Institut des Sciences et Techniques
de l'Ingénieur d'Angers

# Evaluation de trois normes en sécurité fonctionnelle

Projet Industriel 5ème année d'école d'ingénieurs


**Tuteur entreprise** :
KAHN Patrice

**Tuteur pédagogique** :
GUERIN Fabrice

**Groupe projet** :
KARIM Sara
RAKOTONIRINA Manoa Justin
BARNAY Raphaël
IBN HACHMI Nada


Année scolaire 2012-2013

# Plan

- Présentation générale
  - Présentation de l'entreprise
  - Contexte et objectifs du projet
  - Présentation des normes
- Organisation
  - Organisation de l'équipe projet
  - Macro planning
  - Analyse des risques
- Résultats
  - Application
  - Comparaison des résultats et des normes
- Conclusion et perspectives

# Présentation de l'entreprise

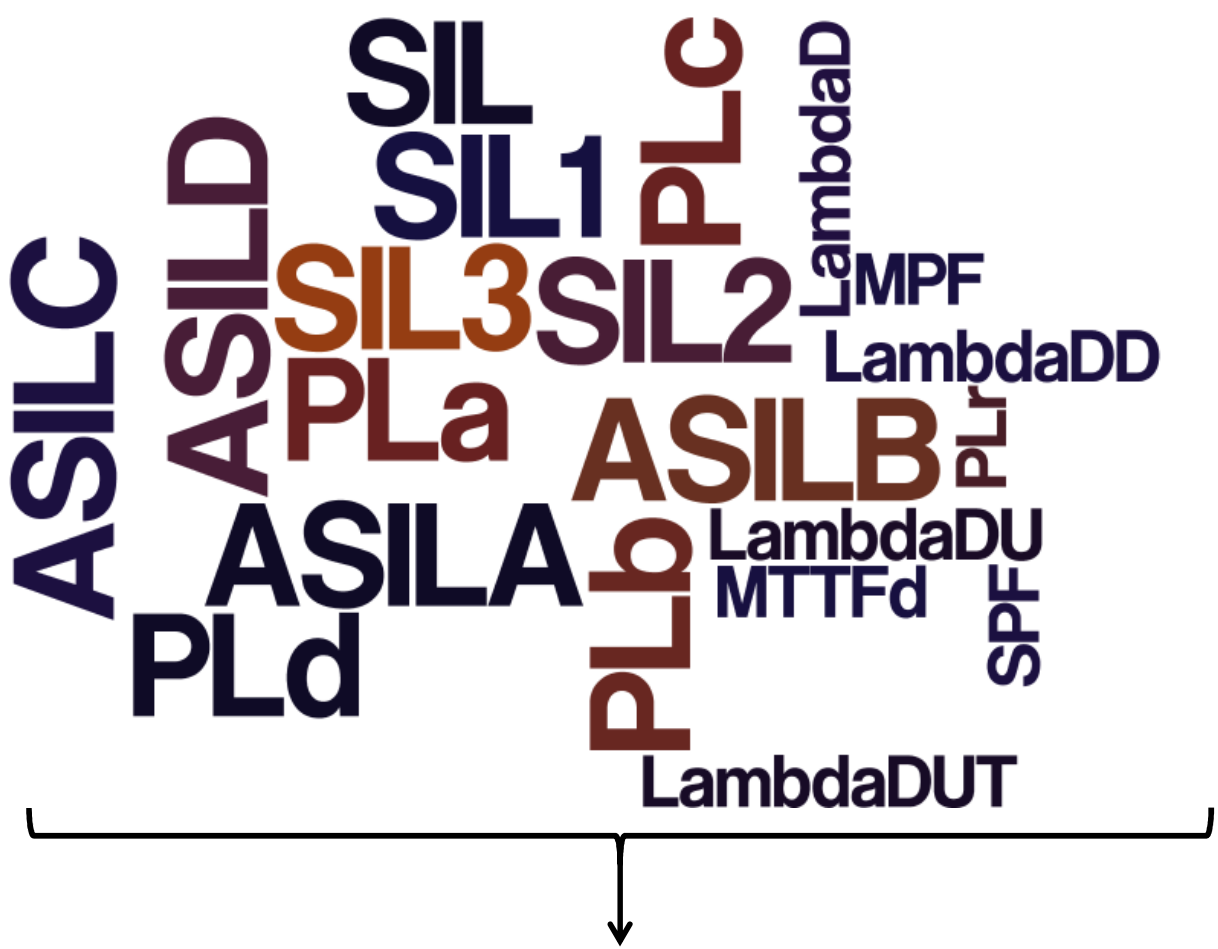
- Expertise et Conseil en Sûreté de Fonctionnement
- Formation en Sûreté de Fonctionnement et en Qualité
- Aide au pilotage par les risques
- Audit et Accompagnement de projets à forte criticité
- Sécurité des systèmes d'informations

# Contexte et objectifs

ISO 26262

ISO 13849

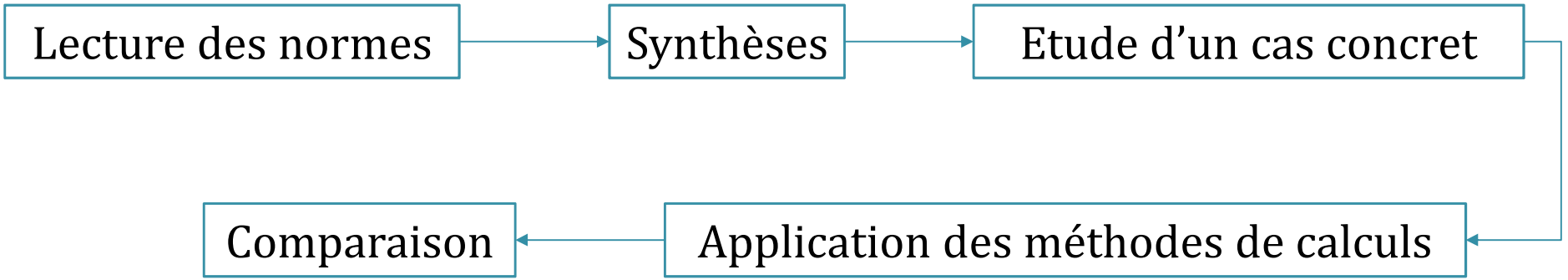
CEI 61508




Quelles différences ?!

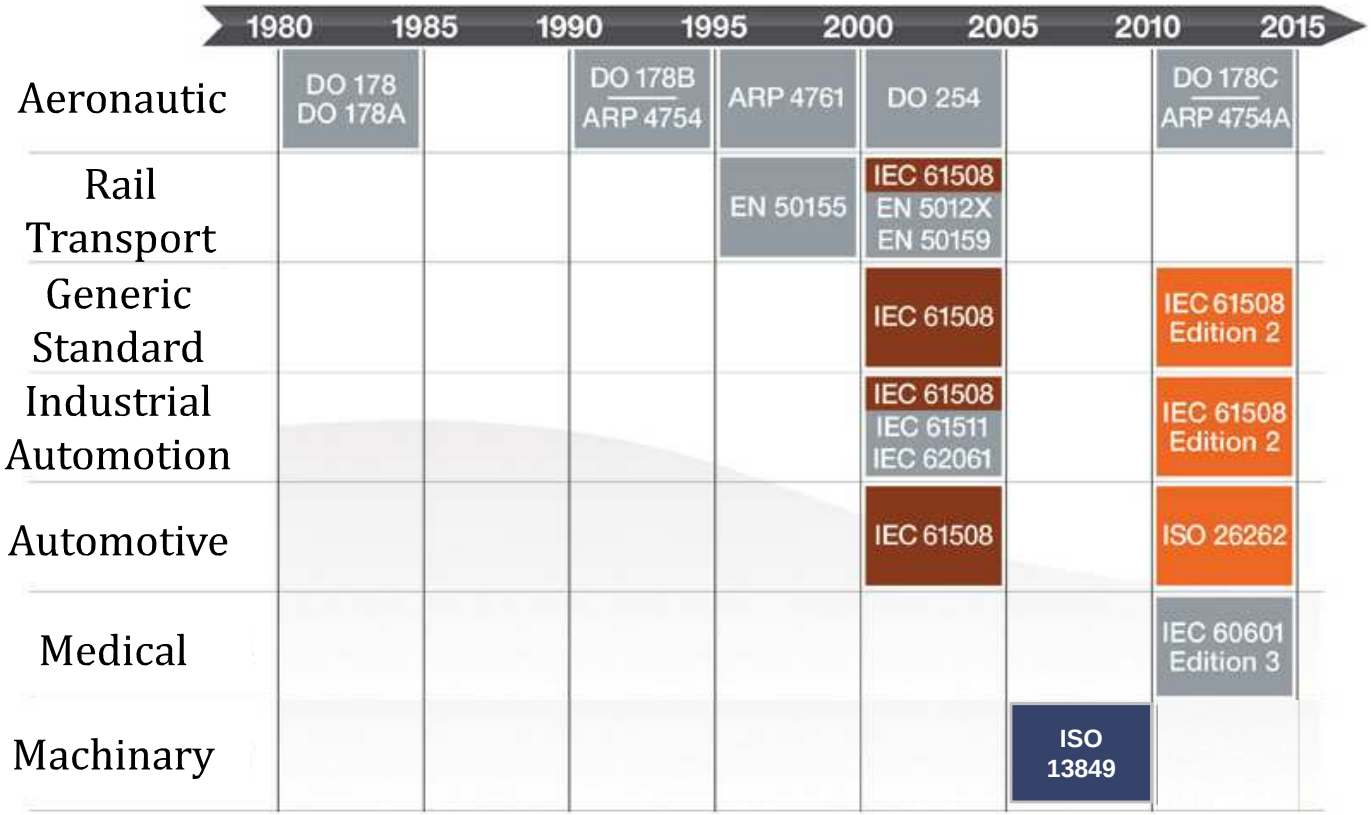
# Contexte et objectifs

**Synthèse des objectifs :**




- Différences entre les normes
- Controverses sur certains principes de calculs

# Présentation des normes en sécurité fonctionnelle




**Source: Freescale products developed to target IEC 61508 , ISO 26262, 13849**

# CEI 61508

## Objectifs

- Elaboration d'une norme spécifique à chaque domaine d'application
- Développement de systèmes E/E/PE relatifs à la sécurité

## Cadre d'application

- Sécurité fonctionnelle E/E/PE relatifs à la sécurité
- Si pas de normes pour cette application

## CEI 61508

## Métriques

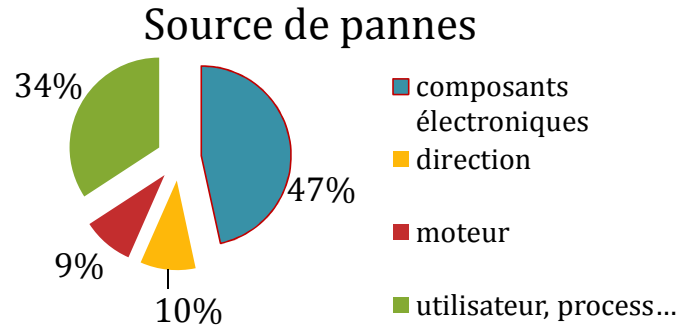
- Echelle **SIL** de 1 à 4
- Métriques pour l'évaluation du SIL
  - PFD: Faible sollicitation
  - PFH: Forte sollicitation
  - SFF: Contrainte architecturale

## Approche

- Toutes les activités liées au cycle de vie de sécurité des systèmes

# ISO 26262

## Problématique




Enquête publiée en 2008 dans le magazine de consommation «Que Choisir»

## Cadre d'application

- Sécurité fonctionnelle des Systèmes:
  Electriques /Electroniques
- Analyse des risques/ fonctions sécuritaires
- Voie de développement (Matérielle/logicielle)

## ISO 26262

## Métriques

- Echelle **ASIL** de A à D pour la(s) fonction(s)
- Métriques:
  - Probability of violation of safety goals (PVSG)
  - Single Point Fault Metric (SPF)
  - Latent Fault Metric (MPF)

## Apports

- La voiture de demain sera (encore) plus fiable !

# ISO 13849 - 1

## Objectifs

- Exigences de sécurité
- Conseils relatifs aux principes de conception
- Sécurité des machines

## Cadre d'application

- Domaine d'application très large
- Electricité/hydraulique /pneumatique/mécanique

## ISO 13849 - 1

## Métriques

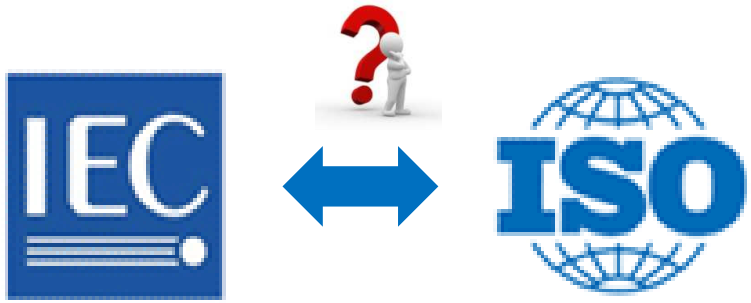
- Echelle **PL** de a à e
- Métriques:
  - Niveau de performance requis PLr
  - Mean Time To Failure dangerous
  - Couverture du diagnostic
  - Architectures désignées

## Apports

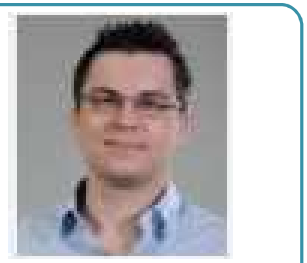
- Approche probabiliste prise en compte dans l'évaluation des systèmes de commande de sécurité

# Problématique

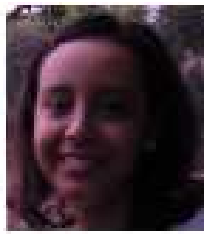
Les différentes métriques et méthodes de calculs traduisent-elles des différences fondamentales entre les normes, ou s'agit- il d'une adaptation aux secteurs d'activités concernés?



# Organisation de l'équipe projet


CEI 61508

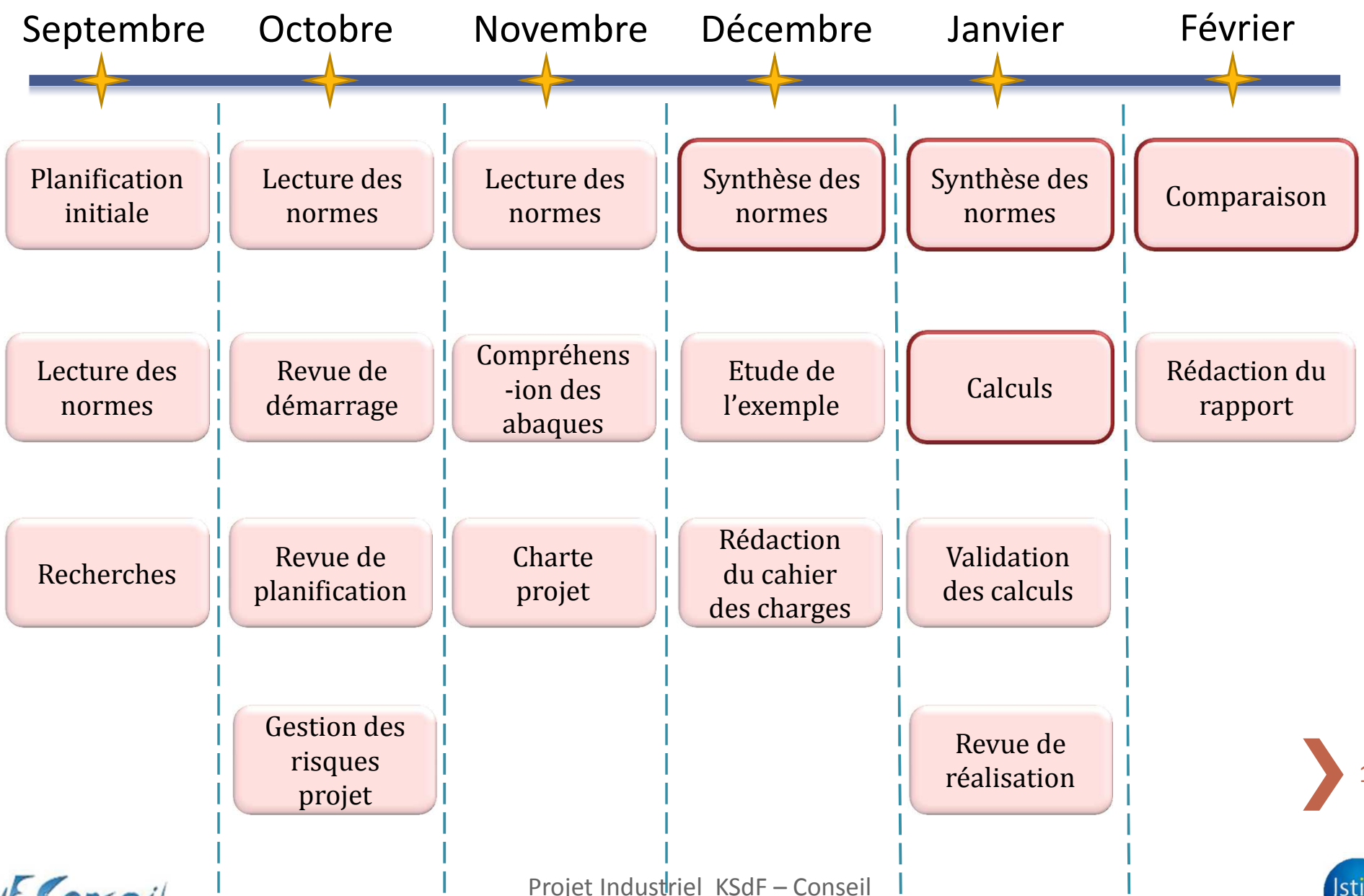

CEI 61508


ISO 26262


ISO 13849

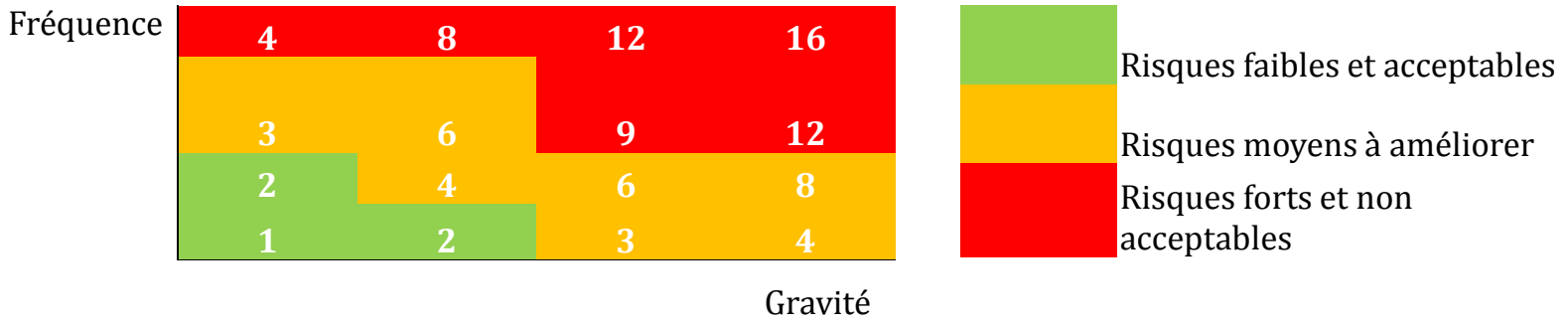
| | |
|---|---|
| **I- Synthèse de la norme** | **Lecture** |
| | **Rédaction du rapport** |
| **II- Traitement de l'exemple de l'ISO 26262 par la CEI 61508 et l'ISO 13849** | **Réalisation des calculs** |
| | **Interprétation des résultats** |
| **III- Comparaison entre cette norme et les autres normes** | |

# Macro planning

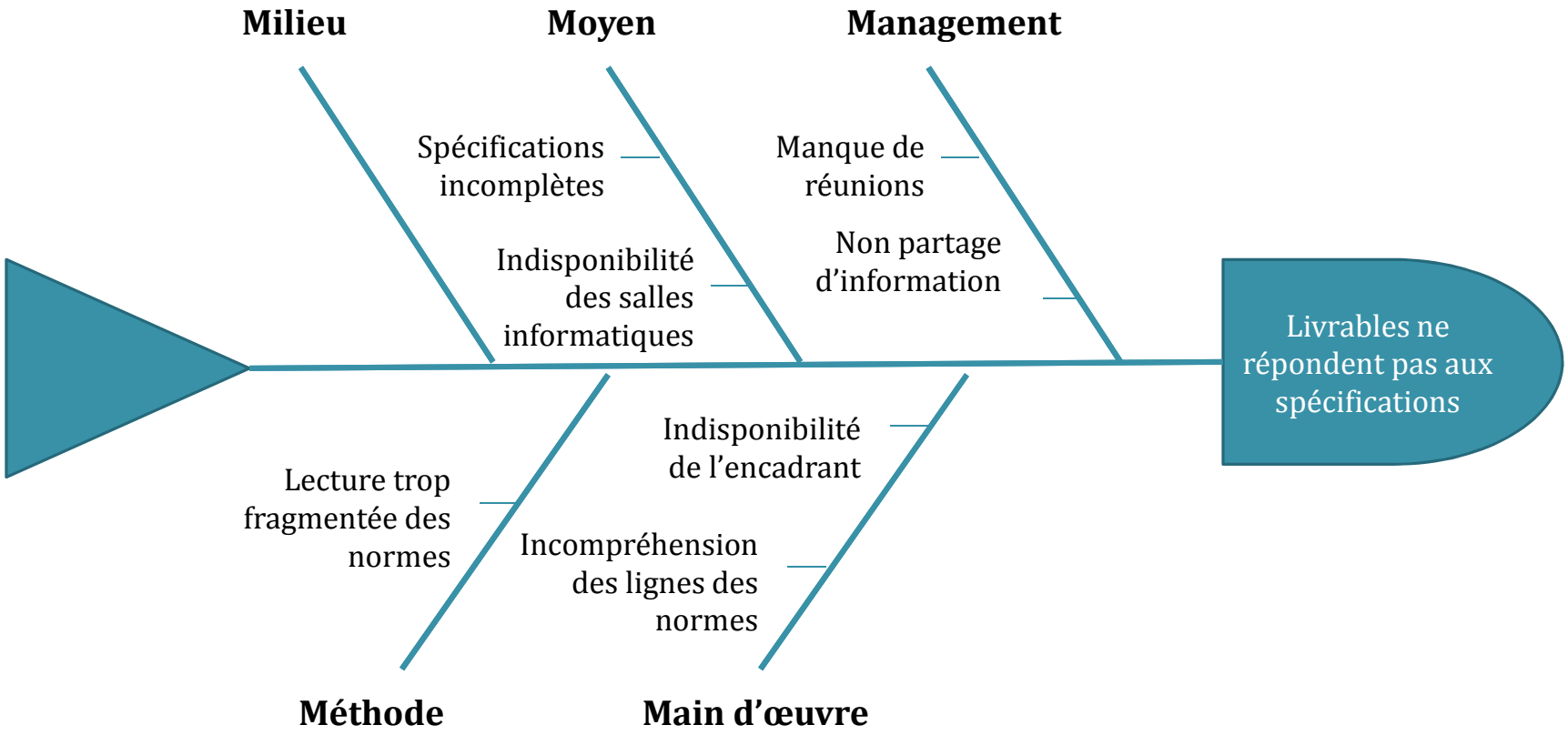


# Analyse des risques

| Risques | Effets | Gravité | Fréquence | Criticité =G*P |
|---|---|---|---|---|
| **Inaccomplissement du projet dans le délai prévu** | Retard sur le planning, surcharge et dépassement du délai fixé | 4 | 1 | 4 |
| **Indisponibilité du tuteur du projet** | Manque d'information et retard | 3 | 3 | 9 |
| **Manque de communication entre les membres du groupe** | Retard + Mauvaise qualité du travail élaboré | 4 | 2 | 8 |
| **Manque de ressources : Calcul de probabilités pour l'AMDEC** | Impossibilité de comparer les résultats entre les normes | 4 | 2 | 8 |
| **Incompréhension des objectifs fixés du projet** | Livrables ne répondent pas aux spécifications | 4 | 4 | 16 |
| **Absentéisme des membres du groupe** | Surcharge des ressources présentes | 3 | 2 | 6 |
| **Mauvaise organisation et répartition des tâches** | Surcharge des ressources | 3 | 2 | 6 |
| **Non-respect des objectifs pour les livrables** | Insatisfaction du tuteur entreprise | 4 | 1 | 4 |
| **Ne pas réussir à faire une comparaison** | Impossibilité de rédiger les livrables | 4 | 3 | 12 |
| **Pas d'exemple concret à modéliser** | Ne pas être en mesure de fournir un standard de calcul | 4 | 2 | 8 |



# Diagramme ISHIKAWA



# Application

**Exemple tiré de l'ISO 26262 :**

Circuit électronique de contrôle de la vanne EGR (Exhaust Gas Recirculation)

» L'EGR en bref :
- Système créé dans les années 70
- Constitué d'une vanne et d'un échangeur thermique

» Son rôle :
- Diminuer la T de combustion
- Diminuer le rejet de NOX

Vanne EGR Opel 2.2 DTI

# Application

Le système est composé de **deux fonctions** :

Fonction 1 : « Vitesse du véhicule »

**Etat sûr** → **Vanne 1 ouverte**

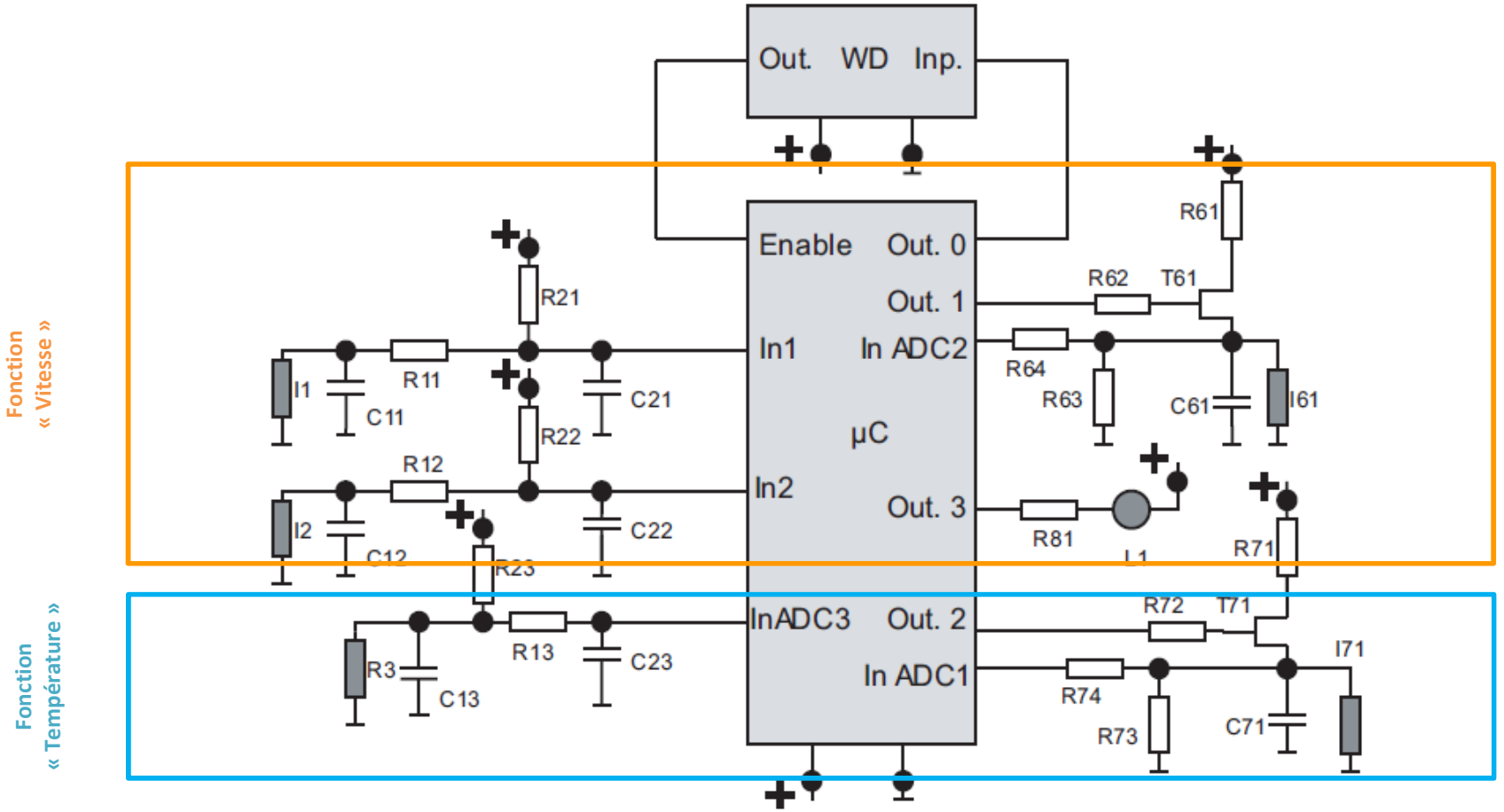
- 2 entrées : Vitesse captée par I1 et I2
- Utilisation de la moyenne des résultats (sinon ouverture vanne 1)
- Sortie sur I61
- Ouverture de la vanne si V > 90 km/h

Fonction 2 : « Température »

**Etat sûr** → **Vanne 2 ouverte**

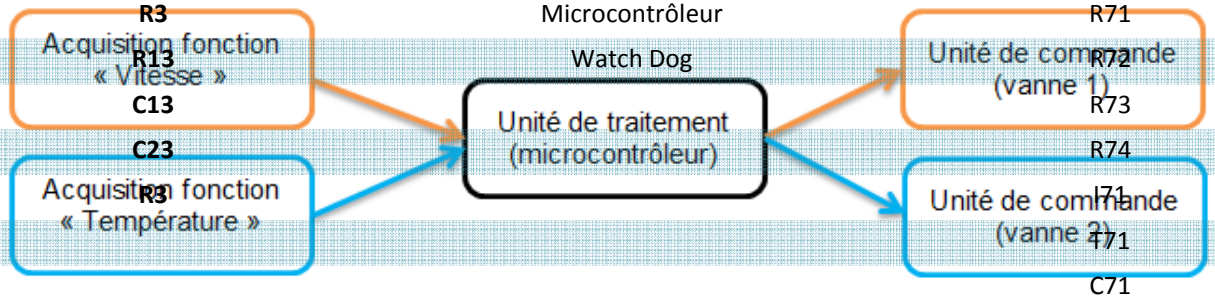
- 1 entrée : Température mesurée par R3
- Sortie sur I71
- Ouverture de la vanne si T > 90 C

# Application



# Application par la CEI 61508

» Approche découpage par fonction




| Acquisition | Microcontrôleur + WD | Commande |
|---|---|---|
| **Fonction « Pilotage de la température »** | | |
| **R3** | Microcontrôleur | R71 |
| **R13** | Watch Dog | R72 |
| **C13** | | R73 |
| **C23** | | R74 |
| **R3** | | I71 |
| | | T71 |
| | | C71 |
| **Fonction « Pilotage de la vitesse »** | | |
| **I1** | Microcontrôleur | R61 |
| **I2** | Watch Dog | R62 |
| **C11** | | R63 |
| **C12** | | R64 |
| **C21** | | T61 |
| **C22** | | I61 |
| **R11** | | C61 |
| **R12** | | |
| **R21** | | |
| **R22** | | |

# Application par la CEI 61508

» Sur un composant

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| C21 | 2 | YES | open | 20 % | | SM2 | |
| | | | closed | 80 % | X | | 99 % |

| Composant | λ | Mode de défaillance | Distribution | DC | $\lambda_{DU}$ | $\lambda_{DD}$ | $\lambda_S$ |
|---|---|---|---|---|---|---|---|
| C21 | 2 E -09 | Open | 20% | | | | 4 E-10 |
| | | Closed | 80% | 99% | 1,6 E-11 | 1,584 E-09 | |

$$\lambda_D = \sum \lambda_{DU} + \sum \lambda_{DD}$$

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$$

$$SFF = \frac{\sum \lambda - \sum \lambda_{DU}}{\sum \lambda}$$

# Application par la CEI 61508

» Unité d'acquisition

**Unité d'acquisition**

| Composant | λ | Mode de défaillance | Distribution | DC | λUD | λDD | λS |
|---|---|---|---|---|---|---|---|
| R3 | 3E-09 | open | 30% | 0% | 9E-10 | 0 | |
| | | closed | 10% | | | | 1,2E-09 |
| | | drift 0,5 | 30% | | | | |
| | | drift 2 | 30% | 0% | 9E-10 | 0 | |
| C13 | 2E-09 | closed | 80% | | | | 1,6E-09 |
| | | open | 20% | 0% | 4E-10 | 0 | |
| R23 | 2E-09 | open | 90% | | | | 1,8E-09 |
| | | closed | 10% | 0% | 2E-10 | 0 | |
| R13 | 2E-09 | open | 90% | 0% | 1,8E-09 | 0 | |
| | | closed | 10% | 0% | 2E-10 | 0 | |
| C23 | 2E-09 | Ce composant n'intervient pas dans la fonction de sécurité | | | | | 2E-09 |

Le mode de défaillance n'est pas considérée comme "sécuritaire".

| | |
|---|---|
| λD = | 4,40E-09 |
| DC = | 0% |
| SFF = | 60% |
| PFH = | 4,40E-09 |

$$\lambda_D = \sum \lambda_{DU} + \sum \lambda_{DD}$$

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$$

$$SFF = \frac{\sum \lambda - \sum \lambda_{DU}}{\sum \lambda}$$

$$PFH = \lambda_{DU}$$

# Application par la CEI 61508

» Niveau de SIL

PFH

| Niveau d'intégrité de sécurité (SIL) | Mode de fonctionnement continu ou à forte sollicitation (PFH) |
|---|---|
| 4 | $\geq 10^{-9}$ à $< 10^{-8}$ |
| 3 | $\geq 10^{-8}$ à $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ à $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ à $< 10^{-5}$ |

SFF (type A)

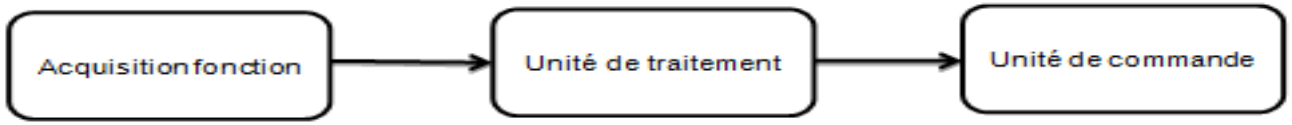
| Proportion de défaillances en sécurité (SFF) | Tolérance aux anomalies matérielles | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | SIL 1 | SIL 2 | SIL 3 |
| 60 % - < 90 % | SIL 2 | SIL 3 | SIL 4 |
| 90 % - < 99 % | SIL 3 | SIL 4 | SIL 4 |
| >= 99 % | SIL 3 | SIL 4 | SIL 4 |
| Un SIS peut être considéré du type A si son comportement en présence d'anomalies est bien déterminé, si les modes de défaillance de ses constituants sont bien définis et si les données concernant leurs défaillances, issues du retour d'expérience, sont connues avec une bonne fiabilité. | | | |

Niveau de SIL par fonction

| Métriques considérées | Acquisition | Microcontrôleur + WD | Commande | SIL retenue pour les fonctions |
|---|---|---|---|---|
| | Fonction « Pilotage de la température » | | | |
| SFF | SIL 2 | SIL 2 | SIL 3 | SIL 2 |
| PFH | SIL 4 | | | |
| | Fonction « Pilotage de la vitesse » | | | |
| SFF | SIL 4 | SIL 3 | SIL 3 | SIL 3 |
| PFH | SIL 4 | | | |

# Application par la CEI 61508

» Approche découpage par bloc




| Acquisition | Microcontrôleur + WD | Commande |
|---|---|---|
| I1 | Microcontrôleur | R61 |
| C11 | Watch Dog | R62 |
| R11 | | R63 |
| R21 | | R64 |
| C21 | | C61 |
| I2 | | I61 |
| C12 | | T61 |
| R12 | | R71 |
| R22 | | R72 |
| C22 | | R73 |
| R3 | | R74 |
| C13 | | C71 |
| R13 | | I71 |
| R23 | | T71 |
| C23 | | R81 |
| | | L1 |

Niveau de SIL du système

| Métriques considérées | Acquisition | Microcontrôleur + WD | Commande | SIL retenue pour les fonctions |
|---|---|---|---|---|
| SFF | SIL 2 | SIL 3 | SIL 4 | SIL 2 |
| PFH | SIL 4 | | | |

# Application par l'ISO 26262

| Composant | Taux défaillance (1/h) | Participation à la fonction | Mode de défaillance | | Violation de l'objectif de sécurité sans SM | SM | Taux de couverture | SPF | MPF |
|---|---|---|---|---|---|---|---|---|---|
| C13 | 2*10^-7 | oui | ouvert | 20% | X | AUCUN | 0% | =0,4 (20*2)/100 | |
| | | | fermé | 80% | | | | | |
| T71 | 5*10^-7 | oui | ouvert | 50% | | SM1 | | =0,25 (100-90)*50*5)/10^4 | =0,45 |
| | | | fermé | 50% | X | | 90% | | |

Σ Taux participant à la fonction

Σ λ SPF  Σ λMPF

SPF %=1-(Σ λ SPF/ Σ Taux)

MPF %= 1-(Σ λMPF/ Σ Taux-Σ λ SPF)

# Application par l'ISO 26262

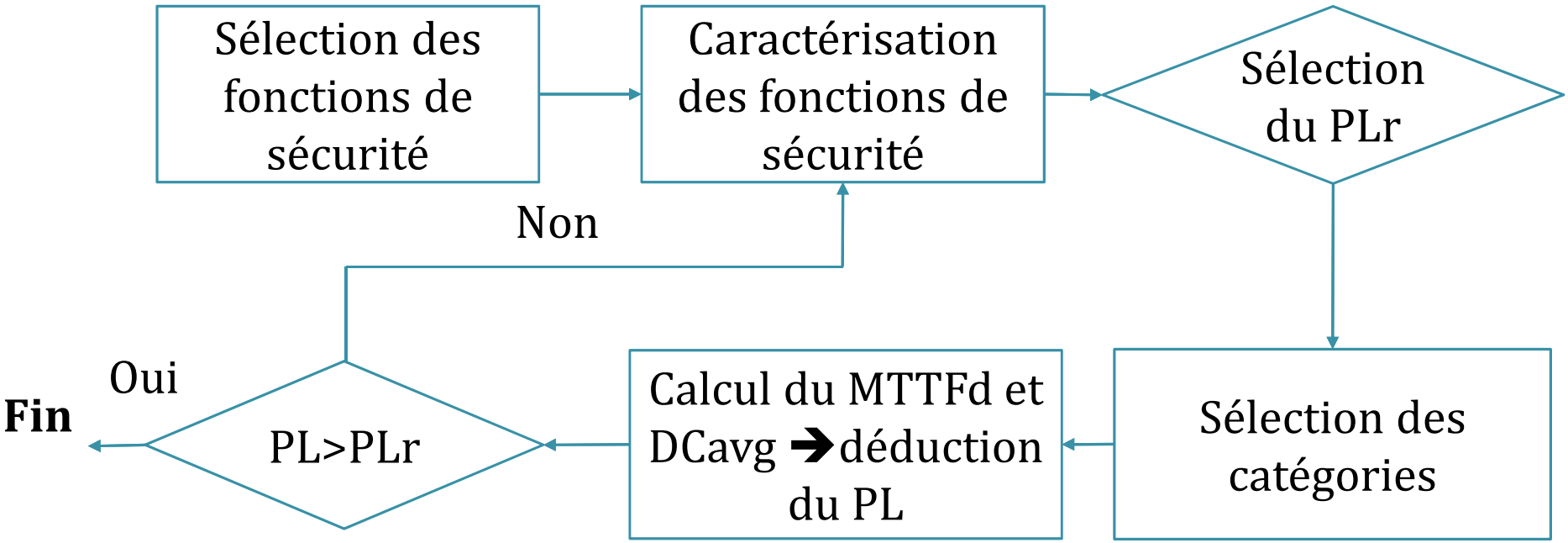
Fonction 2 (SPF= 93,2%; MPF= 90%)

| | ASIL B | ASIL C | ASIL D |
|---|---|---|---|
| PVSG (1/h) | 10^-7 | 10^-7 | 10^-8 |
| SPF | ≥90% | ≥97% | ≥99% |
| MPF | ≥ 60% | ≥80% | ≥90% |

Fonction 2: ASILC

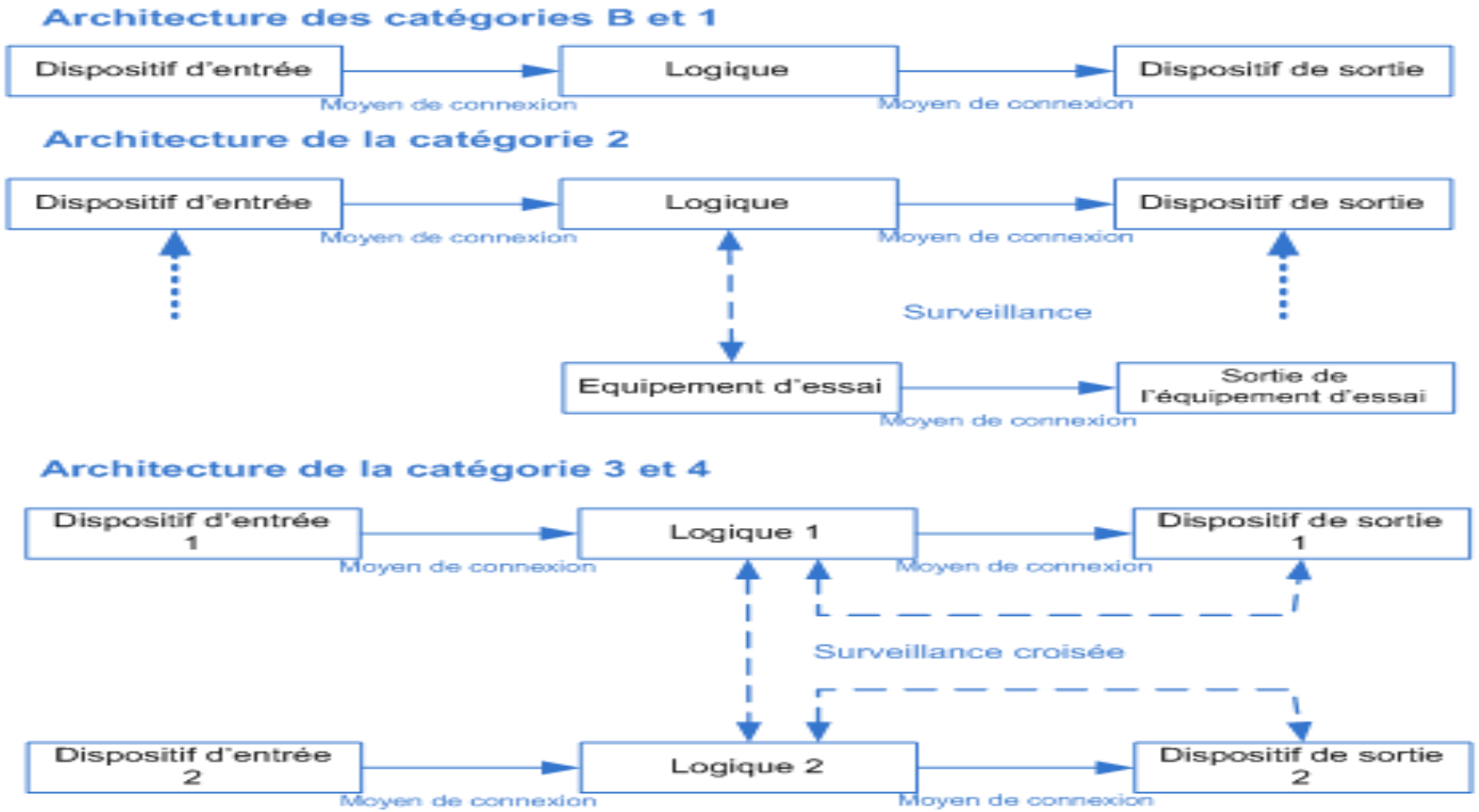
# Application par l'ISO 13849-1

» Approche :



# Application par l'ISO 13849-1

- Pour les deux fonctions on a un PLr d
- Sélection des catégories :



# Application par l'ISO 13849-1

» Calcul du MTTFd:

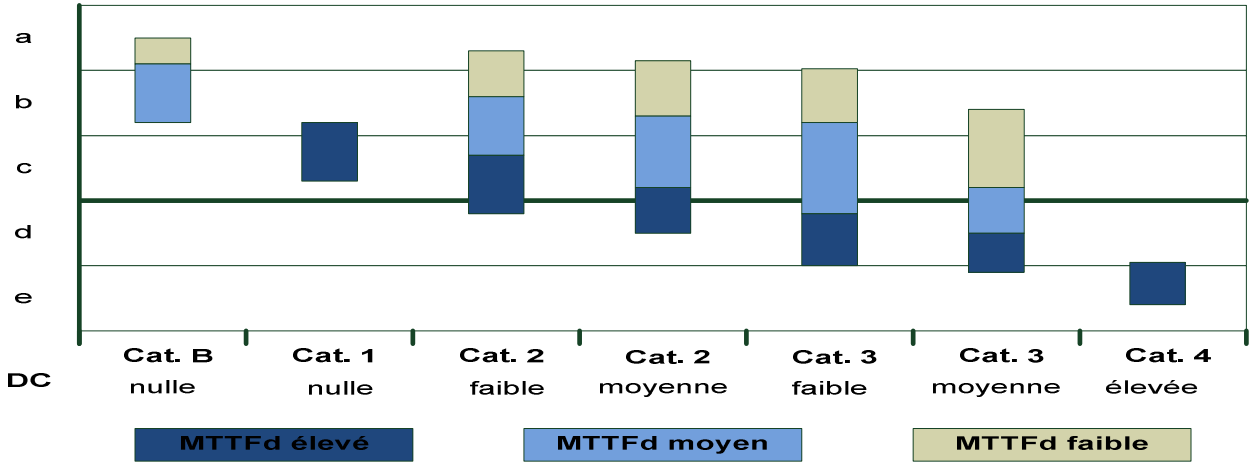
| MTTFd | |
|---|---|
| Indice pour chaque canal | Gamme pour chaque canal |
| Faible | 3 ans < MTTFd ≤ 10 ans |
| Moyen | 10 ans < MTTFd ≤ 30 ans |
| Elevé | 30 ans < MTTFd ≤ 100 ans |

» Calcul du DCavg:

| DCavg | |
|---|---|
| Indice | $DCavg = \frac{\sum Dci/MTTFdi}{\sum 1/MTTFdi}$ Gamme |
| Nulle | DC < 60% |
| Faible | 60% ≤ DC <90% |
| Moyen | 90% ≤ DC <99% |
| Elevé | 99% ≤ DC |

# Application par l'ISO 13849-1

» Détermination du PL:




Les fonctions pilotage de la température et de la vitesse ont un PL c

# Comparaison

**Niveau technologie**

- CEI 61508: Electrique / Electronique / Electronique Programmable
- ISO 13849-1 : Hydraulique/ Pneumatique/ Electromécanique/ Electronique Complexe
- ISO26262: Electrique / Electronique

**Niveau exigence**

- Architecture de découpage du système
- Métriques et niveaux d'intégrité (PFH, SPF, MTTFd, SIL, ASIL, PL, …)

# Comparaison

» Tableau d'équivalence :

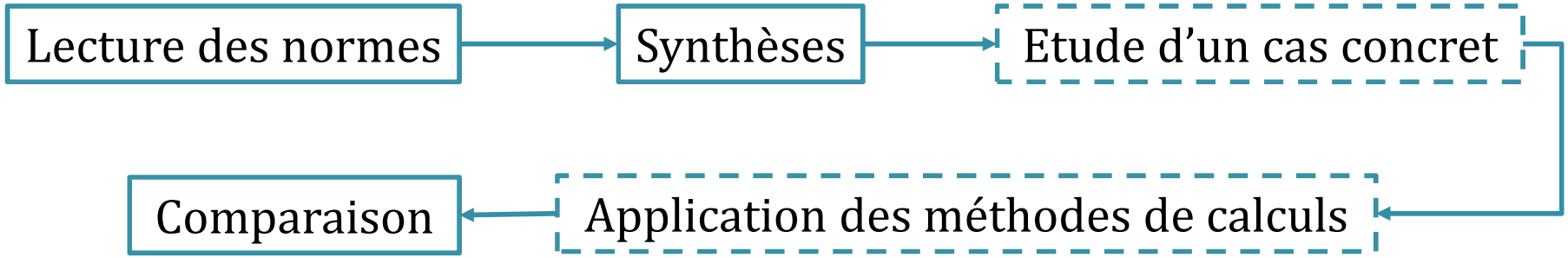
| CEI 61508 | ISO 26262 | ISO 13849-1 |
|---|---|---|
| | | PL a |
| SIL1 | ASIL A | PLb<br>PLc |
| SIL2 | ASIL B<br>ASIL C | PLd |
| SIL3 | ASIL D | PLe |
| SIL4 | | |

» Comparaison des résultats trouvés:

| Normes | Niveau obtenu | | Equivalence |
|---|---|---|---|
| ISO 13849 | PL=c | ⇒ | SIL 1 |
| CEI 61508 | SIL 2 | ⇒ | SIL 2 |
| ISO 26262 | ASIL B | ⇒ | SIL 2 |

# Conclusion et perspectives

**Bilan du projet :**



# Conclusion et perspectives

**Bilan personnel :**

**Points positifs :** 

- Découverte de 3 référentiels métiers
- Travail de groupe
- Application sur un exemple

**Points négatifs :** 

- Lecture parfois fastidieuse
- Durée du projet courte
- Travail à l'ISTIA

**Connaissances en Sûreté de Fonctionnement**

# Conclusion et perspectives

**Perspectives :**

» Reprendre le travail engagé

» Appliquer les directives des normes sur un exemple plus complexe

» Utiliser un logiciel spécialisé

» Elargir l'étude et la comparaison aux autres parties des normes

» Analyser et comparer les recommandations

# MERCI POUR VOTRE ATTENTION

## Des questions ?