Hoofdstuk 10

Veiligheid en automatisering

Doelstellingen

1. Weten wat intrinsieke veiligheid is
2. Weten hoe men tot een veilig systeem komt (proces en machine)
3. Weten dat veiligheid van systemen in normen beschreven staat
4. Weten wat lockout/tagout is

Het is niet de bedoeling om in dit hoofdstuk een volledig overzicht te geven van veiligheid in automatisering, dus zeker niet om van u een deskundige te maken op gebied van veiligheid en risicobeheersing. Toch is het wel de bedoeling om een aantal basisconcepten mee te geven en een aantal termen u eigen te laten maken.Ook zou u van een aantal normen moeten gehoord hebben en weten waar de nodige informatie terug te vinden.Bovendien moet u een onderscheid kunnen maken in een aantal zaken.

10.1 Intrinsieke veiligheid

Dit is een term gebruikt bij het ontwerp van een elektrisch toestel of stroomketen en is eigenlijk een beschermingswijze tegen ontsteking.

Genoteerd: EEx i

Om een stroomkring intrinsiek veilig te mogen noemen, moet de energie-inhoud van de stroomkring zodanig begrensd worden dat vonken of eender ander thermisch effect niet kunnen leiden tot ontsteking van een explosief gasmengsel. De energiebegrenzing van intrinsiek veilige circuits wordt gerealiseerd door begrenzing van zowel spanning als stroom.De energiebegrenzing werkt dan kwadratisch omdat:$W = \frac{1}{2}LI^2 = \frac{1}{2}CU^2$.

De constructie-eisen voor de begrenzing van de energie gelden zowel voor de intrinsiek veilige stroomkring zelf als voor de kabels en de bijbehorende componenten die buiten het gevaarlijke gebied zijn geplaatst omdat hier parasitaire capaciteiten en zelfinducties van bijvoorbeeld lange leidingen een rol kunnen gaan spelen. De energiebegrenzing hangt ook sterk af van de installatie van de intrinsiek veilige stroomkring t.o.v. ander elektrisch materiaal en van de installatie achteraf van ander elektrisch materiaal.Hierbij moet worden voorkomen dat een intrinsiek veilige stroomkring wordt blootgesteld aan storingen welke de intrinsieke veiligheid kunnen teniet doen.

EEx i materiaal moet worden voorzien van een markering voor de gasgroep IIA,IIB of IIC.

EEx i materiaal dat in het gevaarlijke gebied wordt geplaatst moet verder worden voorzien van een markering voor één van de temperatuursklassen T1 tot T6.

EEx i materiaal wordt onderverdeeld in 2 categoriën

- EEx ia: mag geen ontsteking geven onder normaal gebruik bij het optreden van één fout, of bij een combinatie van welke twee fouten dan ook.Dit type mag in alle zones gebruikt worden.

- EEx ib: mag geen ontsteking geven onder normaal gebruik bij het optreden van één fout.Dit type mag enkel gebruikt worden in zone 1 en 2.

10.1.1 Temperatuursklassen

Bij mengsels van verschillende gassen is altijd het gas met de laagste ontstekingstemperatuur bepalend, tenzij nadere gegevens gekend zijn.

De hoogst voorkomende oppervlaktetemperatuur moet, om ontsteking te voorkomen, lager zijn dan de ontstekingstemperatuur van het gas.

Elektrisch materiaal is daarom onderverdeeld in temperatuursklassen of T-klassen.Materiaal dat in een bepaalde temperatuursgroep is onderverdeeld, mag dus worden toegepast voor gassen met een ontstekingstemperatuur, die hoger is dan de bij de groep behorende temperatuur.

Temperatuursgroep	Maximaal toelaatbare oppervlaktetemperatuur
T1	$450\,°C$
T2	$300\,°C$
T3	$200\,°C$
T4	$135\,°C$
T5	$100\,°C$
T6	$85\,°C$

10.1.2 Gasgroepen en zones

Gasgroep	T-klasse	voorbeeld
I	-	methaan
IIA	T1	propaan
IIB	T2	ethyleen
IIC	T1	waterstof

Elektrisch materiaal van groep I is bestemd voor ondergrondse mijnen, groep II is voor de overige situatie's.

Wat betreft de indeling van de zones heeft men volgende indeling:

- 0: explosief gasmengsel is voortdurend of gedurende lange tijd aanwezig. De toegelaten beschermingswijze is EEx ia.
- 1: kans op aanwezigheid van explosief mengsel onder normaal bedrijf is groot. De toegelaten beschermingswijzen zijn hier EEx d,EEx e,EEx ib, EEx m, EEx o,EEx p,EEX q.
- 2: kans op aanwezigheid van een explosief mengsel is gering en slechts gedurende korte tijd. De toegelaten beschermingswijzen zijn allen welke toegelaten zijn in zone 0 en 1 alsmede EEx n.

10.2 Normen

Veiligheid is een zeer uitgebreid onderwerp en zelfs een studiegebied op zich. In dit hoofdstuk gaan we ons beperken tot functionele veiligheid[1].

Wat is nu eigenlijk functionele veiligheid? Functionele veiligheid beoogt alles wat:

- het correcte functioneren van de Safety Related Systems zodat de toegewezen veiligheidsfuncties ten allen tijde en onder alle mogelijke omstandigheden behouden blijven
- het voorkomen en behandelen van het falen van de gevaarlijke veiligheidsgebonden systemen zodat het proces en de machines in een veilige toestand gebracht worden

Om deze doelstellingen te kunnen halen zijn de standaardorganisaties standaarden hieromtrent beginnen te ontwikkelen.

Het is vooral het IEC,International Electrotechnical Commission, die internationaal standaarden ontwikkeld in het studiegebied van de elektrotechniek.We gaan het in deze paragraaf hebben over de standaarden IEC 61508 (generische standaard) en IEC 61511 (Safety Instrumented Systems).

[1]De normen voor scheepvaart kan men terugvinden in de ruleboeken van de classificatiebureaus die lid zijn van het IACS zoals ABS,Lloyds of DNV, en ook het IMO

10.2.1 Generische standaard IEC61508

Deze standaard brengt de specifieke standaarden IEC61511,procesindustrie, en IEC 62061, machinebeveiliging voort.

De IEC 61508 bestaat uit zeven delen en behandelt

- Vereenvoudiging voor het ontwerpen van andere sector of produkt gerelateerde standaarden
- Ondersteuning voor produktie van veiligheidssystemen

Het grote belang van deze norm is dat hij het concept van SIL (Safety Integrity Level) en het begrip lifecycle invoerd.

10.2.2 IEC61511

Deze standaard focust op de Safety Instrumented Systems voor de procesindustrie en bestaat uit drie delen

- Deel1: Raamwerk,definities,hardware en software vereisten
- Deel2: Richtlijnen voor de toepassing van IEC61511-1
- Deel3: Richtlijnen voor het bepalen van de SIL-levels.

Zoals gezegd stelt deze richtlijn, en ook de generische (IEC 61508) en de richtlijn voor machinebeveiliging (IEC 62061), het begrip SIL voorop.

10.2.3 SIL

SIL staat voor Safety Integrity Level.

Elke norm heeft zijn SIL-levels.

61508	61511	62061
4levels	4levels	3levels

Om de SIL te berekenen heeft men de lifecycle.Deze lifecycle wordt in elke norm beschreven, en geeft eigenlijk de manier weer waarmee men een installatie in dienst mag nemen rekening houdende met het waarborgen van de veiligheid. Het model bestaat uit vier stappen

1. Ontwerp
2. Montage en inbedrijfsstelling van de instrumentele beveiligingsinrichting
3. Operationele fase
4. Tijdelijke of definitieve uitdienstname van de instrumentele beveiligingsinrichting

Al de machines die in de EU op de markt komen en daar in dienst genomen worden moeten de essentiele veiligheden respecteren die de machine richlijn van de EU voorschrijft. Ook voor deze machinebeveiliging bestaan een aantal normen zoals: IEC62061, ISO13849 en de EN 954-1.

In het kader van dit hoofdstuk is het belangrijk te vermelden dat de ISO 13849 de veiligheidsniveaus weergeeft in Performance levels (PL). Tussen SIL en PL bestaat er een relatie welke voortvloeit uit de betrouwbaarheid. De PL wordt berekend uit

- $MTTF_d$:mean time to dangerous failure
- DC:diagnostic coverage
- CCF:common cause failure

Hieruit volgt volgend verband

$MTTF_d/h$	PL	SIL
$\geq 10^{-5}$to$< 10^{-6}$	a	no SIL
$\geq 3.10^{-6}$to$< 10^{-5}$	b	1
$\geq 10^{-6}$to$< 3.10^{-6}$	c	1
$\geq 10^{-7}$to$< 10^{-6}$	d	2
$\geq 10^{-8}$to$< 10^{-7}$	e	3

In heel dit verhaal moet men ook rekening houden met de ATEX richtlijn.Deze behandelt werd in het eerste bachelor.

In dit verband werd de Ignition Prevention Level (IPL) ingevoerd.Zo bestaan er twee IPlevels

- IPL1:beproefde componenten, hebben hun betrouwbaarheid bewezen. Ze kunnen weerstaan aan verwachte invloeden, en ze kunnen op aanvaardbare tijdsintervallen nagekeken worden.Als er een controleparameter overschreden wordt zal de ontstekingsbron verhinderd worden het mengsel te ontsteken of er wordt een alarm gegeven.
- IPL2:bezit dezelfde eigenschappen als IPL1. Bovendien zal bij het overschrijden van een controleparameter de ontstekingsbron verhinderd worden effectief te worden. Een enkele fout in het Ignition Prevention System zal niet leiden tot verlies van de veiligheidsfunctie.

  Dit leidt tot onderstaand verband

IPL	SIL
1	1
2	2

  Om SIL aan risicoklassen te koppelen bestaan er een aantal methodes. Deze vallen buiten het bestek van de cursus maar we kunnen wel een tabel laten zien met een onderling verband

Risicoklasse	Risiconiveau	SIL
A	Totaal onaanvaardbaar	4
B	Zeer groot onaanvaardbaar risico	3
C	Groot onaanvaardbaar risico	2
D	Middelmatig aanvaardbaar risico	1
E	Klein aanvaardbaar risico	1
F	Zeer klein aanvaardbaar risico	1

Wat gebeurt er nu om het risico te reduceren

- A: verandering van ontwerp
- B: verandering van ontwerp of inbouwen van mechanische of instrumentele beveiliging
- C: verandering van ontwerp of inbouwen van mechanische of instrumentele beveiliging
- D:instrumentele beveiliging of organisatorische maatregel volgens procedure van hoge kwaliteit
- E:instrumentele beveiliging of organisatorische maatregel volgens procedure
- F: geen reductie

10.2.4 Beschermingslagen

Het principe is eenvoudig; hoe hoger het risico, hoe meer en/of betrouwbaardere beschermingslagen.

De techniek die men hier toepast noemt men de Layers Of Protection Analysis.

Welke beschermingslagen zijn er

- normale controlesystemen
- menselijke interventie
- instrumentele veiligheidskring
- mechanische systemen

Hoe gaat men deze lagen structureren? Er is een vuistregel die zegt dat men de menselijke interactie moet beperken tot een minimum en steeds de voorkeur moet geven aan geautomatiseerde acties.

Instrumentele beschermingslaag

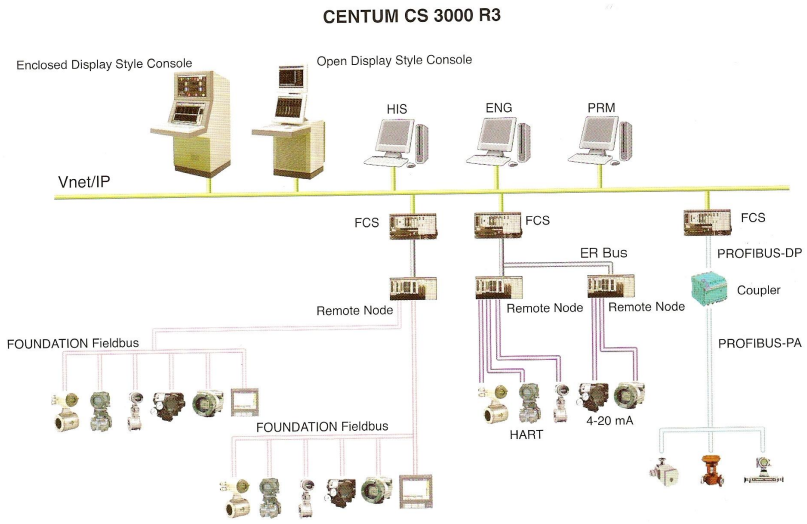
Men onderscheidt een viertal instrumentele inrichtingen namelijk

1. bedrijfsinrichting (DCS:distributed control systeem)
2. bewakingsinrichting
3. schadebegrenzingsinrichting (ESD:emergency shutdown system)
4. beveiligingsinrichting

Wat bepaald nu het SIL niveau in praktijk

- betrouwbaarheid van de componenten
- architectuur (1oo2,2oo3)
- reparatietijd
- aandeel aan gemeenschapelijke fouten
- testinterval
- foutdetectiegraad

10.3 De inrichting



De afkortingen gebruikt in de figuur staan voor

1. HIS:Human Interface Station: dient om het proces te sturen
2. ENG:Engineering PC: dient voor algemene toepassingen en ook voor engineering problemen.Hiermee gebeurt on-line maintenance en systeem configuratie
3. PRM:Plant Resource Manager: verzamelt informatie van de field naar binnen met behulp van de veldbus en zal deze info beheren in een database.
4. FCS:Field Control Station: is de hardware die controle functies uitvoert

Het is nu zo dat de operators het proces bedienen via de console of computer.Als er alarmen binnenkomen gaat de operator moeten reageren om het proces terug bij te sturen, dus instellen nieuw setpunt, kleppen openen of sluiten,... Het gaat echter zo in zijn werk dat er een stuursysteem het proces controleert maar ook een veiligheidssysteem de plant monitort. Beide staan op verschillende parallele systemen. De sturing gebeurt via de DCS:Distributed Controle System, het veiligheidssysteem staat op ESD:Emergency Shutdown System. Deze systemen lopen dus parallel.Dit wil zeggen dat als de operator niet of slecht reageert of het systeem vertoont gebreken waardoor de interventie fout uitdraait (SIL), dat de ESD zal overnemen van de DCS en het proces automatisch stillegt. Het proces

gaat in 'fail safe'.Gewoonlijk krijgt de operator twee alarmsignalen namelijk Hoog (H) en dan Hoog-Hoog (HH) en als er dan nog geen positieve reactie is van het systeem zal het zichzelf veilig stellen en neemt ESD over van DCS. Men heeft uiteraard ook aan de andere kant van het spectrum alarmen namelijk Laag (L) en Laag-Laag (LL) die op dezelfde manier behandelt worden door het fail-safe systeem.

Fail safe gaat ook gepaard met de functie fail to close, fail to open van de kleppen [2].

In heel dit verhaal mag men echter niet uit het oog verliezen dat in dit systeem de operator een cruciale rol speelt zowel als actor als als 'ervaringsdeskundige'.Hij moet de nodige signalen geven in verband met veiligheidsproblemen zowel op hardware-matig als software-matig vlak. Hij moet ook het proces door en door kennen om te kunnen melden waar er verbeteringen kunnen aangebracht worden en waar zich de gevaren situeren.

Hiermee eindigen we het verhaal over continu-werking maar er moet nog vermeld worden dat de normen enkel handelen over continu bedrijf en niet over uitzonderlijke toestanden zoals shutdown of indienstname.Hiervoor gelden andere normen of werkwijzen om de veiligheid te waarborgen.

10.4 Lockout/Tagout

Ook dient in uitzonderlijke situaties, uit dienst name en in dienst name of herstelling, de veiligheid gewaarborgd te worden.

Ook hieromtrent werd in de US al een norm uitgevaardigd namelijk de OSHA standard for control of hazardous energy sources.Deze standaard handelt over lockout/tagout en handelt dus eigenlijk over *de procedures* om machines uit dienst te nemen zodanig dat ze geen gevaar vormen voor het personeel dat deze machines herstelt of onderhoud. Deze veiligstelling gebeurt door de machine alle vorm van energie te ontnemen zodat ze dus geen arbeid kan verrichten.

In Europa bestaat er een richtlijn die in Belgie al van kracht is namelijk de EG-richtlijn 89/655 die minimumvoorschriften geeft inzake veiligheid en gezondheid bij het gebruik door werknemers van arbeidsmiddelen op de arbeidsplaats.

Wat is Lockout/Tagout?

Lockout/Tagout is een vastgelegde veiligheidsprocedure waarbij de energietoevoer van industriële machines en apparatuur wordt uitgeschakeld terwijl er onderhouds-of reparatiewerk wordt uitgevoerd.

[2] Hiervoor verwijs ik naar de cursus pneumatica.

Waarom Lockout/Tagout

1. Veilig werken
2. Ongevallenpreventie
3. Schadepreventie
4. Vormt een beveiliging tegen fouten door een dubbelcheck

10.4.1 Procedurestappen

PHASE I: Lockout/Tagout; blokkeren van het systeem

1. Alle betrokken medewerkers worden op de hoogte gebracht van het begin van de Lockout/Tagout procedure door **één verantwoordelijke medewerker**.
2. De machine wordt alle energie ontnomen.
3. De verantwoordelijke medewerker zal alle eventueel opgeslagen energie die in de machine opgeslagen zit,wegnemen.
4. Alle sloten en tags (waarschuwingsfiche) worden aangebracht en gecontroleerd op fouten. Wordt er een fout vastgesteld wordt dit slot of tag onmiddellijk vervangen
5. De verantwoordelijke medewerker plaatst een *persoonlijke* tag of slot op de machine.
6. De verantwoordelijke medewerker tracht de machine te starten om zeker te zijn dat het systeem geisoleerd is van alle energietoevoer.Dan wordt de machine nogmaals ontdaan van alle energieopslag.
7. Nu mag de machine overgedragen worden aan de onderhoudsdienst

PHASE II:de machine wordt terug overgedragen aan produktie

1. De verantwoordelijke medewerker checkt of er geen voorwerpen vreemd aan de machine werden achtergelaten
2. De verantwoordelijke medewerker checkt of alle veiligheden terug werden geplaatst of werden vervangen.
3. De verantwoordelijke verwittigd iedereen dat de machine terug in dienst kan/zal worden genomen
4. De verantwoordelijke medewerker checkt of er in de omgeving niemand kan worden blootgesteld aan gevaar bij indienstname.
5. De verantwoordelijke neemt alle sloten en tags weg en sluit de machine terug aan aan de energiebron.

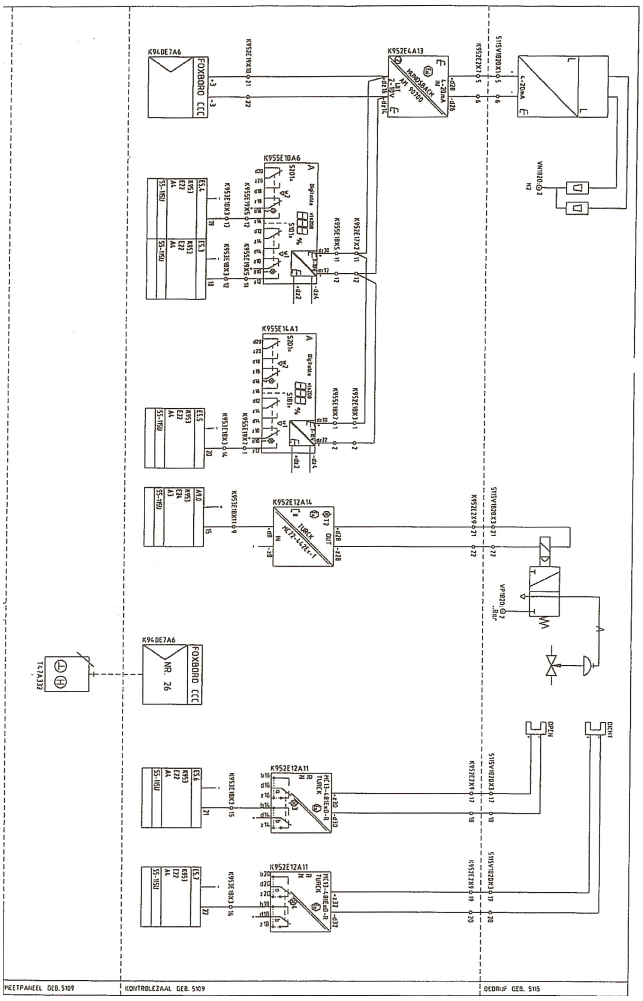
Er moet wel op worden gelet dat de communicatie ook naar contractors toe verloopt en niet enkel het personeel eigen aan de firma op de hoogte wordt gesteld.

Ook bij shiftwissels dient de informatie duidelijk en klaar worden doorgegeven. In de controlekamer ligt steeds een shiftboek die ten allen tijde bijgewerkt wordt en geraadpleegd kan worden.

Ook is het aangewezen dat er werkvergunningen of ander types vergunningen in een speciaal daartoe aangewezen bakje worden verzameld. Bij begin en einde van de job wordt deze afgetekend door verantwoordelijke medewerker en meestergast(chief!!!).

10.5 Intrinsiek veilig schema

Onderstaande figuur geeft een schema van een intrinsiek veilig circuit.(Instrumentatieschema)



10.6 Casestudy

In de les zal over veiligheid een casestudy behandeld worden.