



A magnifying glass with a black handle and a silver frame, positioned over the word 'MAGNET'.

Föreningen för industriell elteknik

MASKINSÄKERHET

Från historik, analyserad risk - till - validerad åtgärd
vad krävs under vägen som håller vid en marknadskontroll ?



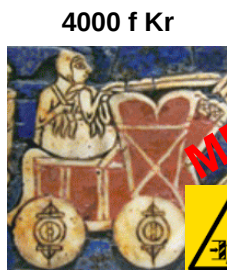
Tomas Beäff
www.mpsa.se
070 6406027



TEKNIKUTVECKLING, TILLSYN OCH RISKER INOM INDUSTRIEN

www.mpsa.se Tomas Beäff

Yrkesfarelagens tillkomst 1889, som trädde i kraft året därpå samtidigt som yrkesinspektionen (numera Arbetsmiljöverket) påbörjade sin tillsyn mot den privata industrin. Ellagen kom 1902 och året därpå, 1903 bildades Statens Elektriska Inspektion, det som senare kom att bli Elsäkerhetsverket.



4000 f Kr

MEKANIKEN



Hjulet uppfanns cirka 4000 f Kr

1642 den första mekaniska räknemaskinen föregångaren till datorn.



1700-tal

ÅNGMASKINER



Den första användbara ångmaskinen byggdes av engelsmannen Thomas Newcomen 1712. De första ångmaskinerna lär ha byggts av greken Heron för 2000 år sedan.

1850-tal



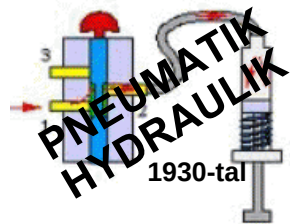
1820 upptäcktes elektromagnetismen sedan även induktionen som ledde fram till elektriciteten

DIODEN



1900-tal

Radion uppfanns 1904, elektronröret (DIODEN) uppfanns 1909 första praktiskt användbara elektroniska förstärkaren och en avgörande komponent i byggandet av långväga telefoni och ljudradio.

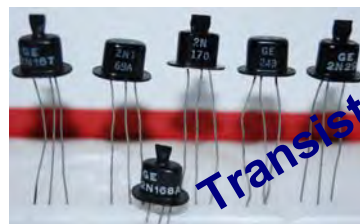


PNEUMATIK HYDRAULIK

1930-tal

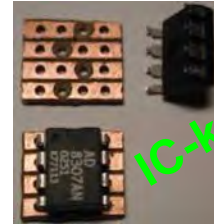
Den tekniska hydrauliken sträcker sig tillbaka till vattenbaserad hydraulik som "uppfanns" 1795. Oljebaserad hydraulik "uppfanns" 1905. Industritillämpning från 1930-talet

1950-tal



Den första transistoren var en JFET transistor byggd med tunnfilmtsteknik. Denna transistor patenterades 1923 1954 utvecklades den första fungerande transistoren baserad på kisel

1950-tal



Nästa stora framsteg kom 1958, då Robert Noyce uppfann den integrerade kretsen

1950-tal



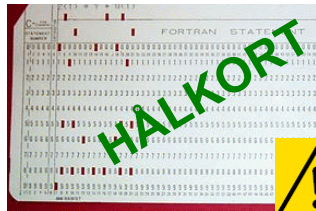
Den första transistorbaserade datorn var TX-0, som utvecklades vid MITs Lincolnlaboratorium med inspiration från det tidigare MIT- 1952.



1960-tal

LASER

Den första användbara lasern gjordes vid Hughes Research Laboratories i Malibu av Theodore Maiman år 1960

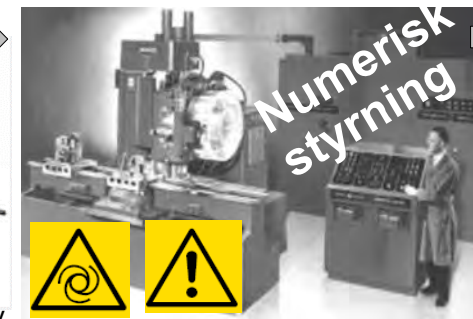


HÅLKORT



Hålkort användes länge för in- och utmatning av data i datorer. Från mitten av 1970-talet började man gå ifrån användningen av hålkort

1960-tal



Numerisk styrning, NS, NC, teknik för elektronisk styrning styrs av program i numerisk form.

Numerisk styrning



1960-tal

En Programmable Logic Controller (PLC) är typ av dator som utformats speciellt för industriella tillämpningar började användas i slutet av 1960-talet

Trådlös överföring, av både energi och kommunikation Tesla ska redan 1891 ha demonstrerat trådlös överföring av el- och kommunikation

2000-tal



TRÅDLÖST

PROCESSER OCH MASKINSTYRNINGAR INOM INDUSTRIEN KAN MEDFÖRA

- Allvarliga personskador eller rent av dödsfall
- Skador på miljön (polluter pay principle)
- Saksador på teknisk utrustning (brand-explosion-haveri etc.)



LEGALA KRAV FINNS I LAGAR-FÖRORDNINGAR, DIREKTIV OCH FÖRESKRIFTER

- Dessa krav bygger helt och hållet på vad som hänt tidigare och är inte framtidskridande (kan ej se in i framtiden)
- Bygger helt och hållet på att arbetsmarknadens parter (arbetsgivaren samt arbetstagare följer och tillämpar dessa krav. Myndigheter kontrollerar och informerar samt sätter upp sanktionssystem och utför marknadskontroller.
- Förr var det nationella Svenska krav som myndigheter utfärdade i föreskrifter utifrån Svenska lagar och förordningar (om än de mesta var taget och omskrivet från Tyska och engelska krav)
- Numer är kraven i huvudsak fastställda av EU inom EU-rätten, främst genom direktiv och bygger på att varje medlemsland inför dessa direktiv via nationell lagstiftning vilket huvudsakligen sker i form av föreskrifter som anger övergripande mål och formella krav.



KRAV INFÖRDES I SLUTET AV 1800-TALET med anledningen av industrialiseringen.

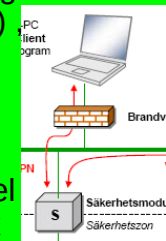
TEKNISKA LÖSNINGAR FÖR ATT PÅ DETALJNIVÅ UPPFYLLA DE FORMELLA KRAVEN ÅTERFINNS FRÄMST I HARMONISERADE STANDARDER

- Grundtanken med EU:s inre marknad är att varor, tjänster, kapital och personer ska kunna röra sig fritt över nationsgränserna utan handelshinder. Rörligheten underlättas genom att EU-ländernas produktregler harmoniseras och specificeras av gemensamma europeiska standarder.



HISTORIK TILL NUTID

- **Härdförtrådan teknik.** Historiskt sett ur ett säkerhetsperspektiv har man härdförtrådat säkerhetsrelaterade styrningar i maskiner
- **Tillförlitliga komponenter.** Övergång till användandet av mera tillförlitliga komponenter så kallade säkerhetskomponenter typ säkerhetsrelän och tvångsstyrda förreglingsbrytare höjde sedan nivån ytterligare, i dessa kretslösningar
- **Redundans.** Mera riskfyllda styrfunktioner krävde även någon form av övervakning för att ha koll på när felen uppträder ofta i kombination med dubblering för att klara enkelfel typ svetsning av kontaktfunktioner, kortslutningar med mera. Infördes på pressar i slutet av 1970 talet via då i krav i nya pressföreskrifter. Var dock huvudsakligen analoga funktioner.
- **Riskkategorisering av säkerhetsfunktioner.** I efterdyningarna till EU:s maskindirektiv 89/392/EG infördes 1992 en B-standard i form av EN 954-1 där man införde krav på kretsuppbyggnad i olika kategorier utifrån aktuell riskbild där kategorierna var B (enkanaliga med std komponenter), 1, (härdförtrådade med väl beprövade komponenter) 2, (en kanaliga kretsar med övervakning) 3 (redundanta kretsar) 4 (redundans med övervakning)
- **Felsäkra styrsystem med felsäkra undersystem, säkra busstyrningar.** I efterdyningarna till maskindirektiv 2006/42/EG infördes med tillämpning från 2013 en rad nya standarder för att tillmötesgå de ökade kraven på hård- och mjukvara då man med tiden mer och mer gått över till kretslösningar baserade på programmerbar elektronisk utrustning.
- En mängd variabler skall beaktas och kretsarna skall PL eller SIL-klassas. Validerad tillförlitlighet i komponenter är en viktigt variabel tillsammans med krav på mjukvaran. Kretsar och komponenter klassas i PL a-b-c-d-e eller SIL 1,2,3 inom industrin beroende på risk



STRUKTUR REGELVERK EU-EES-OMNRÅDET



EG-Direktiv



Lag



Förordning



Föreskrift

MINIMIDIREKTIV

ARBETSGIVARENS
SKYLDIGHETER

EU: direktivens lägsta
krav får ej underskridas
däremot överskridas

Vissa områden är även
dispositiva / t.ex
arbetstidsregler)

Omfattar 24-områden
PRODUKTDIREKTIV
PRODUKTANSVARSDIREKTIV

TILLVERKARENS
SKYLDIGHETER

Identiska krav
inom EU-EES

Enda som skiljer är
de språkliga kraven
på bruksanvisningar



BESIKTNING

UTRUSTNINGS-
ÄGARENS
KONTROLL

SKYLDIGHETER
Nationella eller
Nordiska krav



Lyftanordningar (Nordiska gemensamma krav)

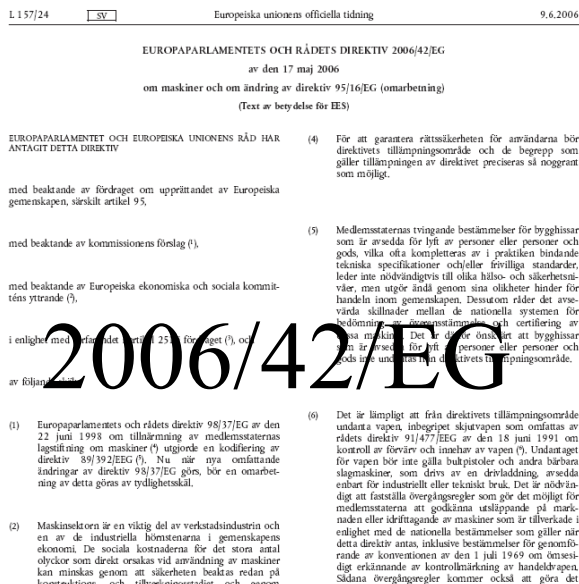
Internationell
besiktning

Återkommande besiktning utförd i enlighet med be-
sikttningsregler som är harmoniserade och accepte-
rade i två eller flera länder inom EES.

Svenska krav
Motordrivna portar
Tryckbärande anordningar



HUR HANTERA RISKER FÖR MASKINER VID CE-MÄRKNING



AFS 2008:3

Maskiner

Svenska versionen av
"maskindirektivet"

TVINGANDE LEGALA DE KRAV

Framgår i Bilaga 1 (Grundläggande hälso- och säkerhetskrav)

Riktlinjer för detaljerad tillämpning för att uppfylla kraven anges ges i harmoniserade standarder i sig inte är tvingande eller bindande

Gå via A-standard

Omvägen

Genvägen (full presumption)

SVENSK STANDARD
SS-EN ISO 12100:2010

Fastställt/Approved: 2010-11-22
Publicerad/Published: 2011-11-16
Utgåva/Edition: 1
Språk/Language: svenska/Swedish
ICS: 01.040.13; 13.110; 14.010

A-std

Maskinsäkerhet – Allmänna konstruktionsprinciper – Riskbedömning och riskreducering (ISO 12100:2010)

Safety of machinery – General principles for design – Risk assessment and risk reduction (ISO 12100:2010)

Avsnitt 6 ger förtydliganden om hur man uppfyller maskindirektivets bilaga 1 krav per kravpunkt samt hänvisar till relevanta standarder på B-nivå för respektive krav/riskområde.

Tillämpa C-standard direkt
(om sådan finns) unik för varje maskin



Följ avsnitt 6
signifikanta
risker med
denna maskinen
samt avsnitt 5
om åtgärder för
att förebygga dessa

SVENSK STANDARD
SS-EN 15093:2008

Fastställt/Approved: 2008-10-10
Publicerad/Published: 2008-11-03
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 14.220; 77.180

Valsverk – Varmvalsverk för platta produkter – Säkerhetskrav
Safety of Machinery – Safety requirements for hot flat rolling mills

Teknik- och områdesspecifika
säkerhetsstandarder

SVENSK STANDARD
SS-EN ISO 4413:2010

Fastställt/Approved: 2010-12-06
Publicerad/Published: 2010-12-21
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 13.110; 14.070; 23.100.01; 23.140

B-std

Maskinsäkerhet – Hydraulik – Allmänna regler och säkerhetskrav för system och deras komponenter (ISO 4413:2010)

Hydraulic fluid power – General rules and safety requirements for systems and their components (ISO 4413:2010)



C standarder
hänvisar även
till relevanta
B standarder
där man inte
fullt ut angett
komplett lösning

RISKANALYS MED INLEDANDE BEDÖMNING (RA 1) SAMT BEDÖMNING EFTER ÅTGÄRD (RA 2)

S (Sannolikhet för oönskad skadehändelse)			F (Frekvens för riskexponering)		G (Grad av möjlig skada)		A (Antal personer utsatta för risk)	
0,033	I princip omöjligt	Endast i extrema undantagsfall	0,5	Ärligen	0,1	Skrapsår eller blåmärke	1	1-2 personer
1	Högst osannolikt	Högst otänkbart	1	Månadsvis	0,5	Skärsår eller mindre ohälsa	2	3-7 personer
1,5	Osannolikt	Men kan inträffa	1,5	Veckovis	2	Brott på mindre ben, mindre ohälsa - tillfällig	4	8-15 personer
2	Möjligt	Men ovanligt	2,5	Dagligen	4	Brott på större ben, större ohälsa - tillfällig	8	16-50 personer
5	Möjlighet finns	Kan inträffa	4	Timvis	6	Förlust av en arm, ett ben eller öga, hörsel - permanent	12	50+ personer
8	Troligtvis	Inte överraskande	5	Ständigt	10	Förlust av två armar, ben eller ögon - permanent skada		
10	Sannolikt	Kan förväntas			15	Katastrofal, dödsfall		
15	Med all säkerhet	Utan tvekan						

K = S*F*G*A		Riskenivå
0-5		Försumbar risk
5-50		Liten till betydande risk
50-500		Stor risk
Över 500		Oacceptabel risk

Typ eller grupp av risk	Härledd risk	Sannolik konsekvens	Kommentar	Inledande analys RA 1						Åtgärd	RA 2 Analys efter åtgärd						Ev. ytterligare åtgärd
				S	F	G	A	K	Riskenivå		S	F	G	A	K	Riskenivå	
Mekaniska risker Exempel på andra typer av risker Elektriska risker Brännskaderisker Bullerisker Vibrationsrisker Strålningsrisker Risker med olika ämnen substanter och material Ergonomirisker Maskinomgivande risker Risker med kombinerade maskiner	Kinetisk energi (orsakad av acceleration eller retardation)	Risk för att bli påkörd															
		Utkastande föremål															
		Krossrisk															
		Skärskada															
		Drunkning															
		Indragningsrisk/intrassling															
		Friktions eller avskavningsskada															
		Kollisionsrisk															
		Sprutskada															
		Skärskada															
		Halk eller fallskada															
		Stick eller punkteringsskada															
		Risk för kvävning															
		Risk för att bli påkörd															
		Utkastande föremål															
Styrsystem risker Oönskad start EMC störning Fel i hårdvara Fel i mjukvara	Vassa kanter eller hörn	Krossrisk															
		Skärskada															
		Drunkning															
		Indragningsrisk/intrassling															
		Friktions eller avskavningsskada															
		Kollisionsrisk															
		Sprutskada															
		Skärskada															
		Halk eller fallskada															
		Stick eller punkteringsskada															
		Risk för kvävning															
		Risk för att bli påkörd															
		Utkastande föremål															
		Krossrisk															
		Skärskada															
		Drunkning															
	Rörliga delar närmar sig fast föremål	Indragningsrisk/intrassling															
		Friktions eller avskavningsskada															
		Kollisionsrisk															
		Sprutskada															
		Skärskada															
		Halk eller fallskada															
		Stick eller punkteringsskada															
		Risk för kvävning															
		Risk för att bli påkörd															
		Utkastande föremål															
		Krossrisk															
		Skärskada															
		Drunkning															
		Indragningsrisk/intrassling															
		Friktions eller avskavningsskada															
	Cutting parts	Kollisionsrisk															
		Sprutskada															
		Skärskada															
		Halk eller fallskada															
		Stick eller punkteringsskada															
		Risk för kvävning															
		Being run over															

Här listas grundtyp av risk

Orsakad av

Vad kan hända
(några exempel)

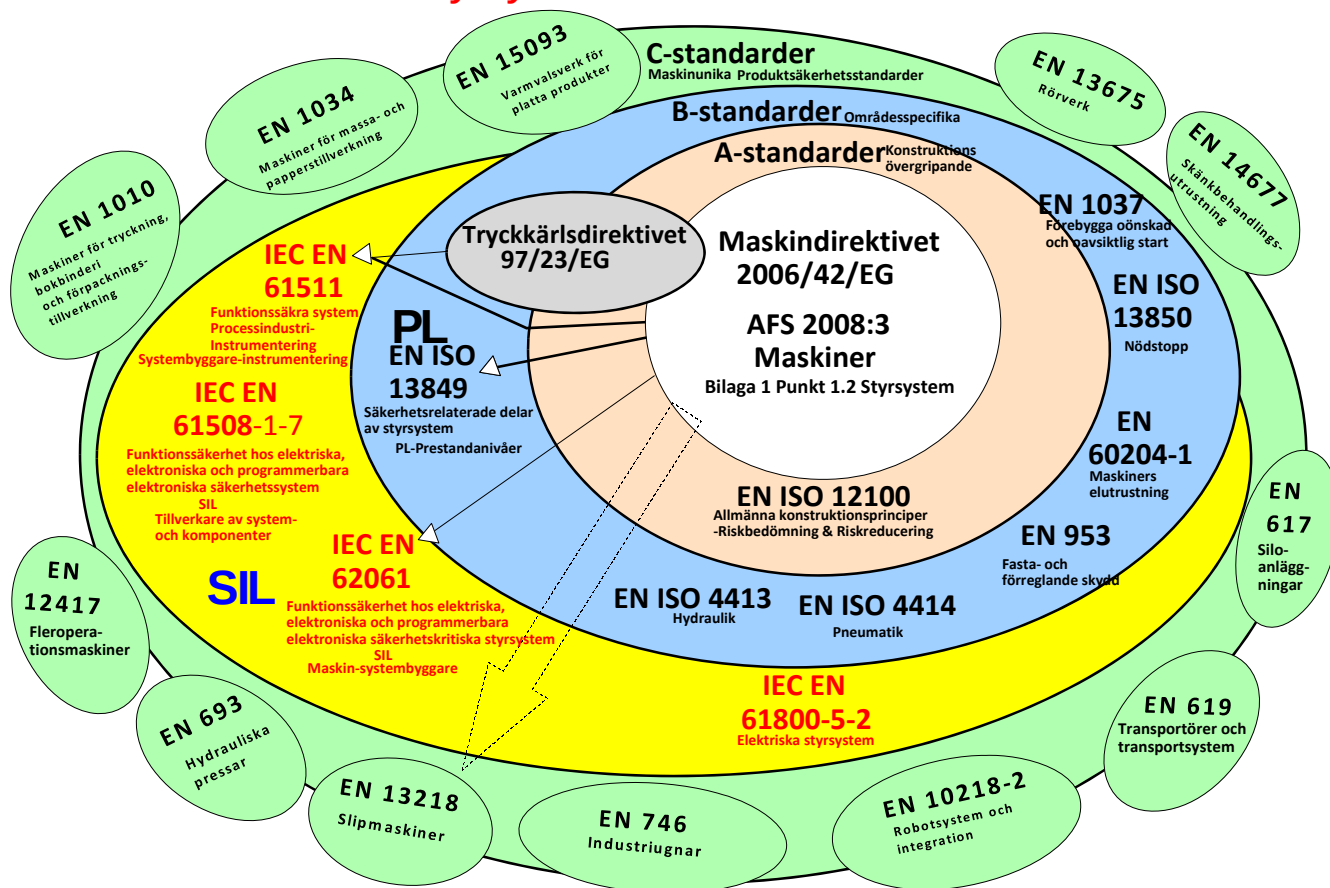
Inledande analys RA 1

Förslag till åtgärd

Analys efter vidtagen
åtgärd (RA 2)

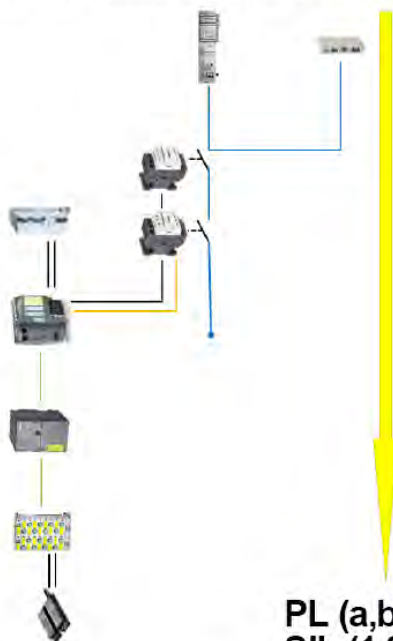
T.ex instruktion,
dokumentation

Översikt Styrskrav direktiv och standarder

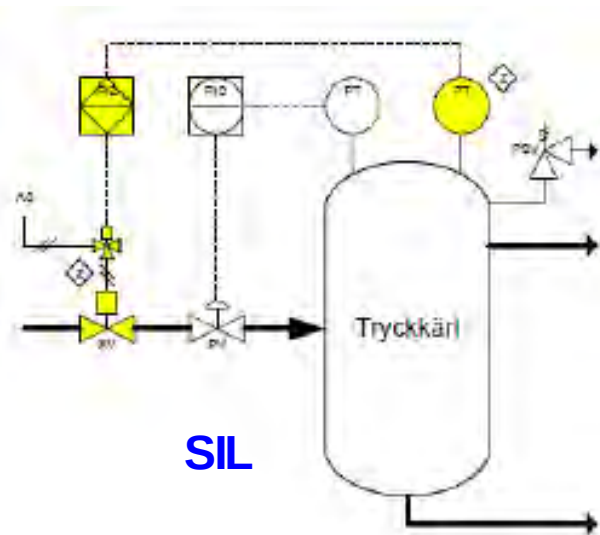
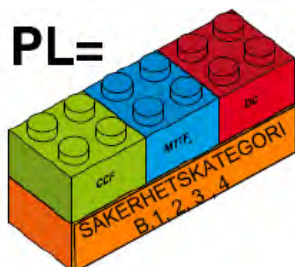


Riskbild, hårdvarutillförlitlighet (MTTF-värde), kategori, övervakning, arkitektur, sällsynta feluppträdanden med mera ger den slutliga kretsens säkerhetsklassificering genom erhållen prestandanivå (PL) eller säkerhetsintegrerad nivå (SIL)

Principen bygger på att konstruera systemet på ett sådant sätt att det förhindrar allvarliga fel eller att ha dem under kontroll när de uppkommer.



PL (a,b,c,d,e) eller
SIL (1,2,3,4)



SIL

SIL

HFT (Hardware Fault Tolerance)
PFHd (Probability Of random Dangerous Hardware Failures)
DC/SFF (Safe Failure Fraction)(Diagnostic Coverage)
CCF (Common Cause Failure)



STOPPTYPER

PRODUKTIONSSTOPP

FÖR ATT SKYDDA PRODUKTEN/DETALJEN ELLER MASKINEN.

EXEMPELVIS MASKINEN STANNAR INTE FÖRRÄN ARBETSCYKELN ÄR KLAR.

ELLER FÖR ATT FÅ ETT SNABBT STOPP UR PRODUKTIONSÄNDAMÅL (SNABBSTOBB) UTAN STÖRRE KRAV PÅ STOPKRETSSENS UPBYGGNAD.

PRODUKTIONSSTOPP ÖVERGÅR DOCK I SKYDDSTOPP OM NÅGON BRYTER EXEMPELVIS ETT FÖRREGLANDE SKYDD

SKYDDSTOPP

BRYTER MASKINENS START/STOPPFUNKTION.

- AVSEDD FÖR OMEDVETEN PÅVERKAN I EN RISKSITUATION. (SKALL ALLTSÅ FUNGERA OAVSETT VAD MÄNNISKAN TAR SIG TILL)
- ÄR ETT SÄKERT STOPP SOM GER MÖJLIGHET TILL ENKEL OCH SNABB ÅTERSTART. KAN T.EX ÅTERSTARTAS DÄR ARBETSCYKELN BRÖTS.
- EXEMPEL ÄR FÖRREGLANDE SKYDD, LJUSRIDÅER, RUSNINGSSKYDD, BRYTLISTER, TRAMPMATTOR ETC.

NÖDSTOPP

- ENDST AVSEDD FÖR MEDVETEN PÅVERKAN VID RISKSITUATIONER
- NÖDSTOPP FÅR ALDRIG ERSÄTTA VANLIGA SKYDDSANORDNINGAR MEN KAN VARA ETT KOMPLEMENT TILL DESSA

SÄKERHETSTEKNISKA SKYDDSÅTGÄRDER-MASKINER UTIFRÅN RISKBEDÖMNING

www.mpsa.se T Beäff

SÄKERHETSAVSTÅND EN ISO 13857

Maskinsäkerhet
- Skyddsavstånd för att hindra att armar och ben når in i riskområden

SS EN 953 FYSISKA SKYDD

Maskinsäkerhet - Skydd - Allmänna krav för konstruktion och tillverkning av fasta och öppningsbara skydd

EN ISO 13855

SKYDDSÅTGÄRDER

Maskinsäkerhet
- Placering av tekniska skydd beroende på kroppsdelars hastigheter

EN ISO 13849

Fasta skydd

Staket Barriärer

Kan endast öppnas med någon form av verktyg eller är elektriskt förreglade.

Rörliga skydd

Luckor Grindar Dörrar

MED LÅS-FUNKTION

UTAN LÅSFUNKTION

SS-EN ISO 13855
Maskinsäkerhet
- Placering av tekniska skydd beroende på kroppsdelars hastigheter

Med närmande funktion

Mekaniskt aktiverade skyddsanordningar

- Brytlistor
- Bumpers
- Tryckkännande mattor
- Linor

SS EN 1760
Maskinsäkerhet
- Tryckkännande skyddsanordningar - Del 1:
Allmänna principer för konstruktion och provning av tryckkännande mattor och golv

ESPE ElectroSensitive Protective Equipment Beröringsfria

- Scanners
- Ljusridåer
- Förreglingar

Fixerat läge

2-Hands manöverdon THC

SS EN 574
Maskinsäket
Tvåhandsmanöveranordningar
- Funktionella aspekter
- Konstruktionsprinciper

Ej fixerat läge

Nödstopp

SS EN ISO 13850
Maskinsäket
- Nödstoppsutrustning
- Konstruktionsprinciper

SS EN 60204-1
Maskinsäket
Maskiners elutrustning
- Del 1:
Allmänna fordringar

Manöverdon (väljare) för olika lägen beroende på maskinens körmode

SS EN ISO 13849-1 /-2

Maskinsäkerhet

- Säkerhetsrelaterade delar av styrsystem

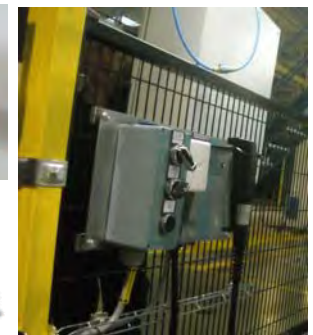
*SS EN 1088

Maskinsäkerhet

- Förreglingsanordningar för kombinerad med skydd
- Principer för konstruktion och urval

*ersätts av

SS EN ISO 14119



Ingreppsrisker, valsar, cylindrar, rullar, fasta delar, klädda ingrepp

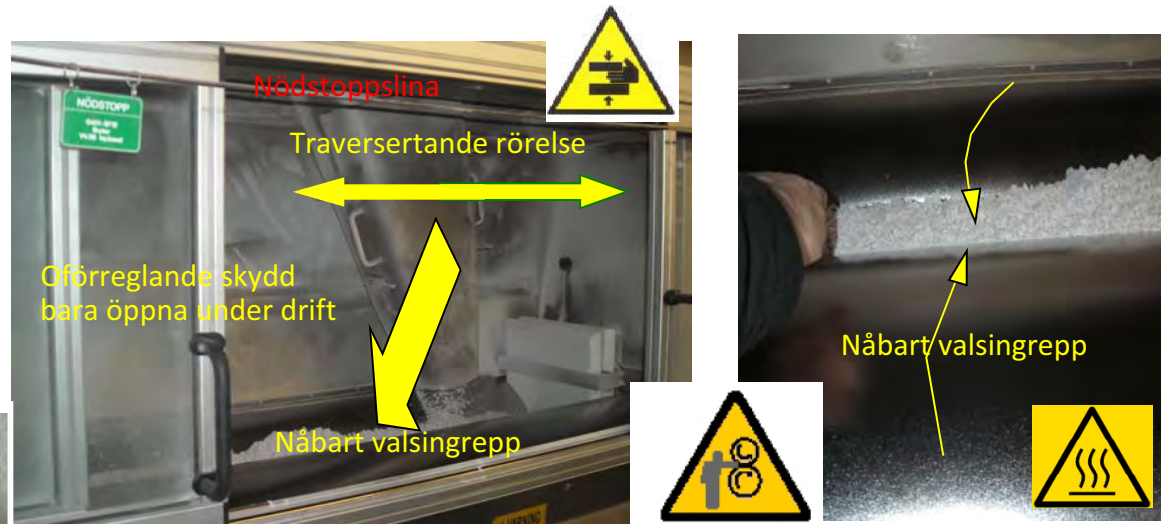
INGREPP

Riskområde vid valsar, cylindrar eller rullar, som vid rotation bildar en förträngning där personer, delar av kroppen eller kläder kan dras in.

Sådana ställen kan bl.a uppstå mellan

a) delar som roterar mot varandra;

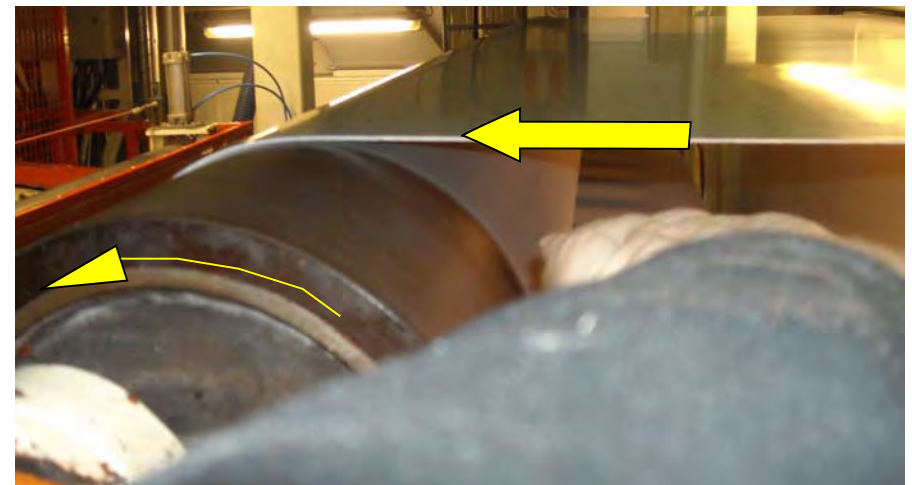
b) en roterande del och en fast intilliggande del;



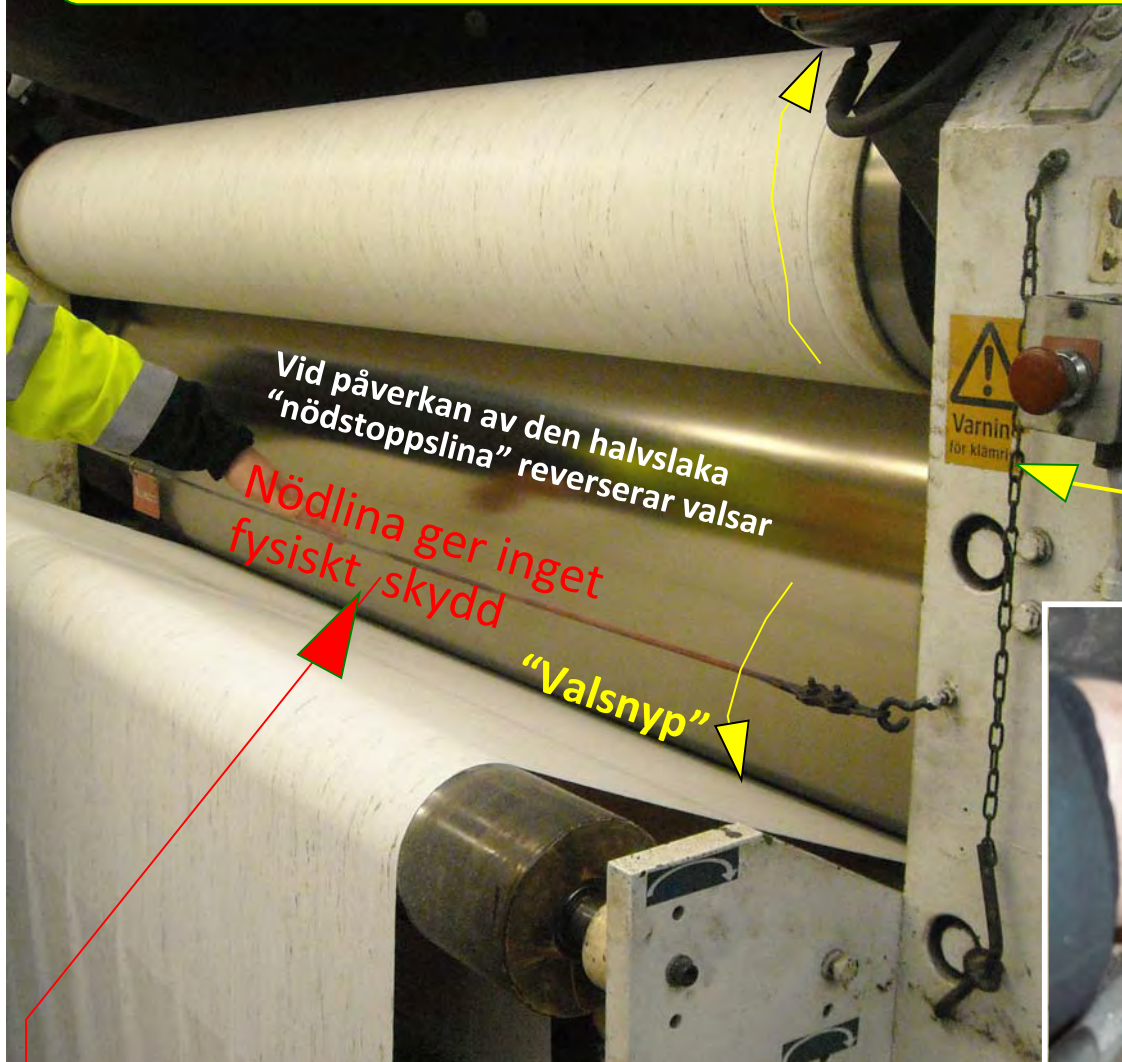
c) delar som roterar i samma riktning, men med olika periferihastigheter och ytegenskaper om lämpliga skyddsavstånd inte respekteras

klädda ingrepp

klädda ingreppsriskområde som uppstår där stark materialbana löper på rörliga delar såsom vals, cylinder eller skiva, så att personer, deras kroppsdelar eller kläder kan dras in, om lämpliga skyddsavstånd inte respekteras.



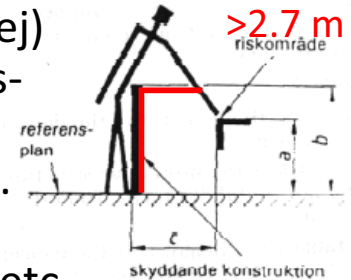
Öppna valsverk som helt saknar skyddsanordningar



Genom fall eller obalans, snubbelrisk eller genom att man sträcker sig in i riskområdet (säkerhetsavstånd enligt SS EN 13857 uppfylls ej) finns stor risk för kläm-kross-skada eller allvarligare vid exempelvis indragning i nyp.

- Spetsförning
- Valsrengörning under drift etc.

Vidare då brännskaderisk



Het yta

Skyltning räcker inte för denna typ av allvarliga risker.



Klarar ej heller frigångsmåttet >120 mm för arm mellan roterande vals sida och fast del.

Nödstoppsstandardern EN 13850

Nödstoppsutrustning skall varken användas som ett alternativ till egentliga tekniska skyddsåtgärder eller som alternativ till automatiska skyddsanordningar men kan användas som ett komplement.

Skyddsåtgärder vid ingreppsrisker-valsar-cylindrar

Skyddsåtgärder vid ingrepp/indragningsrisker vid ingrepp på cylindrar, valser och rullar ska, där det är tekniskt funktionsmässigt möjligt, undvikas genom att se till att det finns tillräckligt avstånd mellan roterande och fasta delar.

1. SKYDDA GENOM ATT TILLÄMPA SÄKERHETSAVSTÅND

Risken för att hela kroppen ska dras in förhindras om det vid ingrepp finns ett skyddsavstånd på 500 mm mellan maskindelarna. Se EN 349 även.

Risken för att en arm ska dras in förhindras om det vid ingrepp finns ett skyddsavstånd på minst 120 mm mellan maskindelarna.

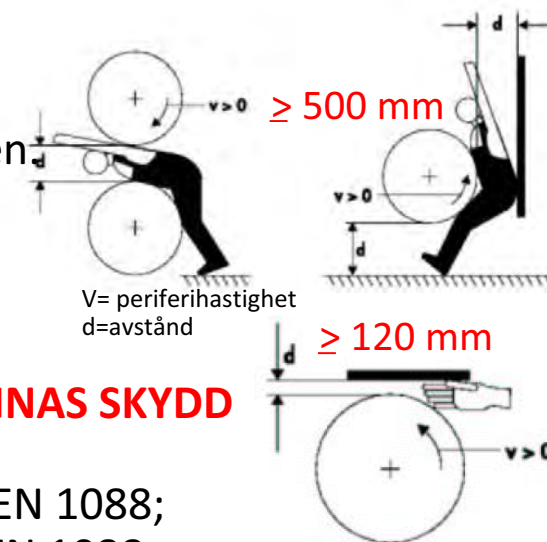
Det är endast tillåtet att tillämpa skyddsavståndet för arm om ingrepp inte kan nås av kroppen.

2. OM INDRAKNINGSRISK VID INGREPP INTE KAN UNDVIKAS SKA DET FINNAS SKYDD

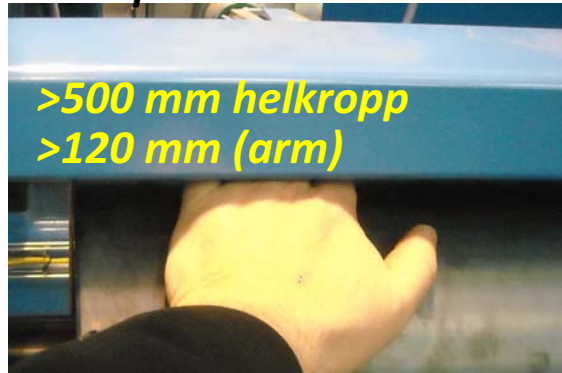
Lämpliga skyddsåtgärder är:

- Fasta eller förreglande ingreppsskydd med låsfunktion enligt EN 953 och EN 1088;
- Fasta eller förreglande avståndsskydd med låsfunktion enligt EN 953 och EN 1088;
- Fasta eller förreglande inhägnader med låsfunktion enligt EN 953 och EN 1088.

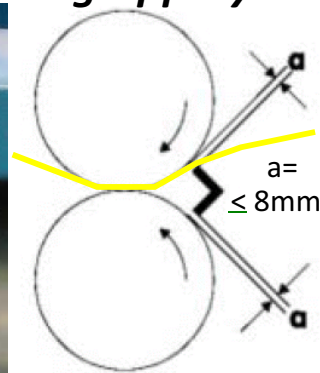
Fasta maskindelar, som t.ex. kåpor och fundament, som förhindrar tillträde till ett riskområde kan också helt eller delvis fungera som skyddsanordning. Fasta skydd ska väljas om tillträde till ingrepp inte krävs.



Tillämpa säkerhetsavstånd



Ingreppsskydd



Fast skydd



Inhägnad med förreglat tillträde

Kan dock tillåtas tillträde under låg hastighet t.ex (< 5 m/min) med

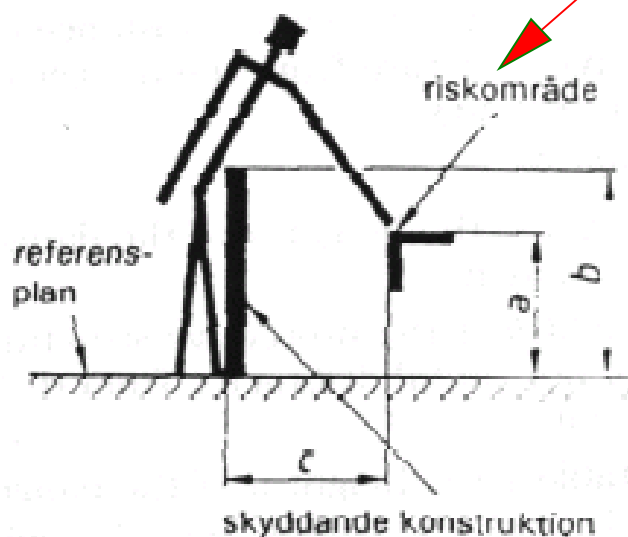
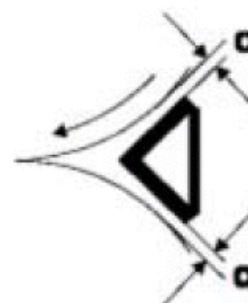
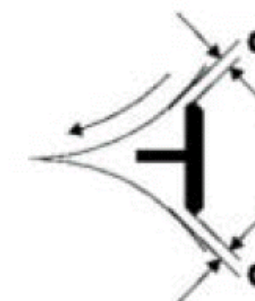
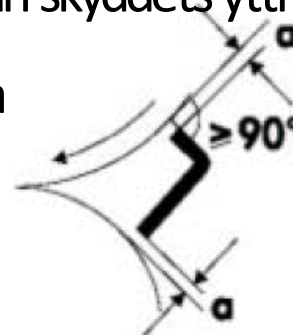
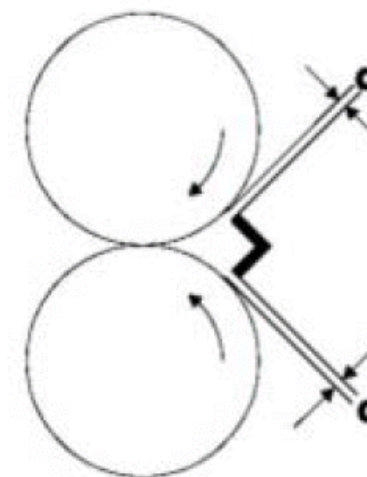


ingreppsskydd, typ av skydd placerat direkt framför ingrepp och klädda ingrepp i ett valspar eller annat ingrepp.

Ingreppsskydd ska vara så konstruerade och monterade att de kan upprätthålla sin skyddande funktion även under mekanisk påkänning, vibration och värme. Om en kraft på 1000 N appliceras på mitten fåravståndet "a" i figur 3 inte vara större än 8 mm.

Rundprofiler är inte lämpliga som skydd eftersom de kan skapa nya ingrepp. Avståndet mellan skyddet och roterande delar bör vara så litet som möjligt och ska inte vara större än 8 mm. Vinkeln mellan skyddets yttre yta och tangenten hos valsens yta ska vara trubbig eller rät.

För skydd som inte placeras direkt framför ingrepp ska avstånden som anges SS EN ISO 13857 tillämpas.



Figur 3 — Exempel på skydd (skyddsstänger) vid ingrepp ($a \leq 8 \text{ mm}$)

1.4.1 Allmänna krav

Skydd och skyddsanordningar ska

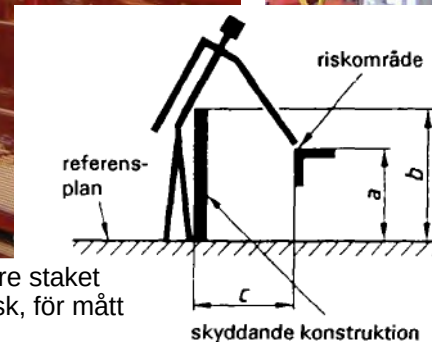
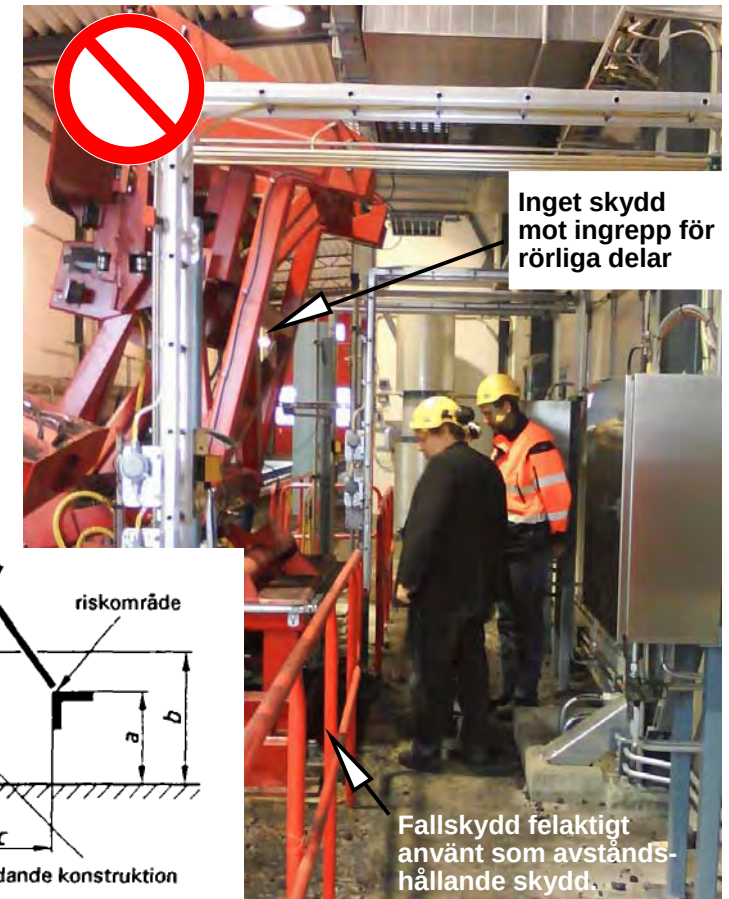
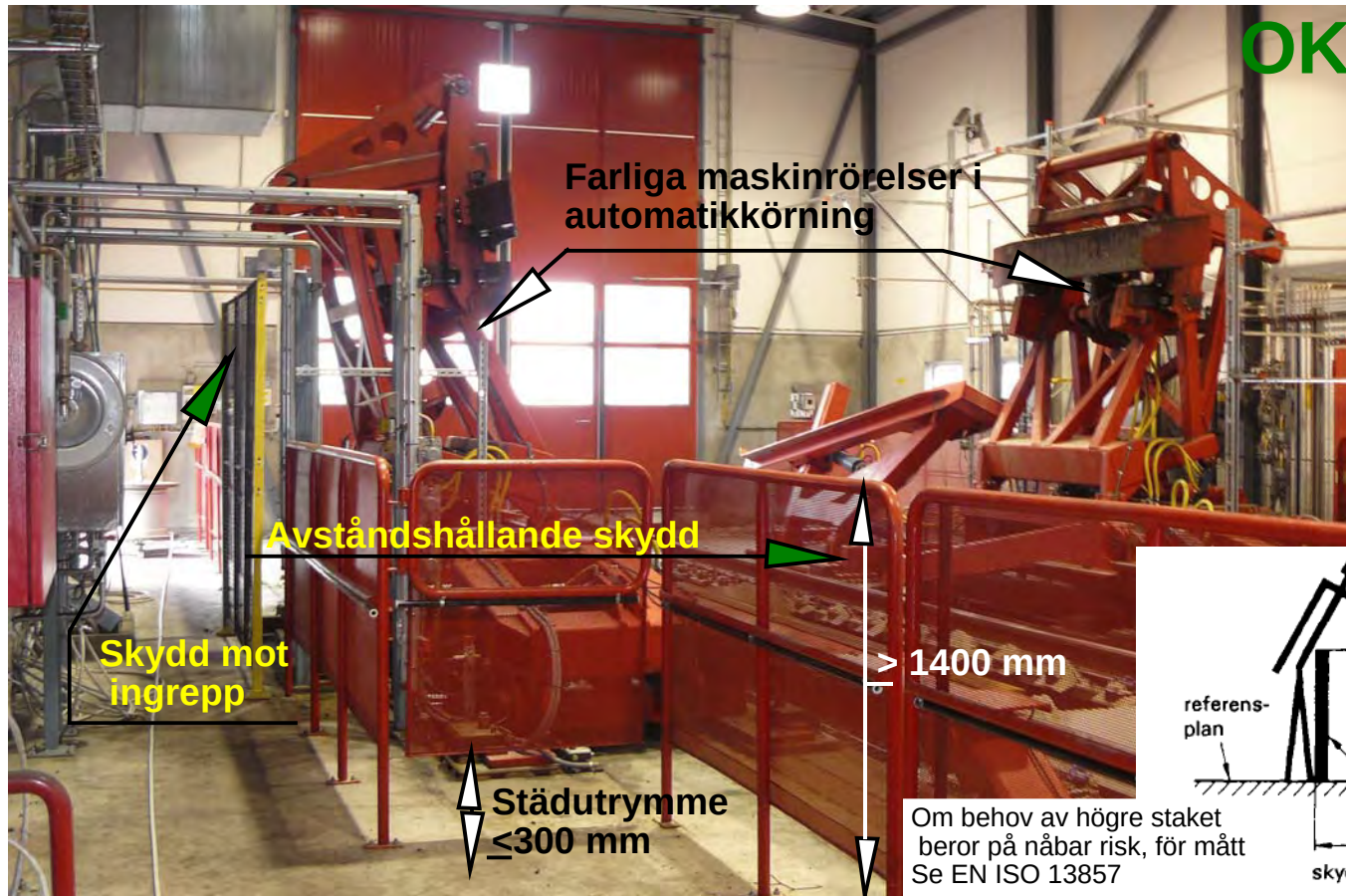
- vara robust tillverkade,
- sitta stadigt på plats,
- inte ge upphov till någon ytterligare riskkälla,
- inte lätt kunna kringgås eller sättas ur funktion,
- placeras på tillräckligt avstånd från riskområdet,
- i minsta möjliga mån begränsa överblicken över produktionsprocessen, och
- möjliggöra att nödvändiga arbeten för installation eller utbyte av verktyg samt för underhåll kan utföras, genom att begränsa tillträde till det område där arbetet ska utföras, om möjligt utan att skyddet måste avlägsnas eller skyddsanordningen sättas ur funktion

Dessutom ska skydd om möjligt skydda mot att material eller föremål kastas ut eller faller samt mot utsläpp som alstras av maskinen.

SKYDD-SKYDDSANORDNINGAR-Allmänna krav på skydd

Krav i MD 2006/42/EG (AFS 2008:3 Maskiner) Bilaga 1

T Beäff www.mpsa.se



Om behov av högre staket beror på nåbar risk, för mått Se EN ISO 13857

SKYDD-SKYDDSANORDNINGAR Krav i nya MD 2006/42/EG (AFS 2003:3) Bilaga 1

Fästanordningarna skall vara kvar på skydden vid demontering

1.4.2.1 Fasta skydd

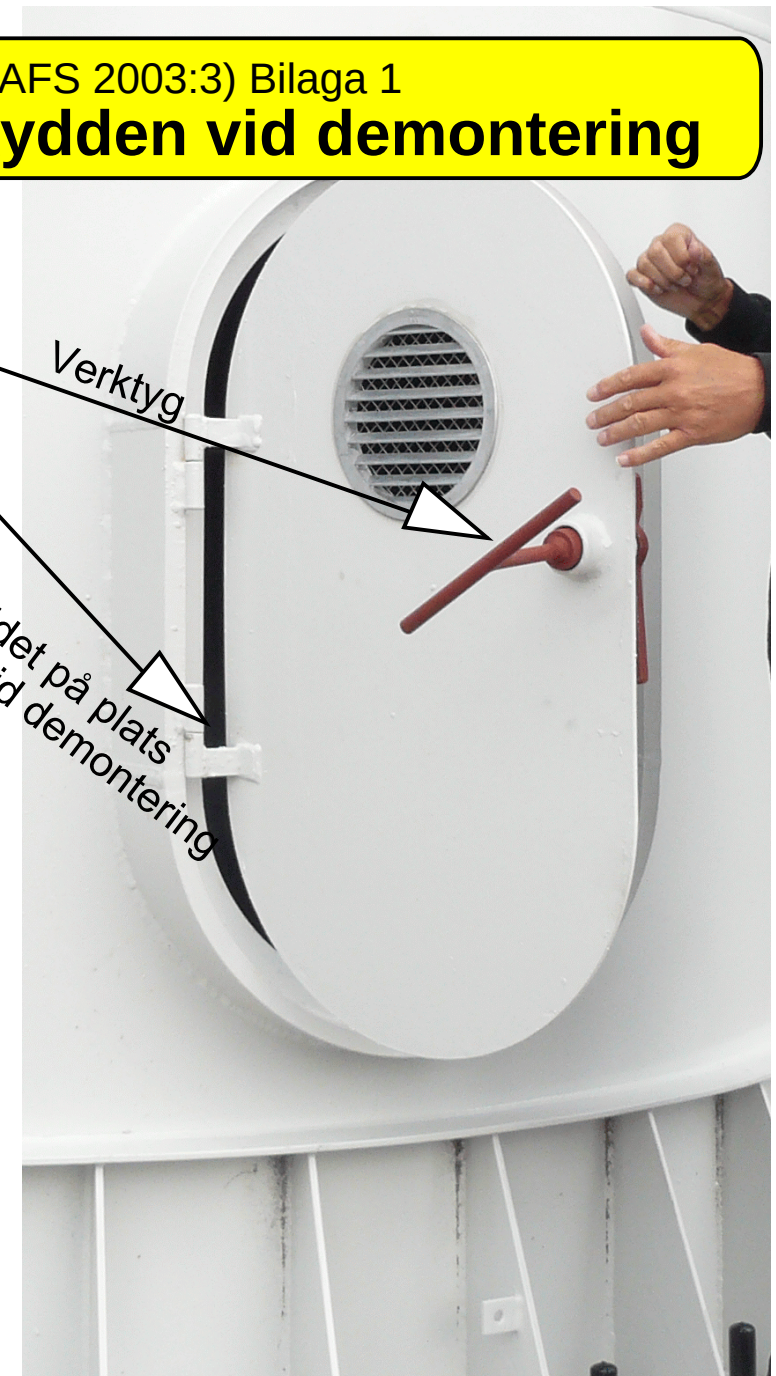
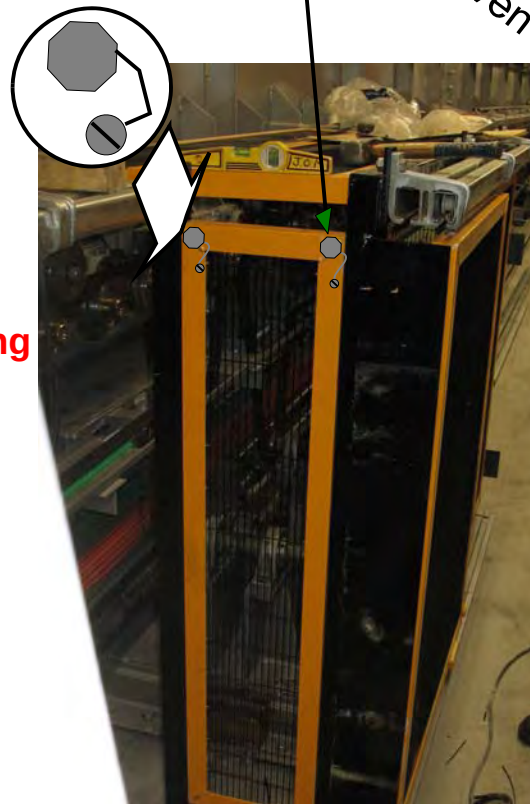
Fasta skydd ska vara fästade så att de inte kan öppnas eller avlägsnas utan verktyg.

Fästanordningarna ska förbli kvar på skydden eller på maskinen när skydden demonterats.

Om möjligt ska skydden inte kunna förbli på plats utan att vara fästade.



Fästanordningar på plats även vid demontering men tyvärr behövs inget verktyg för öppning av skyddet.



SKYDD-SKYDDSANORDNINGAR-Krav i MD 2006/42/EG (AFS 2008:3 Maskiner) Bilaga 1

Förreglande öppningsbara skydd ska så långt möjligt förbli kvar på maskinen när de är öppna

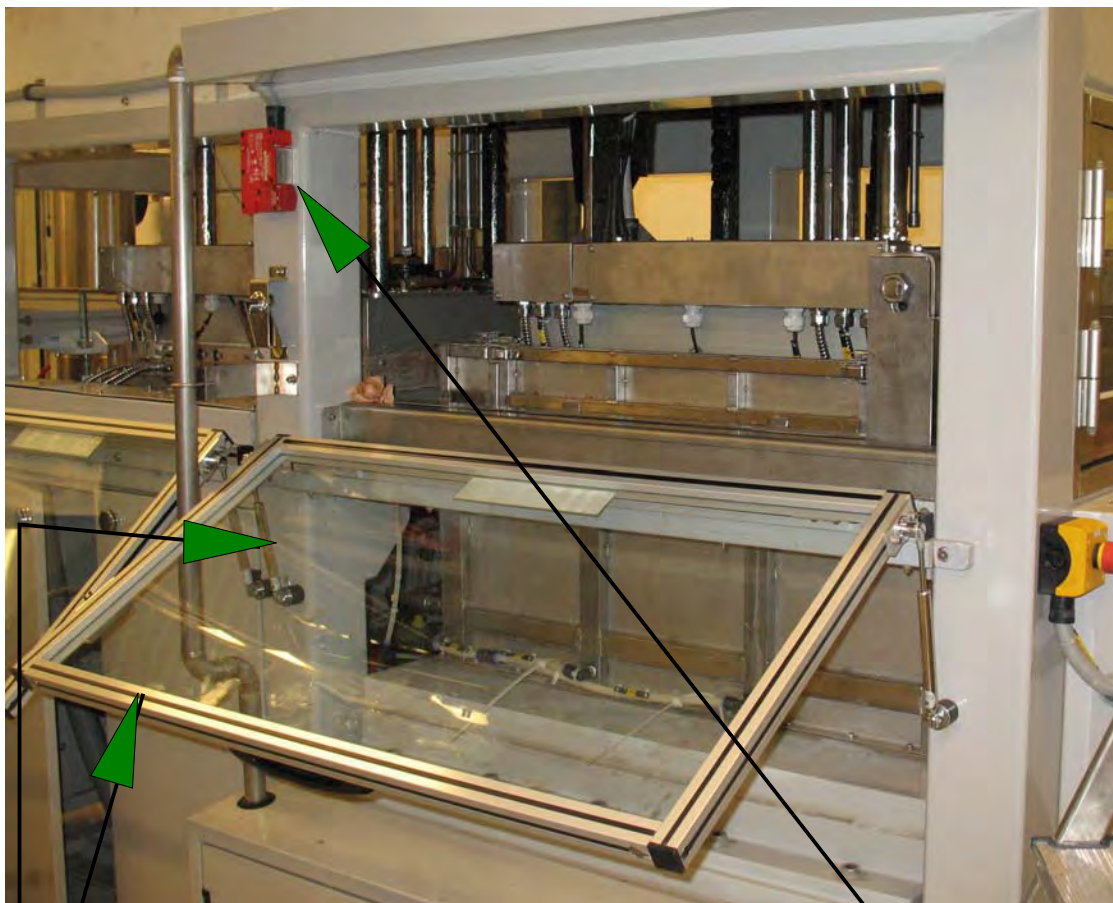


1.4.2.2 Förreglande öppningsbara skydd

Förreglande öppningsbara skydd ska

- så långt möjligt förbli kvar på maskinen när de är öppna,
- vara konstruerade och tillverkade så att de kan ställas in endast genom avsiktlig påverkan.

Förreglande öppningsbara skydd ska vara försedda med en förreglingsanordning



-Skyddet kvar på maskinen när det öppnats

-Skyddet förreglat

-Skyddet ergonomiskt anpassat genom cylinder som tar upp moment vid öppning/stängning



**Ej OK - Skyddet kvar på maskinen men inte förreglat
Kan ej heller klassas som fast skydd då det kan öppnas
utan någon form av verktyg.**

SKYDD-SKYDDSANORDNINGAR Krav i nya MD 2006/42/EG (AFS 2003:3) Bilaga 1

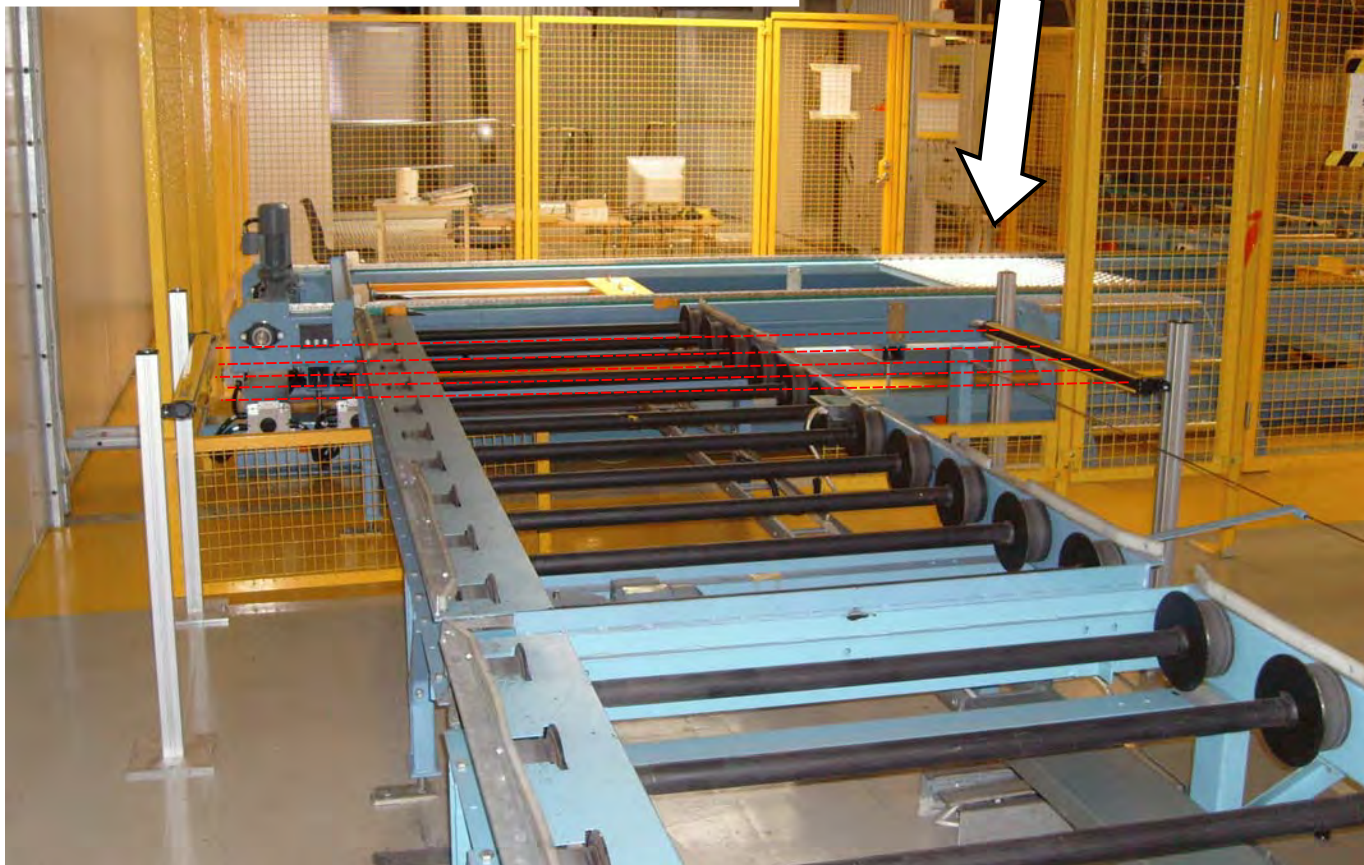
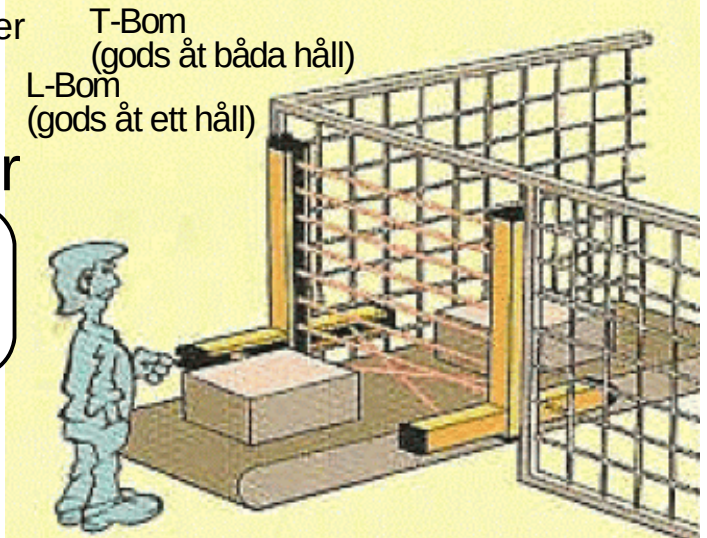
Skall inte lätt kunna kringgås eller sättas ur funktion.

Riskområde: varje område inom eller omkring en maskin där en persons hälsa eller säkerhet kan utsättas för risk,.

Utsatt person: en person som helt eller delvis befinner sig inom ett riskområde,.

Viktigt även att säkerställa att man inte enkelt tar sig in i riskområden där inte staketen täcker.

Material kan ta sig in och ut
men inte operatören då
ljusbom/ridå installerats



SÄKERHET- OCH UNDERHÅLLSANPASSAD LÖSNING BAND



Bandjustering möjlig
att utföra från utsidan
skydd och under drift

FU-möjligt
-Smörjning-kontroll lager

Bilaga 1 Punkt 1.2.4 AFS 2008:3 maskiner

Allmänna krav på skydd

– möjliggöra att nödvändiga arbeten för installation eller utbyte av verktyg samt för underhåll kan utföras, genom att begränsa tillträde till det område där arbetet ska utföras, om möjligt utan att skyddet måste avlägsnas eller skyddsanordningen sättas ur funktion.

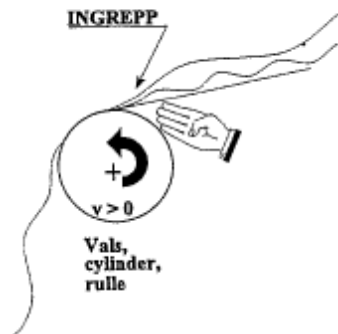
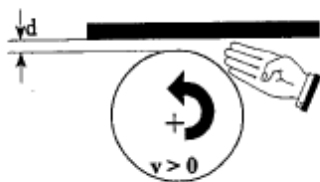
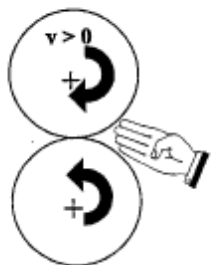
Dessutom ska skydd om möjligt skydda mot att material eller föremål kastas ut eller faller samt mot utsläpp som alstras av maskinen.

Bilaga 1 98/37/EG (AFS 2008:3 Maskiner) 1.6.1 Underhåll av maskiner.

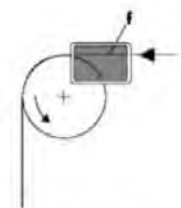
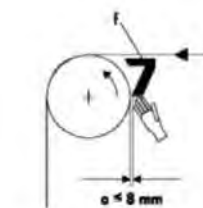
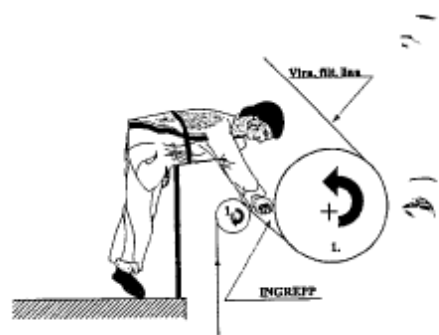
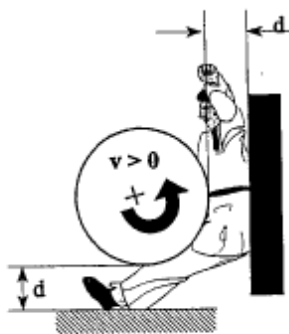
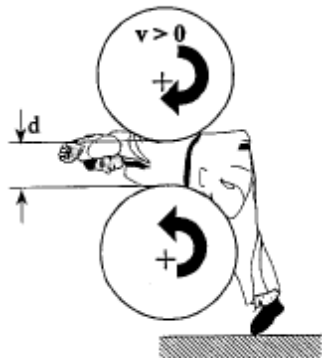
Inställnings- och underhållsställen ska vara placerade utanför riskområden.

Det ska vara möjligt att göra justeringar, underhålla, reparera, rengöra och utföra service när maskinen är stilla.

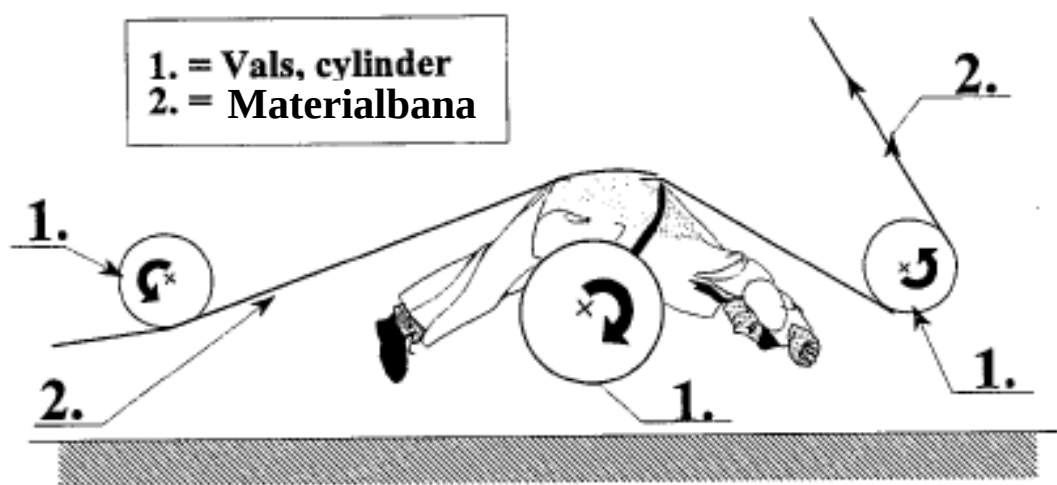
Om ett eller flera av ovanstående villkor av tekniska skäl inte kan uppfyllas, ska åtgärder vidtas för att säkerställa att dessa arbeten kan utföras säkert. På automatiserade maskiner och där det är nödvändigt på andra maskiner ska anslutningspunkter för diagnostisk felsökningsutrustning finnas. Automatiserade maskindelar som måste bytas ofta ska lätt och säkert kunna avlägsnas och bytas. Tillträdesmöjligheterna till delarna ska vara sådana att dessa uppgifter kan utföras med de nödvändiga tekniska hjälpmedlen, i enlighet med en föreskriven arbetsmetod.



Klädda ingrepp finns stor risk mellan materialbana och vals i indragningsriktningen om inte banan går av om man får in handen/armen.



1. = Vals, cylinder
2. = Materialbana



Kritiskt avstånd på måttet d/

Kroppsdelen som kan nå ingreppet	Avståndet d/
Handen	80 mm
Armbågen	120 mm
Hela kroppen	500 mm

LATHUND FÖR VAL AV SKYDDLÖSNING I MASKINER

Enligt maskindirektivet (2006/42/EG AFS 2008:3) anges i Bilaga 1 följande:

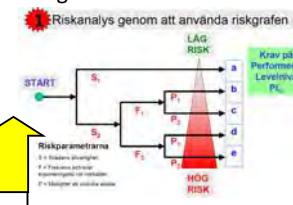
1.3.7 Risker i samband med rörliga delar.

En maskins rörliga delar skall vara konstruerade och tillverkade så att risk för kontakt som kan leda till olyckor förhindras eller i de fall då dessa risker ändå finns, vara försedda med skydd eller skyddsanordningar.

Standarden EN 953 om fasta eller förreglande skydd förtydligar hur dessa krav skall uppfyllas.

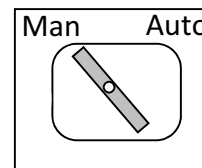
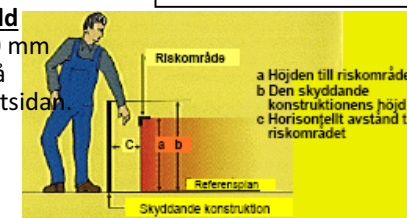
Om man efter riskbedömningen och val av skyddslösning kommer fram till att någon form av förregling krävs av skydd(en) så blir nästa steg att fastställa relevant kretslösning utifrån aktuell riskbild.

Standarderna SSENISO 13849-1 som fastställer Prestandanivåer (a,b,c,d,e) eller standarden EN 62061 som fastställer relevant SIL-klass (1,2 eller 3) tillämpas endera i form av dess riskträd eller via redan angiven "kretslösning" i en C-standard för aktuell maskin.



Avståndshållande skydd

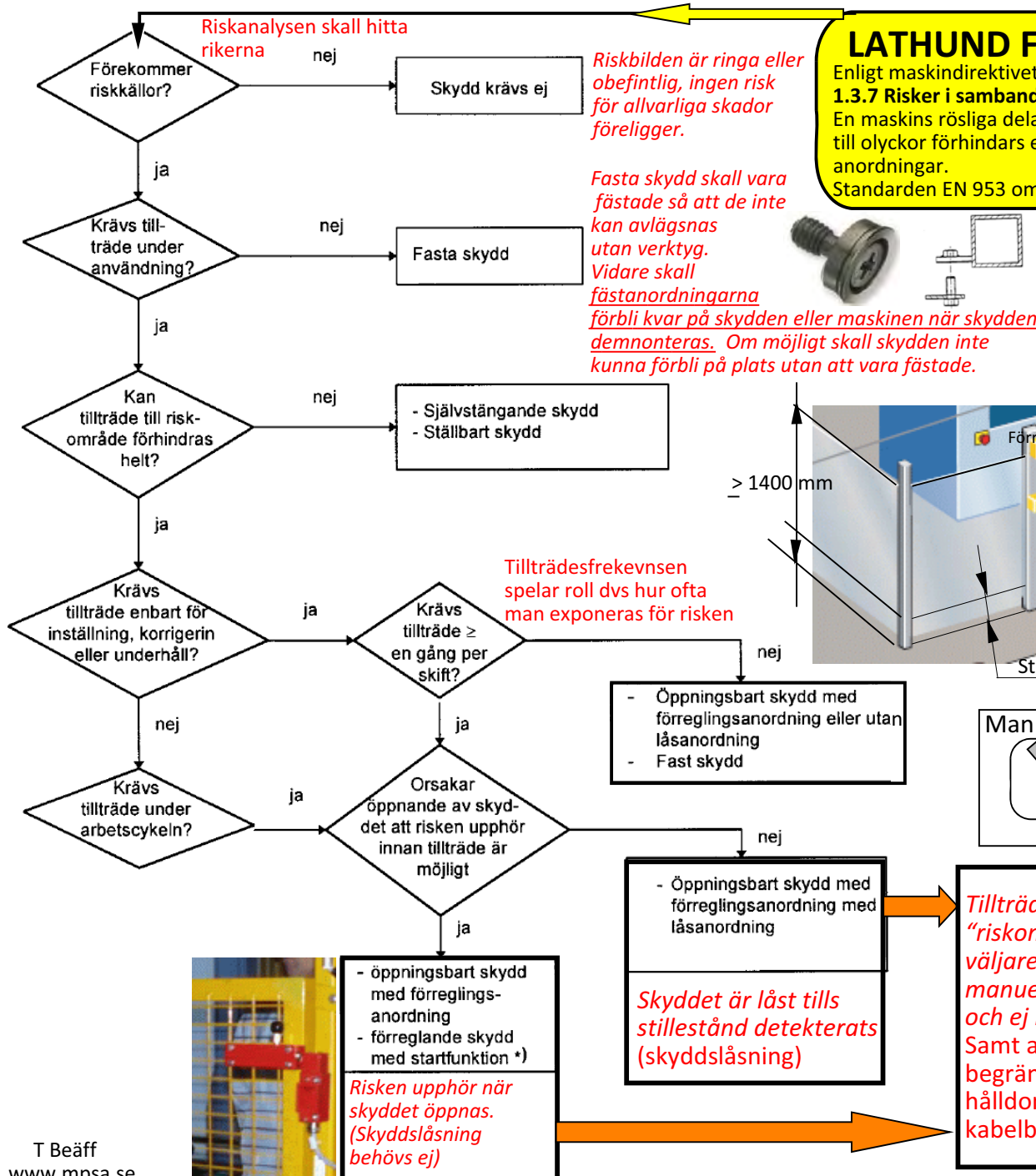
Högre staket än >1400 mm styrs av om man kan nå något på insidan från utsidan. Mått framgår i SS EN ISO 13857



För trådlös styrning skall ett automatiskt stopp ske när korrekta styrsignaler inte går fram inklusive kommunikationsbortfall.

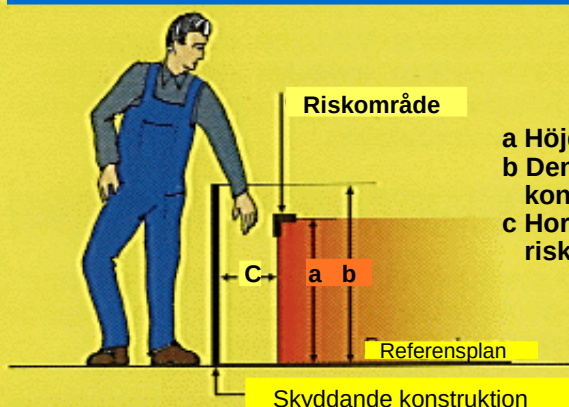


Tillträde kan dock tillåtas inom "riskområden" via hålldon om väljare för körsätt sätts i manuellt läge och ej i automatik. Samt att hastigheten begränsas under denna hålldonskörning med kabelbundet eller trådlöst don.

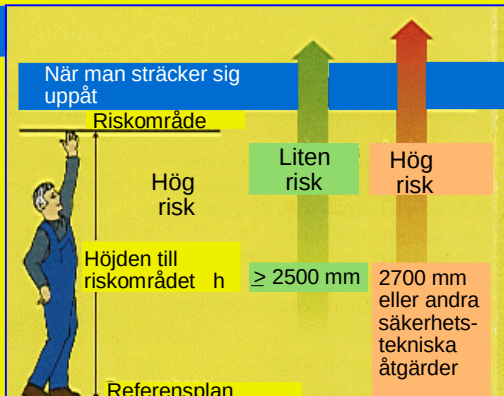


EN ISO 13857 Skyddsavstånd för att förhindra att man når riskområden med händer och armar

När man sträcker sig över skyddande konstruktioner



a Höjden till riskområdet
b Den skyddande konstruktionens höjd
c Horisontellt avstånd till riskområdet



Höjden till riskområdet a ²⁾	Den skyddande konstruktionens höjd b ¹⁾								
	1000	1200	1400	1600	1800	2000	2200	2400	2600
Horisontellt avstånd till riskområdet c ⁴⁾									
2600	00	800	700	00	00	500	400	300	00
2400	00	00	00	00	00	00	00	00	00
2200	00	000	00	800	700	00	400	300	00
2000	00	00	500	500	400	350	250	-	-
1800	300	200	000	00	800	00	400	300	-
1600	00	00	700	00	500	350	-	-	-
1400	400	300	00	00	800	00	400	-	-
1200	00	000	00	00	00	-	-	-	-
1000	500	400	00	00	800	00	-	-	-
800	300	000	00	00	00	-	-	-	-
600	500	400	00	00	800	500	-	-	-
400	300	000	00	800	00	-	-	-	-
200	500	400	00	00	800	-	-	-	-
0	400	000	00	500	-	-	-	-	-
	500	400	00	00	700	-	-	-	-
	400	000	00	00	-	-	-	-	-
	500	400	00	00	-	-	-	-	-
	300	00	00	-	-	-	-	-	-
	500	300	00	-	-	-	-	-	-
	200	500	-	-	-	-	-	-	-
	400	300	800	-	-	-	-	-	-
	200	300	-	-	-	-	-	-	-
	400	200	400	-	-	-	-	-	-
	00	200	-	-	-	-	-	-	-
	200	00	-	-	-	-	-	-	-
	00	200	-	-	-	-	-	-	-
	00	500	-	-	-	-	-	-	-

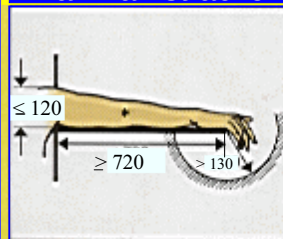
- 1) Skyddande konstruktioner lägre än 1000 mm är inte inkluderade eftersom de inte begränsar kroppens rörelse tillräckligt.
2) Om risken är liten när man sträcker sig uppåt skall höjden (h) till riskområdet vara >2500 mm stor risk >2700 mm eller skydd.
3) Skyddande konstruktioner lägre än 400 mm bör inte användas utan ytterligare skyddsåtgärder.
4) Där liten risk föreligger (typ friktion eller avskavning) skall det övre (gröna fältet) tillämpas.
Där stor risk föreligger för skada i samband med insnärjning tillämpas det under (röda fältet).

Mått i mm

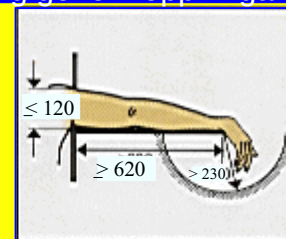
Kroppsdelen	Illustration (bild)	Öppning	Säkerhetsavstånd sr		
			Spaltformad Kvadratisk	Rund	
Fingertopp		$e \leq 4$	≥ 2	≥ 2	≥ 2
		$4 < e \leq 6$	≥ 10	≥ 5	≥ 5
Finger upp till knogen		$6 < e \leq 8$	≥ 20	≥ 15	≥ 5
		$8 < e \leq 10$	≥ 80	≥ 25	≥ 20
eller hand		$10 < e \leq 12$	≥ 100	≥ 80	≥ 80
		$12 < e \leq 20$	≥ 120	≥ 120	≥ 120
Arm upp till axelleden		$20 < e \leq 30$	≥ 850 ¹⁾	≥ 120	≥ 120
		$30 < e \leq 40$	≥ 850	≥ 200	≥ 120
		$40 < e \leq 120$	≥ 850	≥ 850	≥ 850

1) Om längden av den spaltformade öppningen är < 5 mm fungerar tummen som ett stopp och skyddsavståndet kan minskas till 200 mm. mått i mm

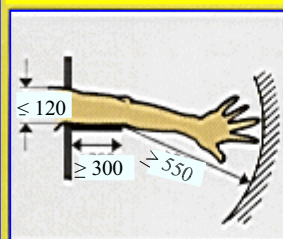
När man sträcker sig genom öppningar



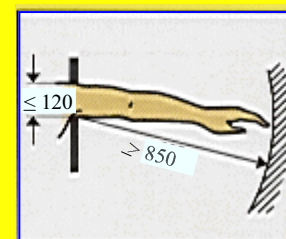
Arm och hand stödda fram till knogarna



Arm stödd fram till handleden



Arm stödd fram till armbågen



Begränsning av rörelse endast vid axel och armbåga

SKYDDSDUTRYMMEN FÖR ATT HINDRA ATT MAN NÅR RISKOMRÅDEN MED FÖTTER OCH BEN EN 13857

DEL AV BEN ELLER FOT	BILD	ÖPPNING	SKYDDSAVSTÅND s_r	
			Spaltformad	Kvadratisk eller rund
TÅSPETS		$e \leq 5$	0	0
TÅ		$5 < e \leq 15$	≥ 10	0
		$15 < e \leq 35$	$\geq 80^{1)}$	≥ 25
FOT		$35 < e \leq 60$	≥ 180	≥ 80
		$60 < e \leq 80$	$\geq 650^{1)}$	≥ 180
BEN UPP TILL KNÄ		$80 < e \leq 95$	$\geq 1100^{1)}$	$\geq 650^{1)}$
BEN UPP TILL GRENEN		$95 < e \leq 180$	$\geq 1100^{1)}$	$\geq 1100^{1)}$
		$180 < e \leq 240$	nicht zulässig	$\geq 1100^{1)}$

1) Om längden av den spaltformade öppningen är < 75 mm kan avståndet minskas till > 50 mm

2) Värde motsvarar "ben upp till knä" 3) Värde motsvarar "ben upp till grenen".

HINDRANDE AV FRI RÖRELSE UNDER SKYDDANDE KONSTRUKTION

Tabeller anger avståndet s för specialfall när tillträde med fötter och ben hindras samtidigt som personen står kvar i upprätt attällning utan något ytterligare stöd.

Om det föreligger risk för halka eller felanvändning kan det vara olämpligt att använda värdena nedan.

mått i mm

a) skyddande konstruktion

Höjd upp till skyddande konstruktion h

$h \leq 200$
 $200 < h \leq 400$
 $400 < h \leq 600$
 $600 < h \leq 800$
 $800 < h \leq 1000$

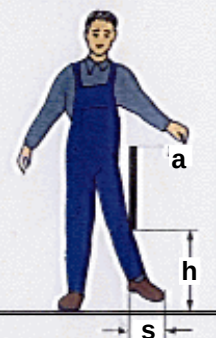
Fall 1



Fall 2



Fall 3

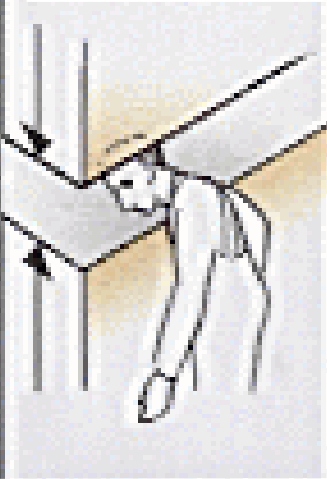
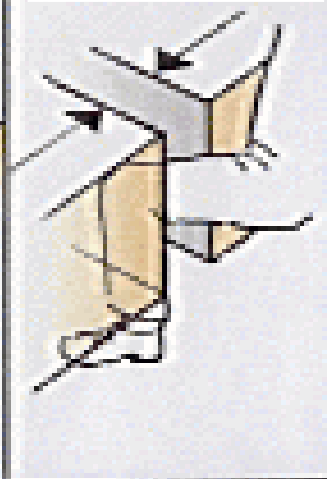
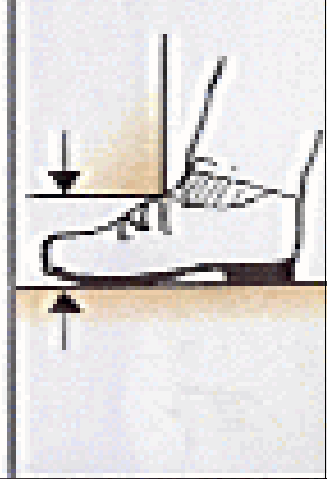
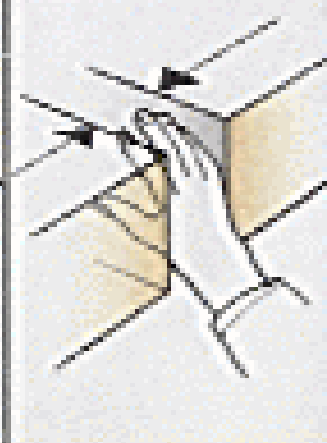
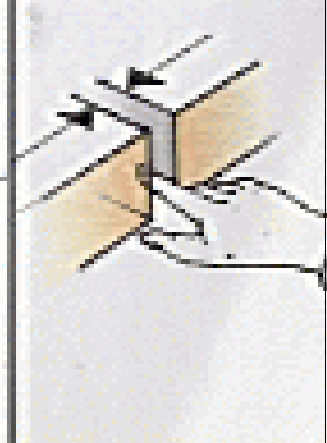


Avstånd s

≥ 340	≥ 665	≥ 290
≥ 550	≥ 765	≥ 615
≥ 850	≥ 950	≥ 800
≥ 950	≥ 950	≥ 900
≥ 1125	≥ 1195	≥ 1015

MINIMIUTRYMMEN FÖR ATT UNDVIKA ATT KROPPSDELAR KROSSAS

SS-EN 349

HELKROPP	HUVUD	BEN	FOT
≥ 500 mm	≥ 300 mm	≥ 180 mm	≥ 120 mm
			
TÅR	ARM	HAND-HANDLED KNYTNÄVE	FINGER
≥ 50 mm	≥ 120 mm	≥ 100 mm	≥ 25 mm
			

PLACERING AV TEKNISKA SKYDD BEROENDE PÅ KROPSSDELARS HASTIGHET SS EN 13855 (Exempel ljusstråleskydd)

Generell formel för beräkning av skyddsavstånd (EU)

$$S = K * T + C$$

S= Minsta tillåtna avstånd mellan ljusstråleskyddet och risken i mm

K= Rörelsehastighet hos relevant kroppsdel i mm/sek

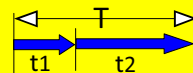
T= Total stopptid ($t_1 + t_2$)
 (t₁ ljusstråleskyddets reaktionstid i sekunder (typ 30-40 ms)
 (t₂ maskinens stopptid i sekunder dvs stoppa farlig maskinfunktion (typ 300 m/s)

- a) påverkan av tekniskt skydd (ljusstråle)
- b) Tekniskt skydd utlöses (frånsignal genereras)
- c) Farlig maskinfunktion upphör (säkert tillstånd)

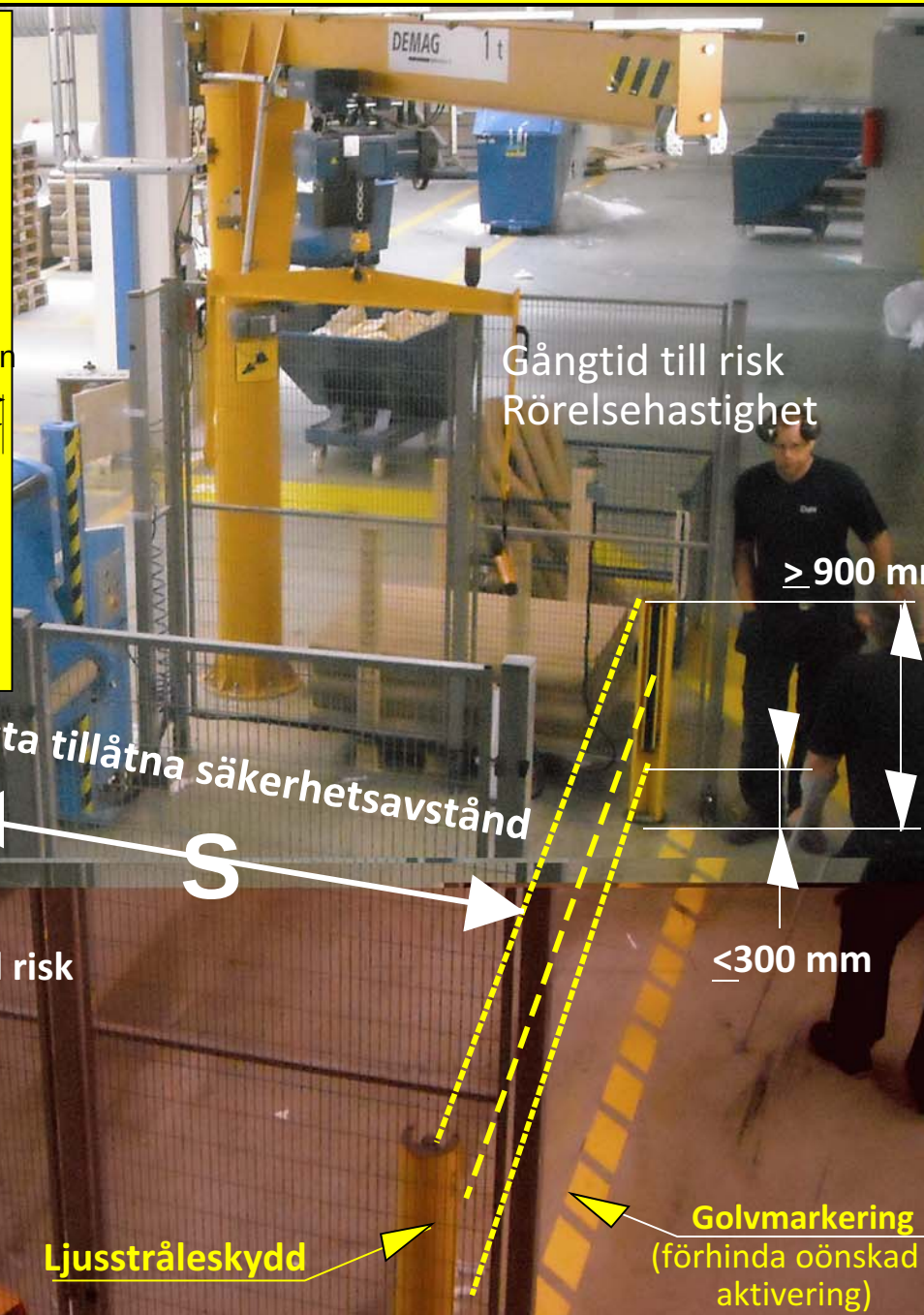
C= Tilläggsavstånd för ljusstrålesskyddets upplösning/plac.

T.ex 8* (känsligheten - 14 mm)

T.ex C = 1 200 mm - 0,4 H, men inte mindre än 850 mm, där H är höjden på skyddsfältet över referens-planet, t.ex. golvet, i millimeter (mm).



Antal strålar	Höjd över golv	C (mm)
1	750	1200
2	400	850
3	300, 700, 1100	850
4	300, 600, 900, 1200	850



NÖDSTOPPSFUNKTION I SAMBAND MED SAMMANBYGGNAD AV FLERA MASKINER

Det får aldrig uppstå någon tvekan i en nödsituation vilket nödstoppsdon som stoppar vad

Vid och runt transportörer skall man aldrig ha längre avstånd än 10 m till en nödstoppsdon eller en nödlinja.
(Se EN 620 C-std bandtransportörer)



AFS 2008:3 Maskiner (2006/42/EG) Bilaga 1 1.2.4.4 Montering av maskiner

Maskiner eller maskindelar som är konstruerade för att arbeta tillsammans ska vara konstruerade och tillverkade så att stoppanordningar, inklusive nödstoppsanordningar, inte bara kan stoppa själva maskinen, utan även all ansluten utrustning, om fortsatt drift av denna kan vara farlig.

Nödstopp skall fungera

- antingen enligt **stoppkategori 0** dvs stoppa genom omedelbart avlägsnande av kraft till drivanordningen(-arna),
- eller mekanisk frångkoppling (urkoppling) mellan de potentiellt farliga delarna och deras drivanordning(-ar), och, om nödvändigt, bromsning (icke styrt stopp)
- eller enligt **stoppkategori 1**, dvs styrt stopp med kraft till drivanordningen (-arna) tillgänglig för att erhålla stoppet och därefter brytning av krafttillförseln när stoppet har åstadkommits.

Se SS EN 60204-1 Maskiners elutrustning eller
SS EN ISO 13850 Funktionella krav på nödstopp

Se även EN 619, EN 620

Tänk på följande

När en maskin är indelad i flera "nödstoppsområden" skall hela systemet vara konstruerat så att det är lätt att se vilket manöverdon som hör till ett visst område så det inte uppstår några betänkligheter vilket don som skall påverkas i en nödsituation.

*Vid zonindelning säkerställ att tydlig uppskyllning sker så alla är medvetna om indelningen

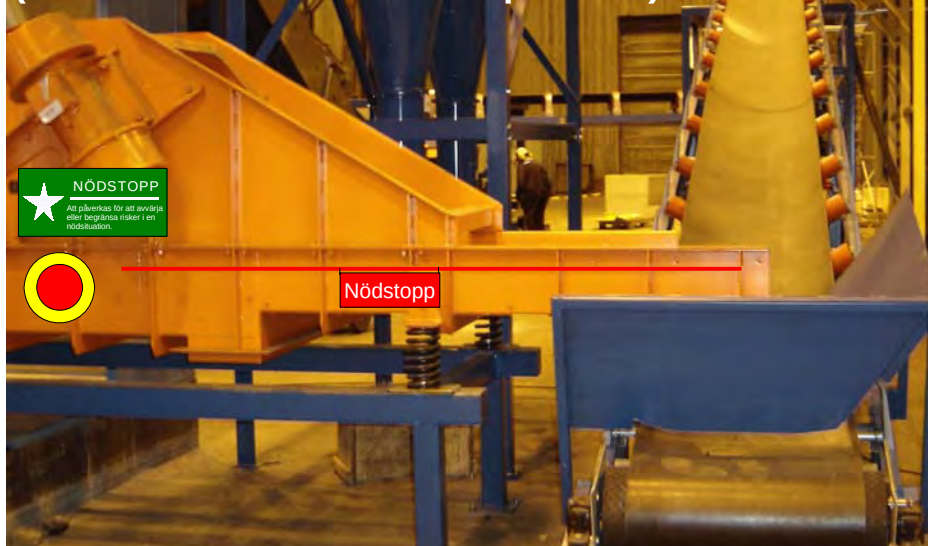
Att nödstoppsdonen placeras så att de lätt kan nås och påverkas utan risk för operatören eller andra som kan behöva påverka dem.

Att det tillstånd i vilket maskinen befinner sig efter ett nödstoppskommando skall inte förändras oavsiktligt (oväntat) under den tid som manöveranordningen är i påverkat tillstånd

NÖDSTOPPSFUNKTION I SAMBAND MED SAMMANBYGGNAD AV FLERA MASKINER

Det får aldrig uppstå någon tvekan i en nödsituation vilket nödstoppsdon som stoppar vad

Vid och runt transportörer skall man aldrig ha längre avstånd än 10 m till en nödstoppsdon eller en nödlina.
(Se EN 620 C-std bandtransportörer)



AFS 2008:3 Maskiner (2006/42/EG) Bilaga 1 1.2.4.4 Montering av maskiner

Maskiner eller maskindelar som är konstruerade för att arbeta tillsammans ska vara konstruerade och tillverkade så att stoppanordningar, inklusive nödstoppsanordningar, inte bara kan stoppa själva maskinen, utan även all ansluten utrustning, om fortsatt drift av denna kan vara farlig.

Nödstopp skall fungera

- antingen enligt **stoppkategori 0** dvs stoppa genom omedelbart avlägsnande av kraft till drivanordningen(-arna),
- eller mekanisk frångkoppling (urkoppling) mellan de potentiellt farliga delarna och deras drivanordning(-ar), och, om nödvändigt, bromsning (icke styrt stopp)
- eller enligt **stoppkategori 1**, dvs styrt stopp med kraft till drivanordningen (-arna) tillgänglig för att erhålla stoppet och därefter brytning av krafttillförseln när stoppet har åstadkommits.

Se SS EN 60204-1 Maskiners elutrustning eller
SS EN ISO 13850 Funktionella krav på nödstopp

Se även EN 619, EN 620

Tänk på följande

När en maskin är indelad i flera "nödstoppsområden" skall hela systemet vara konstruerat så att det är lätt att se vilket manöverdon som hör till ett visst område så det inte uppstår några betänkligheter vilket don som skall påverkas i en nödsituation.

*Vid zonindelning säkerställ att tydlig uppskyltning sker så alla är medvetna om indelningen

Att nödstoppsdonen placeras så att de lätt kan nås och påverkas utan risk för operatören eller andra som kan behöva påverka dem.

Att det tillstånd i vilket maskinen befinner sig efter ett nödstoppskommando skall inte förändras oavsiktligt (öväntat) under den tid som manöveranordningen är i påverkat tillstånd

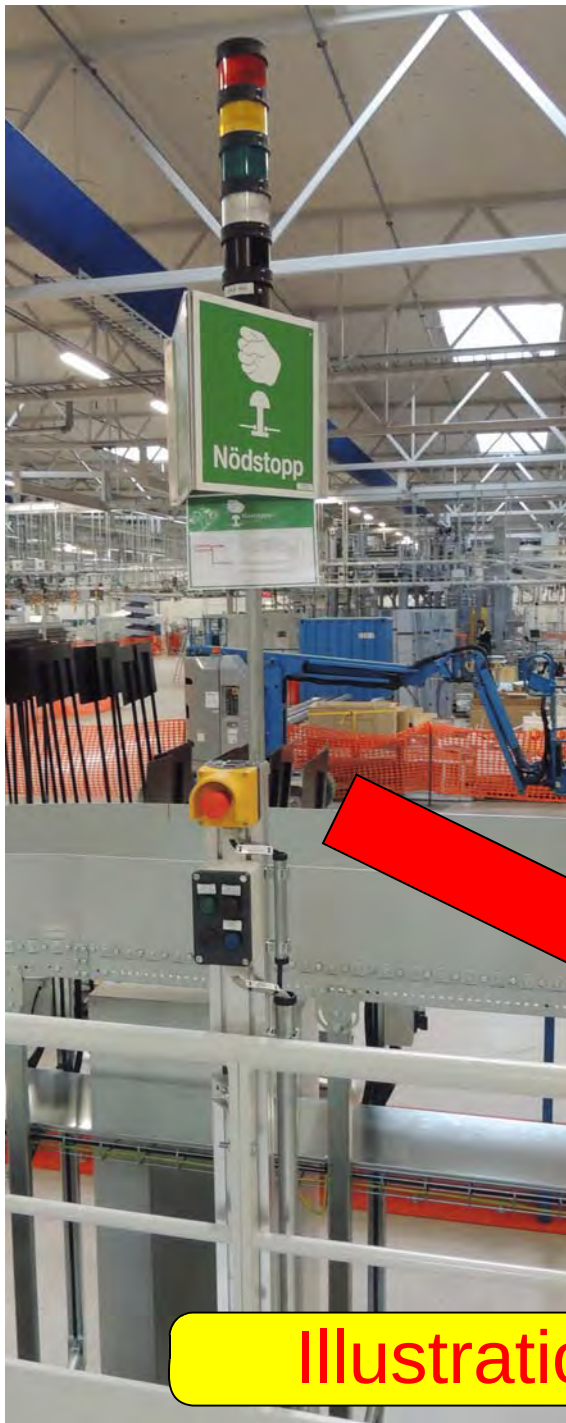


Illustration av nödstoppsområde på ritning

FUNKTION NÖDSTOPP

Funktion som är avsedd:

- att avvärja eller begränsa förekommande risker för personer, skada på maskiner eller arbetsstycken,
- att utlösas av en enda mänsklig handling när den normala stoppfunktionen är otillräcklig för detta ändamål.

Risker enligt nödstoppsstandarden är sådana som kan uppkomma genom:

- oregelbundenheter i funktionen (felfunktion hos maskinen, oacceptabla egenskaper hos material som bearbetas, mänskliga misstag
- normal drift.

EJ SOM ALTERNATIV TILL SKYDDSÅTGÄRDER-SKYDDSANORDNINGAR

Nödstoppsutrustning skall varken användas som ett alternativ till egentliga tekniskaskyddsåtgärder eller som ett alternativ till automatiska skyddsanordningar, men den kan användas som komplement

FUNKTION I SAMBAND MED NÖDSTOPPS PÅVERKAN

Efter påverkan av manöverdonet skall nödstoppsutrustningen fungera på sådant sätt att:

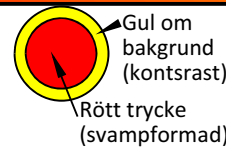
- risken automatiskt avvärjs eller begränsas på bästa möjliga sätt.
- "På bästa möjliga sätt" omfattar bl a:
 - **val av optimal fartminskning**
(stanna farliga rörelser så fort det går utan att skapa nya risker)
 - **val av stoppkategori enligt riskbedömningen.**

"Automatiskt" betyder att verkställandet av nödstoppsfunktionen kan vara resultatet av en bestämd serie av inre funktioner efter påverkan av nödstoppsdonet.

NÖDSTOPPSPRINCIPER

EN ISO 13850

Nödstoppsutrustning-Konstruktionsprinciper



INGA FÖRÄNDRINGAR EFTER NS-PÅVERKAN

Det tillstånd i vilket maskinen befinner sig efter ett nödstoppskommando skall inte förändras oavsiktligt (oväntat) under den tid som manöveranordningen är i påverkat tillstånd.

ÅTERSTÄLLNING-RESETHANTERING



Återställning av manöveranordningen skall endast vara möjlig som resultat av en manuell påverkan på själva manöveranordningen. Återställning av manöveranordningen skall inte i sig själv framkalla ett återstartskommando. Det skall inte vara möjligt att återstarta maskinen förrän alla manöveranordningar som påverkats har återställts manuellt, individuellt och avsiktligt.

STOPPKATEGORI 0 ELLER 1 (EN ISO 13850-EN 60204-1)

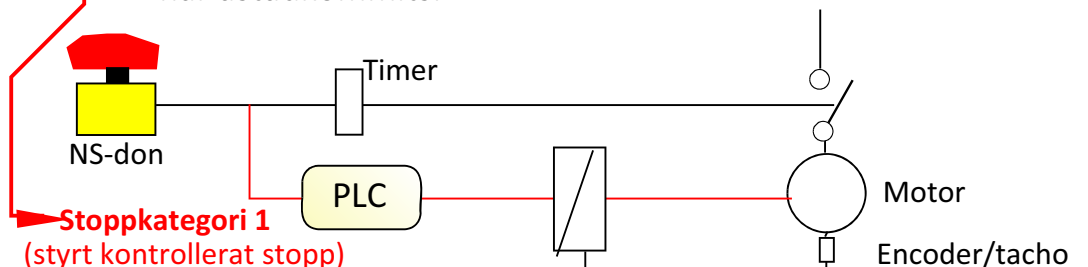
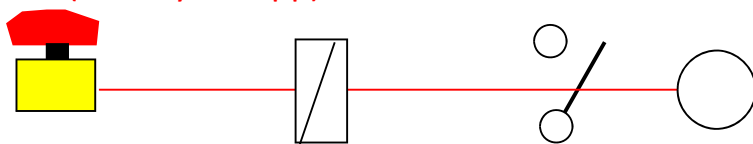
Nödstopp skall fungera antingen enligt **stoppkategori 0** dvs stoppa genom:

- **omedelbart avlägsnande av kraft till drivanordningen (-arna)**

eller mekanisk frångkoppling (urkoppling) mellan de potentiellt farliga delarna och deras drivanordning(-ar) och, om nödvändigt, bromsning (icke styrt stopp)

- **eller enligt stoppkategori 1, dvs styrt stopp** med kraft till drivanordningen(-arna) tillgänglig för att erhålla stoppet och därefter brytning av krafttillförseln när stoppet har åstadkommits.

Stoppkategori 0
(icke styrt stopp)



NÖDSTOPP

Färger och märkning

Ur AFS 2008:13 (92/58/EEG)

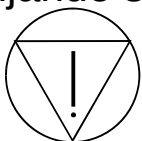
Skyltar och Signaler

5. Färganvisningar avseende skyltar och ljussignaler för hälsa och säkerhet

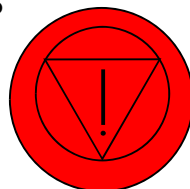
Färg	Betydelse	Användning/information
Röd	Förbud	Farligt beteende
	Larm vid fara	Stopp, stäng, nödstoppsdon*) Utrymningssignal
	Brandbekämpnings- utrustning	Utmärkning och placering
Gul (Orangegul)	Varning	Se upp, vidtag åtgärd, kontrollera
Blå	Påbud	Krav på åtgärd eller beteende Använd personlig skydds- utrustning
Grön	Utrymning, utrymningsväg	Dörrar, utgångar, vägar, utrustning, lokaler
	Förstahjälpen- utrustning	
	Ingen fara	Återgå till det normala

*) Skylt till nödstoppsdon ska vara grön. Om skylten är en del av en nödstoppslina ska den vara röd.

Om symbol tillämpas på nödstoppsdon skall följande symbolmärkning tillämpas



Ur SS EN ISO 13850
Nödstoppsutrustning
konstruktionsprinciper



Skylt till nödstoppsdon ska vara grön.

Nödstoppsdon skall ha röd färg. Om det finns en bakgrund bakom skall den om möjligt ha gul färg (kontrastverkan)

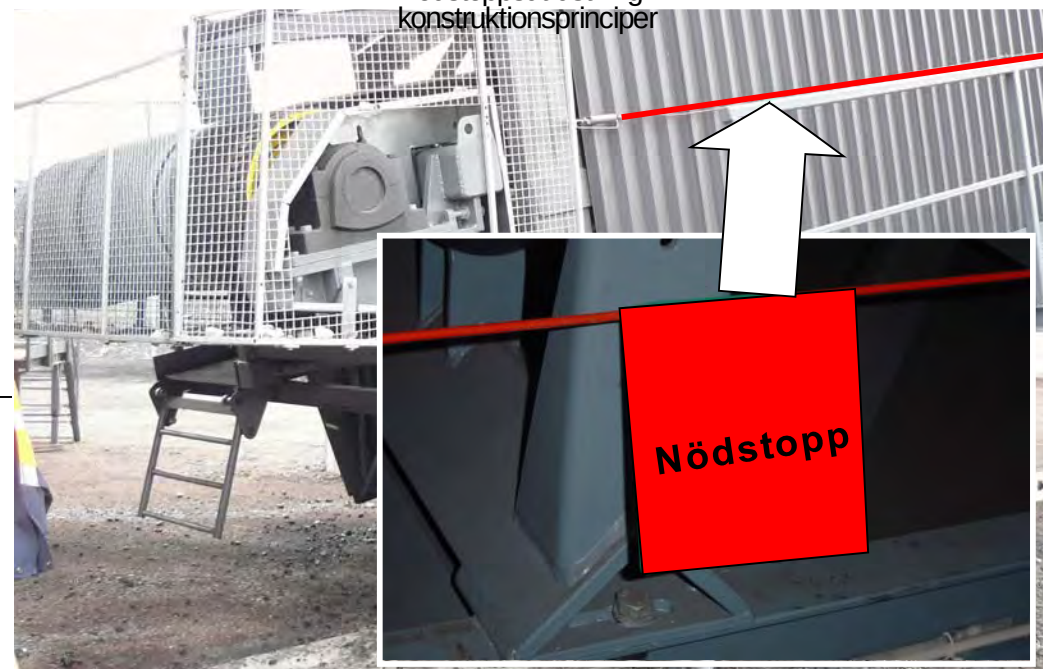
Ur SS EN ISO 13850 Nödstoppsutrustning konstruktionsprinciper



Om skylten är en del av en nödstoppslina ska den vara röd.

Vid användning av linor är det lämpligt att förbättra möjligheten att se dem genom att sätta markörflaggor på dem.

Ur SS EN ISO 13850
Nödstoppsutrustning
konstruktionsprinciper



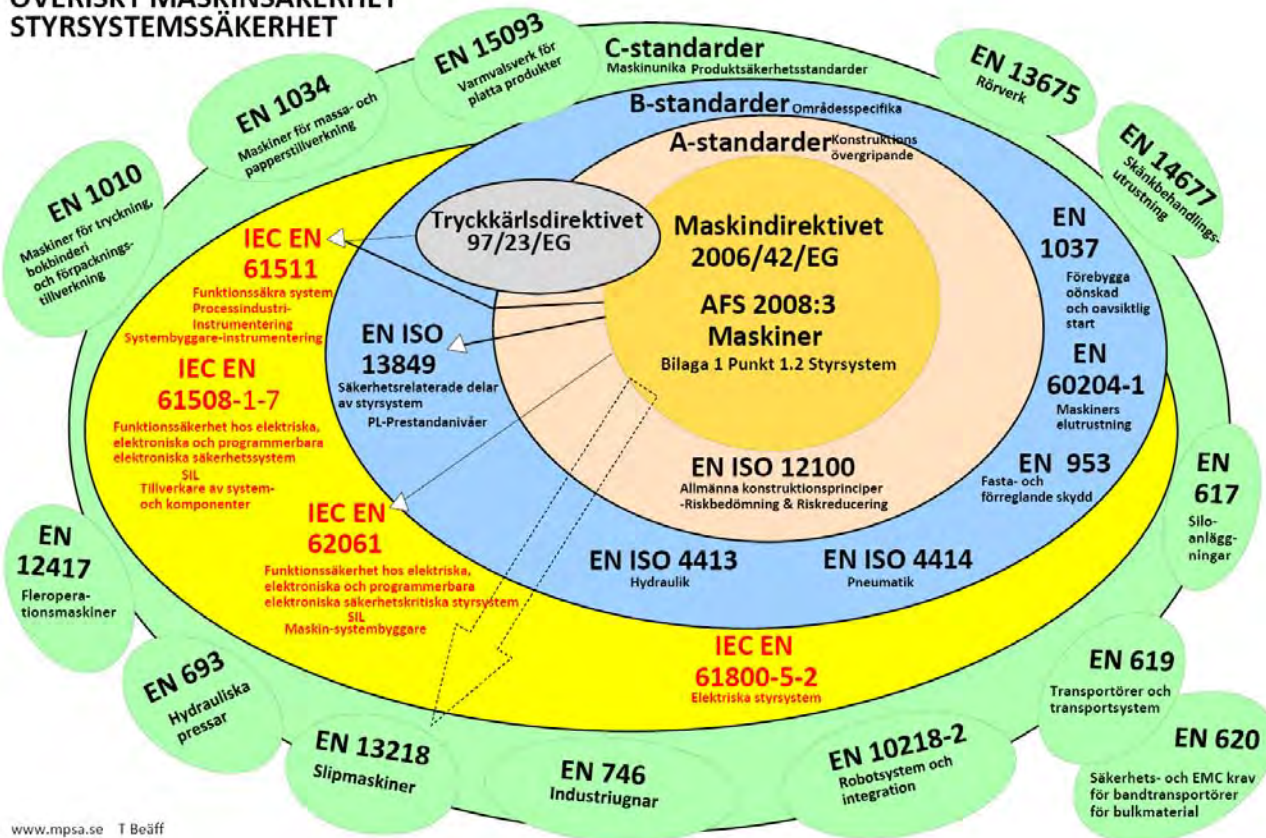
Version november 2013

SÄKERHETSRELATERADE DELAR I STYRSYSTEM

Ett antal standarder finns för att säkerställa att man har kretsar och därtill hörande komponenter som säkerställer en rimlig säkerhetsnivå i förhållande till den aktuella risken utifrån olika direktiv. Finns ingen anledning att skjuta över målet med dyr teknik om inte riskbilden är hög.

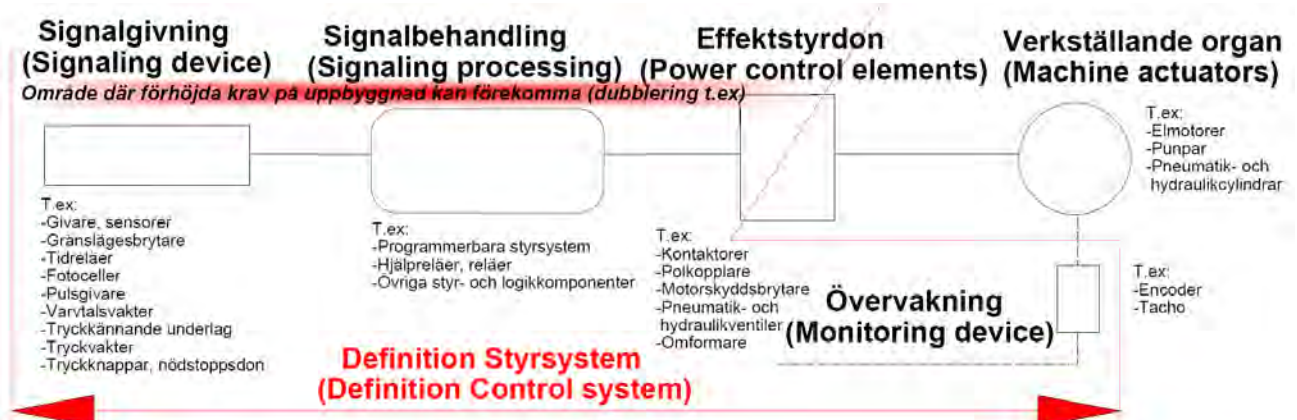
Utöver de legala formella kraven finns ett stort antal standarder som behandlar krav kring säkerhetsrelaterade funktionsstyrningar vilka beskriver mera ingående hur kraven kan uppfyllas. Ur ett maskinsäkerhetsperspektiv med utgångspunkt från att uppfylla säkerhetskraven i bilaga 1 avsnitt 1.2 enligt maskindirektivet 2006/42/EG (I Sverige AFS 2008:3 Maskiner).

ÖVERISKT MASKINSÄKERHET STYRSYSTEMSSÄKERHET



Definition.

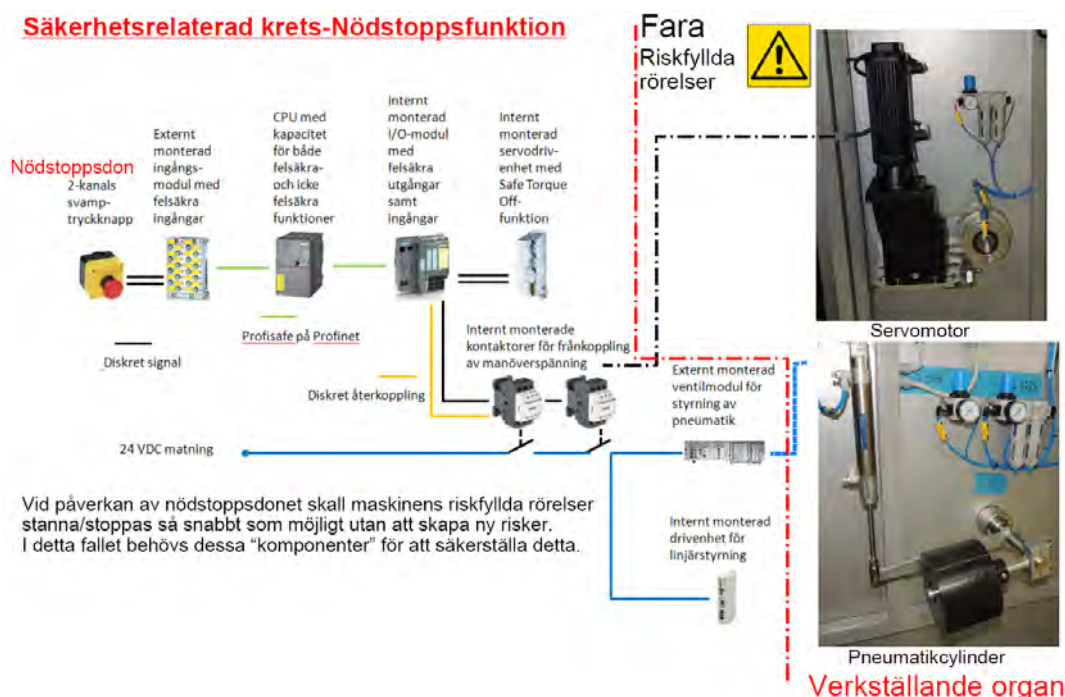
Definitionen av ett styrsystem kan illustreras med denna översiktliga bild ur ett säkerhetsperspektiv.



Säkerhetsrelaterad del i ett styrsystem: del eller underordnad del(ar) i ett styrsystem som svarar på insignaler och genererar säkerhetsrelaterade utsignaler. Kombinationen av säkerhetsrelaterade delar i ett styrsystem börjar där de säkerhetsrelaterade signalerna initieras och slutar vid utgången på effektstyrdonen

Safety-related part of a control system: Part or subpart(s) of a control system which responds to input signals and generates safety-related output signals. The combined safety-related parts of a control system start at the points where the safety-related signals are initiated and end at the output of the power control elements

Säkerhetsrelaterad krets-Nödstoppsfunktion



Historik.

Historiskt sett ur ett säkerhetsperspektiv har man hårdförtrådat säkerhetsrelaterade styrningar i maskin och processtyrningar, användandet av mera tillförlitliga komponenter höjde även nivån ytterligare, mera riskfyllda styrfunktioner krävde även någon form av övervakning för att ha koll på när felet uppträder ofta i kombination med dubblering för att klara enkelfel typ svetsning av kontaktfunktioner, kortslutningar med mera.

Med tiden har man mer och mer gått över till kretslösningar baserade på programmerbar elektronisk utrustning.

A-standarden SS EN ISO 12100 Maskinsäkerhet – Allmänna konstruktionsprinciper – Riskbedömning och riskreducering anger bl.a följande.

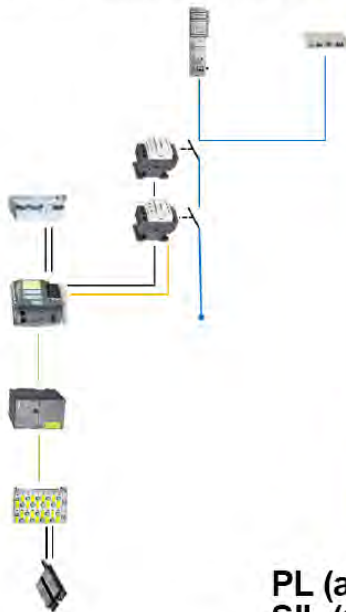
"Ett styrsystem som innehåller programmerbar elektronisk utrustning (t.ex. programmerbara styrdon) kan, när så är lämpligt, användas för utföra skyddsfunktioner hos maskiner. Om ett programmerbart elektroniskt styrsystem används är det nödvändigt att beakta dess prestandakrav i förhållande till kraven på skyddsfunktionerna. Ett programmerbart elektroniskt styrsystem ska vara konstruerat så att det är tillräckligt låg sannolikhet för slumpmässiga fel i hårdvaran och sannolikheten för systematiska fel som ofördelaktigt kan påverka styrsystemets prestanda. Om ett programmerbart elektroniskt styrsystem fullgör en övervakande funktion ska systemets beteende vid detektion av ett fel beaktas.

ANM. Både ISO 13849-1 och IEC 62021 är speciellt framtagna för maskinsäkerhet och ger vägledning som är tillämpbar på programmerbara elektroniska styrsystem. Det programmerbara elektroniska styrsystemet bör vara installerat och validerat för att säkerställa att angivna prestanda [t.ex. säkerhetsintegrerad nivå (SIL - Safety Integrity Level) i IEC 61508] har uppnåtts för varje skyddsfunktion. Validering omfattar provning och analys (t.ex. statisk eller dynamisk analys eller felanalys) för att visa att alla delar samverkar korrekt för att fullgöra skyddsfunktionerna samt att oavsiktliga funktioner inte uppträder

Med tiden och utvecklandet av moderna styrsystemsrelaterade standarder har en mängd variabler införts för att validera och verifiera funktionssäkra styrningar med utgångspunkt bl.a. från helheten och från respektive ingående komponents enskilda tillförlitlighet.

På samma sätt som att fastställa vad en lyftanordning eller lyftredskaps max tillåtna belastning är klassar man numer säkerhetsrelaterade styrningar utifrån vissa kriterier för att fastställa respektive säkerhetsrelaterad krets prestandanivå (PL) alternativt respektive krets säkerhetsintegrerade nivå SIL. Det finns alltså då två olika sätt att göra detta på vilket kan verka lite förvirrande.

Risikbild, hårdvarutillförlitlighet (MTTF-värde), kategori, övervakning, arkitektur, sällsynta feluppträdanden med mera ger den slutliga kretsens säkerhetsklassificering genom erhållen prestandanivå (PL) eller säkerhetsintegrerad nivå (SIL)



**PL (a,b,c,d,e) eller
SIL (1,2,3,4)**

Bl.a säkerhetsfaktor, lyftklass, komponenttillförlitlighet, användningssätt, omgivning-temperatur-miljö ger underlag för lyftredskapets max tillåtna belastning



**F
Max last**

Historik och nutid

	Endast kategorier EN 954-1 (1992)	Kategorier + -DC -CCF -MTTF EN ISO 13849-1	1996 antogs i USA en standard ANSI/ISA S84.01 där implementeringen av processsäkerhetssystem definierades. EN IEC 61508 + sektorstandarder
Enkanaligt std.prylar	Category B	PL a	-
Enkanaligt Bättre tillförlitlighet.	Category 1	PL b	SIL 1
Enkanaligt med övervakning.	Category 2	PL c	
Redundans	Category 3	PL d	SIL 2
Redundans med övervakning	Category 4	PL e	SIL3

PL från 2013 inom EU-EFTA

Stopptyper

Tre stopptyper förekommer normalt i maskiner förutom då säkring i samband med elektriskt och mekaniskt underhåll då "bryt & lås" genom energifrånskiljning och energiavlastning tillämpas.

PRODUKTIONSSTOPP

FÖR ATT SKYDDA PRODUKTEN/DETALJEN ELLER MASKINEN.

EXEMPELVIS MASKINEN STANNAR INTE FÖRRÄN ARBETSCYKELN ÄR KLAR.

ELLER FÖR ATT FÅ ETT SNABBT STOPP UR PRODUKTIONSÄNDAMÅL (SNABBSTOBB) UTAN STÖRRE KRAV PÅ STOPKRETSENS UPBYGGNAD.

PRODUKTIONSSTOPP ÖVERGÅR DOCK I SKYDDSTOPP OM NÅGON BRYTER EXEMPELVIS ETT FÖRREGLANDE SKYDD

SKYDDSTOPP

BRYTER MASKINENS START/STOPPFUNKTION.

- AVSEDD FÖR OMEDVETEN PÅVERKAN I EN RISKSITUATION. (SKALL ALLTSÅ FUNGERA OAVSETT VAD MÄNNISKAN TAR SIG TILL)
- ÄR ETT SÄKERT STOPP SOM GER MÖJLIGHET TILL ENKEL OCH SNABB ÅTERSTART. KAN T.EX ÅTERSTARTAS DÄR ARBETSCYKELN BRÖTS.
- EXEMPEL ÄR FÖRREGLANDE SKYDD, LJUSRIDÅER RUSNINGSSKYDD, BRYTLISTER, TRAMPMATTOR ETC.

NÖDSTOPP

- ENDST AVSEDD FÖR MEDVETEN PÅVERKAN VID RISKSITUATIONER
- NÖDSTOPP FÅR ALDRIG ERSÄTTA VANLIGA SYDDSANORDNINGAR MEN KAN VARA ETT KOMPLEMENT TILL DESSA



Styrsystemskraven

De övergripande formella legala styrsystemskraven finns främst i det så kallade maskindirektivets Bilaga 1 2006/42/EG (AFS 2008:3 Maskiner i Sverige)

Se litet utdrag enligt nedan.

1.2 Styrsystem

1.2.1 Ett styrsystems säkerhet och tillförlitlighet

Ett styrsystem ska vara konstruerat och tillverkat så att riskfyllda situationer inte ska kunna uppstå. Framför allt ska 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 ska 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 ska kunna göras obehindrat.
- Skyddsanordningarna ska fortsätta att vara effektiva fullt ut eller utlösa stoppkommando.
- De säkerhetsrelaterade delarna av styrsystemet ska fungera på ett sammanhängande sätt för en hel grupp av maskiner eller delvis fullbordade maskiner.

För trådlös styrning ska ett automatiskt stopp göras när korrekta styrsignaler inte går fram, inklusive kommunikationsbortfall.

Fel i hård- och mjukvara får alltså inte leda till riskfyllda situationer.

Vidare anges följande

1.2.5 Val av styr- och funktionssätt

Det styrsätt eller funktionssätt som valts ska vara överordnat alla andra styrsätt eller funktionssätt, förutom nödstoppet.

Om en maskin har konstruerats och tillverkats för att kunna styras eller fungera på olika sätt med krav på olika skyddsåtgärder och/eller arbetsrutiner, ska den vara försedd med en väljare för styrsätt eller funktionssätt som kan låsas i varje enskilt läge. Varje läge på väljaren ska vara tydligt angivet och endast motsvara ett styr- eller funktionssätt.

Väljaren kan ersättas av annan anordning som gör det möjligt att begränsa användningen av vissa maskinfunktioner till särskilda operatörskategorier.

Om maskinen för vissa funktioner ska kunna användas med ett skydd flyttat eller avlägsnat eller med en skyddsanordning satt ur funktion, ska väljaren för styr- eller funktionssätt samtidigt

- omöjliggöra alla andra styr- eller funktionssätt,

- tillåta drift av riskfyllda funktioner endast med hålldonsmanöveranordning,
- tillåta drift av riskfyllda funktioner endast under förhållanden där riskerna är begränsade, samtidigt som riskkällor som kan uppstå till följd av sekventiella förlopp förhindras,
- förhindra att riskfyllda funktioner uppkommer genom avsiktlig eller oavsiktlig påverkan på maskinens givare.

Om dessa fyra villkor inte kan säkerställas samtidigt, ska väljaren av styrsätt eller funktionssätt aktivera andra skyddsåtgärder som är konstruerade och tillverkade så att ett säkert arbetsområde garanteras.

Dessutom ska operatören från det ställe där han/hon utför arbete kunna styra driften av de delar han/hon arbetar med.

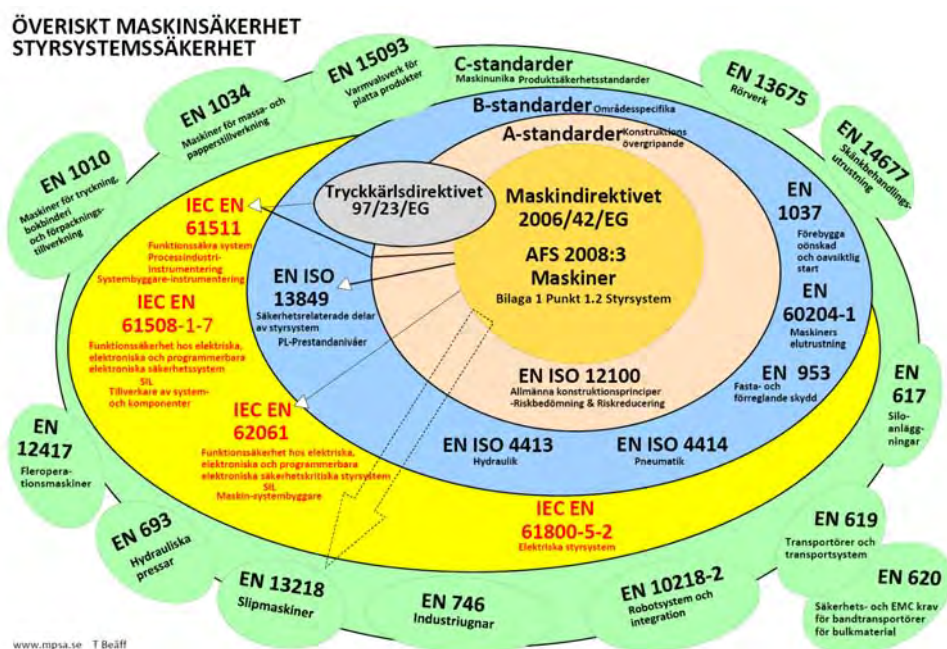
1.2.6 Fel i kraftförsörjningen

Avbrott, återställning efter avbrott eller variationer i kraftförsörjningen till maskinen får inte leda till riskfyllda situationer.

Särskild uppmärksamhet ska ägnas följande punkter:

- Maskinen får inte starta oväntat.
- Maskinens parametrar får inte ändras på ett okontrollerat sätt, om en sådan ändring kan ge upphov till riskfyllda situationer.
- Maskinen får inte hindras från att stoppa 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 ska kunna ske utan hinder.
- Skyddsanordningarna ska fortsätta att vara effektiva fullt ut eller utlösa stoppkommando.

För att tolka ut hur dessa mer formella och legala "styrsystemskrav" skall tillämpas har det då tagits fram ett antal standarder kopplade till direktiven tillika de nationella föreskrifterna för att tydliggöra vad det innebär på ett mera praktiskt sätt vilket framgår av den inledande bilden i detta dokument.

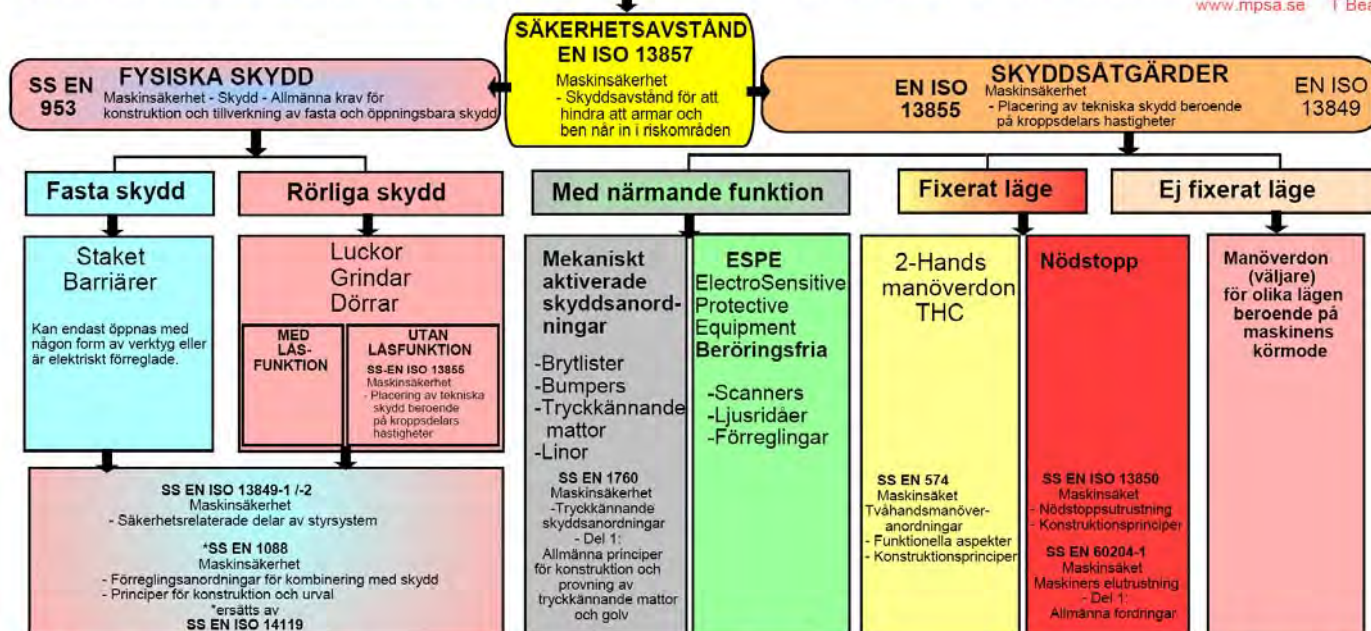


Innan respektive styrkrets valideras med avseende på tillförlitligheten genom så kallad PL-klassning eller SIL-klassning måste man först utifrån en riskbedömning inse behovet av en skyddslösning och sedan välja den eller de lösningar som situationen kräver vilket då på bäst sätt möjliggöres genom att tillämpa relevanta standarder inom området vilket kan illustreras enligt följande översikt.

Viktigt att beakta att det oftast finns många olika lösningar på samma problem.

SAKERHETSTEKNISKA SKYDDSÅTGÄRDER-MASKINER UTIFRÅN RISKBEDÖMNING

www.mpsa.se T Beäff



SÄKERHETSKOMPONENTER LISTAS I BILAGA 5 I MASKINDIREKTIVET

*SÄKERHETSKOMPONENTER

*säkerhetskomponent: en komponent
– som fullgör en säkerhetsfunktion,
– som släpps ut på marknaden separat,
– som om den inte fungerar eller fungerar dåligt utgör risk för personers säkerhet, och
– som inte är nödvändig för att maskinen ska fungera eller som kan ersättas med normala komponenter för att maskinen ska fungera.

2006/42/EC Bilaga 5

Säkerhetskomponenter skall vara CE-märkta



Säkerhetskomponenter är endast komponenter som huvudsakligen har en direkt säkerhetsfunktion ska anses vara säkerhetskomponenter i maskindirektivets mening och när den användes och för vilken fel eller felfunktion medför fara för utsatta personers hälsa- och säkerhet.

Exempelvis:

nödstoppsanordningar

säkerhetsbälten

rök- eller dammsugssystem till maskiner

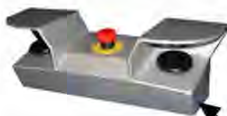
skydd och deras festsättningsanordningar

bullerskydd

skydd mot urspårning

överlastskydd

tvåhandsmanöveranordningar



1. Skydd för avtagbara mekaniska kraftöverföringsanordningar.
2. Skyddsanordningar för detektering av personer.
3. Motordrivna förreglande öppningsbara skydd avsedda att användas som skyddsanordningar i sådana maskiner som avses i bilaga 4, punkterna 9, 10 och 11. 4.
4. Logikenheter för skyddsfunktioner på maskiner.
5. Ventiler med funktioner för feldetektering och som är avsedda för styrning av farliga rörelser i maskiner.
6. Utsugningssystem för utsläpp från maskiner.
7. Skydd och skyddsanordningar för att skydda utsatta personer mot rörliga delar som är direkt involverade i en maskins användning.
8. Anordningar för övervakning av last och rörelse på lyftande maskiner.
9. Anordningar för att hålla kvar personerna på säten.
10. Nödstoppsanordningar.
11. Urladdningssystem för att förhindra att potentiellt farliga elektrostatiska laddningar uppstår.
12. Energibegränsare och avlastningsanordningar enligt bilaga 1, punkterna 1.5.7, 3.4.7 och 4.1.2.6. 13.
13. System och anordningar för att minska emission av buller och vibrationer.
14. Överrullningsskydd (ROPS). Roll Over Protection Structure (ROPS)
15. Skydd mot fallande föremål (FOPS). Falling object protective structures (FOPS)
16. Tvåhandsmanöverdon.
17. Följande komponenter för maskiner som är avsedda att lyfta eller sänka personer mellan olika stannplan:
 - a) Anordningar för att låsa dörrar på stannplan.
 - b) Anordningar för att hindra den lastbärande enheten från fall eller okontrollerad uppgående rörelse.
 - c) Hastighetsbegränsande anordningar.
 - d) Energiackumulerande stötdämpare, – icke-lineära eller – med dämpning av returrörelsen.
 - e) Energiabsorberande stötdämpare.
 - f) Säkerhetsanordningar på cylindrar till hydrauliska kretsar när dessa används för att förhindra fall.
 - g) Elektriska skyddsanordningar i form av brytare med säkerhetsfunktion innehållande elektroniska komponenter.

KRAV KRING SÄRSKILT FARLIGA MASINER SOM LISTAS I BILAGA 4

Gällande styranknutna anordningar förutom alla de så kallade farliga maskiner som listas i maskindirektivets bilaga 4 där särskilda kontrollkrav föreligger av anmälda organ om inte en specifik C-standard tillämpas, se bl.a punkterna 19 och 21 som inbegriper.

19. Skyddsanordningar för detektering av personer.

21. Logikenheter för skyddsfunktioner.

Exempel på ett EG typintyg utfärdat av anmält organ rörande logikenheter för skyddsfunktioner (ligger då till grund för tillverkarens utfärdande av Försäkran om överensstämmelse för aktuell säkerhetsrelaterad logikenhet).

DEKRA

(1) EC-Type Examination Certificate

(2) Directive 2006/42/EG of the European Parliament and of the Council on Machinery

(3) No. of EC-Type Examination Certificate: **ZP/C094/12**

(4) Product: **LKAB signaling system ATP as part of AOS_IF150 mounted on the locomotives KR250LA001, KR250LA002, KR250LA003 for use in underground mining for transport level 1365 LKAB**

(5) Manufacturer: **Bombardier Transportation Sweden AB**

(6) Address: **Arstaängsvägen 29, Marievik
12616 Stockholm
SWEDEN**

(7) The design and construction of this machine and any acceptable variation thereto are specified in the schedule to this type examination certificate.

(8) The certification body of DEKRA EXAM GmbH, Notified Body No. 0158 according to Article 14 of Directive 2006/42/EC of the European Parliament and the Council of 17 Mai 2006, certifies that this machine has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of machinery, given in Annex I to the Directive. The examination and test results are recorded in the test and assessment report No. 2473NN40.

(9) The Essential Health and Safety Requirements are assured by compliance with
DIN EN ISO 13849-1:2008 DIN EN ISO 13849-2:2008

(10) This EC-Type Examination Certificate relates only to the design, examination and tests of the specified equipment in accordance to Directive 2006/42/EC. Further requirements of the Directive apply to the manufacturing process and supply of this equipment. These are not covered by this certificate.

(11) This EC-Type Examination certificate is valid until 2013-09-28.

DEKRA EXAM GmbH
Bochum, 2013-03-28

[Signature]
Certification body

[Signature]
Special services unit

Page 1 of 3 ZP/C094/12
This certificate may only be published in its entirety and without any change.
DEKRA EXAM GmbH, Dinnendahlstrasse 9, 44809 Bochum, Germany, telephone +49.234.3696-105, fax +49.234.3696-110, zs-exam@dekra.com

MASKINER TILLVERKADE FÖRE 1995 OCH STYRSYSTEMSKRAV KRING DESSA (2009/142/EG I Sverige AFS 2006:4)

Styrsystemskrav finns även för arbetsutrustning generellt och rent praktiskt kan man säga att följande krav gäller formellt för maskiners styrsystem ut användarsynpunkt allmänt samt tekniska minimikrav för styrsystem tagna i drift före 1995.

Bilaga A AFS 2006:4

A 2.3 Manöveranordningar och styrsystem

Manöveranordningar på arbetsutrustning skall, om de kan påverka säkerheten, vara klart synliga och identifierbara och, där så är nödvändigt, vara märkta på ett ändamålsenligt sätt.

Om det är möjligt skall manöveranordningarna vara placerade utanför riskområden. De skall också vara placerade så att det inte medför några risker vid handhavandet. De får inte ge upphov till risker på grund av en oavsiktlig manöver.

Om säkerheten kräver att manövrer utförs i en viss ordning skall det finnas blockeringar (förreglingar) som hindrar att de utförs i fel ordning eller på annat sätt vara säkerställt att de inte går att utföra i fel ordning.

Om det behövs skall operatören från huvudmanöverplatsen kunna förvisa sig om att det inte finns någon inom riskområdena. Om det inte går skall det finnas ett säkert varningssystem, som före varje start automatiskt avger en ljud- och/eller ljussignal. Den som helt eller delvis befinner sig inom riskområdet skall ha tid och möjlighet att snabbt undgå risker som beror på att arbetsutrustningen startar eller stoppar.

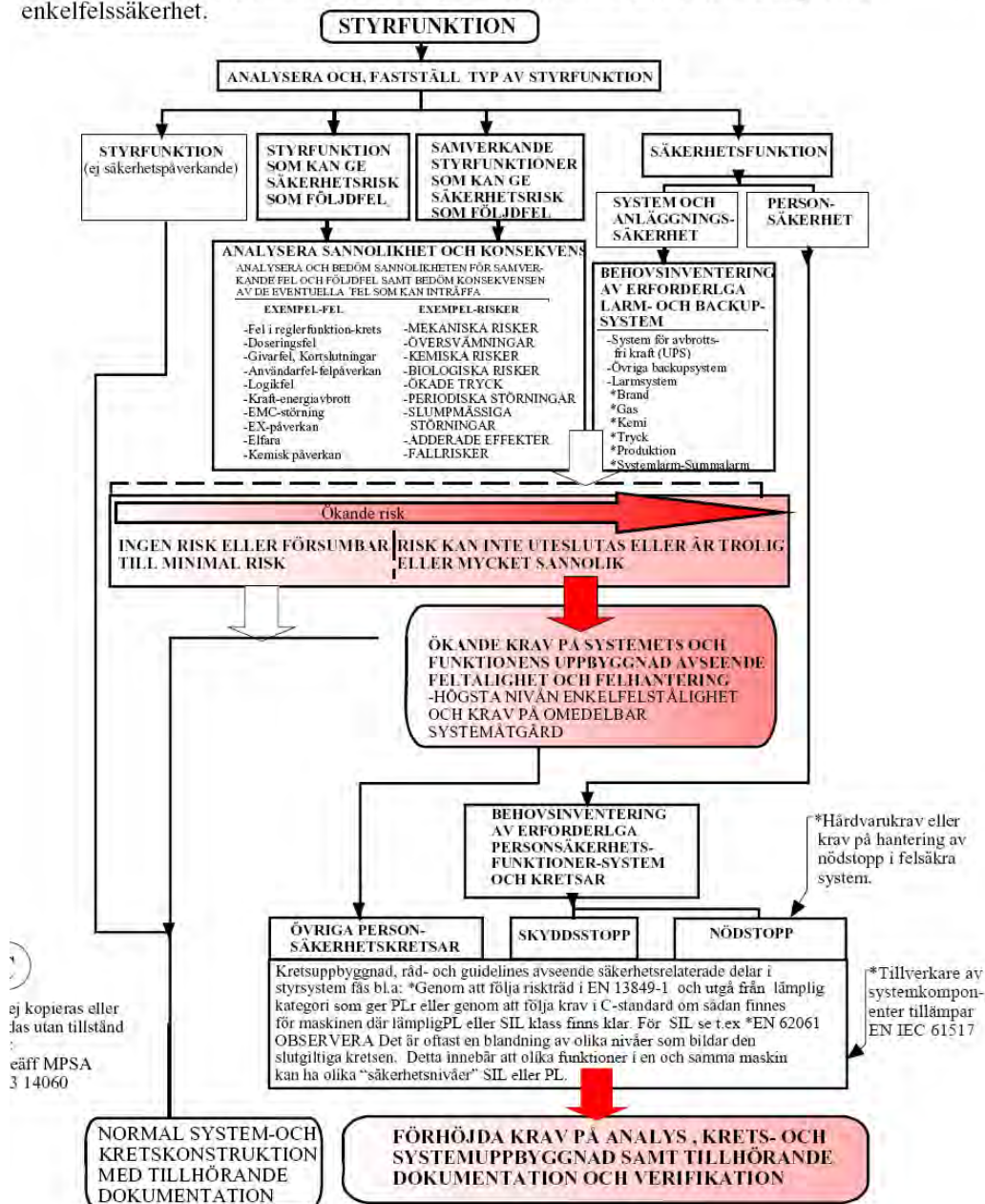
Styrsystem skall vara säkra och utförda med tanke på de fel, störningar och påfrestningar som kan förutses.

Om en enhet i en arbetsutrustning kan startas och stoppas separat skall styrsystem och skyddsanordningar vara utförda så att detta kan ske under säkra förhållanden.

VISSA STYRFUNKTIONER MÅSTE HA HÖGRE SÄKERHETSKRAV

STYRFUNKTIONER PRODUKTION-PERSONSÄKERHET

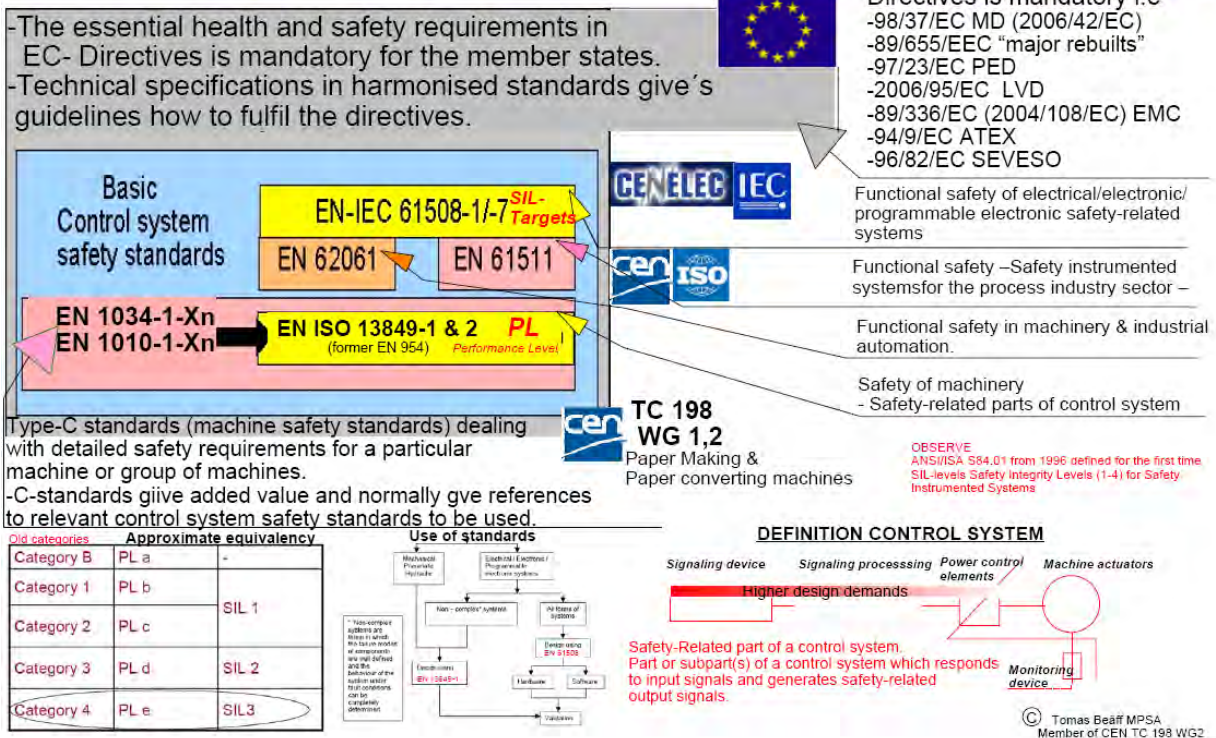
Nedanstående bild visar ett översiktsschema av styrfunktioner där man kan få en god överblick av vad det är för funktioner man avser i sin maskin eller process och hur man kan hantera dessa beroende på de risker som kan uppkomma för respektive funktion. Som bilden visar är schemat uppdelat i en direkt säkerhetsfunktion (till höger) med personsäkerhetsfunktioner i form av nödstopp och skyddsstopp samt en väg för system- och anläggningssäkerhetssystem. Till vänster finns produktions styrfunktionerna som normalt inte är konstruerade med avseende på personsäkerheten utan endast för att realisera produktionsfunktioner. I mitten finns produktionsstyrfunktioner som i vissa situationer kan ge säkerhetsrisker. Dessa funktioner är oftast svåra att analysera och bedöma och om behov finns att konstruera kretsarna med en högre säkerhetsnivå med övervaknings eller enkelfelssäkerhet.



ej kopieras eller
fås utan tillstånd
eäff MPSA
3 14060

STANDARDS SOM ETT HJÄLPMEDEL ATT UPPFYLLA DE LEGALA KRAVEN

CONTROL SYSTEM STANDARDS-SAFETY



Ett antal olika standarder finns för att uppfylla de säkerhetskrav som utgår ifrån föreskrifter för olika områden. För maskiner rör det sig huvudsakligen om SS EN ISO 13849-1 (Prestandanivåer PL) och IEC EN 62061 om Silklasser, på sikt avses dessa slås ihop till en gemensam.

Observera att många (men långt ifrån alla) specifika maskinstandarder så kallade C-standarder redan normalt klassificerat relevanta säkerhetsnivåer enligt SIL alternativt PL som är de moderna klassificeringsnivåerna på säkerhetsrelaterade delar.
Se exempel sist i detta dokument.

Typ standarder för maskiner med likvärdig hantering slås ihop på sikt.

Sammanslagning av EN ISO 13849-1 (Prestandanivåer PL) och IEC EN 62061 (Sektorstandarden för maskiner för fastställande av SIL) fortskrider. En arbetsgrupp jobbar på en gemensam text att föras in som en bilaga i båda standarderna.

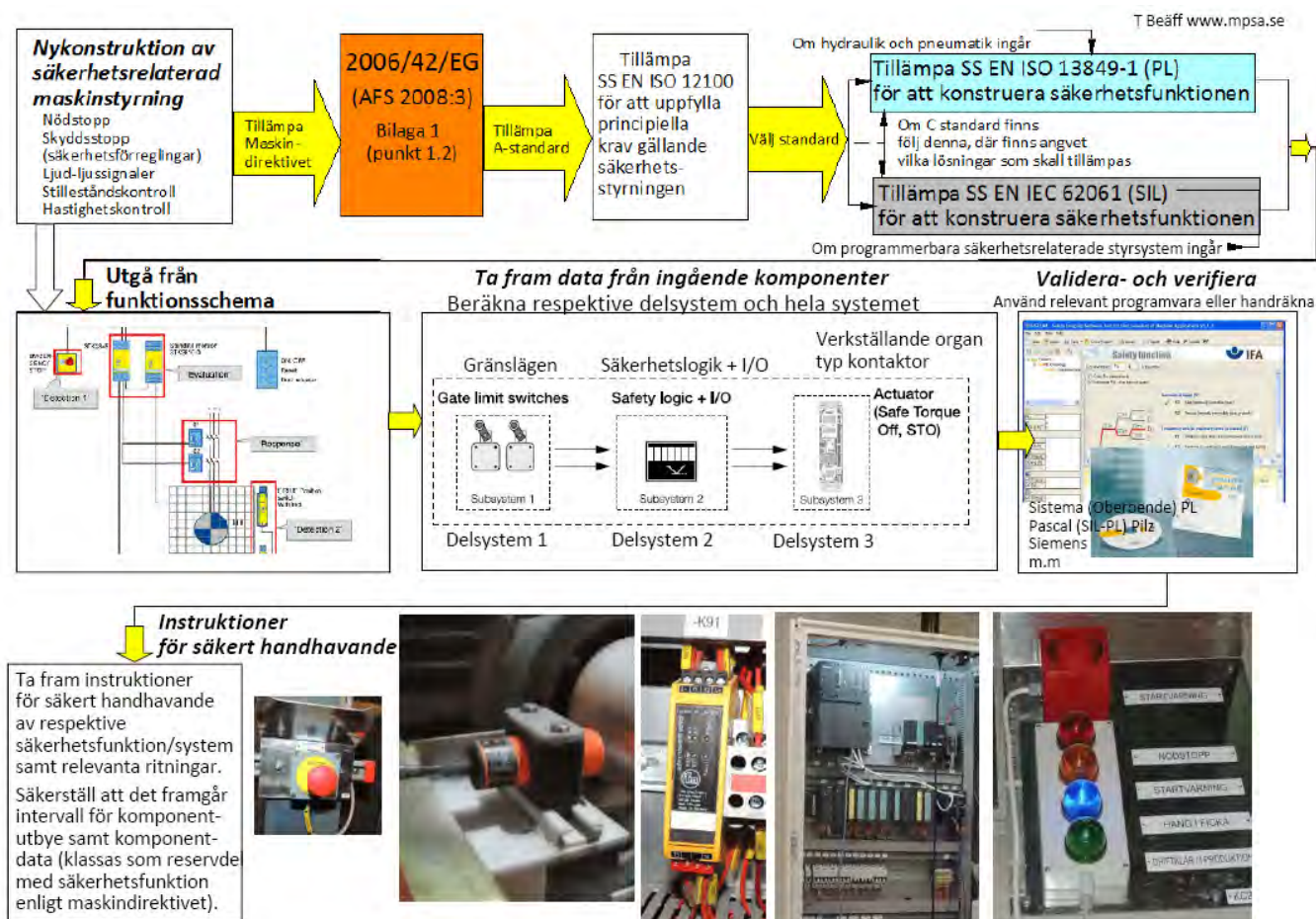
Några önskar att man därefter låter standarderna vara orörda ett tag så att användarna kan bilda sig en uppfattning om dem och därefter kan en sammanslagning till en standard påbörjas. Omkring 2016 räknar man med att en sammanslagning av standarderna vara genomförda.

PRINCIPIELL VÄG FÖR ATT KONSTRUERA FUNKTIONSSÄKRA STYRNINGAR

Följande principiella väg kan tillämpas för att säkerställa en relevant validering och verifiering i samband med konstruktion av säker maskinstyrning.

De formella kraven finns i föreskrifter (utgående från EU-direktiv) utfärdade med stöd av lagar och förordningar medans de detaljerade kraven återfinns i harmoniserade standarder som är vägledande för att uppfylla föreskrifternas krav.

Gällande maskiner utgår då styrsystemskraven utifrån maskindirektivet och dess Bilaga 1.



Sätt 1 PL-klassning

SS EN ISO 13849-1 Säkerhetsrelaterade delar i styrsystem

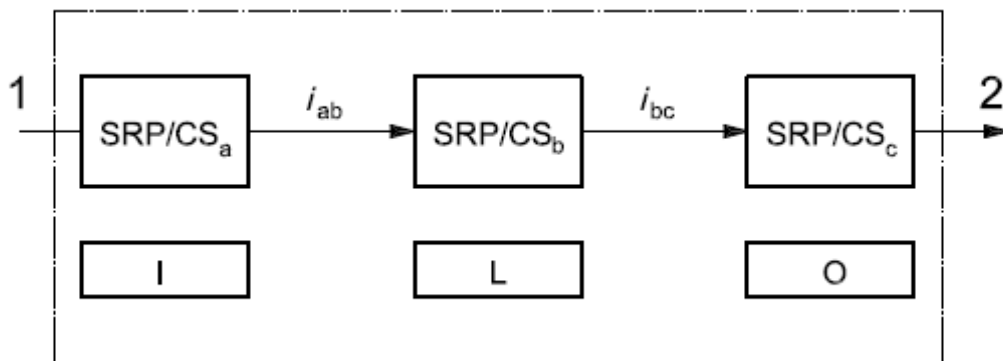
Maskinsäkerhet – Styrssystem – Säkerhetsrelaterade delar i styrsystem

-Del 1 Generella krav

-Del 2: Validering

(Safety-related parts of control systems)

Säkerhetsrelaterad del i ett styrsystem SRP/CS(Safety Related Parts/Control System)del i ett styrsystem som svarar på säkerhetsrelaterade insignaler och genererar säkerhetsrelaterade utsignaler



Förklaring

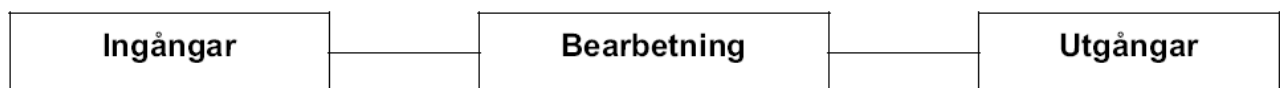
I ingång

L logik

O utgång

1 initierande händelse (t.ex. manuellt aktivera en tryckknapp, öppna ett skydd, bryta stråle i en AOPD)

2 drivanordning (t.ex. motorbromsar)



Ingångsblock

Registrering av information från de olika säkerhetsgivarna genom säkerhetsingångar

Bearbetningsblock

Erforderlig bearbetning för att realisera skyddsfunktionerna som leder till ett säkert tillstånd

Utgångsblock

Styrning av drivanordningarna genom säkerhetsutgångar

FRÅN EN 954-1 till EN ISO 13849-1

Efterföljaren EN ISO 13849-1 är en utveckling av den tidigare numer upphörda standarden EN 954-1 den med kategorierna tillämpas för alla skyddsfunktioner (mek-el-hydraulik-pneumatik) upp till högsta nivån kallad PL e. Från början gällde att man under en övergångsperiod fram till 1 november 2009 kunde tillämpa både den gamla EN 954 samt efterföljaren EN ISO 13849 inom EES, sedan skulle den senare tillämpas.

I sista stund innan nya maskindirektivet infördes 29/12 2009 och efter påtryckningar från maskinkommitten där representanter från medlemsländernas myndigheter sitter med beslutades om en förlängning med tre år där den "gamla EN 954-1 fick tillämpas parallellt med efterföljaren tom utgången av 2011.

Sammanfattningsvis

- Referenser. till gamla EN 954-1 fick åberopas fram t.o m den 31 december 2011.
- (SS) EN 954-1 är en tillbakadragen standard i EU:s officiella tidning OJ.
- Dock gäller att EN 954-1 fortsättningsvis får tillämpas i de fall man åberopar C-standarder och dessa inte är uppdaterade med aktuella SIL och PL nivåer, fram då tills aktuell C-standard uppdaterats.

Principiellt

- EN ISO 13849-1 används för elektronik, mekanik, pneumatik och hydraulik
- konstruktörer av traditionella säkerhetsreläer kan även tillämpa 13849-1
- konstruktörer av säkerhets-PLC:er skall dock tillämpa EN IEC 61508
- maskin- och kretsbyggare för maskiner kan använda EN ISO 13849-1 oavsett om man använder traditionella säkerhetsreläer eller säkerhets-PLC, dock ej för PL=e

Problem med den gamla EN 954-1 var att den

- behandlade inte programmerbara eller komplexa elektroniska system
- beaktade inte komponenternas tillförlitlighet (kvalité)
- kategorierna var inte hierarkisk strukturerade
 - fel i kategori 1
 - komplexitet var inte beaktat

SS-EN ISO 13849 täcker in skyddsanordningar, styrenheter och effektstyrdon och grundar sig på en bedömning av sannolikhet. Närmare bestämt bedömer man hur stor sannolikheten är att ett farligt fel inträffar hos alla de komponenter som ingår i en skyddsfunktion under en timme. Tillförligheten hos skyddsfunktionen anges med måttet Performance Level, PL.

Standarden omfattar (Källa vissa utdrag ur BIA-rapport)

Kategorierna präglas genom att säkerhet fås genom

- bra komponenter ("fel kan uteslutas")
- övervakning ("kontrollera periodiskt")
- feltålighet ("klarar ett eller flera fel")

- Mekaniska system
- Hydrauliska system
- Pneumatiska system
- Elektriska system
- Elektroniska system
- Programmerbara elektroniska system

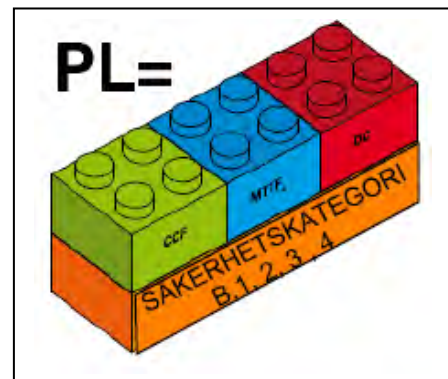
- låg risk
- fullständigt beteende kartlagt och bestämt
- låg medverkan
- diversifierad (HW, OS, SW)
- tillämpliga standarder används (t.ex EN 61508)

Prestandanivån (Säkerhetsnivån) bestäms utifrån följande kriterier

PL: Kapaciteten hos SRP/CS-systemets (Safety related Programmable Control System) prestationsförmåga att uppfylla den förväntade riskreduktionen. Förr var det bara kategoriseringen (B-1-2-3-4) som fastställde nivån utifrån aktuell riskbild nu skall många variabler förutom detta beaktas för att fastställa PL

PL bestäms av:

- Kategori
- $MTTF_d$ - Mean Time to Dangerous Failure
- DC - Övervakningsfunktion/-system
- CCF - Samverkande fel
- Mått/krav för systematiska fel



* $MTTF_d$ För varje enskild komponent (hårdvarutillförlitlighet)

*DC Diagnostic coverage (i hur hög grad farliga fel uppnås)

*CCF Common Cause failure –åtgärder blir relevanta när man arbetar med någon form av redundans eller övervakning (Feltålighetskategorierna 2-4)

En bestämd arkitektur kan motsvaras av en hel skyddsfunktion eller del därav, t ex en ljusridå, scanner eller ett säkerhetsrelä

Vad är prestandanivå

Prestandanivå PL (Performance Level) kvantifierad nivå som används för att ange förmågan hos säkerhetsrelaterade delar i styrsystem att utföra en skyddsfunktion under förutsebara förhållanden

Prestandanivån PL

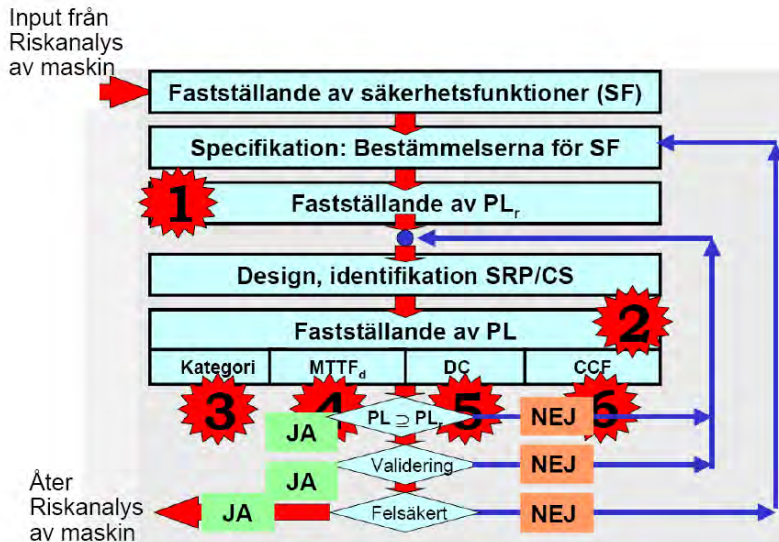
PL	Genomsnittlig sannolikhet för farlig felfunktion per timme 1/h
a	$\geq 10^{-5}$ till $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ till $< 10^{-5}$
c	$\geq 10^{-6}$ till $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ till $< 10^{-6}$
e	$\geq 10^{-8}$ till $< 10^{-7}$
ANM. Förutom den genomsnittliga sannolikheten för farlig felfunktion per timme måste också andra åtgärder vidtas för att uppfylla prestandanivån PL.	

Detta blir rent praktiskt

$10^{-4} \approx$	1 farlig felfunktion per år
$10^{-5} \approx$	1 farlig felfunktion per 10 år
$10^{-6} \approx$	1 farlig felfunktion per 100 år
$10^{-7} \approx$	1 farlig felfunktion per 1000 år

PL i det säkerhetsrelaterade programbara styrsystemet (SRP/CS) baseras förutom på MTTFd värdet på enskilda komponenter, DC värdet, CCF värdet, kategorin (strukturen typ enkanalighet, enkanalighet med övervakning, tvåkanalighet) tillkommer parametrar som säkerhetsfunktionens beteende vid felförhållanden, säkerhetsrelaterad programvara, systemfel samt förmågan att utföra/fullgöra en säkerhetsfunktion under förväntade miljöförhållanden.

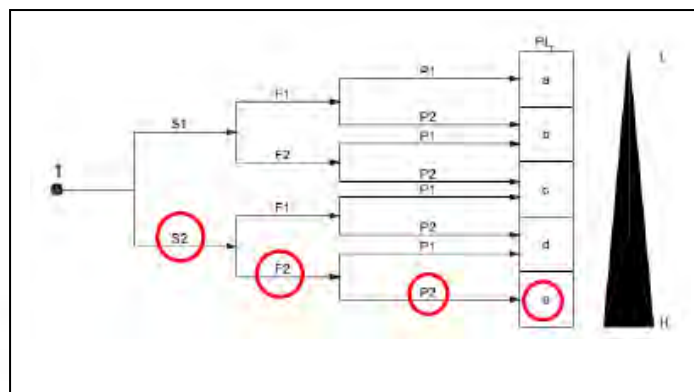
Fastställa PL



1. Riskanalys genom att använda riskgrafen i standarden

För att fastställa aktuell Prestandanivå för en säkerhetsrelaterad funktion finns i standarden ett riskträd. Alternativet till riskträdet är att följa en fastställd nivå utifrån en maskinspecifik C-standard där denna bedömning redan är gjord.

S är skadans allvarighet,
 F är frekvensen eller exponeringen vid riskkällan
 P är möjligheten att undvika riskkällan



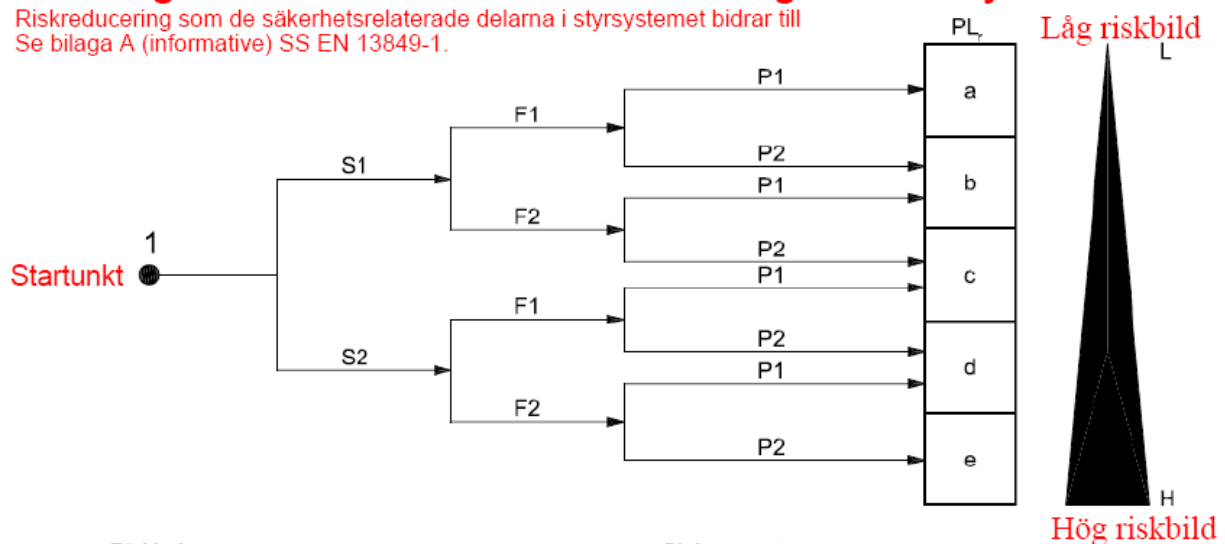
Fastställande av nödvändig prestandanivå (PL)

- S** – Skadans svårighetsgrad
- S₁** – Lätt (ej bestående skada)
- S₂** – Allvarlig (normalt bestående skada inklusive dödsfall)
- F** – Frekvens och/eller exponering för en risk
- F₁** – Sällan till mindre ofta och/eller kort exponeringstid
- F₂** – Frekvent till kontinuerlig och/eller lång exponeringstid
- P** – Möjlighet att undvika risk eller begränsa skadan
- P₁** – Möjligt under specifika förhållanden
- P₂** – Sällan möjligt

Mera ingående att beakta för att fastställa PL behövd nivå (PL_r (r=required))

Riskdiagram för fastställande av erforderlig PLr för skyddsfunktion

Riskreducering som de säkerhetsrelaterade delarna i styrsystemet bidrar till
 Se bilaga A (informative) SS EN 13849-1.



Förklaring

- 1 startpunkt för utvärdering av en skyddsfunktionens bidrag till riskreduceringen
- L lågt bidrag till riskreduceringen
- H högt bidrag till riskreduceringen
- PLr erforderlig prestandanivå

Riskparametrar:

- S skadans allvarighet
- S1 lätt (vanligtvis övergående skada)
- S2 svår (vanligtvis obotlig skada eller dödsfall)
- F frekvens och/eller exponeringstid för riskkällan
- F1 sällan till mindre ofta och/eller kort exponeringstid
- F2 ofta till kontinuerlig och/eller lång exponeringstid
- P möjlighet att undvika riskkällan eller begränsa skadan
- P1 möjligt under vissa omständigheter
- P2 knappast möjligt

S1 eller S2

Skadans allvarighet, S1 och S2 Vid uppskattning av den risk som uppkommer vid felfunktion hos en skyddsfunktion beaktas endast lätta skador (vanligtvis övergående) och svåra skador (vanligtvis bestående) och dödsfall.

För att fatta beslut bör man ta hänsyn till de vanliga konsekvenserna av olyckor och normala läkeprocesser vid fastställande av S1 och S2.

Exempelvis klassas blåmärken och/eller rivsår utan komplikationer som S1, medan amputation eller dödsfall klassas som S2.

F1 eller F2

F2 bör väljas om en person ofta eller kontinuerligt exponeras för riskkällan

Exponeringstiden för riskkällan bör uppskattas på grundval av ett medelvärde, som kan sättas i relation till den totala tidsperiod som utrustningen används. Till exempel, om det är nödvändigt att regelbundet nå in mellan verktygen på maskinen under cyklisk drift för att mata och flytta arbetsstycken bör F2 väljas.

Om tillgänglighet endast krävs då och då kan F1 väljas.

ANM. Om det inte finns någon annan motivering bör F2 väljas, om frekvensen är högre än en gång per timma.

P 1 eller P 2

Till exempel är det viktigt att beakta om riskkällan direkt kan identifieras genom sina fysiska egenskaper eller endast genom tekniska åtgärder som t.ex. indikeringsanordningar.

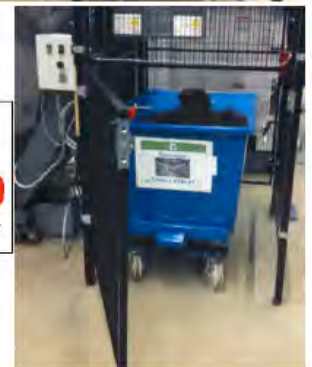
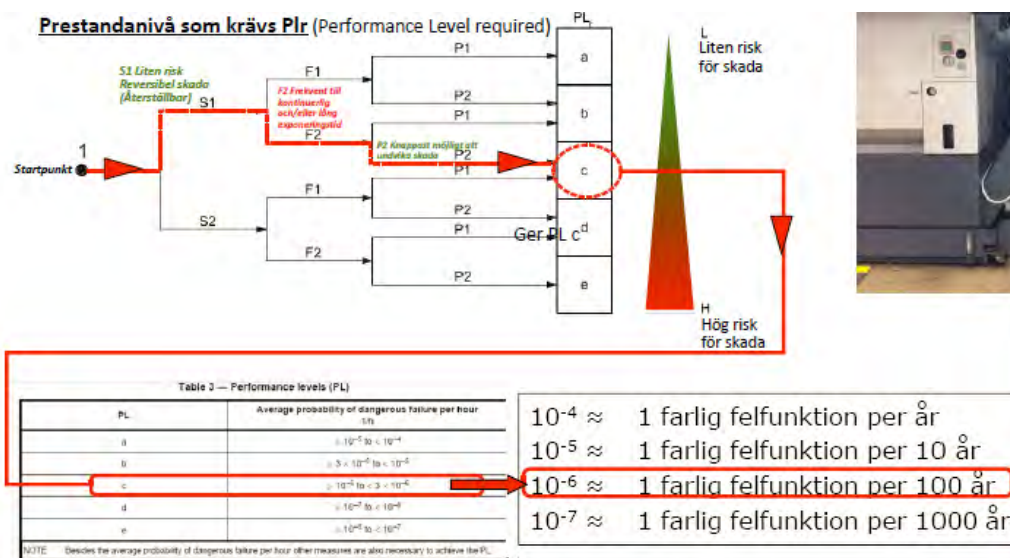
Andra viktiga faktorer som påverkar valet av parameter P är till exempel:

- drift med eller utan övervakning;
- om driftspersonalen är experter eller icke yrkesutbildade;
- den hastighet med vilken risksituationen uppstår (t.ex. snabbt eller långsamt);
- möjligheter att undvika skada (t.ex. genom flykt);
- praktiska erfarenheter av säkerhet i samband med processen.

När en riskfylld situation uppstår bör P1 endast väljas om det finns en realistisk möjlighet att undvika en olycka eller att väsentligt minska dess konsekvens.

P2 bör väljas om det nästan inte finns någon möjlighet att undvika att skadas.

Exemplet nedan visar vilken prestandanivå man bedömer behövas (PLr) för säkerhetskretsen bestående av en förreglingsbrytare på grind in till en spåntransportör som via kontaktor frånskiljer drivmotorn till spåntransportören vid vistelse för hantering av spånbinge i riskområdet.



T Beäff 2012

Eller då tillämpa färdig bedömning i harmoniserad C-standard för aktuell maskin om sådan finns.

2

Fastställande av PL			
Kategori	MTTF _d	DC	CCF
3	4	5	6

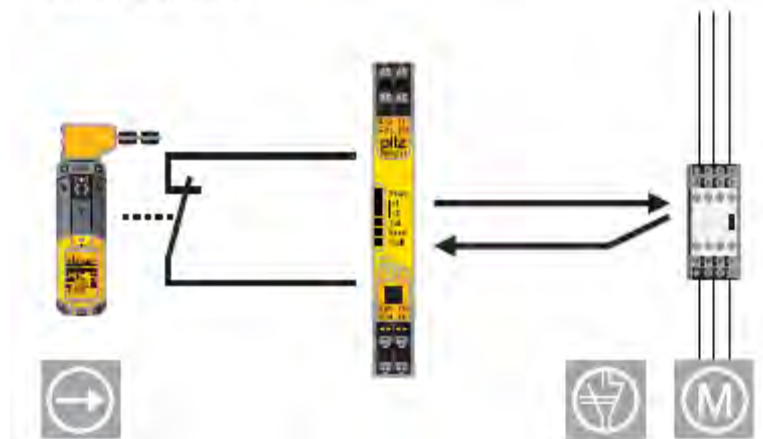
Följande 4 delar skall ingå för fastställande av Prestandanivån
 Kategorin, MTTF d
 MTTF= Medeltid till felfunktion
 MTTF d= Medeltid till farlig felfunktion

Grundkategorierna (feltålighetskategorierna B,1,2,3,4) kvarstår sedan tidigare och har kompletterats med mera variabler.

- B (enkanalighet med MTTF värde 3-10 år eller 10-30 år)
- 1(enkanalighet med högt MMTF-värde 30-100 år)

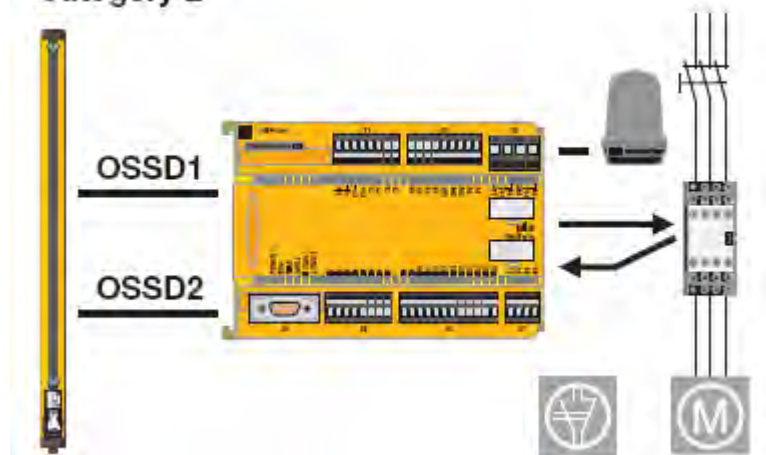
Bildexempel från PILZ

Category B, 1



- 2 (enkanalighet med 3-10 år, 10-30 år eller 30-100 år) + DC värde 0-60-99 % + åtgärder mot CCF

Category 2

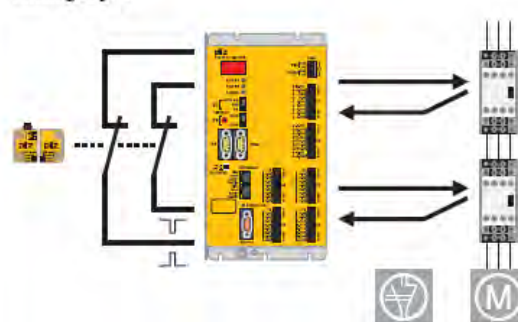


- 3 och 4, (redundans och 4(+övervakning) + DC samt CCF.

Category 3



Category 4



3 Fastställande av kategori

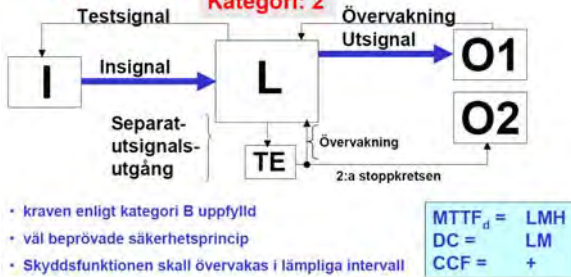
Kategori: B



- Designas i överensstämmelse med relevanta standarder
- motstå/klara förmodad påverkan
- feltolerans på noll
- huvudkaraktistiken genom val av komponenter

3 Fastställande av kategori

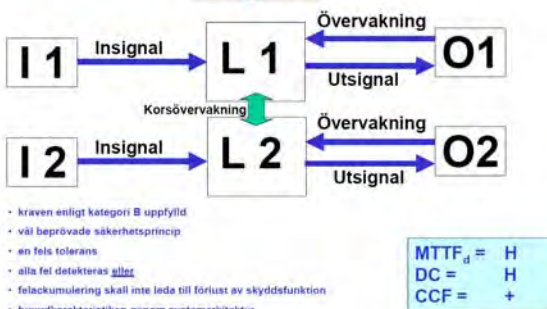
Kategori: 2



- kraven enligt kategori B uppfyllt
- väl beprövade säkerhetsprincip
- Skyddsfunktionen skall övervakas i lämpliga intervall
- feltolerans på noll - men förlust av skyddsfunktionen detekteras
- huvudkaraktistiken genom systemarkitektur

3 Fastställande av kategori

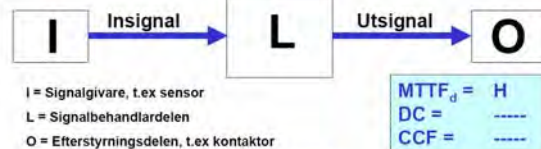
Kategori: 4



- kraven enligt kategori B uppfyllt
- väl beprövade säkerhetsprincip
- en fels tolerans
- alla fel detekteras alltid
- felackumulering skall inte leda till förlust av skyddsfunktion
- huvudkaraktistiken genom systemarkitektur

3 Fastställande av kategori

Kategori: 1



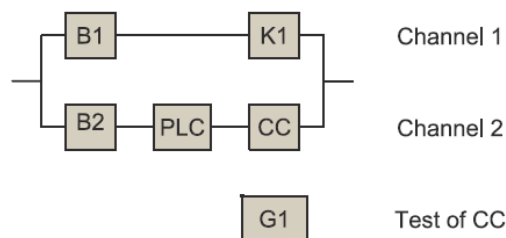
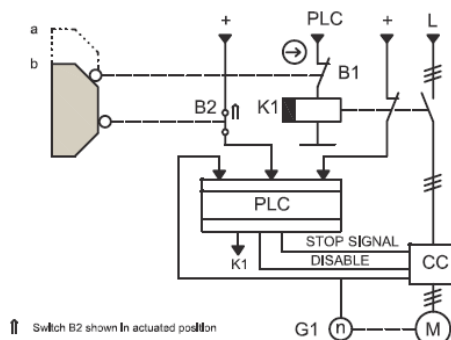
- kraven enligt kategori B uppfyllt
- väl beprövade komponenter och säkerhetsprincip
- feltolerans på noll - men sannolikheten för händelse är lägre än för kategori B
- huvudkaraktistiken genom val av komponenter

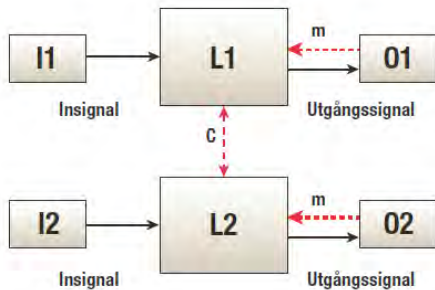
3 Fastställande av kategori

Kategori: 3



- kraven enligt kategori B uppfyllt
- väl beprövade säkerhetsprincip
- en fels tolerans
- vissa men inte alla fel detekteras
- ackumulering av odetekterade fel leda till förlust av skyddsfunktion
- huvudkaraktistiken genom systemarkitektur





Exempel på ett kategori 3 system



$MTTF_d$

$MTTF_d$: medelvärde av operationstid där ett enkanaligt system förväntas ha inga alvarliga fel

Beteckning	Frekvens för $MTTF_d$
Låg	$3 \text{ år} \leq MTTF_d < 10 \text{ år}$
Medel	$10 \text{ år} \leq MTTF_d < 30 \text{ år}$
Hög	$30 \text{ år} \leq MTTF_d < 100 \text{ år}$

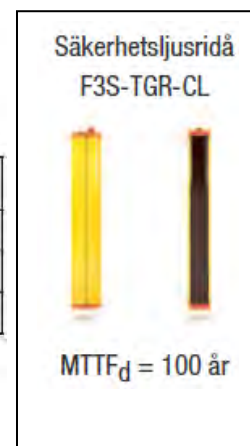
Värden på $MTTF_d$ kan t.ex hämtas från SN 29500 (Siemensstandard)

vissa typiska medelvärden finns indikerade i Annex C i standardförslaget
 t.ex kontakter: $MTTF_d = 32 \text{ år}$ (90% alvarligt fel)

$MTTF$ = Medeltid till felfunktion

$MTTF_d$ = Medeltid till farlig felfunktion

B10 d = Antal cykler tills 10% av komponenterna får farliga fel
 (För pneumatiska och elektromekaniska komponenter)



Exempel från lev.

Tabell C.1 – Internationella standarder som berör $MTTF_d$ eller B_{10d} för komponenter

	Grundläggande och väl beprövade säkerhetsprinciper enligt ISO 13849-2:2003	Andra relevanta standarder	Typiska värden: $MTTF_d$ (år) B_{10d} (cykler)
Mekaniska komponenter	Tabell A.1 och A.2	–	$MTTF_d = 150$
Hydrauliska komponenter	Tabell C.1 och C.2	EN 982	$MTTF_d = 150$
Pneumatiska komponenter	Tabell B.1 och B.2	EN 983	$B_{10d} = 20\,000\,000$
Reläer och hjälpkontakter med låg belastning (mekanisk belastning)	Tabell D.1 och D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 20\,000\,000$
Reläer och hjälpkontakter med maximal belastning	Tabell D.1 och D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 400\,000$
Beröringsfri givare med låg belastning (mekanisk belastning)	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 20\,000\,000$
Beröringsfri givare med maximal belastning	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 400\,000$
Kontakter med låg belastning (mekanisk belastning)	Tabell D.1 och D.2	IEC 60947	$B_{10d} = 20\,000\,000$
Kontakter med märkbelastning	Tabell D.1 och D.2	IEC 60947	$B_{10d} = 2\,000\,000$
Positionsbrytare oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 20\,000\,000$
Positionsbrytare (med separat manöverdon, låsanordning) oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 2\,000\,000$
Nödstoppsanordningar oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947 ISO 13850	$B_{10d} = 100\,000$
Nödstoppsanordningar med maximala driftskrav ^a	Tabell D.1 och D.2	IEC 60947 ISO 13850	$B_{10d} = 6\,050$
Tryckknappar (t.ex. acceptanordning) oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947	$B_{10d} = 100\,000$

Följande prioriteringsordning skall gälla för att hämta värden på MTTF

- Från tillverkarens data (use manufacturer's data)
- Tillämpa metoderna i standarden Bialga C och D (use methods in Annexes C and D)
- Välja 10 år som värde (choose ten years)

Table C.2 — Transistors (used as switches)

Transistor	Example	MTTF for components years	MTTF ₀ for components years		Remark
			Typical	Worst case	
Bipolar	TO18, TO92, SOT23	34 247	68 493	6 849	50 % dangerous failure
Bipolar, low power	TO5, TO39	5 708	11 416	1 142	50 % dangerous failure
Bipolar, power	TO3, TO220, D-Pack	1 941	3 881	388	50 % dangerous failure
FET	Junction MOS	22 831	45 662	4 566	50 % dangerous failure
MOS, power	TO3, TO220, D-Pack	1 142	2 283	228	50 % dangerous failure

Systemets eller enskilda komponenters tillförlitlighet (MTTFd)

Två faktorer är viktiga för säkerhetssystem.

De måste vara säkra och tillförlitliga. Tillförlitligheten är direkt kopplad till produktiviteten och därför viktig, eftersom varje onödig nedstängning på grund av ett fel i systemet eller på grund av att en komponent avbryter produktionen ökar risken för manipulering.

Systemfel sker ofta i början och i slutet av ett systems eller en enskild komponents livslängd.

a) Mekaniska, elektromekaniska, pneumatiska och hydrauliska system

Fel i dessa komponenter är kopplade till livslängden och/eller antalet åtgärder. Ett vanligt sätt att testa och beskriva beteendet är att göra ett livslängdstest tills 10 % av enheterna i testet upphör att fungera.

Detta kallas B10. Av säkerhetsskäl är testet mer specifikt och B10d visar värdet tills 10 % av enheterna i testet upphör att fungera.

B10 d=Antal cykler tills 10% av komponenterna får farliga fel

(För pneumatiska och elektromekaniska komponenter)

Vanliga komponenter i ett B10d-värde är gränslägesbrytare, brytare för säkerhetsdörrar och säkerhetsreläer.

Ofta saknas relevanta underlag för komponenter från tillverkarna och då måste man beräkna fram detta med hjälp av den formel som framgår nedan

För mekaniska, elektromekaniska, pneumatiska och hydrauliska system kan (a) MTTF_d beräknas med parametern B_{10d} som också är en del av dokumentationen och antalet åtgärder per år enligt:

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_a}$$

Se betydelse senare

b) Elektroniska system

I elektroniska system är felfrekvensen ett sannolikt värde, som beräknas av individuella data från alla komponenter som används, eftersom det finns ett FIT-värde (fel över tid) för alla typer av komponenter.

För elektroniska system (b) är MTTF_d en del av dokumentationen och tillhandahålls av tillverkaren.



4

MTTF_d

MTTF_d Delsammanräkningsmetod

Komponent	Antal enheter	MTTF _{di} värsta fall (år)	1/MTTF _{di} värsta fall (år)	N _i /MTTF _{di} värsta fall (år)
Transistor Bipolar	2	1142	0,000876	0,001752
Motstånd Carbin Film	5	11416	0,000088	0,000438
Kondensator standard	4	5708	0,000175	0,000701
Relä (uppgifter från tillverkare)	4	1256	0,000796	0,003185
Kontaktor	1	32	0,031250	0,031250
Summa (n _i /MTTF _{di})			[1/år]	0,037325
MTTF _d = 1/Sum (n _i /MTTF _{di})			[år]	26,79

$$\frac{1}{MTTF_d} = \sum_{j=1}^N \frac{n_j}{MTTF_{d,j}}$$

Beräkning av MTTF_d för komponenter med hjälp av B_{10d}

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}}$$

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 s / h}{t_{cycle}}$$

B_{10d} är antalet arbetscykler innan 10 % av komponenter går söder på ett farligt sätt

n_{op} är medelvärdet av antalet arbetsoperationer per år

h_{op} är medelanvändning i timmar per dag

d_{op} är medelanvändning i dagar per år

t_{cycle} är medeltiden (sek) mellan starten av två lyckosamma arbetscykler för komponenten

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

T_{10d} är medeltid tills 10% av komponenterna går sönder på ett farligt sätt (begränsad användningstid)



Tomas Beäff MPSA

Som ett exempel

$B_{10d} =$	1 369 863	cykler
$h_{op} =$	24	tim/ dag
$d_{op} =$	365	dagar/år
$t_{cycle} =$	3600	s/ cykel

$n_{op} =$	8 760	arb. operationer /år
$T_{10d} =$	156,4	år
$MTTF_d =$	1563,8	år = Hög

Om den farliga delen av B10 inte är angiven, kan 50 % av B10 användas och därför rekommenderas $B_{10d} = 2 B_{10}$

Utdrag ur EN 13849-1 om man endast tillämpar standardens "komponentdata"

Tabell C.1 – Internationella standarder som berör $MTTF_d$ eller B_{10d} för komponenter

	Grundläggande och väl beprövade säkerhetsprinciper enligt ISO 13849-2:2003	Andra relevanta standarder	Typiska värden: $MTTF_d$ (år) B_{10d} (cykler)
Mekaniska komponenter	Tabell A.1 och A.2	–	$MTTF_d = 150$
Hydrauliska komponenter	Tabell C.1 och C.2	EN 982	$MTTF_d = 150$
Pneumatiska komponenter	Tabell B.1 och B.2	EN 983	$B_{10d} = 20\,000\,000$
Reläer och hjälpkontakter med låg belastning (mekanisk belastning)	Tabell D.1 och D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 20\,000\,000$
Reläer och hjälpkontakter med maximal belastning	Tabell D.1 och D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 400\,000$
Beröringsfri givare med låg belastning (mekanisk belastning)	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 20\,000\,000$
Beröringsfri givare med maximal belastning	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 400\,000$
Kontakter med låg belastning (mekanisk belastning)	Tabell D.1 och D.2	IEC 60947	$B_{10d} = 20\,000\,000$
Kontakter med märkbelastning	Tabell D.1 och D.2	IEC 60947	$B_{10d} = 2\,000\,000$
Positionsbrytare oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 20\,000\,000$
Positionsbrytare (med separat manöverdon, låsanordning) oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947 EN 1088	$B_{10d} = 2\,000\,000$
Nödstoppsanordningar oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947 ISO 13850	$B_{10d} = 100\,000$
Nödstoppsanordningar med maximala driftskrav ^a	Tabell D.1 och D.2	IEC 60947 ISO 13850	$B_{10d} = 6\,050$
Tryckknappar (t.ex. acceptanordning) oberoende av belastning ^a	Tabell D.1 och D.2	IEC 60947	$B_{10d} = 100\,000$
För definition och användning av B_{10d} , se avsnitt C.4. ANM. 1 B_{10d} är uppskattad till två gånger B_{10} (50 % farliga felfunktioner). ANM. 2 "Låg belastning" innebär exempelvis 20 % av märkvärdet (mer information finns i EN ISO 13849-2).			
^a Om feluteslutning för tvångsöppning är möjlig.			

Notera: Standarderna EN 982 (pneumatik) och EN 983 (Hydraulik) är ersatta av EN ISO 4413 och 4414.

Diagnostic coverage, DC (Systemets feldetekteringsförmåga)

Avser endast feltålighetskategorierna 2, 3 och 4 (ej då enkanaliga kretsar som B och 1)

En form av övervakning detaljerat i 3 nivåer där DC uppskattas genom att fastställa systemets feldetekteringsåtgärder i tre (3) nivåer.

Värdet på DC anges i fyra nivåer (För att uppskatta DC kan i de flesta fall feleffektanalys (FMEA, se IEC 60812) eller liknande metoder användas. I detta fall bör alla relevanta feltillstånd och/eller felsätt beaktas och PL för kombinationen av SRP/CS som utför skyddsfunktionen bör kontrolleras mot den erforderliga prestandanivån (PLr). Ett förenklat sätt att uppskatta DC finns dock i standardens bilaga E.

Uppskatta DC enligt standarden

Åtgärd	DC
Ingångsenhet	
Cyklisk testimpuls genom dynamisk variation av ingångssignalerna	90 %
Rimlighetskontroll, t.ex. användning av slutande och brytande tvångsförda kontakter	99 %
Korsvis jämförelse av ingångssignaler utan dynamiskt test	0 % till 99 %, beroende på hur ofta signaländring görs i applikationen
Korsvis jämförelse av ingångssignaler med dynamiskt test om kortslutningar inte går att detektera (för flera I/O)	90 %
Korsvis jämförelse av ingångssignaler med direkta och mellanliggande resultat i logiken (L) samt tidsmässig och logisk programvaruövervakning av programflödet och detektering av statiska feltillstånd och kortslutningar (för flera I/O)	99 %
Indirekt övervakning (t.ex. övervakning med tryckvakt, elektrisk positionsövervakning av drivanordningar)	90 % till 99 %, beroende på tillämpningen
Direkt övervakning (t.ex. elektrisk positionsövervakning av styrventiler, övervakning av elektromekaniska enheter genom tvångsförning)	99 %
Feldetektering genom processen	0 % till 99 %, beroende på tillämpningen, enbart denna åtgärd räcker inte till för den erforderliga prestandanivån e!
Övervakning av vissa givaregenskaper (svarstid, analogt signalområde, t.ex. elektriskt motstånd, kapacitans)	60 %
Logik	
Indirekt övervakning (t.ex. övervakning med tryckvakt, elektrisk positionsövervakning av drivanordningar)	90 % till 99 %, beroende på tillämpningen
Direkt övervakning (t.ex. elektrisk positionsövervakning av styrventiler, övervakning av elektromekaniska enheter genom tvångsförning)	99 %
Enkel, tidsmässig övervakning av logiken (t.ex. timer som watchdog (övervakningsfunktion), med triggsignaler i programmets logik)	60 %
Tidsmässig och logisk övervakning av logiken med watchdog (övervakningsfunktion), där testanordningen gör rimlighetskontroller av logikens uppträdande	90 %
Självtest vid start för att detektera latenta fel i delar av logiken (t.ex. program- och dataminnen, ingångs-/utgångsportar, gränssnitt)	90 % (beroende på testtekniken)

DC kan fastställas som förhållandet mellan felfrekvensen för detekterade farliga felfunktioner och felfrekvensen för det totala antalet farliga felfunktioner. Enligt den här definitionen kan en genomsnittlig feldetekteringsförmåga DC_{avg} uppskattas med följande formel:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \dots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \dots + \frac{1}{MTTF_{dN}}} \quad (E.1)$$

Här måste alla komponenter hos SRP/CS utan felutslutning tas med och summeras. För varje block tas $MTTF_d$ och DC med i beräkningen. I den här formeln innebär DC förhållandet mellan felfrekvensen för detekterade farliga felfunktioner i delen (oavsett vilka åtgärder som används för att detektera felfunktionerna) och felfrekvensen för alla farliga felfunktioner i delen. Därför gäller DC den testade delen och inte testanordningen. Komponenter utan feldetektering (som t.ex. inte är testade) har $DC = 0$ och bidrar endast till nämnaren av DC_{avg} .

4

$MTTF_d$

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d} \quad \frac{\text{Sannolikhet för detektering av allvarligt fel}}{\text{Sannolikhet totalt för allvarligt fel}}$$

Exempel:

Cyklisk test genom dynamisk skiftande av inputsignalen

➔ Medel

Beteckning	Grad av DC
Ingen	$DC < 60\%$
Låg	$60\% \leq DC < 90\%$
Medel	$90\% \leq DC < 99\%$
Hög	$99\% \leq DC$

Table 4 — Diagnostic coverage (DC)

Denotation of DC	Range of DC
None	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

NOTE 1 The term safe diagnostic coverage, or diagnostic coverage including safe failures, is used to describe respectively the fractional decrease in the probability of safe hardware failure, or of both safe and dangerous hardware failures, resulting from the operation of the automatic diagnostic tests.

NOTE 2 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in this standard, see E.2 and Figure A.2.

5

Uppskattning av DC ur tabell

Identifiering av alla online-tester och diagnostik

Hämta aktuellt DC-värde ur Tabell

Beräkning av medelvärdes-DC för hela systemet genom interpoleringsformler

Exempel (RexRoth)

Measure	Technology	DC
Process (cyclic test)	Fluid technology	$0 \% \leq DC < 99 \%$
Cross monitoring between 2 channels	Electronics	$DC = 99 \%$
Indirect monitoring (e.g. pressure)	Fluid technology	$90 \% \leq DC < 99 \%$
Direct position monitoring	Fluid technology	$DC = 99 \%$
Integrated self-monitoring	Safety on board	$90 \% \leq DC \leq 99 \%$

CCF-Common Cause Failure –Samverkande fel (ej för B och 1)

-Kvantitativ metod för att uppskatta vidtagna åtgärder mot CCF (feltålighetskategorierna 2-3 och 4).

Uppskattas genom att värdera olika åtgärder mot gemensamma (common) felorsaker i systemet enligt tabeller i standarden.

Externa effekter som överspänning eller hög temperatur kan skada ett säkerhetssystem, även om det har två kanaler. Denna effekt påverkar båda kanalerna på samma sätt, eftersom det finns en vanlig orsak, som får båda kanalerna att sluta fungera.

CCF-Fastställes genom

- metod enligt bilaga F i EN ISO 13849-1
- 100 poäng kan maximalt uppnås
- 65 poäng och mer är godkänt
- under 65 poäng, använd ytterligare åtgärder mot CCF



Samverkande fel (CCF)

CCF: fel av olika orsaker, som resultat av en händelse

Kraven på CCF ställs för flerkanaliga strukturer (arkitekturer) (Kategori 2,3 och 4) och de är överensstämelse med EN 61508-6 Annex D - med "betafaktor på 2% eller mindre"

För system med en summa mindre än 65 poäng (pt) gäller

Separation/segregation av signalfasen	15 pt
Diversifiering	20 pt
Design (t.ex skydd mot överslag/kortsslutning)	15 pt
Väl beprövade komponenter	5 pt
FMEA (Felmod och Effekt analys)	5 pt
Miljöpåverkan - EMC + annat	25 pt + 10 pt

Om t.ex konstruktören har goda kunskaper i ämnet kan man få 5 poäng (tycker jag personligen är en mycket subjektiv bedömning)

Nr	Åtgärd mot CCF	Poäng
1	Separation/segregering	
	Fysisk separation mellan signalvägar: separation av ledningar/rör tillräckligt spelrum och krypavstånd på tryckta kretskort	15
2	Diversitet	
	Användning av olika tekniker/konstruktioner eller fysiska principer, exempelvis: första kanalen programmerbar elektronik och andra kanalen fast förträdad (elektromekanik), typ av initiering, tryck och temperatur, Mätning av avstånd och tryck, digitala och analoga. Komponenter från olika tillverkare.	20
3	Konstruktion/tillämpning/erfarenhet	
3.1	Skydd mot överspänning, övertryck och överström etc.	15
3.2	Komponenterna som används är väl beprövade.	5
4	Bedömning/analys	
	Är resultaten från feleffektanalysen beaktade för att undvika fel av samma orsak vid konstruktionen?	5
5	Kompetens/utbildning	
	Har konstruktörer/underhållspersonal utbildats i att förstå orsak och verkan av fel av samma orsak?	5
6	Omgivning	
6.1	Förebyggande åtgärder mot förorening och elektromagnetisk kompatibilitet (EMC) mot CCF enligt tillämpliga standarder. Tryckstyrda system: Filtrering av tryckmediet, skydd mot inträngande smuts, dränering av tryckluft, t.ex. enligt komponenttillverkarens krav på tryckmediets renhet. Elektriska system: Har systemet kontrollerats avseende elektromagnetisk immunitet, t.ex. enligt specifikation i relevanta standarder mot CCF? För kombinerade tryckstyrda och elektriskt styrda system ska båda aspekterna beaktas.	25
6.2	Annan påverkan Har kraven på tålighet mot all relevant miljöpåverkan såsom, temperatur, våldsam stöt, vibrationer, fuktighet (t.ex. som specificeras i relevanta standarder) beaktats?	10
	Sammanlagt	[max. 100]
Totalpoäng		Åtgärder för att undvika CCF^a
65 eller däröver		Kraven uppfyllda
Under 65		Processen misslyckad ⇒ vidta ytterligare åtgärder
^a När tekniska åtgärder inte är relevanta kan poängen i den här kolumnen tas med i den sammanlagda beräkningen.		



Tomas Beäff MPSA

Exempel Omron

Krav		Maximalt
Separation	Separation av signaler, isolation etc.	15 punkter
Diversitet	Olika teknologier eller komponenter	20 poäng
Konstruktion, tillämpning, erfarenhet	Överbelastning, överspänning eller skydd	15 poäng
	Användning av välbeprövade komponenter eller teknologier	5 poäng
Analys	Felanalys används för att undvika vanliga fel	5 poäng
Kompetens, utbildning	Utbildning av konstruktörer, för att förstå CCF och veta hur det ska undvikas	5 poäng
Miljö	EMC-test	25 poäng
	Stöt-, vibrations- eller temperaturtest	10 poäng

Fastställande av PL

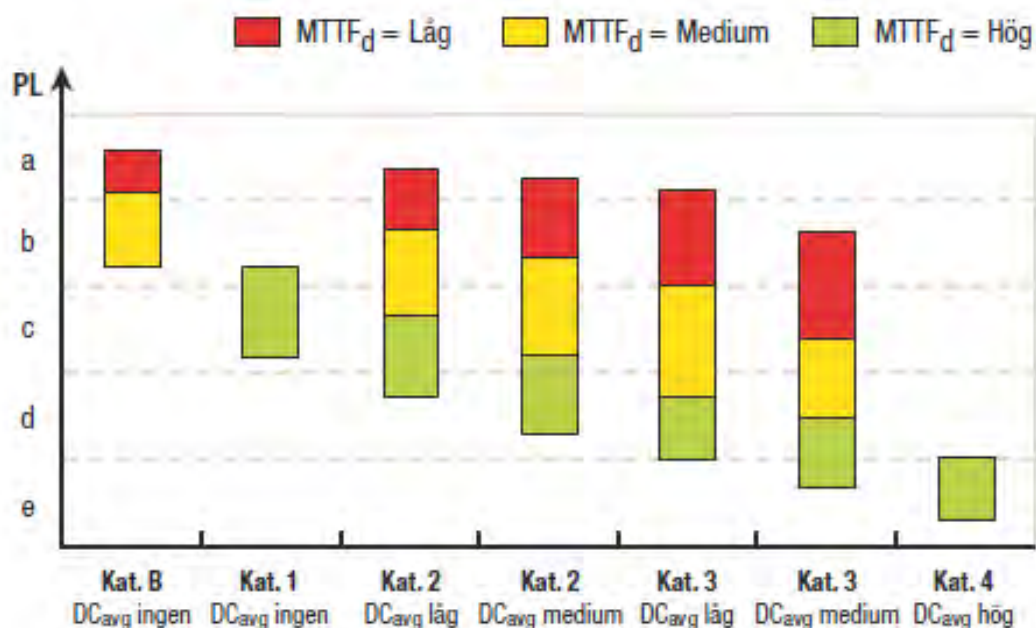


Fastställandet av systemarkitektur utgår ytterst från grundkategorierna (Fletålighetskategorierna) som även fanns i gamla EN 954-1 standarden (B-1-2-3-4)

3-10 år

10-30 år

30-100 år



Så här läser du diagrammet för ett PL = d-system:

Alternativ 1: Kat.2-system med $MTTF_d$ = hög och DC = medium

Alternativ 2: Kat. 3-system med $MTTF_d$ = medium och DC = medium

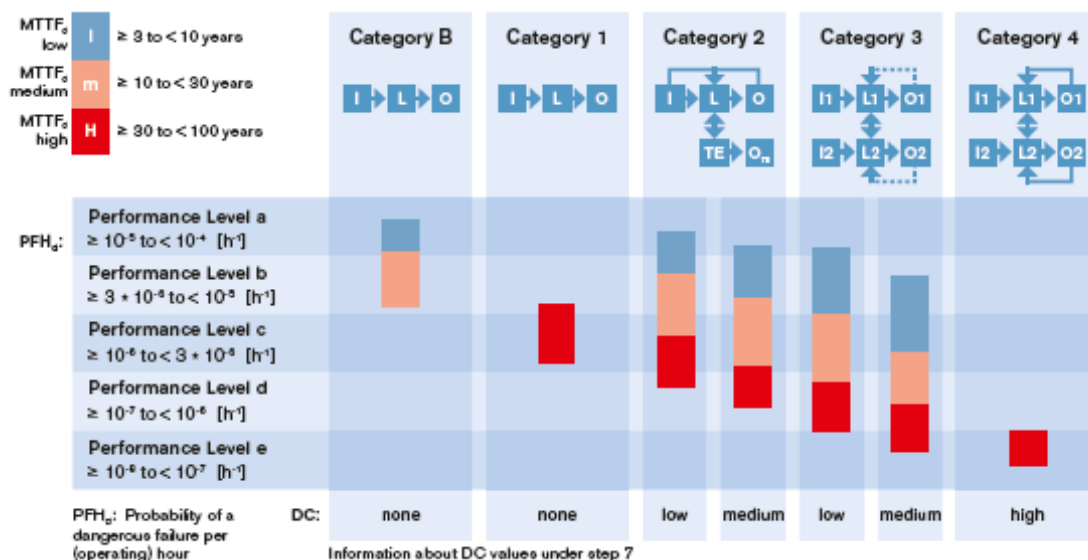
Självklart finns det även andra alternativ enligt detta diagram.

Förenklad bild

Kategori	B	1	2	2	3	3	4
DC_{avg}	ingen	ingen	låg	medel	låg	medel	hög
$MTTF_d$ för varje kanal							
Låg (kort tid)	a	Täcks inte	a	b	b	c	Täcks inte
Medel (medellång tid)	b	Täcks inte	b	c	c	d	Täcks inte
Hög (lång tid)	Täcks inte	c	c	d	d	d	e

Exempel (Rexroth)

Enkanalig bättre komponenter Övervakning Dubblering och med övervakning



Ingen övervakning i kat. B och 1

EN ISO 13849-1 beskriver en enkel process som kombinerar undersystem, om PL för alla undersystem är känd. 1. Fastställ vilket undersystem som har svagast PL (PL låg) 2. Fastställ antalet undersystem (n låg) med PL låg

PL låg	n låg	PL
Svagaste PL i undersystemen	Antal undersystem med PL låg	Maximal PL som kan uppnås
a	>3 →	–
	≤3 →	a
b	>2 →	a
	≤2 →	b
c	>2 →	b
	≤2 →	c
d	>3 →	c
	≤3 →	d
e	>3 →	d
	≤3 →	e

Table 11 — Calculation of PL for series alignment of SRP/CS

PL_{low}	N_{low}	$\Rightarrow$	PL
a	> 3	$\Rightarrow$	None, not allowed
	≤ 3	$\Rightarrow$	a
b	> 2	$\Rightarrow$	a
	≤ 2	$\Rightarrow$	b
c	> 2	$\Rightarrow$	b
	≤ 2	$\Rightarrow$	c
d	> 3	$\Rightarrow$	c
	≤ 3	$\Rightarrow$	d
e	> 3	$\Rightarrow$	d
	≤ 3	$\Rightarrow$	e

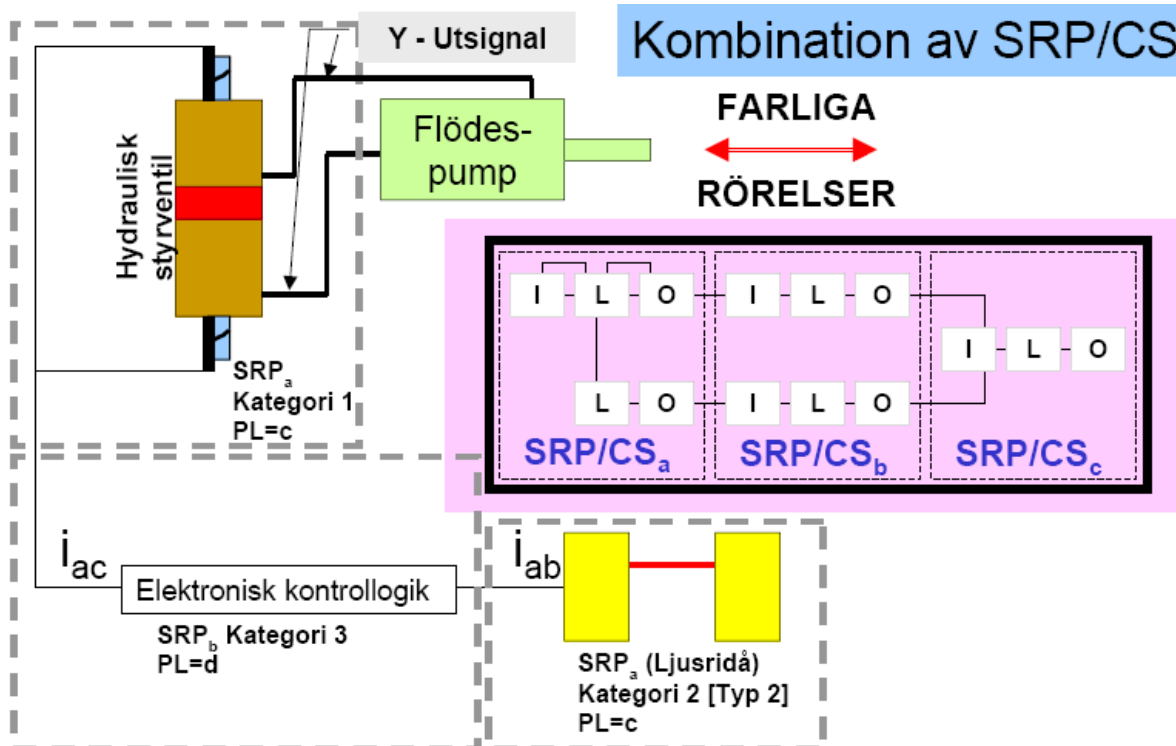
NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

The following method allows the calculation of the PL of the whole combined SRP/CS performing the safety function:

a) Identify the lowest PL_i : this is PL_{low} .

b) Identify the number $N_{low} \leq N$ of SRP/CS_i, with $PL_i = PL_{low}$.

c) Look-up PL in Table 11.



Jämförelse SIL-PL

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
3	1	< 60 %	SIL 1
	1	60 % – 90 %	SIL 2
4	>1	60 % – 90 %	SIL 3 (see Note 3)
	1	> 90 %	SIL 3 (see Note 4)

Sammanfattningsvis- Stegen för att fastställa nivån

1.-Riskbedömning baserad på EN ISO 12100 (ISO TR 14121-2)

Risikanalyt allmänt

En riktigt genomförd riskbedömning har som grund i kontroll och bedömning att de grundläggande hälso- och säkerhetskraven enligt Bilaga 1 är uppfyllda (Se 2006/42/EG i Sverige AFS 2008:3 Maskiner. Styrsystemskraven regleras i Bilaga 1 avsnitt 1,2.

För bedömning av äldre maskiners säkerhet och säkra användning hänvisas till 2009/104/EG i Sverige AFS 2006:4 vars Bilaga A tar upp de säkerhetskrav som minst måste uppfyllas för maskiner tagna i drift före 1995. Vid nykonstruktion av säkerhetsrelaterade kretsar för nya funktioner i gamla maskiner rekommenderas att de nya kraven tillämpas enligt AFS 2008:3 och därtill lämpliga harmoniserade standarder.

Risikanalyt enligt EN ISO 12100

1) fastställ maskinens gränser

Riskbedömningen börjar med att fastställa maskinens begränsningar under hela dess livslängd vilket omfattar avsedda användning och felaktig användning som rimligen kan förutses. Rörelseområde och utrymmeskrav för personer under tex drift och underhåll ska också beaktas samt maskinens livslängd, lämpliga serviceintervaller, vilken miljö maskinen ska stå i mm.

2) riskidentifiering

Efter fastställande av maskinens begränsningar ska bl.a. rimligen förutsebara risker under alla faser av maskinens livscykel identifieras, dvs transport, idrifttagning, användning och urdrifttagning.

Det är sannolikt att en riskkälla som finns i och vid maskinen förr eller senare leder till en skada om åtgärder inte vidtas för att eliminera riskkällan eller tillhandahålla skyddsåtgärder.

3) riskuppskattning

När riskerna har identifierats ska en riskuppskattning göras på varje risksituation. Den risk som förknippas med en viss risksituation beror på följande faktorer:

- skadans allvarlighetsgrad
- sannolikheten för att en skada kan uppstå

Risikvärdering

Om det krävs riskreducering ska lämpliga skyddsåtgärder väljas och tillämpas och proceduren upprepas. Som en

del av denna process ska konstruktören kontrollera om det tillkommer ytterligare riskkällor eller om andra risker ökar när nya skyddsåtgärder vidtas. Att uppnå en tillräcklig riskreducering med trestegsmetoder eller om möjligt med hjälp av ett positivt resultat av riskjämförelsen, kan betraktas som att risken har reducerats tillräckligt.

Trestegsmetoden innebär att riskerna:

1. Först och främst konstrueras "bort-design out"
2. . Går inte detta fullt ut så ska maskinen kompletteras med skydd.
3. Är det sedan inte praktiskt möjligt att reducera risken tillräckligt ska det informeras och varnas för kvarvarande risker.

Som en del i riskvärderingen kan de risker som förknippas med maskinen jämföras med andra liknande maskiner under vissa förutsättningar. Dessa kan till exempel vara att den likande maskinen uppfyller tillämpliga standarder och att maskinerna verkligen är jämförbara vad det gäller, användning, konstruktion, riskkällor, användningsvillkor mm.

C-standarder är unika per maskintyp varför kraven på riskbedömning ej då omfattar annat än vad som C-standarderna inte täcker in. Dock måste man kontrollera att de signifikanta riskerna och åtgärderna enligt C-standarderna då är vidtagna.

2.-Fastställande av säkerhetsfunktioner

(Vilka skall vi ha/har vi i maskinen typ nödstopp- skyddsstopp.

Föreslås att man utarbetar någon form av funktionsbeskrivning för de säkerhetsrelaterade kretsarna som kan bli aktuella för bedömning.

1.2 Ingående komponenter i leveransen.

Instruktionen refererar till följande dokument:

Sammanställningsritning:	013804, 013805, 013806
Flödesschema:	013744
Motor- och apparatlista:	Motor & Apparatlista_54661_29-06-2010.
Ritning över operatörsplatser:	54661-14

1.2.1 Nödstopp.

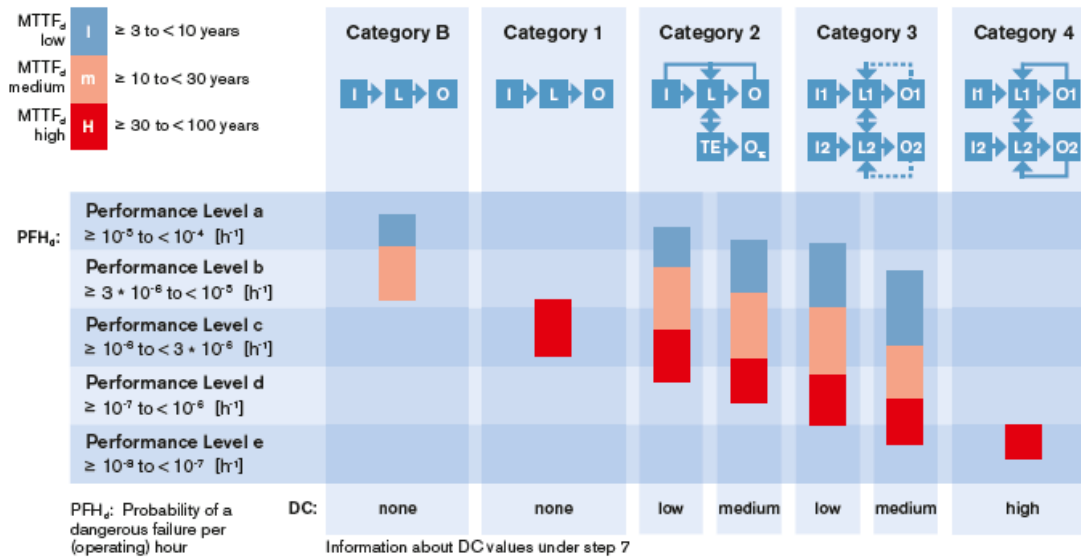
Allmänt:	Anläggningen har 1 st nödstoppskrets innehållande 4 st nödstopp samt 1 st återställning av nödstopp. Kretskategori för nödstoppskretsen enligt kretskategori 3 EN 954-1 (alt PL d) eller Sil 2 EN 62061		
Kabeldragning:	Kabeldragning utförs av SCA.		
Typ	Märkning	Placering	Funktion
Nödstopp	Nödstopp	OP1	Nödstopp stoppar samtliga motorer, ventiler återgår till sitt opåverkade läge samt övriga elektriska komponenter blir spänningslösa, dock aktiveras röd blixtlampa och signalhorn (pos 49) för att informera operatören att en ev. fyllning av silon skall avbrytas.
Nödstopp	Nödstopp	OP2	
Nödstopp	Nödstopp	OP3	
Nödstopp	Nödstopp	OP4	
Tryckknapp / lampa (blå)	Återställning nödstopp	OP4	Återställning av nödstopp. Blå lampa lyser när nödstopp är aktiverat.

3.-Klariläggande av erforderlig Prestandanivå Plr (Required Performance Level)

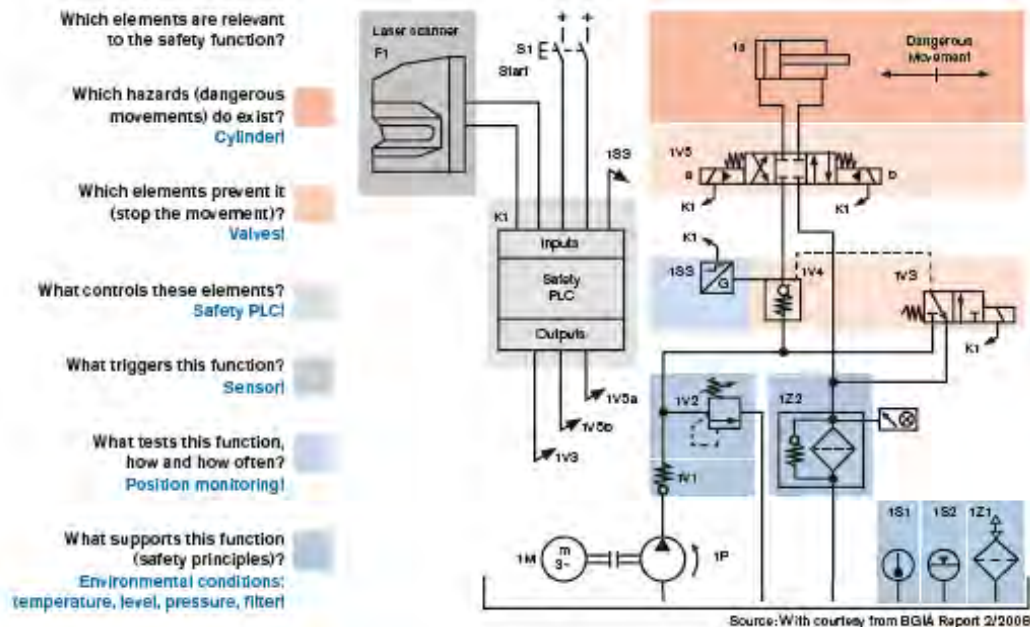
Enligt riskträd eller titta i färdigt val som kan återfinnas i C-standarder då.

4.-Val av systemarkitektur (de gamla kategorierna från EN 954-1 är kvar (B, 1, 2, 3, 4)

(Bild från Rexroth Bosch Group)



5.-Fastställande av krets genom blockdiagram



6.-Val av relevanta komponenter (MTTF d, B10, PL, PFHd)

Exempel nedan från Rexroth

The right parameters for different technologies			
Hydraulic components	Pneumatic components	Hydraulic subsystems	Electronic subsystems
			
Supplier: • MTTF _d	Supplier: • B ₁₀ (MTTF _d) ¹	Supplier: • PL (PFH _d) • Category	Supplier: (certified product) • PL (PFH _d) • Category
Machine builder: • Category • DC • CCF • PL of the system	Machine builder: • Category • DC • CCF • PL of the system	Machine builder: • DC • CCF • PL of the system	Machine builder: • PL of the system ²

¹ To calculate the MTTF_d from the B₁₀ value, see ISO 13849-1.

² Calculation of PL by adding the PFH_d values.

Maskintillverkarens skyldigheter är att fastställa kategori, DC, CCF och PL för systemet medans då säkerhetskomponenttillverkaren skall ange relevant data på sin "komponent"

7. Värdering av övervakningsfunktion DC

Fastställa systemets feldetekteringsförmåga (hämta värde ur tabell i standarden)
Gäller bara då kategorierna 2-4.

Exempel mediasystem-hydraulik-pneumatik enligt Rexroth

Measure	Technology	DC
Process (cyclic test)	Fluid technology	0 % ≤ DC < 99 %
Cross monitoring between 2 channels	Electronics	DC = 99 %
Indirect monitoring (e.g. pressure)	Fluid technology	90 % ≤ DC < 99 %
Direct position monitoring	Fluid technology	DC = 99 %
Integrated self-monitoring	Safety on board	90 % ≤ DC ≤ 99 %

8. Värdering av samverkande fel CCF

Poängsätta CCF-värdet vilket då gäller för systemkategorierna 2-3 och 4
65-100 poäng

Exempel Rexroth

Measure against CCF	Fluid technology	Electronics	Points
Separation between signal paths	Separation in piping	Clearances and creep age distances on printed-circuit boards.	15
Diversity	e.g. different valves	e.g. different processors	20
Protection against over-voltage, over-pressure ...	Assembly acc. to EN 982 or EN 983 (pressure-relief valve)	Protection against over-voltage (e.g. contactors, power supply unit)	15
Components used are well-trying	System designer		5
FMEA in development	FMEA in the design of the system		5
Competency/training	Qualification measure		5
Protection against contaminants and EMC	Fluid quality	EMC test	25
Other influences (incl. temperature, shock)	Fulfillment of EN 982 or EN 983 and product specification	Fulfillment of the environmental conditions acc. to product specification	10
CCF total	Total number of points (65 ≤ CCF ≤ 100):		

OBS EN 982 och EN 983 är ersatta av EN ISO 4413 och 4414

9. Kontrollera säkerhetsprinciper och mjukvarukrav

Bilaga G i EN ISO 13849 sätter principer för vad som skall beaktas gällande systematiska felfunktioner.

Vidare om programvara är i ASIC kretsar (ej enkelt ändringsbara).

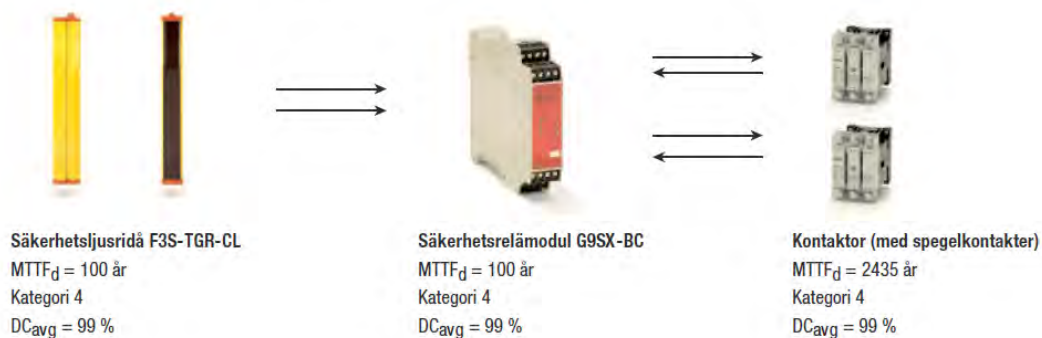
Att beakta gällande säkerhetsprinciper

Basic safety principles	Well-trying safety principles
- De-energisation principle - Pressure limitation - Speed limitation - Avoidance of contamination - Proper range of switching time - Protection against unexpected startup - Proper temperature range - Separation	- Overdimensioning/safety factor - Safe position - Speed limitation - Force limitation - Appropriate range of working conditions - Monitoring of the condition of the fluid

10. Verifiering och validering av uppnådd Prestandanvå PL=PLr

Exempel OMRONS katalog

Steg 7: Beräkning av det kompletta systemet (värden är enbart till för beräkning och representerar faktiska data)



Steg 8: Beräkning av total MTTF_d

$$MTTF_d = \frac{1}{\sum_{i=1}^3 \frac{1}{MTTF_{di}}} = \frac{1}{\frac{1}{100} + \frac{1}{100} + \frac{1}{2435}} = \frac{1}{0,0201} = 48,99 \text{ år}$$

Steg 9: Beräkning av total DC_{avg}

$$DC_{avg} = \frac{\sum_{i=1}^2 \frac{DC_i}{MTTF_{di}}}{\sum_{i=1}^2 \frac{1}{MTTF_{di}}} = \frac{\frac{0,99}{100} + \frac{0,99}{2435}}{\frac{1}{100} + \frac{1}{2435}} = 0,99$$

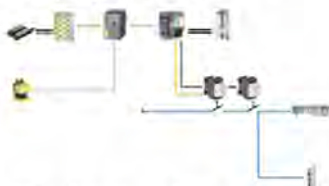
Stegen till Erforderlig Prestandanivå enligt (SS) EN ISO 13849-1 ^(1 av 2)

Riskbedömning-allmänt

Krav i maskindirektivet
T.ex baserad på EN ISO 2100
(ISO TR 14121-2)

Fastställande av behövda säkerhetsfunktioner

(Vilka skall vi ha/har vi i maskinen typ nödstopp-skyddsstopp, ljud-ljussignaler, temp-trycklarm etc.

[illegible]

Klarläggande av erforderlig Prestandanivå Plr

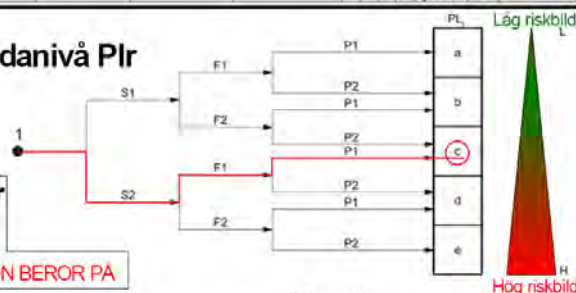
-Via riskträd eller via C-standard
(Performance Level required)
(Behövd PL nivå för aktuella kretsar)

Val av kategori och systemarkitektur

(de gamla kategorierna från EN 954-1 är kvar i EN ISO 13849-1(B, 1, 2, 3, 4))

- VALET AV EN KATEGORI FÖR EN SÄKERHETSFUNKTION BEROR PÅ

- Den riskreducering som skall uppnås med skyddsfunktionen till vilken delen bidrar
- Den erforderliga Prestandanivån Plr
- Använd teknik
- Risken som uppstår i händelse av feltillstånd i den delen
- Möjligheter att undvika feltillstånd i den delen (systematiska fel)
- Sannolikhet för att feltillstånd uppstår i den delen och relevanta parametrar.
- Medeltid till farlig felfunktion (MTTD d)
- Feldetekteringsförmågan DC och
- Fel av samma orsak (CCF) för kategorierna 2,3 och 4.



Förklaring

T: startpunkt för övärdering av en skyddsåtgärds bidrag till riskreduceringen

L: lågt bidrag till riskreduceringen

H: högt bidrag till riskreduceringen

Risikoparametrar	Hög riskbild
S	sludans avfärdighet
S1	läst (väntigets övergående skada)
S2	avir (väntigets oödlig skada eller dödsfall)
F	fräknens oödlighet exponeringstid för riskman
F1	skadan till mindre öls oödlighet kort exponeringstid
F2	ofta till kontinuerlig oödlighet lång exponeringstid
P	möjlighet att undvika riskkänslan med begränsad skadan
P1	möjlighet under vissa omständigheter
P2	knäpptast möjlighet

Fastställande av krets genom blockdiagram

Val av relevanta komponenter

(MTTE d B10 Pl *PFHd)* Från EN 61508 och EN 62061 (SIL)

	MTTF ₁	
Betænkning for varje kanal		Omskrive for varje kanal
Lag (kort tid)		3 år $\leq$ MTTF ₁ $\leq$ 10 år
Media (medium/tid)		10 år $\leq$ MTTF ₁ $\leq$ 30 år
Hög (lång tid)		30 år $\leq$ MTTF ₁ $\leq$ 100 år

Antal cykler tills 10 % av komponenterna får farliga fel (för pneumatiska och elektromekaniska komponenter)

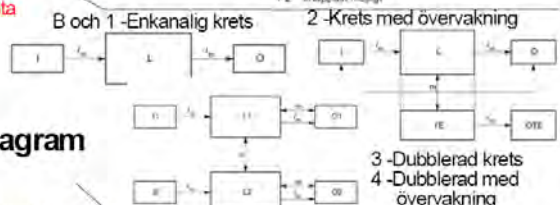
Värdering av CCF

Tabelle 10.10.2		Punkte
1	Beobachtungsvariable	
1.1	Geistig-kommunikative Kompetenz: Wahrnehmung, Verstehen, Reflexion, Argumentation, Problemlösung, Kommunikation, Selbstkompetenz, Sozialkompetenz, Emotionale Kompetenz, Persönlichkeitskompetenz	15
2	Outcome	
2.1	Argumentieren & Diskutieren: Argumente und Gegenargumente entwickeln & bewerten - Sachverhalte verstehen - Argumente verstehen - Argumente bewerten - Argumente entwickeln - Argumente diskutieren - Argumente reflektieren - Argumente kritisieren - Argumente verteidigen - Argumente integrieren - Argumente transferieren	20
3	Instrumente	
3.1	Themenkompass Argumentieren & Diskutieren	10
3.2	Themenkompass Argumentieren & Diskutieren	10
3.3	Themenkompass Argumentieren & Diskutieren	10
3.4	Themenkompass Argumentieren & Diskutieren	10
3.5	Themenkompass Argumentieren & Diskutieren	10
3.6	Themenkompass Argumentieren & Diskutieren	10
3.7	Themenkompass Argumentieren & Diskutieren	10
3.8	Themenkompass Argumentieren & Diskutieren	10
3.9	Themenkompass Argumentieren & Diskutieren	10
3.10	Themenkompass Argumentieren & Diskutieren	10
3.11	Themenkompass Argumentieren & Diskutieren	10
3.12	Themenkompass Argumentieren & Diskutieren	10
3.13	Themenkompass Argumentieren & Diskutieren	10
3.14	Themenkompass Argumentieren & Diskutieren	10
3.15	Themenkompass Argumentieren & Diskutieren	10
3.16	Themenkompass Argumentieren & Diskutieren	10
3.17	Themenkompass Argumentieren & Diskutieren	10
3.18	Themenkompass Argumentieren & Diskutieren	10
3.19	Themenkompass Argumentieren & Diskutieren	10
3.20	Themenkompass Argumentieren & Diskutieren	10
3.21	Themenkompass Argumentieren & Diskutieren	10
3.22	Themenkompass Argumentieren & Diskutieren	10
3.23	Themenkompass Argumentieren & Diskutieren	10
3.24	Themenkompass Argumentieren & Diskutieren	10
3.25	Themenkompass Argumentieren & Diskutieren	10
3.26	Themenkompass Argumentieren & Diskutieren	10
3.27	Themenkompass Argumentieren & Diskutieren	10
3.28	Themenkompass Argumentieren & Diskutieren	10
3.29	Themenkompass Argumentieren & Diskutieren	10
3.30	Themenkompass Argumentieren & Diskutieren	10
3.31	Themenkompass Argumentieren & Diskutieren	10
3.32	Themenkompass Argumentieren & Diskutieren	10
3.33	Themenkompass Argumentieren & Diskutieren	10
3.34	Themenkompass Argumentieren & Diskutieren	10
3.35	Themenkompass Argumentieren & Diskutieren	10
3.36	Themenkompass Argumentieren & Diskutieren	10
3.37	Themenkompass Argumentieren & Diskutieren	10
3.38	Themenkompass Argumentieren & Diskutieren	10
3.39	Themenkompass Argumentieren & Diskutieren	10
3.40	Themenkompass Argumentieren & Diskutieren	10
3.41	Themenkompass Argumentieren & Diskutieren	10
3.42	Themenkompass Argumentieren & Diskutieren	10
3.43	Themenkompass Argumentieren & Diskutieren	10
3.44	Themenkompass Argumentieren & Diskutieren	10
3.45	Themenkompass Argumentieren & Diskutieren	10
3.46	Themenkompass Argumentieren & Diskutieren	10
3.47	Themenkompass Argumentieren & Diskutieren	10
3.48	Themenkompass Argumentieren & Diskutieren	10
3.49	Themenkompass Argumentieren & Diskutieren	10
3.50	Themenkompass Argumentieren & Diskutieren	10
3.51	Themenkompass Argumentieren & Diskutieren	10
3.52	Themenkompass Argumentieren & Diskutieren	10
3.53	Themenkompass Argumentieren & Diskutieren	10
3.54	Themenkompass Argumentieren & Diskutieren	10
3.55	Themenkompass Argumentieren & Diskutieren	10
3.56	Themenkompass Argumentieren & Diskutieren	10
3.57	Themenkompass Argumentieren & Diskutieren	10
3.58	Themenkompass Argumentieren & Diskutieren	10
3.59	Themenkompass Argumentieren & Diskutieren	10
3.60	Themenkompass Argumentieren & Diskutieren	10
3.61	Themenkompass Argumentieren & Diskutieren	10
3.62	Themenkompass Argumentieren & Diskutieren	10
3.63	Themenkompass Argumentieren & Diskutieren	10
3.64	Themenkompass Argumentieren & Diskutieren	10
3.65	Themenkompass Argumentieren & Diskutieren	10
3.66	Themenkompass Argumentieren & Diskutieren	10
3.67	Themenkompass Argumentieren & Diskutieren	10
3.68	Themenkompass Argumentieren & Diskutieren	10
3.69	Themenkompass Argumentieren & Diskutieren	10
3.70	Themenkompass Argumentieren & Diskutieren	10
3.71	Themenkompass Argumentieren & Diskutieren	10
3.72	Themenkompass Argumentieren & Diskutieren	10
3.73	Themenkompass Argumentieren & Diskutieren	10
3.74	Themenkompass Argumentieren & Diskutieren	10
3.75	Themenkompass Argumentieren & Diskutieren	10
3.76	Themenkompass Argumentieren & Diskutieren	10
3.77	Themenkompass Argumentieren & Diskutieren	10
3.78	Themenkompass Argumentieren & Diskutieren	10
3.79	Themenkompass Argumentieren & Diskutieren	10
3.80	Themenkompass Argumentieren & Diskutieren	10
3.81	Themenkompass Argumentieren & Diskutieren	10
3.82	Themenkompass Argumentieren & Diskutieren	10
3.83	Themenkompass Argumentieren & Diskutieren	10
3.84	Themenkompass Argumentieren & Diskutieren	10
3.85	Themenkompass Argumentieren & Diskutieren	10
3.86	Themenkompass Argumentieren & Diskutieren	10
3.87	Themenkompass Argumentieren & Diskutieren	10
3.88	Themenkompass Argumentieren & Diskutieren	10
3.89	Themenkompass Argumentieren & Diskutieren	10
3.90	Themenkompass Argumentieren & Diskutieren	10
3.91	Themenkompass Argumentieren & Diskutieren	10
3.92	Themenkompass Argumentieren & Diskutieren	10
3.93	Themenkompass Argumentieren & Diskutieren	10
3.94	Themenkompass Argumentieren & Diskutieren	10
3.95	Themenkompass Argumentieren & Diskutieren	10
3.96	Themenkompass Argumentieren & Diskutieren	10
3.97	Themenkompass Argumentieren & Diskutieren	10
3.98	Themenkompass Argumentieren & Diskutieren	10
3.99	Themenkompass Argumentieren & Diskutieren	10
3.100	Themenkompass Argumentieren & Diskutieren	10

Uppskattningar av fel av samma orsak
(Common Cause Failure) (För kategorier 2-4)

[illegible]

Minst 65 poäng krävs.



Skillnaden mellan kategori B och kategori 1 är bl.a att det krävs användning av väl beprövade komponenter i kategori 1. Skillnaden mellan kategori 3 och kategori 4 är en högre DCavg i kategori 4 och att den erforderliga MTTFd för varje kanal är "hög".

PL	Genomsnittlig anslutnings- tid	Genomsnittlig felaktighet per timme
a	$\geq 10^{-5}$ s	10 000 h
b	$\geq 10^{-4}$ s	30 000 h
c	$\geq 10^{-3}$ s	100 000 h
d	$\geq 10^{-2}$ s	1 000 000 h
e	$\geq 10^{-1}$ s	10 000 000 h

Denna process bör användas för hela systemet. Varje del av de säkerhetsrelaterade delarna i styrsystemet bör tas med i processen. Tabellen listar åtgärder med tillhörande värden, baserade på ingenjörsmässiga bedömningar, vilka representerar det bidrag varje åtgärd ger för att reducera fel av samma orsak. För varje listed åtgärd kan endast full poäng eller ingenting ges.

Stegen till Erforderlig Prestandanivå enligt (SS) EN ISO 13849-1 (2 av 2)

Värdering av övervakningsfunktion DC

Uppskattningar av feldetekteringsförmågan (DC) hos funktioner och moduler (För kategorier 2-4)

Beteckning	DC	Område
Ingen	<60 %	DC < 60 %
Låg		60 % ≤ DC < 90 %
Medel		90 % ≤ DC < 99 %
Hög	99 %	99 % ≤ DC

Valet av DC-områden baseras på nyckelvärdena 60 %, 90 % och 99 %

För att uppskatta DC kan i de flesta fall feleffektanalys (FMEA) eller liknande metoder användas. Ett förenklat sätt att uppskatta DC finns i bilaga standardens Bilaga E

Uppskattningar av feldetekteringsförmågan (DC) DC=Diagnostic coverage

Åtgärd	DC
Ingångsenhet	
Cyklisk testning genom dynamisk variation av ingångssignalerna	90 %
Reaktionskontroll, t.ex. användning av skakande och trytande tvångslösta kontakter	99 %
Korsvis jämförelse av ingångssignaler utan dynamisk test	0 % till 99 %, beroende på hur ofta signalväxling görs i applikationen
Korsvis jämförelse av ingångssignaler med dynamisk test om korsningar inte går att detektera (för flera I/O)	99 %
Korsvis jämförelse av ingångssignaler med direkta och mellanliggande resultat i logiken (t.ex. tidsslag och logisk programövervakning av programflödet och detektering av statiska fel tillstånd och korsningar (för flera I/O))	99 %
Indirekt övervakning (t.ex. övervakning med tryckvakt, elektrisk position, övervakning av drivordningar)	90 % till 99 %, beroende på tillämpningen
Direkt övervakning (t.ex. elektrisk positionövervakning av styrväxlar, övervakning av elektromekaniska enheter genom tvångslösning)	99 %
Felutvärdering genom processen	0 % till 99 %, beroende på tillämpningen, endast denna åtgärd räcker inte till för den erforderliga prestandanivån
Övervakning av vissa givaregenskaper (svarstid, analogt signalmått, t.ex. elektrisk motstånd, kapacitans)	60 %
Logik	
Indirekt övervakning (t.ex. övervakning med tryckvakt, elektrisk position, övervakning av drivordningar)	90 % till 99 %, beroende på tillämpningen
Direkt övervakning (t.ex. elektrisk positionövervakning av styrväxlar, övervakning av elektromekaniska enheter genom tvångslösning)	99 %
Enkel, tidsbasad övervakning av logiken (t.ex. timer som watchdog (övervakningsfunktion), med färgsgränser i programmet)	60 %
Tidsbasad och logisk övervakning av logiken med watchdog (övervakningsfunktion), där testanordningen gör reaktionskontroller av logikens uppträdande	90 %
Spårbarhet vid start för att detektera latent fel i delar av logiken (t.ex. program- och delamnen, ingångs-utgångsportar, gränssnitt)	90 % (beroende på teststrukturer)

Åtgärd	DC
Kontroll av övervakningsprogramets reaktionsförmåga t.ex. watchdog (övervakningsfunktion) vid start med funktionen eller när reaktionsfunktionen påverkas eller när en annan signal påverkar den via en ingångsport	90 %
Dynamisk program (t.ex. ingångssignaler) måste antas skändas (ON-OFF) när skyddsfunktionen skändas. Ex. Skendeprogram med reaktion	90 %
Statisk program. Signalen med skendeprogram (t.ex. tider)	90 %
Statisk program. Signalen med skendeprogram (t.ex. tider)	99 %
Dynamisk program. RAM-test med hjälp av reaktionsförmåga, t.ex. flaggor, monitor, korrektion, timer och status jämförelse av dessa data	90 %
Dynamisk program. Kontroll av till- och skendeprogram. Skendeprogrammet påverkar	60 %
Dynamisk program. RAM-övervakning med reaktion. Hamningskod eller RAM-jämförelse (t.ex. "gräns"- eller "skendeprogram")	99 %
Processmonitor. Skendeprogram med programmet	60 % till 99 %
Processmonitor. Kontroll av programmet	90 % till 99 %
Felutvärdering genom processen	0 % till 99 %, beroende på tillämpningen, endast denna åtgärd är inte tillräcklig för erforderlig prestandanivån
Utgångsenhet	
Övervakning av utgångar genom en separat utan dynamisk test	0 % till 99 %, beroende på hur ofta signalväxling görs i tillämpningen
Korsvis jämförelse av utgångssignaler utan dynamisk test	0 % till 99 %, beroende på hur ofta signalväxling görs i tillämpningen
Korsvis jämförelse av utgångssignaler med dynamisk test utan detektering av korsningar (för flera I/O)	90 %
Korsvis jämförelse av utgångssignaler med direkta och mellanliggande resultat i logiken (t.ex. tidsslag och logisk programövervakning av programflödet och detektering av statiska fel tillstånd och korsningar (för flera I/O))	99 %
Redundant övervakningsnivå utan övervakning av drivordningar	0 %
Redundant övervakningsnivå med övervakning av en av drivordningarna antingen genom logiken eller en testanordning	90 %
Redundant övervakningsnivå med övervakning av drivordningarna genom logiken och en testanordning	99 %
Indirekt övervakning (t.ex. övervakning med tryckvakt, elektrisk position, övervakning av drivordningar)	90 % till 99 %, beroende på tillämpningen
Felutvärdering genom processen	0 % till 99 %, beroende på tillämpningen, endast denna åtgärd är inte tillräcklig för erforderlig prestandanivån
Direkt övervakning (t.ex. elektrisk positionövervakning av styrväxlar, övervakning av elektromekaniska enheter genom tvångslösning)	99 %

Den genomsnittliga feldetekteringsförmåga DC avg uppskattas med följande formel:

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

Här måste alla komponenter hos SRP/CS utan felutslutning tas med och summeras. För varje block tas MTTF_d och DC med i beräkningen. I den här formeln innebär DC förhållandet mellan felfrekvensen för detekterade farliga felfunktioner i delen (avsatt vilka åtgärder som används för att detektera felfunktionerna) och felfrekvensen för alla farliga felfunktioner i delen.

Säkerhetsrelämodul F3S-TGR-CL
MTTF_d = 100 år
Kategori 4
DC_{avg} = 99 %

Säkerhetsrelämodul GDSX-BC
MTTF_d = 100 år
Kategori 4
DC_{avg} = 99 %

Kontakter (med spagettkontakter)
MTTF_d = 2435 år
Kategori 4
DC_{avg} = 99 %

Exempel från OMRON

$$MTTF_d = \frac{1}{\frac{1}{100} + \frac{1}{100} + \frac{1}{2435}} = 0,0201 = 48,99 \text{ år}$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_d}}{\frac{1}{MTTF_d}} = \frac{\frac{0,99}{100} + \frac{0,99}{100} + \frac{0,99}{2435}}{\frac{1}{100} + \frac{1}{100} + \frac{1}{2435}} = 0,99$$

Kontrollera säkerhetsprinciper och mjukvarukrav

Standardens informativa Bilaga J ger riktlinjer gällande programvara och programmeringsregler. Och behandlar bland annat följande områden.

- Programmeringsregler på programstrukturnivå
- Programmeringsregler vid användning av variabler
- Programmeringsregler på funktionsblocksnivå
- För CCF bör det i allmänhet vara möjligt att styrka programmet med författare, laddningsdatum, version och senaste åtkomsttyp.

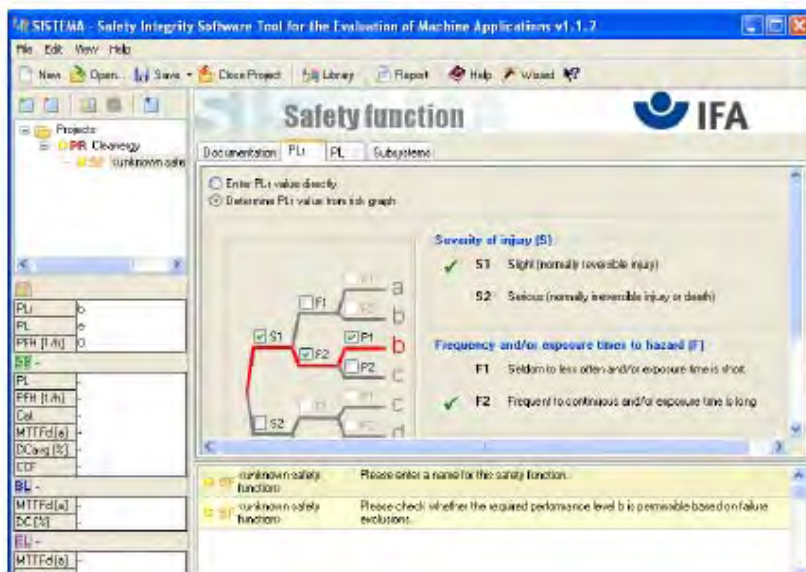
Verifiering och validering av uppnådd Prestandanivå PL=PLr

www.mpsa.se T Beäff

Handräkning eller då använda PROGRAMVARA

Det finns olika typer av programvaror för att hantera alla data och slutligt validera och verifiera aktuell PL-nivå.

Gratisprogrammet SISTEMA är ett oberoende och bra program för att riskbedöma-validera och verifiera kretsar med avseende på PL, detta kan laddas ner från Tyska IFA och är som sagt gratis att använda.



Vidare finns programvaran Pascal från Pilz
 (Hanterar Både SIL-PL)

Siemens har även en programvara (Safety evaluation tool)

Sätt 2 SIL

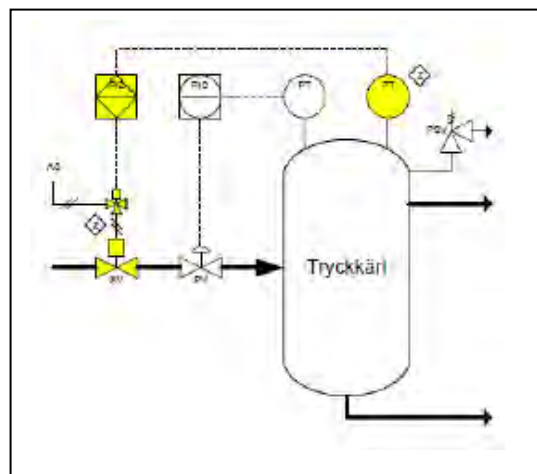
SIL Safety Integrity Level

Etta annat sätt att göra samma sak på.

Historik

Den 24 februari 1992 lagstiftades det i USA att både processen och de tillhörande säkerhetssystemen skulle ingå i en omfattande "Process hazard analysis", PHA. I PHA ingår att identifiera och utvärdera riskerna i processen samt att införa säkerhetssystem som minskar dessa risker.

Designen av säkerhetssystemet skulle följa "good engineering practice".



Ett av problemen var att det inte fanns en standard som definierade vad som var "good engineering practice", vilket ledde till subjektiva bedömningar.

1996 antogs i USA en standard ANSI/ISA S84.01 där implementeringen av processsäkerhetssystem definierades.

Standarden kan beskrivas som en samling av "best practice" bland användare av Säkerhets Integrerad Styrning. Det var i denna standard som "Safety integrity level", SIL infördes för att definiera kraven på säkerheten.

I standarden definieras nivåerna i SIL-systemet enligt tabell nedan.

De europeiska standarderna IEC 61508 (komponentrelaterad) och 61511 (sektorstandar) motsvarar den amerikanska ANSI/ISA S84.01.

Tabell 1 Definitionen av nivåerna i SIL-systemet

SIL	Sannolikhet för fel vid anrop	Riskreduktion
4	10^{-4} - 10^{-5}	10 000 – 100 000
3	10^{-3} - 10^{-4}	1 000 – 10 000
2	10^{-2} - 10^{-3}	100 – 1 000
1	10^{-1} - 10^{-2}	10 – 100
-	$>10^{-1}$	<10

Ett djupare sätt att se på detta

Integritetsnivåer			
SIL	Lågt skyddsbehov		Högt skyddsbehov
	Sannolikhet att fela vid anrop = PFD_{avg}	Riskreduktion (RRF) = $1/PFD_{avg}$	PFH (FIT)
4	$\geq 10^{-5} - 10^{-4}$	$> 10\,000 - 100\,000$	$\geq 1 - 10$
3	$\geq 10^{-4} - 10^{-3}$	$> 1\,000 - 10\,000$	$\geq 10 - 100$
2	$\geq 10^{-3} - 10^{-2}$	$> 100 - 1000$	$\geq 100 - 1000$
1	$\geq 10^{-2} - 10^{-1}$	$> 10 - 100$	$\geq 1000 - 10000$

OBSERVERA att SIL 4 tillämpas inte i industriell miljö dock inom kärnkraften.

Säkerhetsfunktioner sköts allt oftare av elektriska, elektroniska eller programmerbara elektroniska system. (E/E/PES)

De är i regel komplexa och det är då inte praktiskt möjligt att fullt ut bestämma varje feltyp eller att prova alla beteenden som är möjliga. Det är även stor risk för systematiska fel, dvs brister som byggs in under designfasen. Det blir därmed svårt att förutsäga säkerhetsprestanda, även om provningen fortfarande är en viktig del.

Principen bygger på att konstruera systemet på ett sådant sätt att det förhindrar allvarliga fel eller att ha dem under kontroll när de uppkommer.

Ett E/E/PES system innefattar alla delar som är nödvändiga för att säkerhetsfunktionen ska utföras, dvs från Signalgivare typ sensor, genom Signalbehandling typ styrlogik och kommunikationssystem, till Signalbehandlingens/utgångarnas ställdon, inklusive eventuellt kritiska åtgärder av en mänsklig operatör.

Några exempel på säkerhetsrelaterade funktioner (processområdet):

- Nödsystem för frångkoppling i en kemisk processanläggning
- Lågnivåskydd i en ångpanna
- Temperaturvakt för att ej överskrida designtemperatur
- En lyftkransindikator som anger säker last
- Skyddsstoppanordningar med förreglingar
- Nödstoppskretsar
- Stilleståndsvakter, hastighetsövervakning

PED relaterat

Säkerhetsutrustning enligt PED 97/23/EG (AFS 1999:4) tryckbärande anordningar tillhör normalt Kategori IV.

Som "säkerhetssystem" avses bl.a när mekanisk utrustning ersätta med icke mekanisk utrustning som ofta brukar ge anläggningen del slutliga säkerheten.

Exempel på icke mekanisk säkerhetsutrustning kan exempelvis nämnas:

- Lågnivåskydd
 - Högnivåskydd
 - Tryckvaktssystem för stopp av maskiner typ pumpar
 - Temperaturvakter
- samt övriga säkerhetsrelaterade styrfunktioner.

När skall säkerhetsanordningar finnas i trycksatta applikationer

Trycksatta applikationer skall normalt säkerhetsanordningar finnas när PS (tryck) eller TS (temp) kan överskridas.

Vidare skall lämpliga säkerhetsanordningar (§2 AFS 1999:4) samt indikerande ljud-ljus samt övriga larm hanteras på ett säkert sätt.

Konstruktionsprinciperna handlar om

- Felsäkerhet som förebyggs med redundans (2) eller diversifiering-övervakning.
- Diversibel redundans innebär två av varandra oberoende och övervakade funktioner.

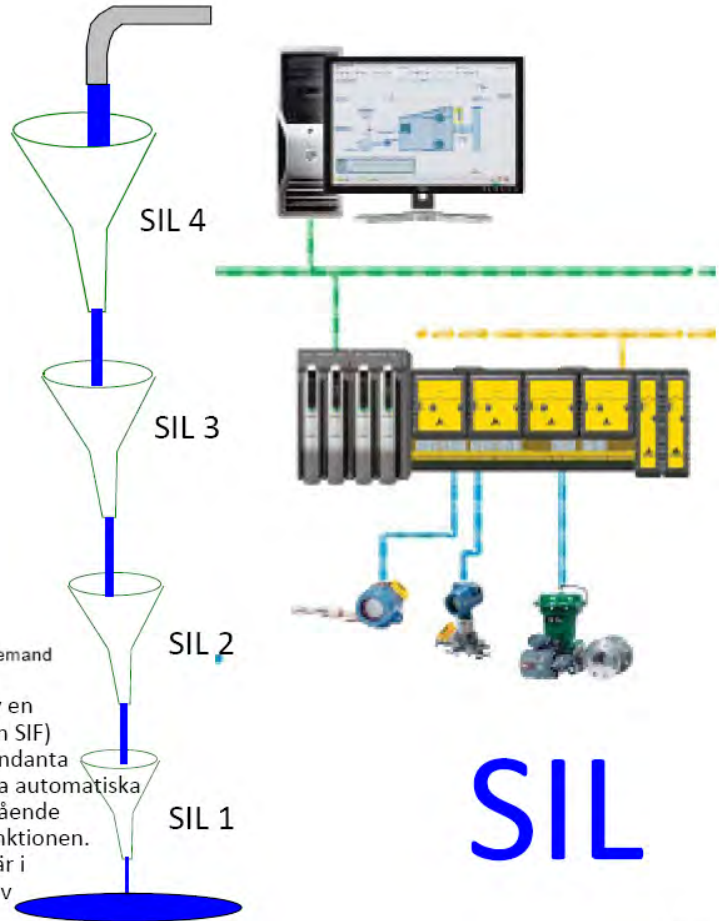
AC 800M High Integrity controller is SIL3-certified both in single and redundant configurations.



* Average probability of failure on demand

SIL Verifiering

Den säkerhetsintegrerade nivån (Safety Integrity Level SIL) av en hel säkerhetsinstrument funktion (Safety Instrument Function SIF) måste verifieras genom beräkning av $*PFD_{avg}$ beaktande redundanta arkitekturer, provningsintervall, effektivitetstester, eventuella automatiska kontroller, allmän reparationstid och feltåligheten på alla ingående produkter som ingår i den säkerhetsrelaterade instrumentfunktionen. Varje delsystem måste kontrolleras för att säkerställa att de är i överensstämmelse med med minsta tillåtna HFT hårdvarukrav (Hardware Fault Tolerance).



SIL

www.mpsa.se

SÄKERHETSKRITISK INSTRUMENTFUNKTION (SIF)

En instrumentfunktion som är avsedd att uppnå eller upprätthålla processens säkra läge i förhållande till en specifik farlig händelse. Instrumentfunktionen består alltid av tre delar: en givardel (en eller flera givare som avläser ett tillstånd i processen eller en order från en operatör), en logikdel (PLC eller reläer som knyter samman givardel och manöverdel) och en manöverdel (en eller flera manöverdon, exempelvis ventiler eller brytare, som kan föra processen till ett säkert läge)

IEC61508 är huvudstandarden för E/E/PES

IEC 61508 är en generell standard för (E)elektriska, (E) elektroniska och (PES) programmerbara elektroniska system, komponenter och system i säkerhetsapplikationer inom alla sektorer och vänder sig främst till tillverkare av komponenter.

För de komponenter som är godkända enligt EN 61508 anger tillverkaren den högsta SIL-nivå som komponenten klarar.

Säkerhets-PLC SmartGuard 600E



- Programmering via EtherNet/IP eller intern USB-port
- Möjlighet att distribuera säkra I/O
- Endast en kabel ut i anläggningen
- Enkel och överskådlig programvara

Säkerhetskategori

PL

SIL

PFH_d

4 enl. EN954-1

e enl. ENISO13849-1

3 enl. IEC 61508

3,89x10⁻¹⁰

Överensstämmelse mot Godkännanden

ODVA-överensstämmelse enligt DeviceNet och DeviceNet säkerhetskrav



Certificate / Certificat Zertifikat / 認証

KTEK 080349 C001

validity confirms that the

AT100, AT100s, AT200

Magnetostrictive Level Transmitter

K-TEK Corporation
Prairieville, LA
USA

Has been assessed per the relevant requirements of:

IEC 61508 Parts 1, 2, 3

and meets requirements providing a level of integrity to:

Systematic Integrity: SIL 3 Capable
Random Integrity: SIL 2 @ HFT=0,
SIL 3 @ HFT=1.

Safety Function:

The AT100, AT100s, and AT200 Magnetostrictive Level Transmitter uses a probe with float to detect a fluid level in a vessel. It subsequently communicates this level to a logic solver.

Application Restrictions:

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements, only the 4-20mA output is certified for use in functional safety applications.

Product Assessor

Auditor

STANDARD FÖR FUNKTIONSSÄKRA STYRNINGAR ENLIGT IEC 61508-SERIEN

Säkerhetsfunktioner i maskiner, processer och övriga styrningar hanteras mer och mer av (E)elektriska, (E)elektroniska eller (PE)programmerbara elektroniska system. (Benäms E/E/RE)

Tillvägagångssättet är

att konstruera styrningarna och systemet på ett sådant sätt att:

I rimligaste mån förhindra allvarliga fel eller ha koll på felen när de uppträder

HISTORIK SIL

ANSI/ISA S84.01 från 1996
definierade första gången
SIL-nivåerna 1-4 (Safety Integrity
Levels) för säkerhetskritisk
instrumentering.

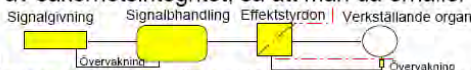
Nivåer av säkerhetsintegritet – SIL (Safety Integrated Level)

Standarden SS EN - IEC 61508 specificerar för varje säkerhetsfunktion fyra nivåer av säkerhetsprestanda. Dessa kallas säkerhetsintegritetsnivåer, där Säkerhetsintegritetsnivå 1 (SIL1) är den lägsta nivån av säkerhetsintegritet och Säkerhetsintegritetsnivå 4 (SIL4) är den högsta nivån. Standarden anger vilka detaljerade krav som ingår för varje säkerhetsintegritetsnivå. Dessa krav är strängare för de högre nivåerna av säkerhetsintegritet, så att man då erhåller den erforderliga lägre sannolikheten för farliga



Omfattar alla delar i systemet

Ett E/E/PE-säkerhetsrelaterat system innefattar alla systemdelar som är nödvändiga för att säkerhetsfunktionen ska utföras (dvs från sensor, genom styrlogik och kommunikationssystem, till utgångarnas ställdon, inklusive eventuellt kritiska åtgärder av en mänsklig operatör). Exempelvis fjärrstyrd övervakning, drift eller programmering av nätansluten processanläggning, HMI-system som hanterar säkerhet, säkerhetsrelaterade positionerings- och indikeringssystem, system som hanterar skyddsstopp och nödstop, larmhantering, varselsystem m.m.



Sektorimplementeringar finns även av standarden EN IEC 61508 i form av bl.a:

EN IEC 61511, Functional safety - Safety instrumented systems for the process industry sector;
EN IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
EN IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

Även järnvägssektorn har motsvarande sektorstandarder i form av
EN 50126; EN 50128 och EN 50129).

Per definition

SIL “discrete level (one out of possible three) for specifying the safety integrity requirements of the safety related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest”.

SIL “Safety integrity” omfattas av

- hardware safety integrity (relaterat till slumpmässiga hårdvarufel) och
- systematic safety integrity (relaterat till systematiska fel, t ex fel i designen)

SS EN 61508 (delar 1-7) är en standardserie för funktionssäkerhet i elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system och avser mera den som konstruerar en säkerhetsrelaterad styrmodul typ en säkerhetsanpassad PLC. Medans den som bygger in den säkerhetsrelaterade modulen typ en säkerhets PLC i ett maskinstyrssystem och gör applikationsprogramvaran normalt använder sig av SS EN ISO 62061-standarderna.

Tillverkare/konstruktörer av traditionella säkerhetsreläer kan tillämpa 13849-1.

I standarderna finns olika typer av riskgrafer som styr en fram till den säkerhetsnivå man skall bygga efter

Livscykelmodellen

I standarden IEC 61508 pratar man om en Säkerhetslivscykel (**Safety Life Cycle, SLC**).

Denna består av tre huvuddelar:

- analysfasen
- realiseringsfasen
- driftsfasen

I analysfasen görs en riskanalys och en detaljerad SRS (**Safety Requirements Specification**) tas fram som tar upp alla de säkerhetsfunktioner som är aktuella för systemet, vilka funktioner som kräver SIL samt vilken SIL-nivå.

I realiseringsfasen verifieras och kontrolleras att den design man gjort verkligen uppnår den SIL nivå som krävs enligt analysen.

I driftsfasen reder man ut hur säkerheten ska bibehållas (testintervall, underhåll mm)

Standarden IEC 61508 specificerar fyra nivåer av säkerhetsprestanda för varje säkerhetsfunktion.

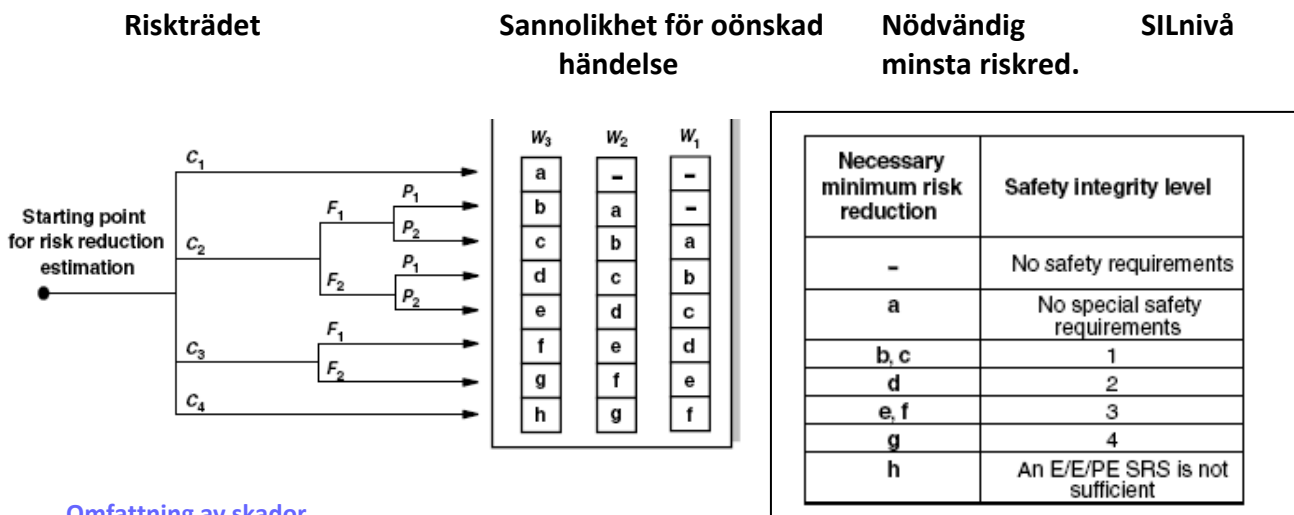
Dessa kallas säkerhetsintegritetsnivåer, där Säkerhetsintegritetsnivå 1 (SIL1) är den lägsta nivån av säkerhetsintegritet och Säkerhetsintegritetsnivå 4 (SIL4) är den högsta nivån. SIL 4 är inte för industritillämpning normalt.

Riskgrafen i 61508 RISKTRÄDET I IEC 61508

I samband med val av tekniska lösningar kommer man ofta in på frågeställningar kring säkerhet och hur bygga funktionssäkra kretsar.

Konstruktion och beräkning av en säkerhetskrets, kan tex. genomföras via SIL-bedömning d.v.s. Fastställa vilken säkerhetsnivå (t.ex. SIL2) som säkerhetskretsen skall följa.

I IEC 61508 (SS EN) används följande riskdiagram för att fastställa nivån:



Omfattning av skador

- C1:** Mindre personskador; mindre skadlig påverkan på omgivningen/miljön.
C2: Allvarliga, ej reversibla skador på en eller fler personer; temporära betydande skadlig inverkan på omgivningen/miljön.
C3: Dödsfall av fler personer; betydande och bestående skadlig inverkan på omgivningen/miljön.
C4: Katastrofala följder, många döda personer.

Hur ofta/hur länge är personer närvarande

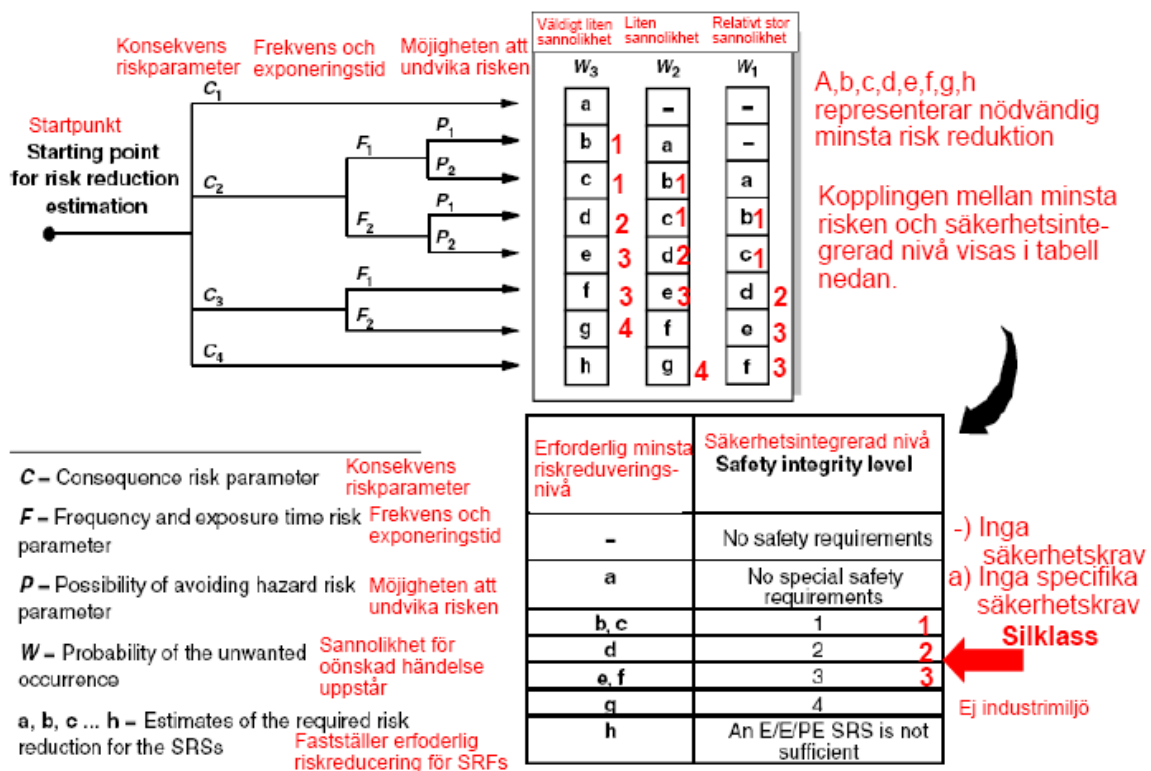
- F1:** Sällan till ibland.
F2: Ofta till permanent.

Undvikande av risk

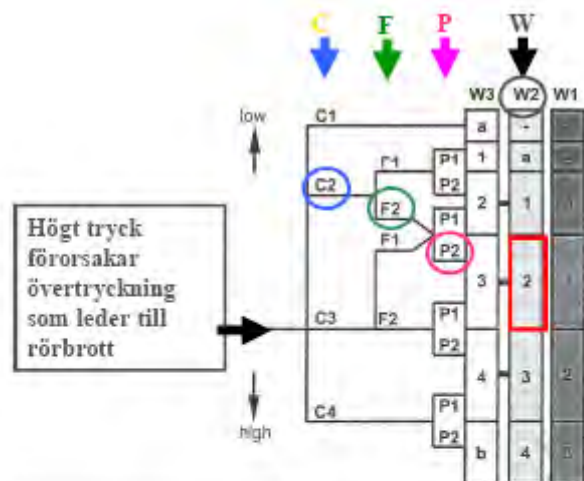
- P1:** Möjligt under speciella omständigheter.
P2: Knappast möjligt.

W Sannolikheten för oönskad händelse	W1 Väldigt liten sannolikhet att oönskad händelse skall ske och endast få oönskade händelser är då troliga. W2 Liten sannolikhet att oönskad Händelse skall uppstå och få oönskade händelser är troliga. W3 En relativ stor sannolikhet att oönskade händelser skall uppstå samt att frekventa oönskade händelser är troliga.
---	---

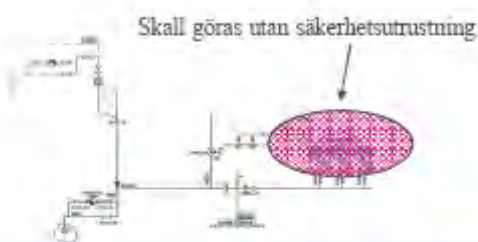
Sammanfattningsvis riskträdet för att komma fram till Säkerhetsintegrerade nivån (SIL-klass)



Riskbedömning i ett processsystem (Exempel från Dekra)



SIL-bedömning i ett processsystem



- a) Inga speciella säkerhetsåtgärder
- b) ett SIS är ohållbart

C = Skadans allvarighet
C1 = Obetydliga skador
C2 = En död eller flera svårt skadade
C3 = Flera dödade
C4 = "Massvis" med dödade

F = Varaktighet/ exponering av risken
F1 = Sällan till ganska ofta vid kort exponering
F2 = Ofta till kontinuerlig

P = Möjlighet att undvika risken
P1 = Möjlig under speciella förhållanden
P2 = Knappast möjlig

W = Sannolikhet
W1 = Mycket låg sannolikhet
W2 = Ringa sannolikhet
W3 = Mycket hög sannolikhet

C, F, P, W är värderade till siffrvärden ► PLL (Probable loss of life) som används vid beräkningar.
Den tolerabla riskvärdet bestäms av varje anläggning.

Sida 14 © 2013 DEKRA

SIL i olika nivåer

Vilka SIL som används beror även på hur säkerhetsfunktionen används.

Vid kontinuerlig användning fås SIL enligt "high demand mode" (se tabell 2), exempelvis tvåhandsmanöverdon.

Vid periodisk användning, det vill säga funktioner som används sällan, fås SIL enligt "low demand mode" (se tabell 3).

Exempel kan vara nödstoppsfunktion. Måttet 'sällan' uppskattas till ungefär 1 gång/år.

Skillnaden mellan de två "moderna" är att om säkerhetsfunktionen används sällan – "low demand mode" formuleras kravet som sannolikheten att ett fel har orsakat att säkerhetsfunktionen inte fungerar precis då funktionen ska användas.

Vid "high demand mode" formuleras kravet som sannolikheten för att ett fel inträffar per timma och som orsakar att säkerhetsfunktionen inte fungerar. Val av SIL beror även i denna standard på en genomförd riskanalys med hjälp av en riskgraf.

**Tabell 2: SIL enligt IEC 61508
– "Low demand mode".**

SIL	Sannolikhet för fel i funktion
-----	-----------------------------------

4	$\geq 10^{-5}$ till $< 10^{-4}$
3	$\geq 10^{-4}$ till $< 10^{-3}$
2	$\geq 10^{-3}$ till $< 10^{-2}$
1	$\geq 10^{-2}$ till $< 10^{-1}$

**Tabell 3: SIL enligt IEC 61508
– "High demand mode".**

SIL	Sannolikhet för fel per timma
-----	----------------------------------

4	$\geq 10^{-9}$ till $< 10^{-8}$
3	$\geq 10^{-8}$ till $< 10^{-7}$
2	$\geq 10^{-7}$ till $< 10^{-6}$
1	$\geq 10^{-6}$ till $< 10^{-5}$

Den mastiga strukturen på 61508 och dess 7 delar



SSEN 61508-1-2-3-4-5-6-7

Del 1

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system –
Del 1: Allmänna fordringar

Functional safety of electrical/electronic/programmable electronic safety-related systems –
 Part 1: General requirements

Del 2

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system –
Del 2: Fordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system

Functional safety of electrical/electronic/programmable electronic safety-related systems –
 Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

Del 3

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system –
Del 3: Fordringar på programvara

Functional safety of electrical/electronic/programmable electronic safety-related systems –
 Part 3: Software requirements

Del 4

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system –
Del 4: Definitioner och förkortningar

Functional safety of electrical/electronic/programmable electronic safety-related systems –
 Part 4: Definitions and abbreviations

Del 5

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system –
Del 5: Exempel på metoder för bestämning av säkerhetsnivåer

Functional safety of electrical/electronic/programmable electronic safety-related systems –
 Part 5: Examples of methods for the determination of safety integrity levels

Del 6

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system –
Del 6: Vägledning vid tillämpning av IEC 61508-2 och IEC 61508-3

Functional safety of electrical/electronic/programmable electronic safety-related systems –
 Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

Del 7

Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system
Del 7: Översikt över metoder och åtgärder

Functional safety of electrical/electronic/programmable electronic safety-related systems
 Part 7: Overview of techniques and measures

Table 2 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 3 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 4 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 5 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 6 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 7 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 8 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 9 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 10 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 11 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 12 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 13 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 14 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 15 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 16 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Table 17 - Safety integrity levels: target failure measures for a safety function operating in high demand mode at operation

Safety integrity level	Target failure measure
1	1.0E-5 to 1.0E-4
2	1.0E-6 to 1.0E-5
3	1.0E-7 to 1.0E-6

Två huvudkoncept

I standarden är de två koncepten "safety lifecycle" och "safety integrity level" fundamentala för tillämpningen.

"Safety lifecycle" betyder att alla faser från idé, design, implementering, drift och underhåll till skrotning av det säkerhetskritiska systemet innefattas av standarden.

Innehållet i standarden kan kort sammanfattas i följande punkter:

- specifikation av krav för att uppnå funktionssäkerhet men inga regler för vem som är ansvarig för att implementera kraven.
- gäller när utrustning som uppfyller kraven i IEC 61508 är integrerade i system i processindustrin. Standarden gäller inte när en tillverkare vill visa att utrustning är lämplig för säkerhetssystem.
- gäller när mjukvara är utvecklad med begränsat programspråk eller konfigureringspråk men inte för mjukvara utvecklad med högnivåspråk.
- redogör för sambanden mellan säkerhetsfunktioner och övriga instrumentfunktioner.
- resulterar i identifikation av säkerhetsfunktioner och krav på dess SIL med hänsyn till den riskreduktion som sker på andra sätt.
- specifikation av krav på systemens arkitektur och hårdvarans konfiguration samt applikation av mjukvara.
- kraven på mjukvara innefattar följande:
 - kontroll i hela livscykeln på att fel inte byggs in och kontroll på de fel som uppstår
 - information om hur systemet valideras måste ges till organisationen som integrerar systemet
 - förberedande av information och procedurer för drift, underhåll och modifieringar i systemet.

- gäller när säkerhetskritiska funktioner används för att uppnå funktionssäkerhet för personal, allmänhet och miljön. Kan även användas för icke-säkerhetsfunktioner som skyddar egendom.
- kräver att riskanalyser görs för att definiera kraven på funktionssäkerhet och SIL för varje kritisk instrumentfunktion.
- fastställer numeriska mål för medelsannolikheten för fel vid anrop och frekvensen av farliga fel per timma för olika SIL.
- definierar den högsta prestanda (SIL 4) som kan uppnås på säkerhetskritiska instrumentfunktioner genom att följa denna standard.
- definierar vilken som är den lägsta prestanda (SIL 1) som säkerhetskritiska instrumentfunktioner måste ha för att standarden ska gälla.
- tillhandahåller ett ramverk för hur SIL fastställs men fastställer inga värden för specifika applikationer.
- fastställer krav på alla delar i ett säkerhetssystem, från sensor till manöverdon.
- kräver att hänsyn tas till mänskliga fel vid design av säkerhetskritiska instrumentfunktioner.
- ställer inga direkta krav på individer bland operatörer och underhållspersonal.

Programmering

Tre olika typer av programmeringsspråk används för SIS Konfigurering, begränsade programspråk och högnivåspråk. Konfigurering innebär att användaren endast kan göra mindre förändringar till exempel ändra området för en transmitter. Med ett begränsat programspråk finns färdig-programmerade funktioner som användaren kan kombinera för att uppnå det som funktionen ska göra. Begränsat programspråk används bland annat i PLC:er. Högnivåspråk är det som används för att programmera datorer, till exempel C++, Pascal och Java.

IEC 61511 rekommenderar användning av konfigurering eller begränsade programspråk. Om högnivåspråk används, vilket inte är förbjudet enligt standarden, ska applikationen vara utvecklad enligt IEC 61508. Trots att de mjukvarubaserade säkerhetssystemen nu är utvecklade enligt IEC 61508 anses de fortfarande mer opålitliga än de traditionella "hardwired" systemen.



Tomas Beäff MPSA

Orsaken till detta är enligt många att inga ny programmeringsspråk, eller ens modifieringar av redan existerande, har utvecklats för säkerhetsapplikationer.

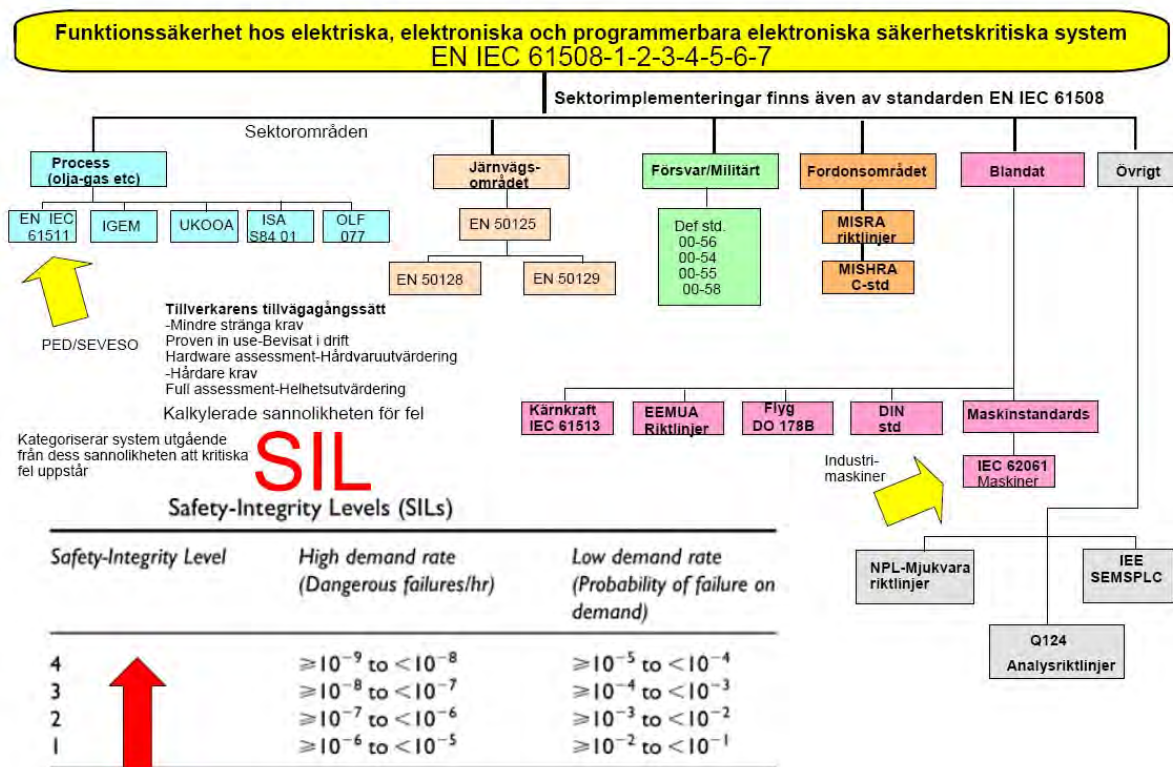
Mjukvaran blir inte för gammal men när den teknologiska utvecklingen går framåt kan det bli svårt att hantera den. SIS programmen måste gå att komma åt. Kontrollen att programmet stämmer överens med säkerhetskraven genomförs i tre steg: förståelse för designens syfte, genomgång av programmet av oberoende person samt verifikation av programmets verkställande. Verifikationen sker genom tester. Testerna är mycket viktiga man anser att det inte går att testa för mycket. Om programmet innehåller fel kommer inte SIS att kunna fungera.

Att göra ändringar i programmet bör behandlas på samma sätt som modifieringar i processen.

Det är även viktigt att kontrollera att ändringarna inte påverkar några andra funktioner.

Sektorimplementeringar av EN IEC 61508

IEC 61508 är främst tänkt att användas vid konstruktion av enskilda komponenter som ska ingå som en del av en säkerhetsfunktion, medan sektorstandarder t.ex. IEC 61511 och IEC 62061 beskriver hur man bygger upp den kompletta säkerhetsfunktionen utgående från komponenter konstruerade m.h.a IEC 61508.



T Beäff MPSA

*För maskinområdet tillämpar vi då Maskinstandards och detta blir då EN IEC 62061
 Inom processidan tillämpas då EN 61511.*

Tillämpning av Sektorstandarden EN 62061 för maskiner

SS EN IEC 62061 om funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system är fastställd sedan 23 maj 2005.

(Finns även **IEC 61511** som är en sektorstandard för processindustrin)

IEC 61511 är SIL-standarden som är specialiserad mot processindustrin.

För hela eller delar av en skyddsfunktion som är mekanisk-hydraulisk eller pneumatisk tillämpas dock normalt SS EN ISO 13849-1 då inte

EN ISO 62061 täcker detta (Non electrical e.g hydraulics).

62061 täcker då endast lösningar som är elektriska, elektroniska och programmerbara

EN IEC 62061- Styrssystem för maskiner

När det gäller SIL för styrssystem för maskiner, är det IEC 62061 som är den standard som är specialiserad mot maskiner.

EN 62061 är inte en designstandard utan till skillnad mot EN ISO 13849-1 ger den en metodik som tillverkare kan följa för att verifiera att den valda styrsystemstrukturen uppfyller de uppställda säkerhetskraven.

I EN 62061 betecknar man säkerhetsnivåerna med **SIL (Safety Integrity Level)** nivå 1-3 där 3 är den högsta nivån.

EN 62061 förklarar hur man kombinerar felsäkra automationssystem med felsäkra komponenter”

Denna standard behandlar hur man kan sätta samman komponenter/system som är SIL-klassade och komponenter som inte är SIL klassade.

1. SIL-klassade komponenter tex: (Komplexa komponenter)

Erhålla SIL värde från tillverkaren (SIL 1-3)

Eller erhålla PFHd (Sannolikhet för farligt fel per timma)

- Säkerhets PLC
- Ljusridå
- Säkerhetsmoduler
- Servodrifter/ frekvensomformare

2. EJ SIL-klassade komponenter dvs elektromekaniska:(Lågkomplexa komponenter)

Beräkna B10 värde, beakta Kvoten farliga fel

- Nödstoppsdon
- Förreglingsbrytare
- Kontakter

Tillämpning av SIL innebär att man utför en systematisk granskning där fakta som t.ex. ett flödesschema, elschema och beräkningar tillsammans med riskbedömning och erfarenhetsgranskning ger ett mer kvalitativt säkerhetssystem.

Saker att ta hänsyn till när man arbetar med EN 62061.

SIL

HFT (Hardware Fault Tolerance)

PFHd (Probability Of random Dangerous Hardware Failures)

DC/SFF (Safe Failure Fraction)(Diagnostic Coverage)

CCF (Common Cause Failure)

SRECS (Safety Related Electrical Control System)

Elektrisk del i en maskins styrsystem, fel i denna kan leda till farlig situation.

SRCF (Safety Related Control Function)

Säkerhetsfunktion med tilldelad SIL-nivå, upprätthåller säkert läge eller förhindrar olycka.

SFF (Safe Failure Fraction)

Feltolerans av hårdvaran. Lämnas av tillverkaren.

DC (Diagnostic Coverage)

Systemets feldetekteringsförmåga.

PFH_D (Probability of dangerous Failure per Hour)

Sannolikhet av farligt fel/timme. Komponenttillverkaren deklarerar SIL, PFH_D och SFF.

Denna standard kan användas upp till den säkerhetsintegrerade nivå som kallas SIL 3. (SIL finns även som SIL 4 men mera för kärkraft och liknande områden) där de olika SIL-klasserna handlar om möjligt fel per timme och uttrycks Probability of dangerous Failure per Hour (PFHD)

Valet av eller konstruktionen av SRECS ska alltid uppfylla följande:

Krav på säkerhetsintegritet för maskinvara, bestående av

- Begränsningar i arkitekturen för säkerhetsintegritet för maskinvara
- Krav på sannolikheten för farliga slumpmässiga maskinvarufel plus krav på systematisk säkerhetsintegritet, bestående av
- Krav på undvikande av fel och
- Krav på kontroll av systematiska fel EN 62061 beskriver även krav på implementering av tillämpningsprogram.

Säkerhetsrelaterade parametrar för undersystem:

- SILCL: SIL-gräns
- PFHD: Sannolikhet för farliga fel per timme
- T1: Livslängd

Säkerhetsrelaterade parametrar för undersystemselement (enheter):

- λ : Felfrekvens
- B10: För slitagedelar
- T1: Livslängd
- T2: Diagnostiskt testintervall
- β : Mottaglighet för vanlig felorsak
- DC: Diagnostisk täckning
- SFF: Säker felandel
- HFT: Feltolerans för maskinvara

Flödesschema ur standard

EN 62061

Sannolikheten för farliga fel i varje säkerhetsrelaterad styrfunktion (SRCF), som ett resultat av farliga slumpmässiga maskinvarufel, ska vara lika med eller mindre än felträskelvärde, som definierats i specifikationerna för säkerhetskraven.

SIL som uppnås av SRECS mot bakgrund av arkitekturs begränsningar, ska vara mindre än eller lika med lägsta SILCL i ett undersystem som krävs för att utföra säkerhetsfunktionen.

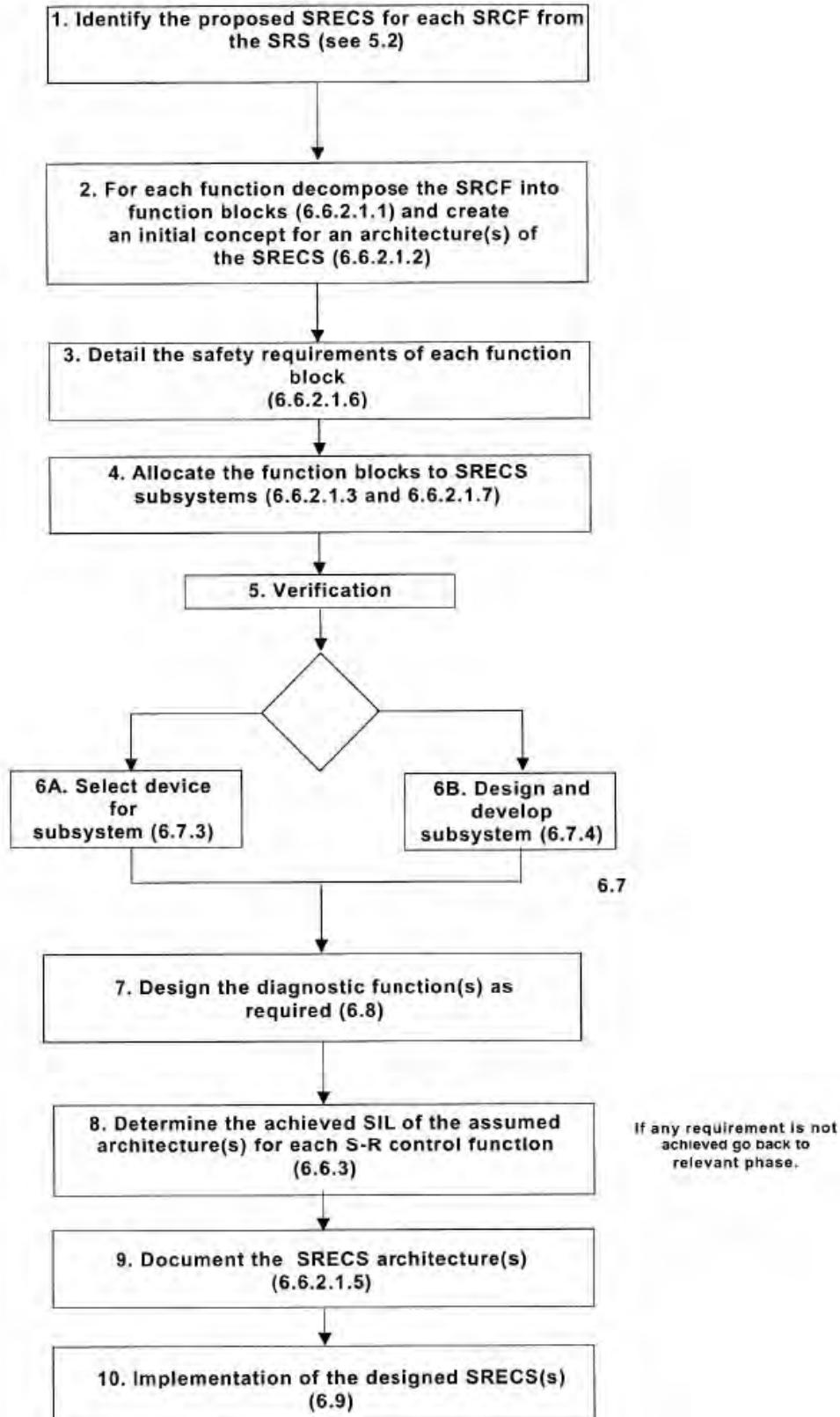
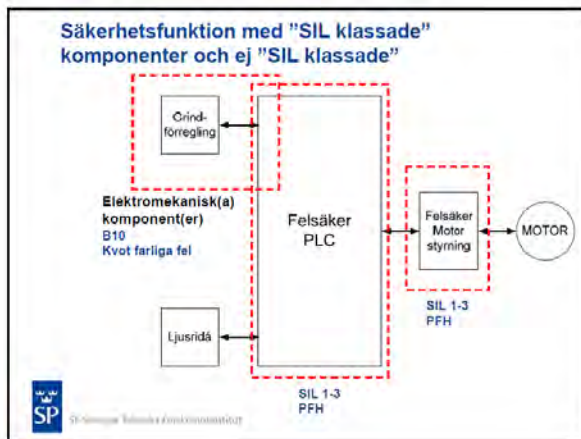
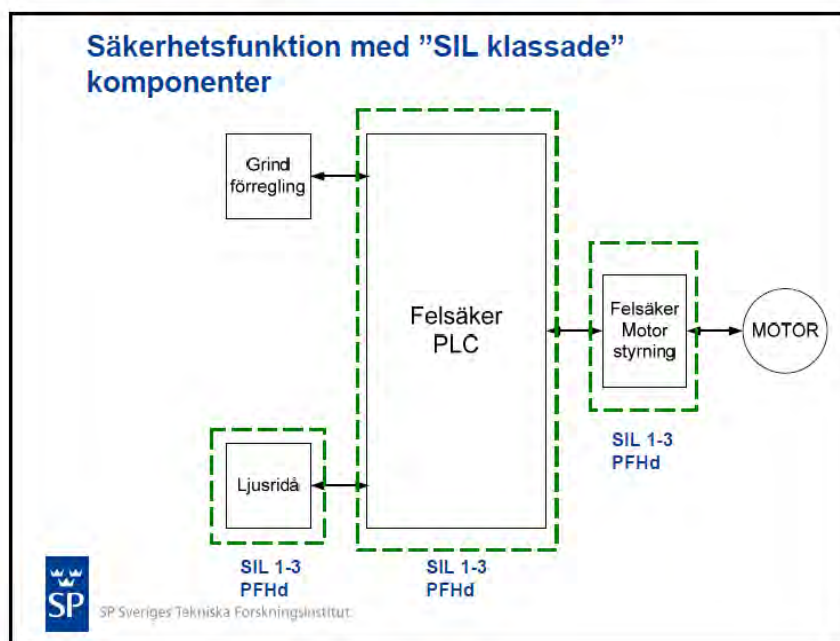


Figure 2 – Workflow of the SRECS design and development process

Exempelbild från (SP) Säkerhetsfunktion med SIL klassade komponenter och utan Silklassade (B10)



Säkerhetsfunktion med SIL klassade komponenter (SP)



SEK Teknisk rapport 62061-1 Utgåva 1, november 2010

En så kallad teknisk rapport CLC/TR 62061-1 finns som ger vägledning hur standarderna SS EN ISO 13849-1 och SS EN 62061 skall tillämpas.

Vägledning vid tillämpning av SS-EN ISO 13849-1 och SS-EN 62061 vid konstruktion av säkerhetsrelaterade styrsystem för maskiner

Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (CENELEC Technical Report 62061-1:2010)

TECHNICAL REPORT **CLC/TR 62061-1**

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

August 2010

ICS 13.110; 25.040.99; 29.020

English version

Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (IEC/TR 62061-1:2010)

Directives relatives à l'application de l'ISO 13849-1 et de la CEI 62061 dans la conception des systèmes de commande des machines relatifs à la sécurité (CEI/TR 62061-1:2010)

Anleitung zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen von Maschinen (IEC/TR 62061-1:2010)

This Technical Report was approved by CENELEC on 2010-07-26.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
 Comité Européen de Normalisation Electrotechnique
 Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

© 2010 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. CLC/TR 62061-1:2010 E

SEK Svensk Elstandard

Relationen mellan SIL och möjligt fel per timme PFH_D (EN 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 $< 10^{-5}$

NOTE Where the required safety integrity of a SRCF is less than SIL 1, as a minimum the requirements of category B of ISO 13849-1 should be met.

Relation mellan SIL och kategorier

När ett subsystem är konstruerat enligt EN ISO 13849-1 och validerat enligt EN ISO 13849-2 kan nedanstående relationer användas med avseende på arkitekturen.

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
3	1	< 60 %	SIL 1
	1	60 % – 90 %	SIL 2
4	>1	60 % – 90 %	SIL 3 (see Note 3)
	1	> 90 %	SIL 3 (see Note 4)

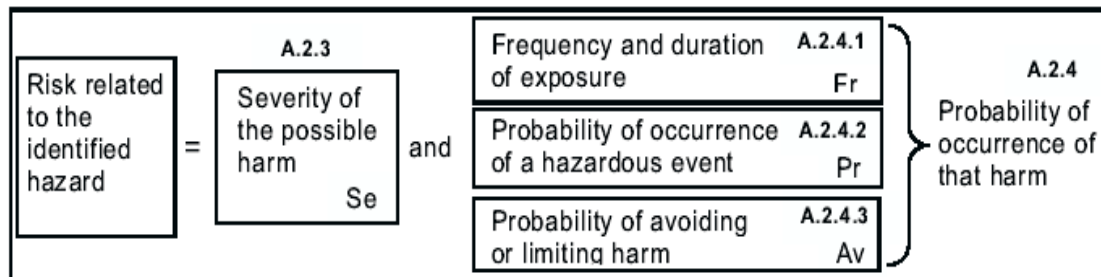
**Det finns även programvaror för att kalkylera SIL (hanterar oftast även PL)
 Tillexempel Pascal från PILZ.**



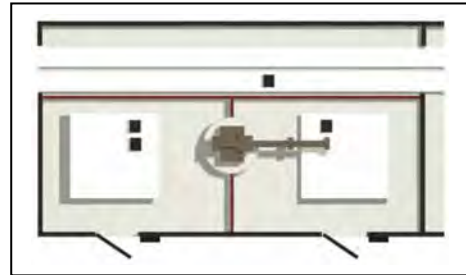
Bestämda arkitekturer enligt EN 62061

- EN 62061 har även bestämda arkitekturer för att förenkla beräkningen av PFH_D och därmed SIL-nivåerna
- Formlerna är förenklingar av tillförlitlighetsanalyser och har marginal åt det säkra hållet"
- Arkitekturer A - D

Riskbedömning enligt EN 62061



Exempel på standardkrav och ett tillämpningsexempel (Källa HSE UK) med riskbedömning för tilldelning av SIL för en robotcell med slipmaskin utifrån sektorstandardEN 62061.



Risker krossrisker mellan robot och slipmaskin (Grinding machine)

Beskrivning av Säkerhetsrelaterad styrfunktion (SRECS)

-Vid begäran om tillträde (förreglad grind) skall roboten förflytta sig till område X och slipmaskinen skall stanna inom 15 sekunder innan personal medges tillträde till Cell Y.

1. Bedöma skadans allvarlighet (EN 62061)

Table A.1 – Severity (Se) classification

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Product: _____
 Issued by: _____
 Date: _____

Black area
Grey area

Consequences	Severity	
Death, losing an eye or arm	4	SII 2
Permanent, losing fingers	3	
Reversible, medical attention	2	
Reversible, first aid	1	

Ser. No.	Hzd. No.	Hazard	Se
		Crushing	4

Skadans allvarlighet bedöms som en **4:a** (Allvarlig skada-Irreversibel skada, dödsfall).

2. Frekvensen och varaktigheten av exponeringen (EN 62061)

Följande är viktigt att ta i beaktning i samband med uppskattning av frekvensen för en viss riskfylld händelse:

- Vid uppskattning av frekvens skall man ej ta hänsyn till säkerhetsfunktioner (SRECS) utan enbart "Other technology" samt "External risk reduction".
- Mänskligt beteende då riskfyllda situationer kan uppstå, t.ex. stress på grund av tidsbrist samt bristande information och kunskap om hur man skall hantera situationen.

Table A.2– Frequency and duration of exposure (Fr) classification

Frequency and duration of exposure (Fr)	
Frequency of exposure	Duration > 10 min
≤ 1 h	5
> 1 h to ≤ 1 day	5
> 1 day to ≤ 2 weeks	4
> 2 weeks to ≤ 1 year	3
> 1 year	2

Om varaktigheten understiger 10 min kan nästa nivå tillämpa. Tabellen hanterar inte frekvens och exponering mindre än 1 timme.

Risk assessment and safety measures

Document No.: _____
 Part of: _____

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 C1	Class C2	Class C3	Class C4	Class C5	Frequency and duration, Fr	Probability of hzd event, Pr	Avoidance Av
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Very high
Permanent, losing fingers	3	OM	OM	SIL 1	SIL 2	SIL 3	> 1 h - <= day	5	Likely
Reversible, medical attention	2	OM	OM	OM	SIL 1	SIL 2	> 1 day - <= 2 wks	4	Possible
Reversible, first aid	1	OM	OM	OM	OM	SIL 1	> 2 wks - <= 1 yr	3	Rarely
							> 1 yr	2	Negligible

Table A.2– Frequency and duration of exposure (Fr) classification

Frequency and duration of exposure (Fr)		Safe
Frequency of exposure	Duration > 10 min	
≤ 1 h	5	
> 1 h to ≤ 1 day	5	
> 1 day to ≤ 2 weeks	4	
> 2 weeks to ≤ 1 year	3	
> 1 year	2	

Ser. No. _____ Hzd. No. _____

Comments _____

Frekvensen och varaktigheten av exponeringen bedöms till 2 veckor till < 1 år vilket ger en 3:a

3. Sannolikhet för att en farlig skadehändelse skall uppstå (EN 62061)

Table A.3– Probability (Pr) classification

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Risk assessment and safety measures

Document No.: _____
Part of: _____

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						Frequency and duration, Fr	Probability of hzd. event, Pr	Avoidance Av
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15				
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Very high	5
Permanent, losing fingers	3		DM	SIL 1	SIL 2	SIL 3	> 1 h - <= day	5	Likely	4
Reversible, medical attention	2			DM	SIL 1	SIL 2	> 1 day - <= 2wks	4	Possible	3
Reversible, first aid	1				DM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2
							> 1 yr	2	Negligible	1

Table A.3– Probability (Pr) classification

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Sannolikhet för att en farlig skadehändelse skall inträffa bedöms som mycket hög vilket ger en **5:a**.

4. Möjlighet att undvika eller begränsa en skada (EN 62061)

Då man uppskattar sannolikheten för att kunna undvika eller begränsa skadan skall man ta hänsyn till maskinens uppbyggnad samt dess tilltänkta användning, där bland annat följande aspekter är viktiga:

- Plötslig, snabb eller långsam hastighet då den riskfyllda händelsen uppstår.
- Möjligheterna att ta sig bort från riskområdet, t.ex. utrymningsvägar.

Table A.4– Probability of avoiding or limiting harm (Av) classification

Probabilities of avoiding or limiting harm (AV)	
Impossible	5
Rarely	3
Probable	1

Table A.6 – SIL assignment matrix

Severity (Se)	Class (CI)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

EXAMPLE: For a specific hazard with an Se assigned as 3, an Fr as 4, an Pr as 5 and an Av as 5 then:

$$CI = Fr + Pr + Av = 4 + 5 + 5 = 14$$

6. Skadans allvarlighet (Severity)

Table A.1 – Severity (Se) classification

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Risk assessment and safety measures

Document No. _____
Part of: _____

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 CI	Frequency and duration, Fr	Probability of hzd. event, Pr	Avoidance Av
Death, losing an eye or arm	4	SIL 2	<= 1 hour	Very high	5
Permanent, losing fingers	3	OM	> 1 h - <= 1 day	Likely	4
Reversible, medical attention	2	OM	> 1 day - <= 2 wks	Possible	3
Reversible, first aid	1	OM	> 2 wks - <= 1 yr	Rarely	2
			> 1 yr	Negligible	1

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

Table A.1 – Severity (Se) classification

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Comments _____

Detta ger om vi då utgår från Se 4 i linjen ut till kolumnen med poäng 11-13 (vi hade fått ihop 13) oss då SIL 3 som vi ser överst.

Vi kan sedan gå vidare och fylla i andra risker och värdera oavsett så har vi fått att säkerhetsåtgärden blir att krossriskerna skall hanteras av ett säkerhetsanpassat elektroniskt styrsystem SRECS= Safety Related Electronical Control System av SIL3.

Company name		Risk assessment and safety measures		Document No.: 101	
Product: Machining cells with conveyor. Cleaning at machine 1.				Part of:	
Issued by: WG 7				☒ Pre risk assessment	
Date: 2005-12-02		Black area = Safety measures required Grey area = Safety measures recommended		☐ Intermediate risk assessment	
				☐ Follow up risk assessment	

Consequences	Severity Se	Class Cl					Frequency and duration, Fr	Probability Pr	Avoidance Av
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15			
Death, losing an eye or arm	4						<= 1hour	5	Very high
Permanent, losing fingers	3						> 1 hr - <=day	5	Likely
Reversible, medical attention	2						>1day - <=2wks	4	Possible
Reversible, first aid	1						>2wks - <=year	3	Rarely
							> 1year	2	Negligible

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe
1	1.1	Crushing between robot and machine	4	3	5	5	13	SRECS	
2	1.2	Shearing from machine tool	3	3	4	3	10	SRECS	
3	1.1	Drawing in by the machine drive unit	3	3	4	3	10	SRECS	
4		Hazards ser nos. 2 & 3 due to access to momentum movement.	2	4	4	3	11	SRECS, SIL 1, SRCE no. 2	
5	1.7	Slipping on floor	2	5	3	3	11	PPE and instructions	

Comments

	Hzd. No. according to Annex A of ISO 14121:1999.
1	It is assumed that the "crushing between robot and grinding machine" hazard cannot occur at the same place as hazards ser. No. 2 and 3. Therefore they are independent hazards and have individual risk parameters. Consequently the safety measures are also i

7. SIL för hela säkerhetsfunktionen

- SIL CL Klass för varje subsystem skall räknas ut (PFH_d)
- Varje subsystem måste ha en SILCL som är minst lika hög som den SIL som hela funktionen skall uppnå, enligt principen inget är bättre en sämsta delen
- För hela funktionen; addera PFH_d för alla subsystem
- Ange SIL för hela funktionen (tabell 3 i EN 62061)
- T.ex $PFH_D = 3 \cdot 10^{-8} + 3 \cdot 10^{-8} + 3 \cdot 10^{-8} = 9 \cdot 10^{-8}$ vilket ger SIL 3

Riskklassificering SIL EN 62061.

På svenska (fritt översatt Tomas Beäff)

MPSA AB +46 553 14060 office +46 553 14911 fax +46 70 6406027 mobile www.mpsa.se		Grovanalysmetod-Hybridmetod Baserad på metodik i EN ISO 14121-2 Fastställande av SIL-klass enligt EN 62061		Analysdeltagare: _____	
RISKBEDÖMNING OCH SILKLASSIFICERING					
Produkt/område: Robotstation med slipmaskin Utfärdat av: _____ Datum: _____		SÄKERHETSINTEGRERAD NIVÅ SIL (3) $\geq 10^{-8}$ till $< 10^{-7}$ 2 $\geq 10^{-7}$ till $< 10^{-6}$ 1 $\geq 10^{-6}$ till $< 10^{-5}$		Sannolikhet av allvarigt fel per timme (PFH D) Dokumentnummer: _____ Del av dokumentet/sida: _____ ☒ Inledande bedömning ☐ Mellanliggande analys ☐ Uppföljning av riskbedömning	
Rött område=Säkerhetsåtgärder krävs Grönt område=Säkerhetsåtgärder rekommenderas					
Konsekvens Dödsfall, förlust av kroppsdel Allvarlig skada-kvarstående men Reversibel skada-Kräver sjukvård Reversibel skada-Första hjälpen		Allvarlighet Se 4 3 2 1		Klass K1 (Fr + Pr + Av) 3-4 5-7 8-10 11-13 14-15 SIL 2 SIL 2 SIL 2 SIL 3 SIL 3 SIL 1 SIL 1 SIL 1 SIL 2 SIL 2 Om < SIL 1 skall Kat B EN ISO 13849-1 tillämpas	
		Frekvens Fr < 1 h 5 > 1 h till < 24 h 5 > 24 h till < 2 veckor 4 > 2 v till < 1 år 3 > 1 år 2		Sannolikhet Pr Mycket hög 5 Troligt 4 Möjligt 3 Knappast möjligt 2 Försumbar 1	
		Möjligt att undvika Av 5 3 2 1			
Nr 1. 2.		Risk nr Enligt bilaga A EN ISO 14122-1 1.1 1.2		Risk Krossrisk mellan robot och slipmaskin Skärrisk på maskinverktyg	
		Se Allvarlighet 4 3		Fr Frekvens 3 3	
		Pr Sannolikhet 5 4		Av Möjliggör att undvika 5 3	
		K1 13 10		Skyddsåtgärder SRECS (Säkerhets PLC) SIL 3	
		Tillräckligt säkert Ja Nej			
Kommentarer enligt Nr _____ _____ _____					
		Ansvarig för åtgärd _____ _____ _____		Åtgärdsdatum _____ _____ _____	
		Uppföljning _____ _____ _____			

MPSA AB +46 553 14060 office +46 553 14911 fax +46 70 6406027 mobile www.mpsa.se		Grovanalysmetod-Hybridmetod Baserad på metodik i TR ISO 14121-2 Fastställande av SIL-klass enligt EN 62061		Analysdeltagare Tomas Beäff, Håkan Jonsson, Lennart Rejlmalm																																																																							
RISKBEDÖMNING OCH SILKLASSIFICERING																																																																											
Produkt/område: Folding Blades omrörare- K 163-63 Utfärdat av: Tomas Beäff Datum: Januari 2011		Dokumentnummer: 2011-01-01 Del av dokumentet/sida: 1 ☐ Inledande bedömning ☒ Mellanliggande analys ☐ Uppföljning av riskbedömning																																																																									
Rött område=Säkerhetsåtgärder krävs Grönt område=Säkerhetsåtgärder rekommenderas																																																																											
<table border="1"> <thead> <tr> <th>Konsekvens</th> <th>Allvarlighet</th> <th colspan="5">Klass K1 (Fr + Pr + Av)</th> <th>Frekvens</th> <th>Sannolikhet</th> <th>Möjligt att undvika</th> </tr> <tr> <th></th> <th>Se</th> <th>3-4</th> <th>5-7</th> <th>8-10</th> <th>11-13</th> <th>14-15</th> <th>Fr</th> <th>Pr</th> <th>Av</th> </tr> </thead> <tbody> <tr> <td>Dödsfall, förlust av kroppsdel</td> <td>4</td> <td>SIL 3</td> <td>SIL 2</td> <td>SIL 2</td> <td>SIL 3</td> <td>SIL 3</td> <td>< 1 h</td> <td>5</td> <td>Mycket hög</td> </tr> <tr> <td>Allvarlig skada-kvarstående men</td> <td>3</td> <td></td> <td></td> <td>SIL 1</td> <td>SIL 2</td> <td>SIL 3</td> <td>> 1 h till < 24 h</td> <td>5</td> <td>Troligt</td> </tr> <tr> <td>Reversibel skada-Kräver sjukvård</td> <td>2</td> <td></td> <td></td> <td></td> <td>SIL 1</td> <td>SIL 2</td> <td>> 24 h till < 2 veckor</td> <td>4</td> <td>Möjligt</td> </tr> <tr> <td>Reversibel skada-Första hjälpen</td> <td>1</td> <td></td> <td></td> <td></td> <td></td> <td>SIL 1</td> <td>> 2 v till < 1 år</td> <td>3</td> <td>Knappast möjligt</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>> 1 år</td> <td>2</td> <td>Försumbar</td> </tr> </tbody> </table>		Konsekvens	Allvarlighet	Klass K1 (Fr + Pr + Av)					Frekvens	Sannolikhet	Möjligt att undvika		Se	3-4	5-7	8-10	11-13	14-15	Fr	Pr	Av	Dödsfall, förlust av kroppsdel	4	SIL 3	SIL 2	SIL 2	SIL 3	SIL 3	< 1 h	5	Mycket hög	Allvarlig skada-kvarstående men	3			SIL 1	SIL 2	SIL 3	> 1 h till < 24 h	5	Troligt	Reversibel skada-Kräver sjukvård	2				SIL 1	SIL 2	> 24 h till < 2 veckor	4	Möjligt	Reversibel skada-Första hjälpen	1					SIL 1	> 2 v till < 1 år	3	Knappast möjligt								> 1 år	2	Försumbar				
Konsekvens	Allvarlighet	Klass K1 (Fr + Pr + Av)					Frekvens	Sannolikhet	Möjligt att undvika																																																																		
	Se	3-4	5-7	8-10	11-13	14-15	Fr	Pr	Av																																																																		
Dödsfall, förlust av kroppsdel	4	SIL 3	SIL 2	SIL 2	SIL 3	SIL 3	< 1 h	5	Mycket hög																																																																		
Allvarlig skada-kvarstående men	3			SIL 1	SIL 2	SIL 3	> 1 h till < 24 h	5	Troligt																																																																		
Reversibel skada-Kräver sjukvård	2				SIL 1	SIL 2	> 24 h till < 2 veckor	4	Möjligt																																																																		
Reversibel skada-Första hjälpen	1					SIL 1	> 2 v till < 1 år	3	Knappast möjligt																																																																		
							> 1 år	2	Försumbar																																																																		
Nr	Risk nr Enligt bilaga A EN ISO 12100	Risk	Se Allvarlighet	Fr Frekvens	Pr Sannolikhet	Av Möjlighet att undvika	K1	Skyddsåtgärder	Tillräckligt säkert Ja Nej																																																																		
1	1-6.2.3	Krossrisk propeller-fast del kärl	3	4	4	3	11	SRECS som uppfyller >minst SIL 2	X																																																																		
2	1-6.2.6	Insnärkning öppen axel, klister på	3	4	4	3	11	SRECS som uppfyller >minst SIL 2	X																																																																		
3	1-6.4.3	Slag stötskada mot roterande axel	2	4	4	3	11	SRECS som uppfyller >minst SIL 1	X																																																																		
Kommentarer enligt Nr		Exempel riskställen omrörare 																																																																									
1	Högsta risken ger säkerhetssystem av minst SIL 2 klass enligt EN 62061. Förregling och skydd som täcker roterande propeller samt axelskydd monteras.		Ansvarig för åtgärd		Åtgärdsdatum		Uppföljning																																																																				
			Casco Adhesives AB		2011-06		Åtgärdat juni 2011																																																																				

Standarder är inte tvingande och typ av standard är valfri att tillämpa

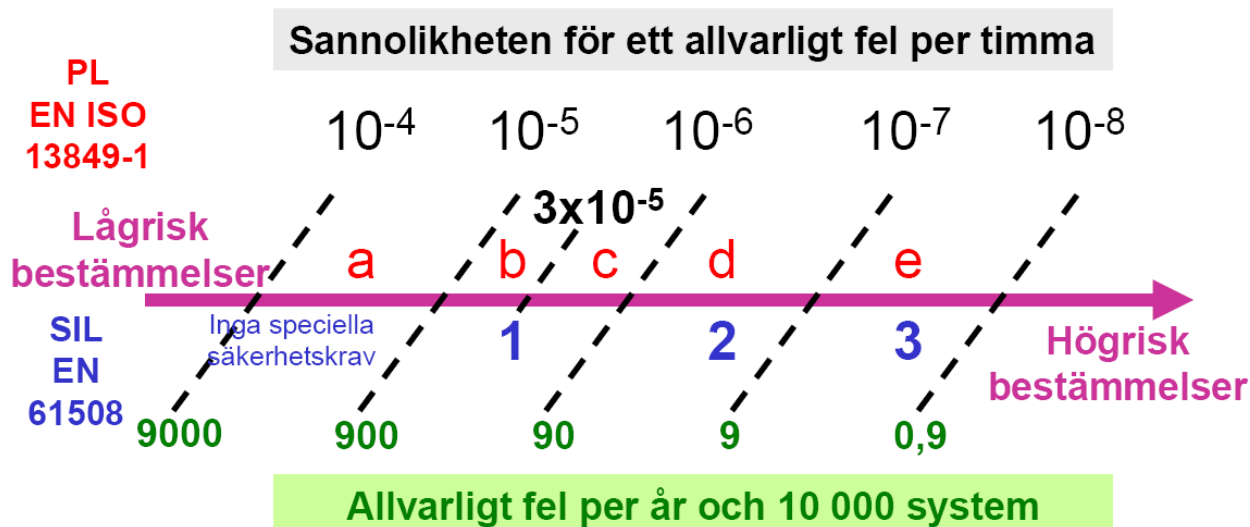
Om man väljer att tillämpa dessa två standarder kommer det att vara valfritt att använda sig av antingen EN ISO 13849-1 eller EN 62061, d.v.s. båda standarderna leder till i princip samma resultat men på olika tillvägagångssätt.

Vem väljer man

Man kan alltså välja vilken standard som passar bäst från fall till fall. Är man van att arbeta efter EN 61508 så kan EN 62061 vara lämplig men är man van den gamla EN 954-1 standarden med kategorierna så känner man igen sig mer i efterföljaren EN ISO 13849-1.

Prestandanivån och SIL (Säkerhetsintegrerad nivå)

Definitionen av PL och relationen till SIL



Riktlinjer för avgränsning mellan EN 62061 och EN ISO 13849-1 finns i tabell

(vilken standard som bör tillämpas i specifika sammanhang).

Sambandet mellan de tre viktigaste standarderna för funktionssäkerhet

OBSERVERA att EN 61508 inte är harmoniserad med maskindirektivet

	EN 61508	EN 62061	EN ISO 13849-1
Industrisegment	Allmänt	Industriautomation	Industriautomation
Säkerhetsfunktion	Säkerhetsfunktion	Säkerhetsrelaterade kontrollfunktioner (SCRF)	Säkerhetsfunktion
Säkerhetsplattform	Säkerhetsrelaterade system	Säkerhetsrelaterade elektriska kontrollsystem (SRECS)	Säkerhetsrelaterade delar av kontrollsystem (SRP/CS)
Typ av produkter	Komponenter	System	Komponenter/System
Riskreduceringsnivåer	SIL 1-4	SIL 1-3	PL a-e
Kräver beräkning av hårdvarufelssannolikhet	Ja	Ja	Ja
Hårdvarufelssannolikhets-förkortning	PFD/PFH	PFH	MTFF _d
Standarden inkluderar en säkerhetslivscykel	Ja	Ja	Ja
Riskgrupper som hanteras av standarden	Personsäkerhet, miljö, ergonomi	Personsäkerhet	Personsäkerhet
Risktyper som hanteras av standarden	Generell	Risker direkt relaterade till en maskin eller en grupp av maskiner	Risker direkt relaterade till en maskin eller en grupp av maskiner
Harmonisering under EU-direktiv	Nej	Ja, maskindirektivet	Ja, maskindirektivet

Rekommenderad tillämpning

Gränssnitt mellan EN ISO 13849-1 och EN 62061

Teknik	EN ISO 13849-1	EN 62061
A Inte elektrisk som hydraulik	Behandlas	Behandlas inte
B Elektromekanisk som reläer, och/eller inte komplex elektronik	Begränsat till systemarkitektur och upp till PL = e	Alla arkitekturer och upp till SIL = 3
C Komplex elektronik som programmeras	Begränsat till systemarkitektur och upp till PL = d	Alla arkitekturer och upp till SIL = 3
D A kombinerad med B	Begränsat till systemarkitektur och upp till PL = e	
E C kombinerad med B	Begränsat till systemarkitektur och upp till PL = d	Alla arkitekturer och upp till SIL = 3
F C kombinerad med A, eller C kombinerad med A eller B	Begränsat till systemarkitektur och upp till PL = d	Alla arkitekturer och upp till SIL = 3 utom elektriska system

Table 1 — Recommended application of IEC 62061 and ISO 13849-1

	Technology implementing the safety-related control function(s)	ISO 13849-1	IEC 62061
A	Non-electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, and/or non complex electronics	Restricted to designated architectures ^a and up to PL = e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures ^a and up to PL = d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures ^a and up to PL = e	X ^c
E	C combined with B	Restricted to designated architectures (see Note 1) and up to PL = d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X ^b	X ^c
X indicates that this item is dealt with by the International Standard shown in the column heading.			
^a Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.			
^b For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.			
^c For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.			

Likheter mellan de olika standarderna översiktligt

ISO 13849-1 Annex A requires **PL e**

IEC/EN 62061 Annex A requires **SIL 3**

There can be equivalency

Performance level (PL)	Average probability of a dangerous failure per hour [1/h]	SIL [EN 61508-1 (IEC 61508-1)] for information
a	$\geq 10^{-5}$ to $< 10^{-4}$	no special safety requirements
b	$\geq 3 \cdot 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \cdot 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Category B	PL a	-
Category 1	PL b	SIL 1
Category 2	PL c	
Category 3	PL d	SIL 2
Category 4	PL e	SIL3

Approximate equivalency

Category of EN 954-1	1	2	3	4
Safety Integrity Level of EN 62061:2005	SIL 1	SIL 1	SIL 2	SIL 3
Performance Level of EN ISO 13849-1:2008	PL b	PL c	PL d	PL e

Tidigare standarden EN 954-1 som ersätts av EN 13850-1 har även ett riskträd men detta inriktade sig bara på kategorierna och ej systemets helhet och beaktade inte felkaraktäristiken på ingående komponenter.

STANDARDER GER NIVÅER

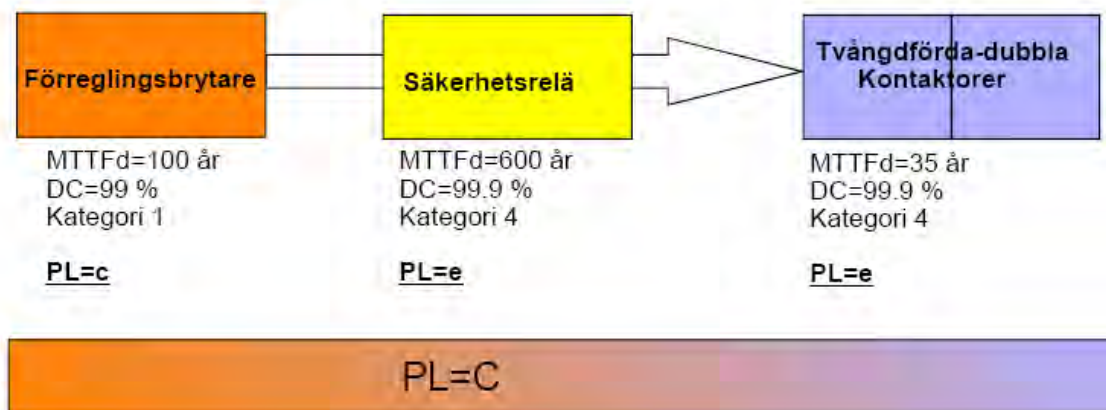
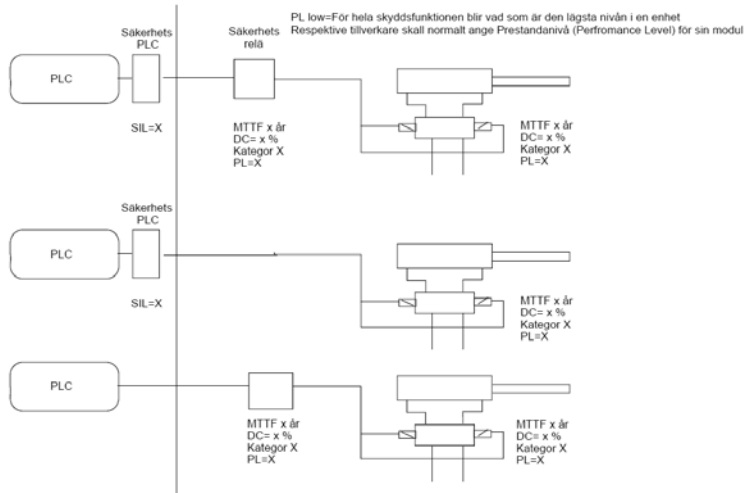
Olika typer av C-standarder har anpassats eller anpassas till dessa nya standarderna och där anges den nivå som standardiseringsgruppen bedömt relevant för aktuell maskin- och skyddsfunktion.

Här ett exempel ur prEN 1034-17 för Tissue maskiner avseende hur det kan se ut
 Där kategorier och SIL-tal fastställts.

Table 3 — List of safety functions, Performance Level and Safety Integrity Level specified in this standard

Safety function	Clause of this standard	Performance Level (at least)	Safety Integrity Level (at least)
start-up warning (interlocking function)	5.3.5	PL c	SIL 1
emergency stop of sectional drives	5.4.3	PL d	SIL 2
emergency stop of linear or swivelling moved parts	5.4.3	PL c	SIL 1
Prevention of unexpected start-up of the sectional drives	5.5.2	PL d	SIL 2
Feedback-function of the device for Prevention of unexpected start-up	5.5.2	PL c	SIL 1
limitation of maximum speed	5.6.3	PL c	SIL 1
limitation of crawl speed	5.6.4 a)	PL c	SIL 1
limitation of crawl speed, (higher risk)	5.6.4 b)	PL d	SIL 2
Hold-to-run function for applying doctor blades	5.12.6	PL b	SIL 1
Safety function protecting water jet knives, tail cutter and severing devices	5.21.1	PL d	SIL 2
Hold-to-run function for movement of machine parts	5.27.1	PL c	SIL 1
Safety function protecting the closing movement of the hood	5.29.5	PL c	SIL 1
Interlocking of safety devices on inrunning nips of calenders	5.30.2	PL d	SIL 2
Safety function of safety devices on measuring units	5.31.1	PL b	SIL 1
Interlocking of safety devices for primary arms	5.32.3	PL d	SIL 2
Interlocking with guard locking on the area of parent reel kick out	5.32.4	PL d	SIL 2
Guiding of reel shafts	5.32.9	PL d	SIL 2
Interlocking of device safeguarding the roll handling equipment in the reel section or in the near vicinity	5.33.1	PL d	SIL 2
Interlocking of the safety device on the opening of the pneumatic tool	5.33.2	PL d	SIL 2
Interlocking of safety device on machine pulper	5.34.1	PL d	SIL 2

Tillämpning



Exempel på hur en tillverkare resonerar

Calculating SIL suitability levels

For General Monitors, calculating the SIL suitability level for individual products is a combined effort between corporate quality, engineering, and a 3rd party for validating calculations. The steps include failure rate prediction, FMEDA, Failure Path Investigation, and a 3rd party validation.

Step 1 Failure Rate Prediction

This initial step is the basis of all product SIL calculations. Within the product all failure rates of individual components contribute to the overall product failure rate.

1. Failure rates of individual components of the BOM

are calculated based on component type and in-circuit bias.

- Product failure rate is the sum of all component failure rates.

Step 2 Failure Mode Effects and Diagnostic Analysis (FMEDA)

Failure Mode Effects and Diagnostic Analysis (FMEDA) is a technique that evaluates and quantifies the product's self-diagnostic ability.

Each component's failure mode and its failure rate are listed.

Failure modes are determined as Safe (product able to detect fire/gas) or Dangerous (product not able to detect fire/gas).

Each safe and dangerous failure mode is determined as Detectable or Un-detectable by the product's diagnostics.

The result is a list of all components, their failure modes, the failure mode classification as Safe-Detected (SD), Safe-Undetected (SU), Dangerous-Detected (DD) or Dangerous-Undetected (DU), and the failure rate of each classification using the Failure Rate Prediction results (ISD, ISU, IDD, IDU).

Step 3 Failure Path Investigation

Known failure modes that were not classified during the FMEDA step are investigated using actual product. This requires shorting and opening component leads and identifying failure classification. SD, SU, DD, DU.

Step 4 Calculate SFF, SIL and PFD

The SIL level of the product is finally determined from the Safe Failure Fraction (SFF) and the Probability of Failure on Demand (PFD).

The following formulas are used.

$$SFF = (ISD + ISU + IDD) / (ISD + ISU + IDD + IDU)$$

$$PFD = (IDU)(\text{Proof Test Interval})/2 + (IDD)(\text{Down Time or Repair Time})$$

SIL level is then determined from the Safe Failure Fraction for type B equipment per the IEC 61508 table below.

Safe Failure Fraction	Hardware Fault Tolerance*		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% - <90%	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 2	SIL 3	SIL 4
? 90%	SIL 3	SIL 4	SIL 4

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



Tomas Beäff MPSA

Step 5 Third Party Review

All results from the above steps are forwarded to a 3rd party for review and validation.

Definitions

MTBF = Many times a customer will ask for the MTBF (mean time between failures) value of a product. This is calculated by the inverse of unit failure rate minus the MTTR (mean time to repair, usually 4 hours for General Monitors products).

The MTTR may be dropped if it is very small compared to the overall product device hours.

$$MTBF = 1/\text{Failure Rate}$$

An expression for the Risk Reduction Factor is...

$$RRF = (\text{existing or inherent risk}) / (\text{tolerable or acceptable risk})$$

Probability of Failure on Demand (PFD) = the probability that a SIF fails to perform its intended safety function during a potentially dangerous condition. This is also called a dangerous failure.

The Average Probability of Failure on Demand (PFDavg) = a useful value if the SIF is regularly inspected and tested. Formulas for PFDavg vary depending on the system architecture.

The simplest formula for a specified proof test interval is...

$$PFD_{avg} = (IDU)(\text{Proof Test Interval})/2$$

FÖRSÄKRAN SÄKERHETSKOMPONENT NY SÄKERHETSKRETS

I de fall man sätter samman en ny kretslösning som bedöms som säkerhetsrelaterad är det viktigt även för gamla maskiner att dessa nya säkerhetskretsar verifieras och valideras (typ med olika programvaror som Sistema, Pascal, Siemens m.m) samt att det utfärdas en Försäkran om överensstämmelse så det framgår att säkerhetskraven är uppfyllda och att någon visar detta. I en ny CE-märkt maskin täcker huvudförsäkran detta redan. Men en slutlig CE-märkare som köper in en sådan funktionslösning bör ställa krav på sin underleverantör om det inte ingår i den egna kretslösningen och verifikationen. Se exempel på sådan mall.

FÖRSÄKRAN FÖR SÄKERHETSKOMPONENT
 Enligt 4§c), Bilaga 5 och 2.1.A
 2006/42/EG (AFS 2008:3)

	Tillverkare (bolag)		Namn på person ansvarig för upprättandet av den tekniska dokumentationen för säkerhetskomponent (etablerad inom EES)
Namn:	Krets Automation AB		Per Komponent elchef
Adress:	Kretsvägen 5 600 60 Silsta		
Land:	Sverige		
Tfn/Fax:	V/xl xxxxx		
Försäkrar att följande säkerhetskomponent/säkerhetsfunktion			
Säkerhetskomponent/ Säkerhetsfunktion:	Linjenödstopp banor rundbrödpackning ,medium,stort runt		
Av typ:	Nödstopp		
Installerad i objektnr/maskinnr:	D-2563 AS1		
uppfyller aktuella krav för säkerhetskomponenter.			
Överensstämmer även med följande övriga EU/EG produktdirektiv:	2006/95/EG Lågspänningsdirektivet (LVD) 2004/108/EG EMC-direktivet		
Följande harmoniserade standarder, övriga standarder eller tekniska krav uppfylls även:	ISO EN 13849-1		
Säkerhetskrets/säkerhets- komponent verifierad enligt SIL eller PL:	Varje enskild säkerhetsfunktion uppfyller SS EN ISO 13849-1 Prestandanivå (PL) ...e....		
Dokumenterat enligt:	Sistema, dok nr: XX_D2563 Checksum:7907b49f6a020c2b0d76512734098a26		
Den tekniska tillverkningsdokumentationen, enligt Bilaga 7 2006/42/EG (AFS 2008:3), finns framtagna som verifierar aktuell säkerhetskomponent/säkerhetsfunktion.			
Säkerhetsfunktionen kontrollerad/verifierad av			
Ort:	Silsta	Signerad:	
Datum:	2011-12-09	Namn/Befattning:	Karl System VD

Bakom denna försäkran finns då ett verifikationsdokument, i detta fallet en Sistemarapport

Maskin & Processsäkerhetsanalys



Överför teoretiska regler till praktisk tillämpning

KOMMENTARER OCH SYNPUNKTER AVSEENDE FÖRESTÅENDE BYTE AV STYRSYSTEM RÖRANDE SÄKERHETSASPEKTER

ALLMÄNT

Byte av styrsystem i maskin- och processteknisk utrustning i sig bedöms som en avsevärd förändring där många säkerhetsaspekter är att beakta. Handlar det bara om produktionstekniska aspekter rörande systemet eller kommer även säkerhetsfunktioner hanteras av och integreras i det systemet som exempelvis nödstoppfunktioner, skyddsstoppfunktioner (t.ex. förreglingar) eller tryckvakter, värmedetekteringar etc.

Om säkerhetsrelaterade funktioner kommer att hanteras av-via styrsystemet ställs helt andra krav på dess uppbyggnad och funktion.

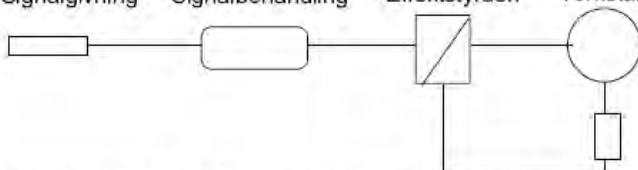
SÄKERHETSRELATERAD DEL I ETT STYRSYSTEM

"Del eller underordnad del(ar) i ett styrsystem som svarar på insignaler och genererar säkerhetsrelaterade utsignaler.

Kombinationen av säkerhetsrelaterade delar i ett styrsystem börjar där de säkerhetsrelaterade signalerna initieras och slutar vid utgången på effektstyrdonen. Även övervakningssystem omfattas".

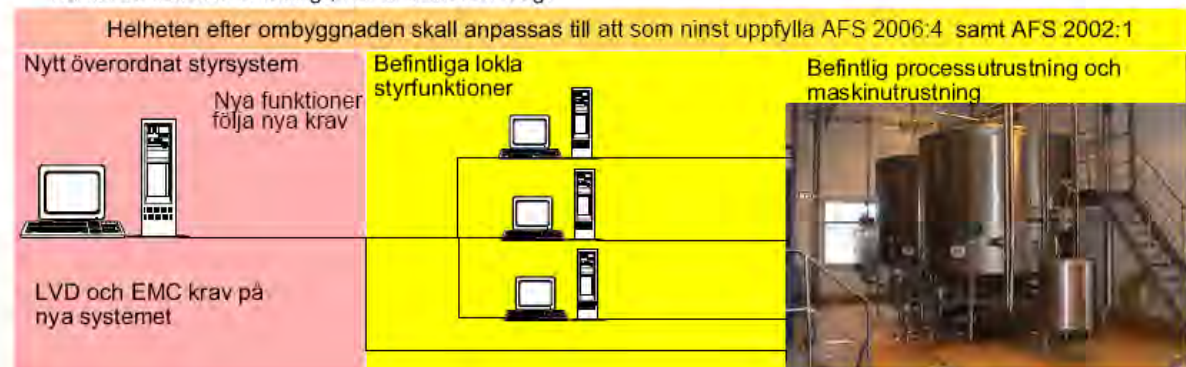
Styrsystem (är helheten)

Signalgivning Signalbehandling Effektstyrdon Verkställande organ



FASTSTÄLL GRÄNSER OCH ANSVARSOMRÅDEN SAMT SYSTEMPÅVERKAN

Vad skall åstadkommas i projektet och vem svarar för vad, hur skall befintlig maskin och processutrustning hanteras säkerhetsmässigt, hur är statusen idag.



TILLVÄGAGÅNGSSÄTT VID OMBYGGNINGER

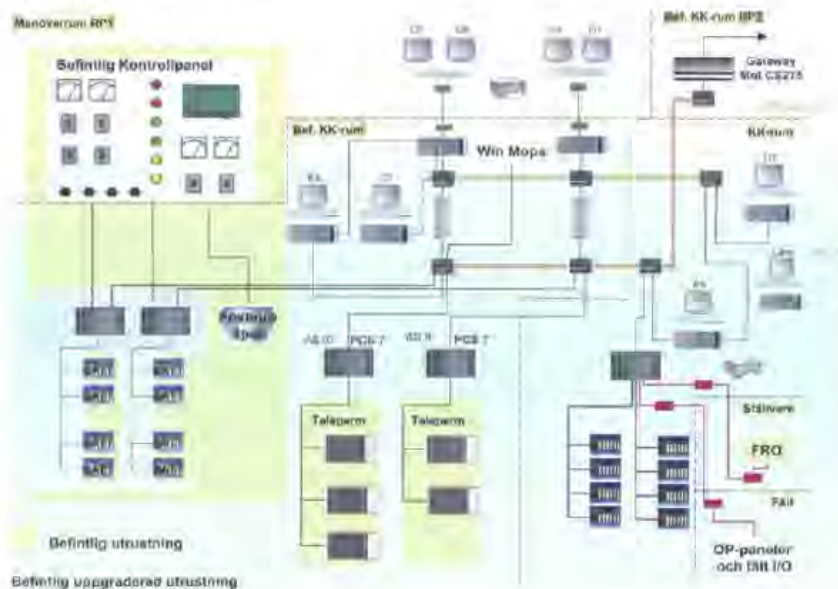
2.

I samband med om- och tillbyggnad t.ex byte av styrsystem, drivsystem etc. så är det viktigt att följande körschema följs för att säkerställa att de säkerhetskrav som finns beaktas.

1. Definiera maskin-process-system-betjänings-styr och eller drivområde etc.
 Fastställ de gränser som avses. Exempelvis upprättas en systemarkitektursöversikt dvs någon form av systemöversiktsbild. I de fall befintlig "gammal" utrustning ingår så är det viktigt att det framgår.

Alla ingående apparater och övrig utrustning av betydelse samt dess ihopkoppling bör ingå så att man kan skapa sig en översikt av det resulterande systemet i fråga.

Exempel systemöversikt



2. Fastställ regelverk som skall tillämpas

Fastställ vilket regelverk som skall tillämpas och följas. Exempelvis om det rör sig om maskin- och processteknisk utrustning så är det viktigt att fastställa om det handlar om att följa CE-kraven på hela det slutliga resultatet av ombyggnationen eller om det handlar om att helheten skall anpassas till minst de minimikrav i AFS 2006:4. Inköpta nya apparater och system skall självfallet vara verifierade och validerade samt inkopplade och anslutna enligt de CE-krav som gäller. Frågan är dock statusen på helheten. Handlar det om ombyggnad av maskin- och processteknisk utrustning tagen i bruk efter 1995 så är det CE-krav som gäller rörande maskinteknisk utrustning. Handlar det om tryckbärande anordningar är årtalet 2002. Motiv- och beslut till tillämpat regelverk skall framgå i dokumentationen kring förändringen så att det framgår för tillsynsmyndigheter vilket regelverk som den ombyggda utrustningen uppfyller efter den genomförda förändringen.

3. Klarlägg ombyggnadens omfattning och konsekvens.

Ombyggnadens omfattning och konsekvens på helheten måste bedömas och dokumenteras för att klarlägga att inga nya risker skapas samt att förutsättningar i övrigt kan uppfyllas. Eventuella förändringar rörande MMI (människa maskin interface) är en viktig del att klarlägga. Vidare övriga gränssnitt som berörs. Vilka förändringar kommer att ske samt får detta några negativa och positiva konsekvenser för såväl utrustning som den enskilde. Kommer säkerhetsfunktioner att påverkas exempelvis. *Konkret hur påverkar det nya styrsystemets installation det övriga.*

3.

4. Utför riskbedömningar

Riskbedömningar av såväl leverantörer som av ägaren är självklara i samband med förändringar i maskiner och processers avseende styr- och drivutrustning.

Viktigt att detta genomförs med verifierade analysmetoder.

I samband med upphandling är det av vikt att kontraktsvägen säkerställa tillgång till riskanalyser från leverantörer.

I detta fallet skulle jag bl.a säkerställa exempelvis en "What IF" analys av styrsystems-leverantören avseende dennes leveransåtagande samt att företaget själva svarar för riskbedömningar rörande det övriga exempelvis en Hazop avseende det processmässiga (avikleser i tryck, temperaturer, flöden, nivåer, flöden etc) som underlag för styrtekniska åtgärder avseende exempelvis styrsystemshantering av dessa funktioner enligt aktuella krav i EN 61508 (utr-system tillv) samt då EN 13849-1 eller EN 62061 (för process EN 61511).

Vidare då att ny säkerhetsrelaterad styrning verifieras och certifieras mot dagens krav (CE).

5. Sammanställ dokumentation

En projektteknisk fil skall sammanställas avseende den aktuella utrustningen

Innehållande verifiering och validering avseende de förändringar som genomförts.

Vidare kompletterande bruksanvisningar och övriga instruktioner som behövs.

6. Utbildning

I samband med (före) idrifttagandet är det av yttersta vikt att operatörerna erhåller utbildning avseende de förändringar som skett i samband med ombyggnaden.

Utbildning med huvudsakliga syftet att beskriva de förändrade funktioner och det handhavande som krävs för att fortsättningsvis kunna köra och sköta den aktuella utrustningen på ett säkert sätt.

Förändrade operatörsgränssnitt, manöverdon, varselsystem, grafiska gränssnitt, säkerhetsfunktioner samt ytterligare utbildningar för felsökare-underhåll etc.

UPPHANDLING

Styrsystem

Som produkt faller styrsystem som apparat (eget hölje egen funktion) eller system (flera samverkande apparater) eller som en elektrisk utrustning under produktdirektiven 2004/108/EG

som anger emissions- och immunitetskrav avseende elektromagnetiska fält och 2006/95/EG det så lågspänningsdirektivet som behandlar produktets säkerheten om spänningssättningen överstiger 50 V AC alternativt 75 VDC, båda anger de grundläggande hälso- och säkerhetskrav som skall uppfyllas gällande produkten.

Ett styrsystem hamnar inte under maskindirektivet som enskild apparat (ingen rörlig del) men väl installerad som en funktion i maskinen kommer även maskindirektivets grundläggande hälso- och säkerhetskrav in enligt dess bilaga 1 eller för befintlig utrustning kraven i AFS 2006:4.

Exempelvis nödstopp, skyddsstopp, MMI-interface, start- och stoppfunktioner, oavsiktlig start, nollspänningsutlösare m.m.

Här måste man gällande maskinkraven avseende styrning via kontrakt säkerställa vem som svarar för vad och vad man köper och vad man behöver för validerings- och verifieringsunderlag av leverantören-leverantörerna avseende bl.a certifikat, bruksanvisningar och riskbedömningar.

Vidare kan det även bli aktuellt att hantera styrfunktioner rörande tryckbärande anordningar via styrsystemet varför särskild uppmärksamhet kan behöva beaktas avseende systemets eventuella hantering av variabler rörande tryckbärande anordningar som exempelvis hantering av säkerhetskritiska funktioner avseende hantering rörande avvikelser i process- och miljöparametrar rörande exempelvis för höga eller för låga tryck, temperaturer, flöden, nivåer vidare även produktionsrelaterade parametrar som exempelvis viskositeter, hastigheter samt servicemedier som ånga, brand, kylvatten etc.

4.

Leveransgränser avseende hård- och mjukvara samt vem som analyserar och validerar vad avseende såväl enskilda leveranser som det slutliga integrerade systemet måste i ett tidigt skede fastställas då uppbyggnaden av styrsystemen styrs av hur kraven på hantering av säkerhetsrelaterade funktioner påverkas, exempelvis kan det bli aktuellt med redundant hantering av vissa säkerhetskritiska funktioner
Via hårdvara, hård- och mjukvara eller enbart via mjukvara genom användning av dubblerade system, dubbla bussystem, ASI hantering eller liknande.

Så i detta projektet är det inledningsvis viktigt att fastställa vad systemet skall hantera enbart produktionsaspekter eller även vissa säkerhetsmässiga funktioner.

SYSTEMANSVAR

För projektering, ombyggnad, drift eller underhåll av styr- och styrsystemsrelaterade drivsystem samt processsystem skall tillräckliga resurser för systemansvar finnas.
I större anläggningar och processer är det inte ovanligt att flera styrsystem direkt samarbetar med varandra alternativt enbart kommunicerar med varandra.
Mastersystem med underordnade slavsysteem ned till enskilda PLC eller PC-baserade styrningar ger mer eller mindre komplexitet åt det hela.

Myndigheterna har bedömt att:

- det finns behov av entydig definition inom området systemansvar, det finns behov av att klargöra ansvarsfrågor vid projektering, drift, underhåll och vid ombyggnad av system
- det finns behov av att inventera riskanalyser och säkerhetsmålsättning vid systemuppbyggnad

Systemansvar under ny- om- och tillbyggnadsskeden

I samband med exempelvis byten av styrsystem i maskiner och processanläggningar så är det viktigt att klargöra **vem som under projektets gång påtar sig systemförvaltaransvaret fram till dess att den avsedda förändringen genomförs.**

Detta bör man skriftligen dokumentera och avtala om i ett tidigt skede av projektet.
Exempelvis kan man komma överens om att exempelvis styrsystemsleverantören påtar sig detta systemansvar och vidtager de åtgärder som bedöms behövas för att säkerställa säkerheten under projektets gång.
När projektet är slutfört och säkerhetsutcheckat (verifierat och validerat) kan man sedan som brukare och förvaltare återta systemansvaret.

OBSERVERA att det är stor skillnad på systemansvarshanteringen gällande industrisystem kontra vanliga "administrativa system"

Så kom överens med systemleverantören om att denne tar systemansvaret från ombyggnadens start tills det är utcheckat och klart samt godkänt.

Frågor man kan ställa sig är:

- Ø görs konsekvensbedömningar/riskbedömningar på de ändringar som genomförs?
- Ø vem ansvarar för att dokumentationen upprättas?
- Ø vem ansvarar för att föregångar återställs?
- Ø hur kommunicerar man genomförda förändringar (status på anl.) tex från ett skiftlag till ett annat?
- Ø hur hanteras programvara, senaste program dump?
- Ø hur systemets funktioner kontrolleras och följs upp?
- Ø hur fungerar systemet i enlighet med uppställda specifikationer?
- Ø Hur sker slutlig verifiering och validering

5.

SYSTEMANSVAR OCH SYSTEMSÄKERHET INFÖR UPPHANDLING

Vad kan ingå i systemansvar och viktigt att beakta vid systemupphandlingen

Varje system (anläggningssystem) som har krav på hög säkerhet måste ha någon som tar SYSTEMANSVAR för produkten.

Huvud punkterna och frågor att diskutera och beakta kan vara:

1. Systemansvar
2. Systemarkitektur
3. Specifikationer
4. Evalueringsmetoder

Att ha systemansvar innebär bland annat att:

- Ø Definiera systemarkitekturen i systemet
- Ø Kontrollera att lagar och förordningar för produkten uppfylls
- Ø Kontrollera att ställda säkerhetskrav är uppfyllda
- Ø Ställa krav vid val av ingående komponenter så att de kan fungera säkert och felfritt i systemet

Med systemarkitektur menas:

Utforma en genomtänkt systemarkitektur för systemet som:

- Ø är väl känd av alla som medverkar i utveckling av systemet
- Ø stöder utvecklingsarbete och långsiktigt underhållsarbete
- Ø sätter upp klara gränssnitt mellan olika delar av systemet
- Ø fördelar funktionalitet till olika delar av systemet
- Ø förklarar skillnaden mellan system och nodfunktion
- Ø analyserar och bestämmer vilka funktioner (processer) som är förlagda till noder eller systemnivå
- Ø bestämmer var i strukturen som olika säkerhetskritiska funktioner är förlagda och hur de verkställs
- Ø verifierar att signaldynamiken stämmer med den systemarkitektur som valts
- Ø identifierar hur informationsflödet ser ut i systemet

Med specifikationer menas:

- Ø ett system med krav på hög säkerhet måste ha någon form av kravspecifikation där dessa krav definieras
- Ø de uppställda kraven måste vara möjliga att verifiera genom provning eller analys

En kravspecifikation bör upprättas som innehåller traditionella produktkrav såsom:

- Ø normala funktionskrav
- Ø miljökrav med verifieringsplan

Krav på säkerhetsaspekter av produkten:

- Ø definition av felmoder
- Ø definition av felintensiter
- Ø verifieringsplan för säkerhet

Med evalueringsmetoder menas:

Vid verifiering och validering av distribuerade säkerhetskritiska system kan man använda sig av såväl traditionella metoder som metoder för distribuerade system.

Vilka metoder man väljer skall framgå av kravspecifikationen för systemet.

Val av metoder för verifiering och validering bör vara känt redan under designfasen av ett utvecklingsprojekt.

Traditionella metoder som kan användas är:

- Ø produkt FMEA för att analysera felmoder och bedöma dess konsekvenser
- Ø FTA för att analysera felorsakssamband och sannolikheter för dessa
- Ø MTBF för att prediktera felintensiteter hos komponenter som ingår i systemet

För distribuerade säkerhetskritiska system finns speciella felmoder som måste utvärderas under såväl design, verifiering och validering av produkten.

Exempel är:

Ø Nod fel	Node Errors
Ø Bus fel	Bus Errors
Ø Timing fel	Timing Errors
Ø Osammanhängande data	Data Consistency Errors
Ø Initiering o återstarts fel	Init & Restart Errors
Ø Skenande noder	Babbling Idiot Errors
Ø Konfigurationsfel	Configuration Errors

DRIFT

För drift av datorsystem skall tillräckliga resurser för systemansvar finnas så att kontinuerligt säkerhetsarbete, nödvändiga programvaruförändringar och blockering eller avstängning av inte önskvärda servertjänster skall kunna ske i den takt som säkerhetsmässigt krävs.

För varje system skall det finnas en person som utsetts att vara systemansvarig. Denna person skall ha undertecknat 'Ansvarsförbindelse för systemansvariga' och tagit del av de regler som ställs där.

Att då ta tag i när projektet går mot sitt slut och systemansvaret övergår till Er igen.

SAMMANFATTNINGSVIS

Upphandla på rätt sätt och klarlägg vem som svarar för vad.

Säkerställ verifierings, validerings och riskanalysdokument samt bruksanvisningar på Svenska.

Kom överens med styrsystemsleverantören om att han svarar för systemansvaret under projektet och fram till slutligt godkännande om möjligt.

Fastställ hur Ni skall hantera det befintliga som påverkas genom detta systembyte

Bilda en projektgrupp (med representanter från såväl leverantör som arbetsgivar- och arbetstagar sidan som beaktar säkerhetsaspekterna i projektet

Rörande exempelvis MMI, grafiska bildskärmsbilder, skyddsförreglingar, larm, maskin- och processaspekter m.m.

Riskbedöm de maskin och processmässiga gränssnitten

Utbilda personalen i det nya och dokumentera detta utifrån utbildningsplanen

Påbörja och slutför en projektteknisk fil rörande förändringen

Sammanställt av

Tomas Beäff Europeisk säkerhetsrådgivare mpsa@telia.com 070 6406027

PL bestäms av:

• Kategori (B, 1, 2, 3, 4)

• $MTTF_d$ - Mean Time to Dangerous Failure

• DC - Övervakningsfunktion/-system

• CCF - Samverkande fel

• Mått/krav för systematiska fel

*MTTF För varje enskild komponent (hårdvarutillförlitlighet) från tillverkarens data eller omräknat via B10 formel

*DC Diagnostic coverage (i hur hög grad farliga fel uppnås)

Measure	Technology	DC
Process (cyclic test)	Fluid technology	0 % ≤ DC < 99 %
Cross monitoring between 2 channels	Electronics	DC = 99 %
Indirect monitoring (e.g. pressure)	Fluid technology	90 % ≤ DC < 99 %
Direct position monitoring	Fluid technology	DC = 99 %
Integrated self-monitoring	Safety on board	90 % ≤ DC < 99 %

*CCF Common Cause failure

-åtgärder blir relevanta när man arbetar med någon form av redundans eller övervakning (Feltålighetskategorierna 2-4)

CCF: fel av olika orsaker, som resultat av en händelse

Kraven på CCF ställs för flerkanaliga strukturer (arkitekturer) (Kategori 2, 3 och 4) och de är överensstämmelse med EN 61508-6 Annex D - med "beträffande på 2% eller mindre"

För system med en summa mindre än 65 poäng (pt) gäller:

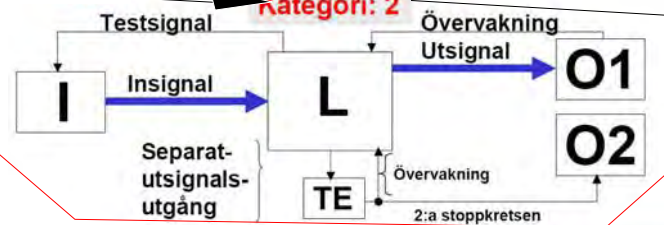
Separation/segregation av signalfasen	15 pt
Diversifiering	20 pt
Design (t.ex. skydd mot överlag/ortslutning)	15 pt
Väl beprövade komponenter	5 pt
FMEA (Felmodes och Effekt analys)	5 pt
Mjölpåverkan - EMC + annat	25 pt + 10 pt

PFHd
Sannolikhet för farligt fel per timma

$10^{-4} \approx$	1 farlig felfunktion per år
$10^{-5} \approx$	1 farlig felfunktion per 10 år
$10^{-6} \approx$	1 farlig felfunktion per 100 år
$10^{-7} \approx$	1 farlig felfunktion per 1000 år

Fastställande av kategori (Från riskträd eller C std)

Kategori: 2



- kraven enligt kategori B uppfyllt
- väl beprövade säkerhetsprincip
- Skyddsfunktionen skall övervakas i lämpliga intervall
- feltolerans på noll - men förlust av skyddsfunktionen detekteras
- huvudkaraktistiken genom systemarkitektur

$MTTF_d = LMH$
 $DC = LM$
 $CCF = +$

$MTTF_d$: medelvärdet av operationstid där ett enkanaligt system förväntas ha inga alvarliga fel

Beteckning	Frekvens för $MTTF_d$
L Låg	$3 \text{ år} \leq MTTF_d < 10 \text{ år}$
M Medel	$10 \text{ år} \leq MTTF_d < 30 \text{ år}$
H Hög	$30 \text{ år} \leq MTTF_d < 100 \text{ år}$

- Från tillverkarens data
- Tillämpa metoderna i standarden Bilaga C och D
- Välja 10 år som värde

Beräkning av $MTTF_d$ för komponenter med hjälp av B_{10d}

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}}$$

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s / h}{t_{cycle}}$$

B_{10d} är antalet arbetscykler innan 10 % av komponenter går sönder på ett farligt sätt

n_{op} är medelvärdet av antalet arbetsoperationer per år

h_{op} är medel användning i timmar per dag

d_{op} är medel användning i dagar per år

t_{cycle} är medeltiden (sek) mellan starten av två lyckosamma arbetscykler för komponenten

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

T_{10d} är medeltid tills 10% av komponenterna går sönder på ett farligt sätt (begränsad användningstid)

Prestandanivå (PL)
Performance Level

PFH_d:

Performance Level a	$\geq 10^{-5}$ to $< 10^{-4}$ [h ⁻¹]
Performance Level b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$ [h ⁻¹]
Performance Level c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$ [h ⁻¹]
Performance Level d	$\geq 10^{-7}$ to $< 10^{-6}$ [h ⁻¹]
Performance Level e	$\geq 10^{-8}$ to $< 10^{-7}$ [h ⁻¹]

DC-Täckningsgrad
För diagnos

DC

	Kategori B (enkanalig)	Kategori 1 (enkanalig Högt MTTF)	Kategori 2 Enkanaligt med övervakning	Kategori 3 2 kanaligt med viss övervakning	Kategori 4 2 kanaligt med övervakning
Diagram	I → L → O	I → L → O	I → L → O ↓ TE → O _n	I1 → L1 → O1 I2 → L2 → O2	I1 → L1 → O1 I2 → L2 → O2
PFH _d (a-e)	Low (a)	Low (a)	Low (a), Medium (b), High (c)	Low (a), Medium (b), High (c)	Low (a), Medium (b), High (c)
DC-Täckningsgrad	none Ingen	none Ingen	low Låg	low Låg	high Hög

Exempel kategori 2 lösning
T Beäff www.mpsa.se

Mata in alla data i typ Sistema, Pascal eller motsvarande programvara för att validera aktuell säkerhetsfunktion

MMI-interface på brukarlandets språk när det gäller maskinstyrning via OP-paneler, bildskärmar, varselskyltmärkningar m.m.



AFS 2006:4 Användningskraven

Vad beträffar märkning, interaktiv programvara och bruksanvisning gäller vid användningen alltid de krav på språk som följer av de svenska föreskrifterna.

Se även AFS 2008;3 maskindirektivet.

Skyllttext och knappmärkning på Svenska för Sverigeanvändning.

Se AFS 2008:13



NOTE! BEFORE ENTERING THE PULPER:

- STOP THE ROTOR AND LOCK OUT THE MOTOR STARTER
- DRAIN AND FLUSH THE PULPER
- CLOSE ALL FEED PIPES BY HAND VALVES OR DISCONNECTING THE PUMPS
- LOCK OUT CONVEYOR OR ANY OTHER AUTOMATICALLY STARTING MACHINE OR DEVICE
- SECURE THE FRESH AIR FEED TO THE PULPER
- BEFORE STARTING ANY MAINTENANCE OR REPAIRWORK SEE INSTRUCTIONS IN THE MANUAL

STO4010752



MASKINDIREKTIVET OCH ELSÄKERHETSKRAVEN I MASKINER

1(2)

Punkt 1.5.1 i Bilaga 1 2006/42/EG behandlar risker i samband med användning av elektrisk energi.

T Beäff www.mpsa.se

Elektrisk energi kan omvandlas till mekanisk energi med hjälp av en elektrisk motor eller användas för att exempelvis producera värme eller strålning för processen. Statisk elektricitet används också i vissa processer som t.ex. målning, separation av material och påskyndande av utfällning.

MASKINTILLVERKAREN MÅSTE FÖREBYGGA ALLA RISKKÄLLOR AV ELEKTRISK NATUR

De huvudsakliga riskerna i samband med elektrisk energi är elektrisk stöt på grund av direktkontakt med strömförande delar (ofrivillig kontakt med delar som normalt är strömförande) eller indirekt kontakt (kontakt med delar som blivit strömförande genom ett fel) samt brännskador, brand eller explosioner på grund av elektriska gnistor eller överhettning av elektrisk utrustning.

Enligt första stycket i punkt 1.5.1 krävs att maskintillverkaren vidtar de åtgärder som är nödvändiga för att förebygga alla riskkällor av elektrisk natur.

Detta allmänna krav gäller oavsett den elektriska matningens spänning.

*(Missat i AFS 2008:3 tyvärr men finns i direktivet)

Enligt *andra stycket i punkt 1.5.1 ska säkerhetskraven i lågspänningsdirektivet 2006/95/EG gälla för maskiner.

Den andra meningen i stycket klargör att förfarandena i lågspänningsdirektivet i samband med utsläppande på marknaden och tagande i drift inte är tillämpliga på maskiner som omfattas av maskindirektivet. Det innebär att försäkringen om överensstämmelse för maskiner, som omfattas av maskindirektivet, inte ska hänvisa till lågspänningsdirektivet.

(Undantaget gäller dock inte elektriska säkerhetskomponenter)

Sammanfattningsvis så kan man alltså för maskiner med integrerad elektriskt materiel och kopplingsutrustning (maskinpåbyggda skåp) uppfylla säkerhetskraven i maskindirektivets säkerhetskrav för att förebygga risker med elektricitet utan att i maskinens Försäkringen om överensstämmelse för maskiner åberopa LVD 2006/95/EG.

Elsäkerheten i maskinen måste dock verifieras

Dock måste man så klart kunna verifiera hur detta åstadkommit.

t.ex genom att uppfylla B standarderna för maskiners elutrustning och i maskinförsäkringen hänvisa till detta, dvs "elsäkerhets"standarderna täcker säkerhetskraven för att förebygga risker med elektrisk matning i maskinen.

EN 60204-1 >50 VAC >75 VDC <1000 VAC < 1500 VDC

EN 60204-11 >1000 VAC >1500 VDC

Risker med el skall vara förebyggda i alla maskiner oavsett spänningsnivå.



ELSÄKERHETSKRAVEN SKALL VARA UPPFYLLEDA OAVSETT OM MAN HÄNVISAR TILL LVD ELLER EJ I 2A

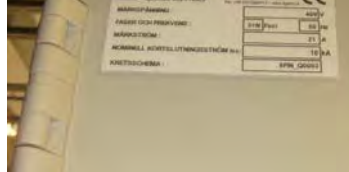


INGÅENDE ELEKTRISKT MATERIAL SOM OMFATTAS AV LVD SKALL SJÄLVKLART VARA CE-MÄRKT MOT 2006/95/EG

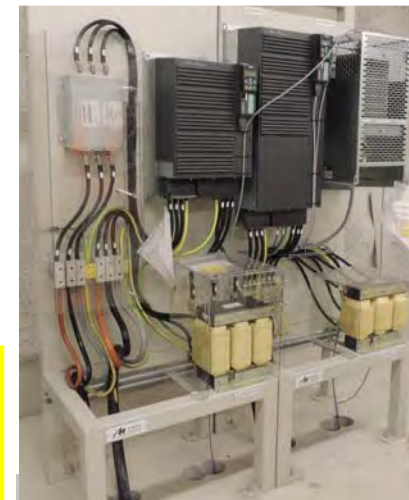
CE-MÄRKNING MOT LVD (IEMC OM EJ KLASSAD SOM FAST INSTALLATION) GÄLLER KOPPLINGSUTRUSTNING <1000 VAC >5100 VDC

Tillverkare av kopplingsutrustning typ bestyckade apparatskåp som levererar till maskintillverkare är inte undantagna krav på CE-märkning mot LVD 2006/95/EG (de skall även beakta EMC (2004/108)/EG även om de åberopar principen för fasta installationer (dvs kundunik lösning för en förutbestämd plats).

Utöver detta kan det då tillkomma att de som leverantör av kundspecifik kopplingsutrustning måste beakta maskindirektivets krav då exempelvis säkerhetsrelä, maskinstyrningar, frekvensdrivning m.m installeras, ur maskindirektivets hänseende lämnar de då sen så kallad försäkras om delvis fullbordad maskin enligt Bilaga 2B 2006/42/EG (drivsystem är t.ex en delvis fullbordad maskin).



KOPPLINGSUTRUSTNING/ELEKTRISKT MATERIEL SKALL CE-MÄRKAS I DE FALL DE OMFATTAS AV DIREKTIVEN HÄR KAN MAN INTE HÄVDA ATT DETTA ÄR EN INTEGRERAD ELDEL I MASKINEN



Över 1000 VAC >1500 VDC ingen CE-märkning mot LVD **Elektrisk högspänningsutrustning**

Transformatorer hamnar oftast utanför CE-märkningskrav enligt lågspänningsdirektivet men det innebär så klart inte säkerhetskrav saknas

Den elektriska högspänningsutrustning, som undantas genom artikel 1.2 I), omfattar kopplingsapparater och kopplingsutrustning och transformatorer, som bildar del av eller är kopplade till en högspänningskälla (över 1000 V för växelström eller över 1500 V för likström).

Sådan elektrisk högspänningsutrustning omfattas i sig inte av maskindirektivet. Om utrustningen är inbyggd i en maskin måste den ha sådana egenskaper att maskinen uppfyller de relevanta grundläggande hälso- och säkerhetskraven i bilaga I till maskindirektivet



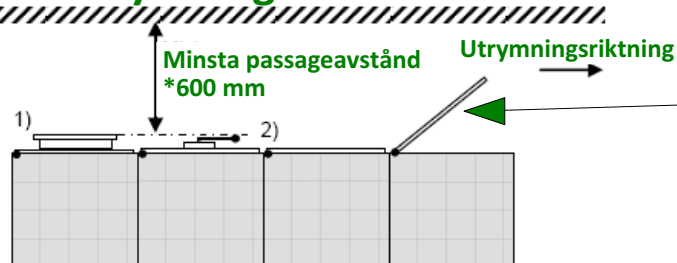
IEC 60364-7-729 Generella skyddskrav i tillträdesbegränsade områden (el-driftrum t.ex) för placering av kopplingsutrustning inkluderande krav rörande operatörs-underhållsplatser och gångbredder



Standarder ger rekommendationer och i vissa fall kan riskbedömningar motivera avvikelser

Såväl elsäkerhetsmässiga som arbetsmiljömässiga aspekter som försäkringsmässiga aspekter måste beaktas
Betjäningsgång för elfara och utrymning mellan elskåp och fast del har historiskt legat på >1200 mm i Sverige

Utrymning fall 1



- *Minsta bredd av 600 mm mellan vägg och fränkskiljare i ytterläge på skåpet
- *2.Fränkskiljare i låst läge
- *1. Handtag-spakar etc. för el-styrutrustning.

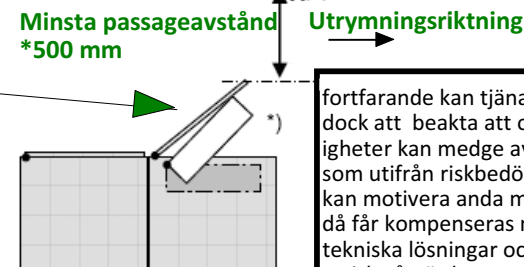
IEC 1159/07



Dörrar och paneler skall kunna öppnas minst 90 grader

IEC 60364-7-729

Utrymning fall 2 Hängade skåpdörrar -paneler



*) Hinged mounting rack

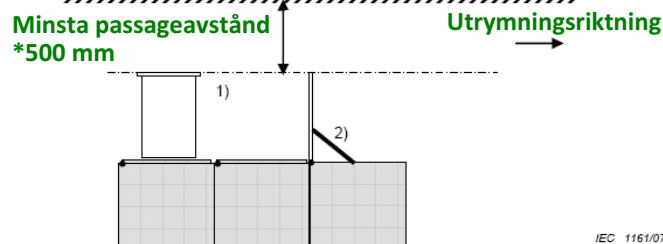
*Skåphängda dörrar eller paneler

IEC 1160/07

Praktiskt

Mått som tillämpats i Sverige historiskt och

fortfarande kan tjäna som riktlinjer, dock att beakta att olika omständigheter kan medge avvikelser som utifrån riskbedömningar kan motivera andra mått vilket då får kompenseras med andra tekniska lösningar och organisatoriska åtgärder (stänga av, begränsa, instruera etc.)



*Ett minsta mått på gångväg av 500 mm skall finnas mellan vägg och fränkskiljarutrustning i fullt utdraget läge eller fixerad öppen dörr

- 1) Helt utdragen
- 2) Fixerad öppen dörr

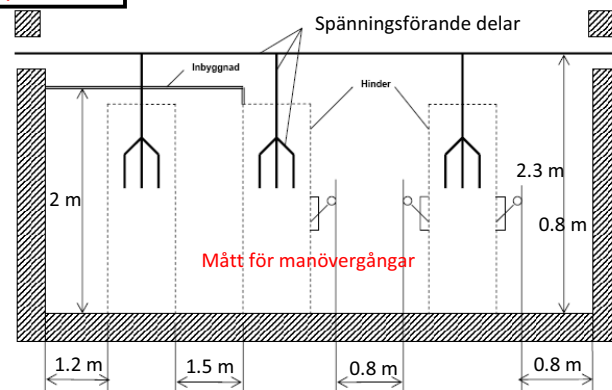
IEC 1161/07

Utformning- och mått driftrum

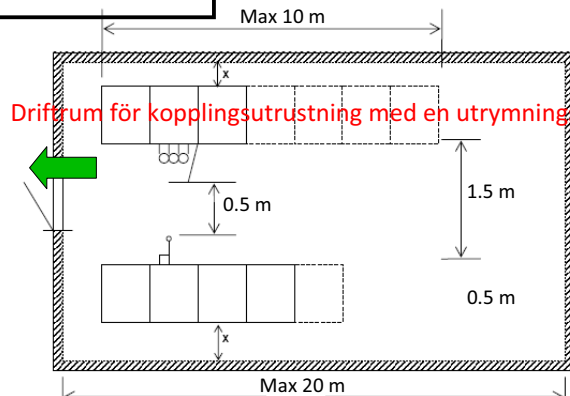
Se SS 4362101 om utrymmen för elektriska kopplingsutrustningar för lågspänning.
Se SS 4210101 för högspänning.

Driftrum är utrymmen i huvudsak för uppställning av elektrisk utrustning avsedda att hanteras av fackkunniga eller instruerade personer

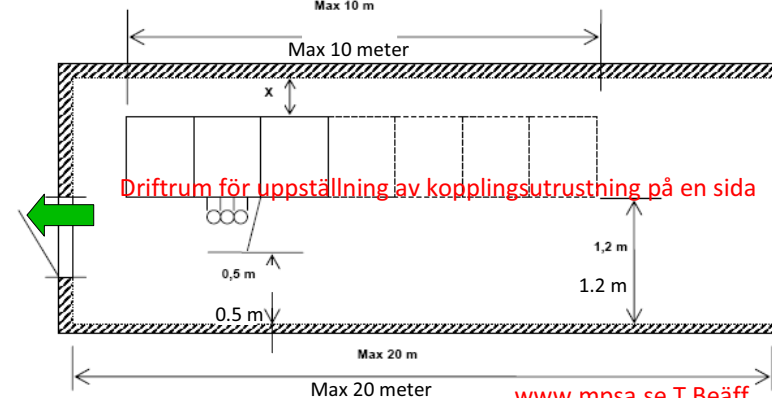
Elrum för placering av kopplingsutrustning, normal avskilda från övriga utrymmen oftast anslutna i närhet till kanalisationen. Normalt försedda med låsbara dörrar.



Driftrum för kopplingsutrustning med en utrymningsdörr



Driftrum för uppställning av kopplingsutrustning på en sida



www.mpsa.se T Beäff

MARKNADSÖVERVAKNING

Säkerhet och konkurrens på lika villkor

Detta syftar inte bara till att tillvara konsumenternas, arbetstagarnas och andra användares intressen, utan också till att skydda de ekonomiska aktörerna från illojal konkurrens.

1

Myndigheterna skall kontrollera om produktdirektivbunden utrustning är konstruerad för att vara säker för användning under förutsebara omständigheter



Huvudsakligen handlar det om att kontrollera om de grundläggande hälso- och säkerhetskraven för aktuell produkt är uppfyllda för att förhindra de särskilda risker som kan uppstå. Och i de fall man som tillverkare inte uppfyller de grundläggande hälso- och säkerhetskraven i aktuella produktdirektiv om dessa brister ger upphov till risker för allvarliga eller dödliga skador för användare av den berörda utrustningen vidtaga åtgärder.

I direktiven fastställs att när en medlemsstat konstaterar att en produkt med CE- märkning som används på avsett sätt kan äventyra människors och eventuellt husdjurs och egendoms säkerhet, skall medlemsstaten vidta alla lämpliga åtgärder för att:

-Avlägsna produkten från marknaden och förbjuda att den släpps ut på marknaden -och tas i bruk samt begränsa dess fria rörlighet.



Medlemsstaterna ansvarar inom sitt territorium för att detta direktiv faktiskt tillämpas och att säkerheten hos de berörda maskinerna så långt det är möjligt förbättras i enlighet med bestämmelserna i detta direktiv. Medlemsstaterna bör se till att de har kapacitet att utföra effektiv marknadskontroll, med beaktande av de riktlinjer som utarbetas av kommissionen, i syfte att se till att direktivet tillämpas korrekt och enhetligt.



Övervakningsmyndigheterna skall ges tillräckliga resurser och befogenheter för sin övervakningsverksamhet, vilken utgörs av att kontrollera produkter som släpps ut på marknaden och om de inte uppfyller gällande krav –vidta lämpliga åtgärder för att säkerställa överensstämmelse.

När det gäller personalresurser måste myndigheten ha eller ha tillgång till ett tillräckligt antal personer med lämpliga kvalifikationer och erfarenheter samt en tillräckligt stark yrkesmässig integritet.



MARKNADSÖVERVAKNING

Säkerhet och konkurrens på lika villkor

Detta syftar inte bara till att tillvara konsumenternas, arbetstagarnas och andra användares intressen, utan också till att skydda de ekonomiska aktörerna från illojal konkurrens.

2

PRIORITERA DÄR DET GÖR MEST NYTTA (STÖRSTA RISKERNA FINNS)

För en effektiv marknadsövervakning bör resurserna koncentreras till områden där riskerna kan förmodas vara högre, där det är vanligare att produkterna inte uppfyller gällande krav eller där man kan identifiera ett särskilt intresse. Statistik och riskanalyser kan användas som grund för denna prioritering.

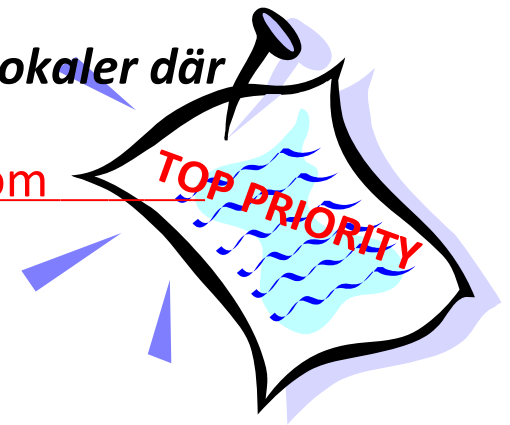


För att kunna kontrollera produkter som släpps ut på marknaden skall övervakningsmyndigheterna ha befogenhet, kompetens och resurser för följande:

- *Att regelbundet besöka affärs-, industri- och lagerlokaler.*
- *Att i lämpliga fall regelbundet besöka arbetsplatser och andra lokaler där produkter tas i bruk.*

Det är viktigast för produkter (t.ex. maskiner och tryckutrustning) som efter tillverkning installeras och tas i bruk direkt i kundens lokaler.

- *Att organisera stick- och punktkontroller.*
- *Att ta stickprover på produkter för att granska och prova dem.*
- *Att begära all nödvändig information*



NYA SANKTIONSSYSTEMET MED SANKTIONSavgIFTER FRÅN DEN 1 JULI 2014



Regeringens prop. 2012/13:143,



SOU 2011:57, rskr 2012/13:284.



Sanktionsavgifter i
föreskrifterna

En bättre arbetsmiljö
genom effektivare sanktioner
regeringens motto

direkt straffsanktionering på ett antal områden ersätts av sanktionsavgifter

Effektivare påföljder för den som bryter mot AML enligt riksdag och regering

Bakgrunden är ett riksdagsbeslut om effektivare påföljder för den arbetsgivare som bryter mot arbetsmiljölagen AML. Idag leder många anmälningar inte till straff, och dessutom tar utredningar lång tid och mycket resurser i anspråk då Arbetsmiljöverket, polis och åklagare är inblandade. Därför har riksdagen beslutat att införa ett nytt system med sanktioner, som ska bli mer effektivt, men också enklare och mindre resurskrävande än dagens.

Sanktionsavgiftens storlek varierar beroende på vilken risknivå överträdelsen har samt antalet anställda;

en överträdelse med en risk för fara för livet kostar exempelvis mer än en överträdelse i en lägre risknivå.

Dessutom är sanktionsavgiften differentierad beroende på företags storlek.

Minimiavgift för överträdelser i risknivå fyra är exempelvis 100 000 kr för de minsta företagen och en miljon kronor för de största. Företagets storlek beräknas utifrån antalet sysselsatta.

Arbetsmiljöverket kan nu direkt utfärda sanktionsavgifter

Det nya systemet innebär att Arbetsmiljöverket kan utfärda sanktionsavgift för en arbetsgivare som bryter mot reglerna, istället för att frågan går till polis, åklagare och domstol.

Om någon skadas eller dör i arbetet är det fortfarande domstolsprocess och straff som gäller.

Arbetsmiljöbrott enligt brottsbalken (vållande till kroppsskada eller sjukdom, vållande till annans död, framkallande av fara för annan) omfattas inte av ändringarna,

I det nya systemet är det ett 40-tal bestämmelser som är förenade med sanktionsavgift. (Mer kommer) Inför att det nya systemet ska träda i kraft har Arbetsmiljöverket sett över majoriteten, 90 stycken, av de idag cirka 120 bestämmelser som är straffsanktionerade. Arbetet fortsätter med att se över övriga bestämmelser.

När den nya lagen träder i kraft, tas i princip alla straff bort från Arbetsmiljöverkets föreskrifter. Några få undantag finns, exempelvis föreskriften om minderårigas arbetsmiljö.

Arbetsmiljöverket kan dock även fortsättningsvis rikta förelägganden och förbud med vite mot den som överträder bestämmelserna.

Det nya systemet träder i kraft den 1 juli 2014. Undantag finns på byggområdet där två bestämmelser om fallskydd träder i kraft först den 1 januari 2015.



ÖVERKLAGAN
↓
Ett beslut om sanktionsavgift kan överklagas, på samma sätt som AV:s övriga beslut i enskilda fall, till allmän förvaltningsdomstol.

**OLIKA SÄKERHETSREGLER OCH CERTIFIERINGSKRAV
FÖRELIGGER PÅ EN GLOBAL MARKNAD**



Vi hjälper till eller guidar dig rätt



Maskin & Processsäkerhetsanalys MPSA AB
Tidafors 346
660 60 Molkom

Kontor
+46 55314060
Hemsida
www.mpsa.se

Organisationsnummer
556741-3462

Bankgiro 5004-4650

VAT SE 556741346201

IBAN SE 48950000996042



Tomas Beäff
Senior konsult-safety
mps@telia.com
+46 70 6406027



Leif Bergström
Senior konsult-safety
Leif.k.bergstrom@telia.com
+46 70 6858323



Carina Haffling
Ekonomi/administration
Carina.haffling@telia.com
+46 70 68227787

Maskin & Processsäkerhetsanalys MPSA AB

SMPSA AB



MPSA AB
Tidafors 346
660 60 Molkom
S-Sweden

+46 553 14060 office
+46 70 6406027 mobile
mps@telia.com
www.mpsa.se



Du betalar inte för att vi skall lära oss det Du vill ha hjälp med.
**VI HJÄLPER TILL MED DET MESTA SOM RÖR
SÄKERHETEN PÅ ARBETSPLATSEN**

Riskinventeringar
Riskanalyser
Projektsupport
Utbildningar



**ARBETSPLATSENS UTFORMNING
TILLSTÅNDSANSÖKAN
KONSTRUKTION
TILLVERKING-CERTIFIERING CE
OM- OCH TILLBYGGNADER
INSTALLATION
KONTROLL
ANVÄNDNING
FÖRVALTNING**

**YRKESHYGIENSIKA
MÄTNINGAR**

**SAM-
ORDNING**

RUTINER-SYSTEMATIK OCH KUNSPAPSÖVERFÖRING

UNIK PROGRAMVARA

Under 15 års tid har vi utarbetat denna unika programvaran som har allt och lite till när det gäller arbetsmiljö, miljö, teknik, säkerhet m.m inom EU-rätten för EES-området. Innehåller även krav för andra maknader som nordamerika, Kina m.m. Bara klicka så får du upp all information, regler eller de mallar Du behöver för riskbedömningar, CE-märkningar, SAM, Byggarbetsmiljösamordning, driva projekt, upprätta tekniska filer, hantera om- och tillbyggnader, utfärda körtillstånd, EU-certifikat, upphandlingar, utcheckningar, miljöbedömningar m.m. Denna mycket lättanvända programvara användes inom många företag och har funnits på marknaden under ständig uppdatering och förbättring de senaste 15 åren.

Hör av er för mera information om kostnader, innehåll och användning.

LEDNINGSSYSTEM

För Teknik och Arbetsmiljö inom EES

Huvudmeny Handledning

Kunskapsbanken	KUNSKAPSBANKEN DET KOMPLETTA ELEKTRONISKA UPPSLAGS- OCH HJÄLPMEDELET SOM SNABBT OCH ENKLT GER ÅTKOMST TILL DATA I FORM AV HJÄLP, LATHUNDAR, INFORMATION, TOLKNINGAR, DIREKTIV, FÖRESKRIFTER ETC. SOM KAN BEHOVAS INOM OMRÅDET TEKNIK OCH ARBETSMILJÖ.
PROJEKTHANTERING	RISKBEDÖMNINGSMALLAR OCH ANALYSOKUMENT AVSEENDE TRYCKBÄRANDE ANORDNINGAR, MASKINER, EL-AUTOMATION SAMT KEMISKA HÄLSORISKEN OCH UTRUSTNING I EXPLOSIONSFÄRLIG MILJÖ
TEKNISK FIL OCH CE-MÄRKNING	VALIDERINGSOKUMENT OCH HJÄLPFALLAR FÖR UPPRÄTTANDE AV TEKNISKA FILER
RISKBEDÖMNING	RIKTLINJER NYTT OCH GAMMALT + DIREKTIV (Snabbmeny)
SNABBMENY REGLER	UTCHECKNINGSDOKUMENT
UTCHECKNING-OVERTAGANDE	KÖP- OCH SÄLJRUTINER BESTÄLLARKOMPETENS
KÖP & SÄLJRUTINER	SYSTEMATISKT ARBETSMILJÖARBETE
SYSTEMATISKT ARBETSMILJÖ	YTTRE MILJÖN
YTTRE MILJÖN	

Denna version licensierad för Saint-Gobain Isover AB för 25 enskilda och utskädda användare

Version 12.4 2012

Alla mallar du arbetar i är word eller excellanpassade. Delvis även på engelska.

Analysera
Dokumentera
Certifiera
Instruera
Skriv kontrakt
Information
Lathundar hur göra
Kontrollera
Regler EU
Regler 3:e land
Miljö-Arbetsmiljö



Ditt företags logotype ingår på alla mallar

13000 sidor sökbar info

DET KOMPLETTA UPPSLAGSVÄRDET MED ÖVER 11500 LÄTT SÖKBARA SIDOR

Arbetsmiljö & teknik
Föreskrifter och lagar
EU-direktiv och EN-standarder
Produktansvar och produktsäkerhet
Systematiskt arbetsmiljöarbete
Information, tolkningar och lathundar om specialområden
Allt om CE-märkning Du behöver veta
Beställarkompetens-avtal och upphandling

Läs eller skriv ut och läs

UTBILDNINGAR

BOKA VÅRA POPULÄRA FÖRETAGSANPASSADE SÄKERHETSUTBILDNINGAR

Kursintyg samt gedigen kursdokumentation ingår

Vi skräddarsyr även utbildningar



Öka kunskapen succesivt i företaget på alla fronter enligt vår speciella kurspyramid.

- Ändra attityder och beteenden
- Förbättra systematiken
- Öka kunskapen steg för steg
- Förbättra tillämpningen

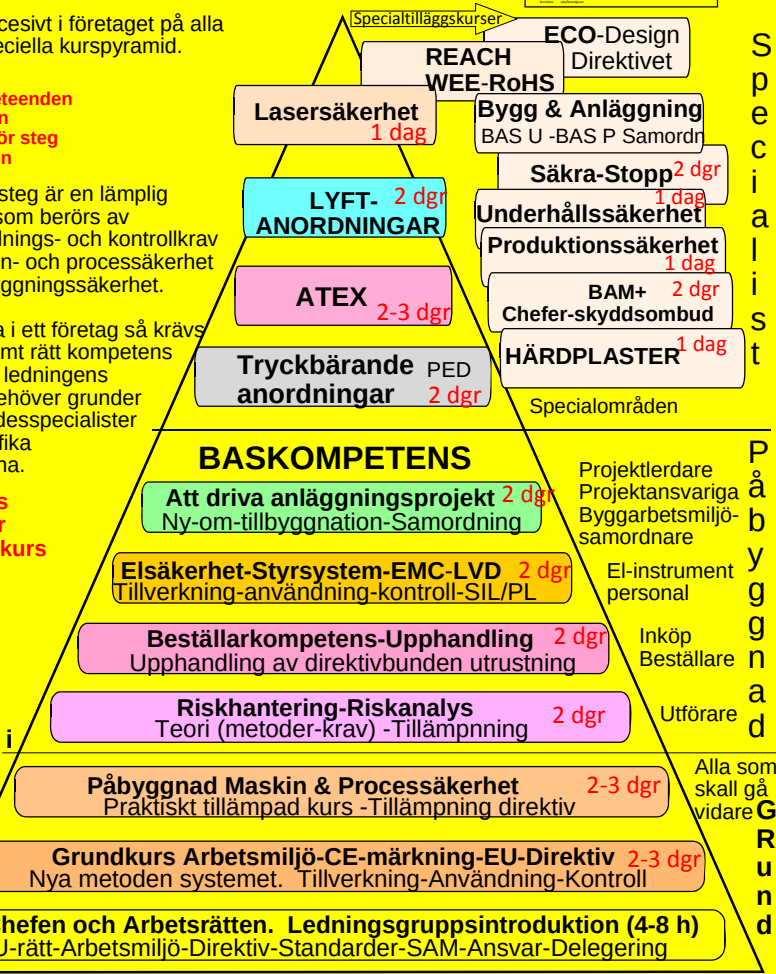
Följande utbildningssteg är en lämplig profil för ett företag som berörs av tillverknings- användnings- och kontrollkrav inom området maskin- och processäkerhet samt bygg- och anläggningssäkerhet.

Om det skall fungera i ett företag så krävs det tydliga rutiner samt rätt kompetens på olika nivåer samt ledningens förståelse. Många behöver grunder medan det för områdesspecialister krävs områdesspecifika kurser efter grunderna.

Rekvirera MPSA:s kursprogram eller offert för önskad kurs

Kompetenshöj dig uppåt i pyramiden eller välj en enskild kurs

Kompetensprofil i ett företag



BESTÄLL MPSA:S POPULÄRA SÄKERHETSTEKNISKA HANDBÖCKER

[illegible][illegible][illegible][illegible]





MPSA AB **MPSA AB** **MPSA AB**
 Telefon 040 Telefon 040 Telefon 040
 602 020 Mollan 602 020 Mollan 602 020 Mollan
 S-Gården S-Gården S-Gården
 Ödgar 1030 N. 3402 Ödgar 1030 N. 3402 Ödgar 1030 N. 3402
 Bernege 2004-3402 Bernege 2004-3402 Bernege 2004-3402
 040 221 3402 040 221 3402 040 221 3402
 040 221 3402 040 221 3402 040 221 3402
 040 221 3402 040 221 3402 040 221 3402

Tomas Beall 2012

Handbok

SÄKRA STOPP

Energifrånskiljning och energiavlastning



Tomas Beall 2012

S Maskin & Processsäkerhetsanalys MPSA AB
A
F
E
T
Y

MPSA AB
M MPSA AB
Tidafors 346
660 60 Molkom
S-Sweden
Org.nr 556741-3462
Bankgiro:5004-4650

+46 553 14060 office +46 70 6406027 mobile
Mail:www.mpsa.se Homepage:mpsa@telia.com

Författare: Tomas Beäff
Rikt illustrerade handböcker

MPSA
Machine & Process safety analysis
www.mpsa.se
+46706406027
CE
European and global
SAFETY
Specialist

[illegible]

MPSA AB
 Box 380
 401 00 Uddevalla
 Sweden
 Tel: +46 (0)31 8234 100
 Fax: +46 (0)31 8234 101
 E-mail: info@mpsab.se
www.mpsa.se

Handbok

TILLFÄLLIGA PERSONLYFT

Med truckar och kranar

Kolla så att arbetskorgen är
märkt med erforderliga
uppgifter och tekniska
data så att Du vet vad som
gäller när Du använder den.

Tomas Beaff 2012

VI HJÄLPER TILL MED ATT TA FRAM FÖRETAGSSTANDARDER

Rutiner och blanketter för att hantera säkerhetskraven



Instruktion för upphandling, tillverkning, installation, användning, besiktning, kontroll, ingrepp och modifiering av tryckbärande anordningar

Dok nr: 20.03.01
Rev: 0
Ersätter:
Utfärdad av: Ronnie Flink
Godkänd av: Cristina Sjöberg
Datum: 2011-07-07

Instruktion för upphandling, tillverkning, installation, användning, besiktning, kontroll, ingrepp och modifiering av tryckbärande anordningar

inom
AB Sandvik Materials Technology
Sverige



Sida 1(92)



Fortlöpande tillsyn av tryckbärande anordningar

Innehållsförteckning:

1. Program för fortlöpande tillsyn	1
2. Kontrollprogram 1	2
2.1. Checklista kontrollprogram 1	2
3. Kontrollprogram 2	3
3.1. Checklista kontrollprogram 2	4
4. Kontrollprogram 3	5
4.1. Checklista kontrollprogram 3	6
5. Kontrollprogram 4	7
5.1. Checklista kontrollprogram 4	7
6. Kontrollprogram 5	8
6.1. Checklista kontrollprogram 5	8
7. Kontrollprogram 6 (Alla ånguppvärmda varmesystem, större förångare)	9
7.1. Checklista kontrollprogram 6	10

1. Program för fortlöpande tillsyn

Inom SMT svarar SPD för samordning, administration, utbildning och viss support av hanteringen av systemet för fortlöpande tillsyn av tryckbärande rörledningar.

Utsedda anläggningsägare ansvarar för att särskilt utsedd person är utsedd inom organisationen för att tillsynen sker med rätt intervall och att tillsynen dokumenteras samt att kontrollprotokollen är uppdaterade.

Det åligger dock varje anläggningsägare att i de fall detta inte kan hanteras inom den egna organisationen beställa tillsynen av FM eller annan lämplig resurs. Viktigt att klargöra var respektive ansvarsgräns går mellan servisledning och anläggningsägarens utrustning.

Gällande SMT är leverantör

Tillsynen anläggs

Det finns När tills den sor anläggs

I de fall anläggs arkivera



Fortlöpande tillsyn av tryckbärande anordningar

2. Kontrollprogram 1

För fortlöpande tillsyn enligt AFS 2002:1 om användning av trycksatta anordningar.

Avsättning

Med avsättning avses visuell kontroll med avseende på:

1. Läckage
2. Vibrationer
3. Yttre skador
4. Funktion hos fixar, stöd och upphängningar
5. Märkning med avseende på position, innehåll och strömningsriktning
6. Kontroll av arbetsplattformar, stegar, ryggskydd, racken eller liknande anordningar som används för att utföra den fortlöpande tillsynen och andra rutinarbeten.

Ventiler och annan armatur

7. Kontrollera att samtliga ventiler går att manövrera och är tät, både med avseende på genomströmning och yttre läckage.

2.1. Checklista kontrollprogram 1

Nr	Kontrollpunkt	Ej godkänt	Godkänt
1	Avsättning, läckage	☐	☐
2	Avsättning, vibrationer	☐	☐
3	Avsättning, yttre skador	☐	☐
4	Avsättning, funktion hos fixar, stöd och upphängningar	☐	☐
5	Avsättning, märkning med avseende på position, innehåll och strömningsriktning	☐	☐
6	Avsättning, kontroll av arbetsplattformar, stegar, ryggskydd, racken eller liknande anordningar som används för att utföra den fortlöpande tillsynen och andra rutinarbeten	☐	☐
7	Ventiler och annan armatur, kontrollera det går att manövrera och är tät, både med avseende på genomströmning och yttre läckage	☐	☐

Nr	Noterad avvikelse, åtgärd	Ansvarig	Klart Datum
----	---------------------------	----------	-------------



Instruktion för maskiner tillverkade 1995 och senare avseende upphandling, tillverkning & CE-märkning

Dok nr: 20.01.01
Rev: 3
Ersätter: Rev 2
Utfärdad av: Petter Jansson
Godkänd av: Cristina Sjöberg
Datum: 2011-05-18

Instruktion för maskiner tillverkade 1995 och senare avseende upphandling, tillverkning & CE-märkning

inom
AB Sandvik Materials Technology
Sverige



Sida 1(148)



Instruktion för maskiner tillverkade 1995 och senare avseende upphandling, tillverkning & CE-märkning

Dok nr: 20.01.01
Rev: 3
Ersätter: Rev 2
Utfärdad av: Petter Jansson
Godkänd av: Cristina Sjöberg
Datum: 2011-05-18

1.3 Kopplade dokument till denna instruktion

- 20.0001 Mall 2.1 A EG-försäkrar
- 20.0002 Mall 2.1 B Försäkrar för inbyggnad
- 20.0003 Mall 2.1 A Säkerhetskomponent
- 20.0004 Mall Bruksanvisning Maskin
- 20.0005 Checklista Bruksanvisning Maskiner
- 20.0006 Checklista Produktöverlagande ny maskin
- 20.0007 Checklista Säkerhetsöverlämnande i projekt
- 20.0008 Checklista Förändring maskin
- 20.0009 Mall Utbildning ny eller ändrad maskin
- 20.0010 Mall Grovriskinventering projektstart
- 20.0011 Mall Riskanalys mot maskindirektiv
- 20.0012 Mall Sammanställning åtgärder efter riskanalys
- 20.0013 Mall Riskbedömning projektfaser för maskin
- 20.0014 Leverantörssammanställning
- 20.0015 Mall Kontrolldokument Teknisk fil
- 20.0016 Katalogstruktur för Teknisk fil (zip)
- 20.0020 Mall Skylt varning maskin
- 20.0021 Mall Skylt samordningsansvar projekt
- 20.0022 Mall Skylt Elansvarig - Eldriftansvarig
- 20.0023 Mall Bortkoppling av skyddsanordning
- 20.0024 Mall Kontroll Nodstopp i maskin