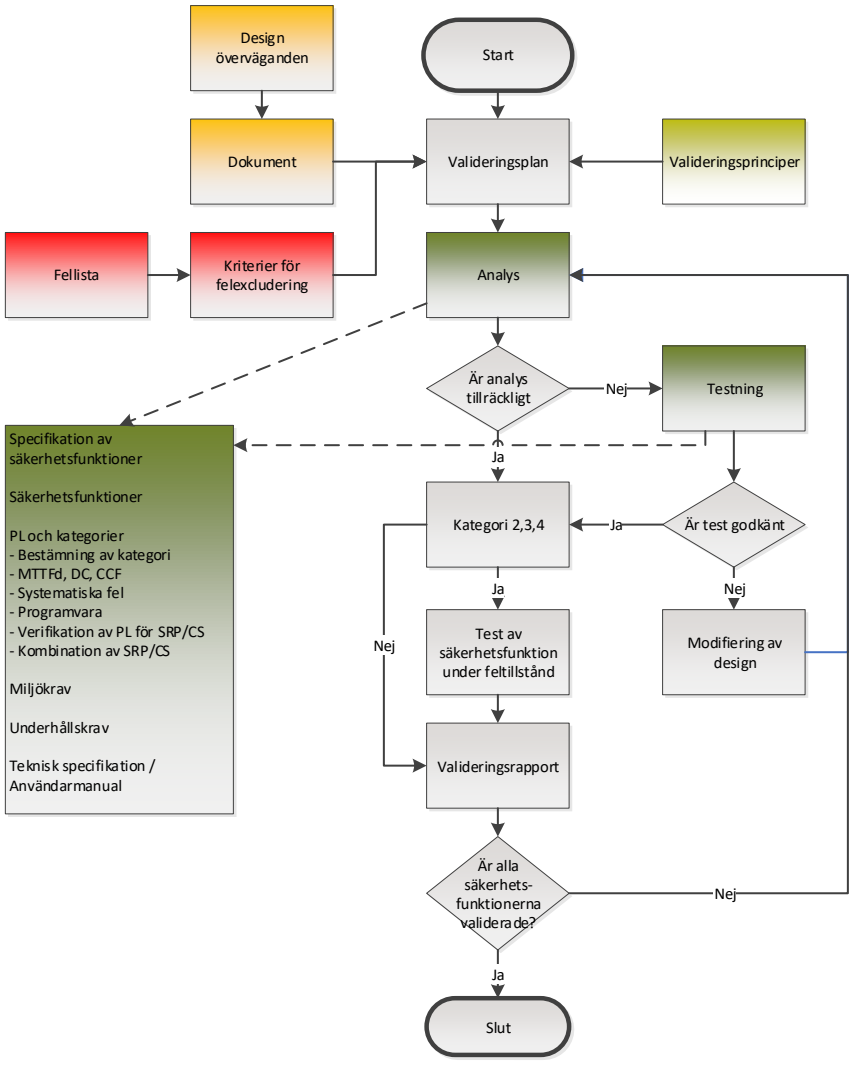
9 Validering (inklusive verifiering)

EN ISO 13849–2:2012

Verifiering – Är valda krav uppfyllda, Dvs följer vi kravspecifikationen och standard?

Validering – Är rätt krav valda för behovet, Dvs kommer den leva upp till beställarens behov?

Syftet med verifieringsprocessen är att bekräfta att utformningen av SRP/CS stöder den övergripande säkerhetskravsspecifikationen för maskinen. Valideringen ska visa att varje SRP/CS uppfyller de krav som den har upphandlats för, där varje krav skall kontrolleras om det är uppfyllt eller inte. Valideringen och verifiering bör utföras av personer som är oberoende av designen av SRP/CS.



Figur 8 Översikt över valideringsprocessen enligt EN ISO 13849–2

Analysen bör startas så tidigt som möjligt och parallellt med designprocessen. Eventuella problem kan sedan korrigeras tidigt i utvecklingsprocessen medan de fortfarande är relativt lätta att korrigera. Analys och test är exempel på verifieringstekniker.

"Modifiering av designen" i figur 8 hänvisar till konstruktionsprocessen. Om valideringen inte kan slutföras är ändringar i designen nödvändiga. Valideringen av de modifierade säkerhetsrelaterade delarna måste sedan upprepas. Denna process upprepas tills alla säkerhetsfunktionerna har validerats. Säkerhetsrelaterade delar som tidigare validerats till

samma specifikation behöver endast en hänvisning till den tidigare valideringen. Validering är ett stort begrepp och kan omfatta både planläggning, specifikation och rapport där resultatet presenteras.

9.1 Valideringsplan

EN ISO 13849–2:2012 kapitel 4.2

Valideringsaktiviteterna ska säkerställa fullständigheten och korrektheten av varje designaktivitet som identifieras i valideringsplanen. En valideringsplan bör skrivas innan testerna startas. Alla krav av betydelse för funktionssäkerheten för SRP/CS måste identifieras, ofta genom att hänvisa till säkerhetskravspecifikationen (SRS). Valideringsplanen ska identifiera och beskriva kraven för att genomföra valideringsprocessen för de angivna säkerhetsfunktioner, deras kategorier och prestandanivåer.

I valideringsplanen där så det är lämpligt bör det anges:

- Identifiering av specifikationsdokumenten
- drifts- och miljöförhållandena under testning
- analyser och tester som ska tillämpas
- referensen till teststandarder som ska tillämpas
- de personer eller parter som ansvarar för varje steg i valideringsprocessen

9.2 Generiska fellistor

EN ISO 13849–2:2012 kapitel 4.3

Valideringsprocessen innebär att SRP/CS: s beteende för alla fel som ska beaktas. En grund för felbedömning ges i tabellerna (Annex A till D) över fellistor:

- Annex A Valideringsverktyg för mekaniska system
- Annex B Valideringsverktyg för pneumatiska system
- Annex C Valideringsverktyg för hydrauliska system
- Annex D Valideringsverktyg för elektriska system
    - Grundläggande säkerhetsprinciper
    - Väl beprövade säkerhetsprinciper
    - Väl beprövade komponenter
    - Fel och felexkluderingar för komponenter

Tabellerna är baserade på erfarenhet och som innehåller:

- de komponenter / element som ska inkluderas, till exempel ledare / kablar

- de fel som ska beaktas, till exempel kortslutningar mellan ledare

- tillåtna felexkluderingar, med hänsyn till miljö-, drifts- och tillämpningsaspekter

- ett avsnitt som anger skälen för felexkludering

9.3 Specifika fellistor

EN ISO 13849–2:2012 kapitel 4.4

Vid behov ska en specifik produktrelaterad fellista genereras som ett referensdokument för valideringsprocessen för den eller de säkerhetsrelaterade delarna. Listan kan baseras på lämpliga generiska listor som finns i bilagorna i EN ISO 13849–2 bilaga A till D. Om den specifika produktrelaterade fellistan är baserad på de generiska listorna ska den ange:

– de fel som tas från de generiska listorna som ska inkluderas
– alla andra relevanta fel som ska inkluderas men inte anges i den generiska listan till exempel fel av samma orsak (CCF)
– de fel som tas från de generella listorna som kan exkluderas på grund av att kriterierna i den generiska listan (se EN ISO 13849–1 7.3) är uppfyllda

Undantagsvis

– andra fel för vilka de generiska listorna inte tillåter exkluderingar, men för vilka motivering och skäl för en exkludering presenteras (se EN ISO 13849–1 7.3)

Om denna lista inte är baserad på de generiska listorna, ska designern ange skälen för felexkludering.

9.4 Valideringsspecifikation

EN ISO 13849–2:2012 kapitel 4.5

Valideringsspecifikation ska bygga på säkerhetskravspecifikationen. Dokument som innehåller tillräcklig information från följande lista bör ingå i valideringsspecifikationen.

- specificering av de nödvändiga egenskaperna för varje säkerhetsfunktion, och dess nödvändiga kategori och prestandanivå;
- ritningar och specifikationer, till exempel för mekaniska, hydrauliska och pneumatiska delar, tryckta kretskort, sammansatta kretskort, intern kabeldragning, kapsling, material, montering;
- blockschema med en funktionell beskrivning av blocken;
- Kretskort, inklusive gränssnitt / anslutningar;
- Funktionsbeskrivning av kretsscheman;
- Tidssekvensdiagram för att växlande komponenter, signaler relevanta för säkerheten;
- Beskrivning av de relevanta egenskaperna hos komponenter som tidigare validerats.
- För säkerhetsrelaterade delar andra än de som anges i ovanstående krav, komponentlistor med produktbeteckningar, nominella värden, toleranser, relevanta driftsspänningar, typbeteckning, felfrekvensdata och komponenttillverkare samt alla andra relevanta säkerhetsuppgifter.
- Analys av alla relevanta fel, som de som anges i tabellerna i EN ISO 13849–2 annex A till D, inklusive motiveringen av eventuella felexkluderingar.
- En analys av påverkan av bearbetat material.
- information för användning, till exempel installations- och bruksanvisning / instruktionshandbok.

Om programvara är relevant för säkerhetsfunktionerna ska programvaru-dokumentationen inkludera:

- en specifikation som är tydlig och som anger prestandan som programvaran skall uppnå,
- bevis på att programvaran är utformad för att uppnå den erforderliga prestandanivån (se EN ISO 13849-2 9.5),
- Detaljer om tester (särskilt testrapporter) som utförts för att bevisa att den nödvändiga säkerhetsprestandan uppnås.

Information som krävs om hur prestandanivån och genomsnittlig sannolikhet för ett farligt fel per timme bestäms. Dokumentationen av de kvantifierbara aspekterna ska omfatta:

- det säkerhetsrelaterade blockschemat (se EN ISO 13849–1 bilaga B) eller designerad arkitektur (se EN ISO 13849-1 6.2)
- bestämningen av $MTTF_D$, DC_{avg}, CCF
- bestämning av kategorin (se tabell 1).

Information krävs för dokumentation om systematiska aspekter av SRP/CS.

Det krävs information om hur kombinationen av flera SRP/CS uppnår en prestandanivå i enlighet med den prestandanivå som krävs (se EN ISO 13849-2 9.7).

9.5 Validering genom analys

EN ISO 13849–2:2012 kapitel 5

Validering av SRP/CS ska utföras genom analys. Indata till analysen inkluderar följande:

- säkerhetsfunktionerna, deras egenskaper och de erforderliga prestandanivåerna identifierade under riskanalysen;
- de kvantifierbara aspekterna ($MTTF_D$, DC_{avg} och CCF)
- systemstrukturen (till exempel designerade arkitekturer)
- de icke-kvantifierbara, kvalitativa aspekterna som påverkar systemets beteende (om tillämpligt, programvaruaspekter)
- deterministiska argument.

9.6 Validering genom testning

EN ISO 13849–2:2012 kapitel 6

När validering genom analys inte är tillräckligt, ska testning utföras för att slutföra valideringen. Testning är alltid ett komplement till analysen och är ofta nödvändigt. Valideringstester ska planeras och implementeras på ett logiskt sätt. Särskilt:

- Ska en testplan tas fram innan testning påbörjas som ska inkludera
  1 testspecifikationerna
  2 det nödvändiga resultatet av testerna för överensstämmelse
  3 testens kronologi

- Testprotokoll ska produceras som inkluderar
  1 namnet på den person som utför testet
  2 miljöförhållandena
  3 testprocedurer och utrustning som används
  4 testdatum
  5 testresultat
  6 Testprotokollen ska jämföras enligt testplanen för att säkerställa att de specificerade funktions- och prestandamålen uppnås.

9.7 Valideringsrapport

EN ISO 13849–2 kapitel 4.6

Validering genom analys och testning ska dokumenteras.

Valideringsrapporten ska visa valideringsprocessen för var och en av säkerhetskraven ihop med resultaten. Om det finns tidigare validerade säkerhetsrelaterade delar kan det räcka med att hänvisa till tidigare utförd validering. En säkerhetskomponent som en säkerhets-PLC kommer att ha en deklaration om överensstämmelse eller ett EG-typgodkännande, som kan användas som ett bevis på tidigare utförda valideringsaktiviteter. För alla säkerhetsrelaterade delar som har misslyckats med en del av valideringsprocessen ska valideringsrapporten beskriva vilka delar i valideringsanalysen / testningen som har misslyckats. Det ska säkerställas att alla säkerhetsrelaterade delar framgångsrikt omvalideras efter modifiering.

10 Användarinformation

EN ISO 13849–1:2015 kapitel 11

Principerna i EN ISO 12100:2010, 6.4.5 och tillämpliga delar av andra relevanta dokument (till exempel EN 60204–1:2005, avsnitt 17) ska tillämpas. I synnerhet ska användaren erhålla den information som är viktig för säker användning av SRP/CS. I den ska minst ingå följande:

- de säkerhetsrelaterade delarnas gränser med avseende på vald(a) kategori(er) och eventuella felexkluderingar.
- för gränserna hos SRP/CS och varje feluteslutning (se EN ISO 13849-1 7.3) ska det, när det är väsentligt för att upprätthålla den valda kategorin eller kategoriernas säkerhetsprestanda, finnas anpassad information (till exempel vid ändring, underhåll och reparation) för att fortsättningsvis säkerställa motiveringen av feluteslutningen(arna).
- effekterna av avvikelser från säkerhetsfunktionen(ernas) specificerade prestanda.
- tydliga beskrivningar av gränssnitten till SRP/CS och skyddsanordningar.
- reaktionstid.
- driftsgränser (inklusive miljöförhållanden).
- indikeringar och larm.
- muting och bortkoppling av säkerhetsfunktioner.
- Körsätt.
- underhåll (se EN ISO 13849–1 kapitel 10.1).
- checklistor för underhåll.
- hur åtkomlighet och utbyte av interna delar underlättas.
- hjälpmedel för lätt och säker felsökning.
- information som förklarar tillämpningarnas relevans för kategorin som hänvisas till.
- kontroll av testintervall där det är relevant.

För ytterligare information se också:
- EN ISO 12100:2010 6.4.5.1
- 2006/42/EG Bilaga 1

10.1 Underhållsmanual

EN ISO 12100:2010 kapitel 6.4.5.1 e.

Information för användningen av SRP/CS ska innehålla instruktioner för underhåll (inklusive regelbunden kontroll) av SRP/CS och ska innehålla minst följande information angående säkerhetsrelaterade delar:

- form och tidsintervall för kontroll av säkerhetsfunktioner;
- uppgifter om reservdelar som ska användas om dessa kan påverka operatörers hälsa och säkerhet;
- anvisningar om underhållsåtgärder som fordrar en viss teknisk kunskap eller särskild utbildning och som därför endast bör utföras av utbildade personer (underhållspersonal, specialister);
- anvisningar om underhåll (till exempel utbyte av delar) vars utförande inte fordrar specifik utbildning och följaktligen kan utföras av användare (till exempel operatörer), och
- ritningar och diagram som möjliggör för underhållspersonal att utföra sina uppgifter rationellt (i synnerhet felsökningsuppgifter);

10.2 Verifiering

EN ISO 13849–2: 2012 kapitel 11, 12

Vid verifiering ska man testa och utvärdera dokumenten för att säkerställa korrektheten med avseende på de standarder och krav som tillhandahålls som input.

Verifieringen ska visa att:

- kraven för den tekniska tillverkningsdokumentationen, användarinformationen och underhållsmanualen är uppfyllda.

Verifieringen bör planeras i en verifieringsplan, specificeras i en verifieringsspecifikation och rapporteras i en verifieringsrapport. Verifieringen bör utföras av personer som är oberoende av framställandet av dokumenten.

Bilaga A

A.1 Referensdokument

Maskindirektivet (2006/42/EG), Svensk version

RISE rapport 2018:02 ”Maskinstyrningar i praktiken

A.2 Standarder

EN ISO 12100:2010	Maskinsäkerhet – Allmänna konstruktionsprinciper – Riskbedömning och riskreducering
EN ISO 13849–1:2015	Maskinsäkerhet - Säkerhetsrelaterade delar av styrsystem - Del 1: Allmänna konstruktionsprinciper
EN ISO 13849–2:2012	Maskinsäkerhet - Säkerhetsrelaterade delar av styrsystem - Del 2: Validering
EN 60204–1:2006	Maskinsäkerhet – Maskiners elutrustning Del 1: Allmänna fordringar
IEC 61508: 2010	Funktionssäkerhet hos elektriska elektroniska och programmerbara elektroniska säkerhetskritiska system
EN 62061: 2005	Maskinsäkerhet - Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska styrsystem
EN 61511: 2017	Funktionssäkerhet - Säkerhetskritiska system för processindustrin
ISO 26262: 2018	Vägfordon - Funktionssäkerhet i el- och elektroniksystem
EN 61131–3: 2013	Programmerbara styrsystem – Del 3: Programspråk
ISO TR 22100–1: 2017	Maskinsäkerhet - Förhållande till ISO 12100 - Del 1: Hur ISO 12100 relaterar till typ-B och typ-C standarder
EN ISO 4413: 2010	Hydraulik – Allmänna regler och säkerhetskrav för system och deras komponenter
EN ISO 4414: 2010	Pneumatik - Allmänna regler och säkerhetskrav för system och deras komponenter
MISRA-C	Motor Industry Software Reliability Association, kodnings-standard för språket C

A.3 Länkar

Europakommissionen ”Maskiner”
http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_sv

Maskindirektivet (2006/42/EG)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042

Europakommissionen ” CE-märkning”
http://ec.europa.eu/growth/single-market/ce-marking_sv

Harmoniserade standarder till Maskindirektivet
https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery_en

SP rapport 2012:21 “Risk Analysis – the key to safe machinery”
http://www.diva-portal.org/smash/get/diva2:962682/FULLTEXT01.pdf

RISE report 2018:01 ”Safety-related Machine Control Systems using standard EN ISO 13849-1”
http://www.diva-portal.org/smash/get/diva2:1178031/FULLTEXT01.pdf

RISE report 2018:02 ”Maskinstyrningar i praktiken”
http://www.diva-portal.org/smash/get/diva2:1180400/FULLTEXT01.pdf

RISE Report 2019:13 “Introduction to Hardware Architecture and Evaluation According to EN ISO 13849–1”
http://www.diva-portal.org/smash/get/diva2:1282544/FULLTEXT01.pdf

Bilaga B Förkortningar

Tabell B.1 Förkortningar

BOM	Stycklista (Bill of materials)
CCF	Fel av samma orsak
DC	Feldetekteringsförmåga
DC_{avg}	Genomsnittlig feldetekteringsförmåga
FMEA	Feleffektanalys
FVL	Programspråk som inte har begränsat språkomfång
I	Ingångsenhet, till exempel givare
L	Logik
LVL	Programspråk med begränsat språkomfång
MTTF	Medeltid till felfunktion
$MTTF_D$	Medeltid till farlig felfunktion
O	Utgångsenhet, till exempel styrdon
PFH_D	Medelfrekvens för farlig felfunktion per timma
PL	Prestandanivå
PLr	Erforderlig prestandanivå
SIL	Säkerhetsintegritetsnivå
SRASW	Säkerhetsrelaterad applikationsprogramvara
SRESW	Säkerhetsrelaterad inbyggd programvara
SRS	Säkerhetskravspecifikation
SRP/CS	Säkerhetsrelaterad del i styrsystem

Through our international collaboration programmes with academia, industry, and the public sector, we ensure the competitiveness of the Swedish business community on an international level and contribute to a sustainable society. Our 2,800 employees support and promote all manner of innovative processes, and our roughly 100 testbeds and demonstration facilities are instrumental in developing the futureproofing of products, technologies, and services. RISE Research Institutes of Sweden is fully owned by the Swedish state.

I internationell samverkan med akademi, näringsliv och offentlig sektor bidrar vi till ett konkurrenskraftigt näringsliv och ett hållbart samhälle. RISE 2 800 medarbetare driver och stöder alla typer av innovationsprocesser. Vi erbjuder ett 100-tal test- och demonstrationsmiljöer för framtidssäkra produkter, tekniker och tjänster. RISE Research Institutes of Sweden ägs av svenska staten.

RISE Research Institutes of Sweden AB
Box 857, 501 15 BORÅS
Telefon: 010-516 50 00
E-post: info@ri.se, Internet: www.ri.se

ELEKTRIFIERING OCH PÅLITLIGHET
RISE rapport 2020:12
ISBN:
978-91-89049-92-5