Håkan Carlsson, IVF
Jan Jacobson, SP

Säkerhet i datorbaserade maskinstyrningar
Abstract

Safety of Computer-based Machine Control

The control systems of most modern machinery contain programmable logic. Assessment of safety is an increasingly important issue. This report summarises a pre-study on how to assess safety in computer-based machine control systems. The work to develop an assessment method will continue during 1996 and 1997.

Basic safety principles are summarised, and a distinction is made between the general parts and the safety related parts of a control system. Different causes of faults are mentioned.

Both the EC machinery directive and old national regulations in Europe contain requirements for safety of machinery. The report summarises what has been said of control systems, both by the EC directives, by European standards and by international standards.

Five case studies have been made to give examples of machines and control systems which will have to be assessed. A packaging machine, an offset press, a tooling machine and two programmable controllers with enhanced safety are described. The safety of these devices is not assessed, neither are the descriptions in this report intended to be complete. The intention is to give examples of safety related control systems.

The general question for an assessment method is; "Is the safety of the control system sufficient for its application?" The assessment method will contain a tool-box of validation methods to be used with different kinds of control systems. Which methods to use will be much depending on the principle for building safety. A machine control system completely based on programmable logic will require extensive assessment. The requirement for fault tolerance will also control the selection of validation methods.

Key words: safety of machinery, control system, programmable controller, computer safety, software safety, safety validation, safety assessment

SP
SP-RAPPORT 1995:58
ISBN 91-7848-585-1
ISSN 0284-5172
Borås 1995

Swedish National Testing and Research Institute
SP REPORT 1995:58

Postal address:
Box 857, S-501 15 BORÅS,
Sweden
Telephone + 46 33 16 50 00
Telefax + 46 33 13 55 02
# Innehållsförteckning

<table>
<thead>
<tr>
<th>Kapitel</th>
<th>Kapitelnamn</th>
<th>Sida</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Datorer och maskinsäkerhet</td>
<td>7</td>
</tr>
<tr>
<td>1.1</td>
<td>Allmänt</td>
<td>7</td>
</tr>
<tr>
<td>1.2</td>
<td>Maskinstyrning</td>
<td>9</td>
</tr>
<tr>
<td>1.3</td>
<td>Säkerhetsystem och styrsystem</td>
<td>10</td>
</tr>
<tr>
<td>1.4</td>
<td>Felorsaker</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>EG-direktiv</td>
<td>13</td>
</tr>
<tr>
<td>2.1</td>
<td>Allmänt</td>
<td>13</td>
</tr>
<tr>
<td>2.2</td>
<td>EGs maskindirektiv</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>EGs direktiv om minimikrav vid användning av arbetsutrustning</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>Europastandarder</td>
<td>17</td>
</tr>
<tr>
<td>3.1</td>
<td>Allmänt</td>
<td>17</td>
</tr>
<tr>
<td>3.2</td>
<td>SS-EN 292</td>
<td>18</td>
</tr>
<tr>
<td>3.3</td>
<td>SS-EN 418</td>
<td>20</td>
</tr>
<tr>
<td>3.4</td>
<td>prEN 574</td>
<td>21</td>
</tr>
<tr>
<td>3.5</td>
<td>SS-EN 775</td>
<td>22</td>
</tr>
<tr>
<td>3.6</td>
<td>prEN 954</td>
<td>23</td>
</tr>
<tr>
<td>3.7</td>
<td>prEN 1037</td>
<td>25</td>
</tr>
<tr>
<td>3.8</td>
<td>prEN 1088</td>
<td>25</td>
</tr>
<tr>
<td>3.9</td>
<td>prEN 1760-1</td>
<td>26</td>
</tr>
<tr>
<td>3.10</td>
<td>prEN 50100</td>
<td>27</td>
</tr>
<tr>
<td>3.11</td>
<td>SS-EN 60204-1</td>
<td>28</td>
</tr>
<tr>
<td>4</td>
<td>Internationella standarder</td>
<td>30</td>
</tr>
<tr>
<td>4.1</td>
<td>Allmänt</td>
<td>30</td>
</tr>
<tr>
<td>4.2</td>
<td>SS-ISO 11161</td>
<td>30</td>
</tr>
<tr>
<td>4.3</td>
<td>IEC 1131</td>
<td>34</td>
</tr>
<tr>
<td>4.4</td>
<td>Draft IEC 1508</td>
<td>37</td>
</tr>
<tr>
<td>5</td>
<td>Utvärderingsmetod</td>
<td>40</td>
</tr>
<tr>
<td>5.1</td>
<td>Projektets mål</td>
<td>40</td>
</tr>
<tr>
<td>5.2</td>
<td>Avgränsningar</td>
<td>40</td>
</tr>
<tr>
<td>5.3</td>
<td>Förslag till utvärderingsmetod</td>
<td>41</td>
</tr>
<tr>
<td>5.4</td>
<td>Fortsatt arbete</td>
<td>43</td>
</tr>
</tbody>
</table>
## Appendix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Fallstudier</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>Förpackningsmaskin</td>
<td>44</td>
</tr>
<tr>
<td>A.1</td>
<td></td>
<td>Offsetpress</td>
<td>47</td>
</tr>
<tr>
<td>A.2</td>
<td></td>
<td>Verktygsmaskin med operatörspanel</td>
<td>52</td>
</tr>
<tr>
<td>A.3</td>
<td></td>
<td>PLC for safety critical applications - Pilz PSS 3000</td>
<td>57</td>
</tr>
<tr>
<td>A.4</td>
<td></td>
<td>PLC för säkerhetstillämpningar - Siemens S5-95F</td>
<td>63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Funktioner beskrivna i standarder</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td></td>
<td>67</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Referenser</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td></td>
<td>68</td>
</tr>
</tbody>
</table>

| C.1 | Rapporter | 68 |
| C.2 | Direktiv | 68 |
| C.3 | Standarder | 68 |
Förord


Dessutom tackar vi representanterna för de företag vilka hjälpt oss med att fallstudier, diskussioner och problemställningar;
Volvo Personvagnar Komponenter, Skövde
Duni, Halmstad
Siemens, Upplands Väsby
Lidköping Machine Tools, Lidköping
Nerikes Allehanda, Örebro
Honeywell, Örebro
ABB Industrial Systems, Västerås
Pilz, Ostfoldern, Tyskland
Treotham, Stockholm

De flesta standarder och standardförslag som citeras i rapporten kan köpas från Standardiseringskommisionen (SIS, tel. 08-613 52 00). Det pågående standardiserings-arbetet gör att nya utgåvor av denna rapporters referenser kontinuerligt utges.
Sammanfattning

De flesta moderna maskiner har någon typ av programmerbar logik i sitt styrsystem. Frågan hur man ska kunna visa att tillräcklig säkerhet uppnåtts är aktuell för varje maskin. Både EGs maskindirektiv och de äldre nationella bestämmelser som funnits i de flesta europeiska länder ställer krav på säkerheten i utrustningen. Det har hittills varit sällsynt att en maskinbyggare medvetet valt att göra säkerhetskritiska funktioner helt beroende av en dator.

Denna rapport syftar till att visa dagens tillämpningar och föreskrifter för datorbaserade maskinstyren. Rapporten sammanfattar både EG-direktiv, europastandarder och internationella standarder inom området maskinsäkerhet. Dessutom har 5 olika fall studerats. Avsikten är att genom exempel ge en bättre förståelse för hur de maskiner och styren avser där det finns behov att verifiera säkerheten.

Projektets mål är att utveckla praktiskt tillämpbara krav och verifieringsmetoder för säkerhet i datorbaserade maskinstyren där risk för personskada finns. Denna rapport beskriver förprojektets resultat. Huvudprojektets egentliga uppgift är sedan att ta fram krav och verifieringsmetoder.

Den övergripande frågan för en metod att utvärdera maskinstyren blir; "Är säkerheten i min maskinstyrning tillräcklig?". Frågan kan ställas många gånger under en maskins livscyklo. Vår ambition är att utvärderingsmetoden ska kunna vara till nytta i alla dessa situationer.

1 Datorer och maskinsäkerhet

1.1 Allmänt

De flesta moderna maskiner har någon typ av programmerbar logik i sitt styrsystem. Maskinen styrs ofta av ett programmerbart styrsystem (PLC) och kommunicerar med operatören via en bildskärm eller textdisplay. Det är sannolikt att flera av maskinens givare och ställdon har mikrodatorer inbyggda. Det finns också exempel på maskiner där all styrning sker genom en inbyggd mikroprocessor vilken styr maskinens funktion. Samtidigt som denna utveckling skett under de senaste 15 åren har frågan om de nya styrsystemens säkerhet diskuterats.

Ett väl beprövat sätt att bygga styrsystem med hög personssäkerhet är att använda dubblerade och övervakade reléer. (Se figur 1.) Enkelrelé räcker inte för att en farlig rörelse ska beordras. Om ett fel uppstår kommer det att upptäckas eftersom säkerhetsreléerna har tvångsförda kontakter. När en dator används i en säkerhetskritisk del av maskinstyningen ska säkerheten förblivit lika god som om samma funktion hade byggts med relässäkerhet. (Se figur 2.)

![Diagram](image)

Figur 1. Maskinstyning med dubblerade och övervakade reléer.

Frågan hur man ska kunna visa att tillräcklig säkerhet uppnåtts är aktuell för varje maskin. Både EGs maskindirektiv och de äldre nationella bestämmelser som funnits i de flesta europeiska länder ställer krav på säkerheten i utrustningen. Reläteknik är enkel att använda och det är förhållandevis enkelt att visa om säkerheten kan upprätthållas vid fel. Det har hittills varit sällsynt att en maskinbyggare medvetet valt att göra säkerhetskritiska funktioner helt beroende av en dator.

När maskiner och maskingrupper växer i storlek kommer också styrsystemen att växa. Ganska snart kan de system för relälogik som används bli både svåröverskådliga och fysiskt stora. Underhållet försvåras och det blir lätt att göra fel vid ändringar i funktionen. Programmerbar logik som ersätter för relälogik påstås ibland vara mer ekonomiskt och lättare att överblicka. Slaget är i de flesta fall mindre.
Figur 2. Maskinstyrning med programmerbart elektroniskt system

En annan fördel med datorbaserade maskinstygningsar är de ökade möjligheterna till självövervakning. Systemet kan innehålla övervakningsfunktioner som varnar eller stänger då fel detekteras. Självövervakningen kan också detektera om systemet uppför sig onormalt, t.ex. om en svarstid blir för lång.

Det finns också tillämpningar där maskintillverkaren är tvungen att förlita sig på säkerheten i datorn. Av olika tekniska skäl kan det var omöjligt att utnyttja säkerhet uppbryggd på elektromekaniska komponenter.

Frågorna om vad som kan anses tillräckligt säkert i en viss tillämpning kommer ofta upp. Vilka funktioner kan man anförra en vanlig PLC? Går det att ersätta relälogik med elektronik utan att säkerheten försämras? Är det rimligt att förlita sig på den mikrodator som sitter inbyggd i en säkerhetskritisk komponent?

Det förekommer att mikrodatorer ingår i säkerhetskompagnentern, t.ex. ljusrädar och enheter för nödstopp. Både Sveriges Provnings- och Forskningsinstitut (SP) och Institutet för verkstads- och teknisk forskning (IVF) har tidigare arbetat med dessa frågor. [SP91:20] [SP93:51] [SP93:52] [IVF91824] [IVF94838]

Denna rapport syftar till att visa dagens tillämpningar och föreskrifter för datorbaserade maskinstygningsar. De allmänna hälsol- och säkerhetskraven för maskiner styrks i Europa av EG:s maskindirektiv. Vår avsikt är inte att täcka alla olika typer av maskiner, utan att inrikta oss på maskiner med säkert läge. Riskerna med sådana maskiner upphör om energiutlösaren stängs av (s.k. säkert läge). De flesta maskiner inom verkstadsindustrin är exempel på sådana maskiner.
1.2 Maskinstyrning

I dagligt tal är ofta orden styrsystem och maskinstyrning synonyma med PLC-system (programmerbara styrsystem) eller CNC-styrning (numerisk styrning av verkstadsmaskiner). Det sätt som begreppet styrsystem används inom den europeiska maskinsäkerheten är dock mer omfattande. Inte bara själva logikenheten ("datorn") avses utan hela kedjan från sensorer och manöverdon via logikenhet till effektsyrdon.


![Diagram som beskriver styrsystem](image)

Figur 3. Principen för styrsystem enligt SS-EN 292

I denna rapport menar vi med maskinstyrning det samma som standarderna menar med styrsystem. Datorberoendet kan finnas i alla led i kedjan; "intelligenta" givare kan ha inbyggda mikroprocessorer, logikenheten har nästan alltid någon typ av programvara och ställdonen har ibland en inbyggd mikrodator.

Den utvärderingsmetod vi syftar att utveckla är mest avsedd att kunna användas på logikenheten. Det kan dock mycket väl tänkas att även logik i givare och ställdon måste beaktas för att kunna utvärdera säkerheten.
1.3 Styrsystem och säkerhetssystem

Det är viktigt att hålla isär begreppen funktionssäkerhet och personsäkerhet. Person-
säkerheten innebär att produkten inte ska orsaka personskada, medan funktions-
säkerheten betecknar om maskinen presterar det som förväntas. Kraven på person-
säkerhet ligger oftast avsevärt högre än kraven på funktionssäkerhet. Ibland används
begreppet produktssäkerhet synonymt med personsäkerhet. [FOA]

Bland maskinstyrningens uppgifter är endast några verkligt kritiska för personsäkerheten.
På funktionssäkerheten behöver normalt inga personsäkerhetskrav ställas. Visserligen är
skador på egendom och stillestånd i produktion inte önskvärt, men med personsäkerhet
avses säkerhet för operatören. Med operatör menas alla som installerar, använder, ställer
in, underhåller, rengör reparerar eller transporterar maskinen.

Ett sätt att tänka leder till att styrningen kan delas in i en allmän maskinstyrning och ett
säkerhetssystem. (Se figur 4.) De funktioner som sköts enbart av den allmänna
maskinstyrningen kan förvisso vara viktiga för funktionssäkerheten, men inte för
personsäkerheten. Funktionerna som är viktiga för operatörsskyddet vid maskinen styrs
huvudsakligen av säkerhetssystemet.

På säkerhetssystemet ställs höga krav eftersom detta är garantin mot operatörsskador.
Den allmänna maskinstyrningen ska givetvis vara av god allmän kvalitet, men behöver
inte ge den högsta graden av säkerhet.

![Diagram](https://via.placeholder.com/150)

**Figur 4.** Maskinstyrning och säkerhetssystem

Genom att lägga funktionerna för personsäkerhet i säkerhetssystemet kan man
förhoppningsvis lättare visa att maskinen är tillräckligt säker för att användas.
Säkerhetssystemet är mindre komplex eftersom endast ett antal grundläggande
funktioner realiseras här. Gränssnittet mellan säkerhetssystemet och dess omgivningar
måste vara väl definierat och enkelt hället.
En maskinstyra kan naturligtvis också byggas med alla funktioner i en enda dator. De parasäkerhetskritiska funktionerna integreras mer eller mindre med den allmänna funktionerna. (Se figur 5.) Höga säkerhetskra kommer då att behöva ställas på alla funktioner om de är kopplade till varandra. Detta leder till att det blir svårare och mer tidsödande att visa säkerheten i maskinstyran.

![Diagram](image)

Figur 5. Maskinstyra med en enda dator

### 1.4 Felorsaker

Fel i en maskinstyra tillhör någon av följande grupper [SP91:20];
- programvarufel
- systematiska hårdvarufel (konstruktionsfel)
- slumpmässiga hårdvarufel (t.ex. åldring)
- miljöstörningsfel
- användarfel

Med hårdvarufel menas här speciellt fel i elektronikhårdvara. Dessa kan finnas både i maskinvaran för själva datordelens av styrningen och i elektronikkomponenter i övriga delar av styrningen.

Det är viktigt att man har klart för sig vilka felorsaker som kan orsaka personskador. Olika utvärderingsmetoder behövs för olika fel. Metoder som t.ex. används för att leta fel i programvara ger inget svar om eventuell feltäthet i hårdvara.

En konventionellt byggd maskinstyra med säkerhetssystemet byggt med elektromekaniska komponenter har ett felrad enligt figur 6. Den oacceptabla funktionen (topphändelsen) utlösas först om det är fel i datorfunktionen samtidigt som det är fel i säkerhetssystemet (rellerna). Ett programvarufel kan i ett sådant system inte ensamt utlösa en oacceptabel funktion.
Figur 6. Säkerheten beror av datordel och övriga komponenter. [FOA]

I ett system där datordelen i maskinstyrningen direkt kan påverka säkerhetskritiska funktioner ser felträdet annorlunda ut. Här kan datorn ensam orsaka oacceptabla funktioner. Denna situation där personsäkerheten inte främst styrs av säkerhetssystemet är givetvis inte den eftersträvade.

Figur 7. Säkerheten beror av datordelen direkt [FOA]
2 Direktiv

2.1 Allmänt

Den europeiska gemenskapen har givit direktiv om de väsentliga hälso- och
säkerhetskraven för maskiner. Dessa krav är obligatoriska och gäller alla maskiner som
används inom EES-området. Inom den Europeiska Unionen ska direktiven från EG-
kommissionen omsättas till förordningar och lagar inom alla medlemsländerna. I Sverige
har Arbetskyddsstyrelsen utgivit maskindirektivet i sin författningssamling. [AFS9448]

Direktiven ger endast de grundläggande kraven och förutsätter sedan att dessa ska tolkas
och preciseras i bl.a. standarder. Standarderna är dock frivilliga att följa. Det viktiga är
att man inte bryter mot direktiven.

I detta kapitel sammanställs några punkter ur maskindirektivet [AFS9448] och minimi-
direktivet [AFS9336] som berör egenskaper hos maskinstyrningar. Sammanställningen
fokuserar på säkerhets-filosofier, funktionalitet och feltålighet.

2.2 EGs maskindirektiv

EGs maskindirektiv utfärdades 1989 (direktiv 89/392/EEG) och har sedan ändrats vid tre
tillfällen (direktiv 91/368/EEG, 94/44/EEG och 93/68/EEG). Den svenska versionen av
maskindirektivet finns i Arbetskyddsstyrelsens författningssamling [AFS9448]. Alla
maskiner som "sätts på marknaden" inom EU måste fr.o.m. 1 januari 1995 uppfylla detta
direktiv.

Princinen är att säkerheten i första hand ska uppnås genom att åtgärder vid konstruktion.
Punkt 1.1.2 b) säger

Vid valet av lämpligaste metoder skall tillverkaren tillämpa följande principer, i
nedan angiven ordning:
- Risker skall så långt möjligt undanröjas eller minskas (säkerheten integreras
  redan på konstruktions- och tillverkningsstadierna).
- Nödvändiga skyddsåtgärder skall vidtas för sådana risker som inte kan
  undanröjas.
- Tillverkaren skall informera om kvarstående risken .....

Maskindirektivet säger i bilaga 1, punkt 1.2.2 "Styrsystems säkerhet och tillförlitlighet":

Styrsystemen skall vara konstruerade och tillverkade på så sätt att de är säkra
och tillförlitliga, så att farliga situationer inte uppstår. Framför allt skall de vara
konstruerade och tillverkade så att
- de kan täla de påfrestningar som härrör från normal användning och yttre
  faktorer, och
- fel i logik inte leder till farliga situationer.
Denna punkt kan tolkas till att maskinen måste kunna hantera fel. Ett fel i logik i programvara eller i hårdvara får definitivt inte leda till farliga situationer. Påkänningar p.g.a. yttre miljöpåverkan får inte heller leda till farliga situationer. Man kan också tolka in att slumpmässiga fel i hårdvara inte får orsaka farliga situationer. Exempel på sådana fel som kan uppkomma under normal användning är att relä "klibbar" och att transistorer går sönder.

Punkt 1.2.8 "Programvara" säger:

*Den interaktiva programvaran för kommunikation mellan operatören och maskinens manöver- eller styrsystem skall vara användarvänlig.*

Vad som menas med en användarvänlig programvara är svårt att exakt beskriva. Tydlig layout på bildskärm, logisk användning av tangenter på tangentbord och ett språk som operatören förväntas behärska är exempel på användarvänlighet. Under denna punkt säger maskindirektivet däremot inget om den programvara vars logik styr maskinens funktioner.

Maskindirektivets bilaga 1 ställer också krav på vissa funktioner hos styrsystemen, speciellt vad det gäller start- och stoppfunktioner. Punkten 1.2.3 "Start" säger bl.a.

*Maskiner skall kunna startas endast genom avsiktlig påverkan på ett för detta ändamål särskilt avsett manöverdon.*

*Samma krav gäller*

- vid återstart av maskiner efter stopp, oavsett orsaken härrör, och
- vid avsevård förändring av driftsförhållanden (t.ex. hastighet, tryck osv.), såvida inte sådan återstart eller ändring av driftsförhållanden kan ske utan risk för utsatta personer.

Punkt 1.2.4 "Stoppanordningar" fortsätter med att bl.a. säga

*Normalt stopp*

Alla maskiner skall vara försedda med ett manöverdon som gör det möjligt att på ett säkert sätt stoppa maskinen fullständigt.

......

När maskinen eller dess farliga delar har stoppat skall kraftförsörjningen till de berörda drivorganen vara bruten.

och

*Nödstopp*

Alla maskiner skall vara försedda med en eller flera nödstoppansökringar som gör det möjligt att avvärja överhängande fara eller fara som redan uppstått.

Punkt 1.2.6 "Fel i kraftförsörjningen" fastställer att

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

Maskindirektivet ger alltså ingen detaljerad vägledning för hur en maskinstyrning ska konstrueras. Styrningen och dess egenskaper får dock inte strida emot vad som sägs i maskindirektivet.
2.3 EGs direktiv om minimikrav vid användning av arbetsutrustning


Minimikraven anges i bilaga 1 av [APS 1993:36]. Bl.a. anger man under punkt 2.1 det viktigaste kravet på styrsystem:

"Styrsystemen skall vara säkra. Ett tekniskt fel eller en skada på styrsystemen får inte leda till en risksituation."

Direktivet slår alltså tydligt fast principen om felfördragligt för enkelfel, men exakt vad som räknas som enkelfel går man inte in på. En rimlig tolkning är att varken ett fel i givare, programvara, styrdatorns hårdvara eller ställdonen kan tillåtas leda till en risksituation. Det finns också andra krav vilka berör styrningens funktion. Punkt 2.2 säger bl.a.

"Start av en arbetsutrustning får endast kunna ske genom en medveten manöver med ett därfor avsett manöverdon."

"Detsamma skall gälla
- vid återstart, oavsett anledningen till stoppet och
- vid styrning av en betydande förändring av arbetsfunktionen (t.ex. hastighet, tryck etc.),
utom i det fall att en sådan återstart eller ändring inte utsätter den/de som arbetar för risk."

Styrningen får alltså inte automatiskt starta en maskins arbete, varken vid spännings- tillslag eller vid återstart efter stopp. Förändringar av viktiga funktioner får inte heller ske utan att operatören ger kommando till styrningen.

Punkt 2.3 behandlar funktionen vid stopp:

All arbetsutrustning skall ha ett manöverdon, som gör det möjligt att stoppa den helt och under säkra förhållanden.

Varje arbetsplats skall ha ett manöverdon, som gör det möjligt att stoppa hela eller delar av arbetsutrustningen beroende på typ av risk, så att utrustningen är i ett säkert tillstånd. Stoppduken skall ha prioritén över startanordningen.

När arbetsutrustningen, eller dess farliga delar, har bringats till stopp, skall energitillförseln till de aktuella drivanordningarna avbrytas.

Ytterligare funktionskrav finns under punkt 2.8 där man bl.a. säger

När det finns risk för olyckor på grund av mekanisk kontakt med arbetsutrustningens rörliga delar, skall dessa ha skydd eller säkerhetsanordningar, som hindrar tillträde till riskområden eller stoppar de farliga delarnas rörelse, innan man når riskområdena.

Ett skydd är ett fysiskt hinder och ingen del av styrsystemet. Skyddsanordningar har däremot någon slags givare som känner av när operatören helt eller delvis tar sig in i riskområdet och ibland även känner av när operatören befinner sig i riskområdet. Optiska givare finns i ljusbommar och ljusridåer. Tryckkänsliga givare finns i kontaktmattor och kontaktlistor. Lägeskopplare används ofta som förrenglingsanordning på förrenglande skydd.

Punkt 2.14 säger om fränkoppling av energi:

Varje arbetsutrustning skall ha lätt identifierbara anordningar för att fränkoppla all energitillförsel.
Återinkoppling skall kunna ske utan risk för säkerheten.

Det ställs krav på hur återinkoppling av energi hanteras. Styrningen får t.ex. inte orsaka en farlig rörelse i utrustningen bara för att tryckluft eller hydraultryck kopplas in.

Direktivet om användning av arbetsutrustning tar även upp flera andra minimikrav. Eftersom de inte direkt berör styrsystemen tas de inte upp i denna sammanfattning.
3 Europastandarder

3.1 Allmänt


Till maskindirektivet kopplas standarder för att ge mer detaljerade regler. En standard sägs vara harmoniserad när den blivit omnämnd i EG:s tidskrift "Official Journal". Om en produkt uppfyller en harmoniserad standard antags automatiskt (presumption) att den också uppfyller direktivet. Detta kallas presumtionsprincipen. Bland de europastandarder vilka är harmoniserade mot maskindirektivet finns EN 292 (se 3.2), EN418 (se 3.3), EN 60204 (se 3.11) och EN 775 (se 3.5).

När en europastandard (EN) antages förutsätts den också sättas i kraft som svensk standard (SS-EN). I vissa fall anses standarden av så allmänt intresse att texten översätts till svenska. I de fall när standarden främst riktar sig till tekniska specialister inom ett begränsat område brukar den engelska originaltexten användas även i den svenska standarden. Under tiden en standard håller på att arbetas fram cirkulerar utkast till europastandard, prEN (pr står för "provisional"), för kommentarer och omröstning.

Det finns flera standarder vilka berör datorbaserade maskintystningar. I de flesta fall är reglerna inte särskilt detaljerade utan lämnar mycket att tolka. Speciellt gäller detta för styrsytemets datordel. Detta gör det komplicerat att komma fram till en verifieringsmetod för datorbaserade maskintystningar.

3.2 SS-EN 292 Maskinsäkerhet, grundläggande begrepp, allmänna konstruktionsprinciper


Punkt 3.7 i del 2 beskriver säkerhetsprinciper vid konstruktion av styrsystem, bl.a. säger punkt 3.7.1

Den primära åtgärden för att starta eller accelerera en mekanisms rörelse bör vara att man tillför eller ökar elektrisk spänning eller vätsketryck...

Omvänt skall den primära åtgärden för att stoppa eller saka ned vara att man avlägsnar eller reducerar elektrisk spänning eller vätsketryck...

Principen kan tyckas enkel och i många fall självläkar. En maskin ska inte starta förrän spänning tillförs, och stoppa om matningsspänningen försvinner. Punkt 3.7.2 fortsätter

Spontan återstart av en maskin när energitillförseln återkommer efter avbrott skall förhindras, om en sådan återstart kan medföra en risk (t.ex. genom användning av självhållande relä, kontaktor eller ventil).

Punkt 3.7.5 säger att farligt beteende kan förhindras genom

Dubbling (eller redundans) av "kritiska" komponenter: andra komponenter än väl beprövade komponenter (med inbyggd säkerhet) kan användas för skyddsfunktioner under förutsättning att en annan (eller andra) kan upprätthålla skyddsfunktionen vid fel i en komponent och sålunda ge den erforderliga säkerhetsnivån. Det är då väsentligt att anordna automatisk övervakning i kombination med olika konstruktionsprinciper och/eller tekniker för att undvika samtidig felfunktion med gemensam orsak...

Automatisk övervakning beskrivs närmare under punkt 3.7.6

Automatisk övervakning säkerställer att en skyddsåtgärd initieras om en komponent eller ett elements förmåga att fullgöra sin funktion minskas, eller om processbetingelserna ändras på ett sådant sätt att risker framkallas.

Skyddsåtgärderna kan vara:
- att stoppa den farliga processen,
- att hindra återstart av processen efter det första stoppet som skett efter det att felet hos komponenten eller elementet inträffat,
- att utlösa en larmsignal.
Punkt 3.7.7 säger för omprogrammerbara styrsystem

När sådana komponenter används i säkerhetskritiska styrsystem skall tillförlitliga anordningar finnas som förhindrar oavsiktlig eller avsiktlig förändring av det lagrade programmet. Sådana anordningar kan inkludera:
- stiftade kamskivor
- oåtkomlig mjukvara, t.ex. läsminne (ROM).
- läs som inskränker åtkomlighet,
- lösenord för åtkomlighet av mjukvara.

För användningssätt med olika säkerhetsnivåer påpekas punkt 3.7.9

Om maskiner har konstruerats och byggs för att tillåta användning med flera manöver- och användningssätt som medför olika säkerhetsnivåer (t.ex. för att tillåta justering, underhåll, inspektion, etc) skall de utrustas med en funktionsväljare som kan läsas i varje läge. Varje läge hos väljaren skall motsvara ett enda manöver- eller användningssätt.

Väljaren kan ersättas av en annan väljaranordning som begränsar användningen av vissa funktioner hos maskinen till vissa operatörskategorier (t.ex tillträdeskoder för vissa numeriskt styrd funktioner, etc).

För andra åtgärder för konstruktion av elektriska styrsystem hänvisar SS-EN 292 dessutom till [EN 60204].
3.3 SS-EN 418  Maskinsäkerhet - Nödstoppssutrustning


Punkt 4.1.1 säger

*Nödstoppfunktionen skall vara tillgänglig och i funktion vid alla tillfällen oberoende av användningssätt.*

Punkt 4.1.12

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 återstartkommando.

Punkt 4.1.13

*Det tillstånd i vilket maskinen befinner sig efter ett nödstoppkommando skall inte förändras oavsiktligt (sovänat) under den tid manöveranordningen är i påverkat tillstånd.*
3.4 prEN 574 Safety of machinery - Two-hand control device

För vissa farliga maskinrörelser där det finns risk för att operatören kan komma i kläm med händerna används s.k. tvåhandsmanöver. För att starta den farliga maskinrörelsen krävs ett don vilket måste manövreras med båda händerna. Ett standardförslag [EN574] beskriver egenskaper hos tvåhandsmanöverdon.

Kraven på feltä仡iet beskrivs under punkt 7.2;

A single fault in the two-hand control device shall not lead to the loss of the safety function(s), in particular,

the two-hand control device shall not be converted into a one hand control device as a consequence of one fault.

An output signal shall not be generated as a consequence of one fault.

För användningar med stora risker krävs automatisk självövervakning. Punkt 7.3 förklarar;

The single fault shall be detected at or before the next operation of the safety function(s), in particular,

after an occurrence of a fault any further output signal shall be prevented.

An output signal being generated at the time of occurrence of the fault may continue, but shall cease when either or both input signals are terminated.

If a single fault cannot be detected then a combination of faults shall not lead to a loss of the safety function.

Punkt 8 säger angående programmerbara system:

Where a programmable electronic system (PES) is used to achieve the functional characteristics of a two-hand control device, the safety performance of the hardware and software of the PES shall be validated to the level indicated by the risk assessment.

Hur man ska göra utvärderingen av hårdvara och mjukvara sägs dock inte.
3.5 SS-EN 775 Industrirobotar - Maskinsäkerhet

Standarden ger vägledning för säkerhetsaspekter vid utveckling, konstruktion, programmering, användning, reparation och underhåll av industrirobotar och system av industrirobotar.

Säkerhetsfilosofin beskrivs allmänt under punkt 4.1:

"Technical measures for the prevention of accidents are based upon two fundamental principles:
- the absence of persons in the safeguarded space during automatic operation;
- the elimination of hazards or at least their reduction during interventions (e.g. teaching, program verification) in the safeguarded space.

"Failure to safety" beskrivs under punkt 5.1:

"The robot system shall be designed, constructed, and implemented so that in case of a foreseeable failure of any single component, whether electrical, electronic, mechanical, pneumatic, or hydraulic, safety functions are not affected or when they are, the robot system is left in a safe condition. Safety functions include but are not limited to
- limiting range of motion,
- emergency and safe stopping,
- reduced speed, and
- safeguard interlocking.

Vilket tänkbart fel som helst förväntas alltså leda till att roboten går till säkert läge, dvs. den blir stående i ett läge där inga risker kan uppkomma. Standarden beskriver inte om, och i så fall till vilken grad, man kan bygga säkerheten på programmerbara system."
3.6 prEN 954 Safety of machinery - Safety related parts of control systems

3.6.1 Part 1: General principles for design


Ett centralt begrepp i standarden är riskkategorierna B, 1, 2, 3 och 4. (Se tabell i figur 8.) Kategorierna talar om hur styrsystemet uppför sig vid fel

<table>
<thead>
<tr>
<th>Kategori</th>
<th>Systemets uppträdande vid fel</th>
<th>Princip för att uppnå säkerhet</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>När ett fel uppträder kan skyddsfunksjonen förloras.</td>
<td>Genom val av komponenter</td>
</tr>
<tr>
<td>1</td>
<td>Som B, men högre tillförlitlighet på skyddsfunksjonen.</td>
<td>&quot;</td>
</tr>
<tr>
<td>2</td>
<td>Felet detekteras genom periodisk kontroll. Uppträdandet av ett fel kan leda till förlorad skyddsfunksjon mellan kontrollerna. Förlust av skyddsfunksjonen detekteras vid kontrollen.</td>
<td>Genom systemstruktur</td>
</tr>
<tr>
<td>3</td>
<td>När ett enkelfel uppträder kvarstår alltid skyddsfunksjonen. Vissa, men inte alla, fel detekteras. Ackumulering av upptäckta fel kan leda till att skyddsfunksjonen förloras.</td>
<td>&quot;</td>
</tr>
<tr>
<td>4</td>
<td>När felet (felet) uppträder kvarstår alltid skyddsfunksjonen. Felet (felet) kommer att upptäckas i tid för att förhindra att skyddsfunksjonen förloras.</td>
<td>&quot;</td>
</tr>
</tbody>
</table>

Figur 8. Tabell över feltäthetskategorier för säkerhetsrelaterade delar av styrsystem

Under punkt 7.1 säger man om hur fel ska ansättas

"... In general, the following fault criteria shall be taken into account:

- if as consequence of a fault further components fail, the first fault and all these following faults shall be considered to be a single fault;

- common mode faults are regarded as a single fault;

- the occurrence of two independent random faults is not considered at the same time.

..."
Följd fel (t.ex. att en transistor skadas för att ett motstånd kortsluts) och fel med gemensam orsak (t.ex. blixtnedslag som slår ut dubbla överspänningsskydd) räknas alltså som ett fel. Däremot ska man inte behöva ta hänsyn till två slumpmässiga fel samtidigt (t.ex. att två reläer svetsar samtidigt).

Punkt 7.2. förklarar också att det inblandade måste få vara möjligt att antaga att vissa fel kan uteslutas. Standarden säger

..... *Fault exclusion can be based on:*

- *the improbability of occurrence of a certain fault(s);*
- *generally accepted technical experience which can be applied independently of the application under consideration;*
- *technical requirements deriving from the application and the specific risk under consideration.*

Det är alltså tillåtet att inte beakta osannolika fel och sådana fel som kan uteslutas med "sunt tekniskt förnuft".

3.6.2 Part 2: Validation

- mekaniska styrsystem
- hydrauliska och pneumatiska styrsystem
- elektriska/elektroniska/programmerbara styrsystem
3.7 prEN 1037 Safety of machinery - Isolation and energy dissipation - Prevention of unexpected start-up

Oavsiktlig start tillhör de farligaste felsätt som kan förekomma hos maskiner. En farlig rörelse som startar när operatören tror att maskinen är säkert stoppad kan vara mycket svår att undvika. Åtgärder för att isolera maskinen från kraftkällor och för att förhindra oavsiktlig start beskrivs i ett standardförslag [EN1037].

Under punkt 6.2.4 talar man om säkerhetsrelaterade delar för datalagring och databehandling (dvs. datorbaserade maskinstyrningar);

*The safety-related parts of the data storage and processing equipment shall be designed - and their components selected - so that the probability for this equipment to generate start commands which may lead to an unexpected start-up is as low as possible.*

Hur man sedan ska konstruera in och verifiera säkerhet förklaras inte i detalj. Man hänvisar dock till den skrivning i [EN60204] som säger att det inte är tillräckligt att förlita sig på ett enk惭nt programvarbart system.

3.8 prEN 1088 Safety of machinery - Interlocking devices with and without guard locking

Många rörliga delar på maskiner förses med skydd för att minska riskerna för skador vid drift. Öppningsbara luckor, grindar etc. förses med brytare som stoppar maskinens arbete då skyddet öppnas. Standardförslaget prEN 1088 [EN1088] definierar grundläggande begrepp och allmänna principer för hur föreglade skydd ska konstrueras.

Standarden koncentreras sig på mekaniska aspekter av hur föreglingar ska konstrueras och säger mycket lite om själva styrsystemet och dess dator.
3.9 prEN 1760-1 Safety of machinery - Pressure sensitive protective devices. Part 1: General principles for the design and testing of pressure sensing mats and pressure sensing floors


Standarden skiljer på själva givardelen och styrenheten som genererar stoppsignalen. Det ställs inga tydliga krav på de datorer som kan ingå i styrenheten, utan i stället hänvisas till [EN954-1]. Punkt 4.15 säger bl.a.

*Pressure sensitive mats and pressure sensitive floors shall meet the requirements of the category for which they are specified, marked and where required certified. These categories are set out in EN 954-1.*

Vidare säger man om provning under punkt 7.17:

*The purpose of this test is to prove that the system meets the claimed category. A fault assessment shall be carried out. This fault assessment shall conform with the stated category given in EN 954-1.*

Det ges alltså ingen direkt vägledning om hur en utvärdering av en eventuell mikrodator och dess programvara ska ske.
3.10 prEN 50100 Safety of machinery:
Electro-sensitive protective equipment

Maskiner kan förses med skyddsanordningar vilka känner av om föremål kommer in i maskinens riskområde. Kraven på skyddsanordningar är höga eftersom konsekvenserna av ett fel är allvarliga. Standarden tas fram i olika delar, men kraven på datorbaserade system förutsätts finnas i den allmänna första delen [EN50100].

För en utrustning i kategori 4 enligt prEN 954-1 säger punkt 4.2.2.3 om feltålighet:

*In the event of a single fault the Type 4 ESPE shall not fail to danger.*

*.... In cases where a single fault is not detected, the occurrence of further faults shall not cause a failure to danger.*

Under punkt 4.2.10 ställs flera krav på programvaran;

*Where devices rely on software for their design or operation, the following requirements shall be met:*

- there shall be an unambiguous software specification written in a language and form clearly understandable to software designers and assessors of the device;

- the software design shall include clear representations of the program's operation, either by means of a formal structural design language, or by means of a suitable graphical diagram i.e. flow chart, structure design etc. such that it can be easily understood;

- where the software design and specification are changed, there shall be a formal procedure for reassessing the conformance to the standard and for recording the change;

- where the safety integrity of the ESPE relies on software, it shall be proven that the possibility of common cause failures between the algorithms of each channel is eliminated;

- the entire ESPE program shall be contained in read only memory which cannot be overwritten by the processor.

*Appropriate software and hardware techniques shall be included for systems to monitor correct programme flow, and to confirm the integrity of the software. Such techniques include a watchdog, RAM/ROM checks, CPU-tests, etc.*

*The watchdog shall be independent of the device/software it is intended to monitor and shall have a safety integrity equivalent to the protective device.*
3.11 SS-EN 60204-1 Maskinsäkerhet -
Maskiners elutrustning -
Del 1: Allmänna fordringar


Under punkt 9.4 behandlas styrfunktioner i händelse av felsfunktion. Speciellt sägs under punkt 9.4.1

*Om felfunktioner eller störningar hos elutrustningen kan medföra fara eller orsaka skada på maskin eller arbetstystecke, skall lämpliga åtgärder vidgas för att minska sannolikheten för att detta skall inträffa. ......*

*... I allmänhet behöver endast enkelfel beaktas. I fall med högre risknivå, kan det vara nödvändigt att säkerställa att ett enkelfel inte kan orsaka fara.*

Den senare skrivningen är otydligt formulerad. En rimlig tolkning är att man för alla styrfunktioner som kan medföra fara ska ta hänsyn till enkelfel. Detta gäller för både låg och hög risknivå.

Punkten 12.3 behandlar också programmerbar utrustning, bl.a. sägs under punkt 12.3.2

*Anordningar skall finnas som hindrar obehöriga personer från att ändra minnesinnehåll.*...

Användningen av programmerbar utrustning i säkerhetsrelaterade funktioner behandlas i punkt 12.3.5:

*Programmerbar elektronikutrustning får inte användas för nödstoppfunktioner enligt kategori 0.*

*För nödstoppfunktioner enligt kategori 1 och alla andra säkerhetsrelaterade stoppfunktioner är elektromekaniska komponenter förbundna med ledningar att föredra (avs. funktionen bör inte vara beroende av programmerbar elektronisk utrustning, se avsnitt 9.2.5.4). När programmerbar elektronisk utrustning används för sådana funktioner skall lämpliga anordningar enligt avsnitt 9.4. användas.*

*Dessa fordringar får inte hindra användning av programmerbar elektronikutrustning för övervakning, provning eller understödande av sådana. Sådan utrustning får dock inte hindra att funktionerna verkar på riktigt sätt.*

**ANM - Det anses för närvarande svårt att med rimlig säkerhetsgrad avgöra om korrekt funktion kan säkerställas hos en enkel kanal i ett programmerbart elektroniskt styrsystem när felfunktion hos styrsystemet kan innebära allvarlig fara. Tills denna fråga kan avgöras, avråds från att läta enbart på den rätta funktionen hos en sådan enkanalgan anordning.**
Det finns alltså i standarden i betydande osäkerhet om i vilken grad man kan förlita sig på programmerbar utrustning. Ämnet har diskuterats och det är sannolikt så att kommande utgåvor kommer att mildra skrivningarna i takt med att tekniken blir ännu mer mogen.

I det senaste förslaget [44/184/CDV] till ändringar i standarden talas i punkt 9.2.7 om "Cable-less control functions". Stoppfunktioner behandlas under punkt 9.2.7.3:

...:
A machine having safety-critical functions and which are equipped with cable-less control shall have a means of automatically and immediately initiating the stopping of the machine and preventing the initiation of potentially hazardous motions, in the following situations:
- when a stop signal is received;
- when a fault is detected in the system;
- when a valid signal has not been detected within a specified period of time.

Ett styrsystem på en maskin med säkerhetskritiska funktioner förutses alltså kunna vara försett med trådlös överföring av signaler. (En radiostyrning av en travers är ett exempel på en sådan tillämpning.) Det är mycket viktigt att maskinen alltid kan stoppa då stoppsignal ges, om styrsystemets automatiska övervakning hittar fel eller om den trådlösa förbindelsen bryts ("timeout").

Punkt 9.2.7.4 [44/184/CDV] säger om datakommunikation:

In a machine where the control of safety critical functions relies on serial data transfer, correct communications shall be ensured by using an error detection method that is able to cope with at least three error bits in any command sequence.

Här förutses man alltså att säkerhetskritisk information kan sändas med seriekommunikation. Det ställs krav på hur överföringen ska kodas för att man ska kunna upptäcka störningar på de skickade meddelanden.
4 Internationella standarder

4.1 Allmänt


Standarderna är frivilliga att tillämpa och har ingen formell koppling till EGs direkter eller de europeiska standarderna. Den som så önskar kan använda standarderna som stöd för de lösningar han väljer i sina konstruktioner.

Det förekommer ofta att internationella standarder antags som Europa-standarder (ibland efter viss omarbete), En sådan standard ingår då i den europeiska standardiseringen och kan kopplas till direktiv. Exempel på detta är standarden IEC 204-1 som i sin europeiska version heter EN 60 204-1.

4.2 SS-ISO 11161 Säkerhet för samverkande tillverkningssystem


Man ger inga detaljerade anvisningar om programmerbara system utan hänvisar till IEC204-1 (i allt väsentligt samma standard som SS-EN 60204-1), avsnitt 9 "Control circuits and control functions". Punkt 5.1 säger allmänt:

"Styrsystemen ska vara konstruerade och tillverkade så att de inte orsakar risk för personskada ....

Den elektriska utrustningen skall vara utförd enligt IEC204-1:1992 och speciellt enligt avsnitt 9."
Under punkt 5.3 sägs

**Styrsystemet skall vara konstruerat, tillverkat och installerat eller unyttjat för att säkerställa att ett komponentfel i systemet inte hindrar att stopp uppnås, men hindrar ny start av eller upprepad arbetscykel till dess felet har blivit åtgärdat.**

Detta krav gäller inte för komponenter vars fel inte kan orsaka risksituationer.

**Vid en felanalys skall följande beaktas:**

- ett fel får inte medföra risksituation;

- ett första fel som inte upptäckts får inte i samband med ett ytterligare fel (andra felet) medföra en risksituation.

**Man utgår ifrån att två av varandra oberoende fel inte skall inträffa samtidigt men konstruktören skall ta hänsyn till samtliga felfunctioner med gemensam orsak.**

Krav ställs alltså bara på de komponenter vilka bedöms som kritiska. För dessa gäller först och främst kravet på täthet mot enkelfel, men också kravet på att två fel tillsammans inte får orsaka en farlig situation. Figur 9 visar hur felbedömningen görs.


Under punkt 5.4.1 talar man också om redundant och diversitet samt hänvisar till IEC 204-1 (dvs. SS-EN 60204).

**Som komplement till kraven enligt 5.3 skall beprövade komponenter och kretsteknik användas (se IEC 204-1:1992, avsnitt 9.4.2.1) tillsammans med en eller flera av följande skyddsmått:**

a) *Delvis eller fullständig redundant, (se IEC 204-1:1992, avsnitt 9.4.2.2).*

..... Skydd mot följderna vid fel på styrkomponenter bör inte baseras enbart på enkel redundant (redundans med lika komponenter).

**Komponentredundans innebör användning av två eller flera styrkomponenter i parallella eller i seriekretsar för att säkerställa tillförlitlig drift. Fel i en av de redundanta komponenterna kan emellertid undgå upptäckt och medföra en skenbar säker funktion. När ytterligare fel därefter uppstår i den redundanta kretsen kan ett osäkert tillstånd uppstå. Övervakning av och reaktion på sådana fel är av väsentlig vikt.***
Figur 9. SS-ISO 11 161 - Felbedömning
Punkt 5.11.1 säger om stoppfunktioner

Stoppfunktioner ska vara överordnade tillhörande startfunktioner. Stoppfunktioner bör väljas i enlighet med riskbedömningen och baseras på nedanstående kategorier.

Det finns tre stoppkategorier enligt följande:

- Kategori 0: stopp genom omedelbar brytning av kraften till maskinens drivanordningar som orsakar risksituationer (dvs ett icke styrt stopp).
- Kategori 1: styrt stopp med kraften tillgänglig till maskinens drivanordningar som orsakar risksituationer för att erhålla stoppet och brytning av kraften när maskinen stannat
- Kategori 2: styrt stopp med bibehållen kraft till maskinens drivanordningar som orsakar risksituationer.

Kategori 0 och 1 skall vara utförda i enlighet med 5.3.

Samma tre stoppkategorier återfinns i SS-EN 60204-1.

Nödstopp behandlas under punkt 5.11.2;

..... När nödstoppfunktionen erhålls genom en elektrisk krets ska den utföras i enlighet med IEC 204-1 ....

Återstart behandlas under bl.a. punkt 5.13

Avbrott och variationer i någon av kraftkällorna skall inte orsaka risksituationer. I annat fall skall omedelbart stopp initieras. Återkomst av energi skall inte orsaka risksituationer eller återstarta systemet.
4.3 IEC 1131 Programmable controllers


4.3.1 IEC1131-2 Equipment requirements and tests


Since programmable controllers are component devices, overall automated system safety including installation and application is beyond the scope of this standard.

Vissa krav på styrsystemets förmåga till självtest och diagnostik ställs ändå under punkt 3.11.2:

1) The following means shall be provided:
   a) a means for monitoring the user's application program (i.e. watchdog timer, etc.);
   b) a hardware or software means to check the memory integrity;
   c) a means to check the validity of the data exchanged between memory(ies), processing unit(s) and I/O modules;
   d) a means to check that internal voltages and currents delivered by the power supply unit(s) do not exceed the limits allowed by the hardware design;
   e) a means to monitor the status of MPU.

I styrsystem ska alltså enligt IEC1131 finnas:
- övervakning av exekveringen av användarprogrammet
- minneskontroll
- kontroll av data skickat mellan olika moduler
- övervakning av matningsspänning
- övervakning av processorn

Punkt 3.11.2 ställer också krav på att det finns en larmutgång:

2) The permanently installed PC-system shall be capable of operating an alarm signal on an alarm output. When the system is monitored as "functioning correctly" this alarm output shall be in a predetermined state; in the other case it shall go to the opposite state. The manufacturer shall specify the conditions of the "correct functioning state" and the self-tests which are executed to drive this alarm output;

Även distribuerade in- och utsignaler (Remote input/output stations, RIOSs) ska uppföra sig på ett väl definierat sätt vid fel:

3) RIOSs shall be capable of operating an alarm signal on an alarm output (for example, through a digital output module) in the event of loss of power or loss of normal communication with the MPU and go to a predetermined state.
Man kan alltså konstatera att även för styrsystem som inte används i kritiska tillämpningar finns krav på självövervakningen och hur den ska skötas.

4.3.2 IEC1131-4 User guidelines


*Overall automated system safety, including installation and application, is beyond the scope of this part of the report.*

Även om man är försiktig med att uttala sig i säkerhetskritiska frågor ger man dock under kapitel 5 allmän vägledning för skydd och säkerhet, men påpekas att dokumentet inte är avsett att täcka alla aspekter då PLC används i säkerhetskritiska styrningar.

En generell varning ges under punkt 5.1.2

*As in any solid-state control system, failure of certain components can result in uncontrolled and/or unpredictable operation. System level failure modes and associated back-ups should be considered. ...*

Det är alltså viktigt att tänka sig i vad som kan hända vid fel. Punkt 5.2.2 tar upp fyra olika sätt på vilka ett PLC kan reagera då en säkerhetsfunktion "lösar ut":

- *alarms of anomalies or malfunctions;*
- *shutting down the system and disconnection of energy source to the controlled process;*
- *forcing the process to a defined standby mode;*
- *shutting down the PC in a safe and predictable manner and providing an acceptable back-up.*

För programvara säger man bl.a. under punkt 5.3.1

*A quality control plan for user software is needed to help assure thorough examination from a safety/protection point of view. Software testing needs to be performed both by the software author(s) and by the PC control system user. Independent testing and evaluation of user’s application software is also recommended.*

Desutom påtalas riskerna vid ändring i programvaran under punkt 5.3.3

*Every modification of user’s application software need a suitable re-evaluation test to help ensure that safety/protection is not compromised, defeated or bypassed. The user should keep change records of each modification.*

*Critical application program software may be unalterable on the plant floor by storing that portion of the program on read only memory or by making the portion unalterable by utilizing the PC manufacturer’s lockout abilities, if provided.*
En speciell funktion som många PLC har är att kunna tvinga ingångar eller utgångar till ett värde (till/från). Funktionen används vid idrifttagning och underhåll. Punkt 5.4.2 påtalar riskerna med att sådan "mjukvarumässig bygling" finns

Care must be taken to insure that:
- forcing operations do not impair safety/protection, which must be adequately guarded by use of PC-independent safety/protective interlocks;
- forced inputs and outputs are to be returned to normal status upon completion of testing.

Under punkt 5.5 konstateras att säkerhet och skydd baseras på noggrann planering. I detta sammanhang nämner man speciellt

...care needs to be taken to help guard against unintended movement of machine parts or unintentional contact with electrically live parts.
4.4 Draft IEC 1508 Functional safety; Safety-related systems


Standarden avser att täcka alla typer av säkerhetskritisiska styrsystem, vilket gör att all text är ganska generellt skriven. IEC1508 är tänkt att användas vid utveckling av nya standarder för speciella tillämpningsområden.

Standarden består av följande delar.

1 Allmänna krav [65A/179/CDV]

2 Krav för elektriska/elektroniska/programmerbara elektroniska system [65A/180/CDV]

3 Krav på programvara [65A/181/CDV]

4 Definitioner och förkortningar [65A/182/CDV]

5 Riktlinjer för tillämpning av del 1 [65A/183/CDV]

6 Riktlinjer för tillämpning av del 2 [65A/184/CDV]

7 Bibliografi över teknik och metoder [65A/185/CDV]

De första tre delarna utgörs av krav. Resten av standarden kan ses som hjälpmodell för att tolka del 1 till 3.

Del ett beskriver huvudsakligen "Safety Lifecycle" som är ett mycket centralt begrepp i hela standarden. Det innefattar alla aktiviteter under realiserandet av ett säkerhetskritisikt system fram tills det tas ur drift. (Se figur 10.)

Dokumentationen är en central del i standarden. Förr varje fas i livscykeln beskrivs bland annat vilka dokument som krävs och vad de skall innehålla.

Intressant att notera är att standarden under "Overall Safety Requirements" kvantifierar kraven på feltäthet beroende på "Safety Integrity Level" (se tabell i figur 11). Olika metoder att komma fram till lämplig "Safety Integrity Level" finns beskrivna i del 5 (riktlinjer för tillämpning av del 1). Observera att det inte finns någon koppling mellan siffrorna i tabellen och de riskkategorier B,1,2,3,4 som finns beskrivna i prEN 954.
Figur 10. Overall Safety Lifecycle

TABLE 2: SAFETY INTEGRITY LEVELS: TARGET FAILURE MEASURES

<table>
<thead>
<tr>
<th>SAFETY INTEGRITY LEVEL</th>
<th>DEMAND MODE OF OPERATION (probability of failure to perform its design function on demand)</th>
<th>CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Probability of a dangerous failure per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-5} ) to (&lt; 10^{-4} )</td>
<td>( \geq 10^{-5} ) to (&lt; 10^{-4} )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-4} ) to (&lt; 10^{-3} )</td>
<td>( \geq 10^{-4} ) to (&lt; 10^{-3} )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-3} ) to (&lt; 10^{-2} )</td>
<td>( \geq 10^{-3} ) to (&lt; 10^{-2} )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-2} ) to (&lt; 10^{-1} )</td>
<td>( \geq 10^{-2} ) to (&lt; 10^{-1} )</td>
</tr>
</tbody>
</table>

Figur 11. Tabell över Safety Integrity Levels (SIL)

Del 4 innehåller en beskrivning av de definitioner och förkortningar som används i standarden.

Del 5, riktlinjer för tillämpning av del 1, innehåller dels beskrivning av olika metoder att fastställa kraven på "Safety Integrity Level", dels precisering av dokumentationskrav.

Del 6, riktlinjer för tillämpning av del 2 och 3, ger förslag på hur man kan uppnå en önskad "Safety Integrity Level". Sex olika typ-arkitekturer presenteras och det görs en gradering av effektiviteten för ett antal olika säkerhets höjande metoder. Del 6 innehåller också ett antal konkreta mer eller mindre starka rekommendationer på användning av olika metoder vid programutvecklingen.

Del 7 innehåller en sammanställning och beskrivning av ett antal säkerhets höjande metoder. Dessa kan indelas i följande tre delar:

1. Metoder för att öka säkerheten i programvara
2. Metoder för att detektera och tolerera hårdsvarfel
3. Metoder för att undvika systematiska hårdsvarfel
5 Utvärderingsmetod

5.1 Projektets mål

Projektets mål är att utveckla praktiskt tillämpbara krav och verifieringsmetoder för säkerhet i datorbaserade maskinstyrningar där risk för personskada finns.

Denna rapport beskriver förprojektets resultat. Avsikten har varit att sammanställa existerande riktlinjer, kontakta industri, göra fallstudier samt bestämma inriktning på huvudprojektet. Huvudprojektets egentliga uppgift är sedan att ta fram krav och verifieringsmetoder.

Den övergripande frågan för en metod att utvärdera maskinstyrningar blir; "Är säkerheten i min maskinstyrning tillräcklig?". Frågan kan ställas många gånger under en maskins livscykel;

- vid specifikation av nya produkter.
- under konstruktionsarbetet.
- vid utvärdering hos oberoende tredje part.
- vid idrifttagning.
- vid reparation och underhåll.
- vid ombyggnad.
- vid utredning av olyckstillbud.

Vår ambition är att utvärderingsmetoden ska kunna vara till nytta i alla dessa situationer. Kanske kan inte hela utvärderingsmetoden utnyttjas vid alla steg i livscyklens, men i alla fall någon del av den ska kunna utnyttjas i samtliga situationer.

5.2 Avgränsningar

Begreppet maskinstyrning är alldeles för stort för att en lösning som täcker alla maskiner och alla aspekter på styrning ska kunna tas fram. Vi måste därför avgränsa oss i detta projektarbete.

Maskindirektivets bilaga 1 räknar upp de risker man måste ta hänsyn till. Utvärderingsmetoden förutsättes främst täcka följande avsnitt;

1.2.1 Styrsystems säkerhet och tillförlitlighet
1.2.3 Start
1.2.4 Stopp
1.2.5 Val av styrsätt
1.2.6 Fel i kraftförsörjningen
1.2.7 Fel i styrkretsen
1.4 Skydd och skyddsanordningar

De övriga riskerna beskrivna i maskindirektivet, t.ex. buller eller strålning, är inte avsedda att täckas av metoden. Inte heller direkta utvärderingar av skyddsanordningar som t.ex. ljustridare och trampmattor ska täckas. För skyddsanordningar finns särskilda standarder. [EN1760] [EN50100]
Utvärderingsmetoden utvecklas för system med säkert läge (dvs. risken upphör då energitillförseln tas bort). System där säkerheten kräver hög tillgänglighet (dvs. avstängning medför risk) täcks inte av denna metod.

Verifieringsmetoder för risker p.g.a. elektrisk matning ingår inte i denna rapport. Utvärdering av elssäkerhet är ett väl etablerat område där många standarder och föreskrifter finns framtagna.

Olika typer av miljöpåkänningar täcks inte heller av denna rapport. Provningsmetoder för miljöpåverkan som t.ex. temperatur, fukt, vibration och elektromagnetisk strålning är etablerade.

5.3 Förslag till utvärderingsmetod

Innan säkerheten kan utvärderas måste riskerna förstå ha analyserats. Riskanalysen ligger utanför den utvärderingsmetod som skissas i denna rapport. Den ger svaret på vilka acceptabla funktioner som inte får förekomma i maskinen. Detta förutsätts vara givna "indata" till metoden.

För att kunna genomföra en utvärdering måste man först gå igenom maskinen för att identifiera och avgränsa, förstå funktionen samt förstå principerna enligt vilka säkerheten är uppbyggd. Frågorna som ska besvaras är
- Vad ska utvärderas?
- Vad gör maskinstyрningen?
- Hur byggs säkerheten upp?

Det första steget i utvärderingen blir sedan att undersöka om erforderliga säkerhets-relaterade funktioner finns. Varje maskin berörs av krav från direktiv och standarder, dvs.
- Uppfylls maskindirektivets krav?
- Har man använt de funktioner standarden föreslår?

För att tillverkaren uppgår att en funktion finns behöver det inte innebära att den är korrekt införd i maskinen. Genom att göra funktionsprov, analysera och prova hårdvara samt analysera och prova programvara besvaras frågan
- Är implementeringen korrekt?

Beroende på tillämpning kommer olika krav att ställas på feltätheten. Felsimulering, analys av redundans, analys och prov av hårdvara samt analys och prov av programvara besvarar frågan
- Är konstruktionen tillräckligt feltälig?
Metoden kommer att innehålla en "verktygslåda" bestående av olika verifieringsmetoder vilka kan användas för olika typer av styrsystem. Vilka metoder som väljs beror på hur säkerheten realiserats. (Se figur 13.) En maskinstyrning där de säkerhetsrelaterade funktionerna är helt beroende av programmerbar logik kräver en omfattande utvärdering. Däremot kan maskinstyrningar där säkerheten baseras på elektromekaniska komponenter utvärderas med metoder som redan i dag är kända.

Kraven på feltäthet styr också vilka verifieringsmetoder som utnyttjas. Utvärderingen av en maskinstyrning i kategori 4 [prEN954] blir mer omfattande än i kategori 3, 2, 1 eller B eftersom kraven på feltäthet är högre.

<table>
<thead>
<tr>
<th>Säkerheten baserad på</th>
<th>endast hårdvara</th>
<th>hårdvara och programmerbar elektronik</th>
<th>endast programmerbar elektronik</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifieringsmetod A</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod B</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod C</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Verifieringsmetod D</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod E</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod F</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod G</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod H</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod I</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verifieringsmetod J</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>......</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figur 12. Frågeställningar

Figur 13. Princip för olika verifieringsmetoder för olika system
5.4 Fortsatt arbete

5.4.1 Tekniskt innehåll

Arbetet kommer att fortsätta byggt på innehållet i denna rapport. Tyngdpunkten i utvärderingsmetoden läggs på maskinstyrningens logikdel ("datorn").

Genom att utgå från maskindirektivets krav och de olika standardernas förslag på åtgärder bildar vi oss en god bild av vilka skyddsfunktioner som krävs av maskinstyningen. Utgångspunkten ska alltid tas i skyddsfunktioner och oacceptabla funktioner för den speciella maskinstyningen. Ett exempel på ett praktiskt resultat av denna del av arbetet är en checklista på programvara i säkerhetskritiska tillämpningar.

Resultatet av arbetet ska också i detalj anvisa hur man kan utvärdera maskinstyrningens funktion. För att kunna göra detta måste detaljerad teknisk information finnas tillgänglig.

Den del av arbetet som behandlar de erforderliga skyddsfunctionerna baseras både på direktiv och standarder samt på kunskaper om hur ett styrsystem är uppbyggt. Arbetet med utvärderingen av styrsystemet kräver ingående kunskaper om en mikrodators funktion. Metoderna för utvärdering av styrsystemets säkerhet kommer att rikta sig till tekniska specialister. Huvuddelen av arbetet ligger i att utveckla dessa metoder till något tillförlitligt och användbart.

5.4.2 Projektstyrning


Arbetet inom den europeiska standardiseringen måste även i fortsättningen följas, speciellt vad gäller utvärdering av styrsystem [EN954].

Den färdiga utvärderingsmetoden publiceras som SP-rapport och presenteras vid ett seminarium under andra eller tredje kvartalet 1997.
Appendix A. Fallstudier

Under kontakternas med olika företag har speciellt 5 olika fall studerats. Avsikten är att genom exempel ge en bättre förståelse för hur de maskiner och styrningar ser ut där det finns behov att verifiera säkerheten. Beskrivningarna är inte avsedda att vara fullständiga, utan lyfter fram olika principer av intresse.

Fallstudie A1 visar en förpackningsmaskin där säkerheten huvudsakligen byggs på konventionellt sätt med relä utanför den programmerbara elektroniken. Fallstudie A2 och A3 ger exempel på maskiner där man i av olika orsaker ansett sig behöva lägga säkerheten i en dator. Fallstudie A4 och A5 ger exempel på programmerbara styrsystem där särskilda åtgärder vidtagits med avsikt att höja säkerheten.

IVF och SP har i dessa fallstudier inte gjort några bedömningar av säkerheten. Maskinstyrningarna redovisas så som de presenterats av tillverkarna.

A.1 Förpackningsmaskin


Maskinen är vid normal drift helt automatiskt. Operatören behöver bara flytta de färdiga förpackningarna till en kartong. För att ladda maskinen med plastfolie eller för att åtgärda driftstörningar behövs manuella ingrepp. Vid detta arbete finns det risk att operatören kan skadas av verktyget som klämmar ihop "plastpåsen" i ändarna och utför svetsningen. Kombinationen av hög temperatur (ca 300 °C under ca 0,2 s då backarna slutar) och mättlig kraft (ca 70 N) medför risk för skador på händerna. Skadorna torde dock i de flesta fall vara lättbara. Svetsen i längsled utförs på ett sådant sätt att operatören knappast riskerar att komma i kontakt med detta plastsvetsverktyg.

Maskinen styrs av ett programmerbart styrsystem (PLC) för allmänt bruk. I själva PLC finns alltså inga speciella åtgärder för att öka säkerheten. Konstruktionen utgår också från att fel kan upptäckas i PLC. Kanske kan det använda flera fungera, eller det kan finnas fel i programvaran.

Säkerheten byggs på att
- Riskområdet med det farliga verktyget byggs in under en huv.
- Huvet är försett med en tvångsbrytande givare, och utgör alltså ett förreglande skydd.
- Två reläer används som ett speciellt säkerhetssystem för nödstopp, återställning och eventuell ytterligare grindbrytare.
- Funktionen hos reläerna i säkerhetssystemet övervakas av PLC.
Figur A.1.1. Princip för huvbrytare som kan stoppa den farliga rörelsen.

Figur A.1.2. Princip för säkerhetssystem övervakat via PLC.

Den farliga maskinrörelsen försöker man alltså bygga in under en huv. Eftersom detailjer måste kunna passera in under huvon finns det dock möjlighet att sträcka handen under huvon in i riskområdet. Sveksverktyget är därför försett med en fjäderbelastad platta och två givare vilka ska känna om t.ex. en hand eller ett finger kommer i kläm. Signalen från dessa givare går till PLCet som då bryter rörelsen.
Om huvun öppnas påverkas en 2-polin tvångsbrytande givare. Den ena polen bryter direkt bort matningsspanningen till den pneumatikventilen som styr den färliga maskinrörelsen. Den andra polen går till PLCet som en informationssignal. PLC bryter också bort utgången.

Nödstoppsbrytarna är kopplade till ett relä (K1A) vilket bryter bort 24V-matningen till PLC-systemets utgångar. Återställning sker sedan med en speciell tryckknapp vilken också känns av med PLC. När PLC känner återställningssignalen drar PLC ett relä (K2A) vilket medverkar till att huvudreläet (K1A) aktiveras och PLC spänningssätts igen. PLC övervakar också att de båda reläerna aktiveras och deaktiveras inom rimlig tid (0,2 s). Om båda reläerna inte drägit inom utsatt tid stänger PLC maskinen.

Styrsystemet måste fungera korrekt för att återställning ska ske samt för att övervakning av samtidigheten i reläerna ska fungera. Övervakningen av om svetsverktyget felaktigt greppar t.ex. ett finger är också PLC-beroende. Nödstopp och tvångsbrytande givare är däremot inte beroende av den programmerbara logiken.

![Diagram](image)

Figur A.1.3. Princip för säkerhetssystem övervakat via PLC.
A.2 Offsetpress

A.2.1 Teknisk beskrivning


![Diagram](image)

**Figur A.2.1 Offsetpress**

- **F** - Falsapparat
- **T** - Tryckverk
- **M** - Motor
- **VK** - Vertikalkoppling
- **HK** - Horisontalkoppling

Styrsystemet är baserat på distribuerade funktioner och centraliserad styrning. Modulerna är sammankopplade med en databuss. Följande delar ingår i systemet:

**Processmoduler**

Operatörsmoduler


Vid varje inmatning av kommandon från tangentbordet kontrollerar operatörsmodulen att den senaste tangentyckningen är en logisk följd av de tidigare. Av säkerhetsskäl består alla kritiska kommandon av flera olika tangentyckningar.

Systemmodul

Systemmodulen tar emot kommandon från operatörsmodulen för till exempel bildväxling och ändring av driftparametrar. Via systemmodulen kan också all konfigurering i hela systemet ändras. Den sköter också övervakning av databussen genom att med jämna mellanrum göra testanrop till de olika modulerna. Modulen utför också kontinuerligt självdiagnos genom vilken hårdvarans funktion kontrolleras. Vid ett allvarligt fel tas systemmodulens uppgifter över av rapportmodulen.

Rapportmodulen


Systembussen


A.2.2 Säkerhetssystemet

A.2.2.1 Funktion


Stegning (eller ryckkörning) innebär att pressen roterar så länge stegningsknappen är aktiverad. Hastigheten är begränsad till 6 m/min.

Krypning innebär att pressen går kontinuerligt med hastigheten begränsad till 6 m/min.

För tryckverken gäller följande:

Om förgärvoksskyddet är stängt tillåts alla körkommandon.
Om förgärvoksskyddet är öppet så tillåts körkommandot stegning från kontrollpanelen intill men inte från något annat ställe.
Om mer än ett förgärvoksskydd är öppet skall pressen säkerhetsstoppas.
Om förgärvoksskyddet öppnas medan pressen roterar säkerhetsstoppas pressen.
Säkerhetsstopp innebär att pressen stannar så fort som möjligt utan att maskinen skadas eller pappersbanorna brister. Normalt tar detta mellan ca 8 och 18 s.


Nödstoppet bryter spänningsmatningen till hela pressen. I detta fall stannar pressen okontrollerat och endast de mekaniska bromsarna stannar den. Nödstoppet är enbart tänkt att användas i farliga situationer.

A.2.2.2 Uppbyggnad

Personsäkerheten i systemet är baserad på processmodulerna och hårdvara uppyggt kring dem. Det så kallade säkerhetsstoppet är uppyggt delvis med hjälp av hårdvara. Reläer för stopptyckknappar (HW-stopprelä), ett relä som styrs av programmet i processmodulens PLC (SW-stopprelä) och ett watch-dog relä kan bryta bort den spänning på 24 V som används för att aktivera motordriften (se bild A.2.2).

Den kontaktor som bryter energin till motorn (K2, se bild A.2.3) styrs dock inte direkt via denna slinga. Slingan strömförsörjer tre reläer K6, K7 och K8. En kontakt från K6 kopplas till motordrifens PLC. PLCa styr sedan huvudkontaktorn K1 via en hjälpkontaktor K2. Sultande och brytande kontakter från K7 och K8 kopplas i serie till motorstyrningens elektronik.
Figur A.2.2  Säkerhetssystemets elektromekaniska del

Figur A.2.3  Motorstyrning i en processmodul
De reläer som styrs av kontakter i horisontal- och vertikalkopplingarna (se bild A.2.1 och A.2.2) gör att säkerhetsstoppet enbart påverkar de maskiner som ingår i den mekaniskt kopplade pressen. Reläernas kontakter liksom kontakterna i kopplingarna övervakas av processmodulens PLC. Uppstår ett motsatsförhållande stängs utgången som styr det så kallade SW-reläet av.

Kontakter från både HW-stoppreläet och SW-stoppreläet läses av PLC:n. Om återkopplad data inte stämmer med reläernas börvärden ges felmeddelande och utgången som styr SW-reläet stängs av.

Stopptryckknapparna är kopplade till HW-stoppreläet som ingår i slingan för säkerhetsstopp. De läses också av PLC:n som bryter spänningen till SW-reläet om stopptryckknappen är påverkad.

När ett färgverksskydd öppnas under drift eller när flera skydd samtidigt är öppna bryter PLC:n säkerhetsstoppkretsen via SW-reläet. Observera att samtliga brytare för färgverksskydden enbart är kopplade till PLC:n och att regler som beskriver samband mellan status på skydd och olika drifttyper realiserats i mjukvara. Ett exempel på en sådan regel är "Om färgverksskyddet är öppet så tillåts körkommandot stegning från kontrollpanelen intill men inte från något annat ställe". För att minska risken för att PLC:n inte upptäcker ett öppet skydd på grund av hårdvarufel innehåller kabeln från brytaren dubbla ledare som är kopplade till varsin ingångskanal. Om data från dessa kanaler inte överensstämmer med varandra stoppas pressen.
A.3 Verktøyssmaskin med operatörspanel

En verktøyssmaskin används för att bearbeta detaljer med höga krav på toleranser. Driften är automatisk, dvs. ämnena och färdiga detaljer matas automatiskt in i och ut från maskinen. Operatören fyller på och tömmer magasin utan att komma in i maskinens riskområde. Vid verktøyssbyte och röjning måste man däremot arbeta manuellt i riskområdet för maskinens rörliga delar. Det är vanligt att operatören vid manuell drift arbetar med ena handen i maskinens riskområde samtidigt som han har andra handen på manöverknapparna. Konstruktionen ska se till att inte persontor i operatörns uppträdan p.g.a. tekniska fel.


![Diagram](image-url)

Figur A.3.1 Principen för det reläbaserte säkerhetssystemet.

Antalet manöverknappar skulle bli för stort om en stor verktygsmaskin konstruerades med en knapp för varje rörelse. Därför används en operatörsbildskärm där menyer definierar knapparnas betydelse. Bildskärmen börjar med att visa en huvudmeny där val av maskinens olika delsystem kan göras. (Se figur A.3.2.) När sedan ett delsystem väljs (knapp SB1 trycks in i exemplet i figur A.3.2) förändras knapparnas betydelse och operatörsbildskärmen visar tryckknapparnas betydelse för just den maskindel som valts. (Se figur A.3.3.)

**Figur A.3.2** Operatörsbildskärm, exempel på huvudmeny

**Figur A.3.3** Operatörsbildskärm, exempel på undermeny
Eftersom samma tryckknapp kan ha olika betydelse på olika menyer, ska den också påverka olika ställdon. Styrsystemet måste hålla reda på vilken meny som är aktiv för att styra rätt grupp ställdon. För att en tryckknapp inte ska påverka fel relä finns s.k. gruppvalsrelä. Ett gruppvalsrelä aktiveras från styrsystemet och gör att reläerna som hör till just denna meny kan aktiveras. I figur A.3.4 är reläet med dioderna D8 och D9 gruppvalsrelä.

Figur A.3.4 Principen för det reläbaserade säkerhetssystemet med gruppvalsrelä.

De använda reläerna är tvångförda säkerhetsreläer och inkopplade på ett sådant sätt att ett eventuellt svetsat relä upptäcks.

Det är mycket viktigt att menyn på operatörsbildskärmen visar korrekt betydelse för varje knapp i varje ögonblick. Annars kommer rörelser att utföras som inte operatören förväntar sig. En oväntad rörelse framåt istället för bakåt kan komma att skada operatören.

Säkerheten i operatörsbildskärmen är helt beroende av programvara. Till motsats till de manuella tryckknapparna finns ingen enkel metod att dubblica funktionen i hårdvara. Man måste vidtaga åtgärder i styrsystemet för att öka säkerheten.

Operatörsbildskärmen sköts av en egen processor, och den egentliga maskinstyrningen sköts av huvudprocessorn. Mellan de båda processorn skickas information om operatörsbildskärmen på en kommunikationsbuss. (Se bild A.3.5.)


Om ett fel skulle göra att styrsystemet missuppfattar vilken knapp som påverkats kommer ändå utsignalen att stoppas av säkerhetssystemet. Även om styrsystemet aktiverar en utgång så är inte rätt säkerhetsrelä aktiverat och signalen blockeras. Den största risken ligger i stället i att fel text visas på bildskärmen så att operatören vilseleds att beordra en annan rörelse än vad han i verkligheten gör.

För att minska risken för att fel text visas beräknas en kontrollsumma på de texter som finns på operatörsbildskärmen. Varje gång nya texter ska visas på bildskärmen beräknas en kontrollsumma för de texter som skickas till skärmen. Denna skickas sedan tillbaka till huvudprocessorn och jämförs med det "facit" som finns lagrat där. Om kontrollsummorna inte stämmer överens är det ett fel på bildskärmen och maskinen stannar.

Operatörsbildskärmen kan inte direkt "läsa" innehållet på bildskärmen utan måste istället beräkna kontrollsumman i den del av programvaran som ligger så nära hårddrevan (dvs. minnet) där texterna lagras. Det är teoretiskt möjligt att ett hårddrevfel kan uppkomma och förvanskas delar av bildskärmens innehåll. Ett sådant fel förväntas dock framträdå så tydligt för operatören ("mörk skärm", "tappade bokstäver", "sned bild" etc.) att det inte ska leda till missuppfattningar av knapparnas betydelse.
Figur A.3.6 Kontrollsummering vid växling av texter
A.4 PLC for safety critical applications - Pilz PSS 3000

A.4.1 Introduction

The German company Pilz GmbH & Co. has developed a programmable logic controller (PLC) intended to be used in safety critical applications. This control system is expected to be used in category 4 applications [EN954-1] such as mechanical presses, hydraulic presses and injection moulding machines. Also other critical applications such as lifts, mines and printing machines are mentioned as possible areas of use.

The control system is available in two models; PSS 3000 and PSS 3056. PSS 3000 is designed in an 19" frame with possible expansion up to 768 inputs and outputs. PSS 3056 is a smaller system with 32 inputs and 24 outputs. This report mainly deals with the PSS 3000.

The application software is written by the user and transferred to the PLC. Since the application software is written as a single source code, possible software faults may affect the operation of the system. Pilz recommends all safety critical software to be assessed by an independant third party before using. There exists a German approval of software for control of excenter presses.

A.4.2 System design

The control system is divided into two sections; the safety section (fail-safe) and the standard section. The two sections are claimed to be independant, i.e. possible failures of the non-safety critical functions of the standard section will not affect the safety critical functions of the fail safe section. Vice versa, if the safety section fails, the standard section will not be affected. Error codes generated by the safety section will be output by the standard section to a data logger via its serial interface. This summary will mainly address the safety section of the PLC.

The safety section is designed as a three channel system. (See figure A4.1.) All three channels will have to produce the same result if the outputs shall be energized. This is called operation according to the three-of-three principle. As soon as one of the channels differs from the other two, the outputs will be de-energized and a safe state will be entered.

The three channels are claimed to be diverse, i.e. designed in three different ways regarding both hardware and software. Three different microprocessors execute the code of the three channels. Three diverse designs are chosen to reduce the risk of design faults affecting the safety. It is considered unlikely that the same design fault should be present in all three channels.
Figure A4.1 Simplified representation of the safety critical control parts

It must be stressed that the original source code is used in all three channels, even if the translation into assembler language is different for the three different processors. Caution must be taken to avoid faults in the source code.

The standard section of the control system is based on a one-channel design which is not claimed to be fault-tolerant. It is claimed that failures in the standard section will not propagate into the fail safe part of the PLC. This is achieved by using separate peripheral busses, different application software, different variable space, checking of timing etc.

Execution of the application software is made by all three processors, but one of them also executes the non safety critical software. This fact stresses the need for measures to stop failures from propagating from the standard section into the fail safe section of the PLC. Different execution speed of the three processors will lead to the need of synchronisation before output and input of signals. (See figure A4.2.)
Processor A

<table>
<thead>
<tr>
<th>Input</th>
<th>Fail-Safe Section</th>
<th>Input (standard)</th>
<th>Standard Section</th>
<th>S</th>
<th>Output</th>
<th>System</th>
<th>S</th>
</tr>
</thead>
</table>

Processor B

<table>
<thead>
<tr>
<th>Input</th>
<th>Fail-Safe Section</th>
<th>S</th>
<th>Output</th>
<th>System</th>
<th>S</th>
</tr>
</thead>
</table>

Processor C

<table>
<thead>
<tr>
<th>Input</th>
<th>Fail-Safe Section</th>
<th>S</th>
<th>Output</th>
<th>System</th>
<th>S</th>
</tr>
</thead>
</table>

1 PLC cycle

\[ S = \text{Synchronisation between processors} \]

Figure A4.2  Execution of one cycle in the PLC

### A.4.3 Self test

The use of self tests is very important to be able to detect faults in one of the channels. The outputs will be de-energized as soon as a fault is detected. However, faults will not be detected instantaneously. It will take the self test some time to detect the fault. During this time the system will host an undetected fault. There is a risk of system failure, should further faults manifest themselves. The self test cycle must be kept short to minimize this risk.

For a two-of-two system, two faults may be enough to cause a system failure. The self test cycle time must be short compared to the mean time between faults. (See figure A4.3.)

The requirements for self test cycle time are lower for the three-of-three system. Three faults are needed to cause a system failure. The self test will not have to find the first two faults before a third fault has occurred. (See figure A4.4.) This reduces the work load of the processor compared to the cycle time required for two-of-two systems.
Self tests are carried out both at power-up and at run time. An extensive 30 second test is carried out at power-up, but such a large test task is not possible during run time. The test task is divided in several time slices, of which one or more are executed every PLC cycle. This will increase the cycle time by typically 3 ms.
A.4.4 Digital inputs and outputs

There are different kinds of fault detection mechanisms for the digital inputs and outputs of the Pilz PLC. The basic input circuit is based on a one-channel optocoupler. The output of the optocoupler is fed to the three channels on the safety section. (See figure A.4.5)

![Digital input diagram]

Figure A.4.5 Digital input

The one-channel digital input is not fail-safe. A single fault in the optocoupler or in the terminals for connections will affect all three channels. To avoid this, two-pole sensors can be used and connected to dual inputs. Another solution provided by Pilz is to feed the sensor from an output of the control system. Dynamic checking is achieved by sending pulses from an output, through the sensor, to the input.

There are different kinds of outputs in the PSS 3000; DO and DOZ. The DO digital output is not fail-safe. A single signal controls the output. (See figure A.4.6.) The status of the output can then be fed back into the controller. A single fault may lock the output to constant ON or OFF, but the feedback will let the fault to be detected. This corresponds to category 2 according to prEN954-1.

![Digital output, type DO diagram]

Figure A.4.6 Digital output, type DO

The DOZ digital output is claimed not to be locked to ON or OFF by a single fault. There are two control signals which both have to be active for the output to go ON. Both outputs can be monitored by feedback signals. (See figure A.4.7.)
Feedback from the final control elements (valves, motor drives etc.) are important for all types of outputs. Fault tolerance in the PLC output will not be effective against faults in the control element itself.
A.5 PLC för säkerhetstillämpningar - SIEMENS S5-95F

A.5.1 Inledning


S5-95F har säkerhetsgranskats av Berufsgenossenschaftlichen Institut für Arbeitssicherheit (BIA) i Tyskland som har utfärdat ett certifikat på att konstruktionen uppfyller kraven för användning i tillämpningar med riskkategori 4 enligt prEN954-1. PLCn har i sitt grundutöverande:

- 16 felsäkra digitala ingångar
- 4 felsäkra interruptingångar
- 2 felsäkra räkningsgångar
- 8 felsäkra digitala utgångar
- 8 icke felsäkra digitala utgångar

Programmering görs i programspråket STEP 5 med möjlighet att välja bland tre olika typer av representation:

- Statement List (STL)
- Control System Flowchart (CSF)
- Ladder Diagram (LAD)

All programmering görs som om systemet vore icke-redundant. Det innebär till exempel att även om en in- eller utgång är dubblerad fysiskt så betraktas den i programmet som enkel.
A.5.2 Systemuppbyggnad

För att motverka inverkan av stokastiska fel består S5-95F av två delsystem (se bild 1). Dessa är identiska (homogen redundans) och kan kommunicera med varandra via en fiberoptisk länk. Kommunikationen används bland annat för att synkronisera delsystemens program och för jämförelse av redundant data.

![Diagram](image)

Figur A.5.1 Systemuppbyggnad

PLC:n innehåller dels systemprogram som medföljer systemet och inte kan ändras av användaren, dels användarens egna program. Systemprogramvaran sköter till exempel hantering av in- och utgångar, alla tester som krävs för att bibehålla säkerheten vid stokastiska fel och exekveringen av användarens program. Ur programmeringsynpunkt är systemet att betrakta som ickeredundant.

S5-95F arbetar cykliskt. I början av varje cykel läser systemprogrammet i de båda delsystemen in aktuell status från respektive ingångar och lagrar informationen i en speciell minnesarea. Därefter synkroniseras systemen och minnesareorna kopieras via optokabeln till det andra delsystemet där de jämförs med varandra. Om någon avvikelse föreligger vidtas felhantering som varierar något beroende på typ av ingång. Om minnesareorna innehåller identisk information startas exekvering av användarprogrammet.

Denna exekvering görs med indata från den tidigare inlästa minnesarean. De förändringar av utdata som uppkommer vid programexekveringen påverkar inte några fysiska utgångar direkt utan placeras i en minnesarea. När exekveringen av användarprogrammet är avslutad sker en ny synkronisering och minnesareorna med utdata kopieras via optokabeln till det andra systemet där de jämförs med varandra. Vid överensstämmelse styrs utgångarna av data i minnesareorna. Om en olikhet detekteras kommer berörda utgångar att stängas av. Detta gör att enkelfel som i ett motsvarande enkanaligt system skulle resultera i en färlig händelse här leder till att en definierad grupp av maskiner stängs av.

Det är inte alla fel som ger sig till känna genom olikheter i in- eller utdata. Ett fel kan ligga dolt i ett av delsystemen som senare, i kombination med ett fel i det andra
delsystemet, kan leda till en farlig händelse. Därför görs kontinuerligt omfattande självtester av båda delsystemen. Dessa självtester består av följande delar:

- Processortest (instruktions- och registertest)
- RAM-test
- EPROM-test
- Programbearbetningsövervakning
- Perreferitest

S5-95F exekverar endast en liten del av självtesten vid varje bearbetningscykel. Genom att på detta sätt dela upp testförloppet på ett antal cyklar kan cykeltiden hållas inom rimliga gränser och alla cyklar bli lika långa. Allvarliga fel som upptäcks av självtesten leder till passivisering av hela systemet medan mindre allvarliga kan göra att endast den signalgrupp som berörs stängs av. Att löpa igenom hela självtesten tar något mindre än en timma.

Läsning av en redundant ingång ger i de flesta fall identiskt resultat för de två delsystemen. I vissa fall kan dock en olikhet uppstå. Skäl till detta kan vara följande:

- Hårdvarufel såsom fel på en givare eller ingångsmodul
- Tidskillnad mellan läsningarna för de två delsystemen
- Olika omflagstider för en tvåkanalig givare

För att skilja mellan hårdvarufel och temporära skillnader har man i S5-95F möjlighet att specificera en maxtid under vilken en skillnad i de två delsystemens insignaler accepteras. Denna så kallade diskrepanstid går att specificera för varje enskild givaringång.
A.5.3 In- och utgångar

Alla felsäkra in- och utgångar har inbyggd hårdvara som används för att kontrollera dess funktion. Till varje ingång är kopplat en testutgång (se bild 2). Oberoende av inkommande signal kan testutgången förändra signalnivån på ingången. Denna test görs automatiskt av systemprogramvaran en gång per timma.

![Diagram](image1)

Figur A.5.2 Ingångstest

Även om ingången är felfri kan till exempel kortslutning i en kabel göra att sensorns signal ersätts med konstant matningsspänning. Användarprogrammet tolkar då sensorn som logisk etta oavsett dess verkliga status. För att minska risken för denna typ av fel kan sensorn matas via speciella utgångar. Vid genomloppning av systemtesten sänks dessa och motsvarande ingång kontrolleras. Om ingången då är hög föreligger ett fel.

Alla felsäkra utgångar har en separat kontrollingång. Via denna kontrollerar systemprogramvaran att utgångens verkliga status stämmer överens med den beordrade.

![Diagram](image2)

Figur A.5.3 Utgångstest
Appendix B  Funktioner beskrivna i standarder

De olika standarderna som beskrivs i denna rapport tar upp olika funktioner hos maskinstyrningarna. Flera av funktionerna finns upptagna i flera olika standader. Det kan vara svårt att finna alla standarder som berör en viss funktion.

I standardförslaget prEN 954 [prEN954] finns en tabell som ger korsreferens mellan funktioner och standarder. Genom att utnyttja denna tabell samt lägga till viss information får man följande korsreferens:

<table>
<thead>
<tr>
<th>Funktion</th>
<th>Standard</th>
<th>EN 292-2</th>
<th>EN 418</th>
<th>EN 574</th>
<th>EN 775</th>
<th>EN 954-1</th>
<th>EN 1037</th>
<th>EN 50100-1</th>
<th>EN 60204-1</th>
<th>ISO 11161</th>
<th>IEC 1131</th>
<th>Draft IEC 1508</th>
</tr>
</thead>
<tbody>
<tr>
<td>Konstruktionsprinciper</td>
<td></td>
<td>3.7</td>
<td>4.1</td>
<td>4.2</td>
<td>9.4</td>
<td>5.1</td>
<td>Del 7</td>
<td>Del 1-7</td>
<td>Del 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programmerbara system, allmänt</td>
<td></td>
<td>8</td>
<td></td>
<td>6.2.4</td>
<td>4.2.9</td>
<td>12.3.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programvara</td>
<td></td>
<td>3.7.7</td>
<td>4.2.10</td>
<td>12.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stopp</td>
<td></td>
<td>3.7.1</td>
<td>5.2</td>
<td></td>
<td>9.2.2</td>
<td>9.2.5.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start &amp; Återstart</td>
<td></td>
<td>3.7.2</td>
<td></td>
<td></td>
<td>9.2.1</td>
<td>9.2.5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nödstopp</td>
<td></td>
<td>6.1.1</td>
<td>4</td>
<td></td>
<td></td>
<td>9.2.5.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oväntad start</td>
<td></td>
<td>3.7.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundans</td>
<td></td>
<td>3.7.5</td>
<td></td>
<td></td>
<td>9.4.2.2</td>
<td>5.4.1</td>
<td>Del 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Övervakning</td>
<td></td>
<td>3.7.6</td>
<td>7.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feltålighet</td>
<td></td>
<td>7.2</td>
<td>5.1</td>
<td>6.2</td>
<td>4.2</td>
<td>9.4.1</td>
<td>5.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ansättning av fel</td>
<td></td>
<td></td>
<td>7.1</td>
<td>7.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Styrsystems självtest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.11</td>
<td></td>
</tr>
</tbody>
</table>

Förslaget IEC1508 i flera avseenden på ett mycket ingående sätt. Detaljerade referenser ges inte i denna tabell.

OBSERVERA! Denna tabell ger exempel på i vilka standarder olika funktioner behandlas. Tabellen är inte avsedd att vara fullständig, dvs. det kan finns punkter som saknas i denna tabell.

I tabellen anges standardernas namn förenklat som EN respektive ISO, även om det korrekt är prEN, SS-EN eller SS-ISO.
Appendix C Referenser

C.1 Rapporter

[FOA] Mats Gunnerhed
Värdering av säkerhetskritisk elektronik och programvara
FOA Rapport C 30636-3.8

[IVF91824] Häkan Carlsson
Mikroprocessorstyrt tvåhandsdon -
konstruktions- och verifieringsexempel
IVF-skrift 91824

[IVF94838] Häkan Carlsson
Konsten att bygga personsäkra styrsystem med dator
IVF-skrift 94838

[SP91:20] Peter Bremer
Säkerhet i mikrodatorbaserade styr- och övervakningssystem
SP-rapport 1991:20

[SP93:51] Peter Bremer, Åke Halldén, Jan Jacobson
Microcomputer-based Protective Functions in Industrial Production
Systems - Assessment method
SP-rapport 1993:51

[SP93:52] Peter Bremer, Åke Halldén, Jan Jacobson
Mikrodatorbaserade skyddsfunktioner i produktionsanläggningar -
kommentarer
SP-rapport 1993:52

C.2 Direktiv

[AFS9336] Arbetarskyddsstyrelsens författningsamling, AFS 1993:36
Användning av arbetsutrustning
1993

Maskiner och vissa andra tekniska anordningar
1994

C.3 Standarder

[EN292] SS-EN 292 Maskinsäkerhet -
Grundläggande begrepp, allmänna konstruktionsprinciper
Del 1: Grundläggande terminologi, metodik
Del 2: Tekniska principer och specifikationer
[EN418] SS-EN 418:1993
Maskinsäkerhet - Nödstoppssutrustning, funktionella aspekter - Konstruktionsprinciper

[EN574] prEN 574:1991
Safety of machinery - Two-hand control device

[EN775] SS-EN 775:1992
Industrirobotar - Maskinsäkerhet

[EN954-1] prEN 954-1:1994
Safety of machinery - Safety related parts of control systems
Part 1: General principles for design

[EN954-2] prEN 954-2
Safety of machinery - Safety related parts of control systems
Part 2: Validation
Under arbete.

[EN1037] prEN 1037:1993
Safety of machinery - Isolation and energy dissipation - Prevention of unexpected start-up

[EN1088] prEN 1088:1993
Safety of machinery - Interlocking devices with and without guard locking - General principles and provisions for design

[EN1760] prEN 1760-1:1994
Safety of machinery - Pressure sensitive protective devices -
Part 1: General principles for the design and testing of pressure sensing mats and pressure sensing floors

[EN50100] prEN 50100-1:1994
Safety of machinery: Electro-sensitive protective equipment -
Part 1: General requirements and tests

[EN60204] SS-EN 60 204-1:1993
Maskinsäkerhet - Maskiners clutrustning -
Del 1: Allmänna fordringar

Programmable controllers - Part 2: Equipment requirements and tests
International Electrotechnical Commission
1992

[IEC1131-4] International Standard IEC 1131-4
Programmable controllers - Part 4: User guidelines
International Electrotechnical Commission
1995
[IEC65A122] IEC65A(Secretariat)122
Software for computers in the application of industrial safety-related systems.
November 1991

[IEC65A123] IEC65A(Secretariat)123
Part 1: General requirements
May 1992

Industriautomation - Säkerhet för samverkande tillverkningssystem - Grundläggande krav

[44/184/CDV] IEC 44/184/CDV
December 1994
Draft Amendment No. 1 to IEC 204-1 : 1992
Electrical equipment of industrial machines
Part 1 : General requirements

[65A/179/CDV] IEC 65A/179/CDV
Draft 1508 - Functional safety: safety-related systems
Part 1: General requirements

[65A/180/CD] IEC 65A/180/CD
Draft 1508-2 : Functional safety: safety-related systems
Part 2: Requirements for electrical/electronic/programmable electronic systems

[65A/181/CDV] IEC 65A/181/CDV
Draft 1508 - Functional safety: safety-related systems
Part 3: Software requirements

[65A/182/CDV] IEC 65A/182/CDV
Draft 1508 - Functional safety: safety-related systems
Part 4: Definitions and Abbreviations of Terms

[65A/183/CDV] IEC 65A/183/CDV
Draft 1508 - Functional safety: safety-related systems

[65A/184/CD] IEC 65A/184/CD
Draft 1508 - Functional safety: safety-related systems
Part 6: Guidelines on the application of Parts 2 and 3.

[65A/185/CD] IEC 65A/185/CD
Draft 1508 - Functional safety: safety-related systems
Part 7: Bibliography of techniques and measures