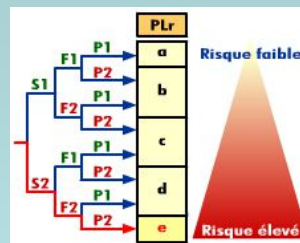
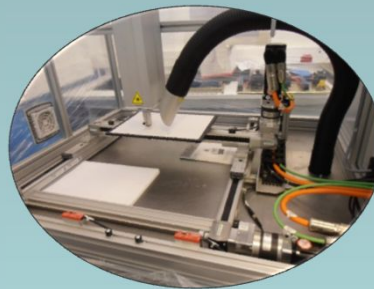


SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

LA SECURITE DES MACHINES



SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

SOMMAIRE

INTRODUCTION

1. Les causes d'accidents dans l'industrie
2. Danger ou risque ?
3. La sécurité pour un niveau de risque acceptable

CONCEPT DE LA SECURITE MACHINE

1. Démarche d'analyse du risque suivant la norme EN 1050
2. Qu'est-ce qu'une directive ?
3. Les normes
4. Evolution des directives et des normes
5. La norme EN ISO 13849-1
6. Le niveau de performance requis PLr
7. Détermination du niveau de performance atteint PL
8. Catégories des systèmes de commande selon norme EN 954-1
9. Calcul du MTTFd d'un composant
10. Valeur du DC d'un composant

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

SOMMAIRE (SUITE)

ETUDE DE CAS – SCIE CIRCULAIRE

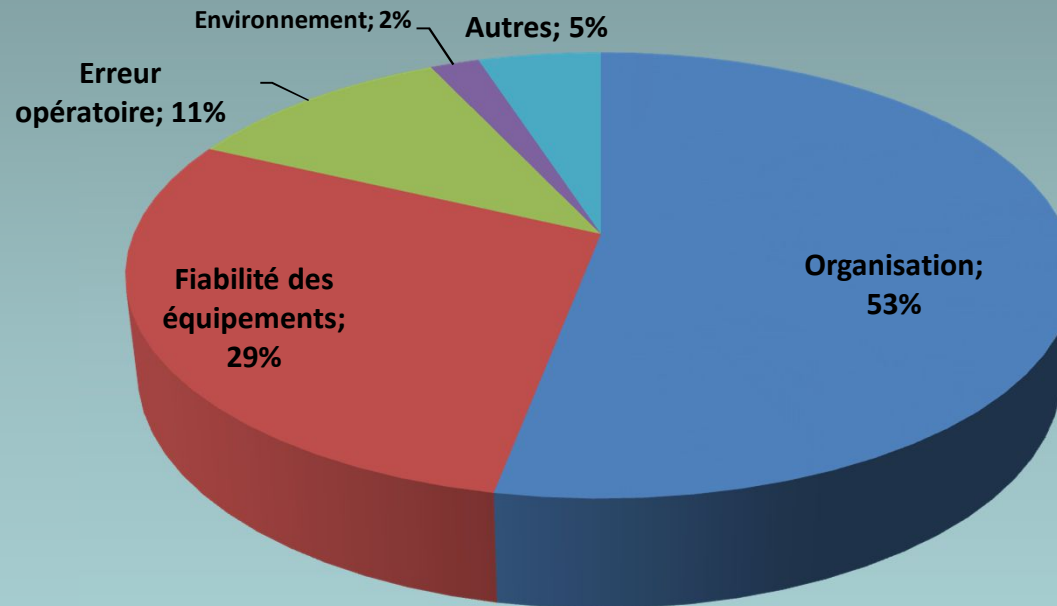
1. Evaluation du niveau de performance requis PLr (sans capot)
2. Evaluation du niveau de performance requis PLr (avec capot)
3. Structure retenue à priori pour le système de commande
4. Identification des composants
5. Calcul du MTTFd global du système de commande
6. Calcul du DC moyen d'un canal du système de commande
7. Evaluation des défaillances de causes communes (CCF)
8. Evaluation du niveau de performance atteint PL

DOCUMENTATION OBLIGATOIRE A FOURNIR

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

1- Les causes d'accidents dans l'industrie :



« Sur la période 1992-2006, les défaillances d'ordre **humaines** ou **organisationnelles** sont à l'origine de près de la moitié des accidents [...] »

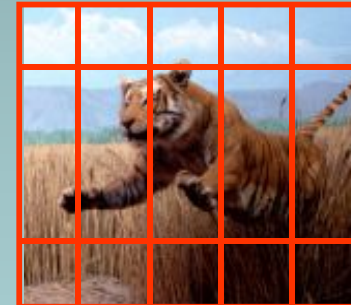
(1) d'après le bureau du Ministère chargé de l'Environnement

CONCEPT DE LA SECURITE MACHINE

2- Danger ou risque ?

- ❑ La confusion est fréquente entre **danger** et **risque** :
 - Un danger est toujours présent,
 - Le risque est la possibilité qu'un évènement dangereux survienne.

- ❑ Prenons comme exemple le tigre :
 - Un tigre affamé est **dangereux**,
 - Un tigre affamé représente un **risque**



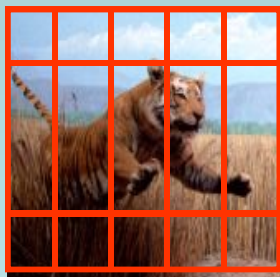
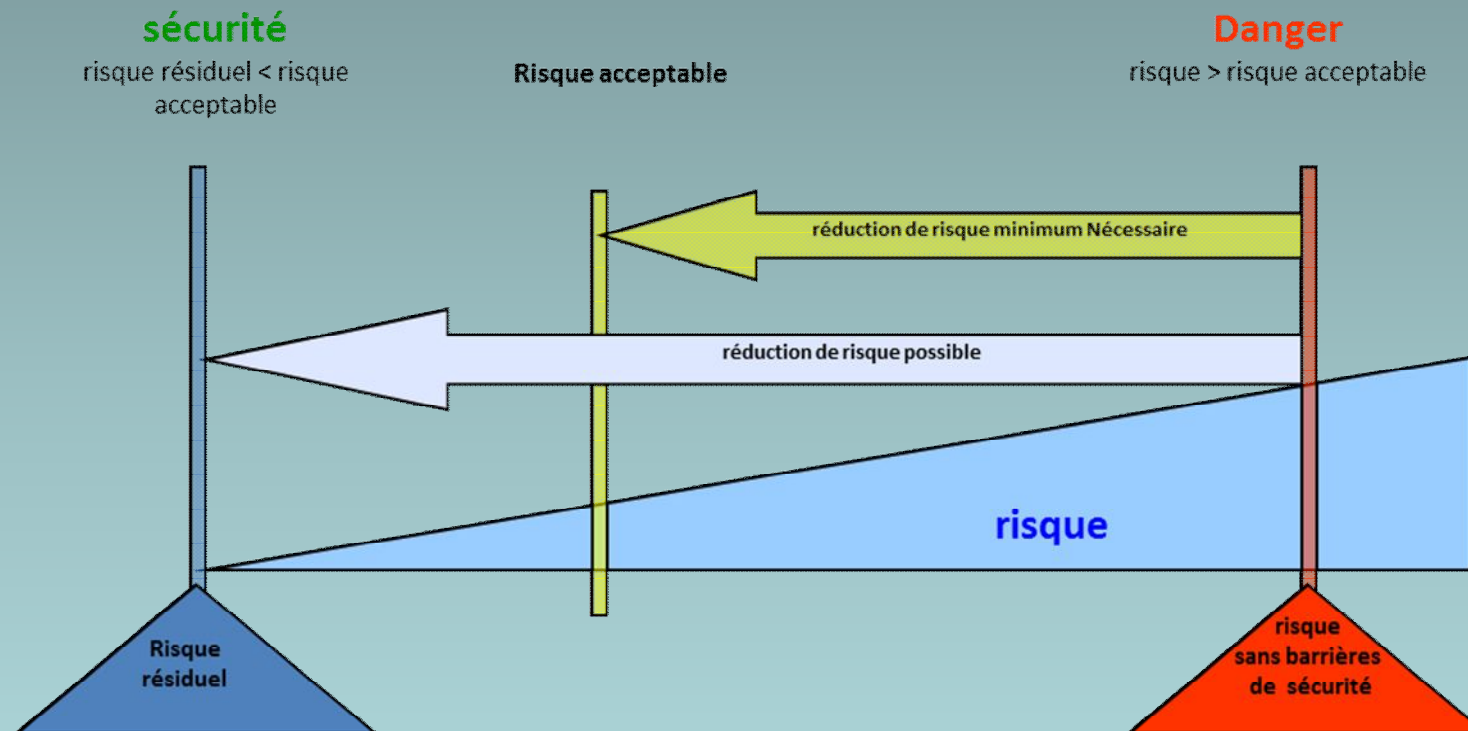
- ❑ Un tigre affamé est dangereux, mais cela représente un risque uniquement si il est à votre contact.

On peut éviter ou réduire le risque par l'isolement du danger !
(le tigre est enfermé à clé dans une cage, ainsi le risque d'une attaque est très faible)

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

3- La sécurité pour atteindre un niveau de risque acceptable :



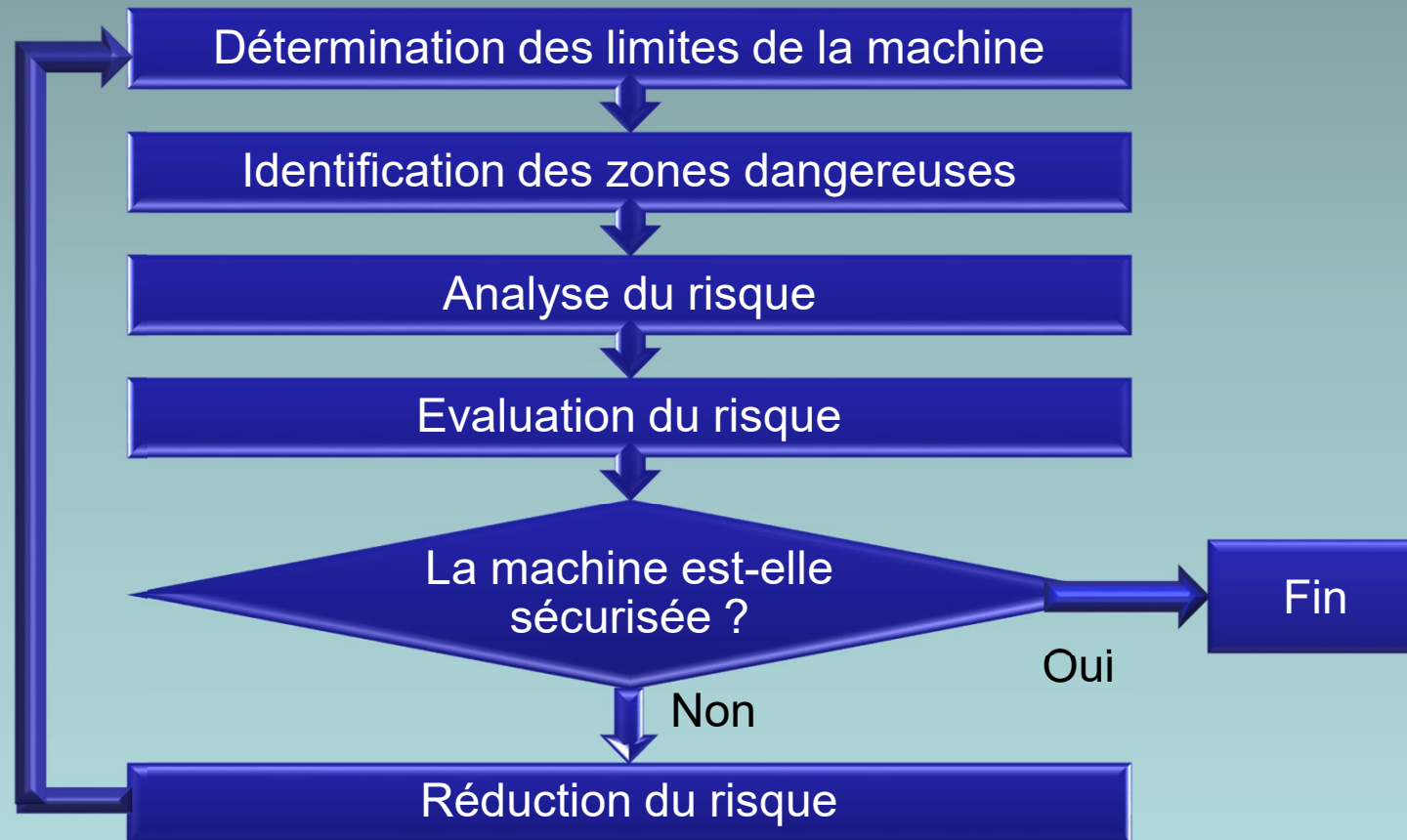
Le **risque 0** n'existe pas
mais doit être réduit à un
niveau acceptable.



SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

1- Démarche d'analyse du risque suivant la norme EN1050 :



CONCEPT DE LA SECURITE MACHINE

2- Qu'est-ce qu'une directive ?

- Une directive est un acte juridique communautaire pris par le Conseil de l'Union Européenne.
- Les états membres doivent transposer la directive dans leur droit national.
- Les directives sont publiées au Journal Officiel des Communautés européennes.

Directive=Loi

Il est obligatoire de respecter une directive !



CONCEPT DE LA SECURITE MACHINE

3- Les normes :

- Une norme est une **spécification technique**, un recueil de **bonnes pratiques** rédigé par un comité d'experts (utilisateurs, constructeurs et fabricants) dont **l'observation n'est pas obligatoire**.

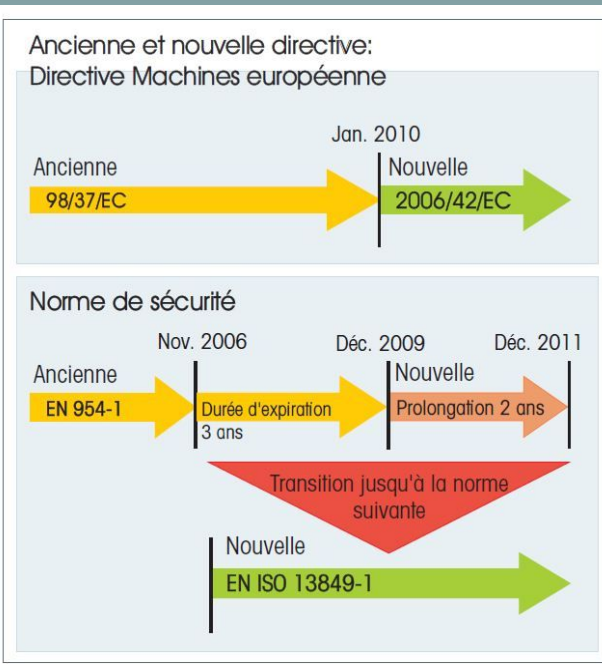
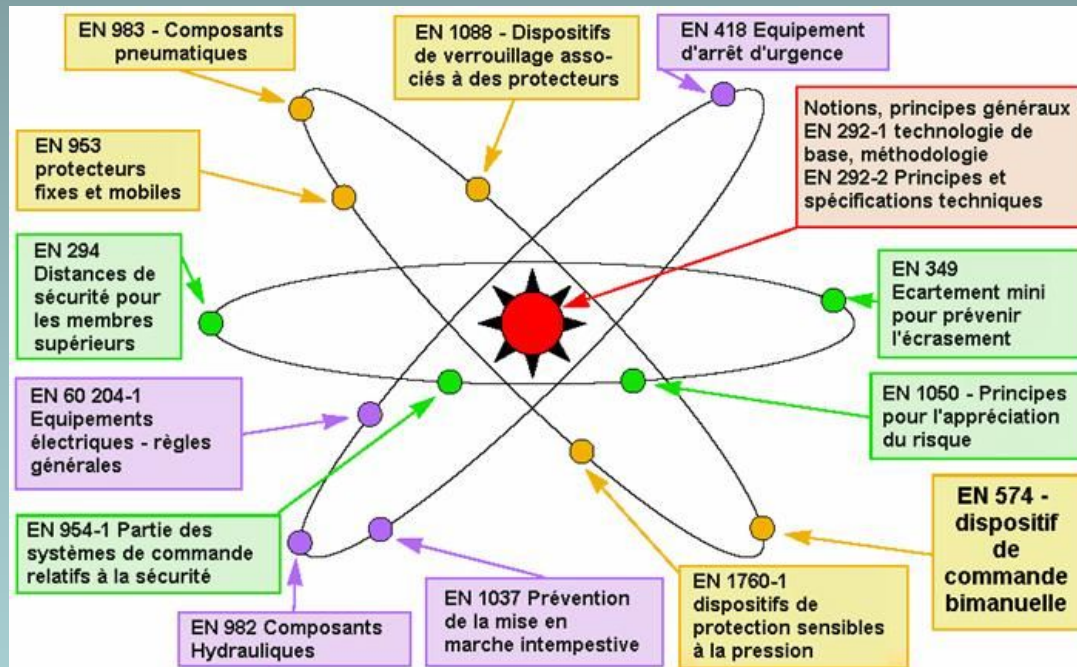
- Une norme est dite **normalisée** quand :
 - elle respecte la directive par rapport à laquelle elle est rédigée,
 - elle donne présomption de conformité pour l'obtention du marquage CE



SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

4- Evolutions des directives et des normes :



❑ Les nouvelles normes **EN62061** et **EN13849-1** sont **harmonisées** au titre de la nouvelle directive machine **2006/42/CE**.

❑ Contrairement à l'ancienne norme EN954-1, ces deux nouvelles normes imposent la prise en compte des **défaillances aléatoires** du matériel par des **calculs probabilistes**.

CONCEPT DE LA SECURITE MACHINE

5- La norme EN ISO 13849-1 :

- Cette norme préconise que les **systèmes de commande** doivent être **sûrs et fiables** , de manière à **éviter toute situation dangereuse** .

- Les systèmes de commande doivent être conçus :
 - pour **résister** aux **contraintes normales de service** et aux **influences extérieures** ,
 - de manière à ne pas avoir de **situations dangereuses** , en cas **d'erreur de manœuvre** , **défaillance aléatoire** ou **détérioration** du circuit de commande.

- La norme EN 13849-1 prend en compte la probabilité d'apparition d'un défaut ou d'une défaillance susceptible de provoquer la perte de la fonction de sécurité.

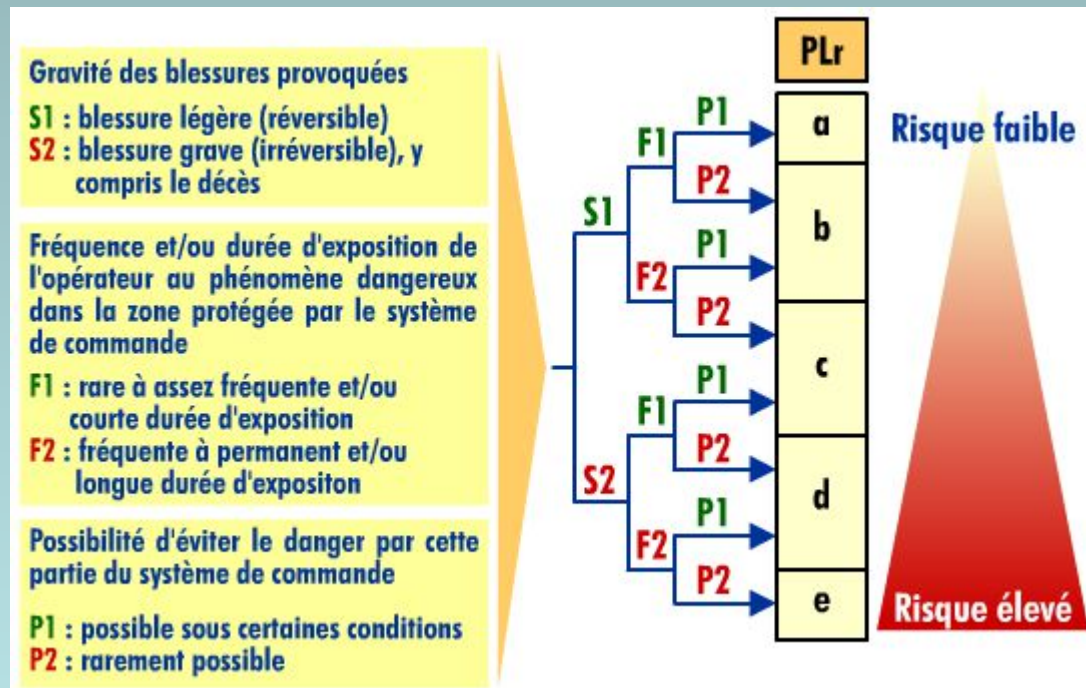
- Pour cela, les systèmes de commande doivent posséder un niveau de performance suffisant (**PL : Performance Level**).

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

6- Le niveau de performance requis PLr :

- ❑ Le niveau de performance requis **PLr** (Requerest Performance Level) par la machine se détermine en caractérisant les risques que le système fait courir à l'opérateur.
- ❑ On défini cinq niveaux de performance à atteindre par le **SRP/CS (Safety-Related Part of Control System)** :



CONCEPT DE LA SECURITE MACHINE

7- Détermination du niveau de performance atteint PL :

- ❑ Le niveau de performances atteint par le système de commande (SRP/CS) se détermine à partir :
 - de sa **catégorie** (selon norme EN 954-1),
 - de son **MTTFd** (Mean Time To Failure dangerous) qui correspond au temps moyen avant défaillance dangereuse,
 - de son **DC_{AVG}** (Diagnostic Coverage Average) qui mesure l'efficacité de la surveillance des défauts,
 - du **CCF** (Common Cause Failure) ou défaillance de cause commune dont le score rend compte de sa capacité à éviter des défaillances affectant plusieurs entités à partir d'un même évènement.

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

8- Catégories des systèmes de commande selon norme EN 954-1 :

Catégories	Base principale de la sécurité	Exigence du système de commande	Comportement en cas de défaut	Structure typique d'un circuit de sécurité en cas de défaut	Commentaires
B	Par la sélection des composants conformes aux normes pertinentes	Contrôle correspondant aux règles de l'art en la matière	Perte possible de la fonction de sécurité		Perte possible de la fonction de sécurité
1	Par la sélection de composants conformes aux normes pertinentes	Utilisation de constituants et de principes éprouvés	Perte possible de la fonction de sécurité. Probabilité plus faible qu'en B	<p style="text-align: center;">* Unité de traitement</p>	<ul style="list-style-type: none"> • Pas de redondance sur E • Pas de redondance interne assurée par un relais à contacts liés mécaniquement • Pas de redondance sur S
2	Par la structure des circuits de sécurité	Test par cycle. La périodicité du test doit être adaptée à la machine et à son application	Défaut détecté à chaque test		<ul style="list-style-type: none"> • Redondance ou pas sur les entrées • La boucle de retour permet d'assurer un test cyclique sur la sortie
3	Par la structure des circuits de sécurité	Un défaut unique ne doit pas conduire à la perte de la fonction de sécurité. Ce défaut doit être détecté si cela est raisonnablement faisable	Fonction de sécurité garantie, sauf en cas d'accumulation de défauts		<ul style="list-style-type: none"> • Redondance sur les E • Redondance sur les S
4	Par la structure des circuits de sécurité	Un défaut unique (ou une accumulation de défauts) ne doit pas mener à la perte de la fonction de sécurité. Ce défaut doit être détecté dès, ou avant la prochaine sollicitation de la fonction de sécurité	Fonction de sécurité toujours garantie		<ul style="list-style-type: none"> • Redondance sur les E • Redondance sur les S • La boucle de retour permet d'assurer un test cyclique sur les sorties

CONCEPT DE LA SECURITE MACHINE

9- Calcul du MTTFd d'un composant :

□ Suivant la norme EN 13849-1, le MTTFd se calcule comme suit :

$$- \text{MTTFd} = \frac{B_{10d}}{0,1 \times n_{op}}$$

- Le paramètre B_{10} est une donnée constructeur qui correspond au **nombre de cycles pour que 10 % des produits testés soient défectueux**

- Le n_{op} correspond au nombre annuel d'utilisation :

$$- n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cycle}}$$

avec h_{op} nombre d'heures d'utilisation par jour

d_{op} nombre de jours d'utilisation par année

t_{cycle} temps moyen entre le démarrage
successif de 2 cycles

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

CONCEPT DE LA SECURITE MACHINE

10- Valeur du DC d'un composant :

- ❑ Le taux de diagnostic DC se définit comme le ratio entre le taux de pannes dangereuses détectées et le taux de pannes dangereuses total.
- ❑ Le DC est une donnée constructeur. Quand sa valeur n'est pas communiquée, on se réfère au tableau E1 de la norme EN 13849-1 (voir extrait ci-dessous) :

Mesure	DC
Dispositif d'entrée	
Stimulus d'essai cyclique par changement dynamique des signaux d'entrée	90 %
Contrôle de vraisemblance, par exemple un contact normalement fermé et un contact normalement ouvert avec utilisation de contacts guidés.	90 %
Surveillance croisée des entrées sans test dynamique	0 % à 90 %, selon la fréquence de changement de signal réalisée par l'application
Surveillance croisée des entrées avec test dynamique dans le cas où les courts-circuits ne sont pas détectables (pour I/O multiples)	90 %

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

1- Evaluation du niveau de performance requis PLr :

Gravité des blessures provoquées :

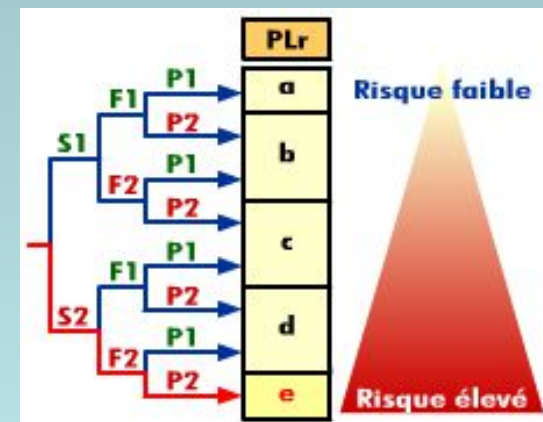
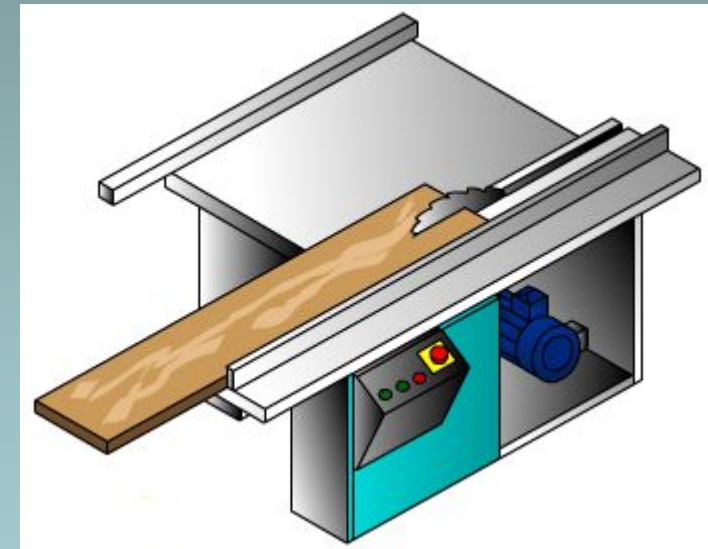
- **S2** blessures graves et irréversibles
(sectionnement de doigts ou de la main)

Fréquence et durée d'exposition de l'opérateur aux phénomènes dangereux :

- **F2** fréquence d'exposition de la main dans la zone très élevée (l'opérateur pousse la planche)

Possibilité d'éviter le phénomène dangereux ou de limiter le dommage :

- **P2** possibilité d'évitement très faible (vitesse de rotation de la scie très élevée)



Le niveau requis PLr = e

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

2- Evaluation du niveau de performance requis PLr :

Gravité des blessures provoquées :

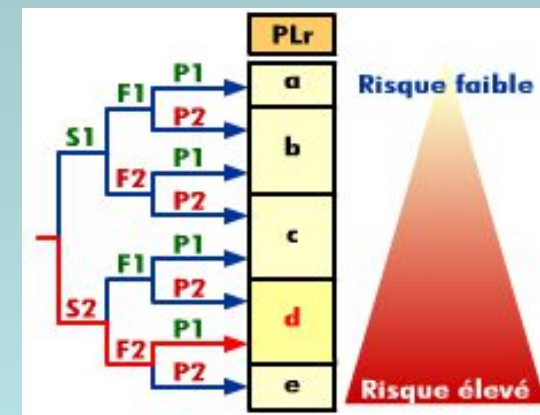
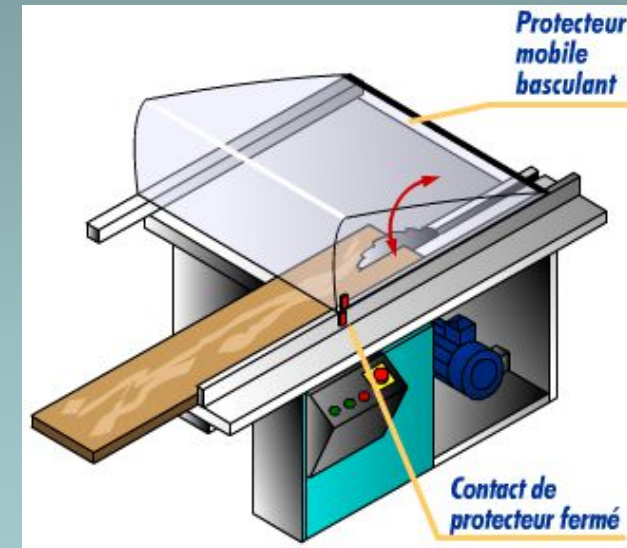
- **S2** blessures graves et irréversibles
(sectionnement de doigts ou de la main)

Fréquence et durée d'exposition de l'opérateur aux phénomènes dangereux :

- **F2** fréquence d'exposition de la main dans la zone très élevée (l'opérateur pousse la planche)

Possibilité d'éviter le phénomène dangereux ou de limiter le dommage :

- **P1** possible sous condition (mise en place d'un capot)



Le niveau requis PLr = d

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

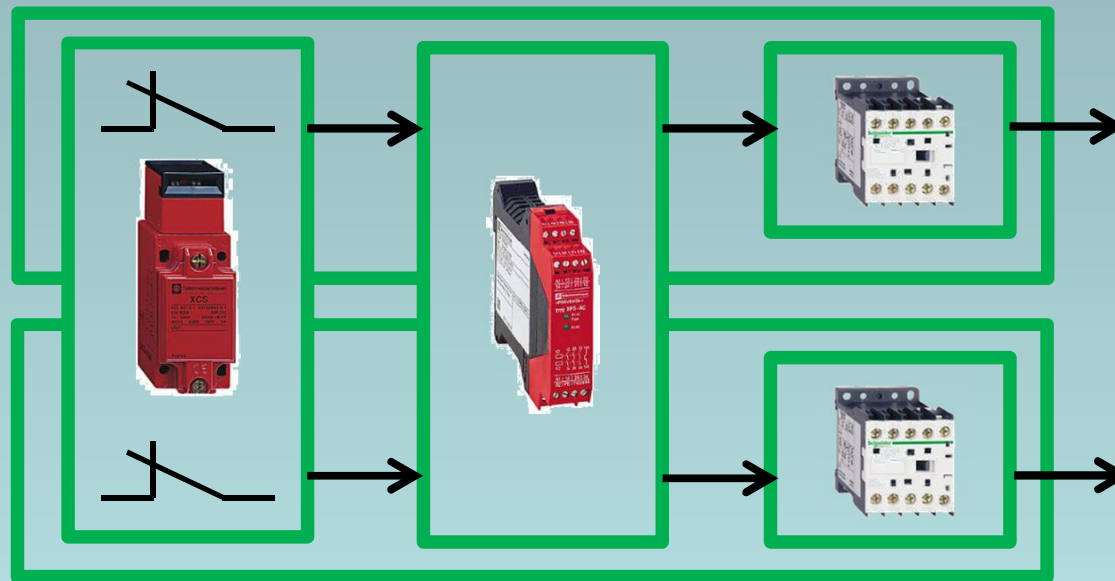
3- Structure retenue à priori pour le système de commande :

Pour obtenir le PLr, il est nécessaire d'utiliser **deux canaux redondants**, ce qui correspond à une **catégorie 3** :



Représentation suivant norme EN 13849-1

Canal 1



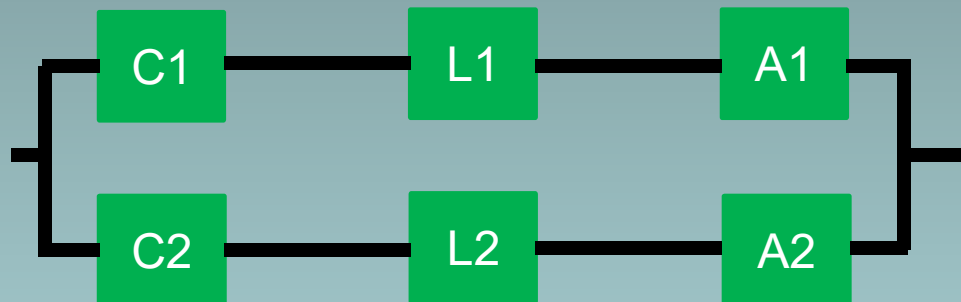
Canal 2

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

4- Identification des composants :

- ☐ Toutes les parties intervenant dans la fonction de sécurité doivent être identifiées.



La machine est utilisée 220 j/an
 Temps de fonctionnement 16 h/j
 Temps moyen entre 2 cycles de 60s
 Nombre d'opérations $n_{op}=211200$ par an

Capteur XCSA



SRP/CSa

Logique



SRP/CSb

Actionneur



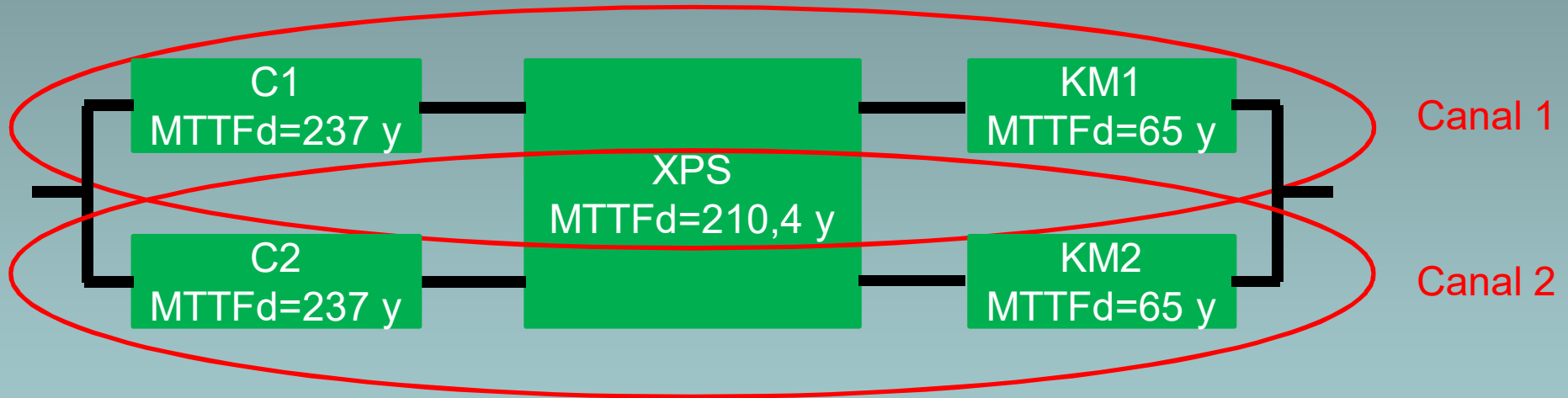
SRP/CSc

Composant	B_{10d}	MTTFd (an)
Capteur C1, C2	5000000	237
Module de sécurité	NA	210,4
Contacteurs	1369863	65

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

5- Calcul du MTTFd global du système de commande :



□ Le MTTFd global se calcule comme suit :

$$\frac{1}{MTTFd} = \frac{1}{MTTF_{\text{capteur}}} + \frac{1}{MTTF_{\text{XPS}}} + \frac{1}{MTTF_{\text{KM}}} \quad \longrightarrow \quad MTTFd=41 \text{ ans}$$

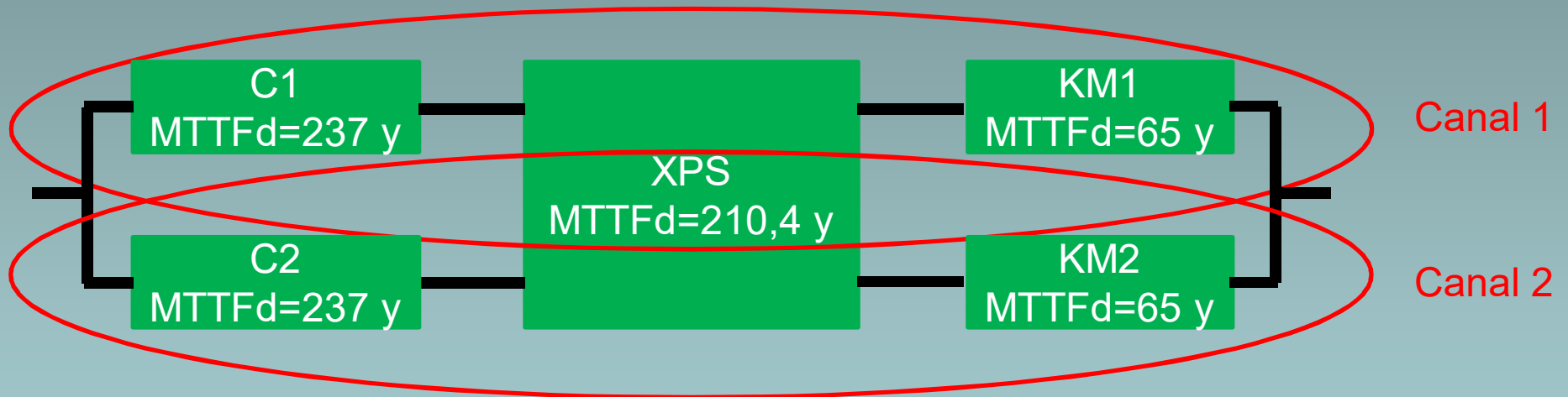
□ Le tableau 5 de la norme indique que le MTTFd de 41 ans correspond à une valeur élevée :

Temps moyen avant panne dangereuse	Echelle de MTTFd
bas	$3 \text{ ans} \leq MTTFd < 10 \text{ ans}$
moyen	$10 \text{ ans} \leq MTTFd < 30 \text{ ans}$
élevé	$30 \text{ ans} \leq MTTFd < 100 \text{ ans}$

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

6- Calcul du DC moyen d'un canal du système de commande :



□ Le DC d'un canal se calcule comme suit :

$$DC_{AVG} = \frac{\frac{DC_1}{MTTF_1} + \frac{DC_2}{MTTF_2} + \dots + \frac{DC_N}{MTTF_N}}{\frac{1}{MTTF_1} + \frac{1}{MTTF_2} + \dots + \frac{1}{MTTF_N}} \quad \longrightarrow \quad DC_{AVG} = 98 \%$$

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

- ❑ Le tableau 6 de la norme indique que le DC_{AVG} correspond à une valeur moyenne :

Taux de couverture de pannes	Niveau du DC
nul	$DC < 10 \%$
bas	$60 \% \leq DC < 90 \%$
moyen	$90 \% \leq DC < 99 \%$
élevé	$99 \% \leq DC$

Avec un $DC_{AVG}=98 \%$, le niveau de détection de pannes est jugé « moyen »

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

7- Evaluation des défaillances de causes communes CCF:

- ❑ Le tableau F1 donne le procédé de notation pour les mesures contre les CCF :
- ❑ Pour satisfaire aux exigences, le score obtenu doit être supérieur ou égal à 65.
- ❑ Un score inférieur à 65 indique qu'il faut prendre des mesures supplémentaires.

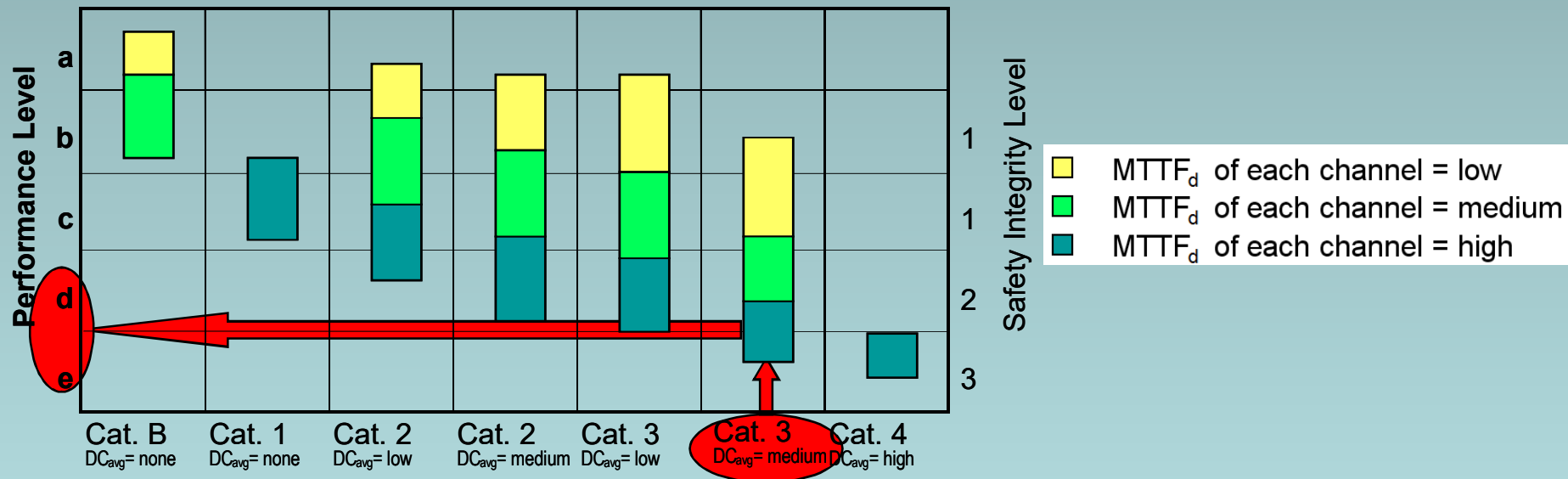
N°	Mesure contre les CCF	Score
1	Séparation/isolément	
	Séparation physique entre les voies de signaux: séparation dans le câblage, le tuyautage, distances d'isolement et lignes de fuite suffisantes sur les cartes de circuits imprimés.	15
2	Diversité	
	Différents principes de conception/technologies ou principes physiques sont utilisés, par exemple: premier canal électronique programmable et second canal câblé sorte d'initiation pression et température Mesurage de la distance et de la pression, par exemple: numérique et analogique, Composants de divers fabricants	20
3	Conception/application/expérience	
3.1	Protection contre surtension, surpression, surintensité, etc.	15
3.2	Utilisation de composants éprouvés	5
4	Appréciation/analyse	
	Les résultats d'une analyse des modes de défaillance et de leurs effets sont-ils pris en compte pour prévenir les défaillances de cause commune à la conception ?	5
5	Compétence/formation	
	Les concepteurs spécialistes de la maintenance sont-ils formés pour comprendre les causes et les conséquences des défaillances de cause commune ?	5
6	Environnement	
6.1	Prévention de la contamination et de la compatibilité électromagnétique (CEM) contre les CCF en conformité avec les normes pertinentes Systèmes fluides: filtration du médium sous pression, prévention de l'absorption des impuretés, drainage de l'air comprimé, par exemple en conformité avec les exigences du fabricant du composant en ce qui concerne la pureté du médium sous pression, Systèmes électriques: l'immunité électromagnétique du système a-t-elle été vérifiée, par exemple comme spécifié dans des normes produits applicables ? Pour des systèmes combinés fluides et électriques, il convient de considérer les deux aspects.	25
6.2	Autres influences Les exigences relatives à l'immunité contre toutes les influences environnementales pertinentes telles que température, choc, vibration, humidité sont-elles prises en compte, par exemple comme spécifié dans les normes applicables ?	10
	Total	(max. réalisable 100)

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

ETUDE DE CAS – SCIE CIRCULAIRE

8- Evaluation du niveau de performance atteint PL :

- Le système de commande choisi permet d'obtenir :
 - un $MTTF_d$ **élevé**,
 - un DC_{AVG} **moyen**,
 - une **catégorie 3**



- Le système de commande permet d'obtenir un **PL atteint=d,e supérieur ou égal** au **PL_r=d**

SECTION DE TECHNICIEN SUPERIEUR ELECTROTECHNIQUE

DOCUMENTATION A FOURNIR

- ❑ Le concepteur de la machine doit fournir, au minimum, les informations suivantes :
 - les fonctions de sécurité réalisées par le système,
 - les caractéristiques de chaque fonction de sécurité,
 - les points précis où commencent les parties relatives à la sécurité et où elles se terminent,
 - les conditions environnementales,
 - le niveau de performance (PL),
 - les catégories sélectionnées,
 - les paramètres relatifs à la fiabilité (MTTFd, DC, CCF et durée de mission),
 - les mesures prises contre les défaillances systématiques,
 - les technologies utilisées,
 - tous les défauts relatifs à la sécurité pris en compte,
 - la justification des exclusions de défauts (voir EN ISO 13849-1),
 - le raisonnement suivi lors de la conception (par exemple les défauts pris en compte, ainsi que les défauts exclus,
 - la documentation du logiciel,
 - les dispositions contre un mauvais usage raisonnablement prévisible.

REFERENCES BIBLIOGRAPHIQUES

- ❑ La rédaction de ce cours sur la sécurité des machines s'est faite à partir des références bibliographiques suivantes :
 - Directive 2006/42/CE du Parlement Européen et du Conseil en date du 17 Mai 2006,
 - Norme ISO 13849-1 « Sécurité des machines — Parties des systèmes de commande relatives à la sécurité » publiée en novembre 2006 (AFNOR),
 - le magazine Intersections « La sécurité machine » de novembre 1999 de Schneider-Electric,
 - « La sécurité des machines automatisées – Tome 1: Notions de base, Réglementation, normes, techniques de prévention » de Schneider-Electric (Collection Technique),
 - « La sécurité des machines automatisées – Tome 2: Techniques et moyens de prévention opératifs, systèmes de commande, utilisation des machines» de Schneider-Electric (Collection Technique),
 - le Guide des Sciences et Techniques version 1,1 de Thierry Schanen.