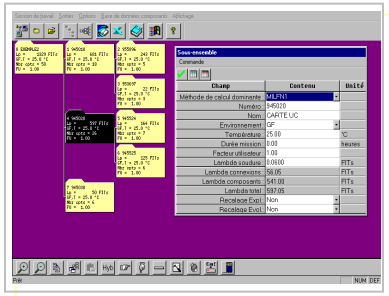
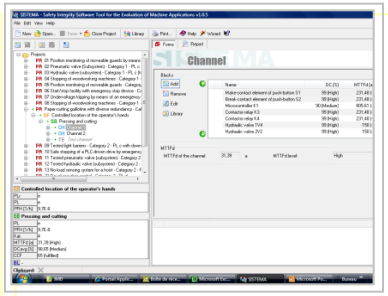
L’Essentiel

Norme EN ISO 13849-1

Sécurité des machines

Parties des systèmes de commande relatives à la sécurité



Direction Technique
DEKRA Industrial SA

Rédacteur : JM DURAND
Date: 13/02/2013
Version: 0

Réglementation

Contexte normatif

98/37/CE

Directive machines

→

2006/42/CE

Directive machines

29 décembre 2009

Le respect d'une norme harmonisée donne présomption de conformité aux directives européennes.

EN 954-1 : 1997

Parties des systèmes de commande relatives à la sécurité

Catégorie:
B, 1, 2, 3, 4

EN 13849-1 : 2007

Parties des systèmes de commande relatives à la sécurité

Performance Level:
a, b, c, d, e

Introduction

Norme EN ISO 13849-1

- **Fournit les exigences de conception des SRP/CS**
  - *Logique filaire*
  - *Logique programmable (conception du logiciel)*
- **S'applique aux SRP/CS de tous types de machines indépendamment de la technologie utilisée**
  - *Électrique, hydraulique, pneumatique, mécanique*
- **Ne donne pas d'exigences spécifiques pour la conception des composants intégrés**
  - *Pour les relais, commandes bimanuelles, dispositifs électrosensibles, …*

Généralités

SRP/CS (Security Relative Part of Control System)

Partie d'un système de commande qui répond à des signaux d'entrée et génère des signaux de sortie relatifs à la sécurité

ENTREE	→	TRAITEMENT	→	SORTIE
Blocs d'entrée		**Blocs traitement**		**Blocs de sortie**
Acquisition de l'information des différents capteurs de sécurité		Traitement requis afin de réaliser les fonctions de sécurité		Commande des actionneurs à partir des sorties liées à la sécurité

Activation
ex: BP AU

SRP/CS

Actionneur
ex: moteur

Généralités

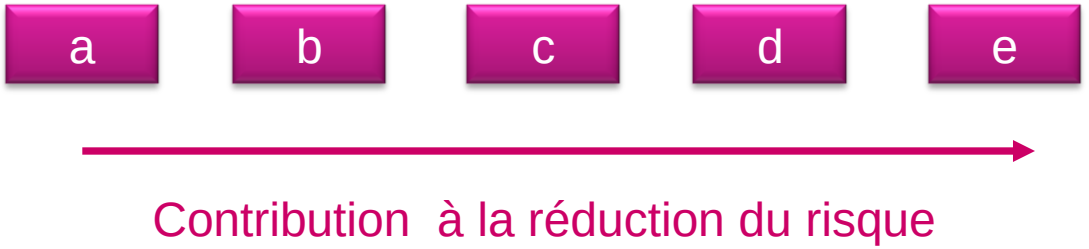
Niveau de performance

Mesure de la capacité du SRP/CS à réaliser une fonction de sécurité

⇨ Notion de **niveau de performance**

Niveau de performance (PL) : niveau discret d'aptitude de parties relatives à la sécurité à réaliser une Fonction de Sécurité (SF) dans des conditions prévisibles.

- On définit 5 niveaux classés de **a** à **e**:



Généralités

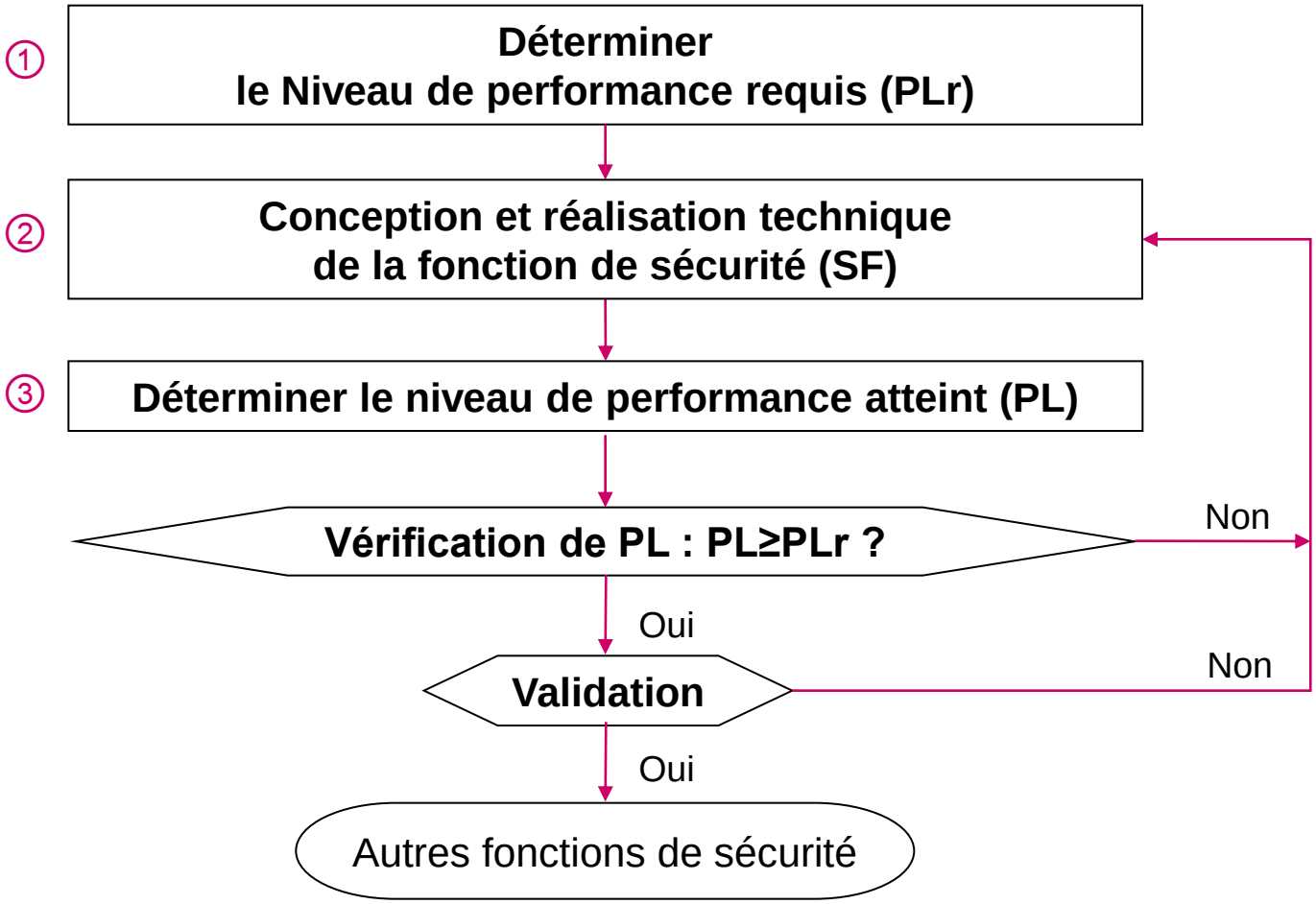
Probabilité moyenne de défaillance dangereuse

Les niveaux de performance sont caractérisés par leur probabilité de défaillance dangereuse par heure

PL	PFH_D (1/H)
a	$\geq 10^{-5}$ à $<10^{-4}$
b	$\geq 3x10^{-6}$ à $<10^{-5}$
c	$\geq 10^{-6}$ à $<3x10^{-6}$
d	$\geq 10^{-7}$ à $<10^{-6}$
e	$\geq 10^{-8}$ à $<10^{-7}$

Conception des SRP/CS

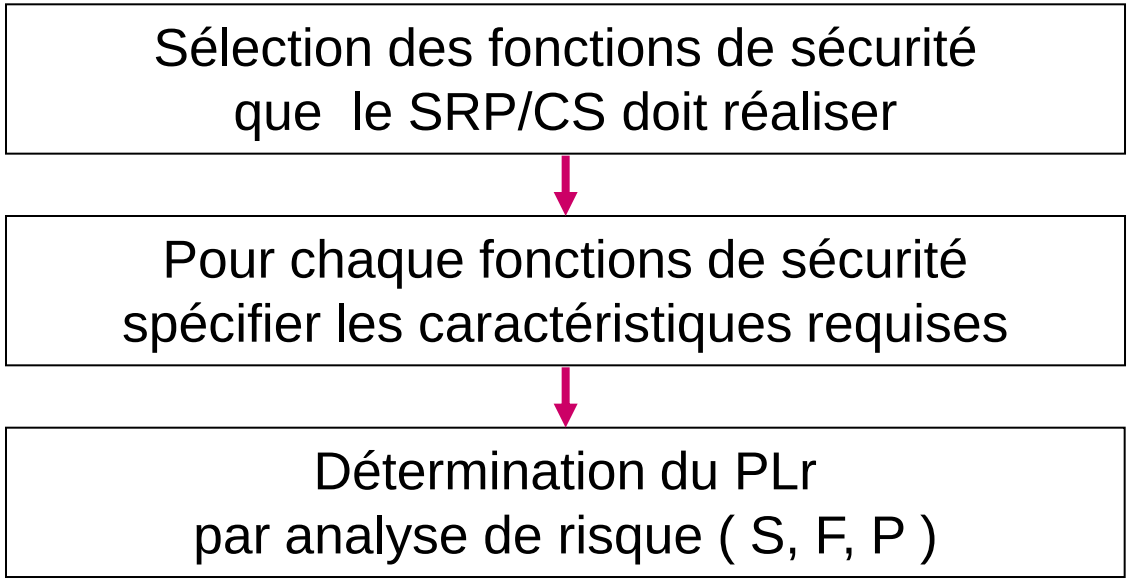
Démarche globale



Conception des SRP/CS

1 – détermination du niveau de performance requis (PLr)

Pour chaque fonction de sécurité le concepteur devra déterminer le PLr requis (valeur cible ou objectif) par la démarche suivante:



Analyse de risque

Paramètres de risque

- **S Gravité de la blessure**
  - S1 blessure légère (réversible)
  - S2 blessure grave (irréversible)

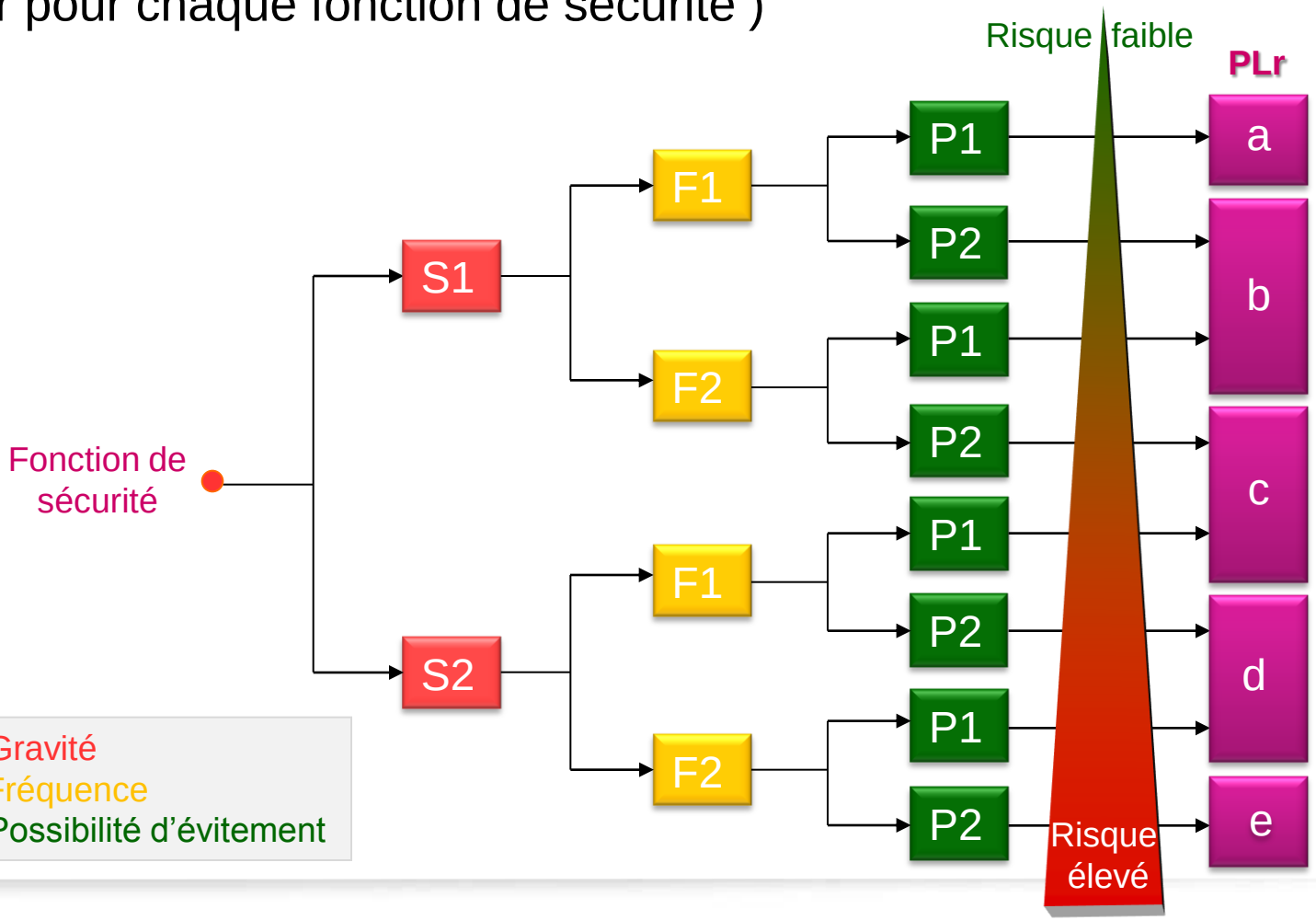
- **F Fréquence et/ou durée d'exposition du phénomène dangereux**
  - F1 rare à assez fréquente et/ou durée d'exposition courte
  - F2 fréquente à continue et/ou durée d'exposition longue

- **P Possibilité d'éviter le phénomène dangereux ou de limiter le dommage**
  - P1 possibilité sous certaines conditions
  - P2 rarement possible

Analyse de risque

Niveau de performance requis (PLr)

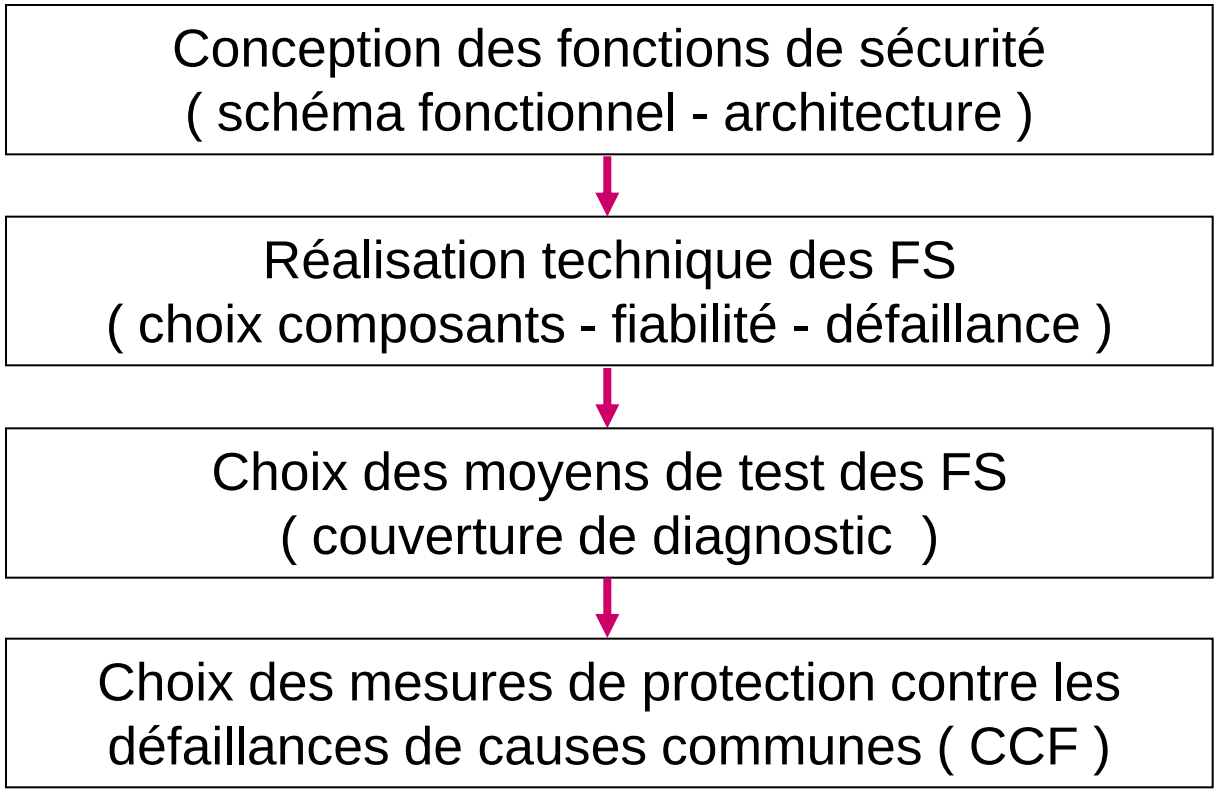
Graphique de risque pour déterminer le niveau de performance requis (PLr pour chaque fonction de sécurité)



Conception des SRP/CS

2 – Conception des fonctions de sécurité

Le concepteur réalisera les fonctions de sécurité en fonction du niveau de performance requis estimé lors de l'analyse de risque.



Calcul de la PFHD

Architecture matérielle (Catégories)

B, 1, 2, 3, 4

Catégorie	Comportement du système	Principes pour atteindre la sécurité
B	L'occurrence d'un défaut peut conduire à la perte de la fonction de sécurité.	Principalement caractérisés par la sélection des composants. Les principes de base de sécurité doivent être utilisées.
1	L'occurrence d'un défaut peut conduire à la perte de la fonction de sécurité, mais la probabilité de cette occurrence est plus faible que pour la catégorie B.	Principalement caractérisés par la sélection des composants. Des composants éprouvés et des principes de sécurité éprouvés doivent être utilisés.
2	L'occurrence d'un défaut peut conduire à la perte de la fonction de sécurité dans l'intervalle entre deux contrôles. La perte de la fonction de sécurité est détectée par le contrôle.	Principalement caractérisés par la structure. La fonction de sécurité doit être contrôlée à intervalles convenables par le système de commande de la machine.
3	Lorsqu'un défaut unique se produit, la fonction de sécurité est toujours assurée. Certains défauts sont détectés mais pas tous. L'accumulation de défauts non détectés peut conduire à la perte de la fonction de sécurité.	Principalement caractérisés par la structure. Autant que cela est raisonnablement réalisable le défaut unique est détecté.
4	Lorsqu'un défaut unique se produit, la fonction de sécurité est toujours assurée. La détection de défauts accumulés réduit la probabilité de perte d'une fonction de sécurité (DC élevé). Les défauts sont détectés à temps pour empêcher la perte de la fonction de sécurité.	Principalement caractérisés par la structure. Défaut unique détecté dés ou avant la prochaine sollicitation de la fonction de sécurité. L'accumulation de défauts non détectés ne doit pas entrainer la perte de la fonction de sécurité.

Calcul de la PFHD

MTTFd (Mean Time To Dangerous Failure)

Temps moyen avant défaillance dangereuse

- Valeur probable de la durée moyenne de fonctionnement avant défaillance dangereuse

MTTFd de chaque canal	
Indice	**Gamme (an)**
Faible	3 ≤ MTTFd < 10
Moyen	10 ≤ MTTFd < 30
Élevé	30 ≤ MTTFd ≤ 100

Calcul de la PFHD

DC (Diagnostic Coverage)

DC

Couverture du diagnostic

- Mesure de l'efficacité du diagnostic; peut être définie comme la fraction de la probabilité de défaillances dangereuses détectées sur la probabilité de toutes les défaillances dangereuses

DC	
Indice	**Gamme (%)**
Nulle	DC < 60
Faible	60 ≤ DC < 90
Moyenne	90 ≤ DC < 99
Elevée	99 ≤ DC

Calcul de la PFHD

CCF (Common Cause Failure)

CCF

Estimation pour les défaillances de cause commune:

- Procédure de notation pour les mesures contre les CCF

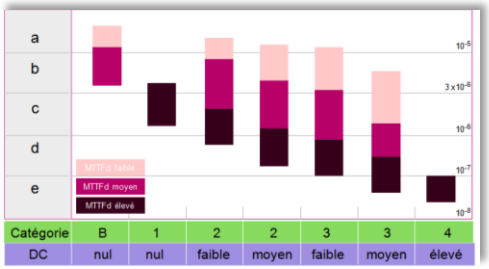
Procédé de notation pour les mesures contre les CCF		
N	**Mesure**	**Score**
1	**Séparation/isolement** (séparation physique entre les voies de signaux)	15
2	**Diversité** (différents principes de conception/technologie ou principes physiques sont utilisés)	20
3	**Conception** (protection contre les surtension, surpression, surintensité, etc)	20
4	**Appréciation/analyse** (les résultats de l'AMDE sont ils pris en compte)	5
5	**Compétence/formation** (les concepteurs spécialistes de la maintenance sont ils formés)	5
6	**Environnement** (CEM, impuretés, température, choc, vibration, humidité, …)	25 10
	Total	100

Conception des SRP/CS

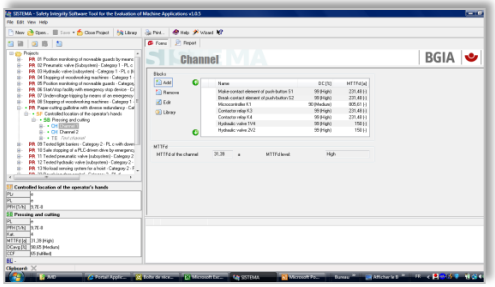
3 – Détermination du niveau de performance (PL)

Pour chaque fonction de sécurité le concepteur devra déterminer le PL à l'aide d'une des démarches suivantes:

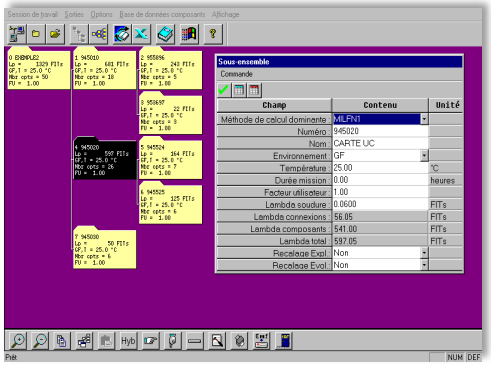
Approche simplifiée → Architecture, DC, MTTFd →



Logiciel de calcul → Analyse de risque, Fonction de sécurité, Caractéristiques des composants (Fiabilité, Tests, CCF) →



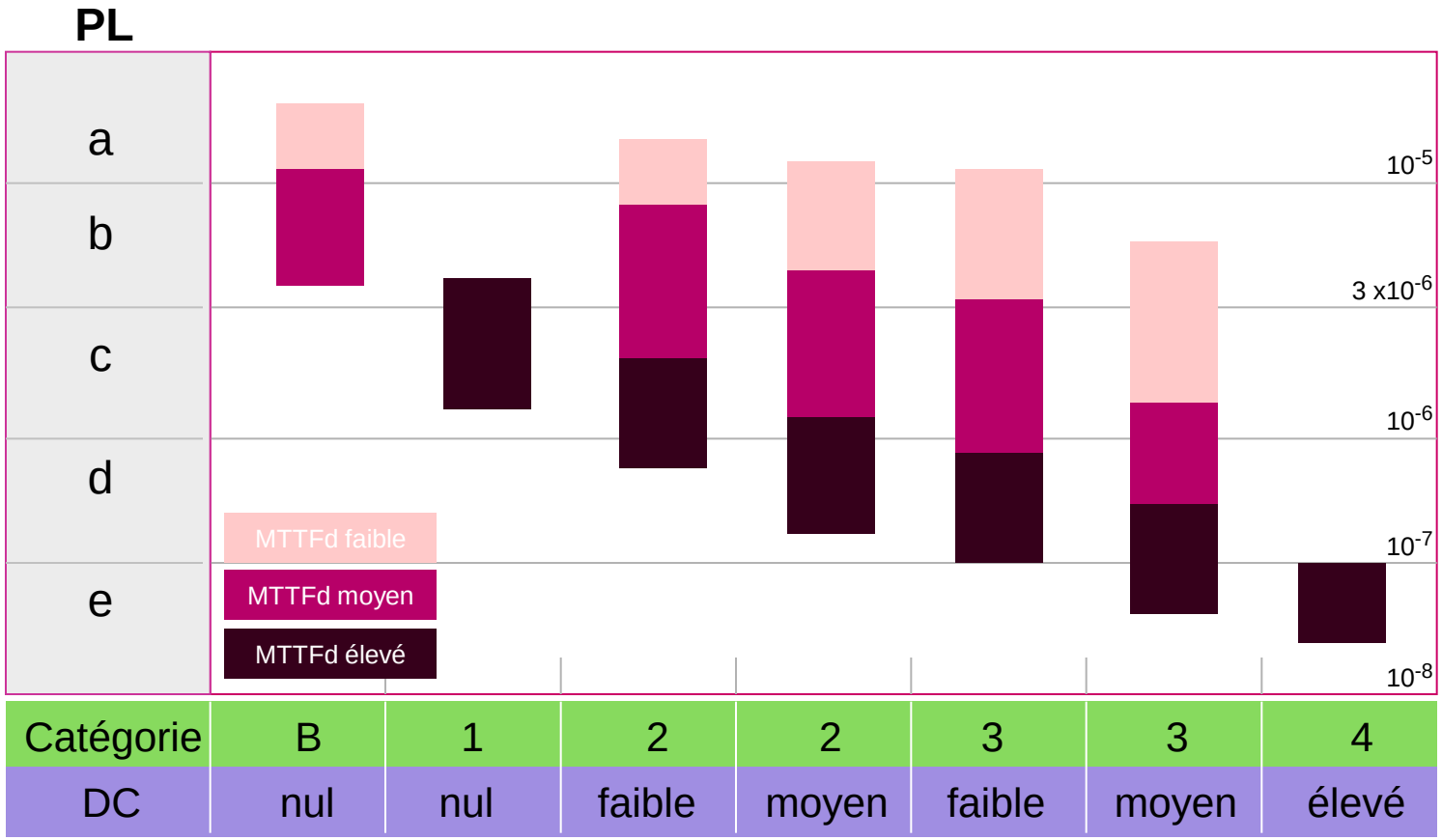
Analyses SdF → Analyse fonctionnelle, Analyse des Défaillances, Analyse de testabilité →



Estimation du niveau de performance

Approche simplifiée de détermination du PL

En fonction de la structure du système de commande (catégorie B, 1, 2, 3, 4), du MTTFd du canal, du niveau de couverture du diagnostic, on peut vérifier le niveau de performance atteint : PL à l'aide du diagramme suivant:



Catégorie	B	1	2	2	3	3	4
DC	nul	nul	faible	moyen	faible	moyen	élevé

Estimation du niveau de performance

Calcul de la PFHD par logiciel

- Projet, SF, Sous-système, Canal, Bloc Logique, Elément