Chapitre 10

Sécurité et automatisation

Objectifs

1. Savoir ce qu'est la sécurité intrinséque
2. Savoir comment on peut arriver à un système sécurisé (processus et machine)
3. Savoir que la sécurité des systèmes est écrite dans des directives
4. Savoir ce qu'est lockout/tagout

Le but dans ce chapitre n'est pas de faire un résumé complèt , donc vous ne serez pas des experts après ce chapitre.Le but ,ici, est de vous donner quelques concepts concernant la sécurité et vous confronter avec quelques termes utilisés dans ce domaine.Nous allons donc traiter des normes concernant la sécurité et les appliquer dans des situations réelles.

10.1 Sécurité intrinsèque

C'est un terme utilisé dans le projet d'un appareil ou d'un circuit électrique et qui est en fait une méthode de protection contre la détente.

Noté : EEx i

Pour qu'un circuit de courant soit intrinsèquement sécurisé, le contenu d'énergie doit être limité d'une telle façon que des étincelles ou d'autres effets thermiques ne puissent pas allumer un mélange explosif.La limitation d'énergie de circuits intrinsèquement sécurisé est obtenue en limitant soit la tension soit le courant. Cette limitation est donc proportionnelle au carré de U ou de I parce que :$W = \frac{1}{2}LI^2 = \frac{1}{2}CU^2$.

Les demandes de construction pour la limitation d'énergie sont en vigueur pour le circuit lui même mais aussi pour les câbles comme les composés qui sont mis en dehors de la zone dangereuse parce qu'il y a des capacités parasitaires et des inductions propres comme par exemple deux longs fils qui peuvent commencer à jouer un rôle.La limitation d'énergie depend de l'installation du circuit sauf intrinseque au point de vue d'autre materiel électrique et de l'installation

d'autres materiels à posteriori.Il faut tenir compte qu'un circuit intrinsèque sécurisé peut être exposé à des perturbations qui peuvent détruire la sécurité intrinsèque.

EEx i materiel doit être prévu d'une marque pour le groupe de gaz IIA,IIB of IIC.

EEx i materiel qui est utilisé dans la zone dangereuse doit être prévu d'un marque pour une des classes de tempèrature T1 tot T6.

EEx i materiel est divisé en deux categories

- EEx ia : ne peut pas allumer dans des conditions d'utilisation normales quand il se manifeste *une* erreur, ou quand il se manifeste une combination de deux erreurs de n'importe quel type.On peut utiliser ce type dans toutes les zones.
- EEx ib : ne peut pas allumer dans des conditions d'utilisation normales quand il se manifeste *une* erreur.On peut utiliser ce type seulement dans les zones 1 et 2.

10.1.1 Classes de température

Pour des mèlanges de différents gaz, c'est toujours le gaz avec la température de détente la plus basse qui est déterminant, sauf quand on a plus de données.

La température de surface la plus haute doit, pour prévenir une détente, être plus bas que la température du gaz.

Pour cette raison le materiel électrique est divisés en classes de températures. Un materiel d' un certain groupe, peut être utilisé dans une situation ou il y a des gaz avec une température de détente qui est plus haute que la température du groupe.

Groupe de température	Température de surface maximale
T1	$450\,°C$
T2	$300\,°C$
T3	$200\,°C$
T4	$135\,°C$
T5	$100\,°C$
T6	$85\,°C$

10.1.2 Groupes de gaz et zones

Groupe de gaz	classe T	exemple
I	-	methane
IIA	T1	propane
IIB	T2	ethylène
IIC	T1	hydrogène

Les materiaux électrique de groupe I sont destinés à des mines souterraines, le groupe II est destiné aux autres situations.

Concernant la division des zones, on a conçu le classement suivant :
- 0 : mélange explosif toujours prèsent ou pendant une long durée. La maniére de protection est EEx ia.
- 1 : il y a un grand risque de présence d'un mélange explosif en fonctionnement normal. Les manières de protection sont EEx d,EEx e,EEx ib, EEx m, EEx o,EEx p,EEX q.
- 2 : Il n'y a pas beaucoup de risque d'obtenir un mélange explosif et ce pour des durées courtes.Les manières de protection sont celles des zones 0 et 1 et aussi EEx n.

10.2 Normes

La sécurité est un sujet vaste et est même une dicipline à part entière. Dans ce chapitre nous allons nous limiter à la sécurité fonctionelle. [1].

Qu'est ce que la sécurité fonctionelle ? La sécurité fonctionelle comprend :
- Le fonctionnement correct des Safety Related Systems pour que toutes les fonctions de sécurité allouées soient preservées à chaque moment et en toutes circonstances.
- LA prévention et le traitement de l'échec des systèmes qui sont liés à la sécurité afin que le processus et les machines soient mis dans une situation sécurisée.

Pour qu'on puisse atteindre ces buts, les organisations de normes ont développé des normes conçernant la sécurité.

C'est notamment le IEC,International Electrotechnical Commission, qui a développé les normes internationales dans la discipline de l'électrotechnique.Nous allons regarder les normes IEC 61508 (norme generique) et IEC 61511 (Safety Instrumented Systems) dans ce paragraphe.

10.2.1 Norme generique IEC61508

Cette norme crée les normes spécifiques IEC61511,procesindustry, et IEC 62061, protection de machines.

Le IEC 61508 est composé de sept parties et traite de :
- Simplification du développement de normes d'autre secteurs ou produits.
- Support pour la production des systèmes de sécurité

La grande importance de cette norme est l'introduction du concept SIL (Safety Integrity Level) et le concept lifecycle.

10.2.2 IEC61511

Cette norme se focalise sur les Safety Instrumented Systems pour l'industrie de processus et consiste en trois parties
- Partie1 : Plan général,definitions,exigences pour le hardware et le logiciel

1. On peut retrouver les normes pour la navigation dans les livres de normes des bureaus de classification qui sont membre de IACS comme IMO,ABS,Lloyds ou DNV, et aussi l'IMO.

– Partie2 : Directives pour l'application de IEC91511-1
– Partie3 : Directives pour la détermination du SIL

Comme déjà dit, cette norme, comme le generique (IEC 61508) et la norme pour la protection de la machine (IEC 62061), accentuent le SIL.

10.2.3 SIL

SIL est l'abbréviation de Safety Integrity Level.
Chaque norme a ces niveaux SIL.

61508	61511	62061
4levels	4levels	3levels

Pour calculer le SIL on utilise le concept Lifecycle.Ce lifecycle est décrit dans chaque norme et décrit la manière de prendre en service une installation en tenant compte de la garantie de la sécurité. Le modèle existe en quatre étapes

1. Le projet
2. Le montage et la mises en service de l'installation de sécurité instrumentale
3. La phase operationelle
4. La mise hors service temporaire ou definitive de l'installation de sécurité instrumentale

Toutes les machines qui arrivent sur la marché de l'UE et qui sont mis en service doivent respecter les sécurités qui sont décrites dans la directive de machines de l'EU.Il existe aussi des normes de sécurité pour cette directive comme : IEC62061, ISO13849 en de EN 954-1.

Dans le cadre de ce chapitre il est important de mentioner que l'ISO 13849 refléte les niveau de sécurité en Performance levels (PL). Il existe une relation entre le SIL et le PL qui est basée sur la fiabilité. On peut calculer le PL grâce :
– $MTTF_d$:mean time to dangerous failure
– DC :diagnostic coverage
– CCF :common cause failure

De cela écoule le rapport suivant

$MTTF_d/h$	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

Dans ce cas ci il faut aussi tenir compte de la directive ATEX,évoquée dans le premier bachelor.

Dans ce rapport, on a introduit l' Ignition Prevention Level (IPL).Il existe deux niveaus IP

- IPL1 :composés éprouvés,ont éprouvé leur fiabilité. Il peuvent résister aux influences éxpectées,et ils peuvent être contrôlés dans des intervalles de temps acceptables.Si un paramètre de controle est franchi la source de détente sera empêchée pour allumer le mélange ou une alerte sera donnée.
- IPL2 :contient les mêmes propriétés que IPL1. En plus quand un paramètre de contrôle est franchi, la source sera empêchée de devenir effective.Une erreur dans l' Ignition Prevention System ne mène pas à la perte de fonction de sécurité.

  Ceci suit au rapport ci dessous

IPL	SIL
1	1
2	2

  Pour coupler le SIL avec les classes de risques il existe quelques méthodes.Cet accouplement n'est pas le but de ce cours mais le tableau ci dessous vous donne un rapport possible

Classe de risque	Niveau de risque	SIL
A	Totalement inacceptable	4
B	Très grand risque inacceptable	3
C	Grand risque inacceptable	2
D	Risque médiocre acceptable	1
E	Petit risque acceptable	1
F	Très petit risque acceptable	1

  Qu'est que l'on fait pour réduire le risque :
  - A : changement de projet
  - B : changement de projet ou introduction d'une sécurité mecanique ou instrumentale
  - C : changement de projet ou introduction d'une protection mecanique ou instrumentale
  - D :protection instrumentale ou mesure organisatoire selon procédure de haute qualité
  - E :protection instrumentale ou mesure organisatoire selon procédure de haute qualité
  - F : pas de reduction

10.2.4 Couches de protection

Le principe de couches de protection (en anglais layers of protection) est simple : Plus le risque est élevé ; plus il y a de couches de protection.
La technique appliquée est nommée Layers Of Protection Analysis.
Couches de protection :(Ceci n'est qu'un échantillon)
– systèmes de contrôle normaux
– intervention humaine
– circuit de sécurité instrumental
– systèmes mécaniques
Comment est ce que l'on va structurer ces couches ? Il y a une règle pratique qui dit qu'il faut limiter l'interaction humaine et préferer les actions automatisées.

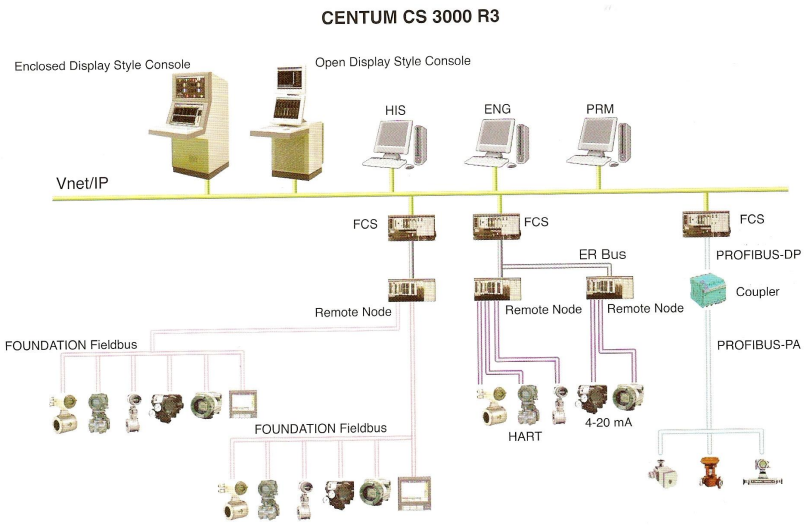
Couche de protection instrumentale

On peut distinguer quatre couches instrumentale

1. institution d'exploitation (DCS :distributed control system)
2. institution de surveillance
3. institution de limitation du dégât (ESD :emergency shutdown system)
4. institution de sécurité

Quels paramètres vont déterminer le niveau SIL en pratique ?
– fiabilité des composés
– architecture (1oo2,2oo3)
– temps de réparation
– participation d'erreurs communes
– intervalle de test
– degrés de detection d'erreur

10.3 L'institution



Les abreviations utilisé dans la figure

1. HIS :Human Interface Station : sert à contrôler le processus
2. ENG :Engineering PC : sert pour des applications générales et pour les problèmes d'engineering.On organise l'entretien on-line et système de configuration
3. PRM :Plant Resource Manager : rassemble l'information du champs à l'intérieur avec l'aide des bus de champs et va gérer cette information dans un database.
4. FCS :Field Control Station : est le hardware qui execute des fonctions de contrôle

Les mécaniciens de contrôle commandent le processus grâce à une console ou un ordinateur.S'il y a des alarmes, le mécanicien de contrôle doit réagir pour corriger le processus ; adapter une consigne,fermer ou ouvrir une vanne ... Mais il n'y a pas seulement un système de contrôle mais aussi un système d'alarme qui observe le processus.Ils sont mis sur deux systèmes parallèle.La commande est mise sur DCS :Distributed Controle System,le système de sécurité sur ESD :Emergency Shutdown System. Donc s'il y a un problème, par exemple le mécanicien de contrôle ne réagit pas ou de manière éronnée ou alors il manque quelque chose dans le système et donc l'intervention tourne mal (SIL), le ESD prendra le contrôle et met le système en 'fail safe'.Généralement le mécanicien de contrôle reçoit deux alarmes ; une haute :Haut (H :high) et puis une très haute :Haut-Haut

(HH :high high) et s'il n'y a pas de réaction positive du système, il se met dans la situation sauve donc fail safe et le ESD prend du DCS. On a de l'autre côté aussi des alarmes, c'est à dire bas (L :low) et bas-bas (LL :low low) qui sont traité de la même manière.
Si on parle de fail safe il faut aussi parler des fonctions fail to close, fail to open d'une vanne. [2].
Dans le système de sécurité, le rôle du mécanicien de contrôle est vraiment crucial. Il joue le rôle d'acteur mais aussi d'expert parce que c'est lui qui connaît le processus et ses faiblesses. Il sait où on peut améliorer la sécurité de façon logiciel comme hardware. Il sait aussi où se trouvent les dangers.
Jusqu'à maintenant nous avons parlé du situation d'exploitation continue mais qu'est ce qu'il se passe dans des situations discontinus comme mettre en marche ou mettre hors service.

10.4 Lockout/Tagout

Dans des situations speciales il faut aussi respecter la sécurité.
Aux Etats Unis, on a déjà promulgué une norme, c'est à dire la norme OSHA (standard for control of hazardous energy sources).Cette norme évoque lockout/tagout et donc évoque *les procedures* pour mettre hors service des machines de façon qu'il n'y ait pas de danger pour le personnel qui fait l'entretien ou les reparations. Le concept de cette procedure est de prendre n'importe quelle forme d'énergie de cette machine pour qu'elle ne puisse pas exécuter d'énergie.
En Europe, il existe une directive qui est déjà en vigueur en Belgique, c'est à dire la directive européene 89/655 qui exige des instructions conçernant la sécurité et la santé pour les travailleurs sur leur lieu de travail quand ils utilisent des moyens de travail.
Qu'est ce que Lockout/Tagout ?
Lockout/Tagout est une procedure de sécurité dans laquelle l'alimentation d'énergie des machines et appareiles est coupée pendant les reparations ou l'entretien.
Pourquoi Lockout/Tagout

1. Travailler en sécurité
2. Prevention de accidents
3. Prevention de dégâts
4. Protection extra contre des erreurs grâce à un double contrôle

2. Pour ceci il faut consulter le cours de pneumatique.

10.4.1 Etapes de procédure

PHASE I : Lockout/Tagout ; bloquage du système

1. Tous les collaborateurs sont avertis du début de la procedure Lockout/Tagout par **un collaborateur responsable**.
2. La machine est enlevée de chaque forme d'alimentation d'énergie.
3. Le collaborateur responsable enlevera toute l'énergie stockée dans la machine.
4. Toutes les serrures et tags (fiche d'avertissement) sont placés et controlés d'erreurs. Si on remarque une erreur ce tag ou serrure est remplacé immédiatement.
5. Le collaborateur responsable met un tag ou serrure *personnel* sur la machine.
6. Le collaborateur responsable essaie de démarrer la machine pour être sûr que le système est isolé de chaque alimentation d'énergie. Encore une fois le collaborateur responsable enlevera toute l'énergie de la machine.
7. Maintenant la machine peut être transférée aux services d'entretien.

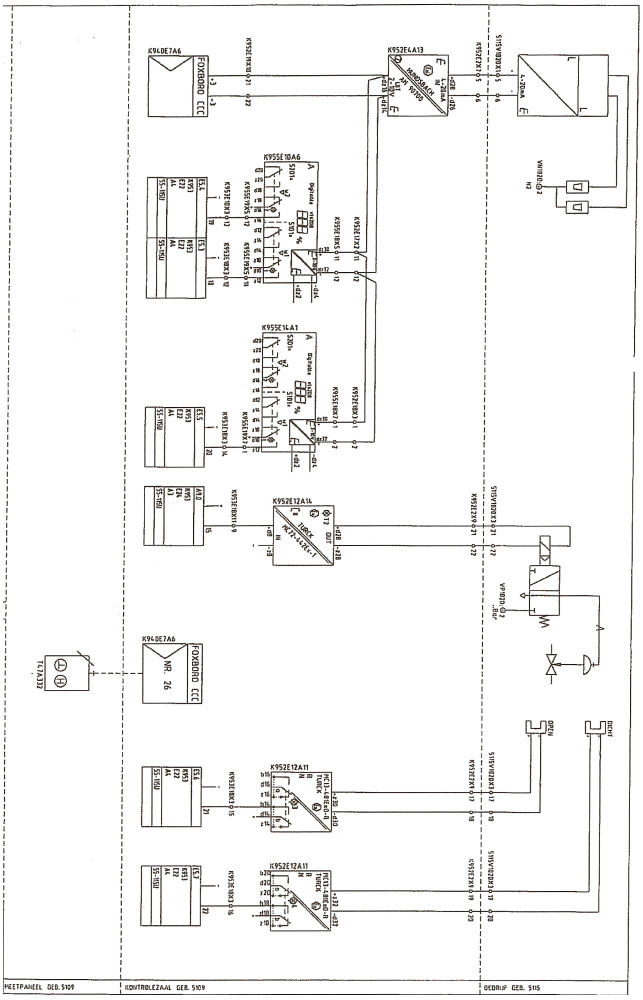
PHASE II :la machine est transférée à la production

1. Le collaborateur responsable contrôle s'il n'y a pas des objets qui sont étranger à la machine.
2. Le collaborateur responsable controle si toutes les protections sont en place ou remplacées.
3. Le collaborateur responsable avertit tout le monde que la machine pourra/sera mise en service de nouveau.
4. Le collaborateur responsable controle s'il n'y a personne aux environs de la machine qui peut être exposé au danger pendant la mise en service.
5. Le collaborateur responsable enlève tous les tags et les serrures et branche la machine à la source d'énergie.

Il faut faire attention que l'information soit communiquée à tout le monde, donc aussi aux contracteurs, et pas seulement au personnel propre de la firme.
Pendant les changements d'équipe l'information doit être communiquée de façon claire et correcte.Dans la chambre de contrôle, il y a toujours un livre d'équipe (logbook) qui est mis à jour et qui peut être consulté à chaque moment.
Il est aussi recommandé que les permis de travail ou autres permis soient gardés dans un bacquet spécial.Au début et à la fin du travail, le collaborateur responsable et le maître (chef!!!) signent les permis.

10.5 Schèma d'un circuit sauf intrinseque

La figure ci-dessous donne le schèma d'un circuit intrinseque sécurisé.(schèma d'instrumentation)



10.6 Casestudy

Pendant les leçons il y aura une étude d'un cas spécial conçernant la sécurité.