MASTER OF SCIENCE
IN ENGINEERING

Sécurité et fiabilité des systèmes (SECU)

# 01 – Introduction au risque, à la sécurité et à la fiabilité

Eric Silva
27.09.2021

# Langue du cours ?

Français ?

Anglais ?

Si le français n’est pas votre langue maternelle et que vous êtes plus à l’aise en anglais vous pouvez:

- Poser vos questions en anglais, j’y répondrai en anglais + français
- Rendre vos travaux en anglais et les présenter en anglais à la classe

Je parle aussi espagnol si nécessaire.

# Détails et administration:

**Moodle ->** Est-ce que tout le monde a accès ?

https://moodle.msengineering.ch/course/view.php?id=1769

**Teams ->** Est-ce que tout le monde a accès ?

https://teams.microsoft.com/l/channel/19%3aH9w9dL1diLkvpUmZcesJb-WOfmJ4duUw31emLR5xm5k1%40thread.tacv2/G%25C3%25A9n%25C3%25A9ral?groupId=82c33f70-ab4c-4f77-8d78-579ed338878f&tenantId=a372f724-c0b2-4ea0-abfb-0eb8c6f84e40

**Email ->** Est-ce que tout le monde a reçu mon email avec les détails du cours ?

Ceux qui n'ont pas accès à l'un ou l'autre des services m'écrire à -> eric.silva@hefr.ch

# Les intervenants

**Eric Silva**

Deputy Director ROSAS Center Fribourg
Enseignant HEIA-FR, genie électrique
Email: eric.silva@hefr.ch

**Wolfgang Berns**

Director ROSAS Center Fribourg
Professeur HEIA-FR, génie électrique
Email: wolfgang.berns@hefr.ch

**Vincent Robatel**

Head of Model-based Engineering
Email: vincent.robatel@hefr.ch

**Jonathan Hendriks**

System Engineer
Email: jonathan.hendriks@hefr.ch

**Frédéric Schenker**

System Engineer
Email: frederic.shenker@hefr.ch

# Quelques mots sur moi:

**Eric Silva**

**Origine et études:** Fribourg

**Sports:** Football, Futsal

**Pourquoi suis-je ici devant vous aujourd'hui?**

- En 2014 j'ai participé à la fondation du centre de compétence ROSAS
- Durant 6 ans, j'ai pu travailler dans différents domaines afin d'aider les entreprises à atteindre leurs objectifs de sécurité
- Depuis 2018 je forme les professionnels sur les normes de sécurité

**Deux moments clés de mon parcours**:

- Evaluation et modification du SW de gestion des sondes de température sur l'entrée des réacteurs pour Rolls-Royce - durant 1 an
- Création, lancement de CertX SA, obtention de l'accréditation pour la certification des produits dans les domaines: Automobile, Machinerie, Ferroviaire, Cybersécurité.

# Mon parcours

**Etudes:**

- 2014 -> Bachelor en Télécommunication à la HEIA-FR
- 2017 -> Master MSE en systèmes embarqués et mobiles (TIC)
- 2021 -> Executive Master in Business Administration (EMBA) à la HEG-FR

**Parcours professionnel:**

- 2014-2018 -> Ingénieur en sécurité à ROSAS Center Fribourg (Machinerie)
- 2018-20.. -> Auditeur responsable machinerie chez CertX SA
- 2018-20.. -> Chargé de cours à la HEIA-FR
- 2020 -> Certified Machinery Safety Expert (CMSE – TÜV Nord)
- 2020-20.. -> Directeur adjoint de ROSAS Center Fribourg

**Normalisation:**

- Expert dans le «TC 65» pour le développement des normes IEC pour la sécurité fonctionnelle dans le domaine des machines industrielles (IEC 61508, IEC 62061…)

# La plus grosse formation ISO 26262 au monde

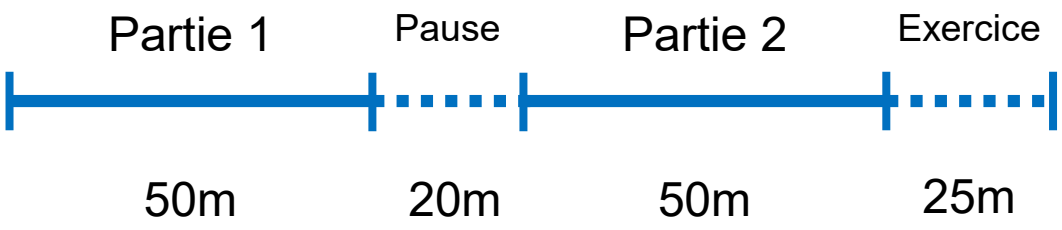
Janvier 2020, 1 semaine à Tianjin (CN), 150 participants, Traduction en direct par deux interprètes chinois

**Pour CertX je donne les formation de certification selon les normes:**
ISO 26262 (Automobile) – IEC 61508 (Sécurité fonctionnelle) – ISO 13849 (Sécurité des Machines) – IEC 62061 (Sécurité des machines)

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | xx.01.2022 | Examen écrit | |
| Total | **42** | | | |

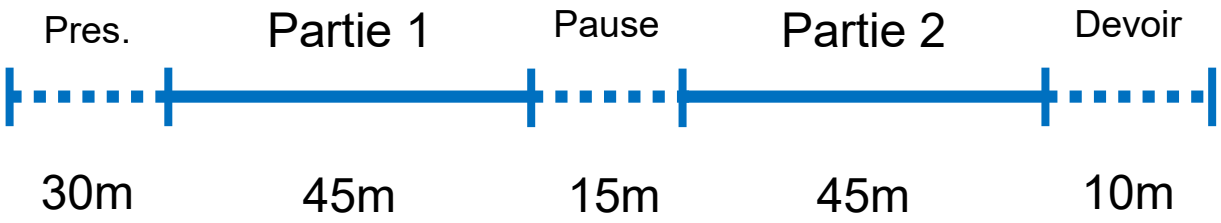
# Format du cours (aujourd'hui)




**Structure du cours:**

17h30: Début du cours
18h20: Pause de 20min
18h40: Reprise
19h30: Temps à disposition pour débuter les exercices

# Format du cours (à partir de la semaine prochaine)




**Structure du cours:**

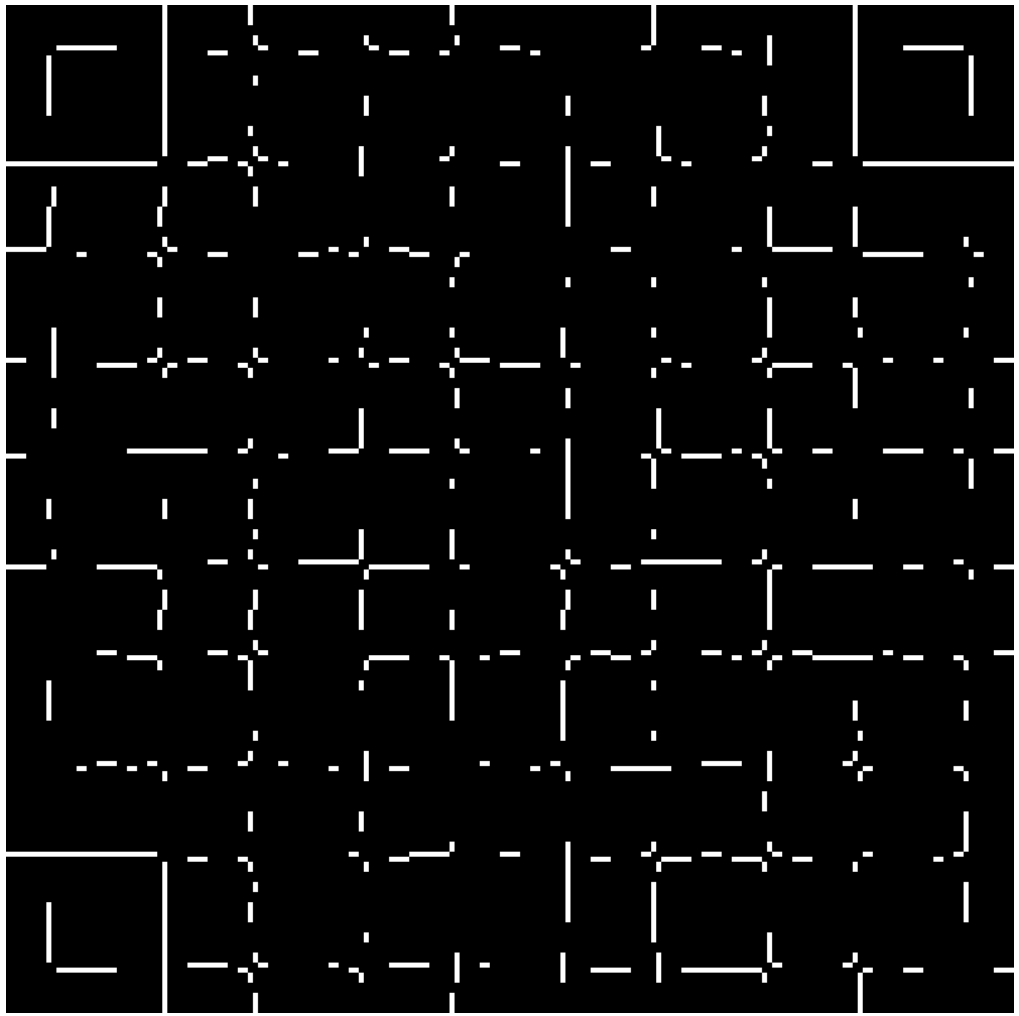
17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Sondage, ce que vous attendez de ce cours

Petit sondage afin de savoir:

- Votre filière d'étude Bachelor
- Votre filière d'étude Master
- Votre lieu de résidence (pas précisément, servira de référence pour les travaux si nécessire)
- Ce que vous attendez du cours
- Ce que veut dire la sécurité des machines pour vous.

https://forms.office.com/r/Fx8j0T0qhk



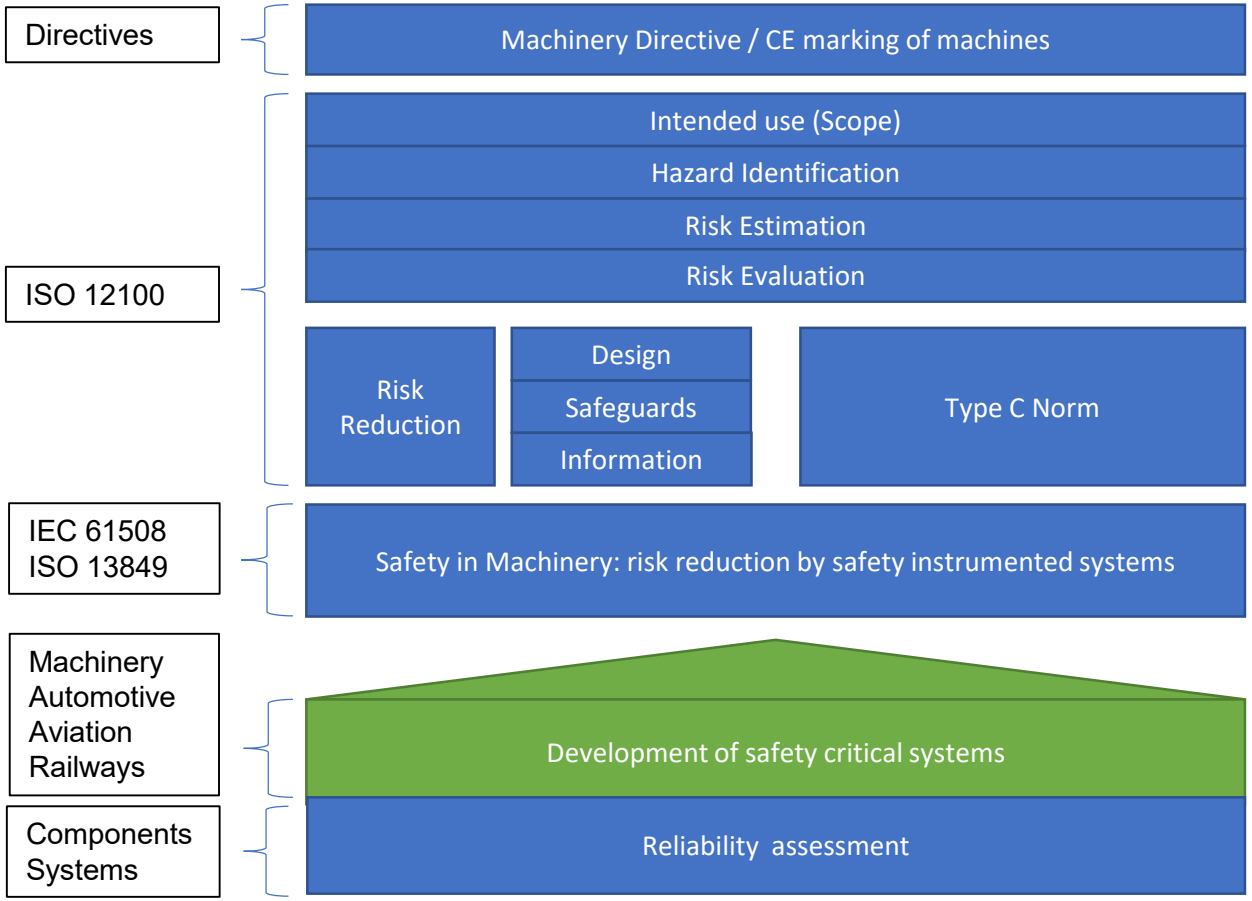
# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

# Structure des différents cours



Source: Contrinex

Cours SRE : Safety and Reliability Engineering (Bachelor - HEIA-FR, Génie électrique, Fribourg)

Cours SecuFS : **Sécurité et Automation (Master – HES-SO, MSE MA, Lausanne)**

# Déroulement du cours

**27.09.2021 Introduction au risque, à la sécurité et à la fiabilité**

- Cours - aperçu, intervenants, déroulement, échéancier
- Risque, sécurité et fiabilité en général

**04.10.2021 Sécurité des systèmes techniques - management des risques**

- Marquage CE - directives applicables
- Directives 2006/42/EC Directive Machines
- Aperçu des normes Type A, B, C
- Normes harmonisées et des normes applicables
- Safe by design, protecteurs, équipements de protection, composants de sécurité
- Causes primaires et secondaires d'accident

# Déroulement du cours

**11.10.2021 Analyse des risques selon la norme ISO 12100**

- Appréciation du risque
- Analyse de risque selon ISO12100
  - Détermination des limites
  - Identification des phénomènes dangereux
  - Estimation du risque
  - Évaluation du risque
  - Documentation
  - Matrice des risques, graphique des risques

**18.10.2021 Workshop «analyse de risque»**

# Déroulement du cours

**25.10.2021 Sécurité des systèmes techniques - sélection de la réduction du risque**

- Modification du système, mesure de protection ou information
- Hiérarchie des contrôles
- Protections Mécaniques
  - Normes de protection mécanique
  - Types de protecteurs
  - Distances de sécurité
  - Bonnes pratiques

**01.11.2021 Sécurité des systèmes techniques - composants de sécurité**

- Dispositifs de protection
- Arrêts d'urgence
- Systèmes de commande de sécurité et actionneurs
- Sélection des composants de sécurité et introduction aux standards de sécurité fonctionnelle

**08.11.2021 Workshop ISO13849 et IEC61508**

# Déroulement du cours

**15.11.2021 Processus de développement des systèmes techniques – Partie 1**

- Cette partie vise à introduire les aspects relatifs à l'ingénierie des systèmes ainsi que les processus de développement de base.

**22.11.2021 Processus de développement des systèmes techniques – Partie 2**

- Dans cette partie, nous allons transposer les concepts de l'ingénierie système sur la base de modèle. L'ingénierie des systèmes basée sur les modèles (MBSE) et le "système thinking" sont des approches de plus en plus répendues au niveau industriel.

**29.11.2021 Workshop «Développement des systèmes techniques»**

- Le workshop servira à appliquer les concepts vu lors des deux cours précédents. Nous allons appliquer cela sur un cas concret : le tensiomètre de bras

# Déroulement du cours

**06.12.2021** **Fiabilité des composants**

- Taux de défaillance
- Mean Time to Failure - MTTF, MTBF
- Probabilité de défaillance et probabilité de succès
- Fonctions de répartition

**13.12.2021** **Fiabilité des systèmes**

- Aperçu des analyses
- Modèle sériel - analyse quantitative
- Modèle parallèle - analyse quantitative
- Exemples

**20.12.2021** **Récapitulatif du cours**

**10.01.2021** **Date de réserve**

# Visite d’entreprises et intervenants:

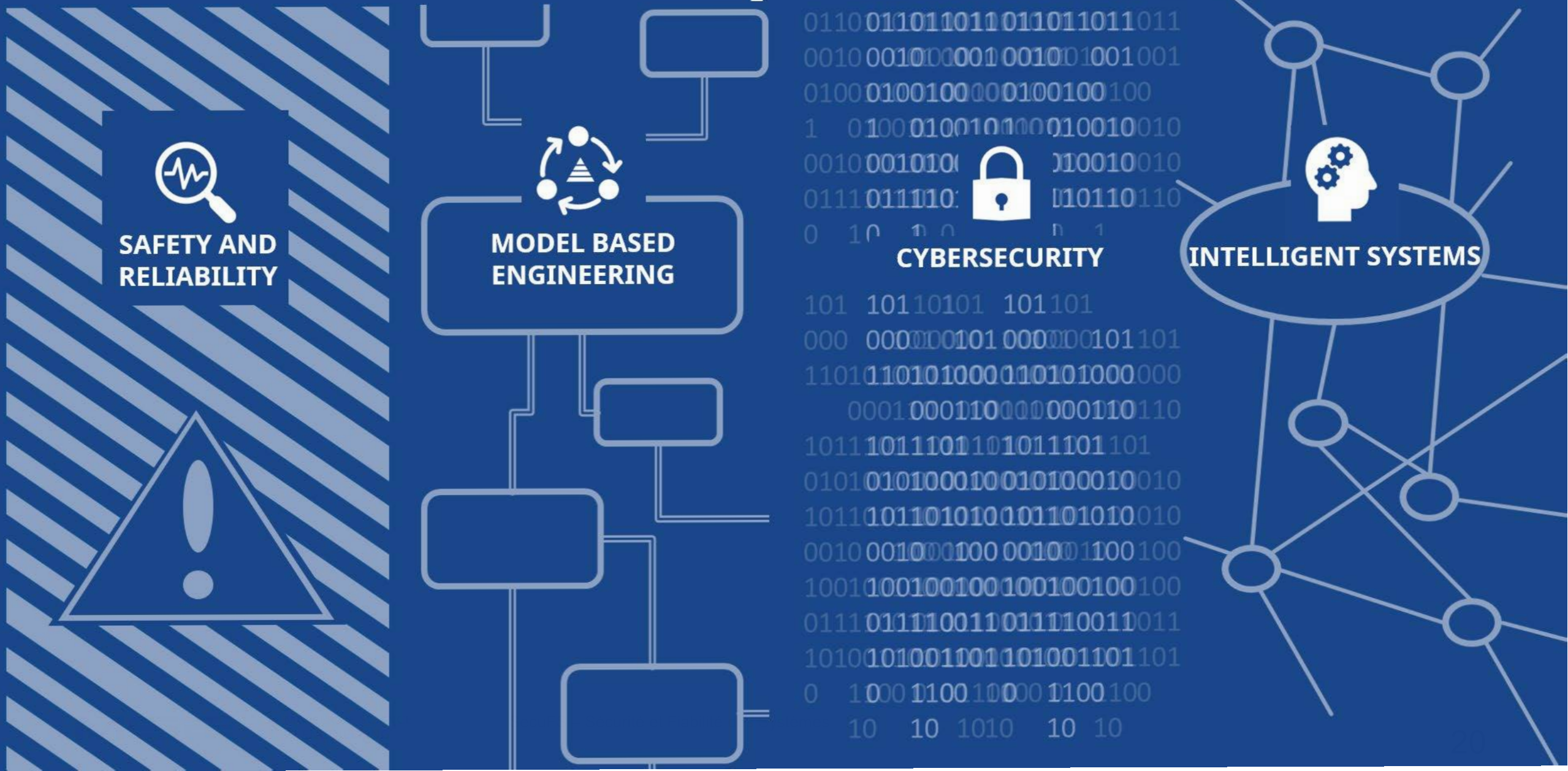
Deux ou trois intervenants feront leur apparition durant le cours pour présenter des cas concrets dans leur entreprise.

Si vous avez des idées ou propositions d’entreprises qui pourraient être intéressantes pour tous, n’hésitez pas à m’en faire part.

Actuellement prévu:

- Entreprise dans le domaine de la maintenance prédictive
- Entreprise dans le domaine des composants de sécurité électroniques (Barrières lumineuses)

# Our Domains of Expertise



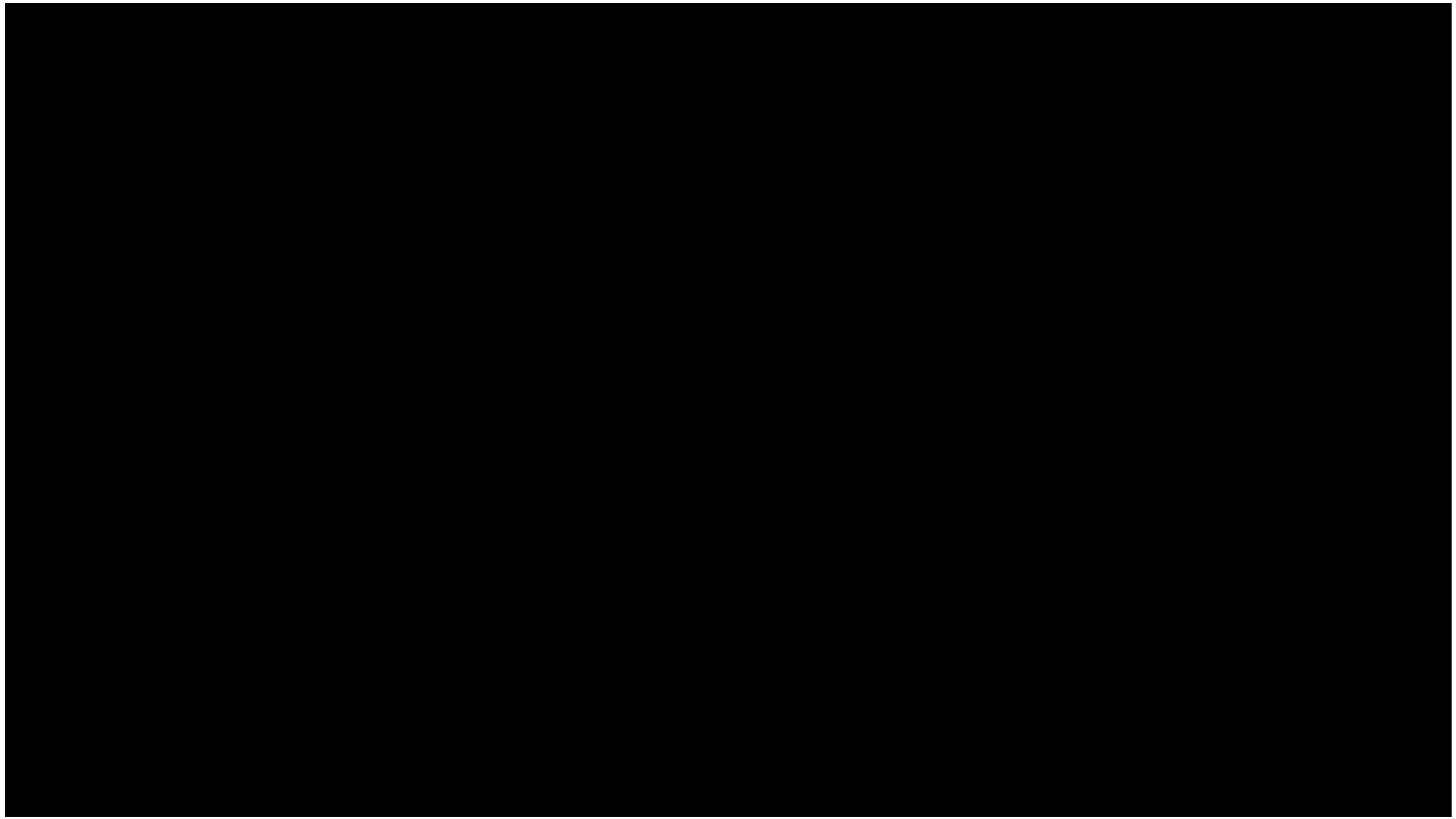
# Partenaires industriels/académiques et clients

BRUSA
JOHNSON ELECTRIC
LIEBHERR
MEGGITT
mercury systems

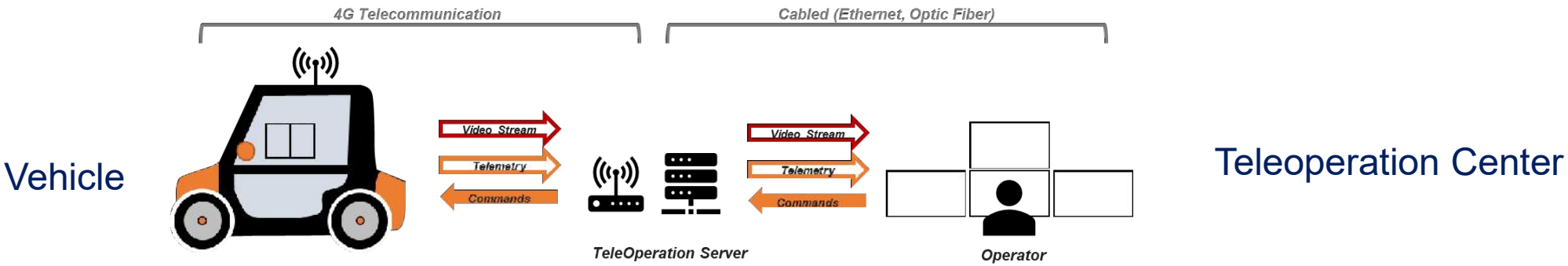
npr Nouvelle politique régionale
tpf
MICHELIN
KYBURZ
GAUSSIN Be Faster. Safer & Cleaner
Together ahead. RUAG
OP PLASTIC OMNIUM
SIEMENS Ingenuity for life
Vestas
polestar
BERNS ENGINEERS
Deutsches Zentrum für Luft- und Raumfahrt e.V. DLR
EASA
itk ENGINEERING
BOSCH
Selectron
Rolls-Royce
ANECOM AEROTEST
STADLER
VOITH
ZF
sbc
CATARC
esa
SYMBIO
TRANSVAN PERFECT FOOD LOGISTIC
regenHU biosystem architects
SWISS HYDROGEN
Schindler
APPLIED AUTONOMY
KALRAY
CONTRINEX
CERTX
AERI 中汽研（天津）汽车工程研究院有限公司

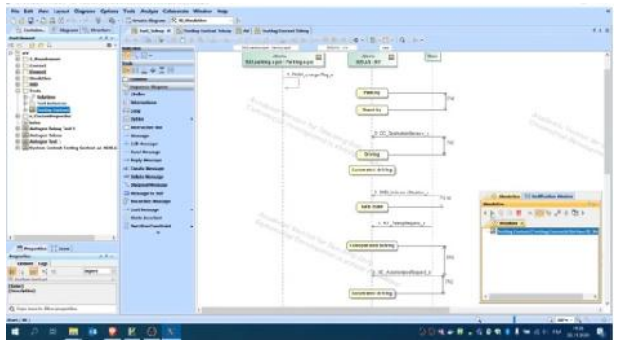
FH CAMPUS WIEN
OPEN RAIL LAB
Hochschule Ulm
Hochschule Kempten
Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg
Hes·so
EPF OOP
UNI FR
SHANGHAI UNIVERSITY
ETH zürich
zh aw School of Engineering
Hochschule Offenburg University of Applied Sciences
TUM Technische Universität München
- FSD
- FTM
HHN Hochschule Heilbronn
Technische Hochschule Ingolstadt
EssentialTech
EPFL ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
STEINBEIS HOCHSCHULE BERLIN

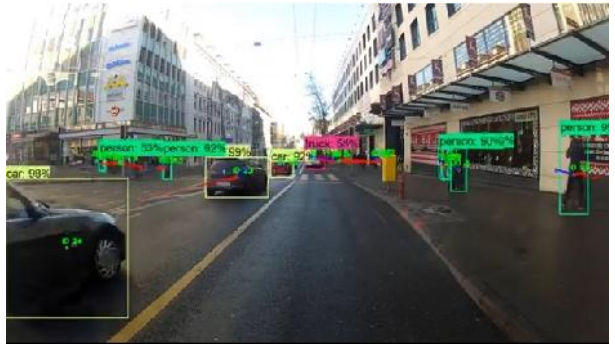
# SwissMoves



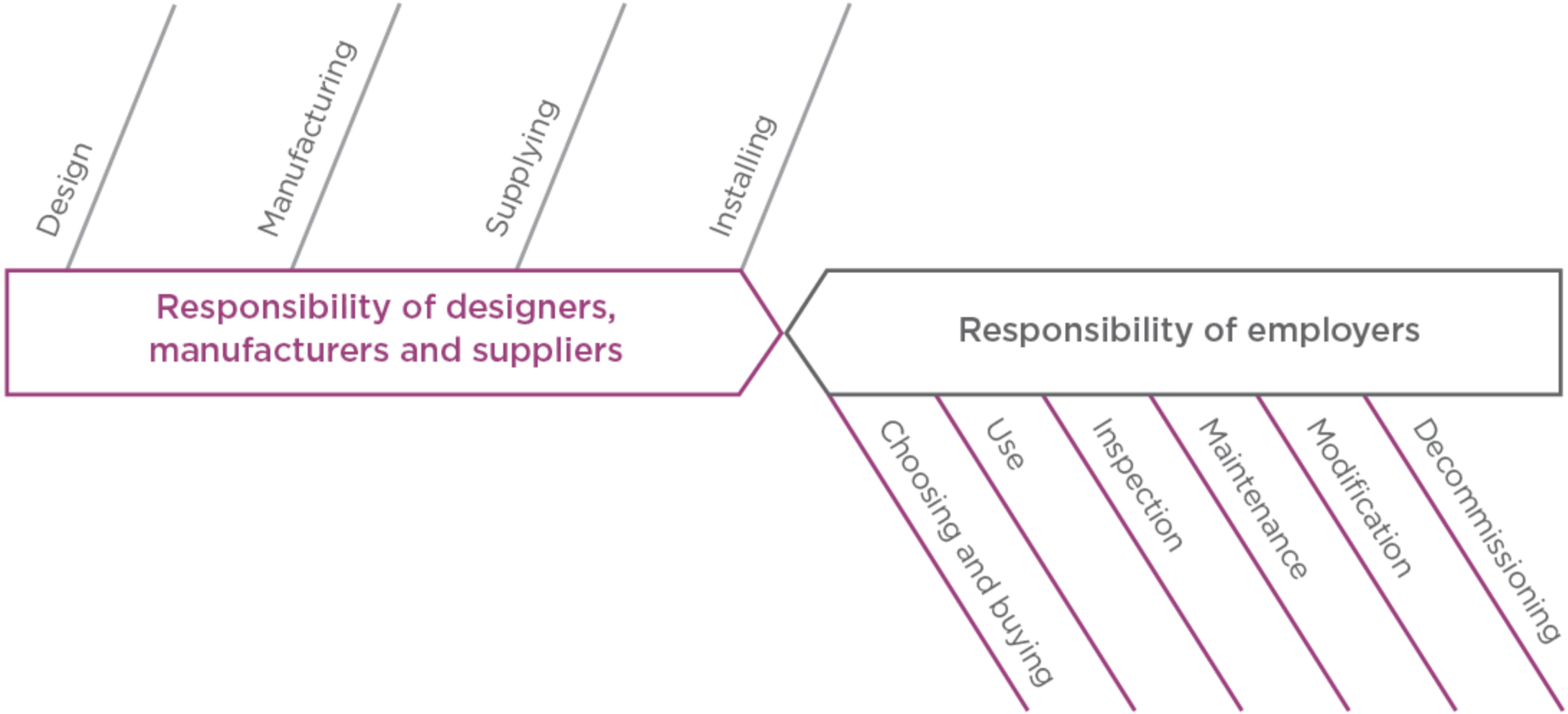
# SwissMoves


4G Telecommunication
Cabled (Ethernet, Optic Fiber)
Vehicle
Video Stream
Telemetry
Commands
TeleOperation Server
Video Stream
Telemetry
Commands
Operator
Teleoperation Center





# Responsabilités dans la fabrication d'un appareil




Source: https://www.worksafe.govt.nz/topic-and-industry/manufacturing/safe-use-of-machinery/

# Que veut dire sécurité fonctionnelle ?

**Type of Accident:** Unintended acceleration

**Car Type**: Toyota Highlander

**Probable Cause:** Lack of the functional safety analysis of the Electronic throttle control system

**Results**: 89 fatalities and 52 injuries (10 years)

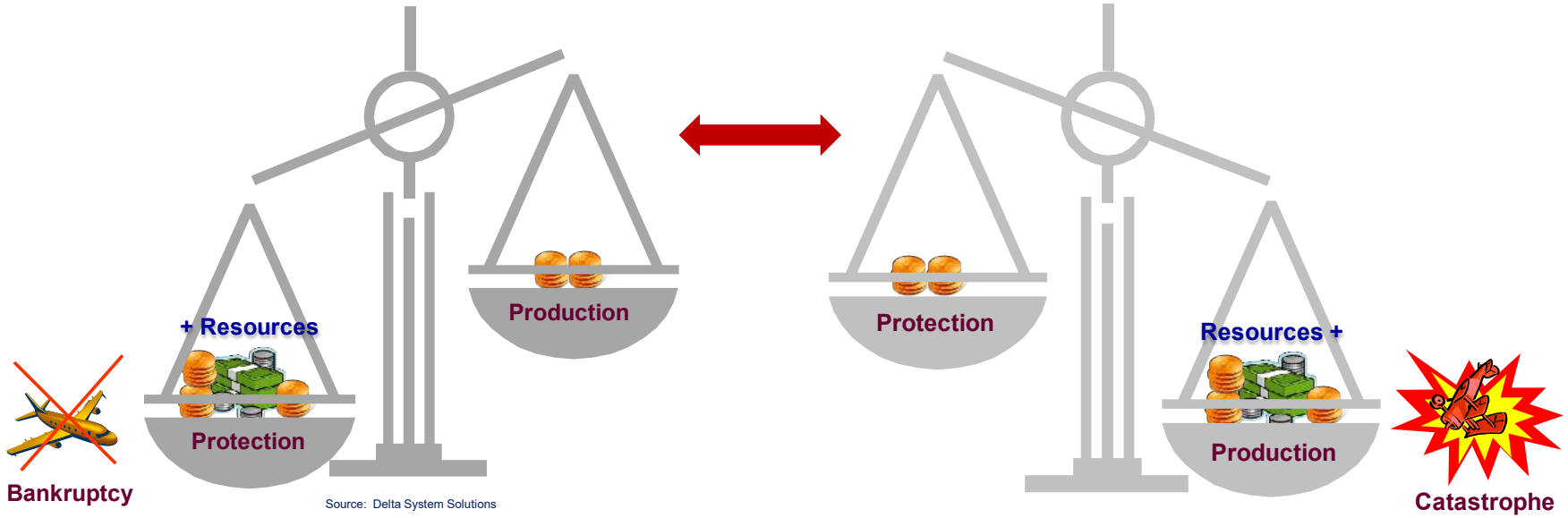
**Solution**: Functional Safety assessment to apply a “safety mechanism”, i.e. to put the brakes and/or clutch, or shift the gear into the “Neutral/Park” position

Sources:

- http://cnnphilippines.com/news/2015/12/04/Montero-Sport-sudden-acceleration-victims-stories.html
- https://en.wikipedia.org/wiki/Sudden_unintended_acceleration
- The National Highway Traffic Safety Administration (NHTSA)
- https://www.youtube.com/watch?v=dsTiPhcaeus

# Que veut dire sécurité fonctionnelle ?

… This is simply impossible!




Real life:

Driven by compromises!

Provide mitigating actions to prevent undesirable situations escalating !

# Que veut dire «Safety»?

**Est-ce que voler est plus dangereux que conduire une voiture?**

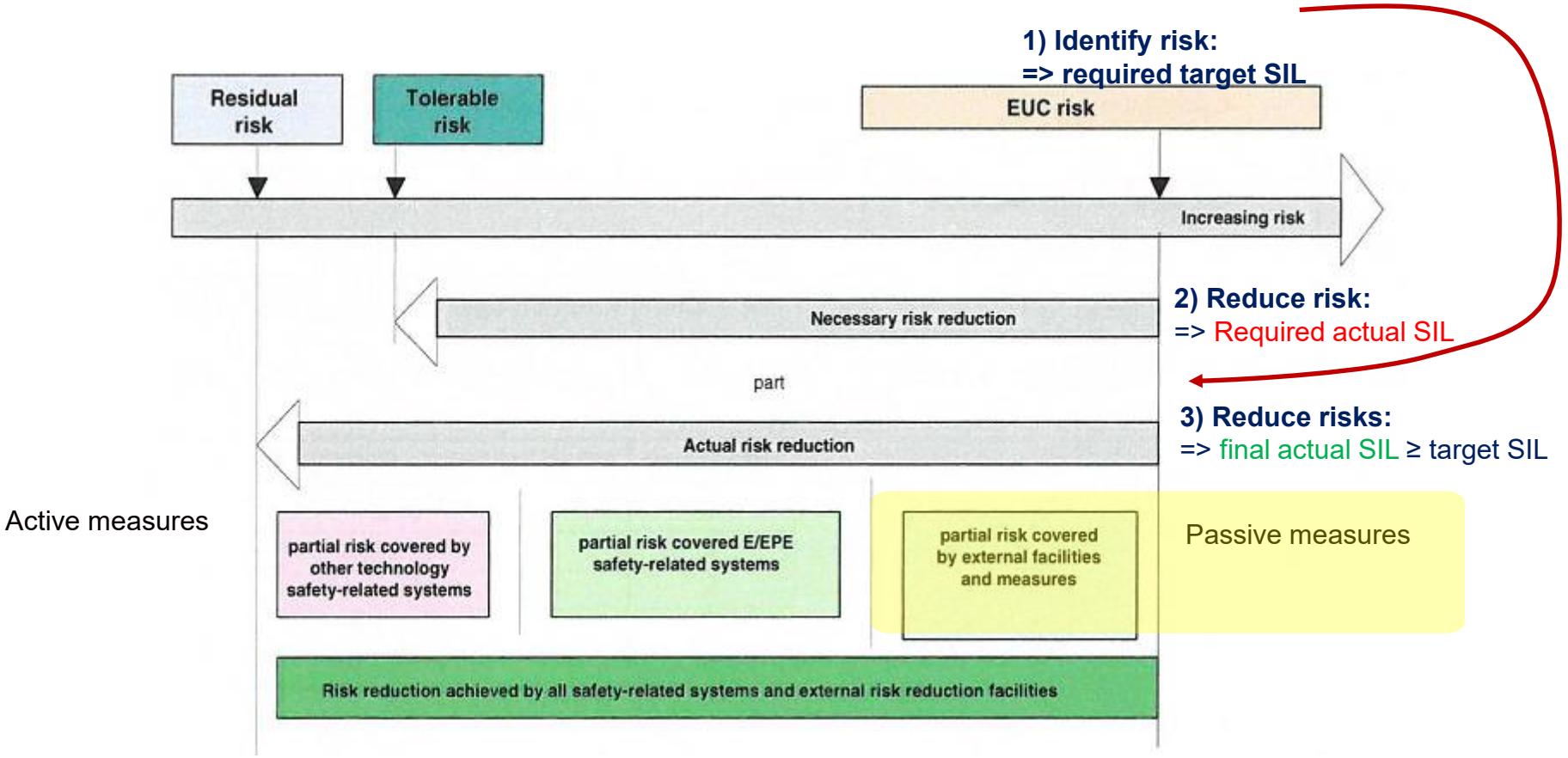
- Les **dangers** sont perçus **individuellement** ! Question clé: Quel est le niveau de tolérance ?
- **L'acceptance** d'un **effet dangereux** (p.ex. mort accidentelle) est lié avec une unité de référence (p.ex. Km parcourus, Temps de fonctionnement, années…)
- Les unités de référence proposent une corrélation entre un danger et sa probabilité d'occurrence**.**
- L'acceptance du danger est liée à la **perception** de celui-ci, à sa **criticité** et à sa **probabilité** d'occurrence.
- Cette corrélation définit le **risque**.

„**Risque**" => Il y a un lien entre la criticité d'un événement et sa probabilité d'occurrence ..

# Comment est classifié le risque ?

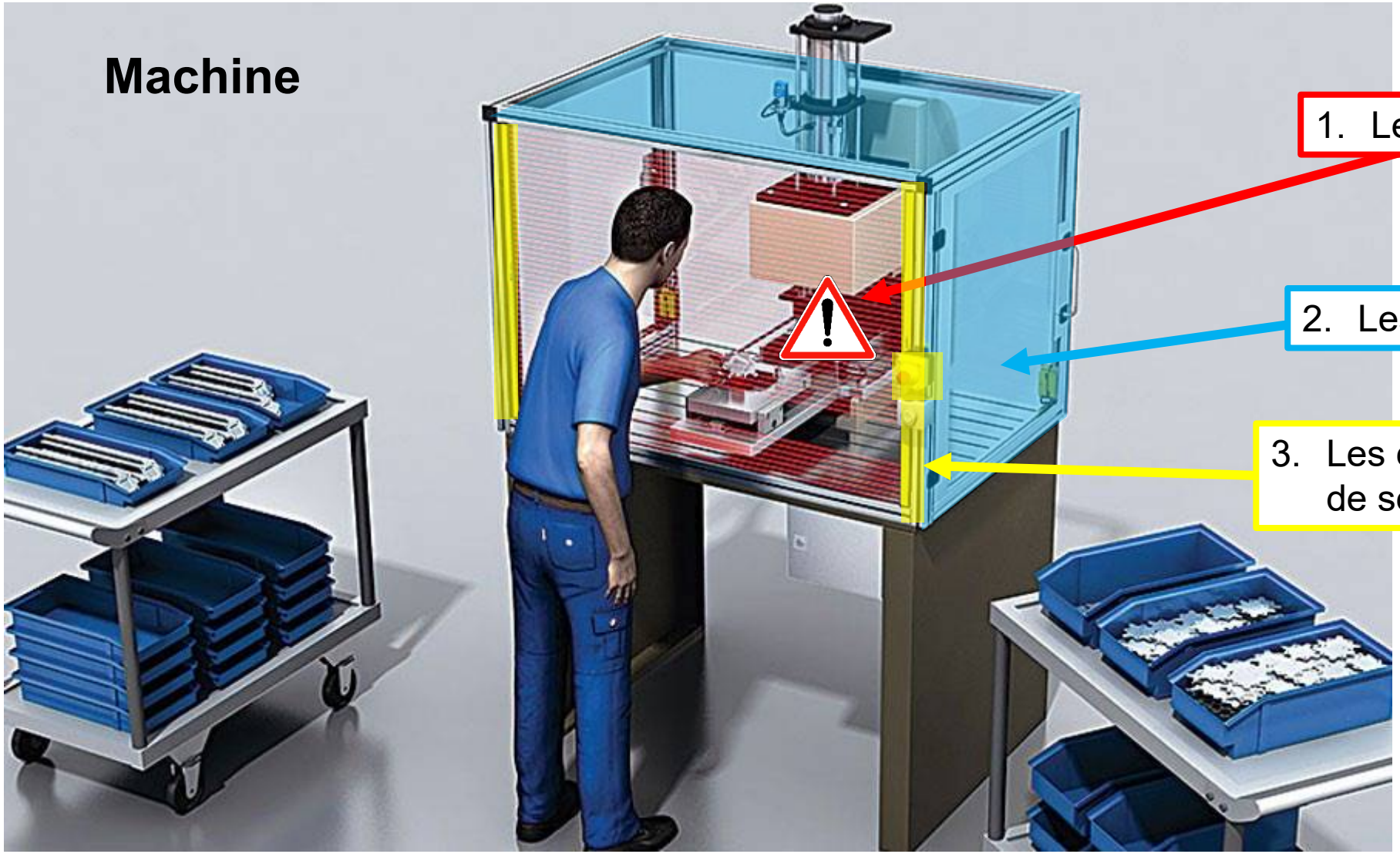
| Industry | Domain Specific **“Safety Integrity Levels”** | | | | |
|---|---|---|---|---|---|
| Aerospace<br>RTCA DO254 (HW) / DO 178C (SW) | DAL E | DAL D | DAL C | DAL B | DAL A |
| General Machinery<br>IEC 61508 | (SIL 0) | SIL 1 | SIL 2 | SIL 3 | SIL 4 |
| Machinery<br>ISO 13849 | PL a | PL b | PL c | PL d | PL e |
| Railway<br>CENELEC EN 50126 / 50128 / 50129 | (SIL 0) | SIL 1 | SIL 2 | SIL 3 | SIL 4 |
| Automotive<br>ISO EN 26262 | QM | ASIL A | ASIL B/C | ASIL D | - |

# Approche de l'analyse de sécurité:




**EUC = Equipment under Control**

# Exemple d’application



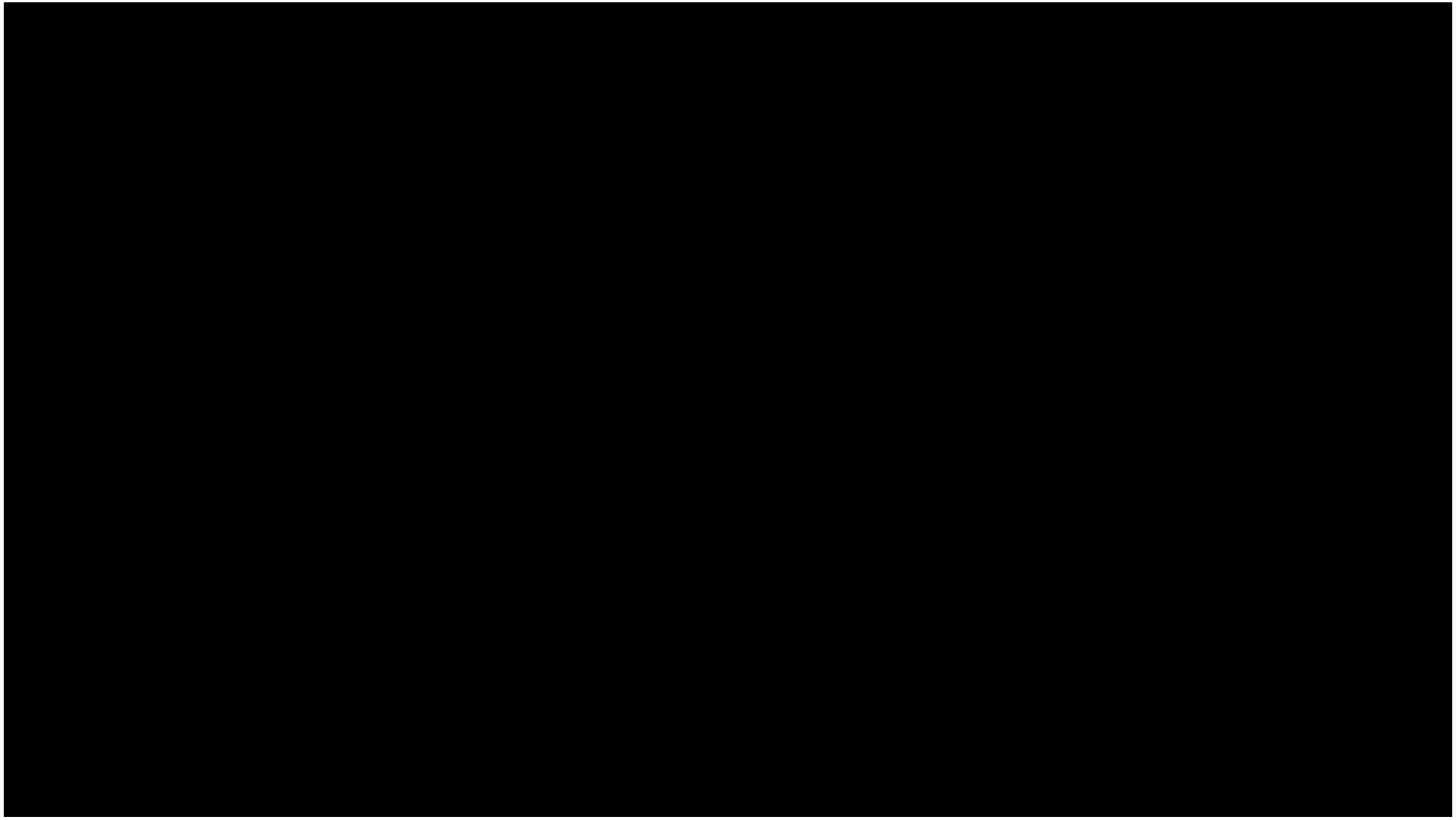

1. Les risques
2. Les protecteurs
3. Les composants de sécurité

Sources: https://www.assemblymag.com/articles/92897-new-technology-for-machine-safety

# Protecteurs mécaniques

Sources: https://safetyskills.com/machine-guarding/

# Protecteurs mécaniques



# Exemple 1: Ordinateur portable

Directives applicables: (au minimum)

- Basse tension (2006/95/EC)
- Compatibilité électromagnétique (2004/108/EC)
- (Equipement Hertzien) (99/5/EC)



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Exemple 2: Ordinateur portable

Directives applicables: (au minimum)

- Sécurité des jouets (2006/95/EC)
- Compatibilité électromagnétique (2004/108/EC)



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Exemple 3: Presse plieuse



Sources: Film: 8 Mile

# Exemple 3: Presse plieuse

Directives applicables: (au minimum)

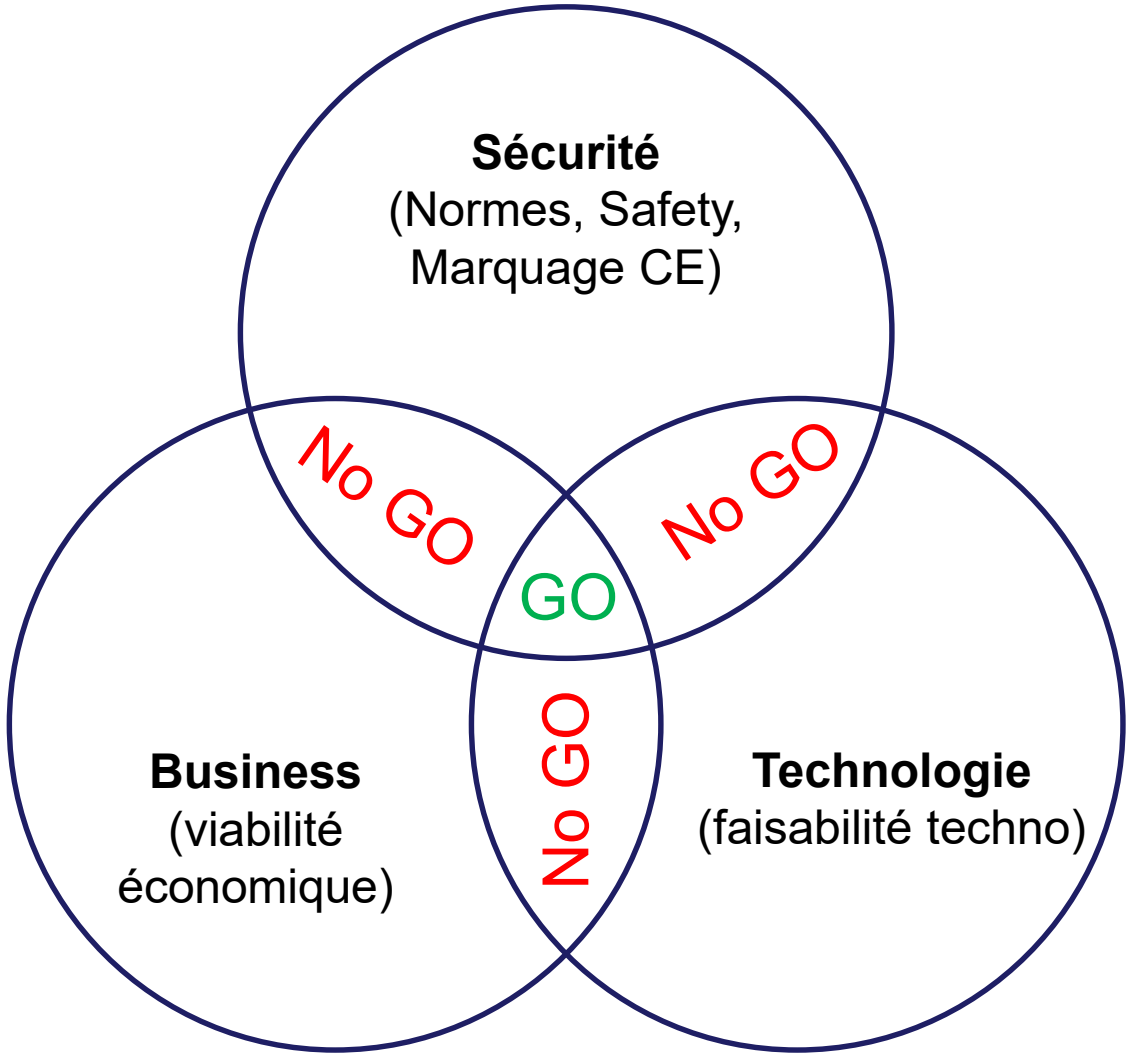
- Directive Machines (2006/42/EC)
- Compatibilité électromagnétique (2004/108/EC)
- EN ISO 16092:2018 – Sécurité des machines outils - Presses



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Pourquoi être autant exigeant sur la sécurité?

# Mise sur le marché d'un nouveau produit:



# Exercice pour le 04.10.2020

De manière individuelle, chaque étudiant doit:

- Choisir un appareil ou une machine à étudier
- Décrire brièvement le produit ainsi que son public cible et son environnement de fonctionnement

Vous pouvez commencer tout de suite

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

# Propositions de thèmes:

# Merci pour votre attention

Questions ou remarques: eric.silva@hefr.ch ou via Teams

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et fiabilité des systèmes (SecuFS)

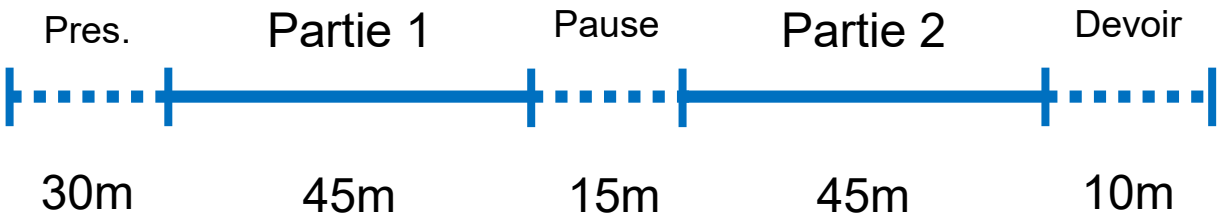
# 02 - Directives, standards et normes applicables

Eric Silva
04.10.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | xx.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Format du cours (à partir de la semaine prochaine)




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Présentations individuelles

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

# Contenu du cours

1. Les risques
2. Les protecteurs
3. Les composants de sécurité



Sources:
https://www.assemblymag.com/articles/92897-new-technology-for-machine-safety

# Qu’est-ce que le Marquage CE?

Le marquage CE est un schéma d’auto-certification ayant pour objectif de démontrer que le produit est conforme à la législation européenne sur le plan de la santé, de la sécurité ainsi que de la protection de l’environnement.

Le produit qui satisfait ces exigences sera marqué du logo CE afin d’afficher sa conformité. Ce marquage est considéré comme le «passeport» du produit, garantissant ainsi sa circulation dans l’espace européen.

Retrait de produit: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=main.listNotifications&lng=en



Sources:
https://www.glazingvision.co.uk/blog/top-questions-on-ce-marking/

# Les 6 étapes du Marquage CE

1. Définir les directives applicables au produit
2. Identifier les exigences essentielles
3. Déterminer les «audits» ou évaluations qui devront être effectués par des tiers
4. Evaluer la conformité du produit
5. Préparer le dossier de conformité
6. Remplir la déclaration de conformité européenne et marquer le produit

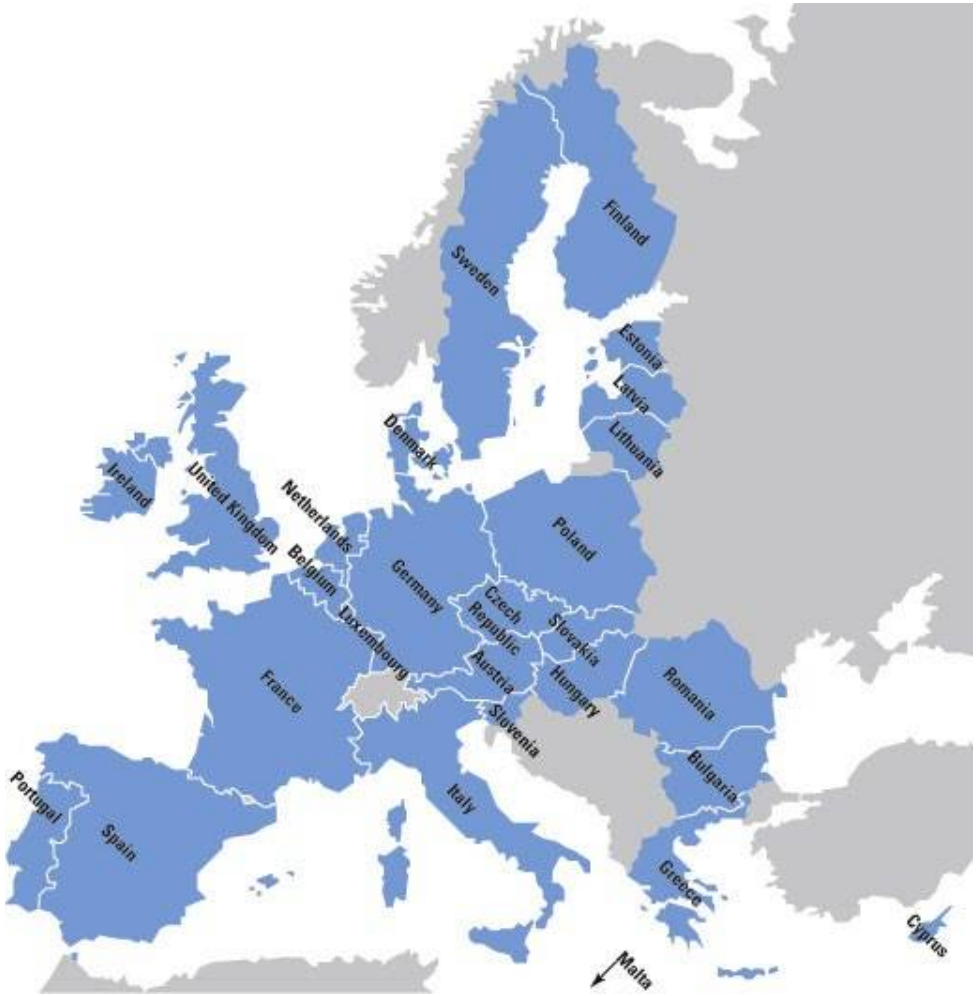
Sources:
https://labtestcert.com/ce-marking-declaration-of-conformity (picture)

# 1. Définir les directives applicables au produit

**Trouvez la ou les directives qui s'appliquent à votre produit**
Comment savoir si votre produit doit porter le marquage CE? La première étape consiste à vérifier si votre produit est régi par une ou plusieurs des 24 directives de la CE figurant dans la liste ci-après. Si tel est le cas, vous êtes tenu d'y apposer le marquage CE.

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Pays dans lesquels le marquage CE s’applique




- Austria
- Belgium
- Bulgaria
- Croatia
- Czech Republic
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland*
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Norway
- The Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden*
- Switzerland*
- Turkey*
- United Kingdom

* Pays où la directive des machines est mise en application



Sources:
http://www.newsteelconstruction.com/wp/ce-marking/

# Directives qui requièrent un marquage CE

| Numéro de la directive | Catégories de produits |
|---|---|
| 2014/35/EC | Basse tension |
| 2009/105/EC | Récipients à pression simples |
| 2009/125/EC | Écoconception des produits liés à l'énergie |
| 2000/14/EC | Émissions sonores des matériels destinés à être utilisés à l'extérieur des bâtiments |
| 2009/48/EC 88/378/EEC, 93/68/EEC | Sécurité des jouets |
| 89/106/EEC, 93/68/EEC | Produits de construction |
| 2014/30/EC | Compatibilité électromagnétique |
| 2006/42/EC | Machines |
| 89/686/EEC, 93/68/EEC, 93/95/EEC, 96/58/EC | Équipements de protection individuelle |
| 2009/23/EC (ex. 90/384/EEC) | Instruments de pesage à fonctionnement non automatique |
| 2009/142/EC (ex 90/396/EEC) | Appareils à gaz |
| 92/42/EEC, 93/68/EEC, 2004/8/EC, 2005/32/EC | Chaudières à eau chaude (combustibles liquides ou gazeux) |
| 93/15/EEC | Explosifs à usage civil |
| 93/42/EEC, 98/79/EC, 2000/70/EC, 2001/104/EC, | Dispositifs médicaux |
| 90/385/EEC, 93/42/EEC, 93/68/EEC, 2007/47/EC | Dispositifs médicaux implantables actifs |
| 98/79/EC | Dispositifs médicaux de diagnostic in vitro |
| 94/9/EC | Matériel pour utilisation en atmosphères explosibles |
| 94/25/EC, 2003/44/EC | Bateaux de plaisance |
| 95/16/EC | Ascenseurs |
| 97/23/EC | Équipements sous pression |
| 99/5/EC | Équipements hertziens et équipements terminaux de télécommunication |
| 2000/9/EC | Installations à câbles transportant des personnes |
| 2004/22/EC | Instruments de mesure |
| 2007/23/EC | Articles pyrotechniques |



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Difficulté du choix des directives applicables

Il peut être difficile de déterminer si votre produit est régi par une ou plusieurs directives.

Ainsi, si vous fabriquez des **machines d'empaquetage électronique munies d'un transporteur à courroie**, vous devrez respecter **plusieurs directives**. Pour déterminer lesquelles s'appliquent à votre produit, il vous faudra examiner chacune des 24 directives (les produits visés se trouvent parfois en annexe).

Il n'existe aucun outil de référence ni base de données indiquant quelles directives pourraient s'appliquer à certains produits.



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Exemple 1: Ordinateur portable

Directives applicables: (au minimum)

- Basse tension (2006/95/EC)
- Compatibilité électromagnétique (2004/108/EC)
- (Equipement Hertzien) (99/5/EC)



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Exemple 2: Ordinateur portable

Directives applicables: (au minimum)

- Sécurité des jouets (2006/95/EC)
- Compatibilité électromagnétique (2004/108/EC)



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# 2. Identifier les exigences essentielles

**Informez-vous des exigences essentielles auxquelles doit répondre votre produit**
Chaque directive décrit en détail ce que les lois de l'UE prévoient pour que votre produit soit jugé conforme. Il s'agit des « exigences essentielles » de la directive. Ces exigences sont très générales. Les directives ne décrivent pas en détail la façon de concevoir les produits pour qu'ils respectent les exigences essentielles.

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Les exigences de la directive machines (2006/42/EC)

1. Effectuer une analyse des risques afin de déterminer les exigences de santé et de sécurité
   a) Déterminer les limites de la machine
   b) Recenser les dangers et situations dangereuses associées
   c) Estimer les risques (gravité d'une éventuelle blessure ou atteinte à la santé et probabilité)
   d) Evaluer les risques afin de déterminer si une réduction est nécessaire
   e) Eliminer les dangers ou réduire les risques associés à ces dangers en appliquant des mesures de protection
2. Evaluer les risques dus à des situations anormales prévisibles, définir le marquage nécessaire ainsi que les notices d'instructions
3. Si des objectifs ne peuvent pas être atteints au vu de l'état de la technique, s'en approcher le plus possible.



Sources:
Directive Machines (2006/42/EC)

# Principes d’intégration de la sécurité

1. **Fonctionnement, réglage, entretien sans risque pour des personnes**, si effectué selon les conditions prévues, mais en tenant compte des mauvais usages raisonnablement prévisibles (Supprimer tout risque durant l’existence de la machine, y compris le transport, montage, démontage, mise hors service et mise au rebut)
2. En choisissant les solutions les plus adéquates, le fabricant ou son mandataire doit appliquer les principes suivants, dans l'ordre indiqué:
   - ✓ **éliminer ou réduire les risques**
   - ✓ prendre les mesures de protection nécessaires vis-à-vis des risques ne pouvant être éliminés,
   - ✓ informer les utilisateurs des risques résiduels, indiquer si une formation particulière est requise et signaler s'il est nécessaire de prévoir un équipement de protection individuelle.
3. La machine doit être conçue et construite de manière à **éviter qu'elle soit utilisée de façon anormale**, si un tel mode d'utilisation engendre un risque. Le cas échéant, la notice d'instructions doit attirer l'attention de l'utilisateur sur les contre-indications d'emploi de la machine qui, d'après l'expérience, pourraient se présenter.
4. La machine doit être conçue et construite **pour tenir compte des contraintes imposées à l'opérateur** par l'utilisation nécessaire ou prévisible d'un **équipement de protection** individuelle.
5. La machine doit être **livrée avec tous les équipements** et accessoires spéciaux essentiels pour qu'elle puisse être réglée, entretenue et utilisée en toute sécurité.



Sources:
Directive Machines (2006/42/EC)

# Principes d’intégration de la sécurité, exemple

La SUVA propose des supports pour de nombreux sujets:

Dispositifs de protection des mains autorisés sur les presses, liste

Presse Hydraulique, checklist



Sources:
https://www.machine-outil.com/t57/p198-sicmi.html

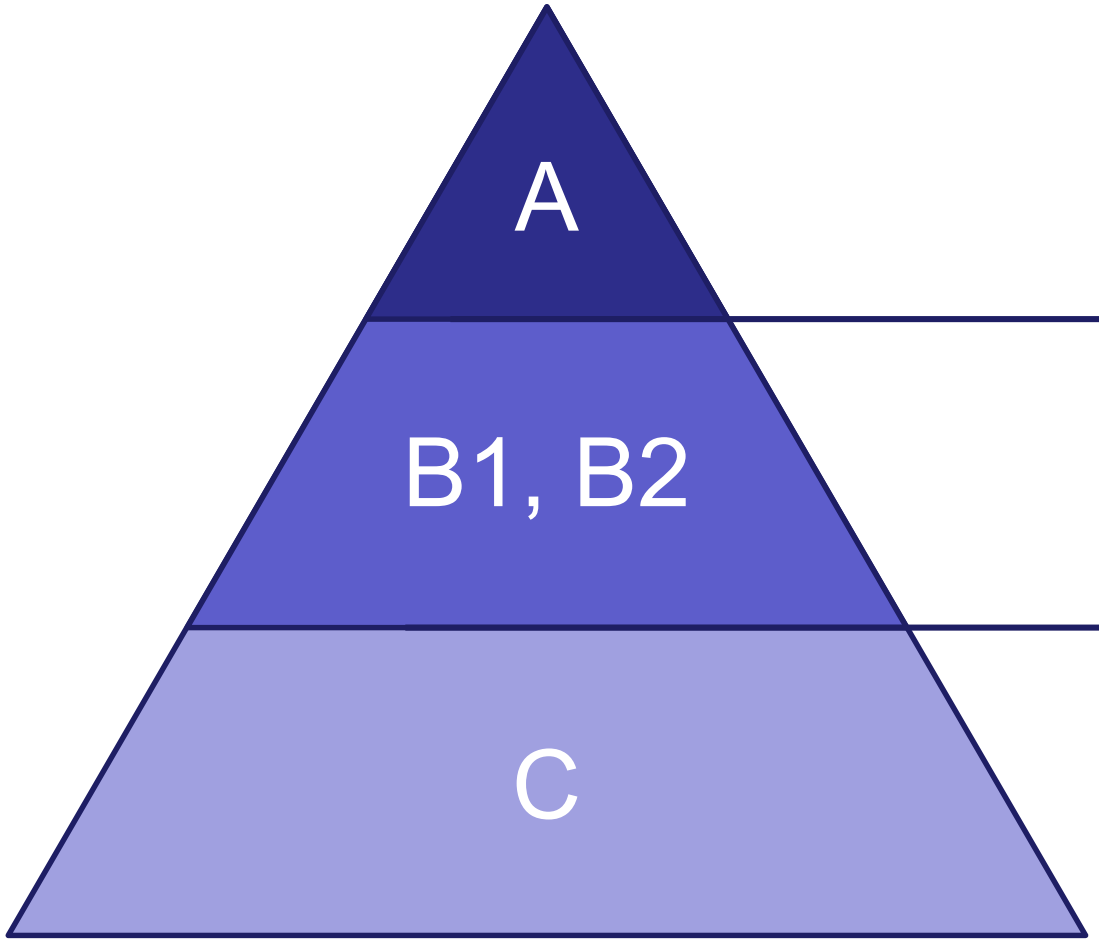
# Autres exigences de la directive

1. Les matériaux et produits
2. L'éclairage
3. La conception de la machine en vue de la manutention
4. Ergonomie
5. Poste de travail
6. Siège
7. **Systèmes de commande** (sécurité et fiabilité, organes de service, mise en marche, arrêt, sélection de modes, défaillance de l'alimentation)
8. **Mesures de protection contre les risques mécaniques** (perte de stabilité, rupture, chute, éjection, arêtes et angles…)
9. **Caractéristiques requises pour les protecteurs et dispositifs de protection** (protecteurs fixes, protecteurs mobiles, protecteurs limitant l'accès…)
10. Risques dus à d'autres dangers (alimentation électrique, électricité statique, alimentation autre, erreur de montage, température extrême, incendie, explosion, bruits, vibrations, rayonnements…)
11. Informations (Avertissements, dispositifs d'information, dispositifs d'alerte, marquage des machines, notice d'instructions
12. Exigences pour machines spécifiques (pharma, portatives, à bois…)



Sources:
Directive Machines (2006/42/EC)

# Les types de normes




**Les normes de type A** sont des normes de **sécurité de base** qui traitent des termes de base, des principes de conception et des **aspects généraux** pouvant être appliqués aux machines.

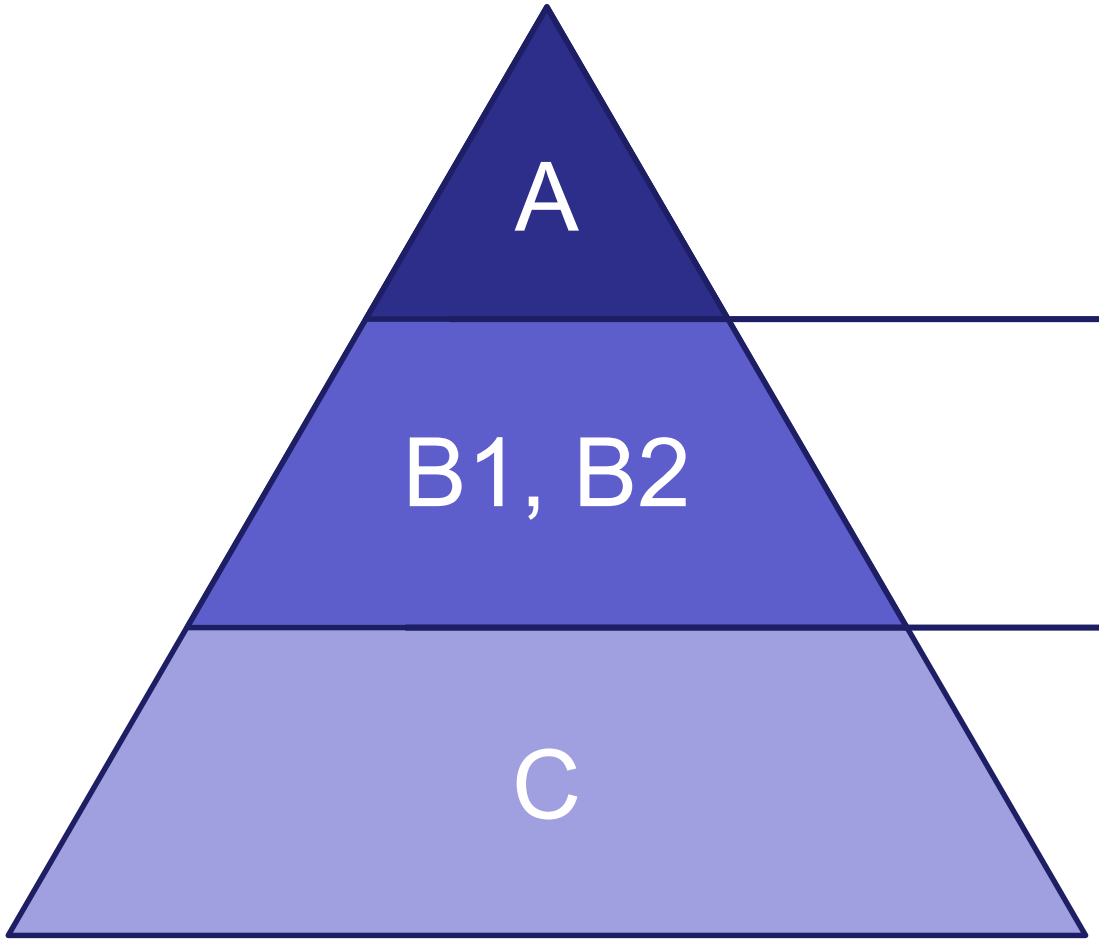
**Les normes de type B** sont similaires au type A mais traitent des **aspects de sécurité spécifiques à une série de machines (B1)** ou des **dispositifs de protection** spécifiques **(B2)**

**Les normes de type C** sont des normes pour la sécurité des machines qui indiquent des exigences de sécurité détaillées sur une machine précise ou un groupe de machines.



Sources:
https://www.pilz.com/fr-FR/support/knowhow/faq/standards/articles/167667

# Exemples de normes de type A,B,C




EN ISO 12100 – Principes généraux de conception

**B1**
EN ISO 13849-1 - Systèmes de commande relatives à la sécurité
EN ISO 13855 - Positionnement des moyens de protection

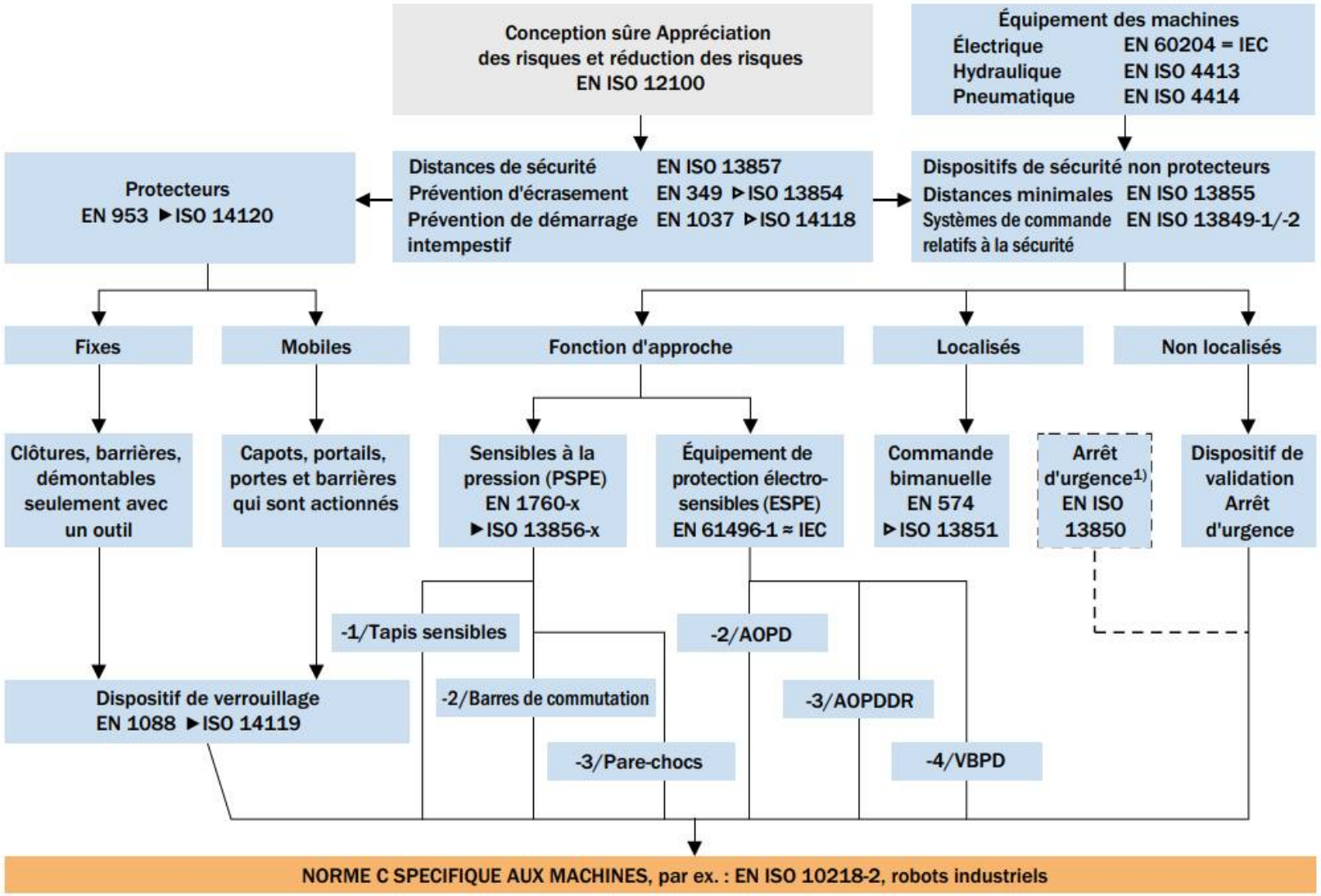
**B2**
EN ISO 13851 - Dispositifs de commande bimanuelle et
DIN EN ISO 14120 - Protecteurs fixes

EN ISO 16092-3 – Presses hydrauliques
EN 415, 1-10 – Machines d'emballage
EN 12409 – Machines de thermoformage



Sources:
https://www.pilz.com/fr-FR/support/knowhow/faq/standards/articles/167667

# Moyens de protection et normes correspondantes






Sources: https://cdn.sick.com/media/docs/3/03/403/Special_information_Guide_for_Safe_Machinery_fr_IM0062403.PDF

# Exercice 2

**En groupes de 3 ou 4** -> Les personnes à distance font ensemble via Teams si possible

1. Parcourez ensemble les fiches produits que vous avez préparé pour aujourd'hui.
2. Sélectionner un des produits qui vous semble intéressant
3. Recherchez et définissez les directives devant être suivies afin de mettre ce produit sur le marché européen
4. Recherchez si des normes harmonisées existent pour votre produit et les mentionner
5. Résumer en quelques mots les principales exigences qui vous seront demandées (celles qui vous semblent les plus importantes)

Vous avez 45 minutes à disposition, pause café comprise.

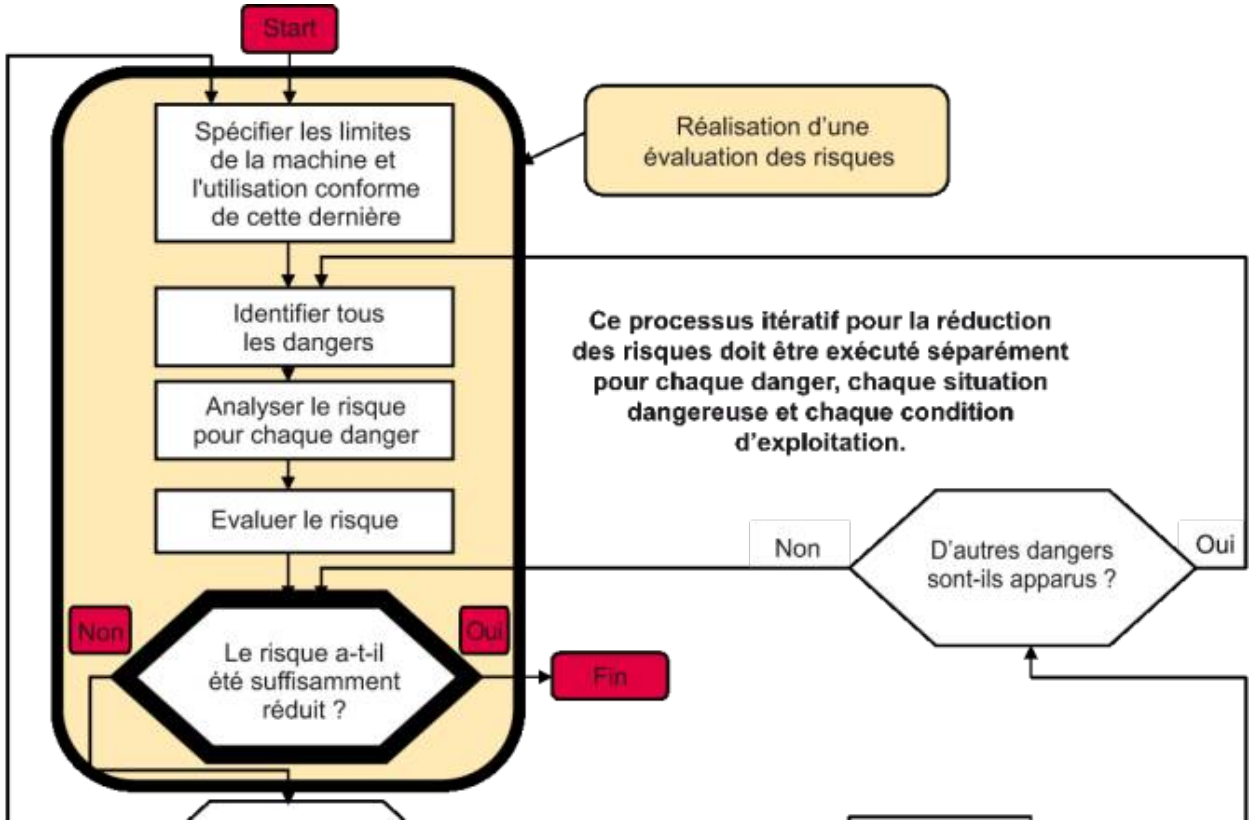
Liste des normes harmonisées:
https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/


Sources:
https://www.leuze.com/fr

# Quelques normes pertinentes relatives au machines

## ISO 12100

Sécurité des machines – Principes généraux de conception, appréciation du risque et réduction du risque



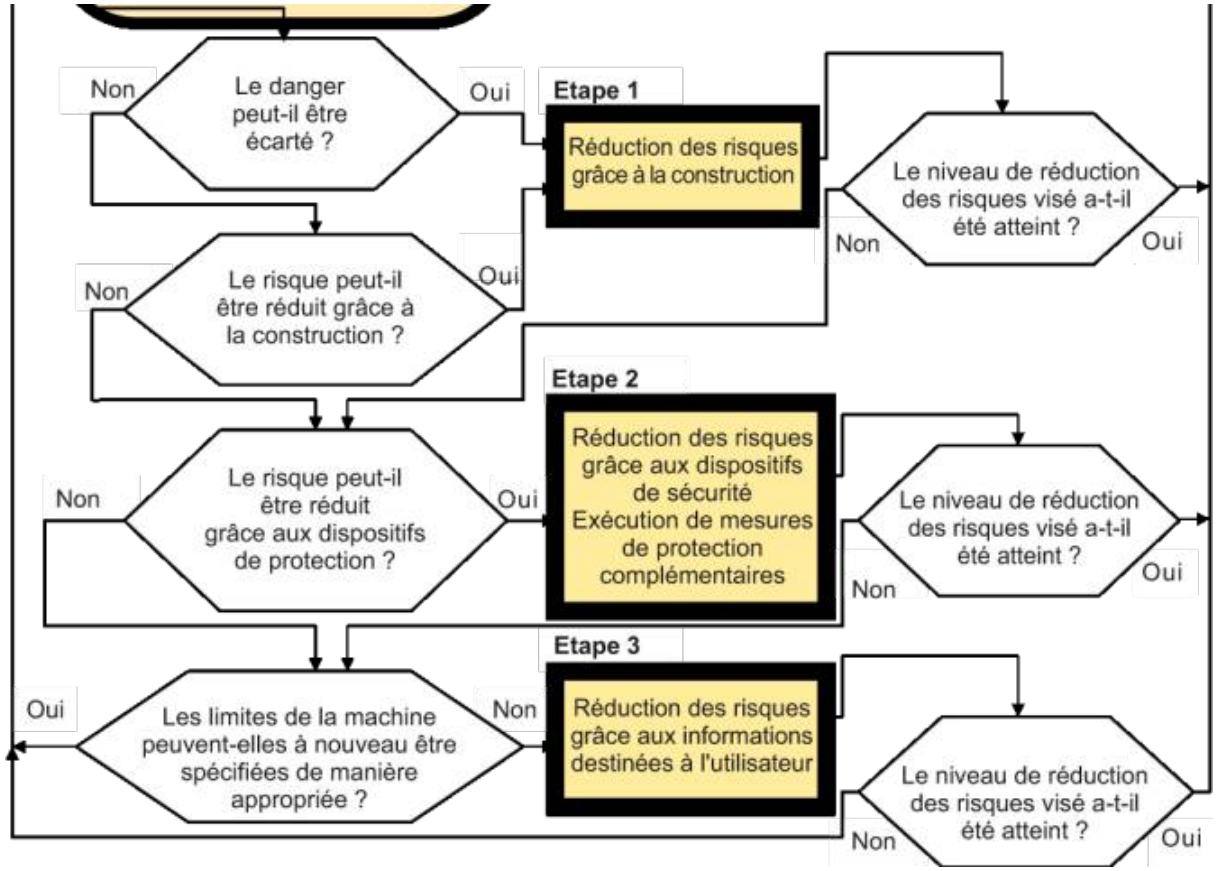



Sources:
https://www.leuze.com/fr

# Quelques normes pertinentes relatives au machines

## ISO 12100(2)

Sécurité des machines – Principes généraux de conception, appréciation du risque et réduction du risque



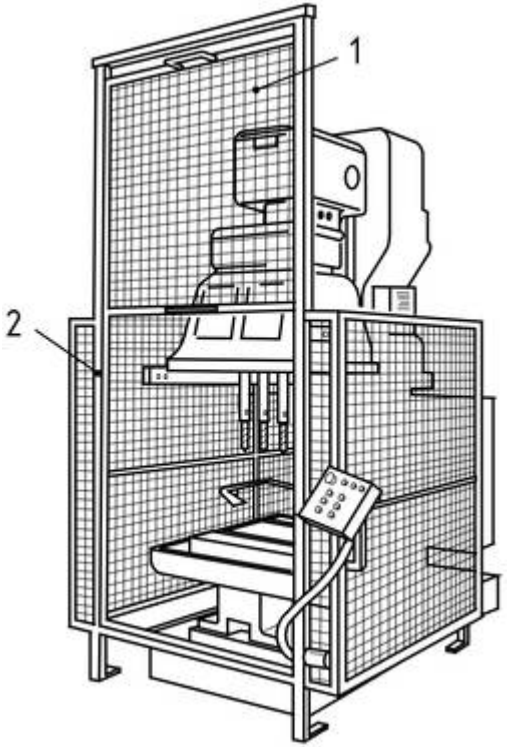



Sources:
https://www.leuze.com/fr

# Quelques normes pertinentes relatives au machines

## ISO 14120

Sécurité des machines – Prescriptions générales pour la conception et la construction de protecteurs fixes et mobiles






Sources:
https://cdn.sick.com/media/docs/3/03/403/Special_information_Guide_for_Safe_Machinery_fr_IM0062403.PDF

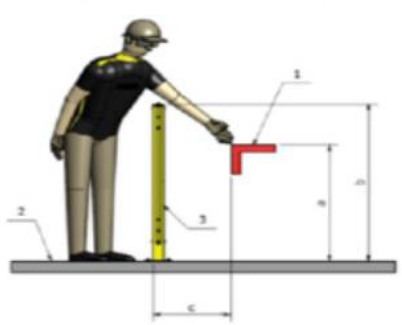
# Quelques normes pertinentes relatives au machines

## ISO 13857

Sécurité des machines – Distances de sécurité empêchant les membres supérieurs et inférieurs d'atteindre les zones dangereuses (Membres inférieurs et supérieurs)

La plupart des règles ne s'applique qu'à des personnes de plus de 14 ans (utilisation dans des usines)

| Height of the danger zone *a* (mm) | Height of the Shelter *b* ( mm ) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1000 | 1200 | 1400 | 1600 | 1800 | 2000 | 2200 | 2400 | 2500 | 2700 |
| | Safety distance horizontal danger zone *c* ( mm ) | | | | | | | | | |
| 2700 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2600 | 900 | 800 | 700 | 600 | 600 | 500 | 400 | 300 | 100 | 0 |
| 2400 | 1100 | 1000 | 900 | 800 | 700 | 600 | 400 | 300 | 100 | 0 |
| 2200 | 1300 | 1200 | 1000 | 900 | 800 | 600 | 400 | 300 | 0 | 0 |
| 2000 | 1400 | 1300 | 1100 | 900 | 800 | 600 | 400 | 0 | 0 | 0 |
| 1800 | 1500 | 1400 | 1100 | 900 | 800 | 600 | 0 | 0 | 0 | 0 |
| 1600 | 1500 | 1400 | 1100 | 900 | 800 | 500 | 0 | 0 | 0 | 0 |
| 1400 | 1500 | 1400 | 1100 | 900 | 800 | 0 | | | | |
| 1200 | 1500 | 1400 | 1100 | 900 | 700 | 0 | | | | |
| 1000 | 1500 | 1400 | 1000 | 800 | 0 | 0 | | | | |
| 800 | 1500 | 1300 | 900 | 600 | 0 | 0 | | | | |
| 600 | 1400 | 1300 | 800 | 0 | 0 | 0 | | | | |
| 400 | 1400 | 1200 | 400 | 0 | 0 | 0 | | | | |
| 200 | 1200 | 900 | 0 | 0 | 0 | 0 | | | | |
| 0 | 1100 | 500 | 0 | | | | | | | |





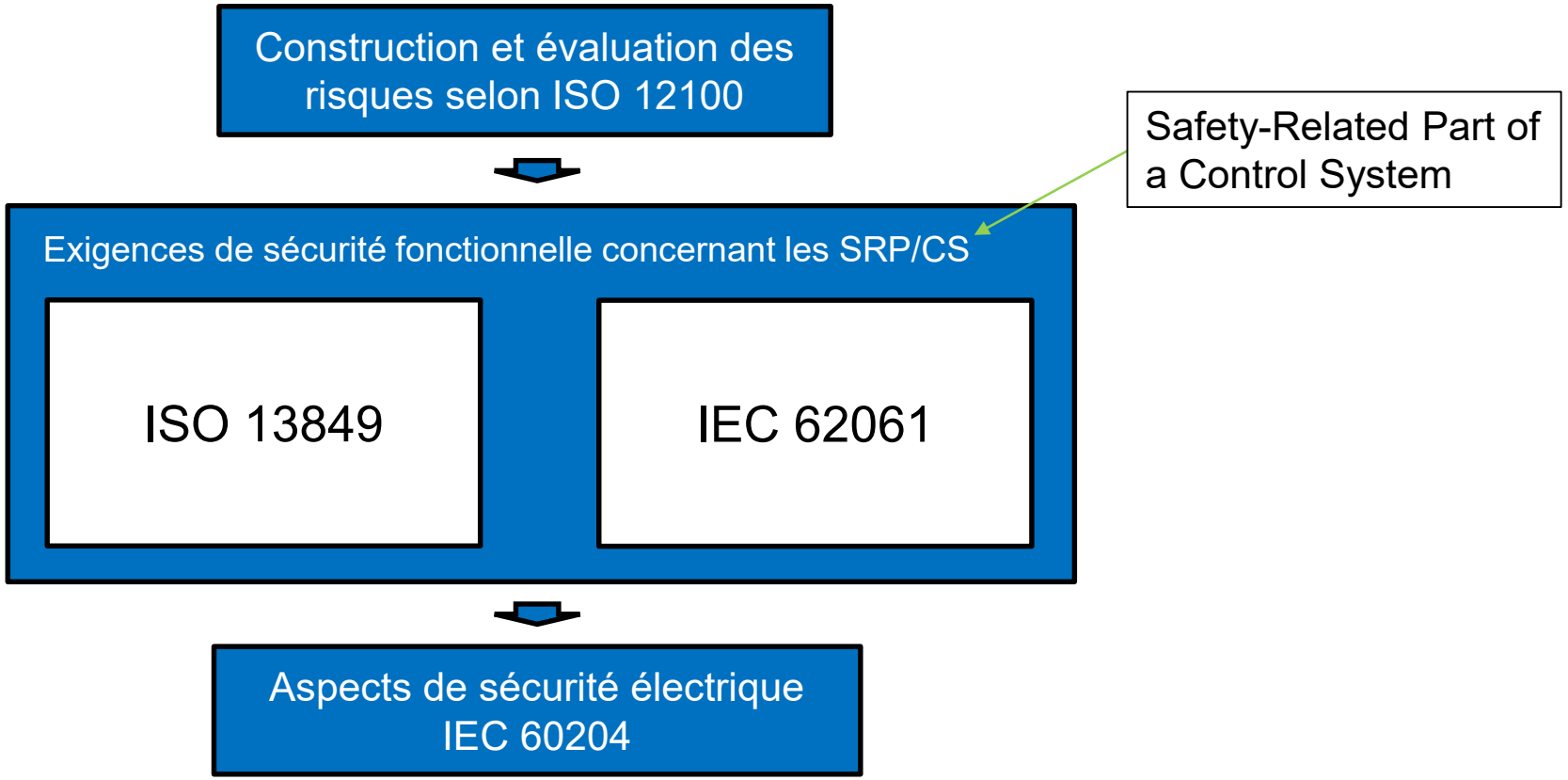
Sources: http://www.strafil.com/images/strafil/docs/STRAFIL-ACCESS-DOC-TECH.pdf

# Quelques normes pertinentes relatives au machines

## ISO 13849 et IEC 62061

Sécurité des machines – Parties des systèmes de commande relatifs à la sécurité

La norme IEC 62061 s'applique plus particulièrement aux systèmes contenant des logiques programmables.






Sources:
http://www.strafil.com/images/strafil/docs/STRAFIL-ACCESS-DOC-TECH.pdf

# Quelques normes pertinentes relatives au machines

## IEC 60204

Sécurité des machines – Equipements électriques des machines

Fournit les recommandations générales et spécifiques sur les aspects lié à la sécurité du câblage et de l'équipement électrique des machines

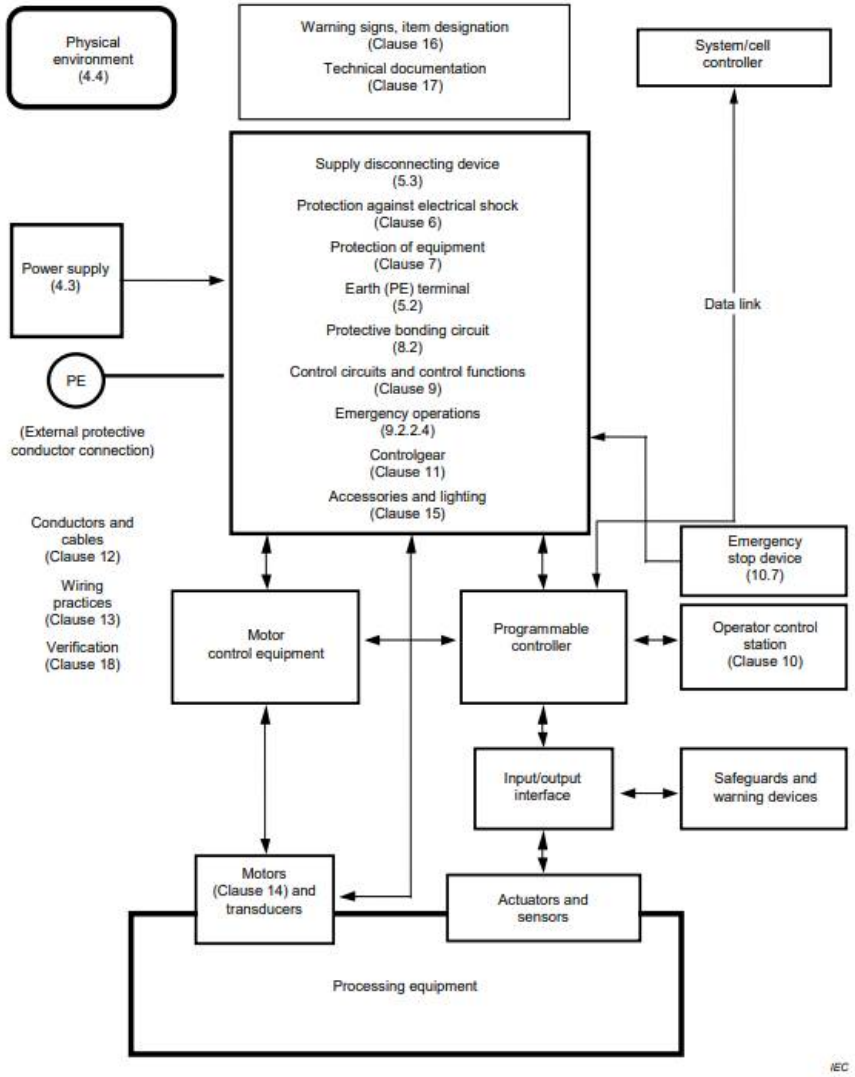



**Figure 1 – Block diagram of a typical machine**



Sources:
IEC 60204-1

# 3. Déterminer les «audits» ou évaluations qui devront être effectués par des tiers

**Informez-vous des exigences essentielles auxquelles doit répondre votre produit**
Certaines directives exigent qu'une tierce partie mette les produits à l'essai et en certifie la conformité avec les exigences essentielles, on appelle ces tierces parties des organismes notifiés (ON). Si les directives concernées n'exigent pas le recours à un ON, les fabricants peuvent faire évaluer la conformité de leurs produits dans leurs propres installations.

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Annexe IV – Machines dangereuses

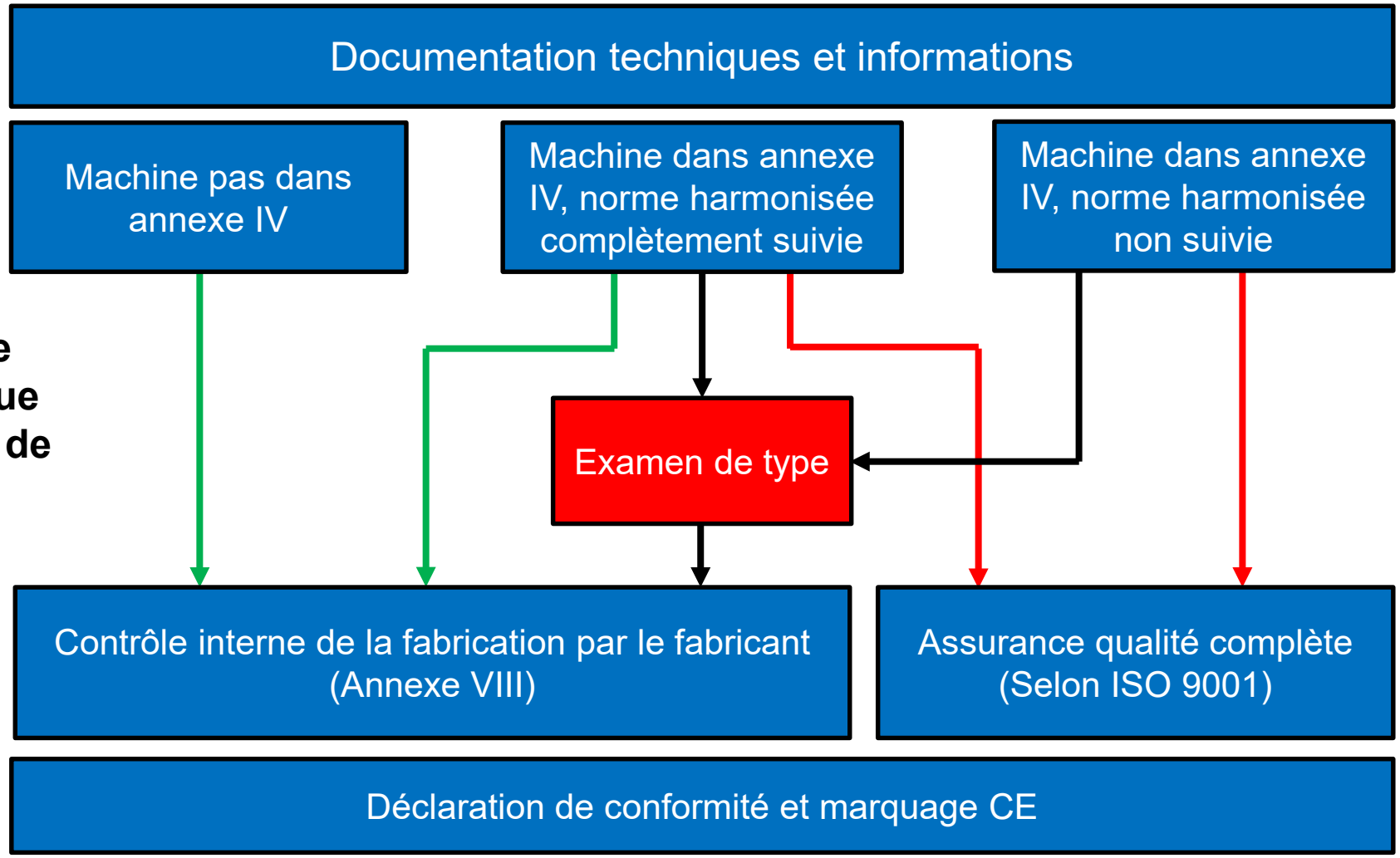
1. **Scies** circulaires pour le travail du bois ou de la viande
2. **Machines à dégauchir** à avance manuelle pour le travail du bois.
3. **Machines à raboter** sur une face
4. **Scies** à ruban à chargement et/ou à déchargement manuel pour le travail du bois ou de la viande
5. Machines combinées des types visés aux sections 1 à 4 et section 7
6. **Machines à tenonner** à plusieurs broches à avance manuelle pour le travail du bois.
7. **Toupies** à axe vertical à avance manuelle pour le travail du
8. **Scies à chaîne** portatives pour le travail du bois
9. **Presses**, y compris les plieuses, pour le travail à froid des métaux
10. **Machines de moulage** des plastiques par injection ou compression
11. **Machines de moulage** de caoutchouc par injection ou compression
12. **Machines pour les travaux souterrains**
13. **Bennes** de ramassage d'ordures ménagères à chargement manuel, comportant un **mécanisme de compression**.
14. Dispositifs amovibles de **transmission mécanique**
15. Protecteurs des dispositifs amovibles de transmission mécanique.
16. **Ponts élévateurs** pour véhicules
17. **Appareils de levage** de personnes ou de personnes et d'objets (3m)
18. Machines portatives de fixation **à charge explosive** et autres machines à chocs.
19. **Dispositifs de protection** destinés à détecter la présence de personnes.
20. **Protecteurs mobiles motorisés** avec dispositif de verrouillage destinés à être utilisés dans les machines mentionnées sections 9, 10 et 11.
21. **Blocs logiques assurant des fonctions de sécurité**.
22. Structures de protection **contre le retournement**
23. Structures de protection **contre les chutes d'objets**



Sources:
https://leuze.com

# Procédure d'évaluation de la conformité (Machine)

**La procédure dépend presque exclusivement de l'annexe IV**






Sources:
https://leuze.com

# 4. Evaluer la conformité du produit

**Comment savez-vous que votre produit répond aux exigences essentielles figurant dans les directives applicables?**

Vous devrez faire des essais et attester que votre produit est réellement conforme. Chaque directive décrit les procédures - aussi appelées « modules » - pour l'évaluation de la conformité que peut entreprendre un fabricant. Il y a huit modules d'évaluation de la conformité. Les directives applicables précisent le ou les modules qui s'appliquent à une catégorie de produits donnée.

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Les modules d’évaluation

- **Module A :** Contrôle interne de la fabrication
- **Module B :** Examen CE de type
- **Module C :** Conformité avec le type
- **Module D :** Assurance de la qualité production
- **Module E :** Assurance de la qualité produits
- **Module F :** Vérification sur produits
- **Module G :** Vérification à l’unité
- **Module H :** Assurance qualité complète (EN ISO 9001)

Ces 8 procédures peuvent se réduire à deux approches fondamentales.



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Approche 1: Contrôle de la qualité par le fabricant

Le fabricant peut engager un fournisseur de services pour avoir accès aux installations d'essai, mais il payera seulement pour l'essai ou pour d'autres éléments de l'évaluation de la conformité, pas pour la consultation ni la certification, ce pourquoi on a aussi recours à un ON.

Une entreprise peut faire, **par elle-même**, l'évaluation de la conformité des produits, si elle **possède les installations nécessaires pour faire l'essai de son produit**. Cette méthode est beaucoup moins coûteuse.



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Approche 2: Evaluation de la conformité par un ON

Le fabricant est tenu de s'adresser à un ON qui évaluera la conformité de ses produits et les certifiera, mais il reste en fin de compte responsable de leur conformité avec les exigences essentielles de l'UE.

En ce qui concerne le marquage CE, l'évaluation de la conformité avec les directives européennes peut consister en différentes activités, y compris l'essai du produit, l'inspection visuelle, l'analyse du risque ainsi que l'examen des étiquettes et des instructions relatives au produit.

Les étapes typiques qui peuvent faire partie de l'évaluation de la conformité sont notamment les suivantes :

- examen de la documentation technique relative à la conception, à la fabrication et au fonctionnement du produit;
- essai d'un ou de plusieurs aspects plus précis de chaque produit, ou d'un échantillon des produits, ou d'un exemplaire représentatif du produit;
- évaluation des systèmes liés à la qualité de la production du fabricant;
- vérification continue de la conformité de l'unité de produit.



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# 5. Préparer le dossier de conformité

**Préparez votre documentation technique et tenez-la à jour**
Toutes les directives relatives au marquage CE obligent le fabricant à produire et à rendre disponible de la documentation technique (ou un fichier technique) contenant de l'information qui démontre que le produit est conforme aux exigences de la directive.

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Préparer le dossier de conformité

Le dossier technique doit démontrer que la machine est conforme aux exigences de la présente directive.

Il doit couvrir la conception, la fabrication et le fonctionnement de la machine, dans la mesure nécessaire à l'évaluation de la conformité.

Le dossier technique doit être établi dans une ou plusieurs des langues officielles de la Communauté, à l'exception de la notice d'instructions de la machine qui doit habituellement être disponible dans la langue de tous les pays où le produit sera exporté (à quelques exceptions près)

Le contenu du dossier de conformité selon la directive machines:

*Annexe VII de la directive machines 2006/42/CE*



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# 6. Remplir la déclaration de conformité européenne et marquer le produit

**Informez-vous des exigences essentielles auxquelles doit répondre votre produit**
Certaines directives exigent qu'une tierce partie mette les produits à l'essai et en certifie la conformité avec les exigences essentielles, on appelle ces tierces parties des organismes notifiés (ON). Si les directives concernées n'exigent pas le recours à un ON, les fabricants peuvent faire évaluer la conformité de leurs produits dans leurs propres installations.

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Remplir la déclaration de conformité européenne

La déclaration devrait être mise à la disposition des autorités au point d'entrée dans l'UE. Contrairement à la documentation technique complète. Elle devrait être mise à la disposition des distributeurs de l'UE, qui peuvent être tenus de la fournir sans délai aux autorités nationales sur demande.

En général, la Déclaration de conformité est un document d'une seule page qui précise ce qui suit :

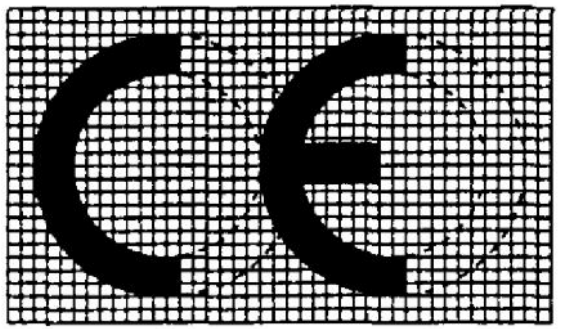
1. qui vous êtes;
2. à quel produit la déclaration renvoie;
3. quelles directives sont concernées;
4. quelles normes ont été suivies;
5. où l'on peut trouver les résultats des essais;
6. qui est responsable au sein de votre entreprise.



Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra

# Marquer le produit

Le marquage «CE» de conformité est constitué des initiales «CE» avec le graphisme suivant:



En cas de réduction ou d'agrandissement du marquage «CE», les proportions du modèle ci-dessus doivent être respectées.

Les différents éléments du marquage «CE» doivent avoir sensiblement la même dimension verticale, qui ne peut être inférieure à 5 mm. Il peut être dérogé à cette dimension minimale pour les machines de petite taille.

Le marquage «CE» doit être apposé à proximité immédiate du nom du fabricant ou de son mandataire selon la même technique.

Lorsque la procédure d'assurance qualité complète a été appliquée, le marquage «CE» doit être immédiatement suivi du numéro d'identification de l'organisme notifié.



Sources:
Directive Machines

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. ?
4. ?
5. ?
6. ?
7. ?

# Exercice 2 pour le 08.10.2021

Compléter l’exercice commencé en classe et le rendre jusqu’à vendredi 08.10.2021 – 23h59 sur le dépôt d’exercice ouvert sur Moodle.

Vous pouvez commencer tout de suite

# Merci pour votre attention

Questions ou remarques: eric.silva@hefr.ch ou via Teams

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et fiabilité des systèmes (SecuFS)

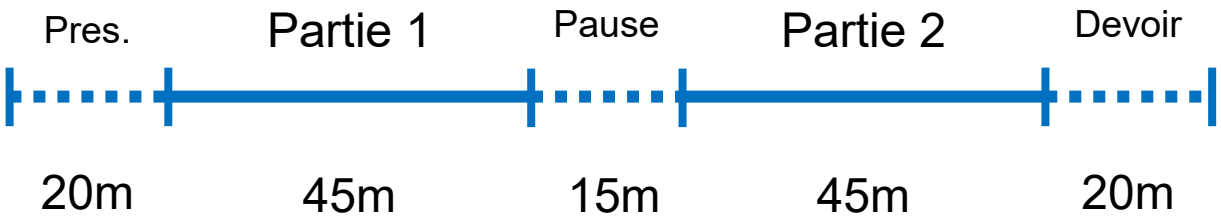
# 03 – Analyse de risque selon la norme ISO 12100

Eric Silva
11.10.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | xx.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours




**Structure du cours:**

17h30: Présentations individuelles
18h50: Début du cours
18h35: Pause de 15min
18h50: Reprise
19h35: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. Nathanaël Jaquet - Mesure acoustique de machines
4. Alexandre Murisier - ISO 13851
5. Juliette McMichael – Consignation (Lockout Tagout)
6. Mattéo Meister – ISO/PRF 22916 – Dispositifs microfluidiques
7. Harjeet Nagi - Norme de sécurité électrique et régimes de neutres

# Feedback exercices

Directive RoHS: (2002/95/CE -> 2011/65/UE -> Directive UE 2017/2012)

Limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques.

Ne demande pas de marquage CE à elle seule mais doit être appliquée dans le cadre d'un marquage pour d'autres directives.

- Catégorie 1 : gros appareils ménagers froid et hors froid (GEM)
- Catégorie 2 : petits appareils ménagers (PAM)
- Catégorie 3 : équipements informatiques et de télécommunications
- Catégorie 4 : matériels grand public
- Catégorie 5 : matériel d'éclairage
- Catégorie 6 : outils électriques et électroniques
- Catégorie 7 : jouets, équipements de loisirs et de sport
- Catégorie 8 : dispositifs médicaux
- Catégorie 9 : instruments de contrôle et de surveillance, y compris instruments de contrôle et de surveillance industriels
- Catégorie 10 : distributeurs automatiques
- Catégorie 11 : autres EEE n'entrant pas dans les catégories ci-dessus. (Electrical or Electronical Equipment)

# Feedback exercices (1)

**ISO 12100** - Appréciation du risque et réduction du risque

S'applique à tous les produits que l'on souhaite mettre sur le marché.

**2009/48/CE** - Directive, sécurité des jouets:

- S'applique aux produits conçus ou destinés, exclusivement ou non, à être utilisés à des fins de jeu par des enfants de moins de 14 ans
- Les produits énumérés à l'annexe I ne sont pas considérés comme des jouets au sens de la présente directive. (Annexe I, liste les objets non-considérés)
- La présente directive ne s'applique pas aux jouets suivants:
  a) équipements pour aires collectives de jeu destinées à une utilisation publique
  b) machines de jeu automatiques, à pièces ou non, destinées à une utilisation publique
  c) véhicules de jeu équipés de moteurs à combustion
  d) jouets machine à vapeur
  e) frondes et lance-pierres
- **Exigences**: propriétés physiques et mécaniques, inflammabilité, propriétés chimiques, propriétés électriques, hygiène, radioactivité

# Feedback exercices (2)

Normes harmonisées pour les jouets:

| N° | Référence de la norme |
|---|---|
| 1. | EN 71-1:2014+A1:2018 Sécurité des jouets — Partie 1: Propriétés mécaniques et physiques |
| 2. | EN 71-2:2011+A1:2014 Sécurité des jouets — Partie 2: Inflammabilité |
| 3. | EN 71-3:2019 Sécurité des jouets - Partie 3: Migration de certains éléments |
| 4. | EN 71-4:2013 Sécurité des jouets — Partie 4: Coffrets d'expériences chimiques et d'activités connexes |
| 5. | EN 71-5:2015 Sécurité des jouets — Partie 5: Jouets chimiques (coffrets) autres que les coffrets d'expériences |
| 6. | EN 71-7:2014+A3:2020 Sécurité des jouets — Partie 7: Peintures au doigt — Exigences et méthodes d'essai |
| 7. | EN 71-8:2018 Sécurité des jouets — Partie 8: Jouets d'activité à usage familial |
| 8. | EN 71-12:2016 Sécurité des jouets — Partie 12: N-nitrosamines et substances N-nitrosables<br>Note d'information: les valeurs limites indiquées au point a) du tableau 2 de la clause 4.2 de la norme EN 71-12:2016 Sécurité des jouets — Partie 12: N-nitrosamines et substances N-nitrosables sont inférieures aux valeurs limites à respecter indiquées au point 8 de l'annexe II, partie III de la directive 2009/48/CE. En particulier, les valeurs concernées sont les suivantes: |
| 9. | EN 71-13:2014 Sécurité des jouets — Partie 13: Jeux de table olfactifs, ensembles cosmétiques et jeux gustatifs |
| 10. | EN 71-14:2018 Sécurité des jouets - Partie 14: Trampolines à usage familial |
| 11. | EN IEC 62115:2020 Jouets électriques — Sécurité<br>EN IEC 62115:2020/A11:2020 |

| Substance | Norme EN 71-12:2016 | Directive 2009/48/CE |
|---|---|---|
| N-nitrosamines | 0,01 mg/kg | 0,05 mg/kg |
| Substances N-nitrosables | 0,1 mg/kg | 1 mg/kg |

Exemple:

La directive des jouets ne doit pas être appliquée si le produit est destiné aux personnes âgées d'au moins 14 ans, elle exige par contre l'indication de l'âge minimum sur le produit.

# Feedback exercices (3)

**Général**:

Ne pas se baser sur son expérience personnelle ni sur des «clichés» pour définir les paramètres des utilisateurs cibles (genre, âge).

Un appareil mentionné «professionnel» est souvent un argument marketing et non une réalité.

Ne pas oublier de mentionner les normes applicables, une directive est généralement difficile à appliquer telle quelle. Normes harmonisées et directives ne sont pas équivalentes.

Différence?

La procédure d'évaluation ne peut pas se limiter à des tests mais demande une analyse lors du développement

Ne pas oublier la directive machine, lorsqu'on réfléchit à un produit on a tendance à penser à ses spécificités et on en oublie la directive de base.

# Feedback exercices (3)

**Général**:

Des informations importantes peuvent être trouvées sur le site de la SUVA:

**Machine**

1. La machine est-elle équipée d'un **interrupteur de sécurité** (interrupteur principal) cadenassable? (Fig. 1) ☐ oui ☐ non
   - L'interrupteur de sécurité doit couper les alimentations en énergie électrique, pneumatique ou autre et libérer les énergies accumulées présentant un danger.

2. La machine est-elle munie d'un **interrupteur d'arrêt d'urgence** en parfait état de fonctionnement (bouton, câble, etc.)? ☐ oui ☐ non

**Protection des outils**

3. La machine est-elle munie d'un **protecteur fixe** dont l'arête inférieure est située à 400 mm max. (a) de la surface d'appui de la pièce? (Fig. 2 et 3) ☐ oui ☐ en partie ☐ non

4. Des **rideaux souples** couvrent-ils les ouvertures nécessaires pour l'usinage? (Fig. 2, pos. 1) ☐ oui ☐ en partie ☐ non

5. Les **rideaux souples** satisfont-ils aux exigences suivantes? ☐ oui ☐ en partie ☐ non
   - Les rideaux souples sont complets et en bon état.
   - Ils retombent jusqu'au niveau du support de la pièce (hauteur max.: 400 mm) (Fig. 3).
   - Ils n'entrent pas en contact avec l'outil (à contrôler avec le plus grand outil, arbre arrêté).
   - Ils correspondent aux indications de la notice d'instructions du fabricant (matériau, p. ex. PVC, PU, PP, PA, dimensions, épaisseur, nombre de couches, etc.).

Fig. 1: interrupteur de sécurité cadenassable.

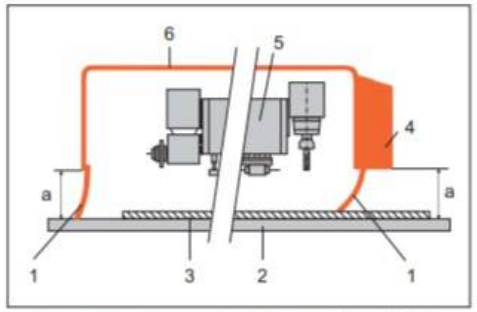



Fig. 2: dispositifs de protection d'une machine CNC à travailler le bois.

**1** Rideaux souples **2** Support de pièce **3** Pièce à travailler **4** Dispositif sensible d'arrêt (bumpers) **5** Tête d'usinage **6** Protecteur fixe

# Feedback exercices (4)

La procédure d'évaluation de la conformité dépend de la directive applicable -> Si directive machines alors selon ce qui a été vu en cours la semaine passée.

Exemple sur Compliancegate.com: https://www.compliancegate.com/bluetooth-speakers-regulations-european-union/

**Attention:**

- Parfois des directives ou normes applicables dépendent non seulement du type de machine mais aussi:
  - Des matériaux traités
  - De l'environnement de fonctionnement (espace, corps…)
  - Des produits utilisés durant le fonctionnement (Gaz, Essence…)

# Feedback exercices (5)

**Directive 2000/14/EC** (bruit de machine en extérieur)

Cette directive est applicable pour un bon nombre de machines et est souvent oubliée

**Directive 2001/95/EC** – Sécurité générale des produits

S’applique à tout produit qui est **destiné aux consommateurs** ou susceptible, d'être utilisé par les consommateurs, même s'il ne leur est pas destiné, et qui est fourni ou mis à disposition dans le cadre d'une activité commerciale, à titre onéreux ou gratuit, qu'il soit à l'état neuf, d'occasion ou reconditionné.

Cette définition ne s'applique pas aux produits d'occasion qui sont fournis en tant qu'antiquités ou en tant que produits devant être réparés ou reconditionnés préalablement à leur utilisation, pour autant que le fournisseur en informe clairement la personne à laquelle il fournit le produit;

Il est souvent difficile d’accéder aux normes harmonisées sans les acheter. Une solution est de chercher de l’aide auprès des organismes européens ou d’experts du domaine.

# Feedback exercices (5)

Exemple de recherche ensemble -> Google

# Motivations - Législation

**Législation aux États-Unis ->** https://www.osha.gov/Publications/osha3165.pdf

U.S. Department of Labor

OSHA®
Occupational Safety and Health Administration

## Job Safety and Health
## IT'S THE LAW!

**All workers have the right to:**

- A safe workplace.
- Raise a safety or health concern with your employer or OSHA, or report a work-related injury or illness, without being retaliated against.
- Receive information and training on job hazards, including all hazardous substances in your workplace.
- Request a confidential OSHA inspection of your workplace if you believe there are unsafe or unhealthy conditions. You have the right to have a representative contact OSHA on your behalf.

**Employers must:**

- Provide employees a workplace free from recognized hazards. It is illegal to retaliate against an employee for using any of their rights under the law, including raising a health and safety concern with you or with OSHA, or reporting a work-related injury or illness.
- Comply with all applicable OSHA standards.
- Notify OSHA within 8 hours of a workplace fatality or within 24 hours of any work-related inpatient hospitalization, amputation, or loss of an eye.
- Provide required training to all workers in a language and vocabulary they can understand.



Sources:
https://www.osha.gov/Publications/osha3165.pdf

# Motivations – Législation (2)

**Législation en Europe ->** Directive Machine

(23) Le fabricant ou son mandataire devrait également veiller à ce qu'une évaluation des risques soit effectuée pour la machine qu'il souhaite mettre sur le marché. À cet effet, il devrait déterminer quelles sont les exigences essentielles de santé et de sécurité qui s'appliquent à sa machine et pour lesquelles il doit prendre des mesures.



Sources:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:fr:PDF

# Motivations – Législation (3)

**Législation en Europe ->** Directive sur l'utilisation des équipements de travail (2009/104/CE)

## OBLIGATIONS DES EMPLOYEURS

*Article 3*

### Obligations générales

1. L'employeur prend les mesures nécessaires afin que les équipements de travail mis à la disposition des travailleurs dans l'entreprise ou l'établissement soient appropriés au travail à réaliser ou convenablement adaptés à cet effet, permettant d'assurer la sécurité et la santé des travailleurs lors de l'utilisation de ces équipements de travail.



Sources:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:fr:PDF

# Structure de la norme:

1. Domaine d'application
2. Références normatives
3. Termes et définitions
4. Stratégie d'appréciation du risque

**1. Généralités**

5. Appréciation du risque
   2. Information pour l'appréciation du risque
   3. Détermination des limites de la machine
   4. Identification des phénomènes dangereux
   5. Estimation du risque
   6. Evaluation du risque

**2. Appréciation du risque**

6. Réduction du risque
   2. Mesures de prévention intrinsèque
   3. Protection et mesures de prévention complémentaires
   4. Informations pour l'utilisation

**3. Réduction du risque**

7. Documentation relative à l'appréciation et la réduction du risque

**4. Documentation**


Sources:
ISO 12100

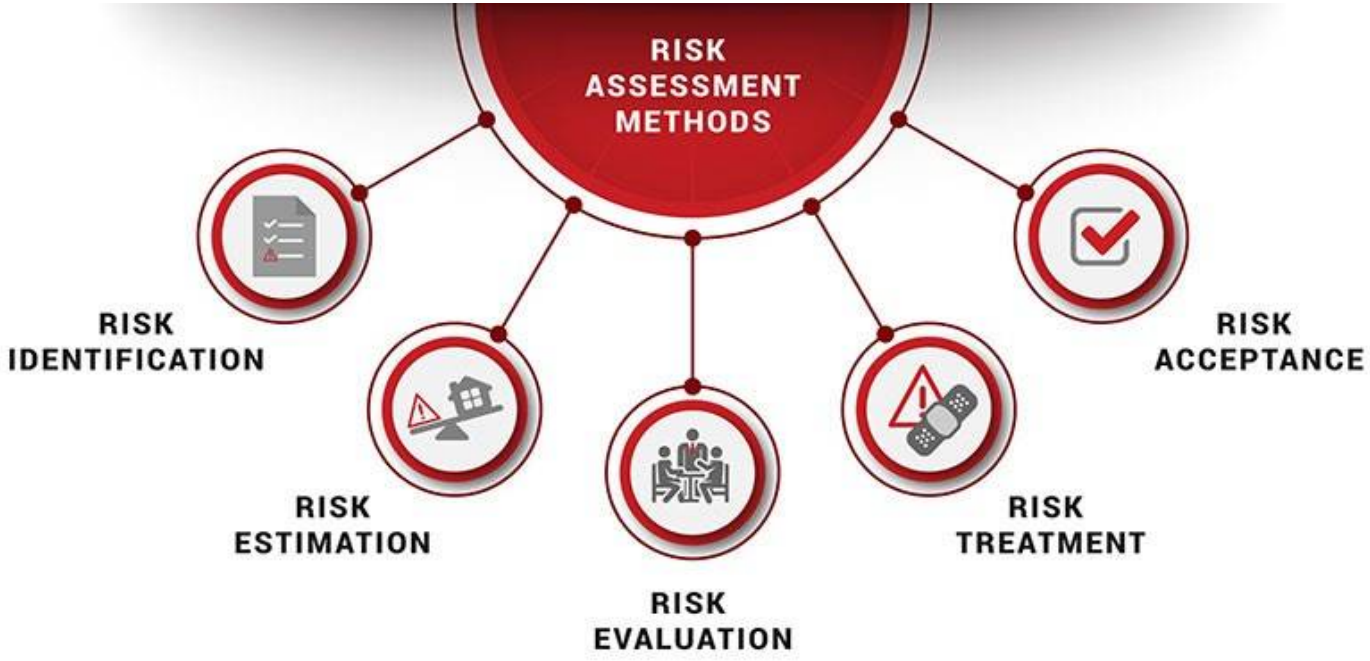
# 1. Généralités

- Domaine d’application
- Références normatives
- Termes et définitions
- Stratégie d’appréciation du risque

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Les objectifs de l'ISO 12100

1. Garantir une approche systématique
2. Identifier les dangers liés à la machine
3. Evaluer et estimer tous les risques potentiels
4. Déterminer l'étendue des systèmes de sécurité requis






Sources:
https://pecb.com/en/education-and-certification-for-individuals/risk-assessment-methods-training

# Termes et définitions

**Fiabilité:**

- aptitude d'une machine, ou de ses composants ou équipements, à accomplir sans défaillance une fonction requise, dans des conditions données et pendant un laps de temps donné

**Phénomène dangereux:**

- source potentielle de dommage, le phénomène dangereux est:
  - soit présent en permanence pendant l'utilisation normale de la machine (par exemple déplacement d'éléments mobiles dangereux, arc électrique pendant une phase de soudage, mauvaise posture, émission de bruit, température élevée),
  - soit il peut apparaître de manière inattendue (par exemple explosion, écrasement résultant d'une mise en fonctionnement intempestive ou inattendue, projection résultant d'une rupture, chute résultant d'une accélération ou d'une décélération).


Sources:
ISO 12100

# Termes et définitions (2)

**Dommage:**

- blessure physique ou atteinte à la santé

**Situation dangereuse:**

- situation dans laquelle une personne est exposée à au moins un phénomène dangereux

**Risque**

- combinaison de la probabilité d'un dommage et de la gravité de ce dommage

**Risque résiduel**

- risque subsistant après que des mesures de prévention ont été appliquées



Sources:
ISO 12100

# Termes et définitions (3)

**Estimation du risque:**

- définition de la gravité probable d'un dommage et de la probabilité de ce dommage

**Analyse du risque:**

- combinaison de la détermination des limites de la machine, de l'identification des phénomènes dangereux et de l'estimation du risque

**Evaluation du risque:**

- jugement destiné à établir, à partir de l'analyse du risque, si les objectifs de réduction du risque ont été atteints

**Réduction adéquate du risque:**

- réduction du risque répondant au moins aux exigences légales, l'état de la technique du moment étant pris en considération

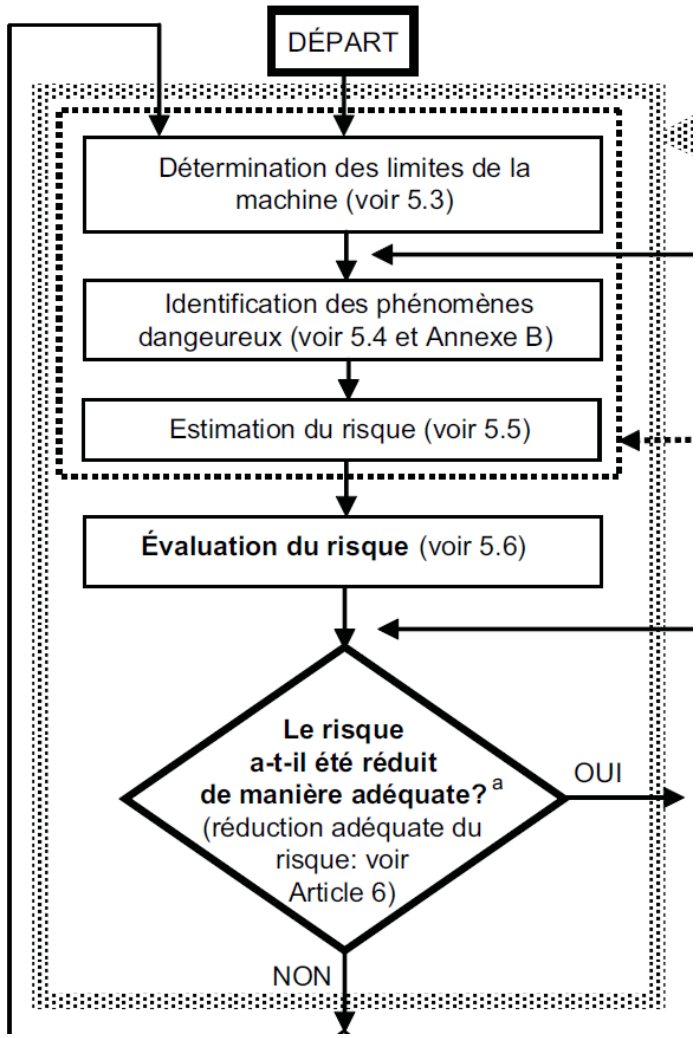


Sources:
ISO 12100

# Stratégie d'appréciation et réduction du risque

Pour mettre en œuvre une appréciation du risque et une réduction du risque, le concepteur doit accomplir les actions suivantes, dans l'ordre donné:

a) déterminer les limites de la machine, qui incluent l'utilisation normale et tout mauvais usage raisonnablement prévisible;
b) identifier les phénomènes dangereux et les situations dangereuses qui leur sont liées;
c) estimer le risque pour chacun des phénomènes dangereux et situations dangereuses identifiés;
d) évaluer le risque et prendre des décisions quant à la nécessité de le réduire;
e) supprimer le phénomène dangereux, ou réduire le risque qui lui est associé, en prenant des mesures de prévention.




Sources:
ISO 12100

# Facteurs d’appréciation du risque

Lorsqu'on procède ainsi, il est nécessaire de prendre en compte les quatre facteurs suivants, dans l'ordre de préférence suivant:

- la sécurité de la machine pendant toutes les phases de son cycle de vie;
- l'aptitude de la machine à accomplir sa fonction;
- la commodité d'emploi de la machine;
- le coût de la réalisation, de l'exploitation et du démantèlement de la machine.

NOTE 1
Pour appliquer au mieux ces principes, il est nécessaire de connaître l'utilisation de la machine, l'historique des accidents et les données enregistrées en ce qui concerne la santé, les techniques de réduction du risque disponibles et le cadre législatif et réglementaire dans lequel la machine est destinée à être utilisée.

NOTE 2
Une conception de machine acceptable à un moment donné peut cesser de l'être lorsque le progrès technique permet de concevoir une machine équivalente présentant un risque plus faible.


Sources:
ISO 12100

# Que doit couvrir l'appréciation du risque?

L'appréciation du risque de la machine entière doit couvrir **toutes les phases de son cycle de vie**:

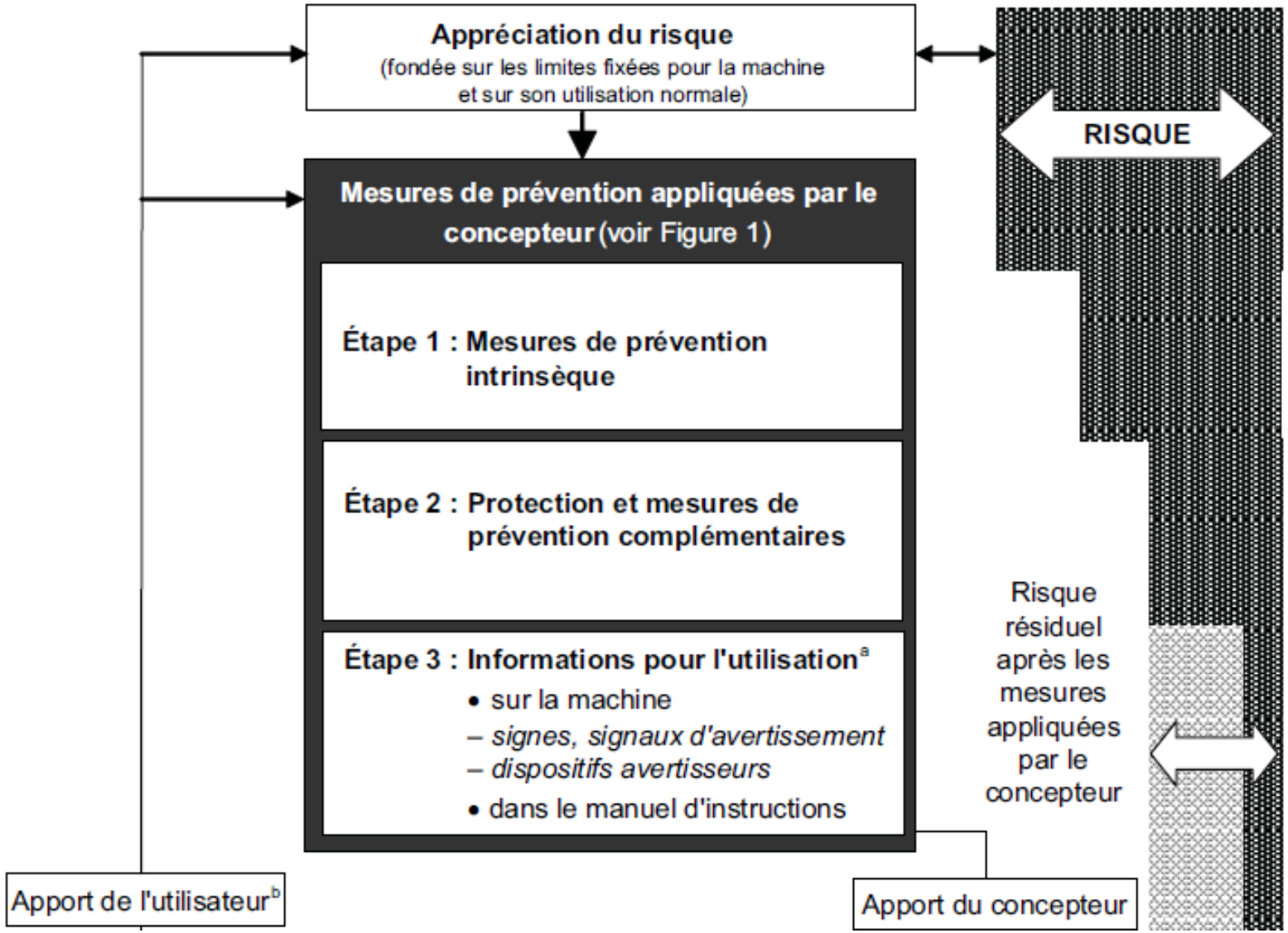
- Construction
- Transport
- Assemblage
- Installation
- Mise en service
- Réglage
- Utilisation (réglage/nettoyage et maintenance)
- Mise hors service
- Démantèlement
- Mise au rebut

L'appréciation du risque de la machine entière doit couvrir **toutes les personnes interagissant avec elle durant son cycle de vie**

L'appréciation du risque de la machine entière doit prendre en compte **l'utilisation normal et le mauvais usage raisonnablement prévisible**.


Sources:
ISO 12100

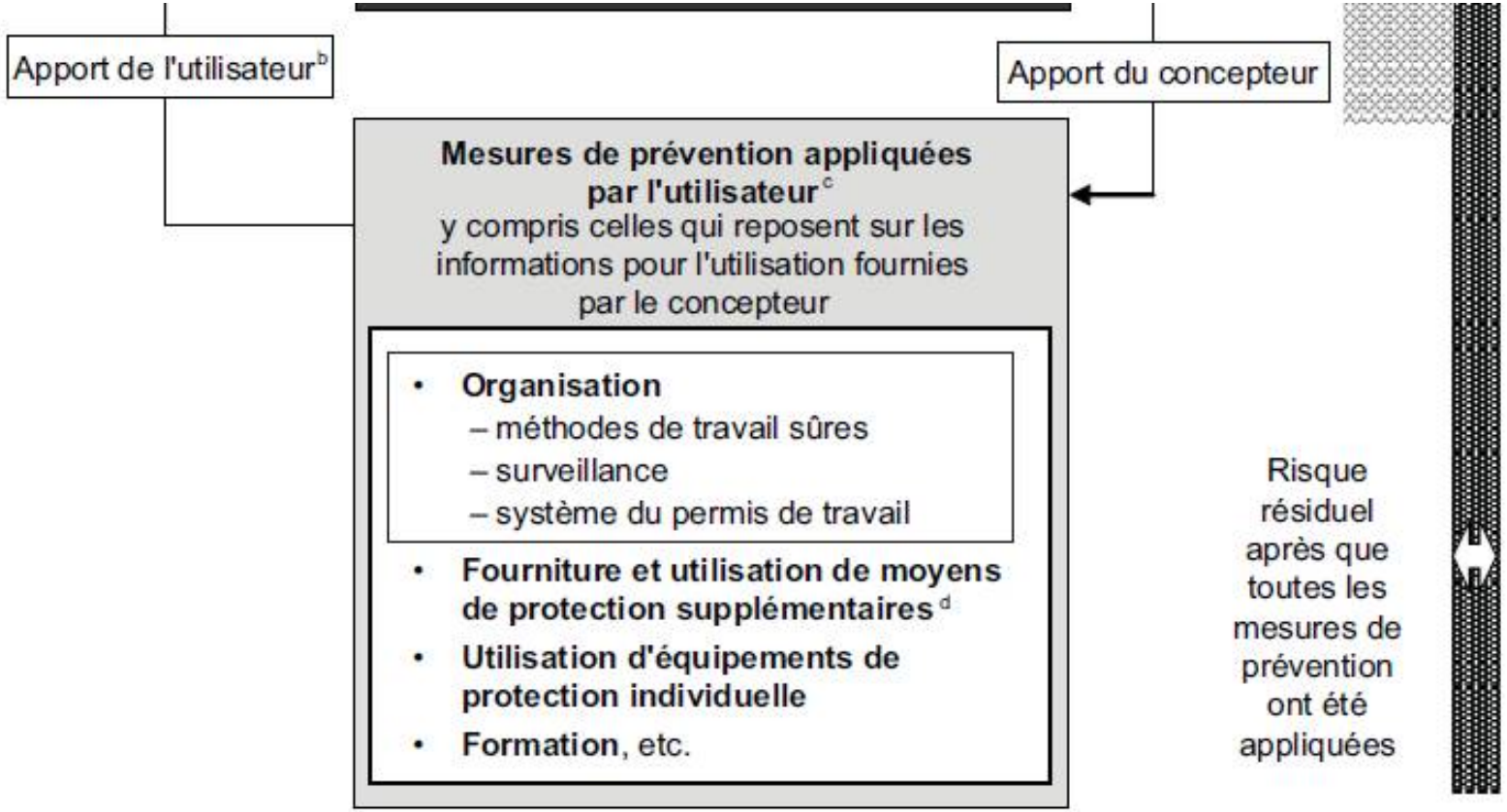
# Combinaison des mesures concepteur-utilisateur






Sources:
ISO 12100

# Combinaison des mesures concepteur-utilisateur (2)






Sources:
ISO 12100

# Structure de la norme:

1. Domaine d'application
2. Références normatives
3. Termes et définitions
4. Stratégie d'appréciation du risque

**1. Généralités**

5. Appréciation du risque
   2. Information pour l'appréciation du risque
   3. Détermination des limites de la machine
   4. Identification des phénomènes dangereux
   5. Estimation du risque
   6. Evaluation du risque

**2. Appréciation du risque**

6. Réduction du risque
   2. Mesures de prévention intrinsèque
   3. Protection et mesures de prévention complémentaires
   4. Informations pour l'utilisation

**3. Réduction du risque**

7. Documentation relative à l'appréciation et la réduction du risque

**4. Documentation**



Sources:
ISO 12100

# 2. Appréciation du risque

- Information pour l'appréciation du risque
- Détermination des limites de la machine
- Identification des phénomènes dangereux
- Estimation du risque
- Evaluation du risque

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Information pour l'appréciation du risque

Afin de procéder à l'appréciation du risque, les informations suivantes sont nécessaire:

1. **Description de la machine**
   a. Spécifications de l'utilisateur final
   b. Spécifications de la machine
      - Phases du cycle de vie
      - Plans de conception et autre moyens de définition de la machine
      - Sources d'énergie requises et mode d'alimentation
   c. Documentation relative aux conceptions précédentes de machines similaires (si applicable)
   d. Informations pour l'utilisation de la machine
2. **Réglementations, normes et autres documents applicables**
   a. Réglementations applicables
   b. Normes pertinentes
   c. Spécifications techniques pertinentes
   d. Fiches de données de sécurité pertinentes


Sources:
ISO 12100

# Information pour l'appréciation du risque (2)

Afin de procéder à l'appréciation du risque, les informations suivantes sont nécessaire:

3. **Expérience d'utilisation**
   a. Historique d'accidents, incidents ou dysfonctionnements de la machine ou machine similaire
   b. Historique d'atteintes à la santé résultant, par exemple d'émissions (bruits, vibrations, poussière, fumée), de produits chimiques ou de matériaux traités par la machine
   c. Expérience acquise par des utilisateurs de machines analogues
4. **Principes ergonomiques pertinents**
   a. Position de l'utilisateur
   b. Charges à transporter par l'utilisateur
   c. Qualité de l'interface entre l'utilisateur et la machine
   d. …

**L'absence d'historique d'accidents**, un petit nombre d'accidents ou de faible gravité ne devraient **pas être automatiquement considérés comme une présomption de faible risque**.

# Déterminer les limites de la machine

Elles sont divisées en quatre principaux types:

1. Limites d'utilisation
   - Mode de fonctionnement et exigences d'intervention (y compris interventions dues à un dysfonctionnement de la machine
   - Utilisation de la machine (industrielle, domestique…), par des personnes différenciées par leur sexe, âge, main dominante, capacités physiques limitées, taille, force…
   - Niveau de formation attendu, expérience ou aptitudes prévisible des utilisateurs
     - Opérateurs, Techniciens ou personnel de maintenance, stagiaire ou apprentis, tout public
   - Exposition d'autres personnes au phénomènes dangereux propres à la machine
     - Opérateurs de machines voisines
     - Personnes ne connaissant pas la machines mais connaissant les protocoles de sécurité du site (personnel administratif)
     - Personnes n'ayant pratiquement aucune connaissance des phénomènes dangereux ni des règles de sécurité en vigueur sur le site


Sources:
ISO 12100

# Déterminer les limites de la machine (2)

2. Limites dans l'espace
   - Amplitude des mouvements de la machine
   - Exigences dimensionnelles pour les personnes interagissant avec la machine
   - Interaction humaine, par exemple l'interface opérateur-machine
   - Interface machine-source d'énergie
3. Limites dans le temps
   - Durée de vie de la machine et/ou de certains de ses composants estimée en tenant compte de son utilisation normale et son mauvais usage raisonnablement prévisible
   - Fréquences d'entretien recommandées
4. Autres limites
   - Propriétés de matériaux traités
   - Environnementales (températures minimales et maximales, humidité, intérieur/extérieur…)
   - Nettoyage et niveau de propreté requis


Sources:
ISO 12100

# Identifier les phénomènes dangereux (Tâches)

Les phénomènes dangereux peuvent subvenir par exemple lors des tâche suivantes:

- réglage;
- essais;
- apprentissage/programmation;
- changement de processus/outil;
- démarrage;
- tous les modes de fonctionnement;
- alimentation de la machine;
- retrait de produits de la machine;
- arrêt de la machine;
- arrêt de la machine en cas d'urgence;
- reprise du fonctionnement après bourrage ou blocage;
- redémarrage après arrêt imprévu;
- recherche de défauts/de pannes (intervention de l'opérateur);
- nettoyage et entretien;
- maintenance préventive;
- maintenance corrective.

En outre, les phénomènes non liés à des tâches peuvent devoir être considérés selon la machine: foudre, charge dues à la neige, bruit, rupture de la machine, éclatement de tuyau hydraulique…


Sources:
ISO 12100

# Identifier les phénomènes dangereux (Etat machine)

Les phénomènes dangereux peuvent, par exemple, subvenir dans les états suivants de la machine:

1. la machine accomplit la fonction prévue (fonctionnement normal);
2. la machine n'accomplit pas la fonction prévue (dysfonctionnement) pour différentes raisons, comprenant
   - la variation d'une caractéristique ou d'une dimension du matériau travaillé ou de la pièce,
   - la défaillance d'un ou de plusieurs de ses composants ou des circuits auxquels elle est reliée,
   - des perturbations d'origine externe (par exemple chocs, vibrations, perturbations électromagnétiques),
   - une erreur ou une imperfection dans la conception (par exemple erreur affectant un logiciel),
   - une perturbation dans son alimentation en énergie, et
   - les conditions d'environnement (par exemple un sol endommagé).

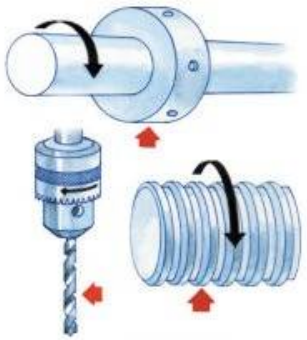
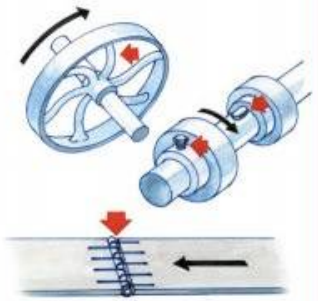
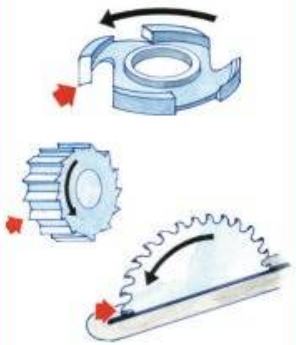
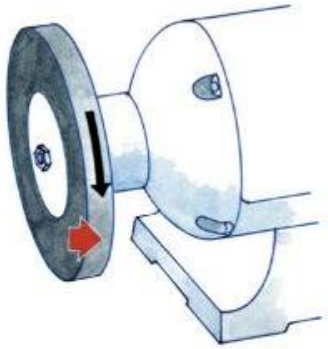
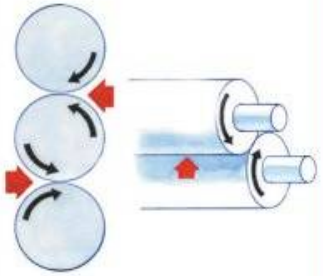
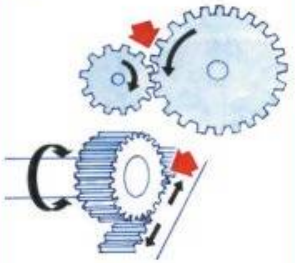

Source
ISO 12100

# Identifier les phénomènes dangereux (Opérateur)

Les phénomènes dangereux peuvent apparaître à cause du comportement de l'opérateur:

- la perte de contrôle de la machine par l'opérateur (particulièrement pour les machines portatives ou mobiles);
- le comportement réflexe d'une personne en cas de dysfonctionnement, d'incident ou de défaillance en cours d'utilisation de la machine;
- un comportement résultant d'un défaut de concentration ou d'une négligence;
- un comportement résultant de l'application de la «loi du moindre effort» au cours de l'accomplissement d'une tâche;
- un comportement résultant d'une incitation à maintenir la machine en marche à tout prix;
- le comportement de certaines personnes (par exemple les enfants, les personnes handicapées).

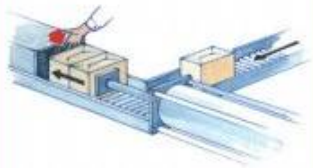
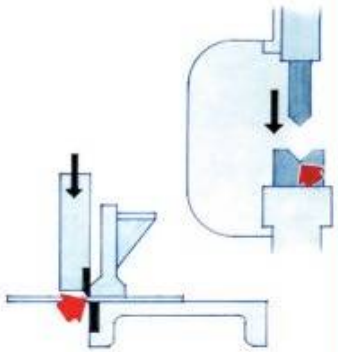
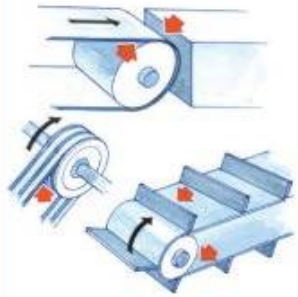
# Identifier les phénomènes dangereux (Exemples)

| PHÉNOMÈNE DANGEREUX | CONSÉQUENCES POSSIBLES | PHÉNOMÈNE DANGEREUX | CONSÉQUENCES POSSIBLES | PHÉNOMÈNE DANGEREUX | CONSÉQUENCES POSSIBLES |
|---|---|---|---|---|---|
| 1  | • Enroulement<br>• Happement<br>• Entraînement | 2  | • Enroulement<br>• Happement<br>• Choc<br>• Écrasement<br>• Entraînement<br>• Brûlure<br>• Piqûre | 3  | • Coupure<br>• Sectionnement<br>• Projection<br>• Entraînement |
| 6  | • Happement<br>• Abrasion<br>• Entraînement<br>• Brûlure<br>• Projection | 7  | • Entraînement<br>• Écrasement<br>• Brûlure | 8  | • Entraînement<br>• Écrasement<br>• Sectionnement |



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

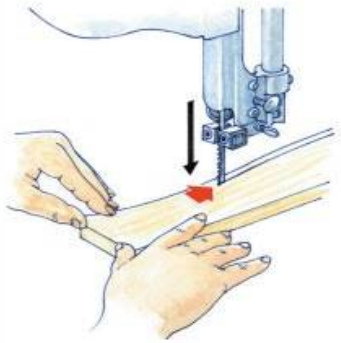
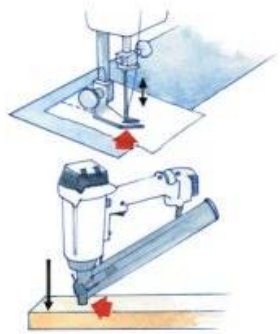
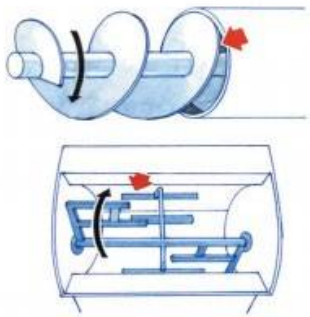
# Identifier les phénomènes dangereux (Exemples)

| | | | | | |
|---|---|---|---|---|---|
| 11 | • Choc<br>• Écrasement | 12 | • Entraînement<br>• Abrasion | 13  | • Cisaillement<br>• Sectionnement<br>• Entraînement<br>• Écrasement<br>• Choc |
| 16 | • Perforation<br>• Projection<br>• Brûlure<br>• Choc | 17  | • Écrasement<br>• Cisaillement<br>• Sectionnement<br>• Projection | 18  | • Entraînement<br>• Écrasement<br>• Arrachement<br>• Sectionnement<br>• Choc |



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

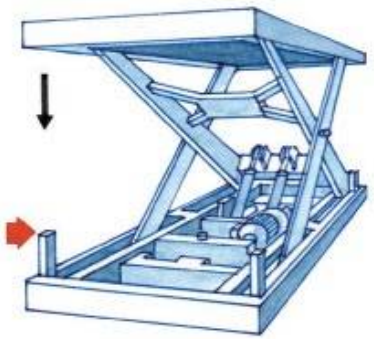
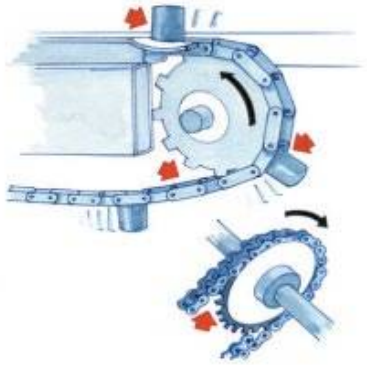
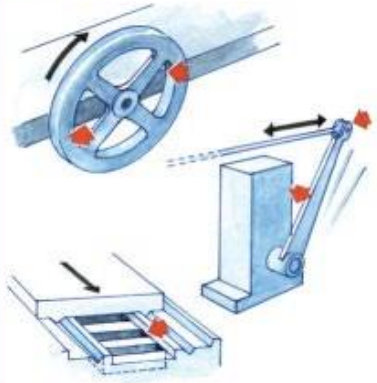
# Identifier les phénomènes dangereux (Exemples)

| PHÉNOMÈNE DANGEREUX | CONSÉQUENCES POSSIBLES | PHÉNOMÈNE DANGEREUX | CONSÉQUENCES POSSIBLES |
|---|---|---|---|
| 4  | • Coupure<br>• Sectionnement<br>• Projection | 5  | • Perforation<br>• Piqûre<br>• Poinçonnement<br>• Projection |
| 9  | • Enroulement<br>• Happement<br>• Choc<br>• Entraînement<br>• Sectionnement<br>• Cisaillement | 10 | • Choc<br>• Écrasement |



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Identifier les phénomènes dangereux (Exemples)

| | | | |
|---|---|---|---|
| 14  | • Écrasement<br>• Cisaillement<br>• Sectionnement | 15 | • Choc<br>• Écrasement<br>• Entraînement |
| 19  | • Entraînement<br>• Écrasement<br>• Arrachement<br>• Sectionnement<br>• Choc | 20  | • Cisaillement<br>• Sectionnement<br>• Enroulement<br>• Happement<br>• Choc<br>• Écrasement<br>• Entraînement |



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Identifier les phénomènes dangereux (Dommages)

Les dommages occasionnés par les différents phénomènes dangereux peuvent être:

**Mécaniques:**

- Fracture/entorse/foulure
- Coupure/lacération
- Amputation
- Perforation/piqûre
- Écorchure/égratignure/ecchymose/contusion/plaie ouverte
- Irritation
- Brûlure par friction
- Blessures multiples
- Décès



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Identifier les phénomènes dangereux (Dommages)

**Electriques:**

- Choc électrique
- Brûlure électrique
- Électrisation (sans décès)
- Électrocution (avec décès)

**Thermiques:**

- Brûlure par la chaleur (y compris le feu et les flammes) ou l'eau bouillante
- Effet de la chaleur ou de la lumière
- Engelure/hypothermie

**Bruit:**

- Détérioration de l'acuité auditive, de l'équilibre
- Fatigue, stress, baisse de la vigilance



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Identifier les phénomènes dangereux (Dommages)

**Vibrations:**

- Lombalgies/traumatismes vertébraux
- Troubles neurologiques et ostéoarticulaires
- Troubles vasculaires (par ex. phénomène dit « des doigts blancs »)
- Inconfort (par ex. engourdissement)

**Rayonnements:**

- Brûlures
- Mutations génétiques

**Contamination par des matériaux ou produits:**

- Dommages pour la santé
- Décès
- Brûlure chimique
- Dommages résultant d'incendies/d'explosions



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Identifier les phénomènes dangereux (Dommages)

**Principes ergonomiques:**

- Effets physiologiques (par ex. troubles musculosquelettiques « TMS ») résultant, par ex., de postures contraignantes, d'efforts excessifs ou répétitifs
- Effets psycho-physiologiques (effets de la surcharge mentale, notamment le stress)
- Blessures résultant de fonctionnements intempestifs, eux-mêmes causés par des erreurs humaines favorisées par une mauvaise conception de l'interface « homme-machine » (par ex. une disposition inadéquate des organes de service)



Sources
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Estimation du risque (Gravité du dommage)

Gravité du dommage : **G**

- **G1**
  Lésion légère (normalement réversible) ; par ex. écorchure, lacération, bleu, blessure légère qui nécessite des premiers soins, etc.
- **G2**
  Lésion grave (normalement irréversible, y compris le décès) ; par ex. membre brisé ou arraché, blessure grave avec points de suture, décès, etc.


Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Estimation du risque (Fréquence)

Fréquence et/ou durée d'exposition au phénomène dangereux : **F**

Selon le besoin d'accès à la zone dangereuse (par ex. pour des raisons de production, d'entretien ou de réparation), la nature de l'accès (par ex. l'alimentation manuelle de matières), le temps passé dans la zone dangereuse, le nombre de personnes demandant l'accès et la fréquence d'accès

- **F1** Rare à assez fréquente et/ou courte durée d'exposition
- **F2** Fréquente à continue et/ou longue durée d'exposition


Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Estimation du risque (Probabilité d'occurrence)

Probabilité d'occurrence de l'événement dangereux : **O**

Selon les données de fiabilité, l'historique en matière d'accidents et la comparaison des risques

- **O1** Très faible : technologie stable, éprouvée et reconnue pour les applications de sécurité
- **O2** Faible : événement relié à une défaillance technique de probabilité supérieure ou égale à 10-5 bris/heure (1 bris/100 000 heures); ou bien, événement entraîné par l'action d'une personne qualifiée, expérimentée, formée, effectuant une tâche unique, etc.
- **O3** Élevée : événement relié à une défaillance technique de probabilité supérieure ou égale à 10-3 bris/heure (1 bris/1 000 heures); ou bien, événement entraîné par l'action d'une personne sans expérience ou formation particulière.



Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Estimation du risque (Possibilité d’évitement)

Possibilité d’évitement du dommage : **P**

En fonction du mode d’exploitation de la machine (avec ou sans travailleur, par des travailleurs expérimentés), de la rapidité d’apparition de l’événement, de la conscience du risque, de la possibilité humaine d’éviter ou de limiter le risque, de l’expérience ou de la connaissance pratique du phénomène dangereux

- **P1** Possible dans certaines conditions
- **P2** Impossible ou rarement possible


Sources:
https://www.cnesst.gouv.qc.ca/Publications/200/Documents/DC200-1581web.pdf

# Evaluation des risques

Elle est réalisée après une estimation des risques visant à déterminer si une réduction des risques est nécessaire ou si la sécurité été obtenue.

Si une réduction du risque est nécessaire, la méthode en 3 étapes de l'ISO 12100 est recommandée.

Il est important de vérifier qu'aucun danger supplémentaire n'a été créé après la mise en place des mesures de sécurité

**La méthode d'évaluation du risque sera approfondie lors de la prochaine session de ce cours.**

# Structure de la norme:

| | |
|---|---|
| 1. Domaine d'application<br>2. Références normatives<br>3. Termes et définitions<br>4. Stratégie d'appréciation du risque | **1. Généralités** |
| 5. Appréciation du risque<br>2. Information pour l'appréciation du risque<br>3. Détermination des limites de la machine<br>4. Identification des phénomènes dangereux<br>5. Estimation du risque<br>6. Evaluation du risque | **2. Appréciation du risque** |
| 6. Réduction du risque<br>2. Mesures de prévention intrinsèque<br>3. Protection et mesures de prévention complémentaires<br>4. Informations pour l'utilisation | **3. Réduction du risque** |
| 7. Documentation relative à l'appréciation et la réduction du risque | **4. Documentation** |


Sources:
ISO 12100

# 3. Réduction du risque

- Mesures de prévention intrinsèque
- Protection et mesures de prévention complémentaires
- Informations pour l'utilisation

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Sélection de la réduction du risque

**Trois critères de sélection de la réduction du risque:**

- **Efficacité**: La réduction du risque permet-elle de le contrôler de manière adéquate en réduisant sa probabilité ou gravité tout en évitant de mettre en péril le système?
- **Faisabilité**: La réduction du risque visée peut-elle être appliquée dans un laps de temps acceptable et grâce à une technologie existante?
- **Coût**: Est-ce que le coût de la réduction du risque pourra être supporté?

**Trois étapes de décision pour la réduction du risque:**

**Etape 1**: Modification de la conception

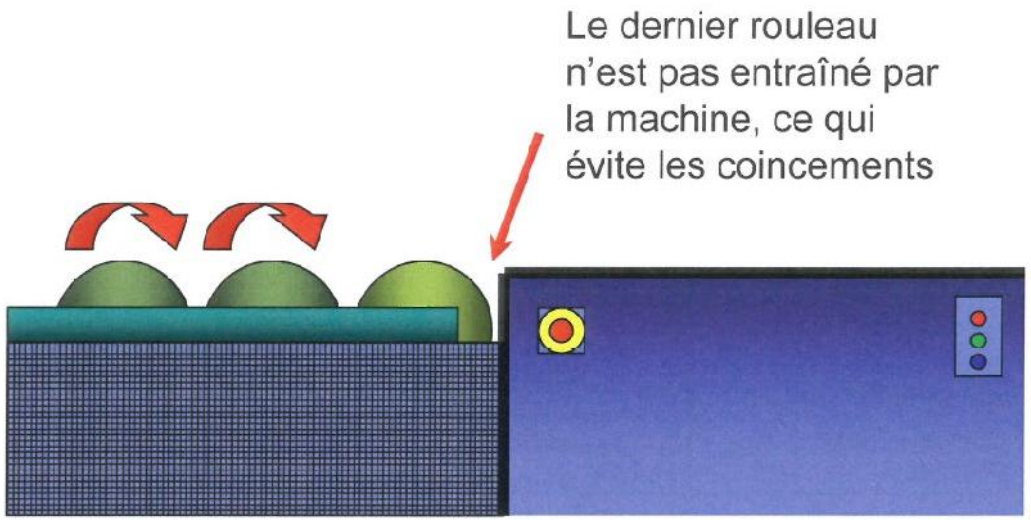
**Etape 2**: Application de mesures de protection

**Etape 3**: Information concernant l'utilisation

Il est important de vérifier qu'aucun danger supplémentaire n'a été créé après la mise en place des mesures de sécurité.

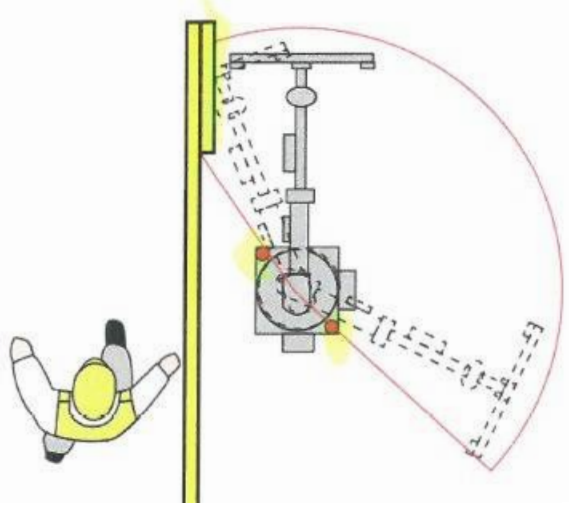
# Hiérarchie et priorisation des réduction de risque:

1. Elimination ou substitution du risque
   - Modification du processus afin d'éliminer l'interaction humaine
   - Elimination des points de pincements
   - Manutention automatisée des matériaux



# Hiérarchie et priorisation des réduction de risque: (2)

2. Technologie de protection
   - Butées mécaniques
   - Barrières
   - Dispositifs de verrouillage
   - Présence de dispositifs de détection, bandes de sécurité
   - Commandes bimanuelles



Des points d'arrêt attachés au robot et des protecteurs renforcés permettent d'empêcher au robot d'emprunter ce passage au-delà du protecteur.

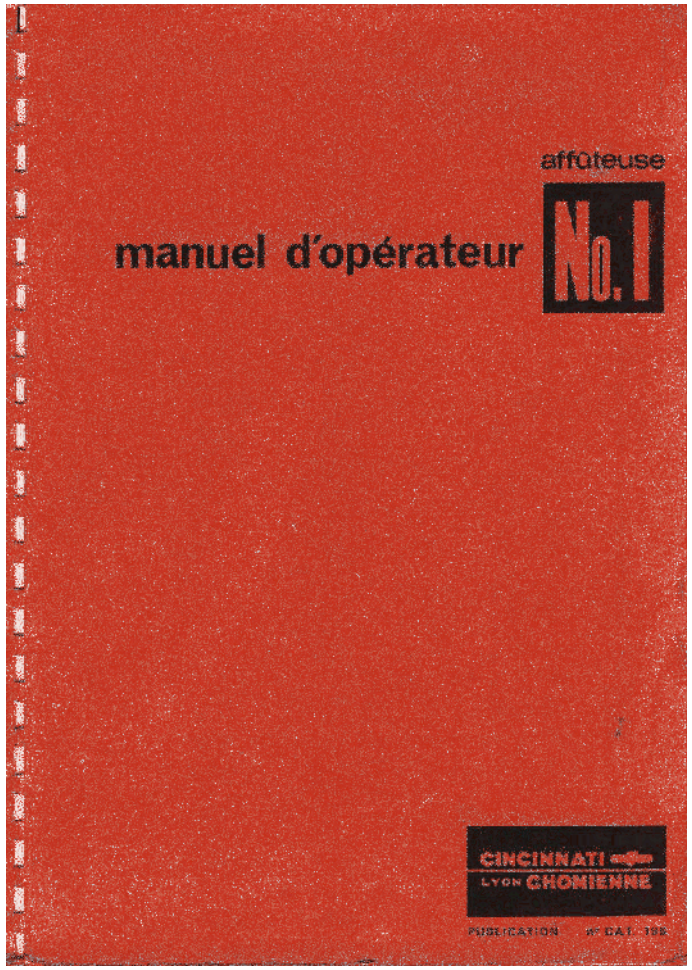
# Hiérarchie et priorisation des réduction de risque: (3)

3. Mesures d'information
   - Eclairage, balises et lumières stroboscopiques
   - Avertissement avec une supervision informatique
   - Signalisation
   - Marquage peint sur le sol de l'espace restreint
   - Beepers
   - Klaxons
   - Etiquettes

Sour
Pilz – Formation CMSE

# Hiérarchie et priorisation des réduction de risque: (4)

4. Formation et procédures
   - Procédures de travail sûres
   - Inspection des équipements de sécurité
   - Formation
   - Verrouillage



# Hiérarchie et priorisation des réduction de risque: (5)

5. Equipements de protection individuelle
   - Lunettes de sécurité
   - Bouchons d'oreilles
   - Masques
   - Gants
   - Casques de protection

Source
Pilz – Formation CMSE

# Structure de la norme:

| | |
|---|---|
| 1. Domaine d'application<br>2. Références normatives<br>3. Termes et définitions<br>4. Stratégie d'appréciation du risque | **1. Généralités** |
| 5. Appréciation du risque<br>2. Information pour l'appréciation du risque<br>3. Détermination des limites de la machine<br>4. Identification des phénomènes dangereux<br>5. Estimation du risque<br>6. Evaluation du risque | **2. Appréciation du risque** |
| 6. Réduction du risque<br>2. Mesures de prévention intrinsèque<br>3. Protection et mesures de prévention complémentaires<br>4. Informations pour l'utilisation | **3. Réduction du risque** |
| 7. Documentation relative à l'appréciation et la réduction du risque | **4. Documentation** |


Sources:
ISO 12100

# 2. Documentation

- Documentation relative à l'appréciation du risque et à la réduction du risque

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# La documentation doit inclure

- Les informations concernant la machine pour laquelle l'appréciation a été faite (spécifications, limites, utilisation normale)
- Les phénomènes dangereux identifiées – Situations et événements considérés
- Les informations sur lesquelles l'appréciation des risques a été fondée (données utilisées et sources)
- Les objectifs à atteindre par les mesures de sécurité
- Les mesures de sécurité mises en œuvre
- Tous les risques résiduels associés à la machine
- Les résultats de l'évaluation finale des risques

# Exercice pour le 19.10.2020

De manière individuelle, chaque étudiant doit:

- Choisir un appareil ou une machine à étudier (potentiellement le même que la semaine précédente)
- Définir les phénomènes dangereux se rapportant à ce produit
- Définir un niveau de gravité pour chaque phénomène dangereux
- Réfléchir à des phénomènes dangereux qui pourraient se produire à d'autres moments que lors du fonctionnement normal de la machine (p.ex. Installation, mise au rebut…)

À rendre jusqu'au 19.10.2020 à 12h sur Moodle

Vous pouvez commencer tout de suite

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. Nathanaël Jaquet - Mesure acoustique de machines
4. Alexandre Murisier - ISO 13851
5. Juliette McMichael – Consignation (Lockout Tagout)
6. Mattéo Meister – ISO/PRF 22916 – Dispositifs microfluidiques
7. Harjeet Nagi - Norme de sécurité électrique et régimes de neutres

# Merci pour votre attention

Questions ou remarques: eric.silva@hefr.ch ou via Teams

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et Automatisation (SecuFS)

# 05 – Méthodologies d’analyse de risque et workshop

Eric Silva
18.10.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | xx.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours

**Structure du cours:**

17h30: Intro
18h50: Workshop
19h55: Fin du cours

# Avant de démarrer une analyse de risque

1. **Identifier les ressources à protéger:**
   - Les opérateurs
   - Le personnel de nettoyage
   - Le personnel de la maintenance
   - Les équipements (éviter d'endommager la machine)
   - Le produit
   - L'environnement

2. **Identifier, pour chaque ressource, le niveau de risque acceptable**

3. **Sélectionner la méthode d'analyse**


Sources:
Pilz – Formation CMSE

# Les 2 principales approches

**Méthode déductive:**

On part de l'hypothèse d'un événement final et on recherche les événements susceptibles d'en être la cause (Approche Top-down)

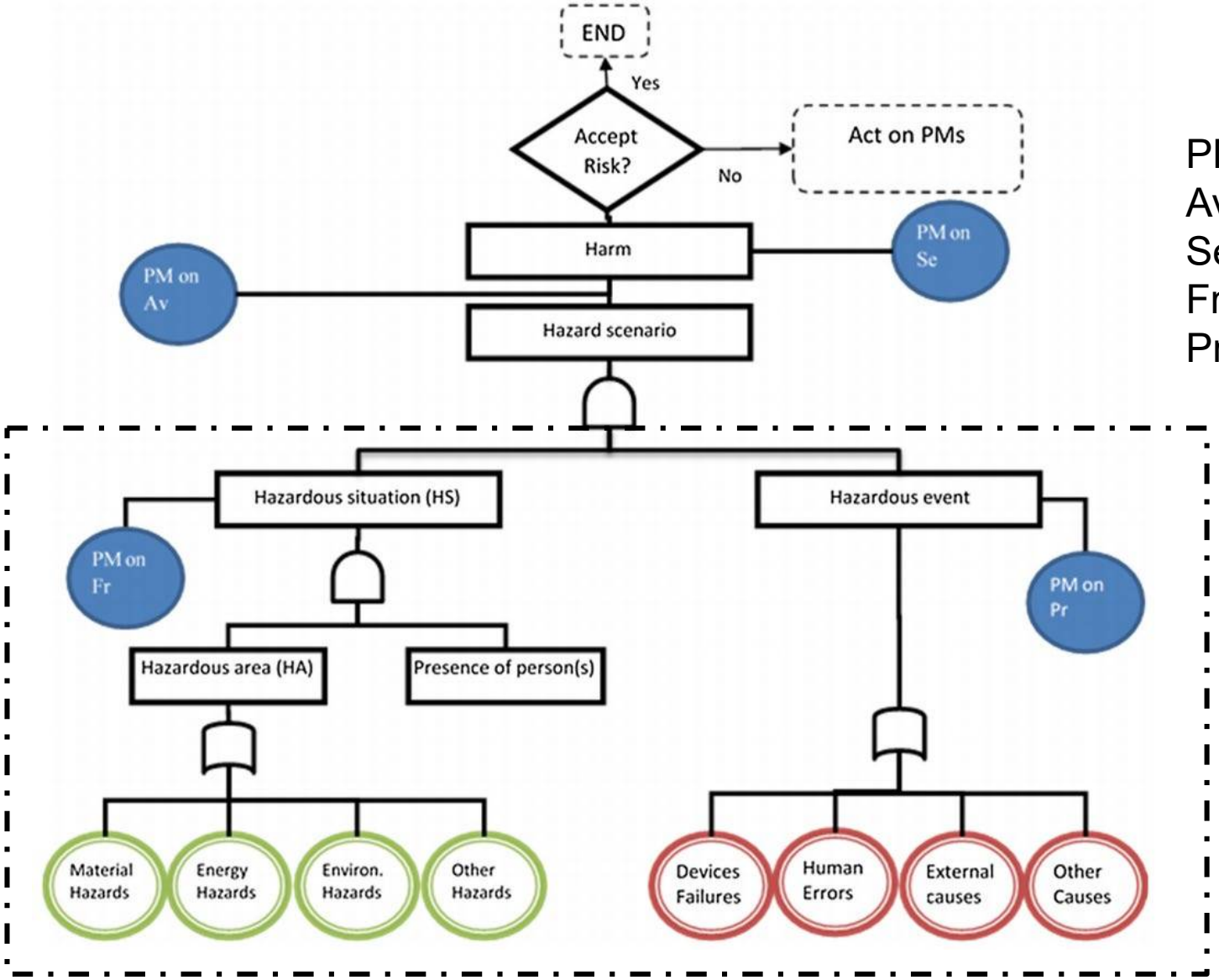
- Analyse par arbre de défaillance

**Méthode inductive: -> Présentée dans ce cours**

On part de l'hypothèse de la défaillance d'un composant puis on identifie les événements susceptibles d'être déclenchés par cette défaillance (Approche Bottom-Up)

- Analyse préliminaire des modes de défaillance et des Effets
  - Matrice des risques
  - Graphique des risques
  - Indice de criticité
- Analyse des Modes de Défaillance et des Effets (AMDE ou FMEA)

# Représentation de l'analyse de risque




PM = Protective Measure
Av = Avoiding Harm
Se = Scenario Severity
Fr = Frequency of exposure
Pr = Probability of occurence

Probability of the scenario



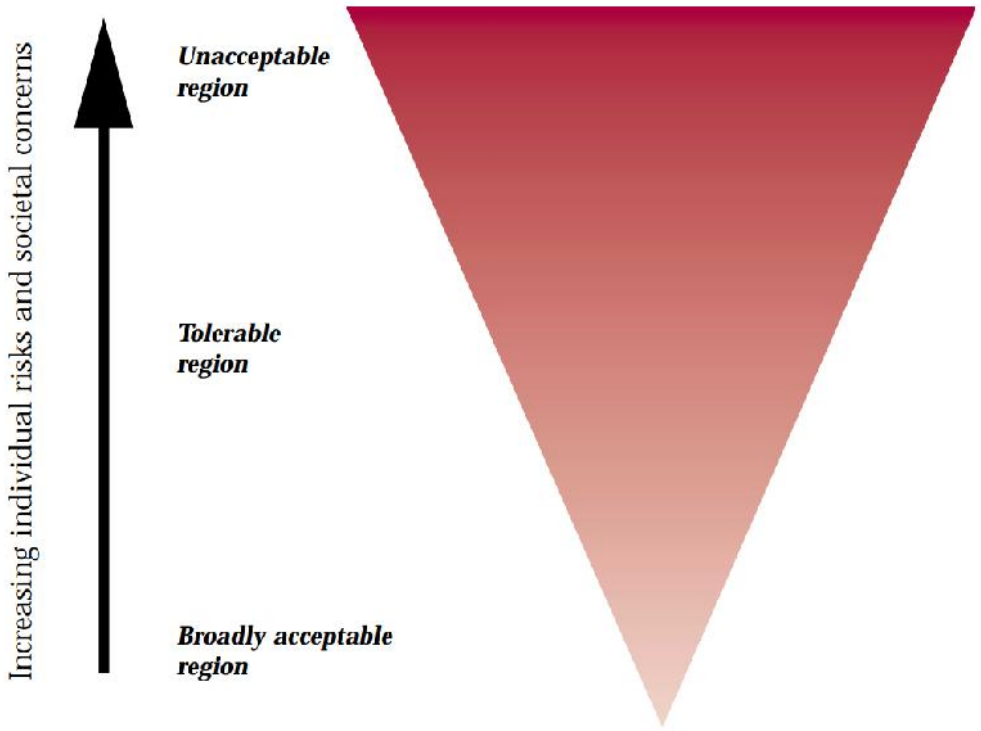
Sources:
https://hal.archives-ouvertes.fr/hal-01988939/file/1-s2.0-S0925753518306532-main.pdf

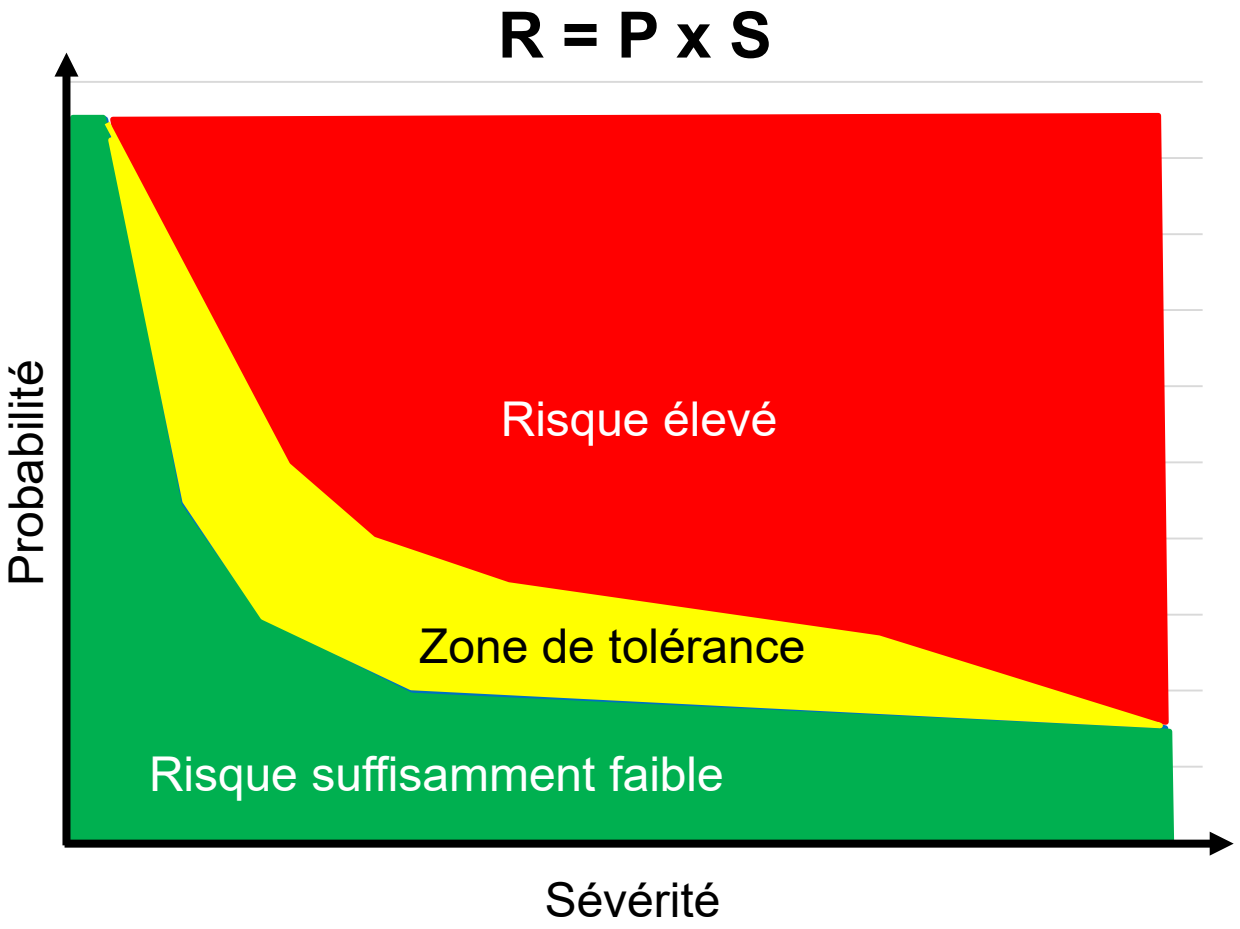
# Méthode 1: La matrice des risques

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# La matrice des risques

Cette méthode repose sur la définition du risque (combinaison de la probabilité et de la gravité des blessures) et le principe de la courbe isorisque.



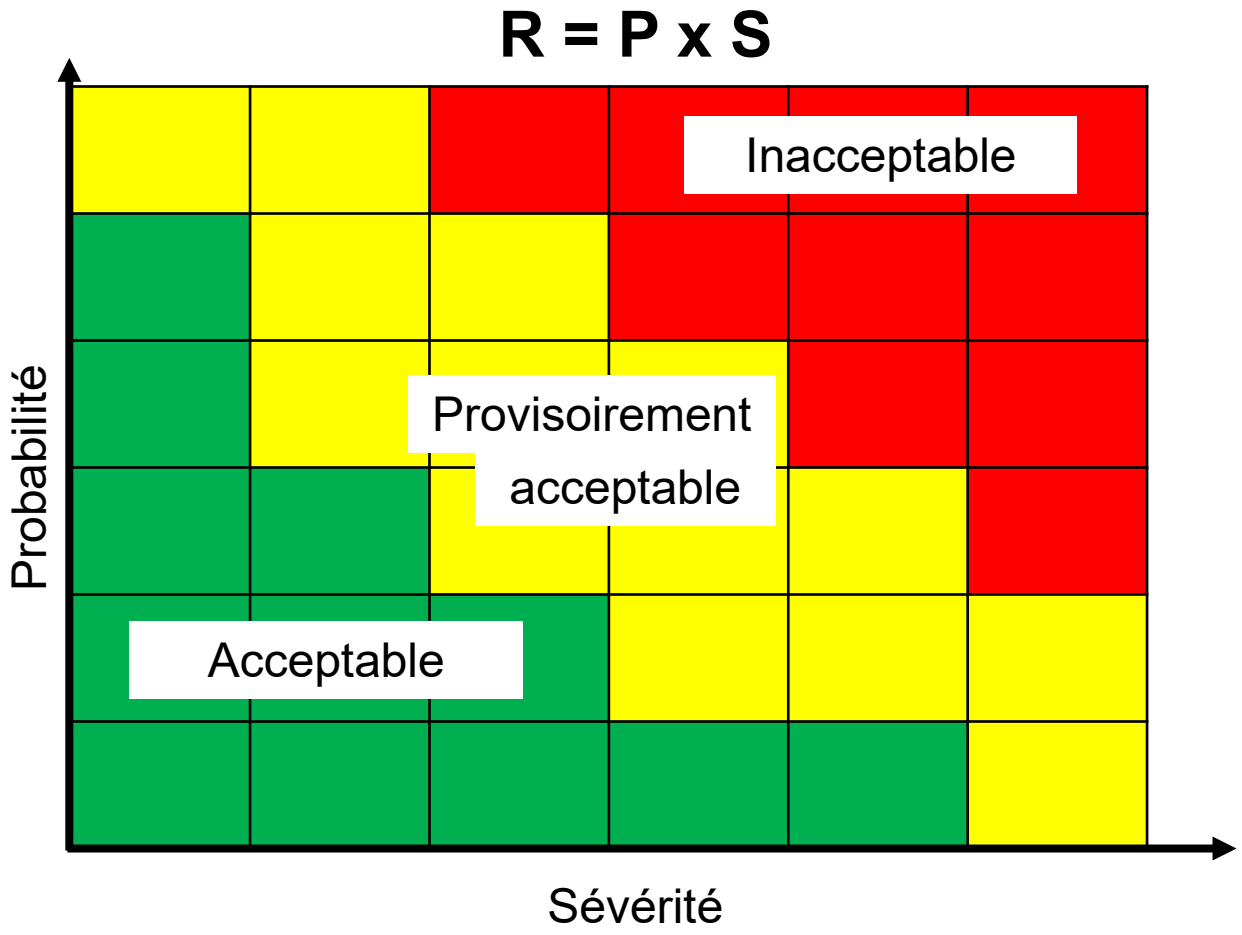






Sources:
Pilz – Formation CMSE

# La matrice des risques (2)

Ce graphique peut ensuite être représenté de manière discrète en utilisant une matrice comme celle-ci:



# La matrice des risques (3)

Ce qui donnerait une table comme suit:

**Table 1 — Risk estimation matrix (example)**

| **Probability of occurrence of harm** | **Severity of harm** | | | |
|---|---|---|---|---|
| | Catastrophic | Serious | Moderate | Minor |
| Very likely | **High** | **High** | **High** | **Medium** |
| Likely | **High** | **High** | **Medium** | **Low** |
| Unlikely | **Medium** | **Medium** | **Low** | Negligible |
| Remote | **Low** | **Low** | Negligible | Negligible |



Sources:
ISO TR 14121-2

# La matrice des risques (4)

Les critères pour l'estimation de la sévérité:

- **Catastrophique** – Décès ou infirmité permanente résultant d'une blessure ou une maladie
- **Grave** – Invalidité grave résultant d'une blessure ou maladie (capacité de reprendre une activité)
- **Modérée** – Blessure ou maladie significative nécessitant plus que les premiers soins
- **Mineure** – Pas de blessure ou blessure légère ne nécessitant que les premier soins

Les critères pour l'estimation de la probabilité:

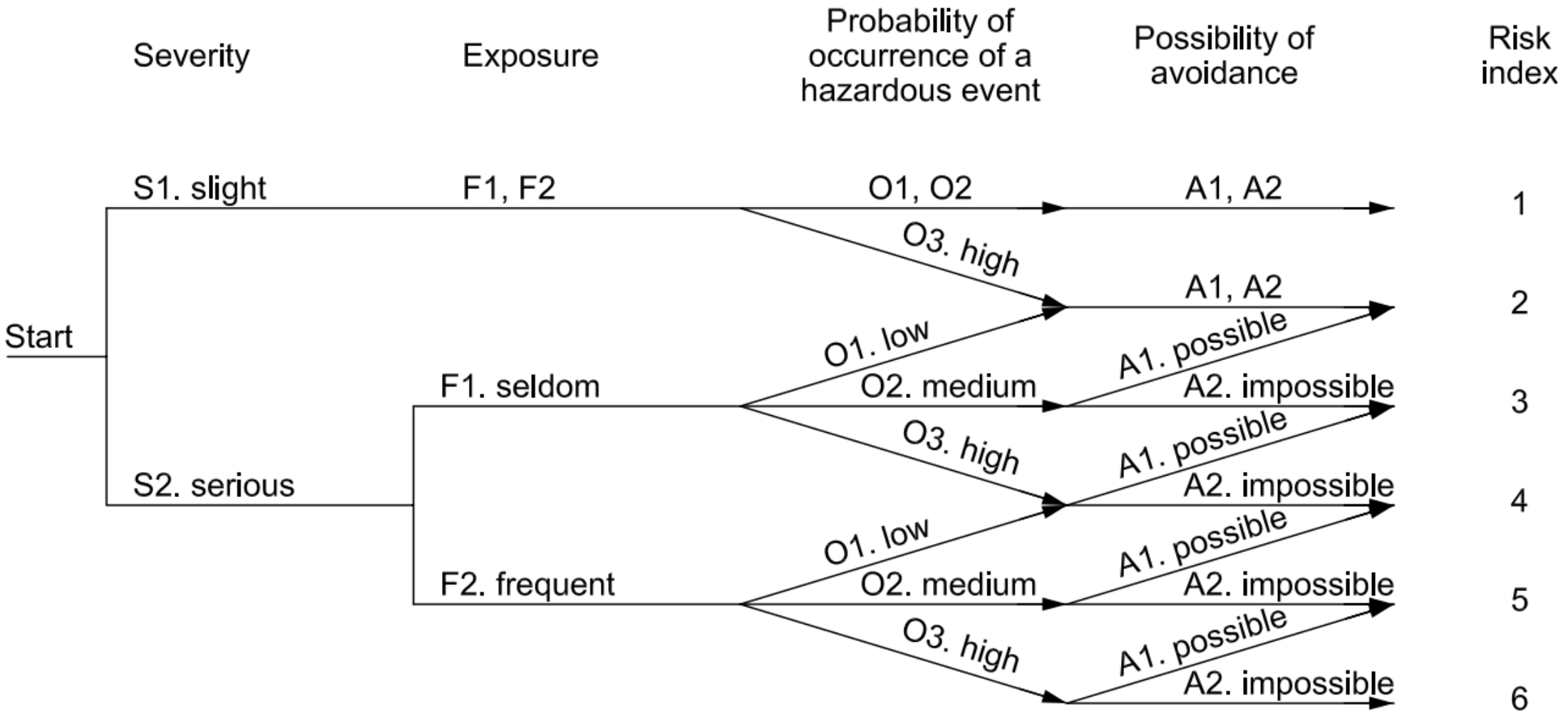
- **Très probable** – Va très certainement se produire
- **Probable** – Peut se produire
- **Peu probable** – N'est pas susceptible de se produire
- **Très peu probable** – Si peu probable que la probabilité est quasi nulle


Sources:
ISO TR 14121-2

# Méthode 2: Le graphe du risque

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Le graphe du risque



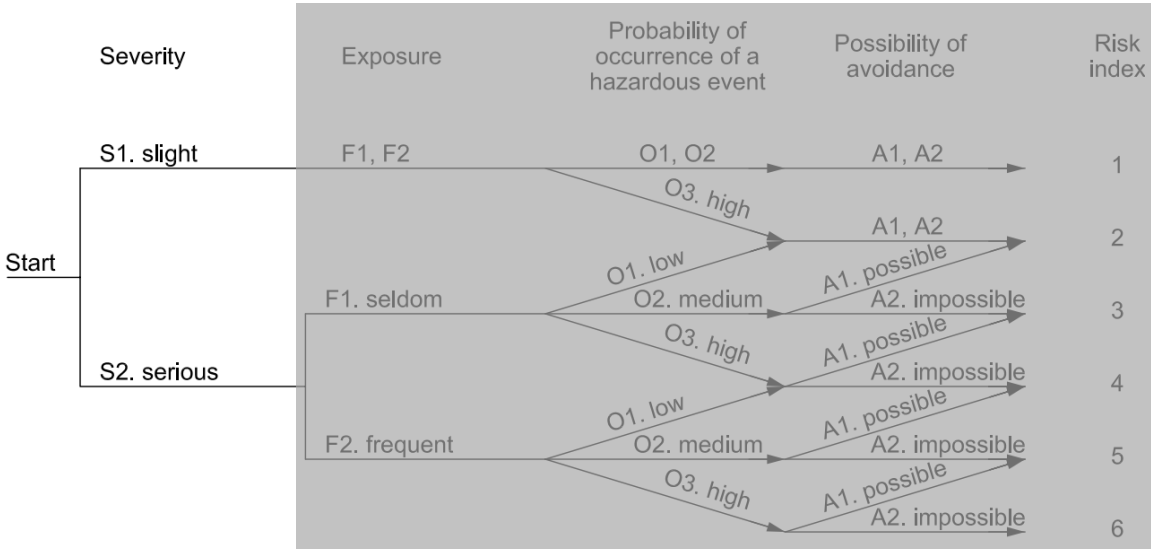



Sources:
ISO TR 14121-2

# Le graphe du risque (sévérité)

Les critères pour l'estimation de la sévérité:

- **S1 – Blessure légère** (généralement réversible). Exemples: écorchures, lacérations, contusions ou plaie ne nécessitant que des premiers soins.
- **S2 – Blessure grave** (généralement irréversible, pouvant inclure le décès). Exemples: Membres cassés, arrachés ou écrasés, fractures, blessures graves nécessitant des points de suture, trouble musculosquelettique grave (TMG), décès.



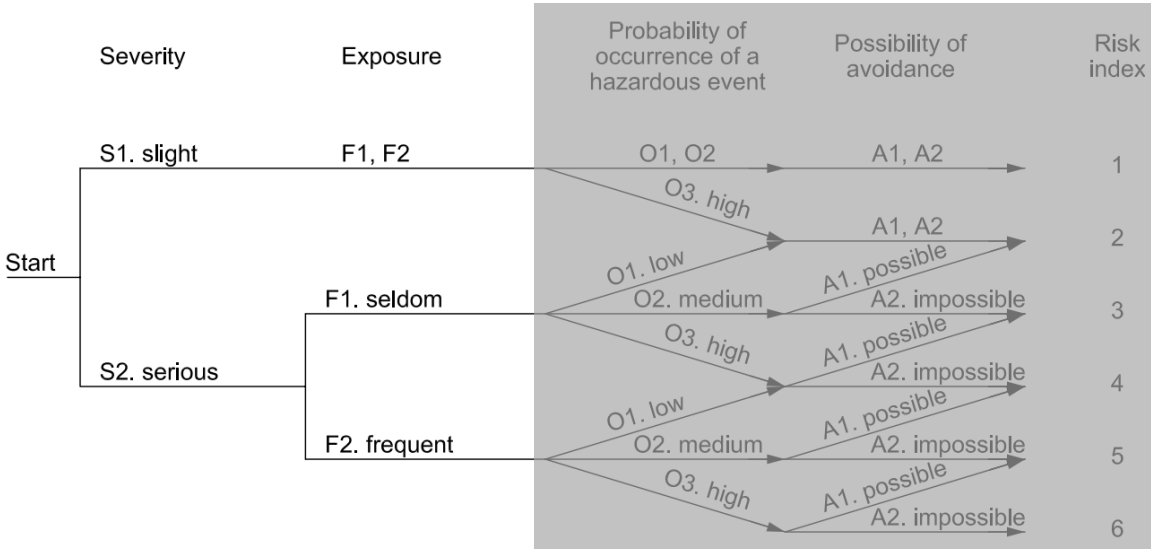



Sources:
ISO TR 14121-2

# Le graphe du risque (Exposition)

Les critères pour l'estimation de la fréquence et/ou durée d'exposition au phénomène dangereux:

- **F1 –** Jusqu'à deux fois par période de travail, et moins de 15 minutes d'exposition cumulée par période de travail
- **F2 –** Plus de deux fois par période de travail, ou plus de 15 minutes d'exposition cumulée par période de travail



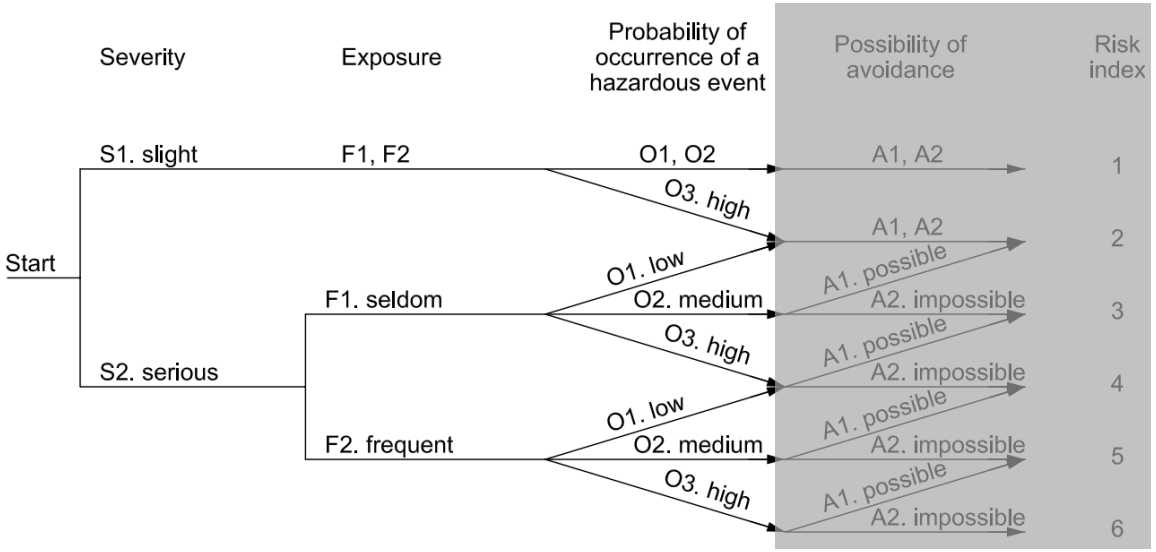



Sources:
ISO TR 14121-2

# Le graphe du risque (Occurence)

Probabilité d'occurrence de l'événement dangereux:

- **O1 –** Technologie mature et robuste (par exemple, éprouvée et reconnue dans le domaine des applications de sécurité) Action inadéquate non prévue
- **O2 –** Défaillance technique remarquée au cours de ces deux dernières années (par exemple, boulons manquant sur des protecteurs) Action inadéquate prévisible par une personne formée
- **O3** – Défaillance technique régulièrement remarquée (par exemple, protecteurs manquants) Action inadéquate prévisible par une personne non formée



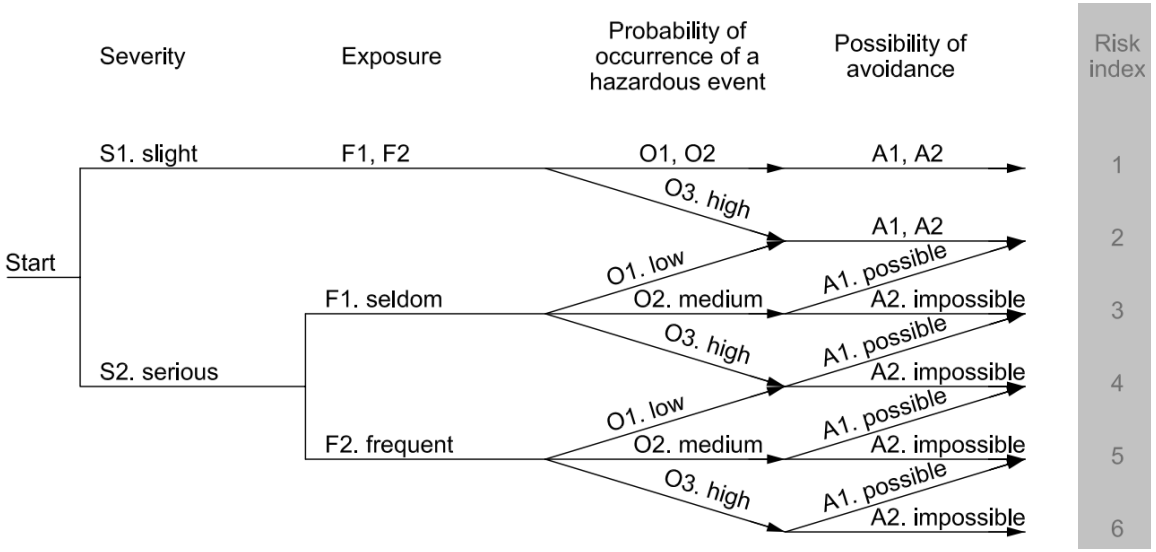



Sources:
ISO TR 14121-2

# Le graphe du risque (Evitement)

Possibilité d'évitement du danger:

- **A1 – Possible sous certaines conditions** (parties ne se déplaçant pas à une vitesse supérieure à 0.25m/s ET si le travailleur exposé à été informé et connait les risques et indications relatifs à un événement dangereux
- **A2 – Impossible**






Sources:
ISO TR 14121-2

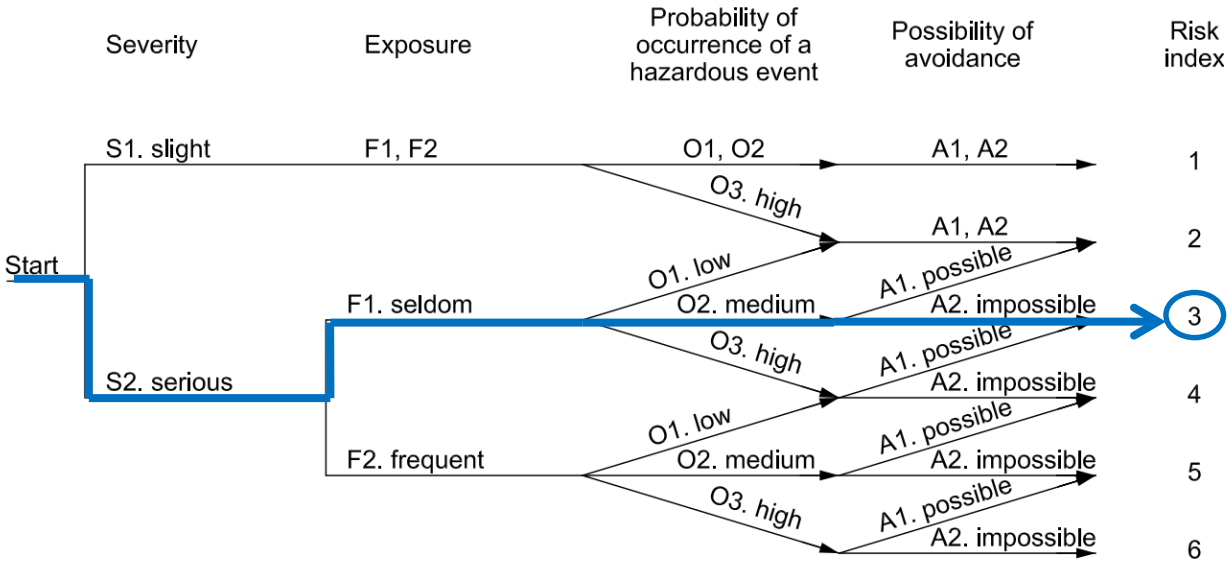
# Le graphe du risque (Exemple)

**S2** **Sévérité –** Perte d'un doigt

**F1** **Fréquence d'exposition –** Exposition lors de maintenances uniquement

**O2** **Probabilité d'occurrence –** Protection incomplète

**A2** **Probabilité d'éviter le danger –** Impossible






Sources:
ISO TR 14121-2

# Le graphe du risque (Evaluation des risques)

Une fois l'estimation des risques effectuées pour tous les dangers, ceux-ci sont classés selon leur indice de risque:

a) Un risque entre 1 et 2 est considéré comme faible (acceptable)
b) Un risque entre 3 et 4 est considéré comme moyen (potentiellement tolérable ou justifiable)
c) Un risqué entre 5 et 6 est considéré comme élevé (inacceptable)


Sources:
ISO TR 14121-2

# Méthode 3: Une combinaison de méthodes via Excel

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Template Excel pour analyse de risque

Très souvent des méthodes graphiques sont définies dans les standards mais ces méthodes sont très laborieuses à utiliser dans un projet réel.

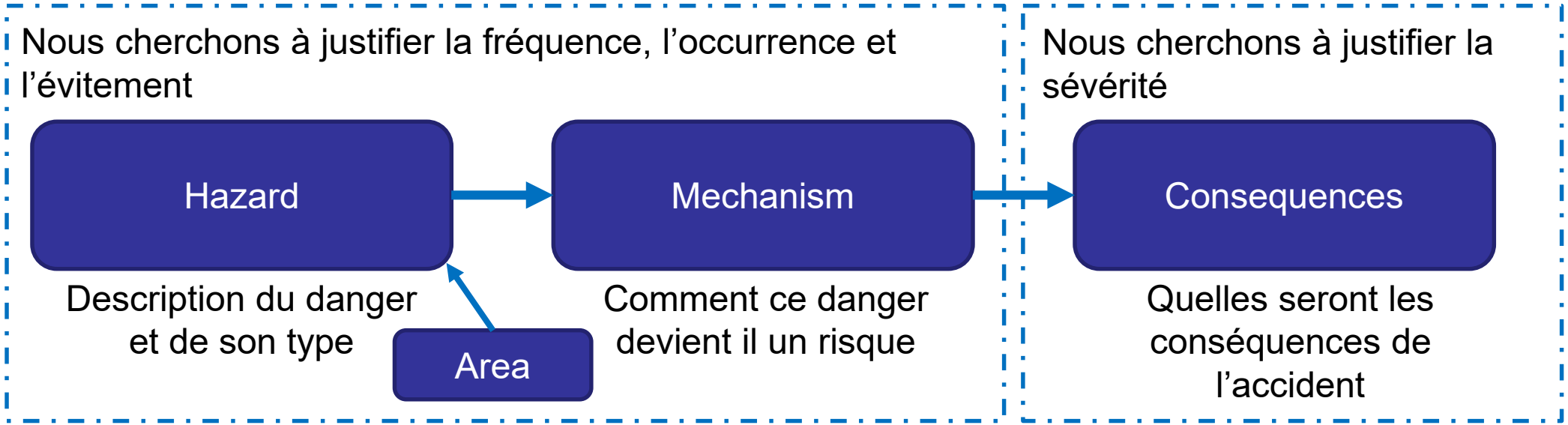
Le modèle Excel disponible sur Moodle/Teams propose une alternative pour l'analyse de risque qui nous permet de récolter les informations sur les dangers et les risques de manière méthodique et structurée.

C'est l'exemple que nous utiliserons dans ce travail.

# 4. Quelques rappels sur le cours de la dernière fois

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Du danger à sa conséquence




| Exemples de dangers: | Exemples de mécanisme: | Exemples de conséquence: |
|---|---|---|
| - Écrasement | - Écrasement par le chariot mobile | - Écrasement probable des doigts de l'opérateur |
| - Brûlure | - Brûlure lors en déplaçant la pièce | - Brûlure au 2ème degré au niveau des bras |


Sources: ISO 12100

# Exemples de phénomènes dangereux et conséquences

1. Mécaniques
2. Electriques
3. Thermiques
4. Bruit
5. Vibrations
6. Rayonnements
7. Contamination par des matériaux ou produits
8. Ergonomie
9. Environnement dans lequel la machine est utilisée
10. Combinaison de dangers

ISO 12100 – Page 58 (Table B.1 et B.2)

| Hazard | Consequences |
| --- | --- |



Sources:
ISO 12100

# Exemples de situations dangereuses:

ISO 12100 – Page 63 (Table B.3)

Mechanism

Quelques exemples de situations dangereuses comprennent

a) le travail à proximité de pièces en mouvement,
b) l'exposition à l'éjection de pièces,
c) le travail sous une charge,
d) le travail à proximité d'objets ou de matériaux à des températures extrêmes, et
e) l'exposition de l'opérateur à des phénomènes dangereux engendrés par le bruit.

# Exemples d’événements dangereux

ISO 12100 – Page 65 (Table B.4)

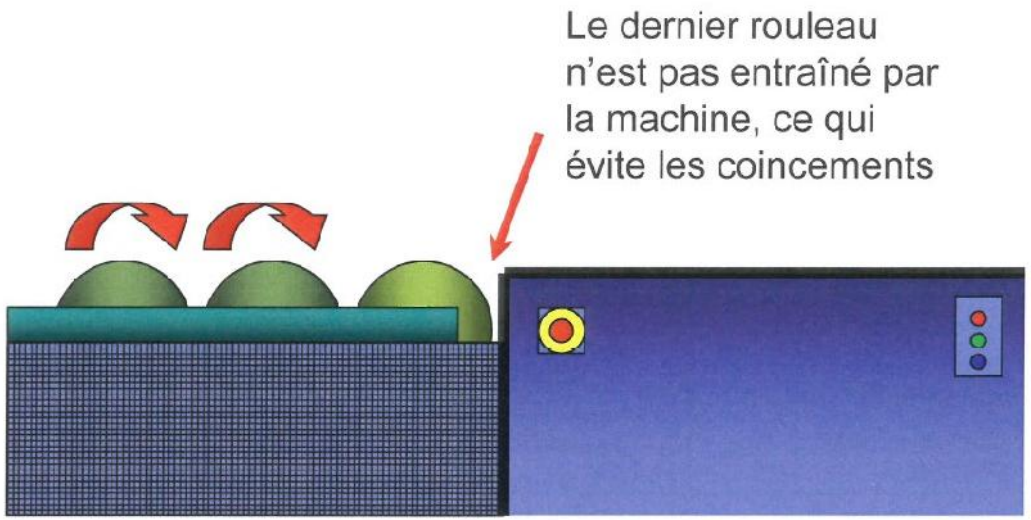
Mechanism

Un phénomène dangereux peut avoir différentes causes. Par exemple, le contact avec des pièces en mouvement du fait d'un démarrage intempestif peut être dû à l'actionnement involontaire d'un organe de service ou à une défaillance du système de commande.

Chaque cause peut à son tour être le résultat d'un autre événement ou d'une combinaison d'événements

# Hiérarchie et priorisation des réduction de risque:

1. Elimination ou substitution du risque **-> Design**
   - Modification du processus afin d'éliminer l'interaction humaine
   - Elimination des points de pincements
   - Manutention automatisée des matériaux

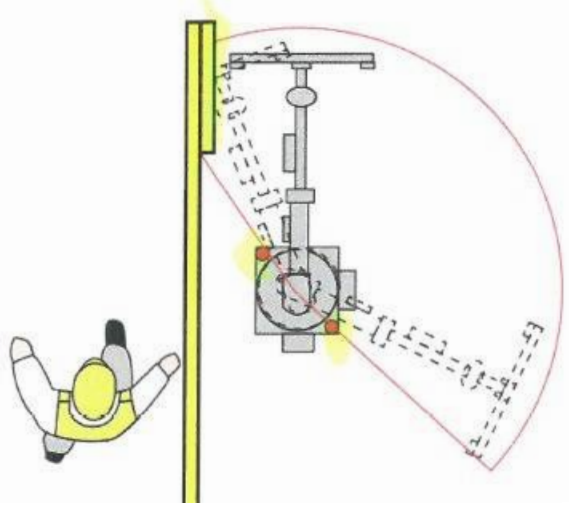




Source
Pilz – Formation CMSE

# Hiérarchie et priorisation des réduction de risque: (2)

2. Technologie de protection **-> Protecteur ou fonction de sécurité**
   - Butées mécaniques
   - Barrières
   - Dispositifs de verrouillage
   - Présence de dispositifs de détection, bandes de sécurité
   - Commandes bimanuelles



Des points d'arrêt attachés au robot et des protecteurs renforcés permettent d'empêcher au robot d'emprunter ce passage au-delà du protecteur.



Sources:
Pilz – Formation CMSE

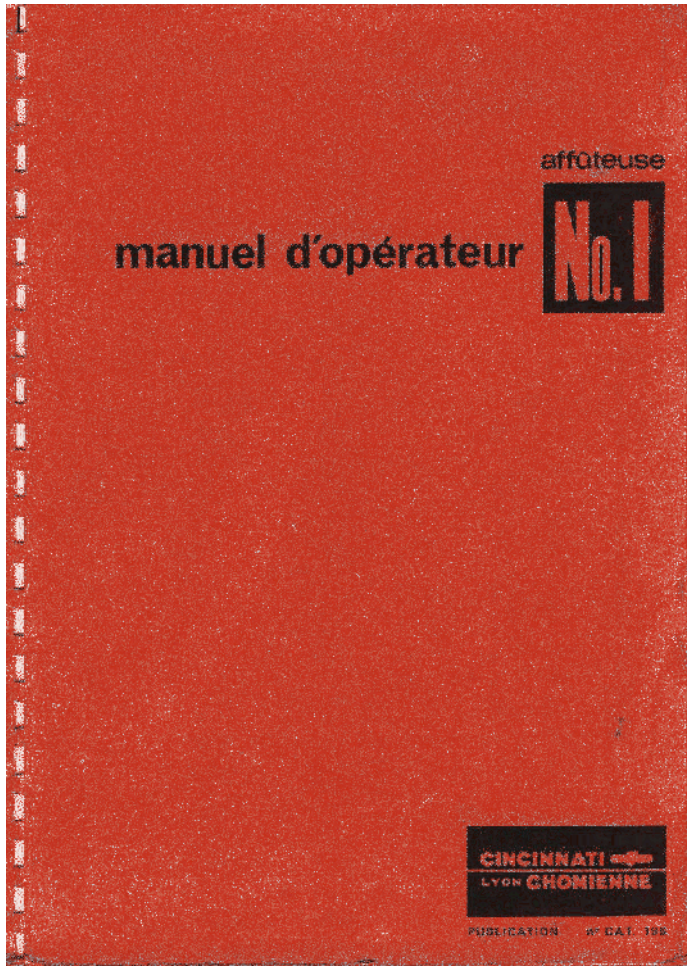
# Hiérarchie et priorisation des réduction de risque: (3)

3. Mesures d'information **-> Information**
   - Eclairage, balises et lumières stroboscopiques
   - Avertissement avec une supervision informatique
   - Signalisation
   - Marquage peint sur le sol de l'espace restreint
   - Beepers
   - Klaxons
   - Etiquettes

Sources:
Pilz – Formation CMSE

# Hiérarchie et priorisation des réduction de risque: (4)

4. Formation et procédures **-> Information**
   - Procédures de travail sûres
   - Inspection des équipements de sécurité
   - Formation
   - Verrouillage






Sources:
Pilz – Formation CMSE

# Hiérarchie et priorisation des réduction de risque: (5)

5. Equipements de protection individuelle **-> Protective Equipment**
   - Lunettes de sécurité
   - Bouchons d'oreilles
   - Masques
   - Gants
   - Casques de protection

Sources:
Pilz – Formation CMSE

# Analyse de risque par groupes de 3 ou 4 personnes

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Marche à suivre

Lors des premiers exercices vous avez:

- Choisi une machine
- Défini son fonctionnement et son environnement
- Défini les normes qui s'y appliquent

Aujourd'hui, vous devez approfondir le thème en:

- Choisir le thème d'un des membres de votre groupe
- Réfléchir à tous les dangers que cette machine engendre
- Définir les mécanismes de mise en danger des personnes et les conséquences de ces accidents
- Définir un niveau de risque en fonction du tableau d'analyse
- Proposer des mécanismes de réduction du risque en se basant sur ce qui a été implémenté sur la machine ainsi que sur les idées que vous aurez trouvé en groupes
- Evaluer le risque résiduel après mise en place de ces mécanismes

# Délivrables du «workshop»:

- Le tableau d'analyse rempli disponible sur le canal Teams/Moodle
- Un rapport d'analyse contenant:
  - Le résultat des deux premiers exercices
  - Les phénomènes dangereux définis
  - Une conclusion sur les réductions mises en places ainsi que le risque résiduel

Conseils:

- Réfléchissez ensemble aux dangers potentiels et aux situations dangereuses
- Une fois que les informations sujettes à discussions sont connues, répartissez vous les tâches (Ecriture du rapport (partie introductive) , Estimation du risque, Mécanismes de protection, Nouvelle estimation du risque, Conclusion au sujet de la table dans rapport)

# Merci pour votre attention

Questions ou remarques: eric.silva@hefr.ch ou via Teams

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et Automatisation (SecuFS)

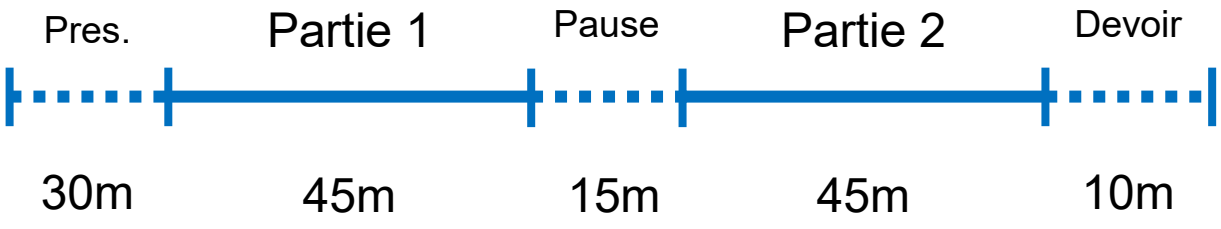
# 05 – Réduction du risque et protection mécanique

Eric Silva
25.10.2020

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | xx.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Format du cours (à partir de la semaine prochaine)




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

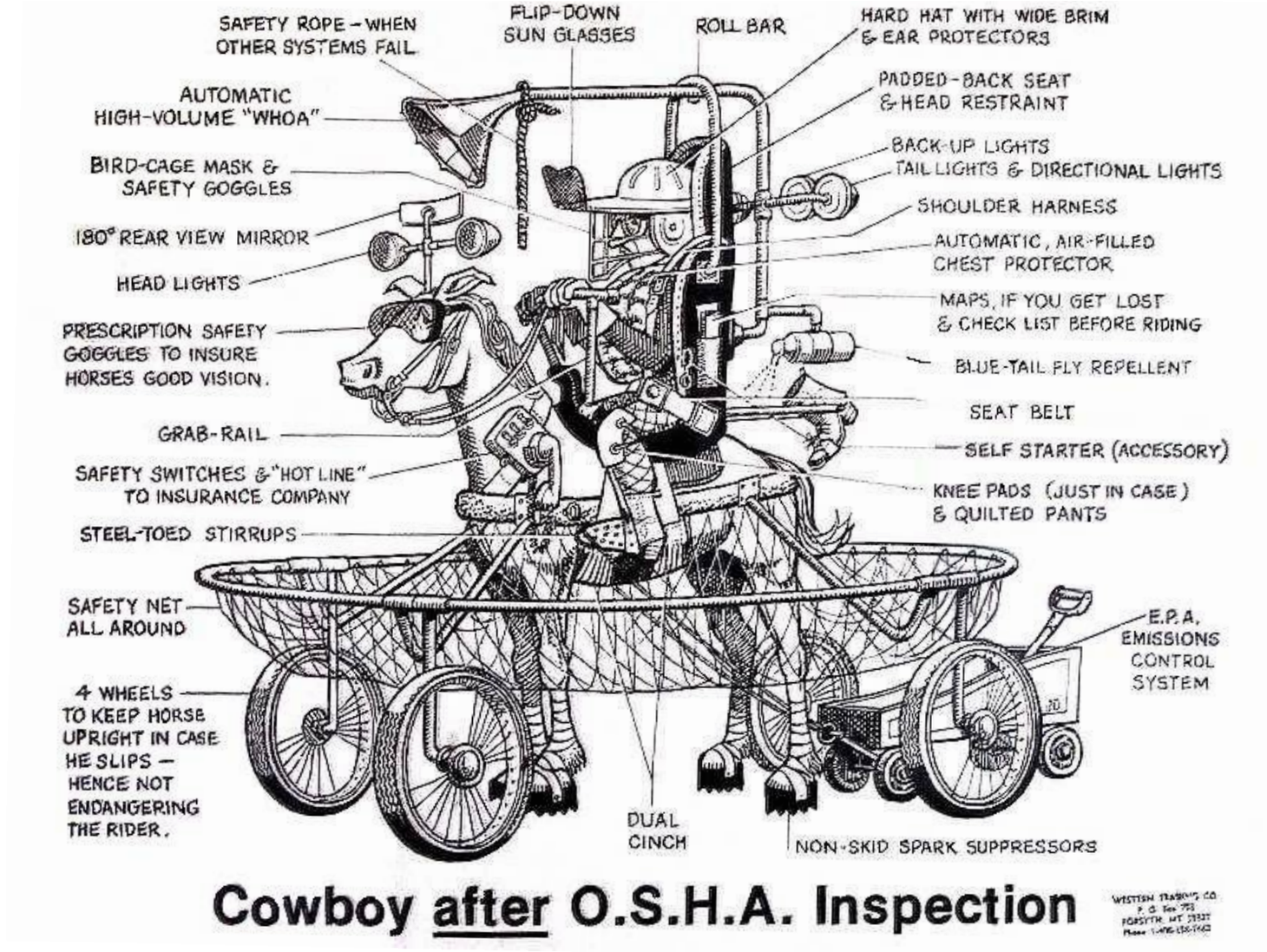
Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. Nathanaël Jaquet - Mesure acoustique de machines
4. Alexandre Murisier - ISO 13851
5. Juliette McMichael – Consignation (Lockout Tagout)
6. Mattéo Meister – ISO/PRF 22916 – Dispositifs microfluidiques
7. Harjeet Nagi - Norme de sécurité électrique et régimes de neutres
8. Shukri Ramadani - Les EPI
9. Quentin Müller – ISO 13857 les distances de sécurité
10. César Michaud – Les jouets radioactifs
11. Philippe Gaêl Dubuis – Chariots de Manutention
12. Julien Pernet – Retour sur l'ISO 12100

# Introduction à la protection mécanique

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# La réduction du risque et les protecteurs mécaniques






Sources: OSHA

# Autres protections

En plus des protections contre les dangers mécaniques, des protections contre le bruit, les vibrations excessives, les émissions et le rayonnement doivent être mises en places.

Bruit:

- Des mesures de protection supplémentaires incluent par exemple:
  - Les enceintes
  - Les écrans installés sur la machine
  - Les silencieux

Vibrations:

- Des mesures de protection supplémentaires incluent, par exemple
  - Les dispositifs d'amortissement afin d'isoler la personne exposée de la source de vibrations, tels que le support élastique et les sièges à suspension

# Autres protections (2)

Emission de substances dangereuses:

- Des mesures de protection supplémentaires incluent par exemple:
  - Le confinement de la machine (enceinte à pression négative)
  - La ventilation par aspiration localisée avec filtration
  - Le mouillage par des liquides
  - Une ventilation spéciale dans la zone de la machine (rideau d'air, cabine pour opérateur)

Rayonnement:

- Des mesures de protection supplémentaires incluent, par exemple
  - Le recours au filtrage et a l'absorption
  - L'utilisation d'écrans atténuateurs ou de protecteurs

# Normes relatives à la protection mécanique ISO 14120

Sécurité des machines – Protecteurs – Prescriptions générales pour la conception de protecteurs fixes et mobiles.

La norme définit les types de protecteurs comme suit:

- Protecteurs fixes
- Protecteurs enveloppants
- Protecteurs de maintien à distance
- Protecteurs mobiles
- Protecteurs motorisés
- Protecteurs à fermeture automatique
- Protecteurs commandant la mise en marche
- Protecteurs réglables
- Protecteurs avec dispositif de verrouillage (capteur détectant la fermeture)
- Protecteurs avec dispositif d'interverrouillage (capteur + actionneur pouvant bloquer la porte)

# Normes relatives à la protection mécanique ISO 14120 (2)

L'annexe A de la normer ci-dessus permet la détermination des protecteurs contre les dangers liés aux pièces en mouvement. Elle aide à choisir entre les protecteurs fixes, et les protecteurs mobiles verrouillés.

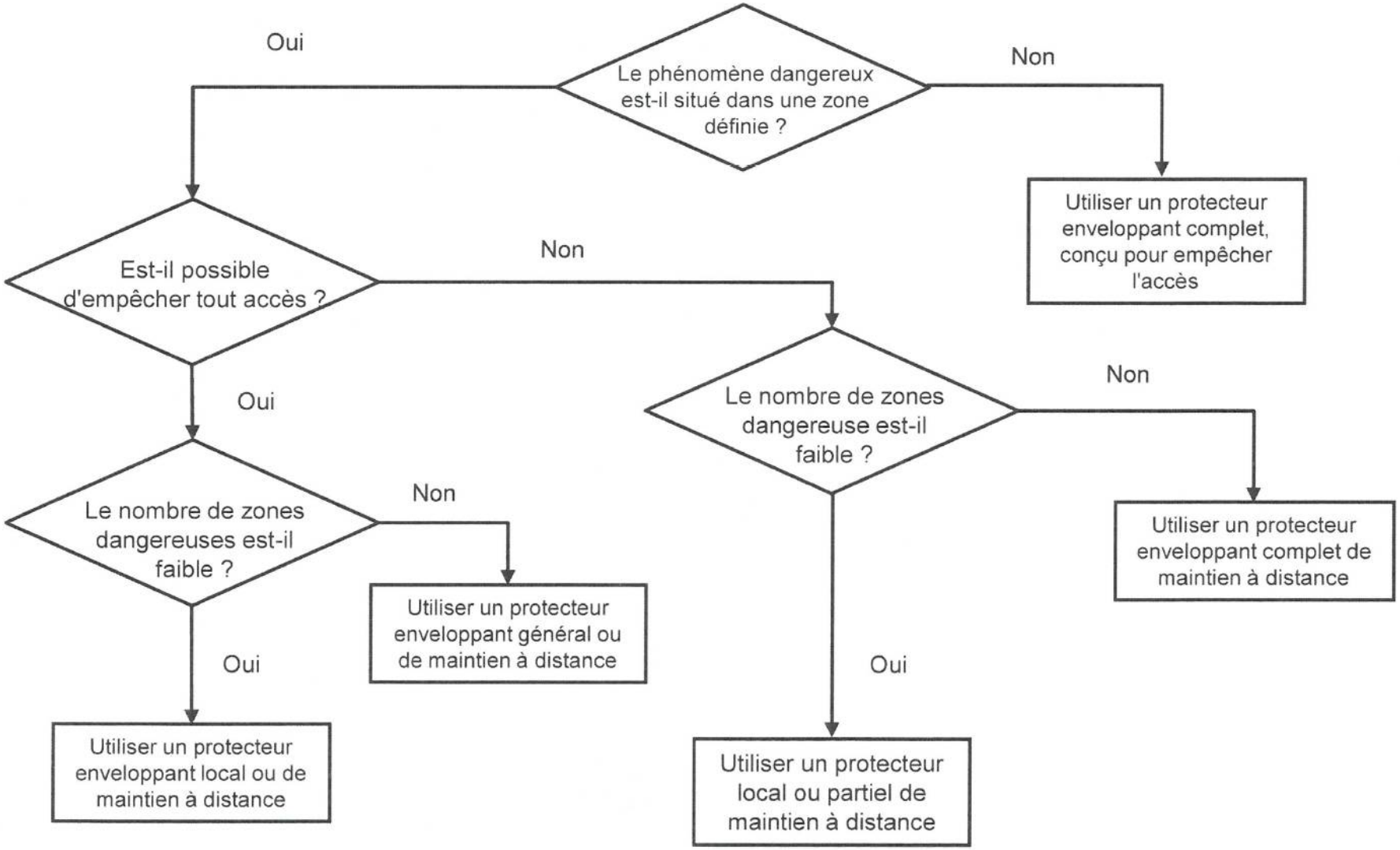
Les protecteurs fixes ne doivent pas être utilisés si l'accès à la zone dangereuse est nécessaire:

- Pendant une opération normale
- Lors d'opérations de maintenance avec une fréquence d'accès haute (> 1fois /mois)

Les protecteurs fixes ne peuvent pas être utilisés comme seule mesure de réduction du risque:

- Si il y a un risque que les protecteurs fixes ne soient pas remontés
- Si le travail a réaliser lors d'une maintenance nécessite le fonctionnement de la machine

# Recommandation sur le choix du protecteur (ISO 14120)






Sources: Pilz CMSE

# Exigences générales pour les protecteurs

En général, les protecteurs doivent avoir les caractéristiques suivantes:

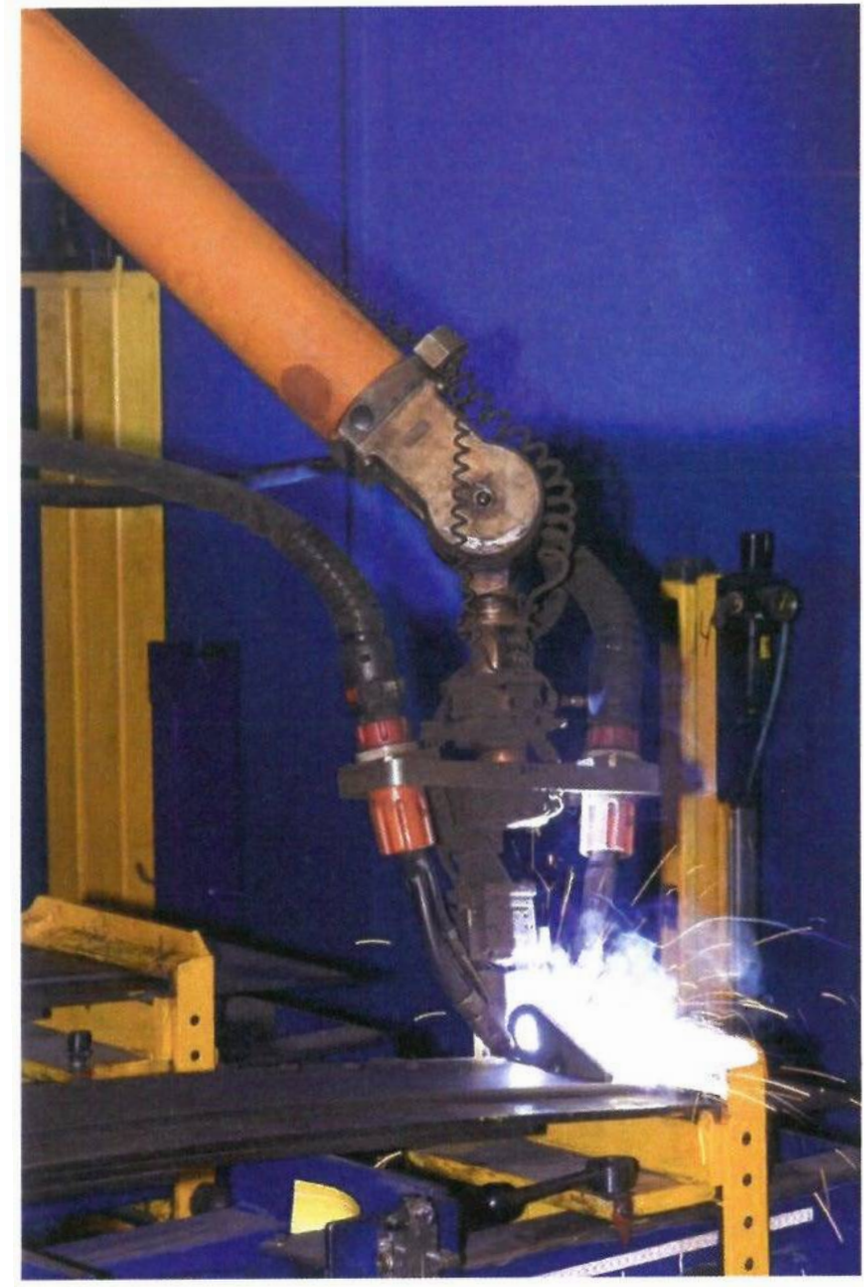
- Robuste
- Résistance suffisante aux chocs
- Fixation sûre
- Capable de protéger contre l'éjection de pièce ou de matière
- Taille et dimensionnement permettant une manutention aisée

Dans la mesure du possible les protecteurs mobiles ne doivent pas pouvoir se fermer tant qu'il y a des personnes dans la zone dangereuse. En alternative, il faudra utiliser un autre moyen de détecter la présence d'une personne.

# Matériaux à utiliser

Lors du choix du matériau à utiliser pour le protecteur de cette machine, il est important de tenir compte de différents facteurs:

- Les phénomènes dangereux engendrés par la machine
  - Les arcs électriques
  - Les étincelles
  - La projection de débris
  - L'émission de fumée
- La méthode la plus couramment utilisée est de recouvrir l'intérieur du grillage par un écran de protection, ce qui permet de voir la zone de soudure tout en empêchant la projection de débris.
- Une ventilation peut être requise pour éviter le phénomène de fumée



Sources: Pilz CMSE

# Matériaux à utiliser (2)

Le choix des couleurs est aussi important, il aide l'opérateur à reconnaître le protecteur et délimite donc la zone dangereuse, tout en lui indiquant la zone dans laquelle il est sensé interagir avec la machine.

Sources: Pilz CMSE

# Matériaux à utiliser (3)

D'autres critères que la protection peuvent influer le choix des matériaux d'un protecteur, par exemple, pour l'alimentaire, les machines d'emballage alimentaire et le pharmaceutique:

- La conception esthétique
- La facilité d'entretien

Les matériaux le plus souvent retenus pour ces applications sont:

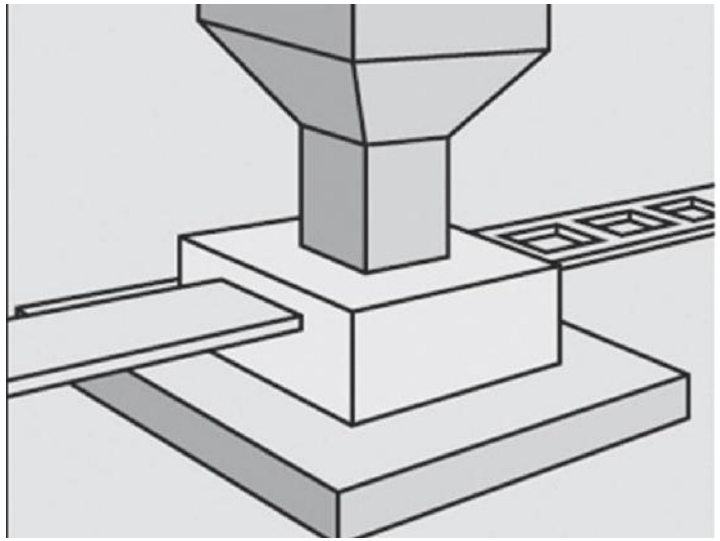
- L'acier inoxydable
- Le polycarbonate

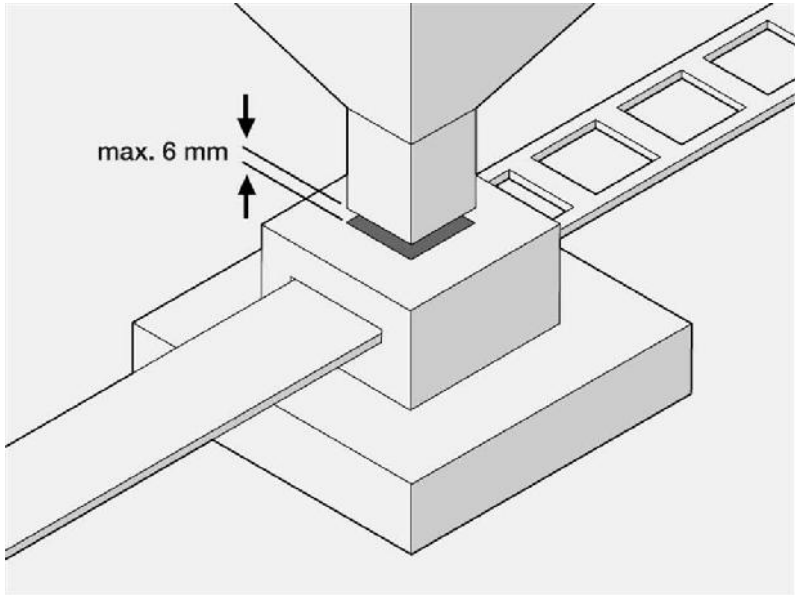
Sources: Pilz CMSE

# Outil noyé/fermé

Le poinçon de la partie supérieure de l'outil doit être enfoncé dans la matrice inférieure de manière à ce qu'in n'y ait plus aucun espacement.

S'il y a un espacement, celui-ci ne doit pas excéder 6mm. Sinon un autre protecteur doit être ajouté.








Sources: OSHA Academy

# Outil noyé/fermé (2)

| Action protective | Avantages | Limitations |
|---|---|---|
| • Accès à la partie en mouvement de la machine protégé complètement | • Evite presque tous les danger possibles avec la machine<br><br>• Permet parfois de laisser une machine sans surveillance sans risquer de blesser un autre opérateur | • N'est pas adapté à tous les types de machines ni à tous les types d'utilisations (presse, poinçonnage…)<br><br>• Demande une réflexion dans le design de la machine et non seulement après développement<br><br>• La forme du matériau doit être constamment identique |

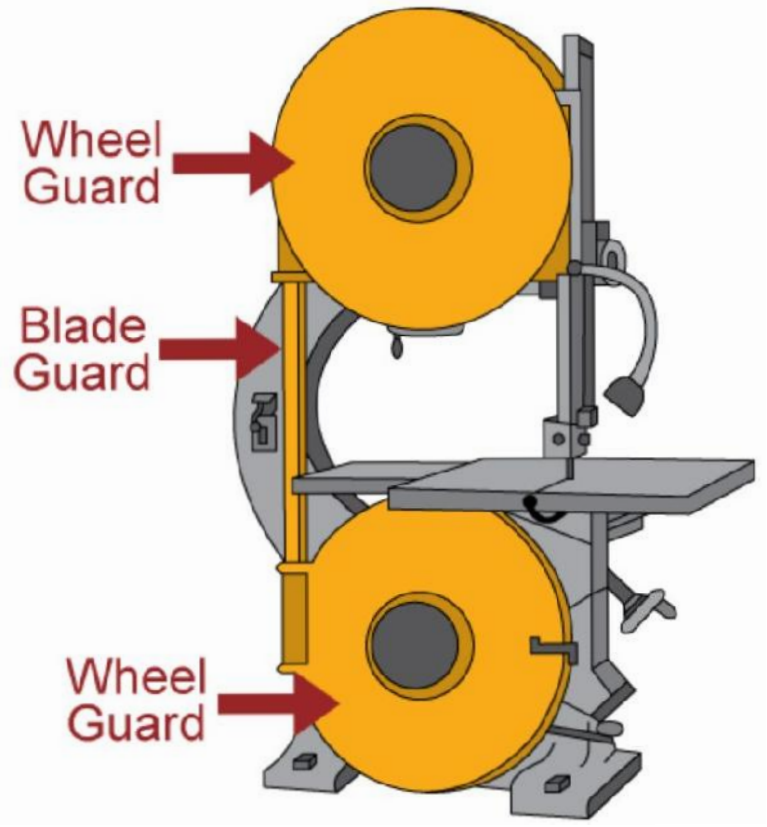


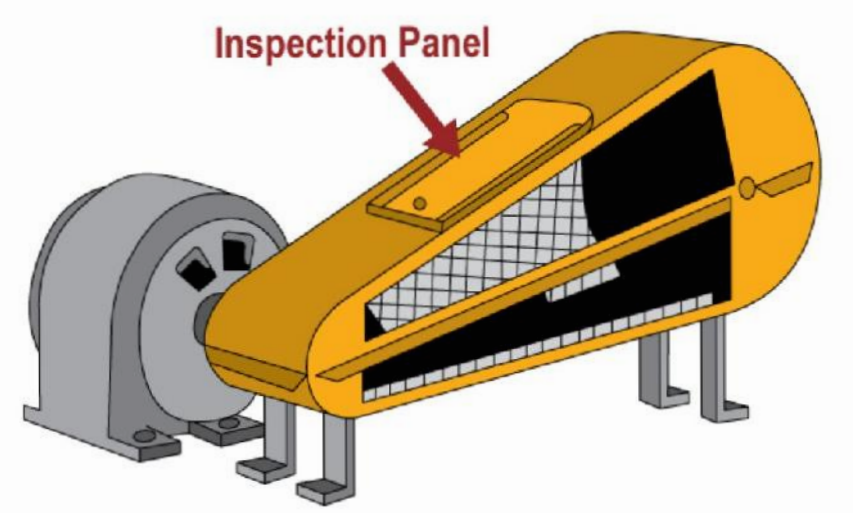
Sources: OSHA Academy

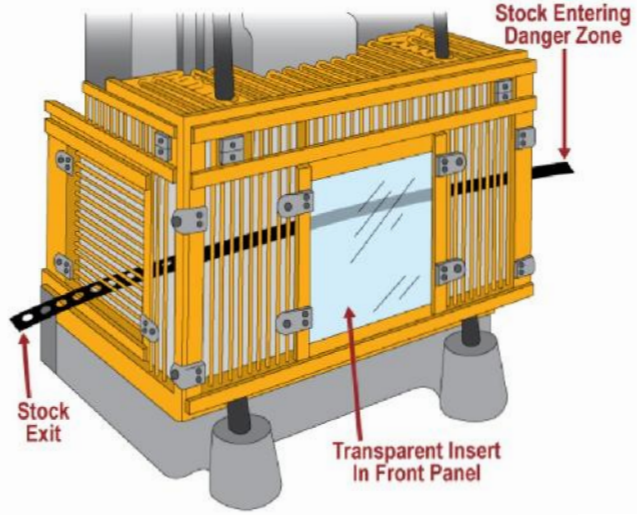
# Protecteur fixe

Comme son nom l'indique, un protecteur fixe est une partie permanente de la machin. Il ne dépend pas des parties en mouvement pour effectuer sa fonction.

Il peut être construit dans le matériaux souhaité tant que cette matière est capable de supporter les impacts qu'elle peut recevoir et garantir un usage prolongé.






Sources: OSHA Academy

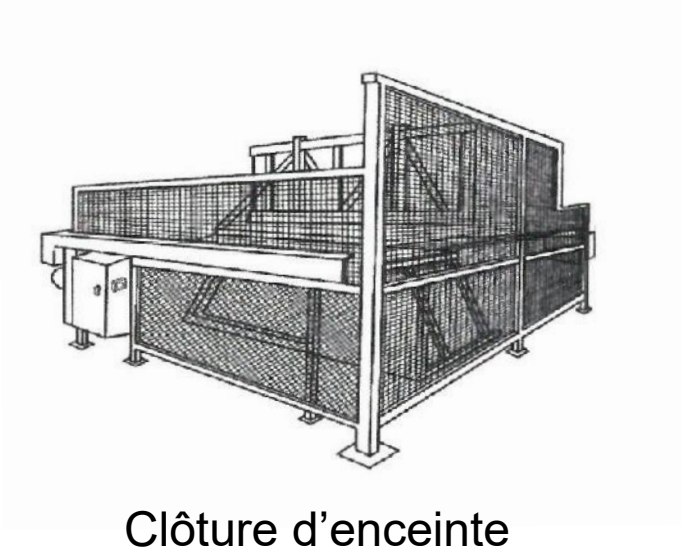
# Protecteur fixe (2)

| Action protective | Avantages | Limitations |
|---|---|---|
| • Agit comme barrière de protection | • Peut être adapté à de nombreuses applications spécifiques<br>• Sa mise en place dans une usine est souvent possible<br>• Requiert une maintenance minimale<br>• Peut être utilisé pour de la production de masse avec des opérations répétées | • Peut limiter la visibilité<br>• Peut parfois être limité à des opérations spécifiques<br>• Les ajustements et réparations de la machine requièrent souvent un démontage des protecteurs fixes et demandent donc d'autres moyens de protection pour le personnel de maintenance |

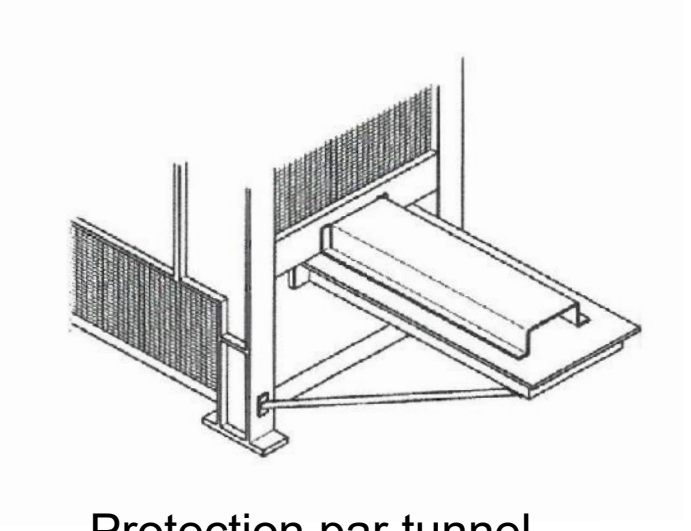


Sources: OSHA Academy

# Protecteurs fixes, exemples



Clôture d'enceinte



Protection par tunnel

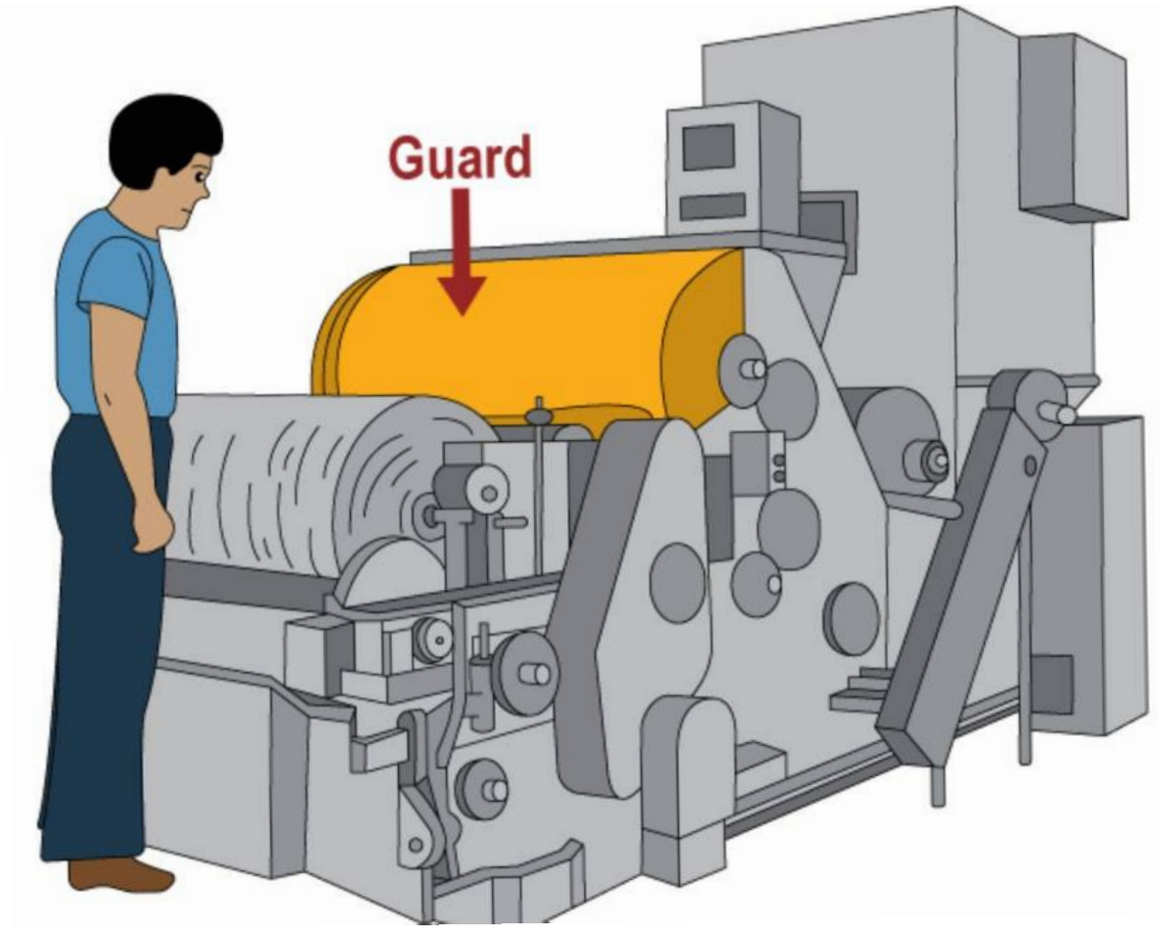
Protecteur enveloppant

Sources: OSHA Academy

# Protecteur à interverrouillage

Lorsque ce type de protecteur est ouvert ou démonté, le mécanisme de déclenchement ou l'alimentation de la machine est automatiquement coupé ou désengagé. La machine ne peut pas redémarrer de cycles tant que le protecteur n'est pas en place.

Un protecteur à interverrouillage peut être actionné de manière électrique, hydraulique, pneumatique ou une combinaison de ceux-ci.






Sources: OSHA Academy

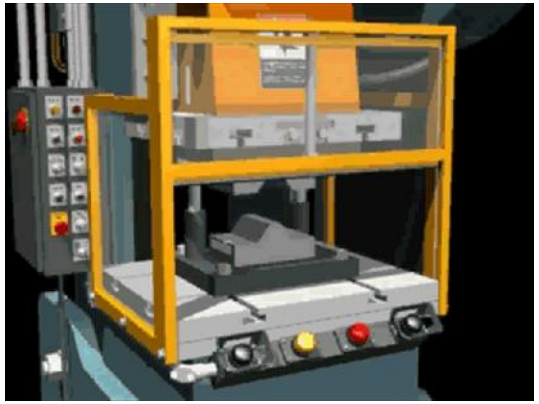
# Protecteur à interverrouillage (2)

| Action protective | Avantages | Limitations |
|---|---|---|
| • Eteint ou désengage automatiquement la machine, bloque les parties en mouvement et évite l'enclanchement de la machine tant que le protecteur est ouvert. La machine est ainsi stoppée avant que l'opérateur n'atteigne la zone dangereuse | • Peut fournir une protection maximale<br>• Permet un accès à la machine pour une les actions requises en évitant la perte de temps due au démontage des protecteurs fixes | • Requière un ajustement et une maintenance minutieuse<br>• Est parfois facile à désactiver |



Sources: OSHA Academy

# Protecteurs à interverrouillage, exemples



Ecran mobile

Portes

Système de sécurité
par interverrouillage

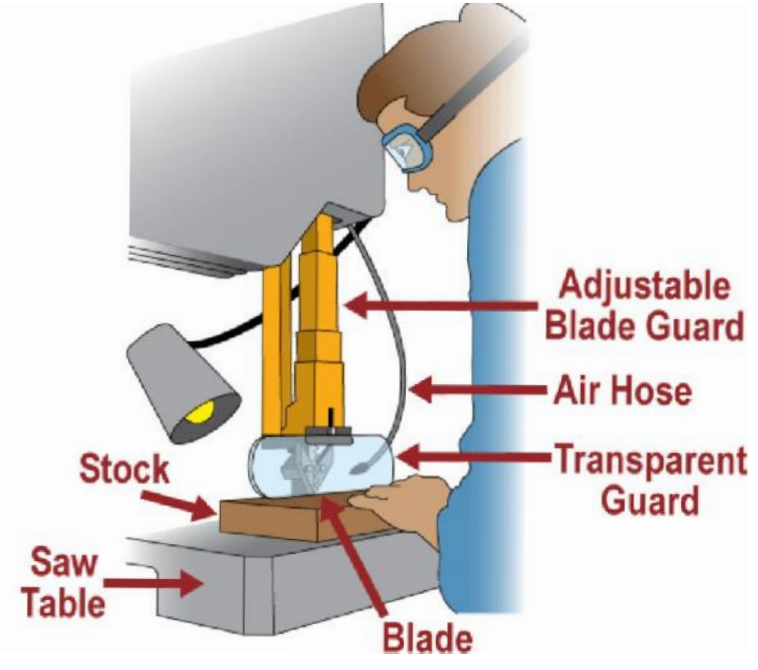


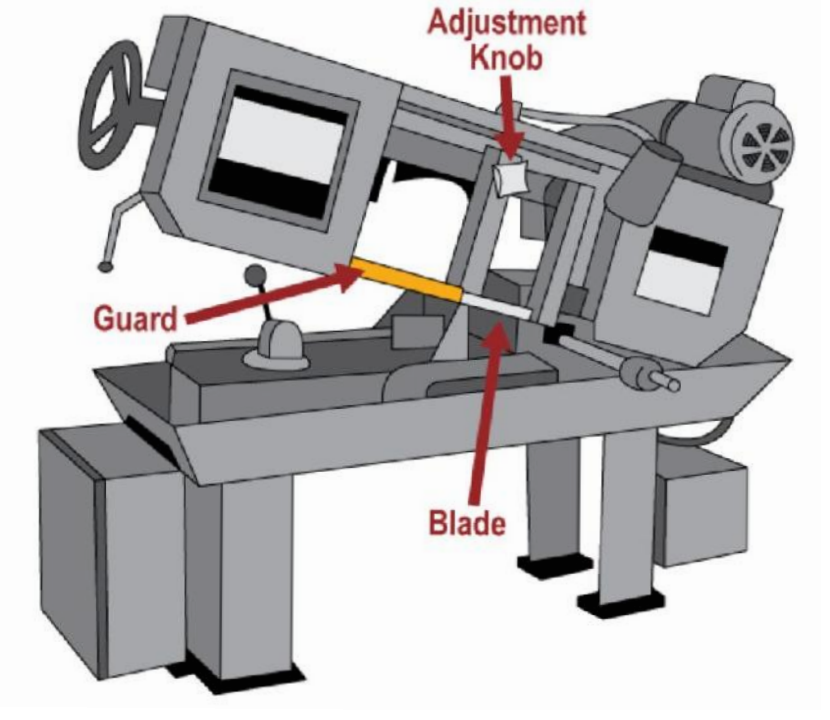
Sources: OSHA Academy

# Protecteur ajustable

Les protecteurs ajustables sont utiles car ils proposent de la flexibilité afin de s'adapter aux différentes tailles de pièces à travailler.

Ils peuvent être ajustés afin de proposer une opération adaptée selon l'opération à effectuer.






Sources: OSHA Academy

# Protecteur ajustable (2)

| Action protective | Avantages | Limitations |
|---|---|---|
| • Propose une protection ajustable selon l'opération à effectuer et la pièce à travailler | • Peut être construit pour de nombreuses applications<br><br>• Peut être ajusté pour autoriser une variation de la taille de la matière à travailler | • Les mains de l'opérateur pourraient pénétrer la zone de danger (la protection ne peut pas être total en tout temps)<br><br>• Peut demander des ajustements ou maintenances fréquents<br><br>• L'opérateur peut rendre ce protecteur ineffectif<br><br>• Peut limiter la visibilité |



Sources: OSHA Academy

# Protecteurs ajustables, exemples

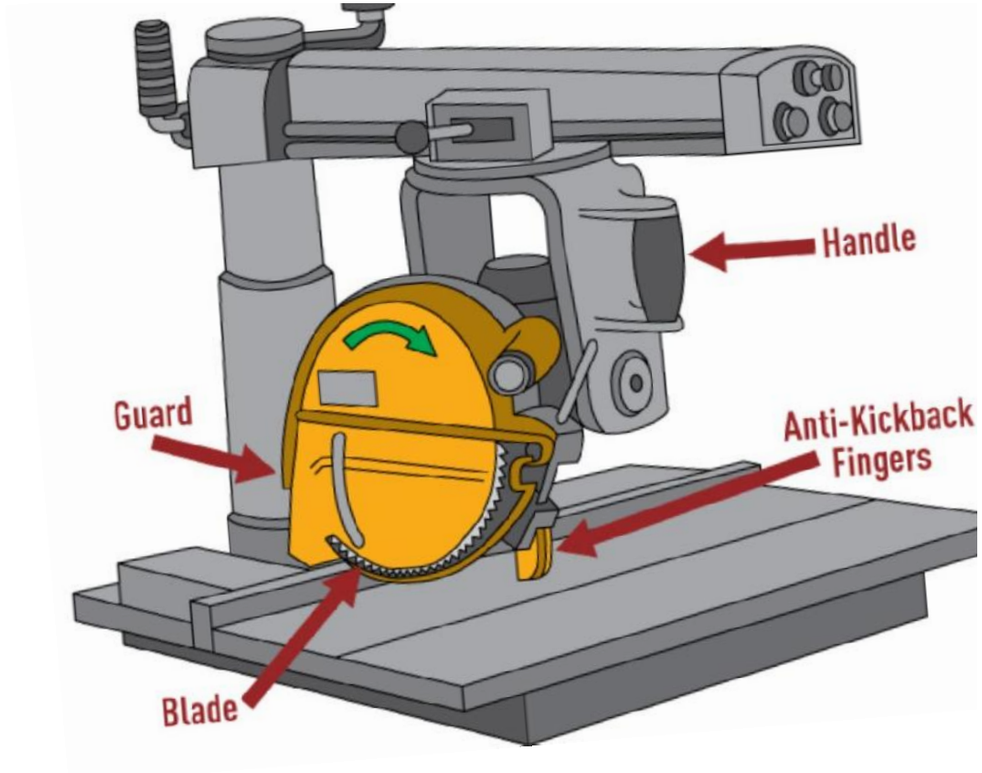
Sources: OSHA Academy

# Protecteur auto-ajustables

L'ouverture de ces protections est déterminée par le mouvement de la matière à travailler.

Lorsque l'opérateur place le matériau dans la zone de danger, le protecteur est repoussé afin d'offrir une ouverture permettant uniquement au matériaux de passer.

Une fois la matière retirée, le protecteur retourne à sa position d'origine.






Sources: OSHA Academy

# Protecteur auto-ajustable (2)

| Action protective | Avantages | Limitations |
|---|---|---|
| • Propose une protection qui s'adapte en fonction de la taille du matériau entrant dans la zone dangereuse | • Des protecteurs ajustables prêt à l'emploi sont disponible sur le marché | • Ne produit pas toujours la protection maximale<br>• Peut limiter la visibilité<br>• Peut nécessiter des maintenances et calibration spéciales |



Sources: OSHA Academy

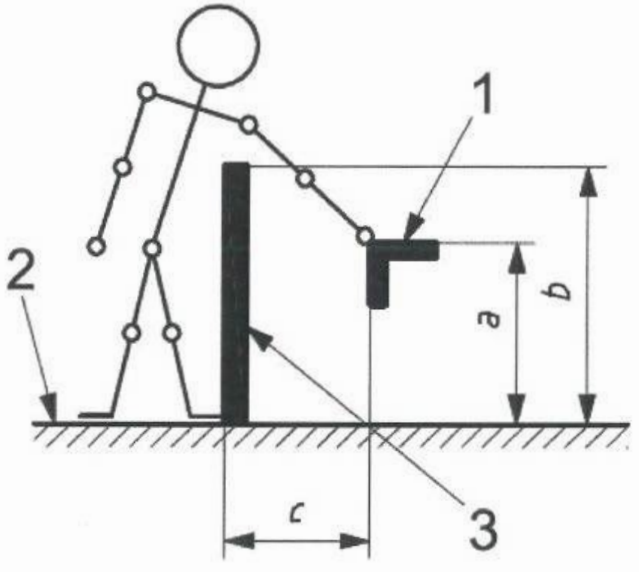
# Protecteurs auto-ajustables, exemples

Sources: OSHA Academy

# Les distances de sécurité

- La distance minimale à laquelle une structure de protection doit être placée d'une zone dangereuse est décidée grâce à la norme ISO 13857.

| | | | |
|---|---|---|---|
| Hauteur d'une zone dangereuse | a | Zone dangereuse (point le plus proche) | 1 |
| Hauteur d'une structure de protection | b | Plan de référence | 2 |
| Distance horizontale jusqu'au danger | c | Structure de protection | 3 |






Sources: OSHA Academy

# Les distances de sécurité – Tableau risque faible

| hauteur a (mm) | Hauteur de la structure de protection - b (dimensions en mm) (*) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 1 000 | 1 200 | 1 400 (**) | 1 600 | 1 800 | 2 000 | 2 200 | 2 400 | 2 500 |
| | distance horizontale par rapport à la zone dangereuse - c (mm) | | | | | | | | |
| 2 400 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | |
| 2 200 | 600 | 600 | 500 | 500 | 400 | 350 | 250 | | |
| 2 000 | 1 100 | 900 | 700 | 600 | 500 | 350 | | | |
| 1 800 | 1 100 | 1 000 | 900 | 900 | 600 | | | | |
| 1 600 | 1 300 | 1 000 | 900 | 900 | 500 | | | | |
| 1 400 | 1 300 | 1 000 | 900 | 800 | 100 | | | | |
| 1 200 | 1 400 | 1 000 | 900 | 500 | | | | | |
| 1 000 | 1 400 | 1 000 | 900 | 300 | | | | | |
| 800 | 1 300 | 900 | 600 | | | | | | |
| 600 | 1 200 | 500 | | | | | | | |
| 400 | 1 200 | 300 | | | | | | | |
| 200 | 1 100 | 200 | | | | | | | |
| 0 | 1 100 | 200 | | | | | | | |

* Les structures de protection de hauteur inférieure à 1 000 mm ne sont pas prises en compte car elles ne limitent pas suffisamment les mouvements.

** Les structures de protection de hauteur inférieure à 1 400 mm ne conviennent pas si elles sont utilisées sans mesures de sécurité supplémentaires.

# Les distances de sécurité – Tableau risque élevé

| hauteur a (mm) | Hauteur de la structure de protection - b (dimensions en mm) (*) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 1 000 | 1 200 | 1 400 (**) | 1 600 | 1 800 | 2 000 | 2 200 | 2 400 | 2 500 |
| | distance horizontale par rapport à la zone dangereuse - c (mm) | | | | | | | | |
| 2 600 | 900 | 800 | 700 | 600 | 600 | 500 | 400 | 300 | 100 |
| 2 400 | 1 100 | 1 000 | 900 | 800 | 700 | 600 | 400 | 300 | 100 |
| 2 200 | 1 300 | 1 200 | 1 000 | 900 | 800 | 600 | 400 | 300 | |
| 2 000 | 1 400 | 1 300 | 1 100 | 900 | 800 | 600 | 400 | | |
| 1 800 | 1 500 | 1 400 | 1 100 | 900 | 800 | 600 | | | |
| 1 600 | 1 500 | 1 500 | 1 100 | 900 | 800 | 500 | | | |
| 1 400 | 1 500 | 1 400 | 1 100 | 900 | 800 | | | | |
| 1 200 | 1 500 | 1 400 | 1 100 | 900 | 700 | | | | |
| 1 000 | 1 500 | 1 400 | 1 000 | 800 | | | | | |
| 800 | 1 500 | 1 300 | 900 | 600 | | | | | |
| 600 | 1 400 | 1 300 | 800 | | | | | | |
| 400 | 1 400 | 1 200 | 400 | | | | | | |
| 200 | 1 200 | 900 | | | | | | | |
| 0 | 1 100 | 500 | | | | | | | |

* Les structures de protection de hauteur inférieure à 1 000 mm ne sont pas prises en compte car elles ne limitent pas suffisamment les mouvements.

** Les structures de protection de hauteur inférieure à 1 400 mm ne conviennent pas si elles sont utilisées sans mesures de sécurité supplémentaires.



Sources: Pilz CMSE

# Les bonnes pratiques d'ingénierie

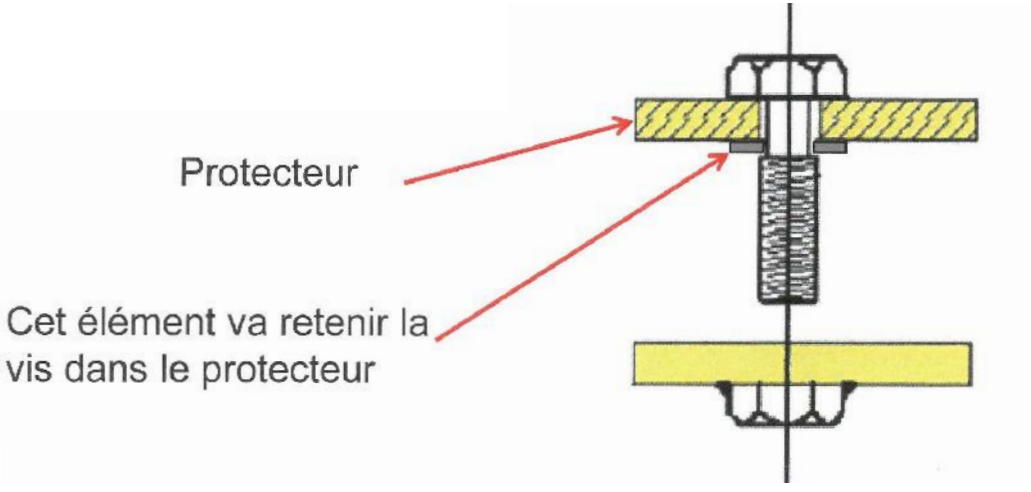
- Les protecteurs doivent solidement être maintenus en place
- Si possible, les protecteurs doivent protéger de l'éjection, de la chute de matériaux ou d'objets et des émissions générées par les machines
- Les systèmes de fixation doivent rester solidaires des protecteurs ou de la machine lors du démontage
- Dans la mesure du possible, les protecteurs ne doivent pas rester en place sans leurs fixations
- Les protecteurs mobiles avec dispositifs de verrouillage doivent être conçus de telle sorte que l'absence ou la défaillance de l'un de leurs composants empêche le démarrage ou arrête les fonctions dangereuses de la machine



Sources: OSHA Academy

# Exigences – ISO 14120

- Les systèmes de fixation doivent rester solidaires des protecteurs ou de la machine lors du démontage des protecteurs:
  - Cette mesure vise à réduire les risques suscités par la perte des fixations lors du démontage des protecteurs afin d'éviter que:
    - Les protecteurs ne soient pas remis en place
    - Qu'ils soient partiellement fixés
    - Qu'ils soient installés avec des fixations de remplacement inappropriées






Sources: OSHA Academy

# Les composants de sécurité

# A quoi servent les composants de sécurité ?

Les composants de sécurité sont des moyens permettant d'appliquer les principes de sécurité adéquats aux machines. Ils permettent souvent d'obtenir plus de flexibilité pour l'opérateur que les protecteurs mécaniques.

Les progrès techniques actuels et la qualité des composants électromécaniques permettent plus de souplesse dans l'application des principes de sécurité. La confiance placée dans les systèmes électroniques a augmenté

Les machines produites ainsi sont plus productives et plus faciles d'utilisation mais surtout plus sûres.



Sources: Pilz CMSE

# Définition d’un «Composant de sécurité»

Un composant de sécurité est un composant:

- Qui sert à assurer une fonction de sécurité
- Qui est mis sur le marché de manière indépendante aux machines
- Dont la défaillance ou le mauvais fonctionnement met en danger la sécurité des personnes
- Qui n’est pas indispensable au fonctionnement de la machine ou qui peut être remplacé par des composants normaux permettant à la machine de fonctionner

# Liste des composants de sécurité

1. Protecteurs des dispositifs amovibles de transmission mécanique
2. Dispositifs de protection destinés à détecter des personnes
3. Protecteurs mobiles motorisés avec dispositif de verrouillage destinés à être utilisés dans les machines mentionnées sections 9, 10 et 11 de l'annexe V
4. Blocs logiques assurant des fonctions de sécurité sur les machines
5. Vannes avec moyens supplémentaires de détection des défaillances, destinées au contrôle des mouvements dangereux sur les machines
6. Systèmes d'extraction des émissions des machines
7. Protecteurs et dispositifs de protection destinés à protéger les personnes exposées contre les éléments mobiles concourant directement au travail sur la machine
8. Dispositifs de contrôle des sollicitations et des mouvements des machines de levage
9. Dispositifs de retenue des personnes sur leur siège
10. Dispositifs d'arrêt d'urgence
11. Systèmes visant à empêcher l'accumulation de charges électrostatiques potentiellement dangereuses



Sources: Pilz CMSE

# Liste des composants de sécurité (2)

12. Limiteurs d'énergie et dispositifs de secours visés sections 1.5.7, 3.4.7 et 4.1.2.6 de l'annexe I
13. Systèmes et dispositifs destinés à réduire les émissions sonores et les vibrations
14. Structures de protection contre le retournement (ROPS)
15. Structures de protection contre les chutes d'objets (FOPS)
16. Dispositifs de commande à deux mains
17. Composants pour machines de levage et/ou de déplacement de personnes entre différents paliers et compris dans la liste suivante:
    a) dispositifs de verrouillage des portes palières;
    b) dispositifs visant à empêcher la chute ou le mouvement incontrôlé vers le haut de l'habitacle;
    c) dispositifs limiteurs de survitesse;
    d) amortisseurs à accumulation d'énergie: — non linéaire, ou — à amortissement du mouvement de retour;
    e) amortisseurs à dissipation d'énergie;



Sources: Pilz CMSE

# Liste des composants de sécurité (3)

f) dispositifs de sécurité montés sur les vérins des circuits hydrauliques lorsqu'ils sont utilisés comme dispositifs antichute;

g) dispositifs de sécurité électrique composés d'interrupteurs de sécurité comprenant des composants électroniques.

# Procédure de certification

Pour rappel, la certification des produits selon la directive machines est le plus souvent une auto-certification, sauf pour les produits apparaissant dans l'annexe IV de la directive.

Certains composants de sécurité s'y retrouvent:

- 15. Protecteurs des dispositifs amovibles e transmission mécanique
- 19. Dispositifs de protection destinés à détecter la présence de personnes
- 20. Protecteurs mobiles motorisés avec dispositif de verrouillage destinés à être utilisés dans des machines mentionnées dans les points 9,10 et 11 (Presse, Machine de moulage)
- 21. Blocs logiques assurant des fonctions de sécurité
- 22. Structures de protection contre le retournement (ROPS)
- 23. Structures de protection contre les chutes d'objets (FOPS)

La certification de ces composants-ci doit se faire avec le soutien d'un organisme notifié.

Exemple: SUVA

# Composants de sécurité - Protection

Les protecteurs sont mis en place afin de protéger les personnes des phénomènes dangereux qui n'ont pas pu être éliminés par la conception.

Il existe deux types de moyens de protection: les protecteurs (vus la semaine passée) et les dispositifs de protection.

- Un **protecteur** est défini dans la norme ISO 12100 comme:
  - Barrière matérielle conçue comme un élément de la machine afin d'assurer une protection
- Un **dispositif de protection** est défini dans la norme ISO 12100 comme:
  - Moyen de protection autre qu'un protecteur

# Dispositifs de verrouillage

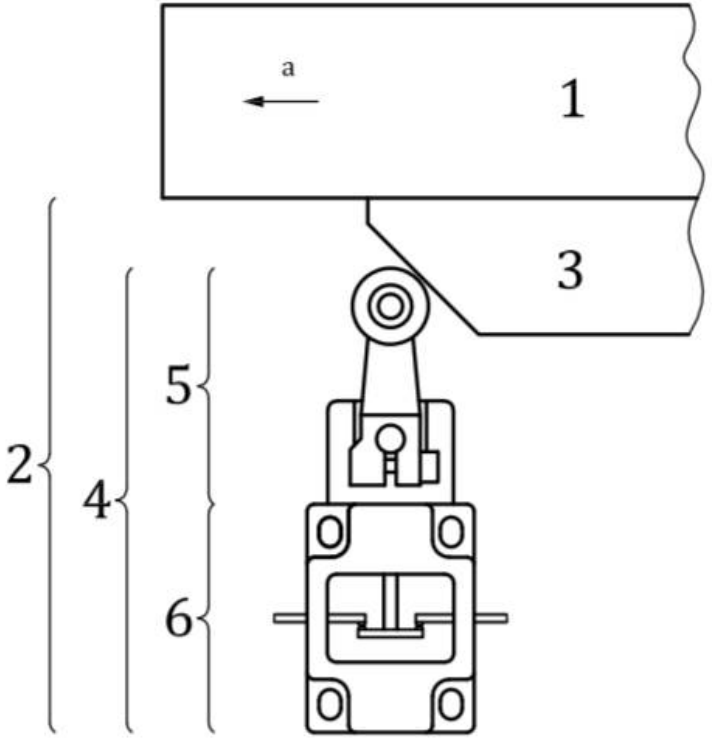
Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Dispositifs de verrouillage - Définition

«Dispositif mécanique, électrique ou autre, destiné à empêcher le fonctionnement d'éléments de la machine dans certaines conditions (en général, tant que le protecteur n'est pas fermé)»

Protecteur avec dispositif de verrouillage:

- Les fonctions dangereuses de la machines « couvertes » par le protecteur ne peuvent pas s'accomplir si pas fermé
- Si protecteur ouvert durant le fonctionnement, un ordre d'arrêt est donné.
- La machine ne doit pas redémarrer d'elle-même lorsque le protecteur est refermé




**Key**

1 protecteur
2 dispositif de verrouillage
3 actionneur
a Sens d'ouverture.
4 interrupteur de position
5 système d'actionnement
6 système de sortie



Sources: ISO 14119

# Dispositifs de verrouillage – Types de dispositifs

| Exemples de principes d'actionnement | | Exemples d'actionneurs | | Type | Exemples: voir Annexe[a] |
|---|---|---|---|---|---|
| mécanique | contact physique, force | non codé | came en rotation | Type 1 | A.1 |
| | | | came linéaire | | A.2, A.4 |
| | | | charnière | | A.3 |
| | | codé | languette (actionneur façonné) | Type 2 | B.1 |
| | | | à transfert de clé | | B.2 |
| sans contact | inductif | non codé | métal ferreux approprié | Type 3 | C |
| | magnétique | | aimant, électroaimant | | |
| | capacitif | | tout objet approprié | | |
| | à ultrasons | | tout objet approprié | | |
| | optique | | tout objet approprié | | |
| | magnétique | codé | aimant codé | Type 4 | D.1 |
| | RFID | | étiquette RFID codée | | D.2 |
| | optique | | étiquette à codage optique | | — |

[a] Des exemples d'autres dispositifs de verrouillagesont donnés dans l'Annexe E.



Sources: ISO 14119

# Dispositifs de verrouillage – Spécifications de conception

Installation mécanique:

- Les éléments de fixation des interrupteurs de position doivent être fiables et leur desserrage doit nécessiter l'utilisation d'un outil.
- Positionner et, si nécessaire, protéger le dispositif de verrouillage de manière à ne pas l'endommager sous l'effet de causes extérieures prévisibles (tout en gardant un accès pour la maintenance
- L'interrupteur ne doit pas être utilisé comme butée mécanique
- Les dispositifs de verrouillage de type 1 doivent être conçus pour garder de façon permanente leur position après réglage (par exemple au moyen de goupilles)

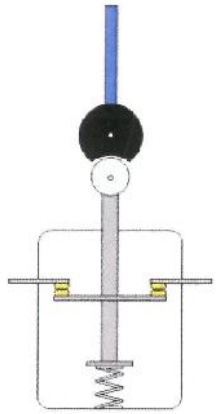
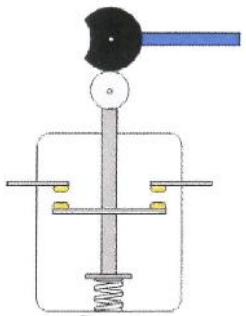
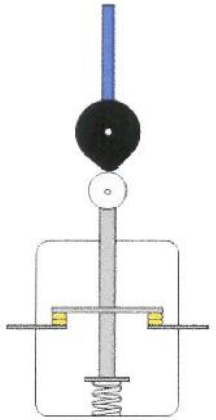
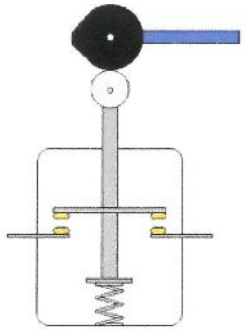
Gestion des défauts et intégration de la commande:

- Les défauts courants doivent être pris en compte (p.ex rupture de l'actionneur, contacts soudés…)
- Le système de sortie des dispositifs de verrouillage doit pouvoir être intégré dans un système de commande conçu conformément aux normes
- Un test manuel à intervalles réguliers peut être nécessaire pour éviter les défauts



Sources: ISO 14119

# Dispositifs de verrouillage – Type 1

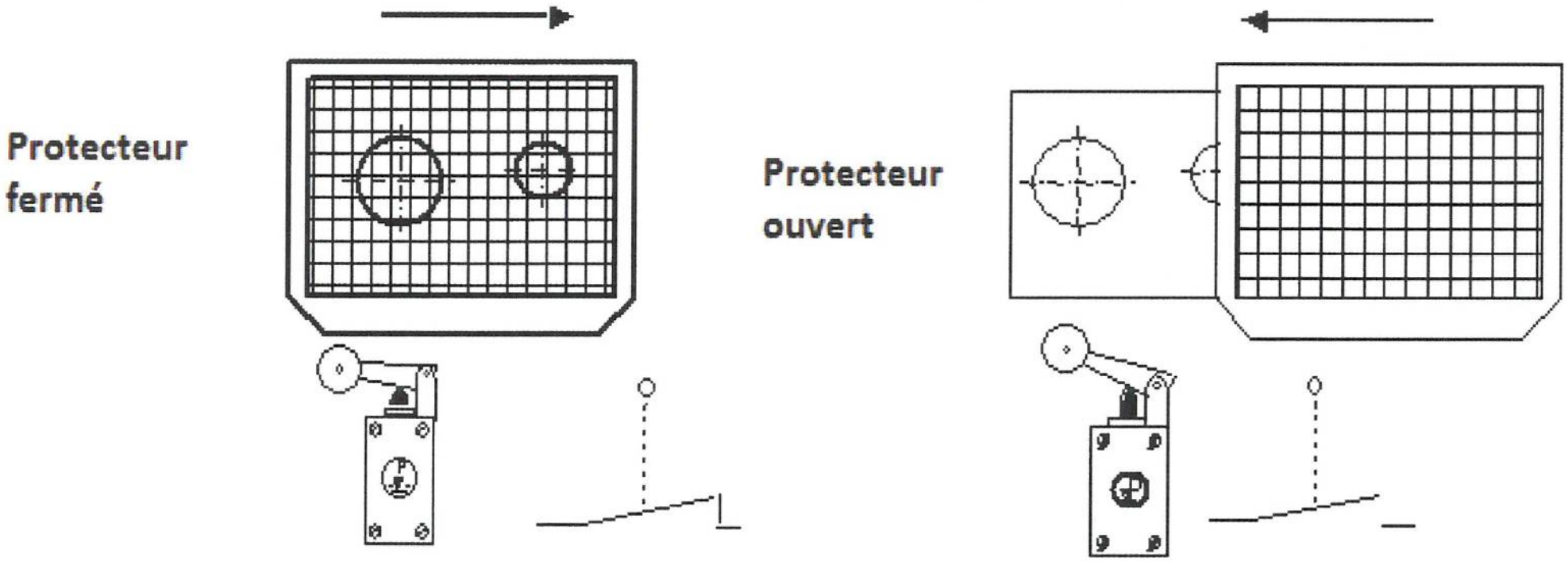
| Action mécanique | Protecteur fermé | Protecteur non fermé | Mode de fonctionnement | Exemple de comportement en cas de défaillance (voir 8.3.2) |
|---|---|---|---|---|
| directe |  |  | Le poussoir est maintenu enfoncé par une came tant que le protecteur n'est pas fermé.<br>Lorsque le protecteur est fermé, le système de sortie change d'état sous l'effet d'un ressort de rappel. | Le système de sortie reste à l'état de sécurité lorsque le protecteur n'est pas fermé, même en cas de rupture du ressort. |
| non directe |  |  | Le poussoir est maintenu enfoncé par une came tant que le protecteur est fermé.<br>Lorsque le protecteur n'est pas fermé, le système de sortie change d'état sous l'effet d'un ressort de rappel. | En cas de rupture du ressort, le système de sortie peut passer à un état de non sécurité, même si le protecteur n'est pas fermé. |



Sources: ISO 14119

# Dispositifs de verrouillage – Type 1

Est-ce une action directe ?

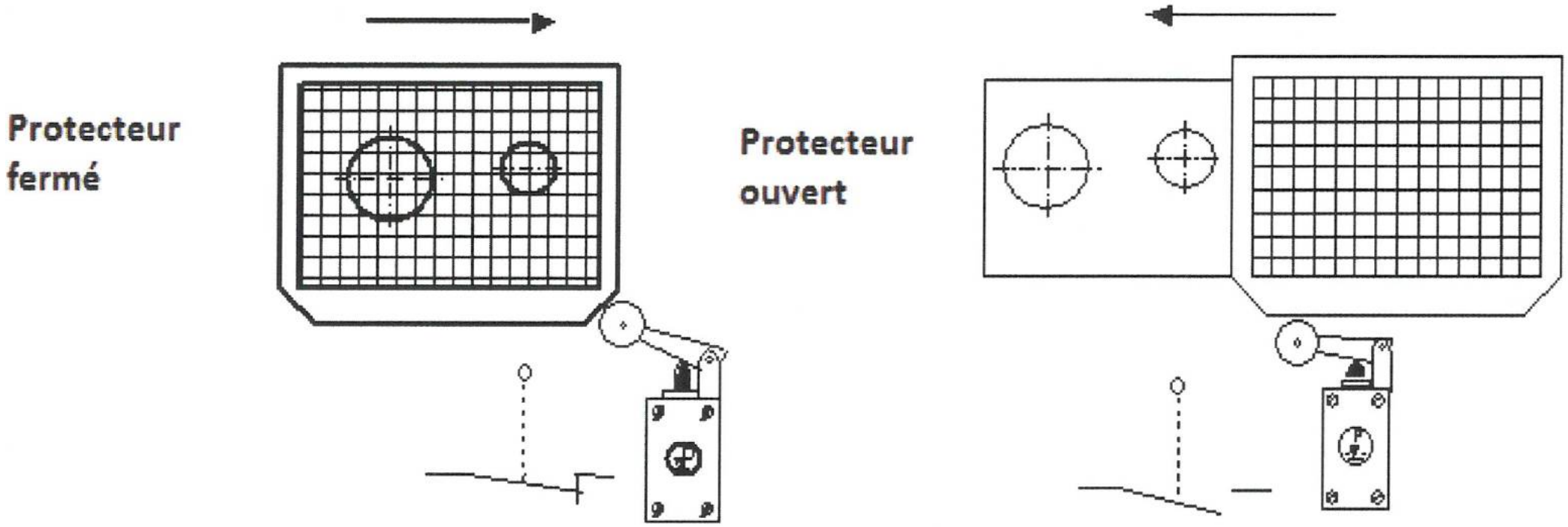





Sources: ISO 14119

# Dispositifs de verrouillage – Type 1

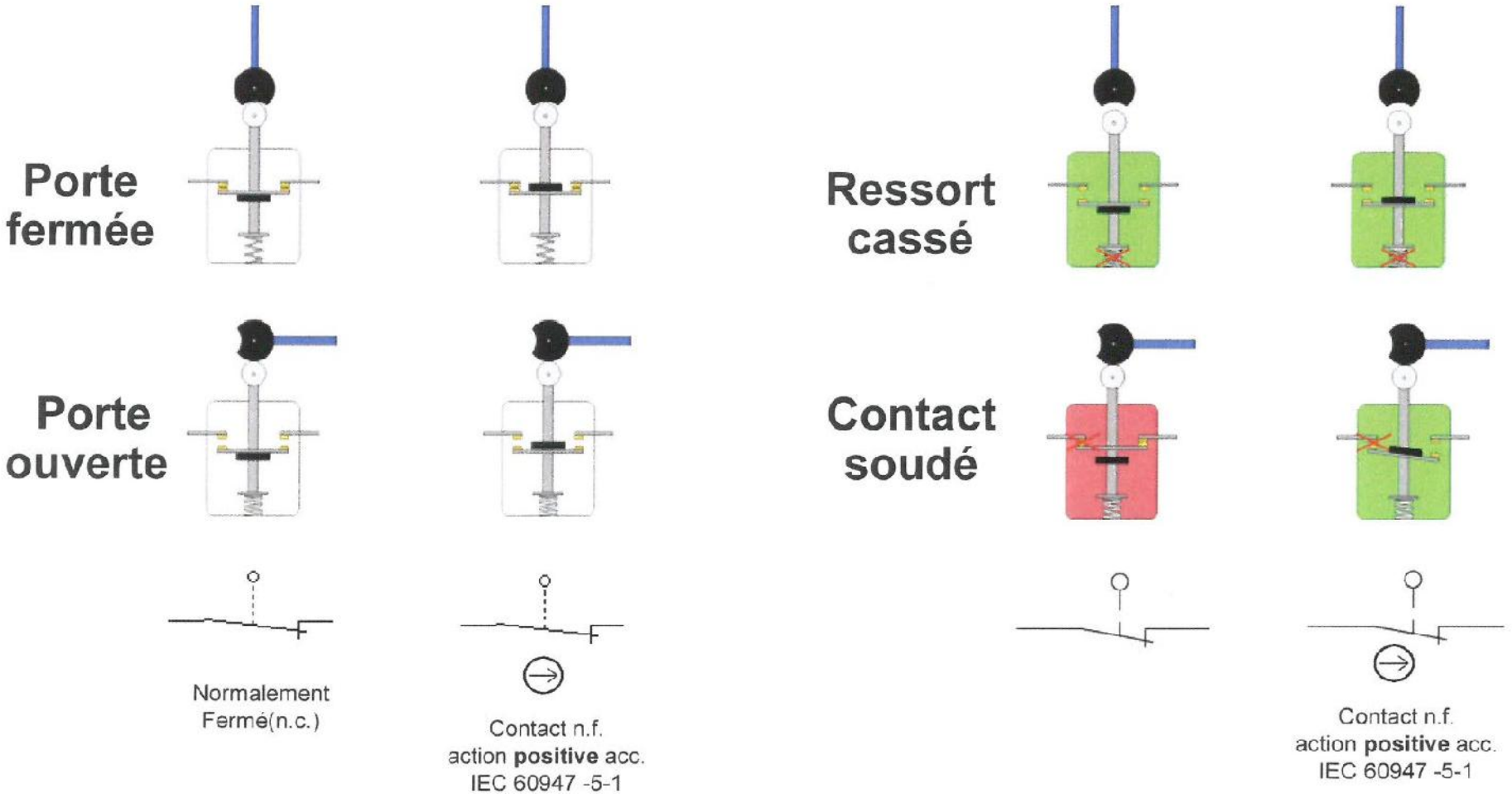
Est-ce une action directe ?





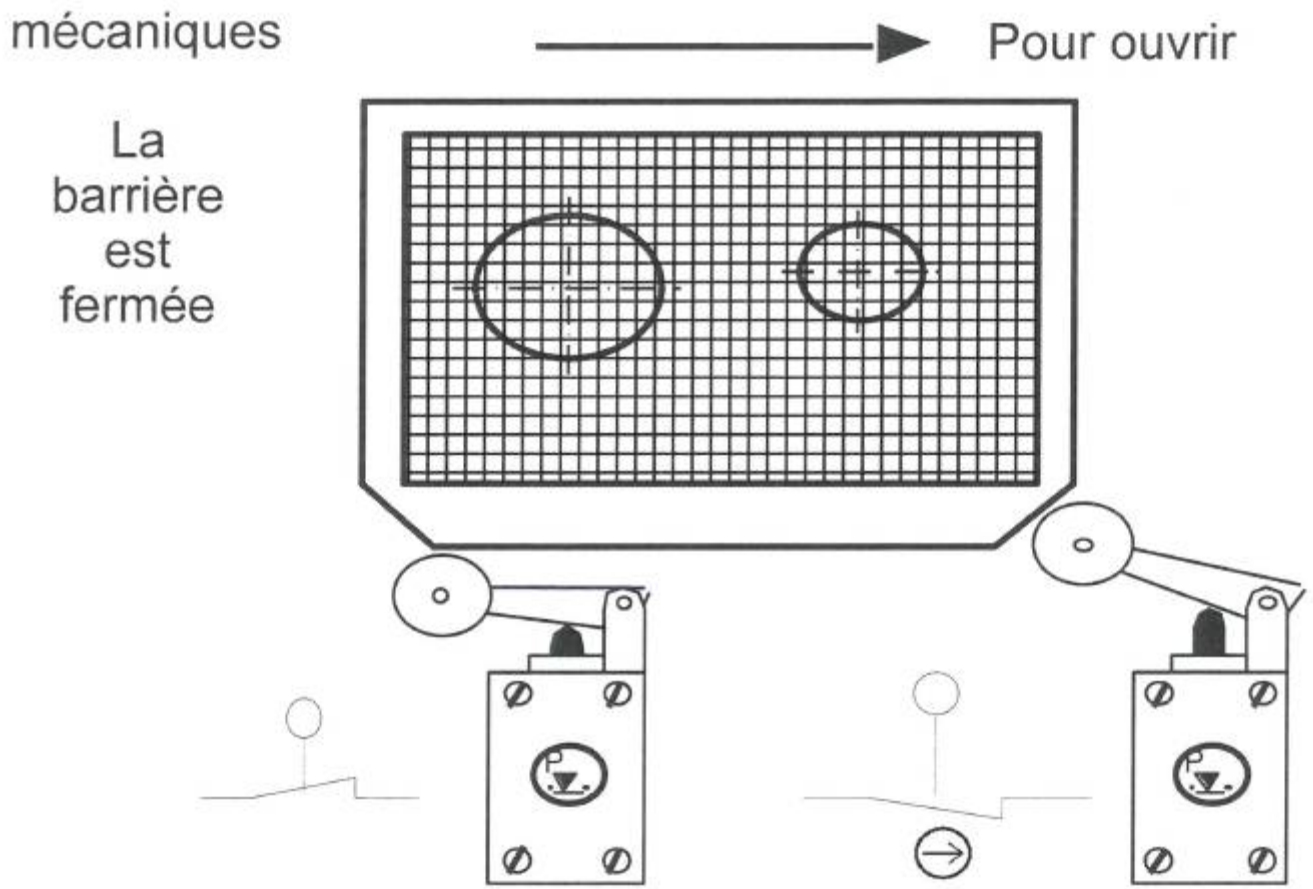

Sources: ISO 14119

# Dispositifs de verrouillage – Type 1 - Défaillances




Pour les application demandant un niveau de sécurité élevé, un seul dispositif de verrouillage n’est parfois pas acceptable.

# Dispositifs de verrouillage – Redondance et diversité




Interrupteur de fin de course qui ne possède pas une action directe mécanique

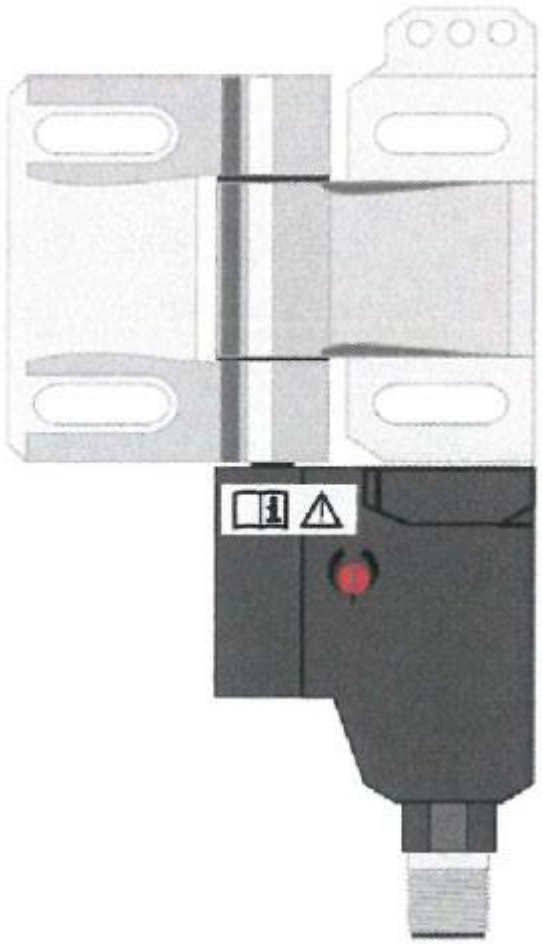
Interrupteur de fin de course à action mécanique directe

# Dispositifs de verrouillage – Type 1 – Exemple

**Interrupteur de sécurité sur charnière:**

Monté sur l'axe de la charnière d'une porte ou d'une barrière

- Difficile à neutraliser sans le démonter
- Ne nécessite qu'une petite rotation pour activer le circuit de commande
- Ne convient parfois pas pour les portes trop grandes (ouverture sans détection trop grande



Sources: Pilz CMSE

# Dispositifs de verrouillage – Type 2 – Exemple

**Dispositifs de verrouillage de sécurité à broche**

- Constitué d'un corps d'interrupteur et d'une broche d'actionneur.
- Action mécanique directe à l'ouverture
- Généralement conçu de manière à ce que la broche reste dans l'actionneur (avec une force de maintien), à moins d'être fixée sur une porte.
- Un alignement raisonnablement précis est nécessaire
- Difficile de tricher si la broche est de bonne qualité
- Ne convient pas à des applications pour lesquelles l'hygiène et la propreté sont esentielles.
- Peuvent être intégrés à un dispositif de verrouillage monté sur un protecteur

Sources: Pilz CMSE

# Dispositifs de verrouillage – Type 3 et 4 – Exemple

**Dispositifs de verrouillage magnétiques**

- Complètement hermétiques, résistants à la poussière, aux liquides…
- Conviennent à des applications pour lesquelles l'hygiène et la propreté sont essentielles
- Utilisent des aimants codés (Type 4)
- Un ensemble d'aimants peut n'être codé qu'à partir de bandes magnétiques multipolaires
- Impossible qu'un aimant simple ne contourne l'interrupteur
- Doit avoir une surveillance de la surintensité et/ou de la redondance et un contrôle automatique
- Tolérance au désalignement (contrairement aux broches)
- Peuvent être actionnés sans contact

Sources: Pilz CMSE

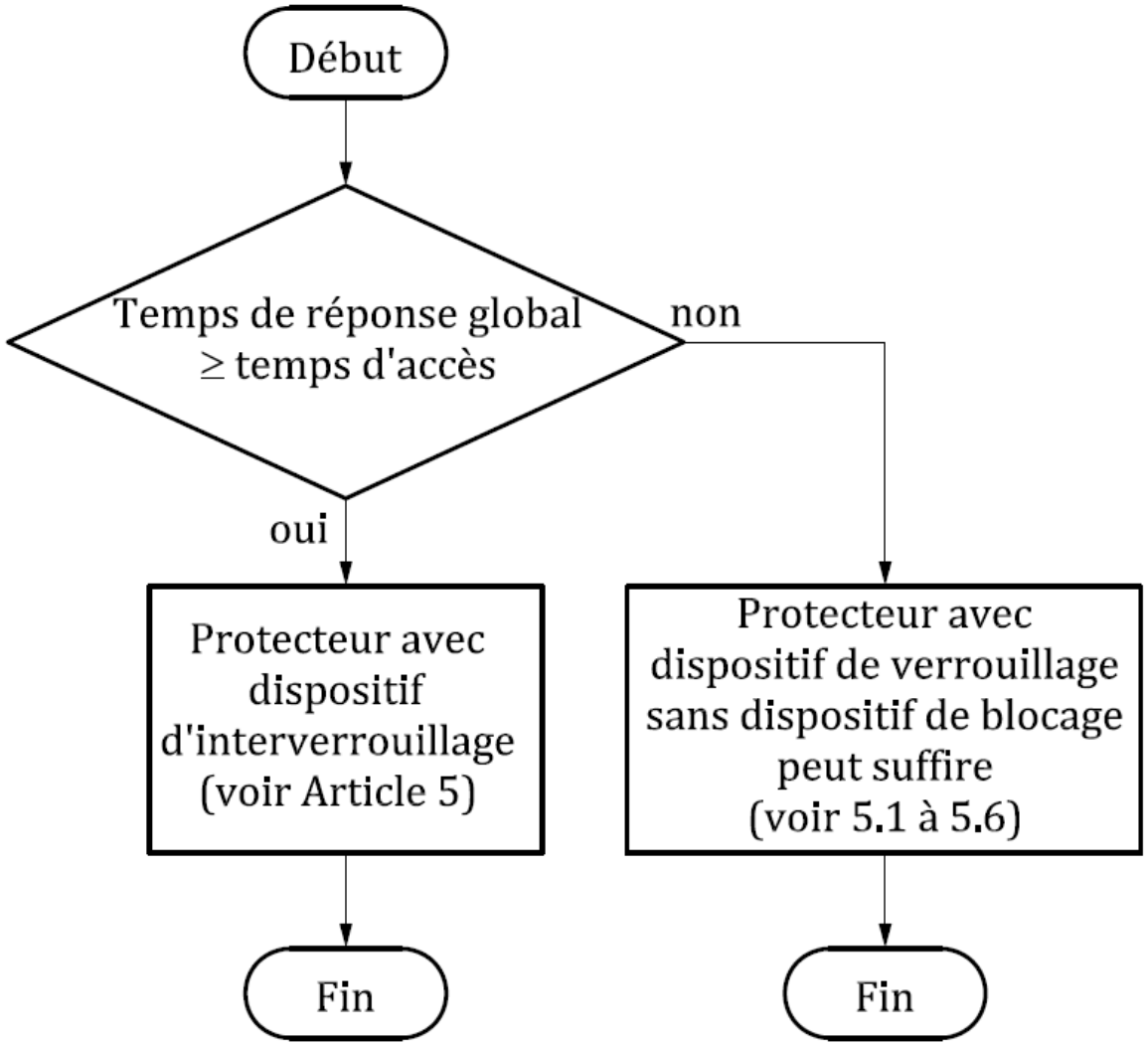
# Dispositifs d’interverrouillage

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Dispositifs d'interverrouillage – Choix

Un dispositif d'interverrouillage doit être utilisé lorsque les temps d'arrêts globaux du système (exemple: inertie de la machine) dépasse le temps nécessaire pour accéder à la zone dangereuse une fois le protecteur ouvert.

Le temps d'accès doit être calculé à partir de la distance entre la zone dangereuse et le protecteur ainsi que la vitesse d'approche (voir ISO 13855 pour les valeurs types)






Sources: Pilz CMSE

# Dispositifs d’interverrouillage – Définition

Le dispositif d’interverrouillage ne doit autoriser les fonctions dangereuses de la machine uniquement lorsqu’il est enclenché et verrouillé.

Exigences de conception:

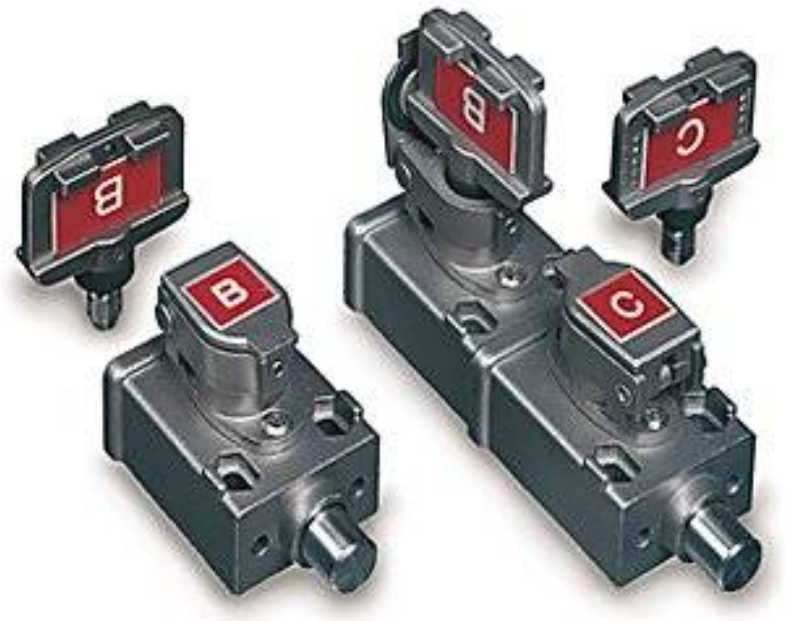
- Résister aux forces mécaniques
- Résistance suffisante pour empêcher l’ouverture du protecteur
- La position verrouillée doit être surveillée par le système
- Pour la protection du personnel, la fonction d’interverrouillage doit généralement être réalisée par manque de tension (tension à 1 pour effectuer le déverrouillage)
- Un déblocage auxilière du protecteur doit être considéré pour sortir de la zone dangereuse (risque d’enfermement)

# Dispositifs d'interverrouillage – Clé captive

Le système de verrouillage à clé captive est un système:

- Éprouvé et à haut niveau d'intégrité
- Qui permet d'avoir toutes les sources d'énergie réduites à néant
- Qui est facile à adapter et personnaliser
- Qui force à effectuer une série d'opérations pour accéder à la machine

La clé de sécurité permettant d'entrer dans la zone dangereuse peut être intégrée au système.






Sources: Pilz CMSE

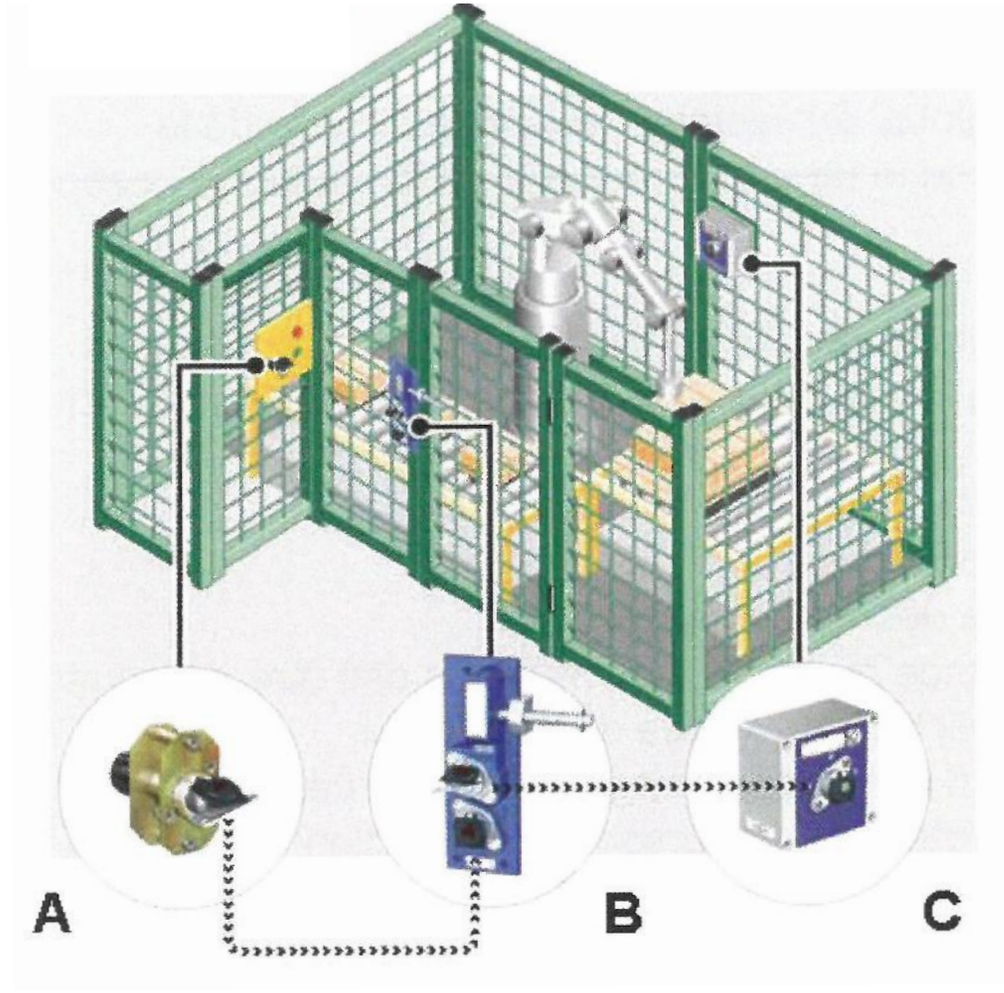
# Dispositifs d’interverrouillage – Clé captive - Exemple

Afin de pénètrer dans la zone dangereuse, l’opérateur doit enlever la clé du point A ce qui coupe l’alimentation de la machine.

Placer cette clé dans le point B permet de libérer une seconde clé qui était captive du point B et d’ouvrir la porte.

Cette seconde clé permettra d’activer le mode maintenance (dégradé) en l’utilisant dans le point C.

Afin de relancer la machine, la seconde clé devra être replacée dans le point B afin de verrouiller la porte et libérer la clé permettant l’enclenchement de la machine.






Sources: Pilz CMSE

# Dispositifs de verrouillage – Prévention de la neutralisation

| Principes et mesures | Dispositif de verrouillage de type 1, excepté les dispositifs de verrouillage à charnière et de type 3 | Dispositif de verrouillage de type 1, à charnière uniquement | Dispositifs de verrouillage de type 2 et de type 4 à codage de bas niveau ou de niveau moyen comme indiqué en 7.2 b) 1) ou 7.2 b) 2), avec ou sans blocage électromagnétique du protecteur | Dispositifs de verrouillage de type 2 et de type 4 à codage de haut niveau comme indiqué en 7.2 b) 3), avec ou sans blocage électromagnétique du protecteur | Systèmes à transfert de clé (codage de niveau moyen ou de haut niveau, voir Note 2) |
|---|---|---|---|---|---|
| Montage hors de portée, voir 7.2 a) 1) | X | | X | | |
| Obstacle physique/écran, voir 7.2 a) 2) | | | | | |
| Montage en position cachée, voir 7.2 a) 3) | | | | | |
| Surveillance de l'état ou essais cycliques, voir 7.2 d) 1) i) et ii) | | | | | |
| Fixation non détachable de l'interrupteur de position et de l'actionneur, voir 7.2 c) | | | | | |
| Fixation non détachable de l'interrupteur de position, voir 7.2 c) | | M | | | M |
| Fixation non détachable de l'actionneur, voir 7.2 c) | | M | M | M | M |
| Dispositif de verrouillage supplémentaire et vérification de la plausibilité, voir 7.2 d) 2) | R | | R | | |

X Il est obligatoire d'appliquer au moins l'une des mesures.

M mesure obligatoire

R mesure recommandée (supplémentaire)

NOTE 1 Le Tableau 3 est destiné à être utilisé pour le choix de mesures appropriées de prévention de la neutralisation des dispositifs de verrouillage. Selon l'appréciation du risque, l'application de plusieurs des mesures indiquées peut être nécessaire.

NOTE 2 Si le nombre de dispositifs à transfert de clé utilisé dans un site est connu, des actionneurs codés peuvent constituer une mesure suffisante de prévention de la neutralisation raisonnablement prévisible dans les conditions suivantes:

— si le codage est marqué sur le dispositif, il convient que chaque dispositif de verrouillage ait un codage différent et

— il convient que l'actionneur ait un codage de niveau moyen ou de haut niveau.

NOTE 3 Il convient de bien distinguer le niveau de codage des clés d'actionneur et le codage des «mécanismes à pêne ou loquet de blocage» dans un système à transfert de clé. Ce tableau concerne uniquement le niveau de codage des clés d'actionneur.

NOTE 4 Les mesures du Tableau 3 satisfont aux spécifications minimales.

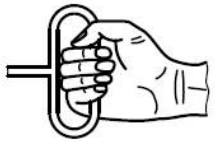
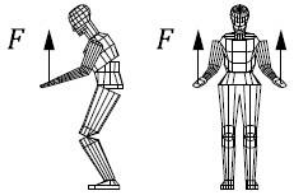
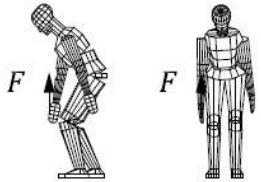
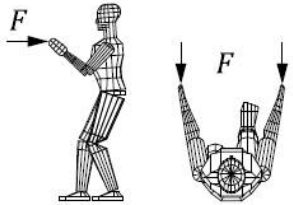
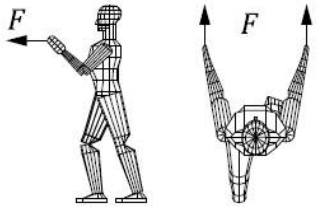


Sources: Pilz CMSE

# Dispositifs de verrouillage et d’interverrouillage

Exemples dans les Annexes A, B, C, D, E, F et G de la norme ISO 14119

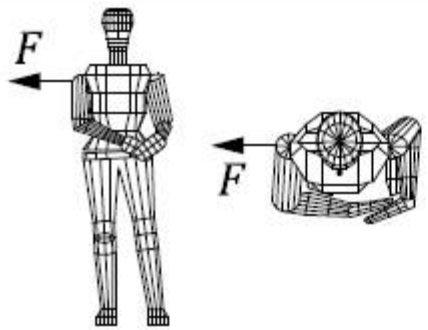
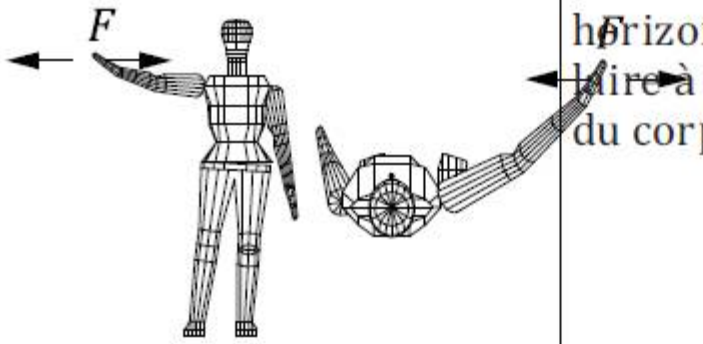
# Dispositifs de verrouillage, force maximale autorisée

| Direction de la force | | Posture | Application de la force | Valeur de la force N |
|---|---|---|---|---|
|  | traction horizontale (traîner) | assis | à une seule main | 600 |
|   | verticale vers le haut | debout, torse et jambes fléchis, pieds parallèles | à deux mains, prises horizon-tales | 1 400 |
|   | verticale vers le haut | debout, libre | à une seule main, prises horizontales | 1 200 |
|   | horizontale, parallèle à l'axe de symétrie du corps, vers l'arrière<br>traction | droit debout, pieds parallèles, ou posture de marche | à deux mains, prises verticales | 1 100 |
|   | horizontale, parallèle à l'axe de symétrie du corps, vers l'avant<br>poussée | debout, pieds parallèles, ou posture de marche | à deux mains, prises verticales | 1 300 |



Sources: Pilz CMSE

# Dispositifs de verrouillage, force maximale autorisée

| Direction de la force | | Posture | Application de la force | Valeur de la force N |
|---|---|---|---|---|
|  | horizontale, perpendiculaire à l'axe de symétrie du corps, vers l'extérieur | debout, torse fléchi sur le côté | épaule poussant une plaque métallique sur le côté | 1 300 |
|  | horizontale, perpendiculaire à l'axe de symétrie du corps | debout, pieds parallèles | à une seule main, prise verticale | 700 |



Sources: Pilz CMSE

# Barrières immatérielles

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Barrières immatérielles – Application et fonctionnement

Les barrières immatérielles sont en général utilisées lorsqu'il est nécessaire d'accéder régulièrement aux zones dangereuses.

Celles-ci ne conviennent que s'il n'y a pas de risque d'éjection de matériaux.

Principes de fonctionnement:

- Sont constituées d'un émetteur et d'un récepteur
- Le faisceau étroit émis ne doit pas avoir une divergence de plus de 10 degrés
- Le faisceau lumineux est modulé
- Des impulsions d'essai sont émises à intervalle régulier
- Ces barrières utilisent la sécurité positive (tous les faisceaux émis doivent être reçus)
- Les unités de commande peuvent être redondantes
- Résolution minimale 14mm (largeur d'une main)
- Fournissent une solution d'inhibition (Muting)



Sources: Pilz CMSE

# Barrières immatérielles – Distances de sécurité

Formule: S = (K x T) + C (selon ISO 13855)

S = distance minimale entre la barrière immatérielle et le phénomène dangereux

K = vitesse d'approche (mm/s)

T = performance globale d'arrêt (s)

C = distance supplémentaire (mm) requise dans certains cas

Sources: Pilz CMSE

# Barrières immatérielles – Inhibition (Muting)

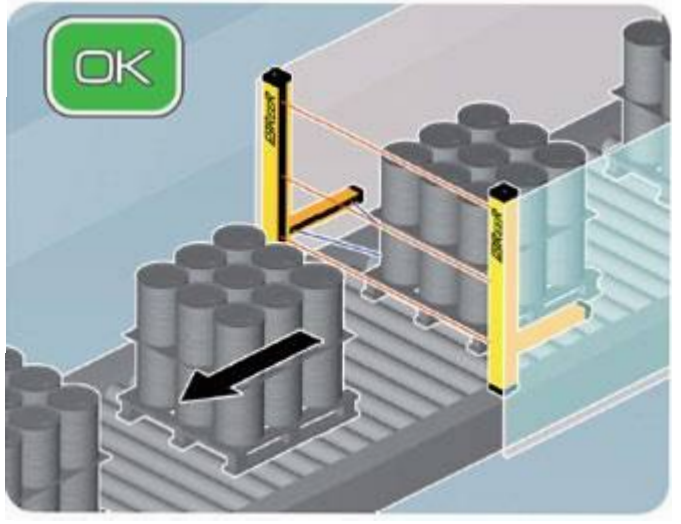
L'inhibition est la suspension automatique temporaire de la fonction de sécurité de la barrière.

Celle-ci permet l'entrée ou la sortie de matériel dans les cellules de la machine (p.ex. une palette)

La barrière immatérielle est inhibée au moment du passage du matériel afin d'éviter le déclenchement de la fonction de sécurité

Le système est conçu pour que le personnel ne puisse pas le tromper

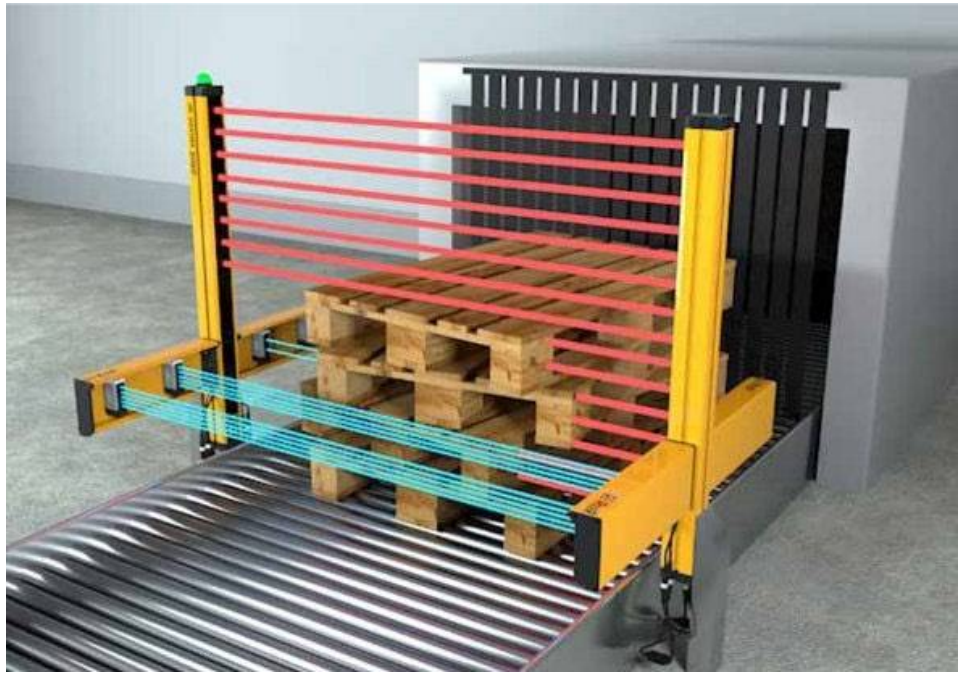
Convient aux lignes de production automatisées continues



Sources: Pilz CMSE

# Barrières immatérielles – Conditions d'inhibition

- Ne peut se produire uniquement lorsque le matériel bloque l'accès à la zone dangereuse
- Doit être automatique
- Ne doit pas dépendre d'un signal électrique unique
- Ne doit pas complétement dépendre des signaux des logiciels standards
- Les signaux d'inhibition se produisant dans le cadre d'une combinaison non valide ne doivent pas permettre l'inhibition mais le verrouillage de la machine
- L'inhibition doit être désactivée tout de suite après le passage ud matériel à travers la barrière de sécurité





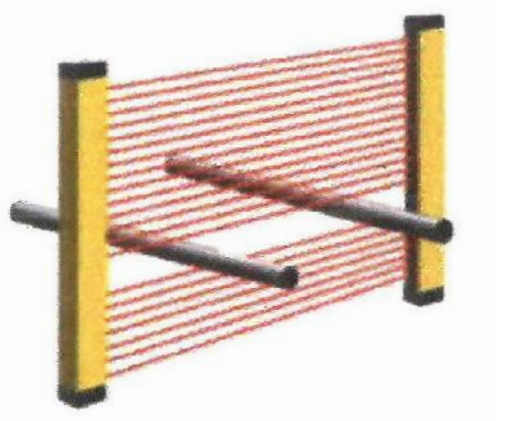
Sources: Pilz CMSE

# Barrières immatérielles – Occultation

Dans certains cas d'utilisation, les barrières lumineuses peuvent être programmées pour permettre une occultation de certain faisceaux sans activer la fonction de sécurité:

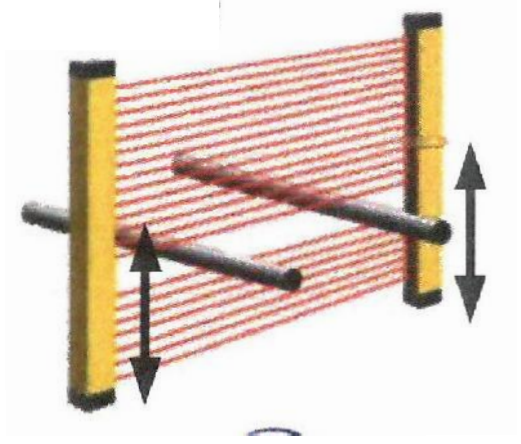
Occultation fixe

- Des faisceaux prédéterminés sont coupés
- Si un autre faisceau est coupé, la machine sera stoppée



Occultation flottante

- Un nombre fixe de faisceaux sont coupés
- Seul les faisceaux prévus dans la trajectoire peuvent être coupés





Sources: Pilz CMSE

# Tapis sensibles à la pression

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Tapis sensibles – Définition

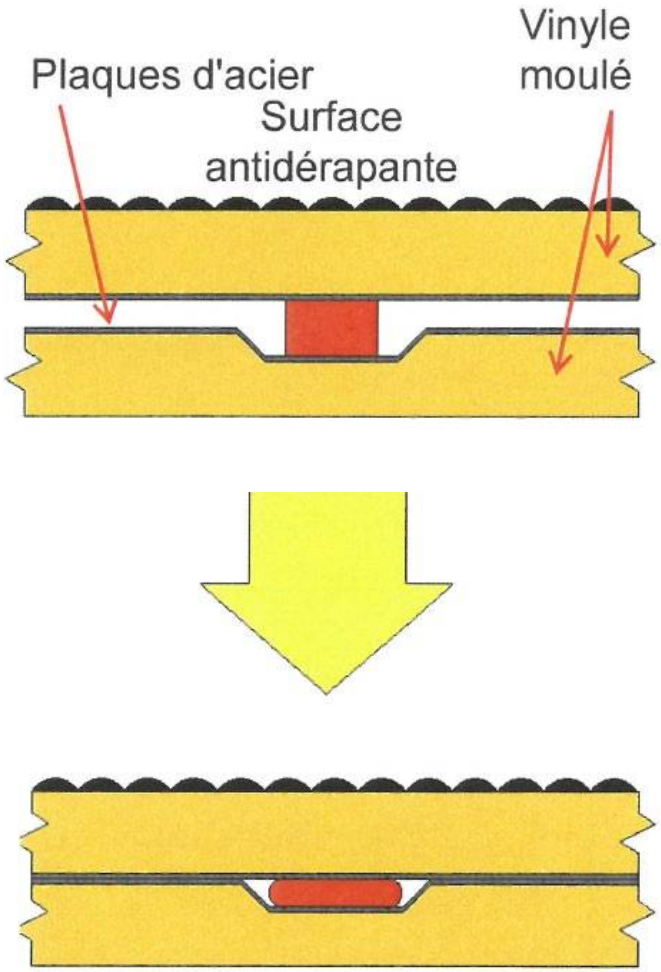
- L'objectif de ces tapis est d'arrêter les fonctions dangereuses de la machine lorsqu'une pression est appliquée.
- Ils assurent une protection autour des phénomènes dangereux de la machine.
- Généralement, ils sont associés à d'autres mesures de sécurité.

Sources: Pilz CMSE

# Tapis sensibles – Fonctionnement

**Principe de fonctionnement (Type normalement ouvert):**

- Surface de contact séparées par des ressorts en caoutchouc
- Lorsqu'une pression est appliquée à la surface du haut, la distance d'isolement est comprimée
- Les deux surfaces de contact se touchent
- La résistance intégrée tombe en dessous de la valeur définie
- Un dispositif de commutation évalue constamment les contacts afin de détecter une rupture de fil



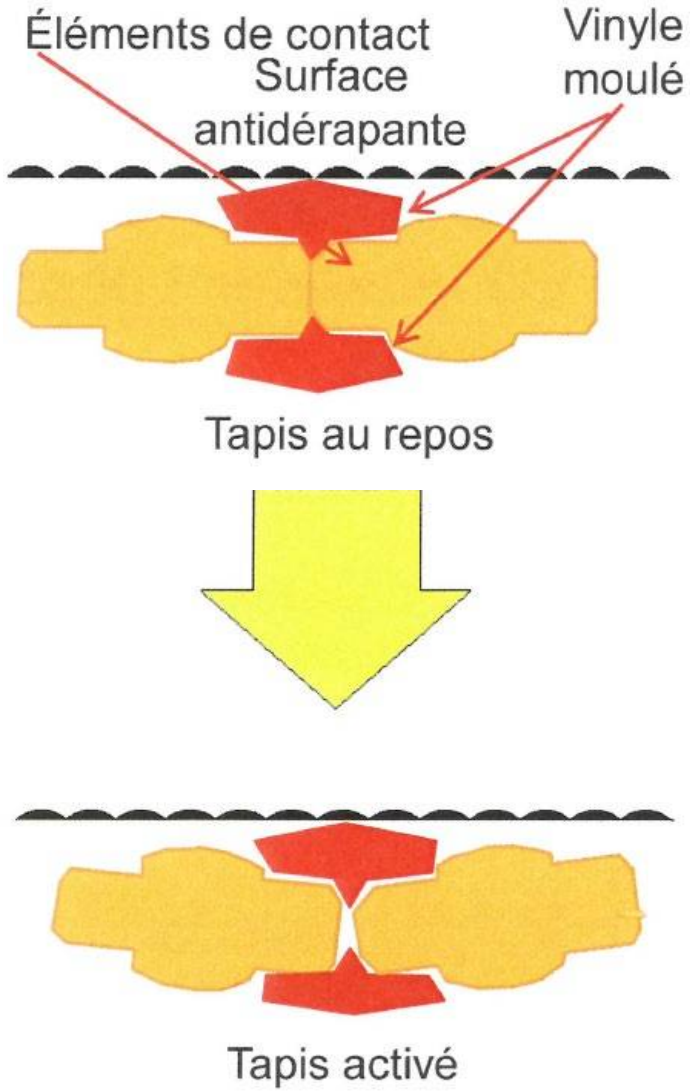



Sources: Pilz CMSE

# Tapis sensibles – Fonctionnement (2)

**Principe de fonctionnement (Type normalement fermé):**

- Le tapis contient une série d'éléments de contact à ouverture positive
- S'il n'y a pas de pression appliquée, le courant circule
- Si une pression est appliquée, les contacts s'ouvrent
- Le dispositif de commutation évalue les contacts à la façon d'un système de verrouillage






Sources: Pilz CMSE

# Commandes bimanuelles

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Commandes bimanuelles – Définition

L'objectif des commandes bimanuelles est de s'assurer que l'opérateur utilise ses deux mains pour activer la machine afin d'éviter qu'une d'entre elles ne soit blessée.

- Ce type de dispositif ne protège qu'un opérateur
- D'autres moyens de protection doivent être envisagés le cas échéant

Les commandes bimanuelles ne doivent être utilisées que lorsque l'accès aux parties dangereuses de la machine sont sous la supervision directe de l'opérateur.

Sources: Pilz CMSE

# Commandes bimanuelles – Types

Trois types existent:

- Type I
  - Deux organes de service (boutons) et leur actionnement simultané par les deux mains
  - Actionnement simultané continu
  - Le fonctionnement s'arrêtera après le relâchement d'un bouton ou des deux
- Type II
  - Exigences du type I
  - Nécessite également le relâchement des deux boutons avant réarmement de la machine
- Type III
  - Exigences du type II
  - Nécessite un intervalle < 0.5s entre la pression des deux boutons
  - Si le délai est dépassé, il faudra relâcher les deux boutons pour réarmer la machine

# Commandes bimanuelles – Types et exigences minimales

| Exigences | Paragraphe | Type | | | | |
|---|---|---|---|---|---|---|
| | | Ia | II | III | | |
| | | | | A | B | C |
| Usage des deux mains (manœuvre simultanée) | 5.2 | X | X | X | X | X |
| Relation entre signaux d'entrée et signaux de sortie | 5.3 | X | X | X | X | X |
| Interruption du signal de sortie | 5.4 | X | X | X | X | X |
| Prévention d'une manœuvre accidentelle | 5.5 | X | X | X | X | X |
| Prévention de la fraude | 5.6 | X | X | X | X | X |
| Réinitialisation du signal de sortie | 5.7 | | X | X | X | X |
| Manœuvre synchrone | 5.8 | | | X | X | X |
| Au minimum PL c (conformément à l'ISO 13849-1) ou SIL 1 (conformément à l'IEC 62061) | | X | | X | | |
| Au minimum PL d avec la catégorie 3 (conformément à l'ISO 13849-1) ou SIL 2 avec HFT = 1 (conformément à l'IEC 62061) | | | X | | X | |
| Utilisation de PL e avec la catégorie 4 (conformément à l'ISO 13849-1) ou SIL 3 avec HFT = 1 (conformément à l'IEC 62061) | | | | | | X |

[a] Chaque fois que l'on envisage le choix d'un dispositif de commande bimanuelle de type I, il est important de réaliser soigneusement l'appréciation du risque afin de déterminer si les caractéristiques de manœuvre synchrone et de réinitialisation du signal de sortie peuvent être négligées.



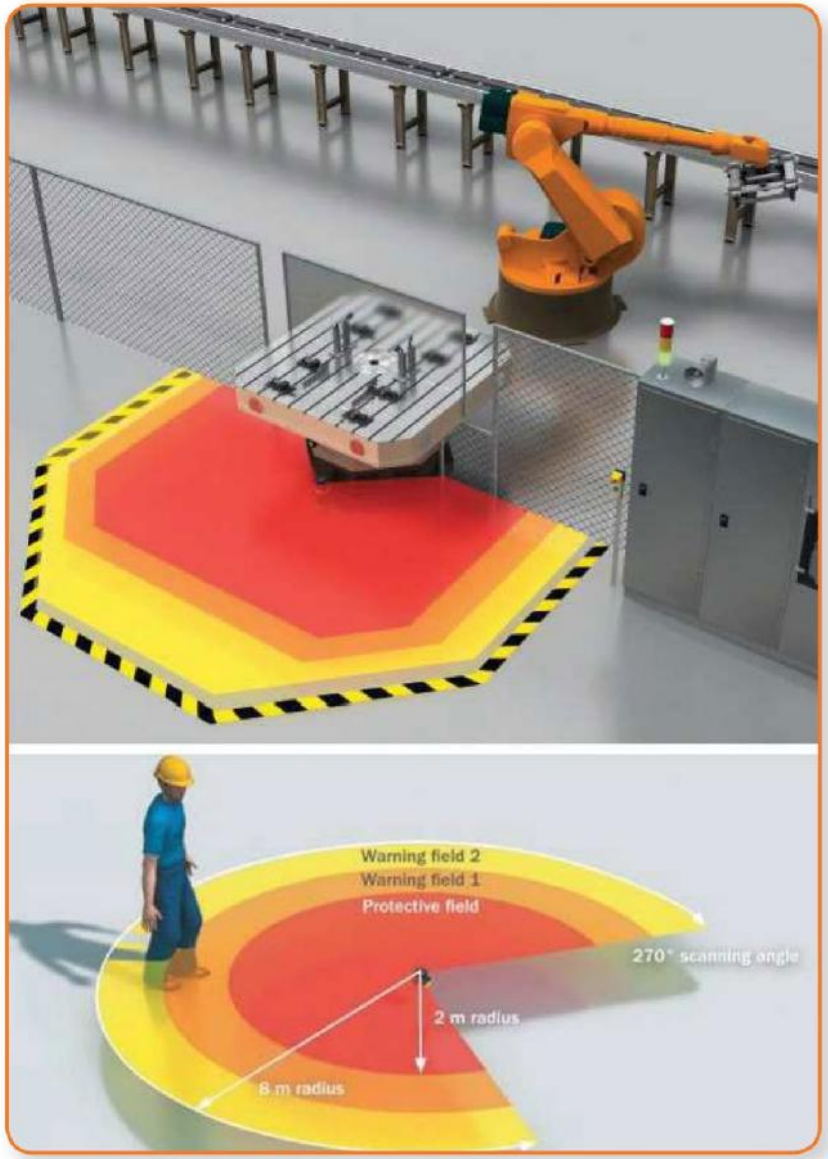
Sources: ISO13851

# Scanners de sécurité

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Scanners de sécurité - Définition

- Mesure les distances selon le principe du temps de vol
- Balayage 2D
- Zone de balayage pouvant habituellement atteindre 270°
- Zone de détection et d'avertissement définies
- Peut être programmé pour s'adapter à différents contours de champ et configurations
- Convient aussi bien à des véhicules de guidage automatiques qu'à des zones de protection autour de grandes machines

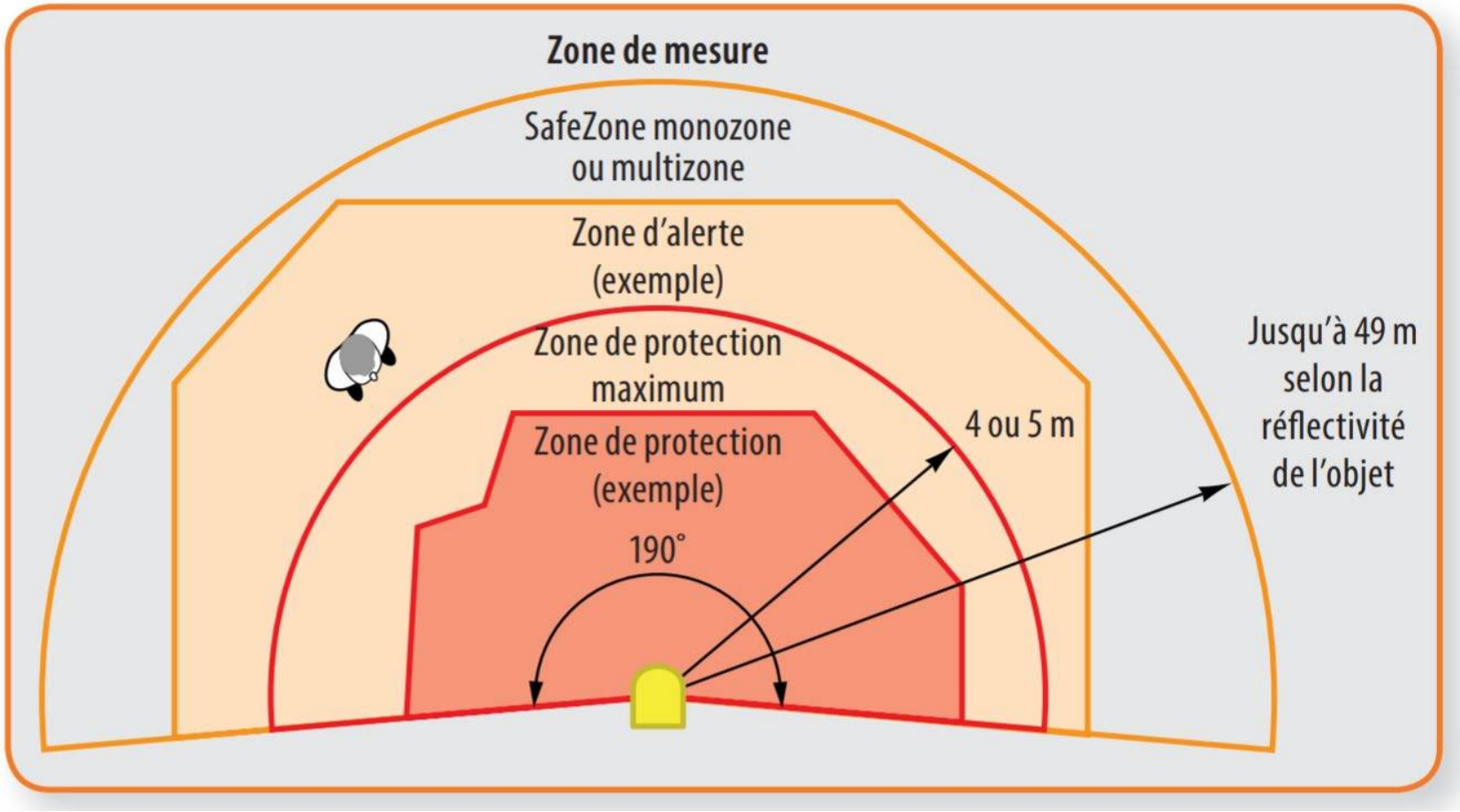





Sources: Electropoint.ch

# Scanners de sécurité - Zones

Remarque: La zone de balayage maximale peut être plus grande que celle qui et montrée





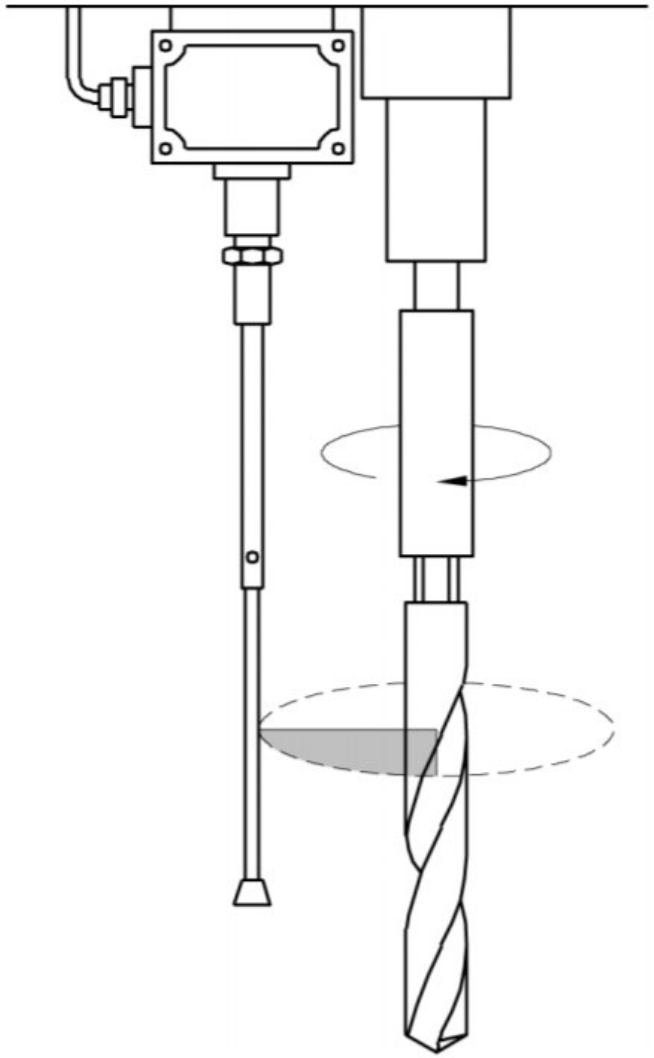

Sources: Electropoint.ch

# Autres dispositifs de sécurité

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Interrupteur d’arrêt télescopique

- Similaire aux interrupteurs de fin de course
- Mode de fonctionnement positif
- Simple d’utilisation
- Assure une protection à l’aide d’une sonde télescopique qui détecte les mouvements



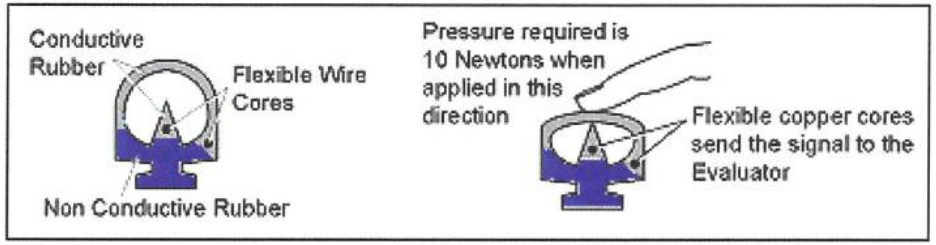


Sources: EN 12717

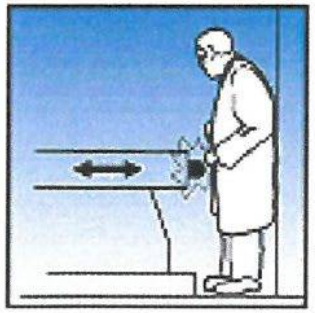
# Bandes sensibles

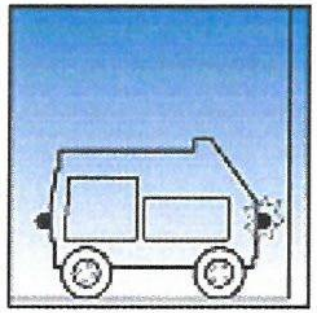
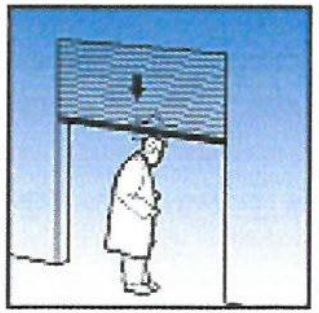
Utilisées pour:

- La détection de véhicules
- Les portes motorisées
- Les portes à enroulement




Remarque: La pression appliquée par une personne ou un objet doit être supérieure à celle requise pour activer la bande sensible





Sources: Pilz CMSE

# Les arrêts d’urgence

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Arrêts d’urgence - Catégories

Les arrêts d’urgences sont développés selont la norme ISO 13850. Deux catégories d’arrêts d’urgence existent:

Catégorie 0:

- «Arrêt par la suppression immédiate de l’alimentation des actionneurs de la machine» (C’est-à-dire arrêt non contrôlé)

Catégorie 1:

- «Arrêt contrôlé avec alimentation des actionneurs jusqu’à l’arrêt de la machine. L’alimentation des actionneurs est ensuite coupée une fois l’arrêt réalisé.

**Un dispositif d’arrêt d’urgence ne doit pas remplacer d’autres mesures de protection mais les compléter** (Conformément à l’Annexe I de la directive des machines)

# Arrêts d’urgence - Exigences

- Action mécanique positive
- Un actionneur générant une commande d’arrêt d’urgence doit rester enclenché lorsqu’il est actionné
- Afin de réarmer la commander d’arrêt d’urgence, il sera nécessaire de déverrouiller l’actionneur
- Le dispositif de commande générant le signal d’arrêt d’urgence doit maintenir la commande d’arrêt d’urgence jusqu’à son réarmement
- Le réarmement du dispositif de commande doit uniquement s’effectuer manuellement
- Le réarmement du dispositif de commande à lui seul ne doit pas entraîner un redémarrage de la machine

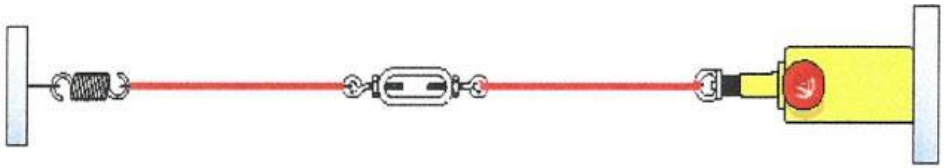


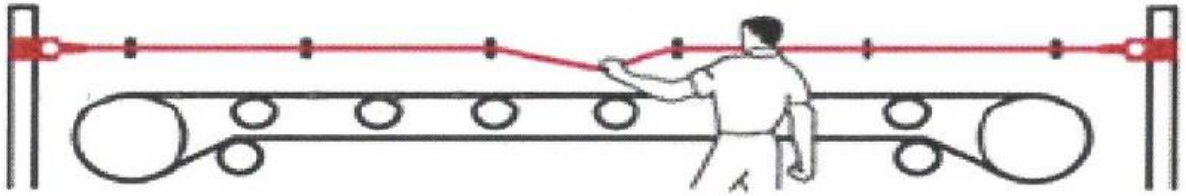
Sources: Pilz CMSE

# Arrêts d’urgence – Types d’actionneurs

Différentes sortes d’actionneurs d’arrêt d’urgence existent:

- Interrupteur actionné par un bouton-poussoir, de type coup de poing
- Fil ou câble
- Pédale sans protection mécanique
- Poignée ou interrupteurs rouge et jaune







Sources: Pilz CMSE

# Arrêts d’urgence – Couleurs

Couleurs des arrêts d’urgence

- Couleur de l’actionneur – **Rouge**
- Couleur de fond – **Jaune**

Autres éléments à prendre en compte:

- Etiquettes
- Repères sur les fils ou les câbles

Sources: Pilz CMSE

# Choix des composants: Avantages et limites

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Avantages et limites

| Composant | Avantages | Limites | Application |
|---|---|---|---|
| Protecteur fixe | Facile à installer, rentable, protection totale contre les phénomènes dangereux | Nécessite des outils pour le démontage, interdit l'accès à la zone | Zones dangereuses dans lesquelles une maintenance régulière n'est pas nécessaire |
| Protecteur mobile | Rentable, protection totale contre les phénomènes dangereux | Probabilité de le neutraliser | Zones dans lesquelles un accès régulier est nécessaire |
| Protecteur réglable | Permet le passage de produits de différentes dimensions | Facile à contourner, assure un faible niveau de sécurité, nécessite des mesures de sécurité supplémentaires | Opérations de perçage, machines à scier |
| Protecteur avec dispositif de verrouillage | Garantit que les fonctions dangereuses ne peuvent avoir lieu si le protecteur est ouvert | Plus d'un dispositif de verrouillage nécessaire au-delà d'un d'un PL c (ISO 13849) | Zones dans lesquelles un accès régulier est nécessaire |
| Distance de sécurité | Garantit une distance appropriée par rapport à la zone dangereuse | - | Protection mécanique |



Sources: Pilz CMSE

# Avantages et limites (2)

| Composant | Avantages | Limites | Application |
|---|---|---|---|
| Interrupteur de fin de course à déclenchement positif | Sécurité intégrée | Les pièces mécaniques peuvent s'user, nécessite plus d'un interrupteur au delà d'un PL c (ISO 13849) | Verrouillage de porte / protecteur |
| Protecteur avec dispositif d'interverrouillage | Peut restreindre l'accès à la zone dangereuse dans le cas d'un temps d'arrêt important | Accès à la zone dangereuse si le temps d'arrêt n'est pas correctement calculé | Verrouillage de porte / protecteur |
| Verrouillage à broche | Facile à installer, principe de sécurité éprouvé, coût avantageux | Neutralisation possible avec une broche supplémentaire, ne convient pas aux applications nécessitant de la propreté, ne tolère pas le désalignement | Verrouillage de porte / protecteur |
| Interrupteurs magnétiques | Tolère les désalignements, pas de pièce mécanique, totalement fermé, convient à des applications nécessitant de la propreté | Doit être protégé de la surintensité, sensible à l'interférence électromagnétique | Verrouillage de porte / protecteur |



Sources: Pilz CMSE

# Avantages et limites (3)

| Composant | Avantages | Limites | Application |
|---|---|---|---|
| Dispositifs de déclenchement | Rentables, faciles à mettre en place | Assurent une protection très limitée | Perceuses |
| Bandes sensibles | Peu coûteux, facile à mettre en oeuvre | S'endommage facilement | Portes motorisées, phénomènes dangereux d'écrasement, détection de véhicule |
| Commande bimanuelle | Contribue au changement fréquent de matière première. Garantit que les deux mains de l'opérateur sont hors de la zone de danger avant que le mouvement n'opère | Ne procure une protection que pour l'opérateur | Petite machine de manutention, presse |
| Barrière immatérielle | Peut être inhibée pour faciliter le chargement et déchargement automatique de matériel | Ne convient pas en cas de risque d'éjection de la machine | Accès fréquent nécessaire pour le chargement et déchargement ou chargement déchargement automatique |



Sources: Pilz CMSE

# Avantages et limites (4)

| Composant | Avantages | Limites | Application |
|---|---|---|---|
| Scrutateur laser | Programmation aisée de zones dangereuses | Sensible à un environnement sale, Zone de protection non matérialisée | Applications mobiles, zones de protection autour d'une machine |
| Tapis sensible | Rentable pour de petites surfaces, peut s'adapter à toutes les formes et tous les types | Sujet à des dommages mécaniques | Zone de protection autour d'une machine |



Sources: Pilz CMSE

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. Nathanaël Jaquet - Mesure acoustique de machines
4. Alexandre Murisier - ISO 13851
5. Juliette McMichael – Consignation (Lockout Tagout)
6. Mattéo Meister – ISO/PRF 22916 – Dispositifs microfluidiques
7. Harjeet Nagi - Norme de sécurité électrique et régimes de neutres
8. Shukri Ramadani - Les EPI
9. Quentin Müller – ISO 13857 les distances de sécurité
10. César Michaud – Les jouets radioactifs
11. Philippe Gaêl Dubuis – Chariots de Manutention
12. Julien Pernet – Retour sur l'ISO 12100
13. Anuraag Pothula – Les types de redondance
14. Gabriele Pescatore – Compatibilité électromagnétique
15. Maël Forestal – Dispositifs sensibles à la pression
16. ?
17. ?

# Questions ?

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et Fiabilité des Systèmes (SecuFS)

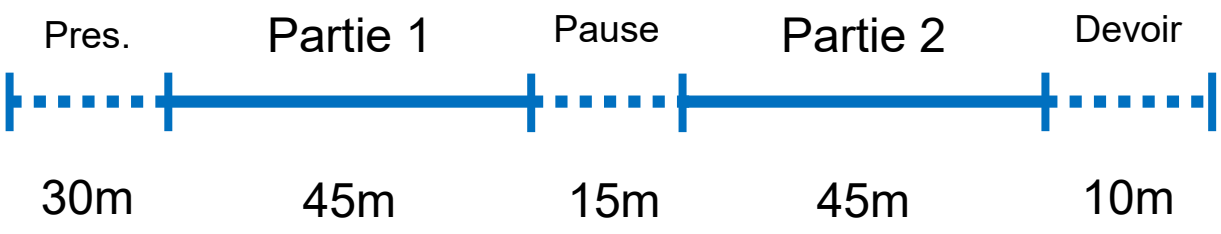
# 06 – Développement d’un composant de sécurité

Eric Silva et Semra Sezen
01.11.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | xx.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Format du cours (à partir de la semaine prochaine)




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. Nathanaël Jaquet - Mesure acoustique de machines
4. Alexandre Murisier - ISO 13851
5. Juliette McMichael – Consignation (Lockout Tagout)
6. Mattéo Meister – ISO/PRF 22916 – Dispositifs microfluidiques
7. Harjeet Nagi - Norme de sécurité électrique et régimes de neutres
8. Shukri Ramadani - Les EPI
9. Quentin Müller – ISO 13857 les distances de sécurité
10. César Michaud – Les jouets radioactifs
11. Philippe Gaêl Dubuis – Chariots de Manutention
12. Julien Pernet – Retour sur l'ISO 12100
13. Anuraag Pothula – Redondance
14. Pescatore Gabriele – CEM
15. Forestal Maël – ISO 13856-2
16. Adrien Périchon – ISO 14120
17. Monia Baouab – ISO 13731-1

# Introduction

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# ISO 13849 - Introduction

- Cette norme est une norme de type B1 qui a remplacé l'EN 954-1:1996 le 31 décembre 2011.
- Elle traite des parties des systèmes de commande relatives à la sécurité (SRP-CS)
- Elle fournit des recommandations à ceux qui sont impliqués dans la conception et l'évaluation des SRP-CS
- Elle est applicable, quelle que soit la technologie ou l'énergie utilisée (électrique, hydraulique, pneumatique, mécanique…)
- Elle a été mise à jour en 2015

# EN Standards Types

**Basic safety standard**

**Type A**

| |
|---|
| **EN ISO 12100** Safety of machinery – Risk assessment and risk reduction |

**Safety group standards**

**Type B1**

| | | | |
|---|---|---|---|
| **EN ISO 13857** Safety distances | **EN ISO 13849-1** Safety-related parts of controls | **EN ISO 13855** arm/hand speeds | **EN 62061** functional safety of control systems |

**Type B2**

| | | | |
|---|---|---|---|
| **EN ISO 13850** Emergency stop devices | **EN 61496** opto-electronic protective devices | **EN 60204-1** electrical equipment | ... more |

**Safety product standard**

**Type C**

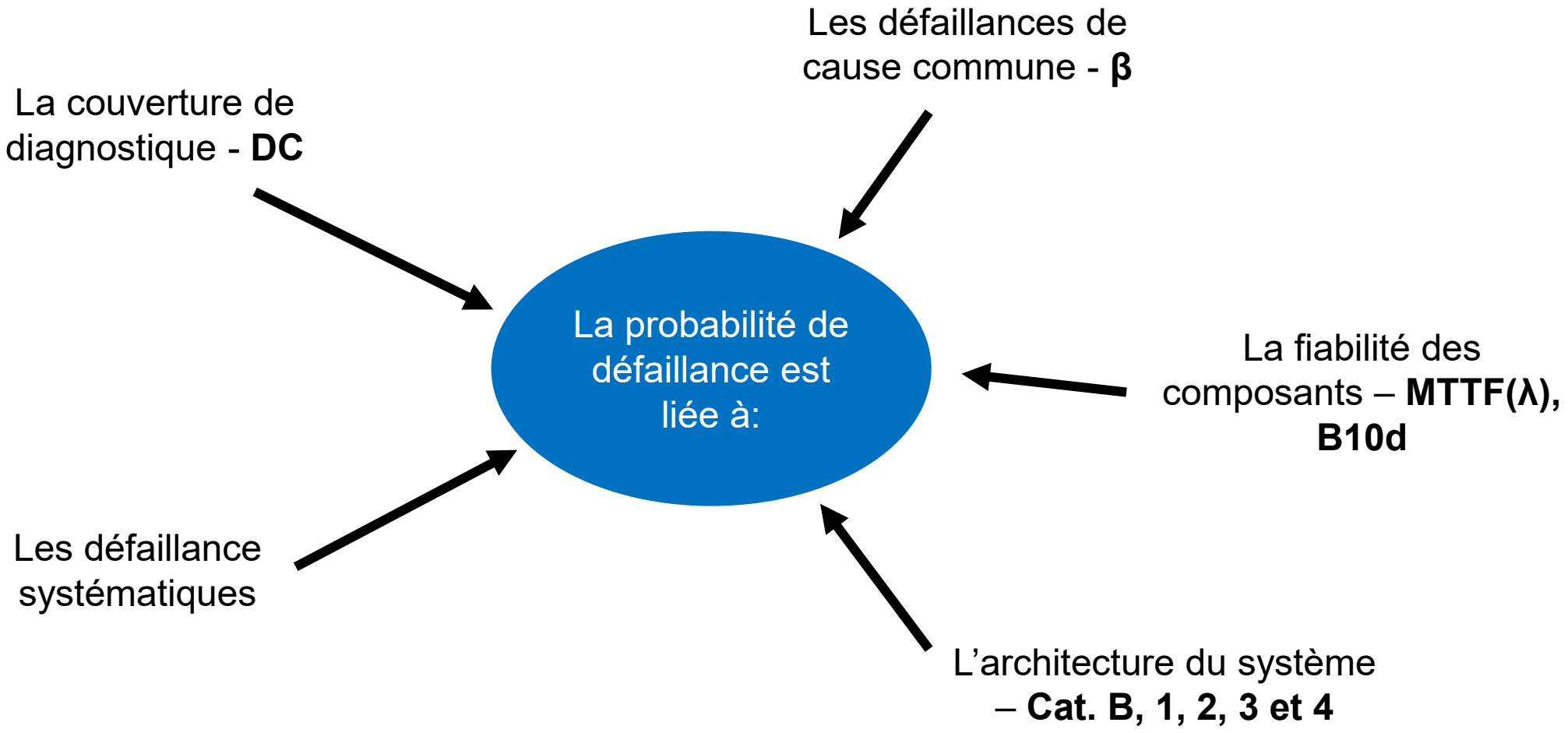
| | | | |
|---|---|---|---|
| **EN 691** Woodworking machines | **EN 10218-1** Robots | **EN 1114** Extruders | |
| **EN 692** Mechanical presses | **EN 415** Packaging machines | **EN 201** Rubber and plastics machines | ... more |
| **EN 693** Hydraulische Pressen | **EN 620** Conveyer systems | **EN 619** Continuous handling equipment piece goods | |

Une machine satisfait aux exigences de base en matière de sécurité et de protection de la santé lorsqu'elle a été construite selon ces normes harmonisées.

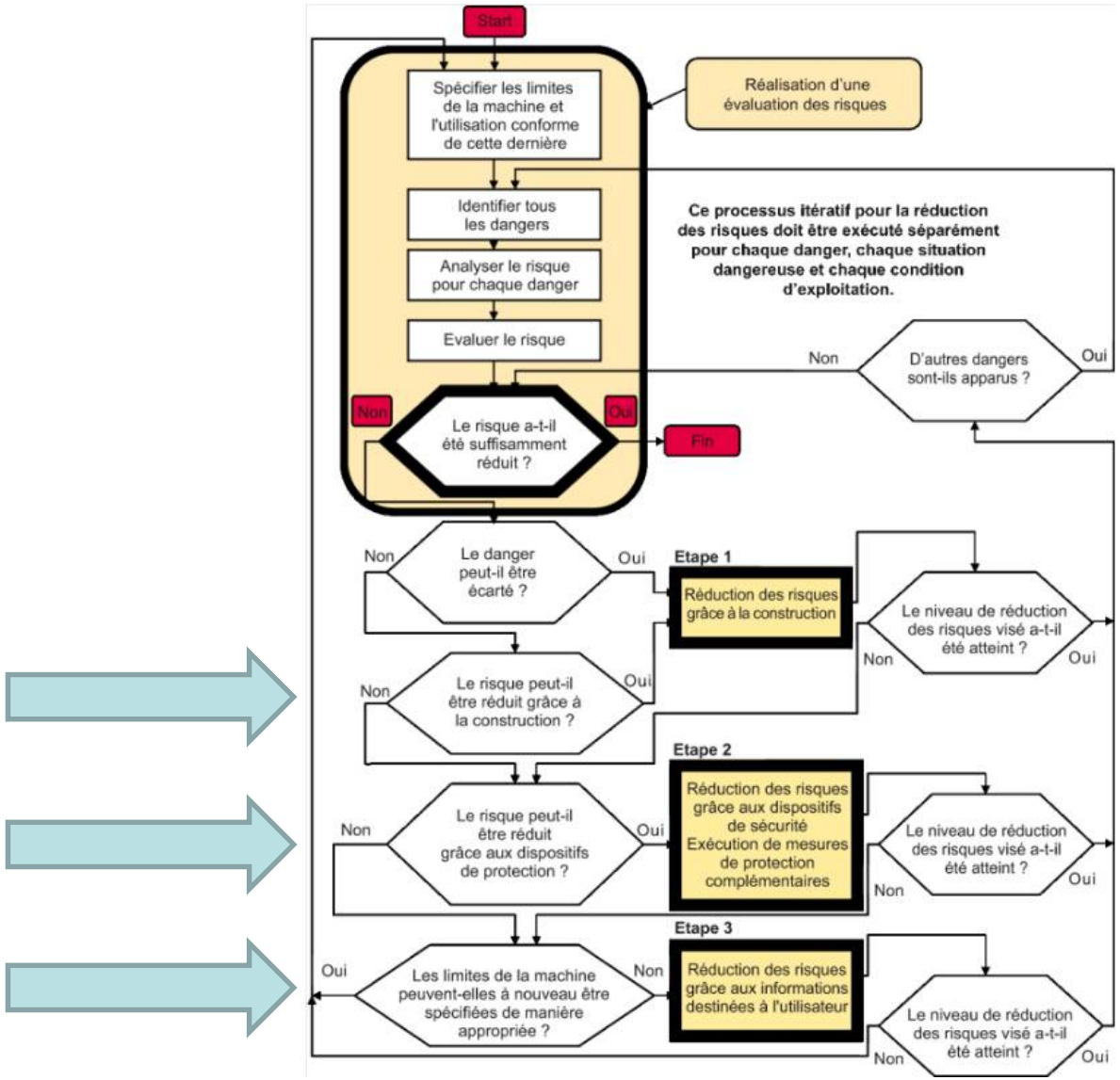
Les normes EN se divisent en différents types :

- ❑ Type A – norme de sécurité fondamentale
- ❑ Type B – norme de sécurité relative à un groupe
- ❑ Type C – norme de sécurité relative à un produit

# ISO 13849 – Les paramètres de la sécurité

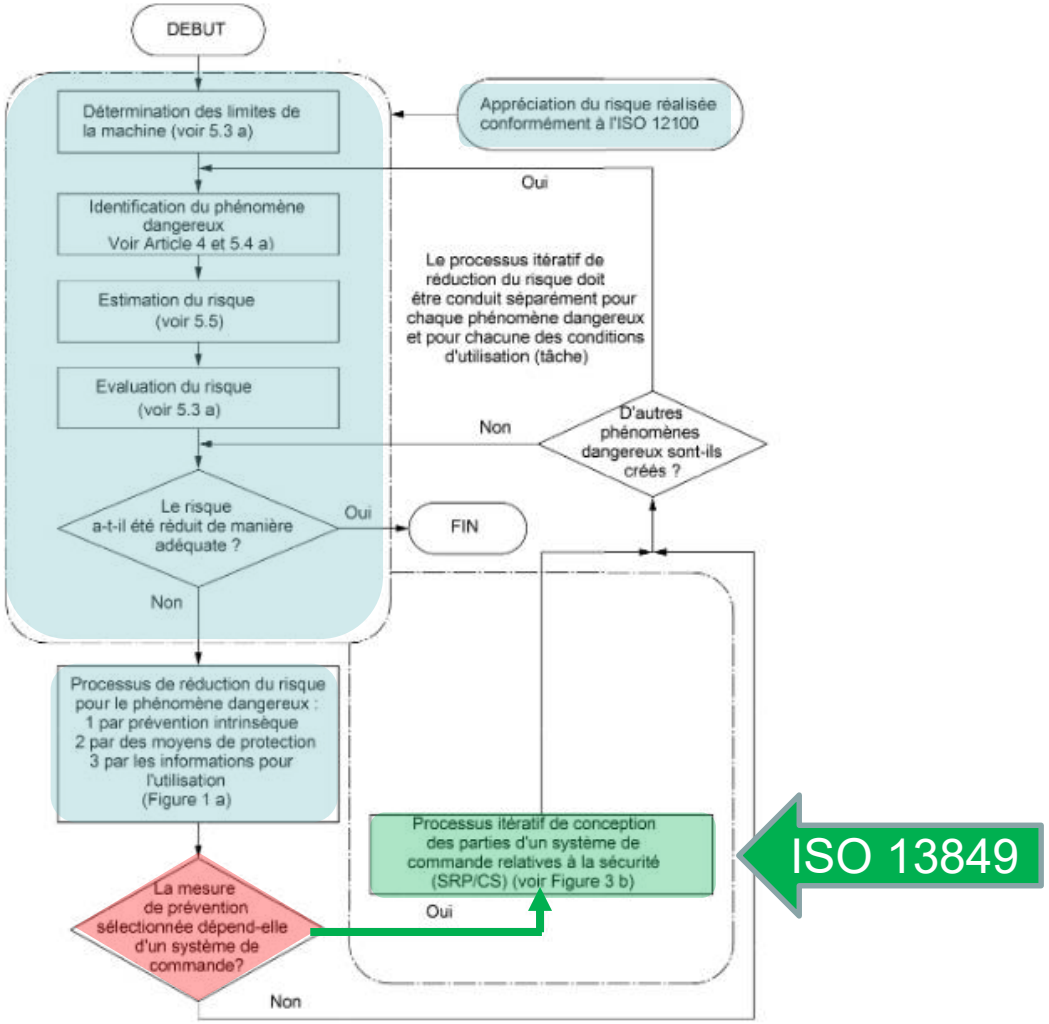


# ISO 12100 – Analyse de risque

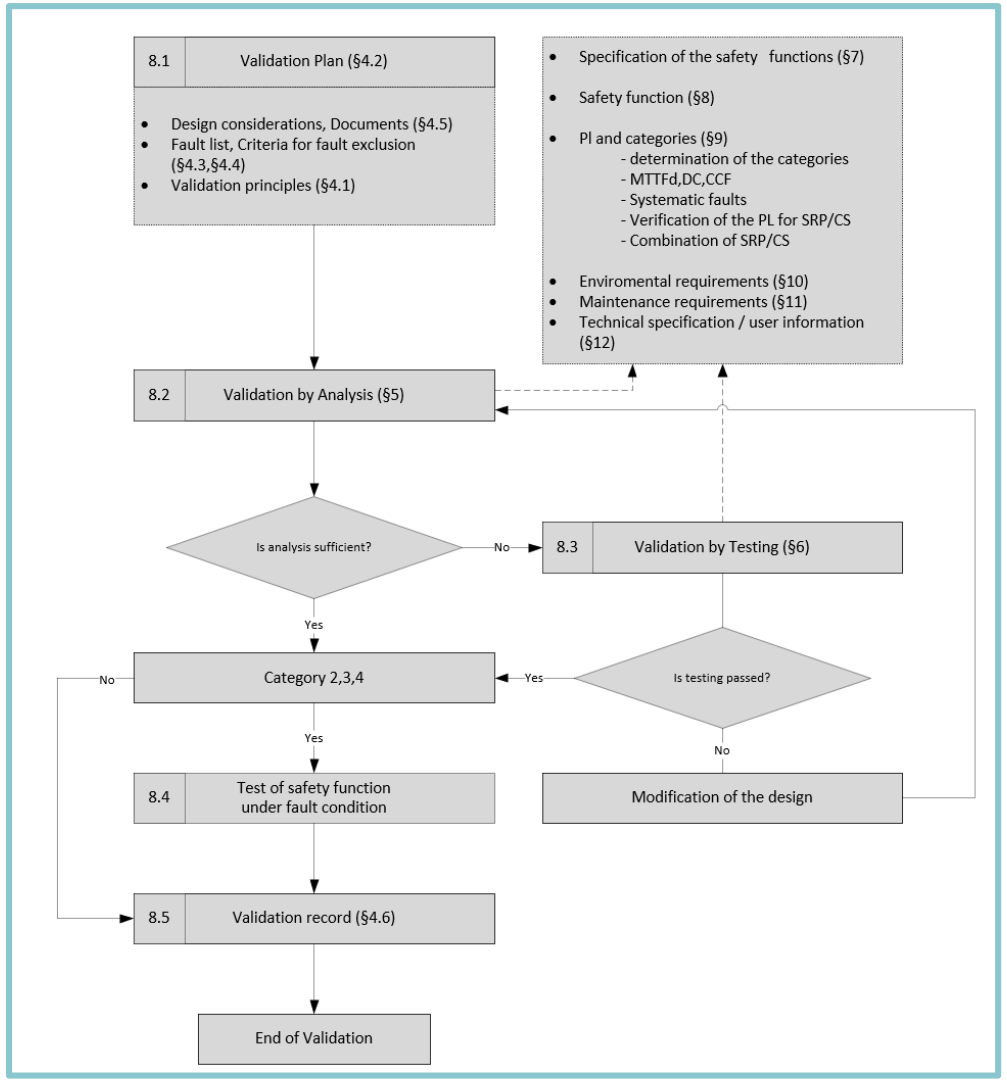


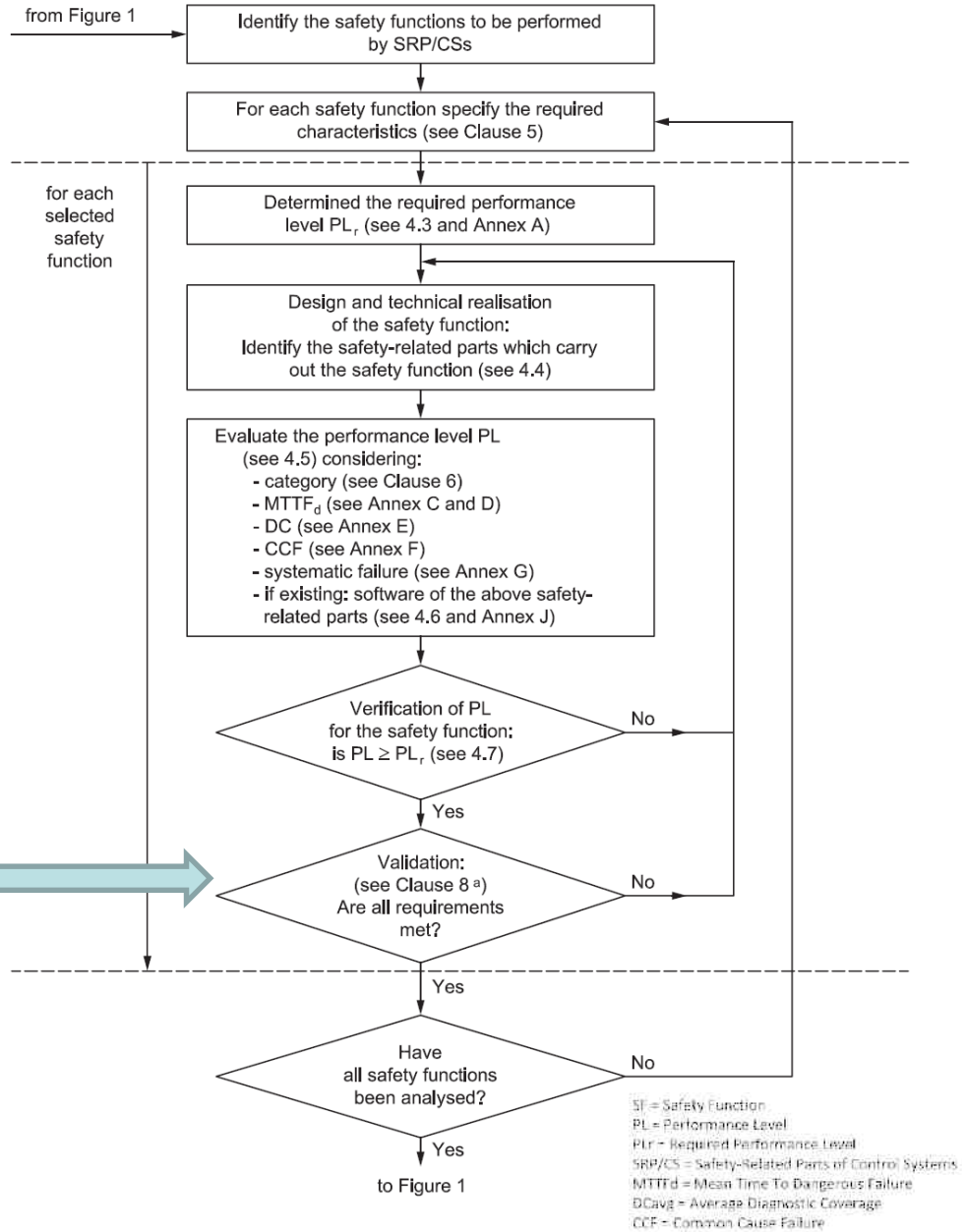

Sources: ISO 13849-1

# ISO 12100 – Analyse de risque → ISO 13849



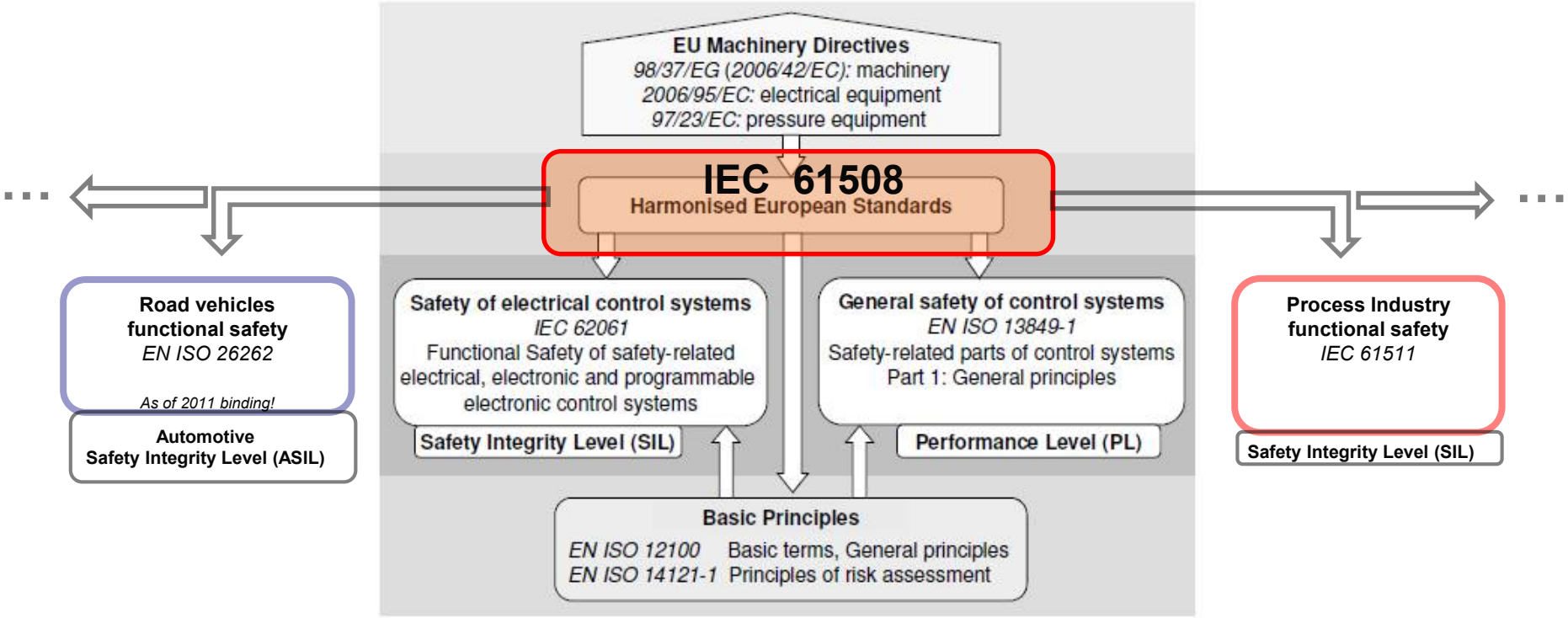
# ISO 13849 – Design itératif




Sources: ISO 13849-1

# IEC 61508 – La sécurité fonctionnelle





Sources: Berns Engineers

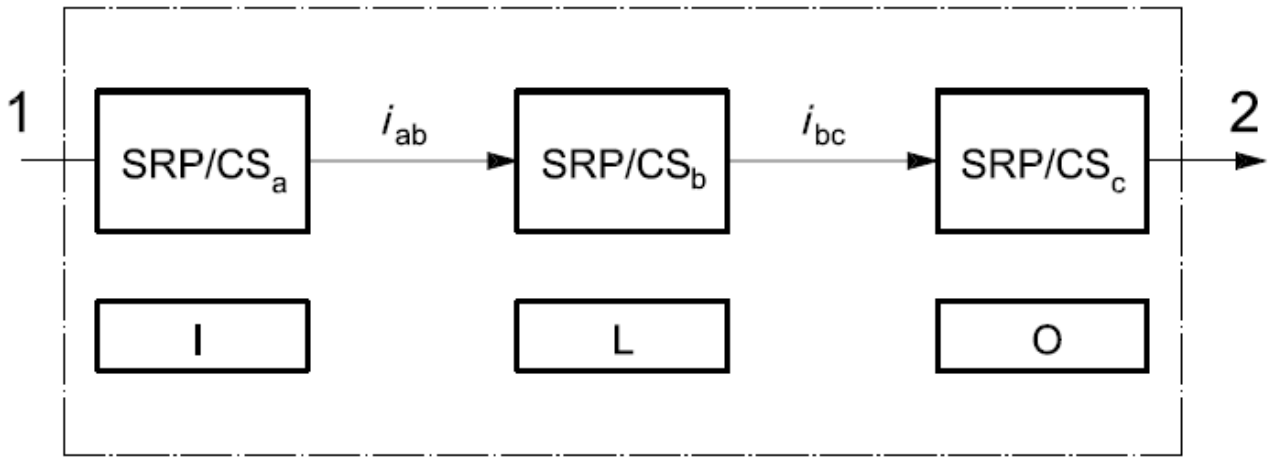
# Le niveau de sécurité selon le domaine d'application

| Industry | Domain Specific "Safety Integrity Levels" | | | | |
|---|---|---|---|---|---|
| Aerospace<br>RTCA DO254 (HW) / DO 178C (SW) | DAL E | DAL D | DAL C | DAL B | DAL A |
| General Functional Safety<br>IEC 61508 | (SIL 0) | SIL 1 | SIL 2 | SIL 3 | SIL 4 |
| Railway<br>CENELEC EN 50126 / 50128 / 50129 | (SIL 0) | SIL 1 | SIL 2 | SIL 3 | SIL 4 |
| Automotive<br>ISO EN 26262 | QM | ASIL A | ASIL B/C | ASIL D | - |
| Machinery<br>ISO 13849 | PL A | PL B/C | PL D | PL E | - |

Sources: Berns Engineers

# Qu’est-ce qu’un SRP-CS?

**safety–related part of a control system**
**SRP/CS**
part of a control system that responds to safety-related input signals and generates safety-related output signals



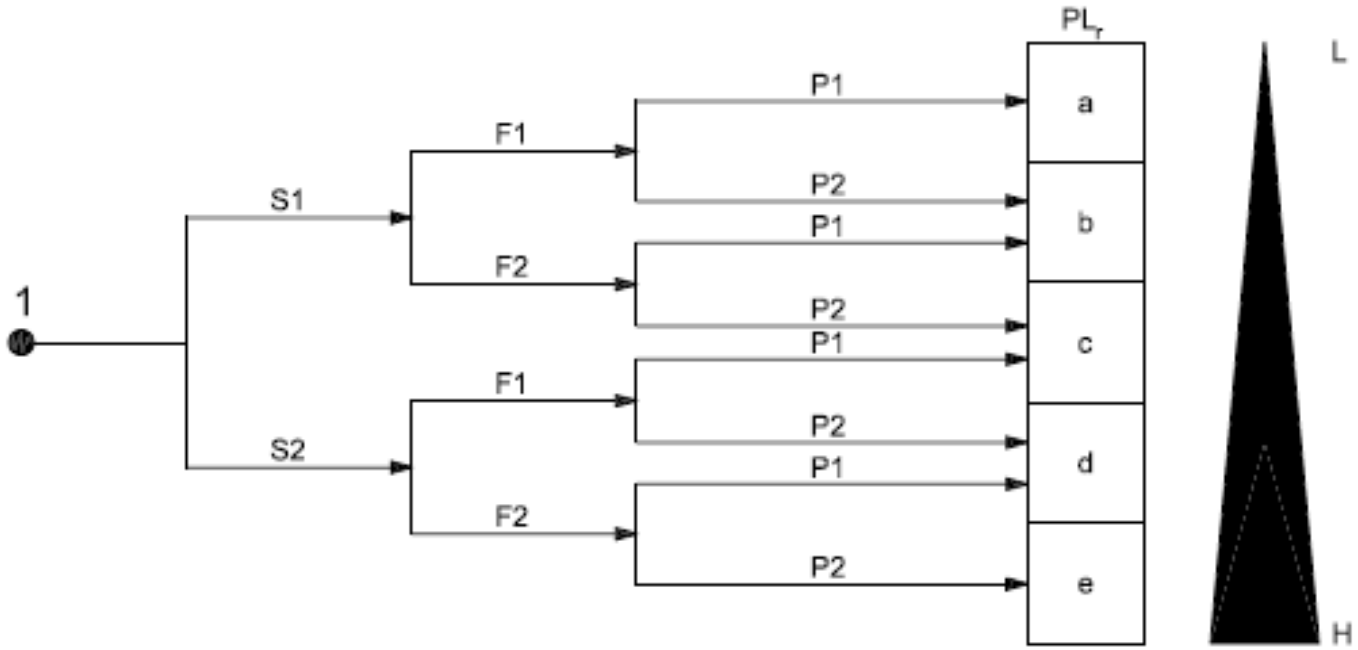

**Key**

I input (e.g. limit switch, sensor, AOPD)
L logic
O output (e.g. valve, contactor, current converter)
1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)
2 machine actuator (e.g. motor, cylinder)


Sources: ISO 13849-1

# La définition du niveau de performance requis (PLr)

Toutes les fonctions de sécurité (par exemple la prévention d'un démarrage intempestif) réalisées par les SRP-CS doivent être identifiées et leurs caractéristiques, définies, y compris le niveau de performance requis $PL_r$. Pour définir ce dernier paramètre, nous pouvons utiliser l'analyse par graphe des risques :





Sources: ISO 13849-1

# Le graphe des risques – Paramètres

Tout comme pour certaines méthodes d'évaluation du risque selon la norme ISO 12100, nous devons estimer le risque en prenant en compte 3 facteurs:

La sévérité – S:

- S1 – Blessure sans complications
- S2 – Blessures avec complications (p.ex. amputation, paralysie, mort…)

La fréquence d'exposition au danger – F:

- F1 – Il est rare qu'une personne soit exposée au danger
- F2 – Une personne est fréquemment ou continuellement exposée au danger

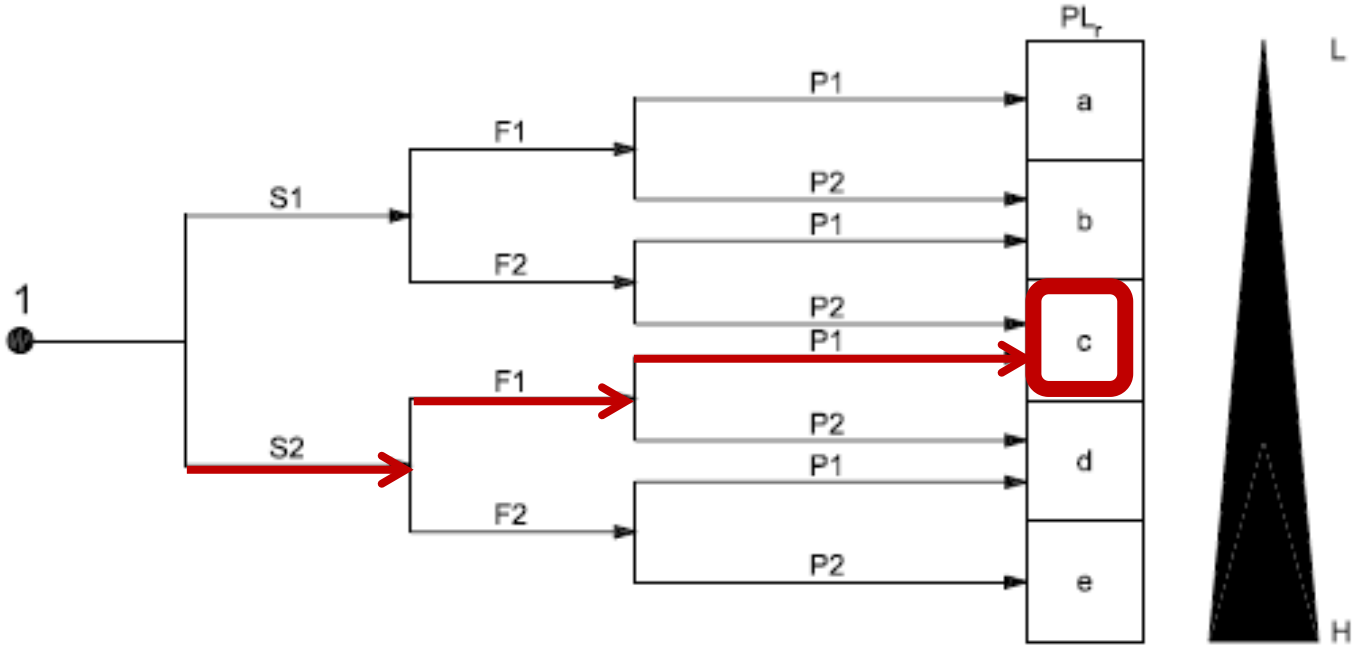
La possibilité d'éviter le danger – P:

- P1 – Il y a une chance réaliste que le danger soit évité ou que sont impact soit limité
- P2 – La personne en danger ne pourra pas éviter le danger



Sources: ISO 13849-1

# Niveau de performance requis exemple (PLr)




**Key**

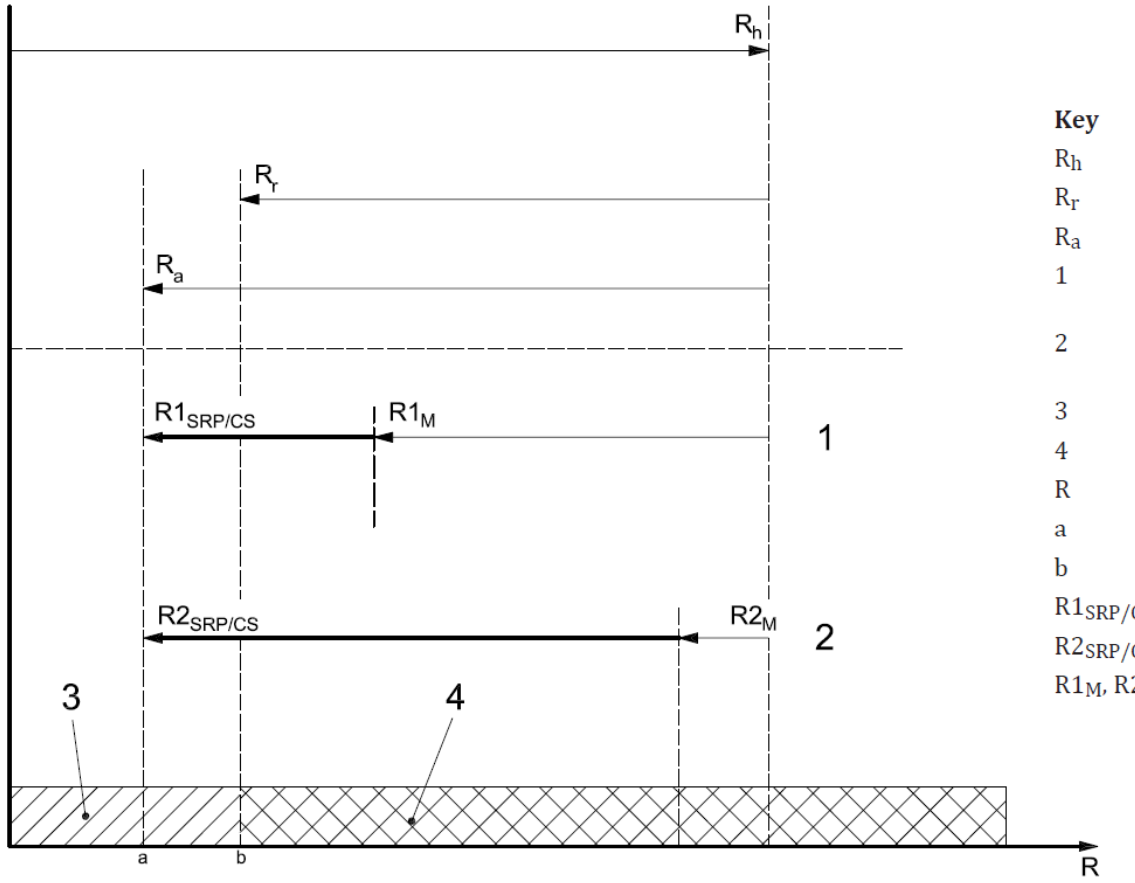
| | |
|---|---|
| 1 | starting point for evaluation of safety function's contribution to risk reduction |
| L | low contribution to risk reduction |
| H | high contribution to risk reduction |
| $PL_r$ | required performance level |

**Risk parameters:**

| | |
|---|---|
| S | severity of injury |
| S1 | slight (normally reversible injury) |
| S2 | serious (normally irreversible injury or death) |
| F | frequency and/or exposure to hazard |
| F1 | seldom-to-less-often and/or exposure time is short |
| F2 | frequent-to-continuous and/or exposure time is long |
| P | possibility of avoiding hazard or limiting harm |
| P1 | possible under specific conditions |
| P2 | scarcely possible |


Sources: ISO 13849-1

# La réduction du risque

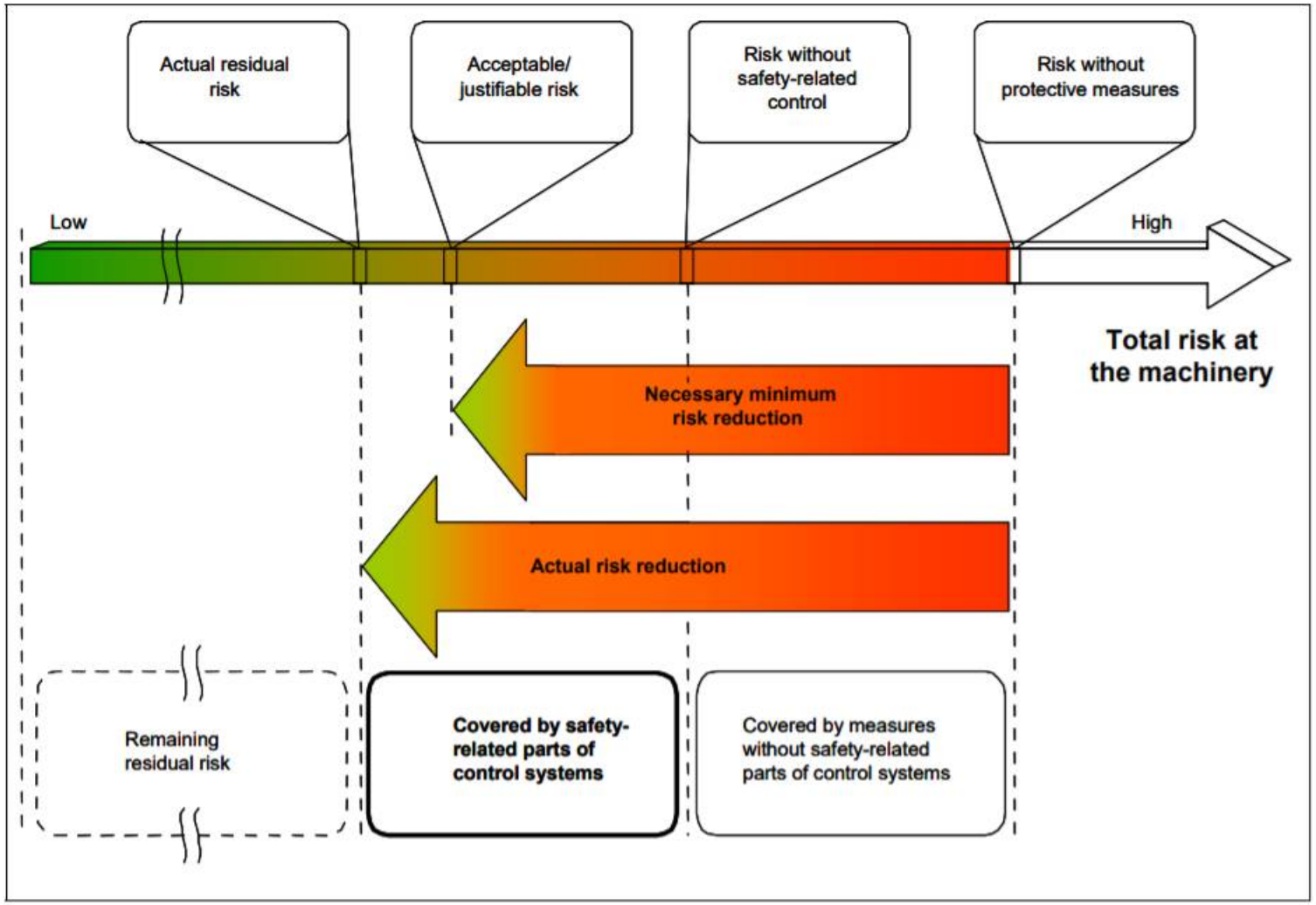



**Key**

| | |
|---|---|
| $R_h$ | for a specific hazardous situation, the risk before protective measures are applied |
| $R_r$ | risk reduction required from protective measures |
| $R_a$ | actual risk reduction achieved with protective measures |
| 1 | Solution 1 — important part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures), small part of risk reduction due to SRP/CS |
| 2 | solution 2 — important part of risk reduction due to the SRP/CS (e.g. light curtain), small part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures) |
| 3 | adequately reduced risk |
| 4 | inadequately reduced risk |
| R | risk |
| a | residual risk obtained by solutions 1 and 2 |
| b | adequately reduced risk |
| $R1_{SRP/CS}$<br>$R2_{SRP/CS}$ | risk reduction from the safety function carried out by the SRP/CS |
| $R1_M$, $R2_M$ | risk reduction from protective measures other than SRP/CS (e.g. mechanical measures) |


Sources: ISO 13849-1

# La réduction du risque



# Les types de défaillances

Lors du développement d'un système relatif à la sécurité, nous différencions deux types de défaillances possibles qui devront être couvertes:

**Les défaillances aléatoires:**

- Défaillance ne pouvant être prévue, elle est souvent due à une ou plusieurs dégradations dans le matériel. Ces défaillances peuvent être dues aux conditions dans lesquelles la machine évolue (humidité, température, vibrations…)

**Les défaillance systématiques:**

- Défaillances souvent liées à une erreur humaine ou une erreur de design
  - Mauvaise formulation des spécifications
  - Erreur de conception de la partie matérielle
  - Erreur de production
  - Erreur d'installation de la machine
  - Erreur de conception ou d'intégration du logiciel



Sources: ISO 13849-1

# Prévenir les défaillance systématiques

Quelques exemples de mesures qui peuvent être mises en place pour détecter et corriger certaines erreurs systématiques se trouvent dans l'annexe G de l'ISO 13949-1.

## Annex G
(informative)

## Systematic failure

### G.1 General

ISO 13849-2 gives a comprehensive list of measures against systematic failure which should be applied, such as basic and well-tried safety principles.

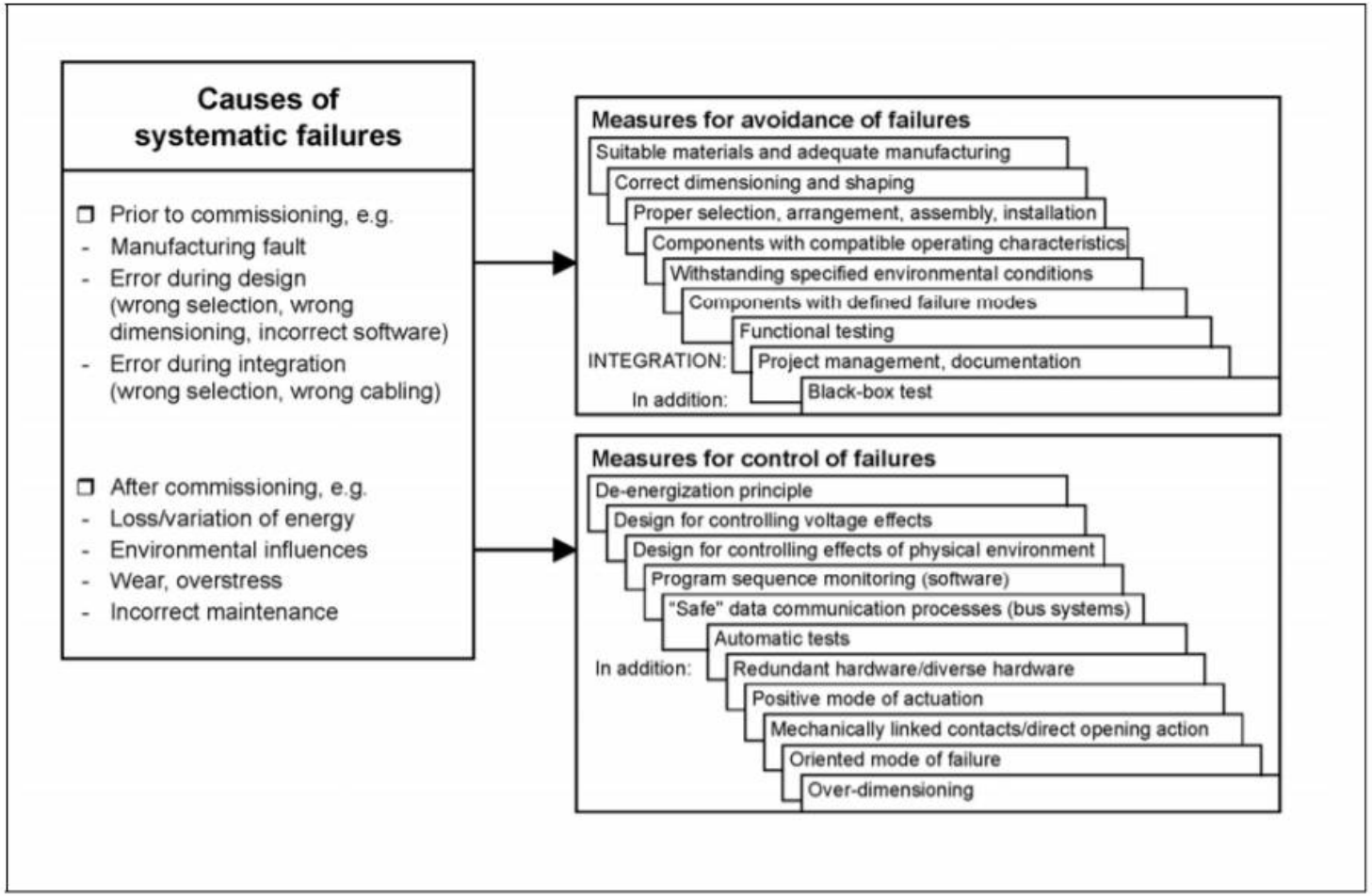
### G.2 Measures for the control of systematic failures

The following measures should be applied.



Sources: ISO 13849-1

# Prévenir les défaillance systématiques



# Prévenir les défaillance aléatoires

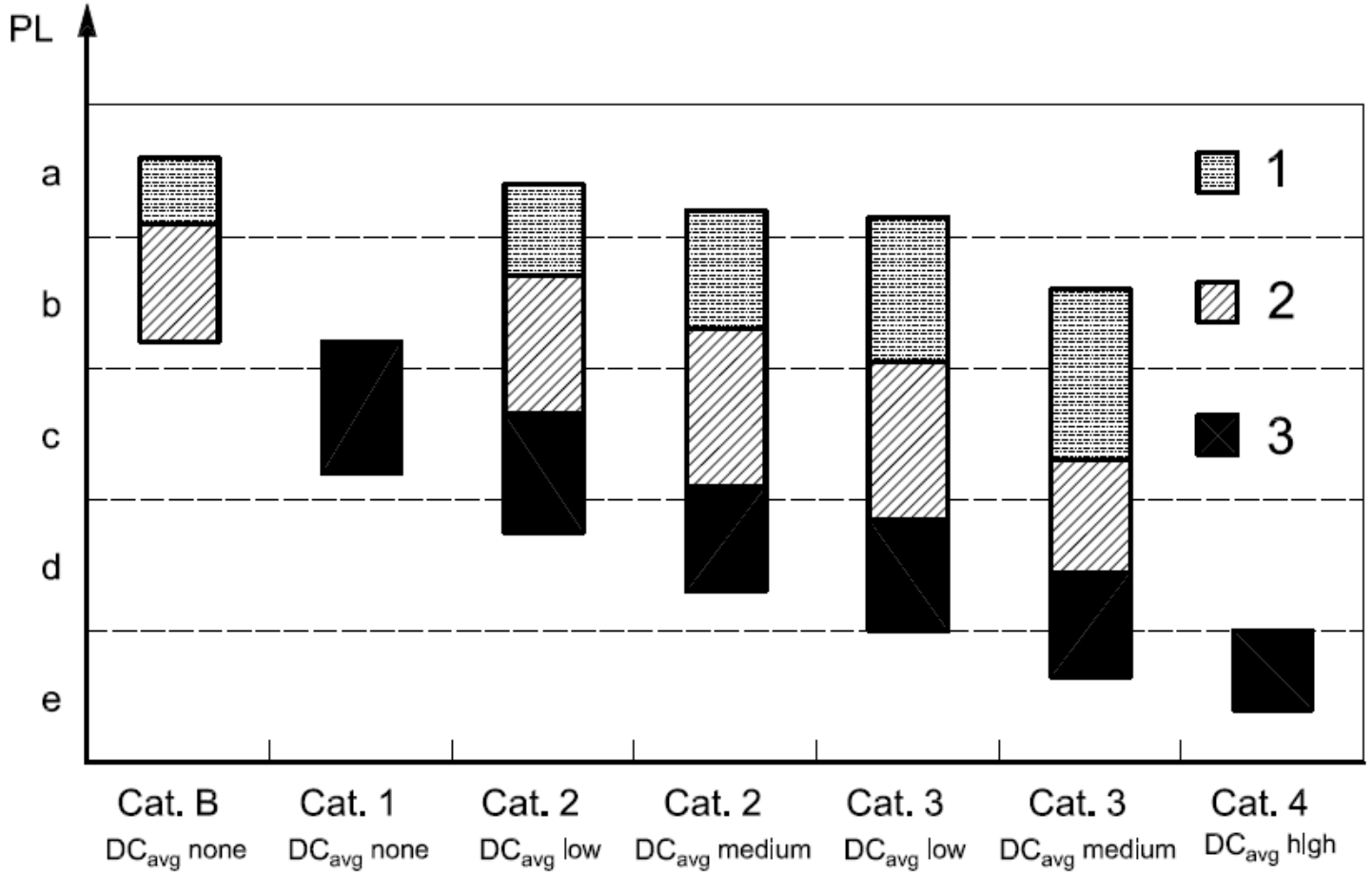
Afin de prévenir les défaillance aléatoires, il est nécessaire de calculer le taux défaillance de notre système grâce à l'indice PFH (Probabilité de défaillance par heure)

| PL | Average probability of dangerous failure per hour ($PFH_D$) 1/h |
|---|---|
| a | $\geq 10^{-5}$ to $< 10^{-4}$ |
| b | $\geq 3 \times 10^{-6}$ to $< 10^{-5}$ |
| c | $\geq 10^{-6}$ to $< 3 \times 10^{-6}$ |
| d | $\geq 10^{-7}$ to $< 10^{-6}$ |
| e | $\geq 10^{-8}$ to $< 10^{-7}$ |

Sources: ISO 13849-1

# Les paramètres requis valider le PL atteint

Ce graphique propose, de manière simplifiée, l'évaluation du niveau PL atteint par un système:




**Key**

| | |
|---|---|
| PL | performance level |
| 1 | $MTTF_D$ of each channel = low |
| 2 | $MTTF_D$ of each channel = medium |
| 3 | $MTTF_D$ of each channel = high |


Sources: ISO 13849-1

# Représentation numérique

**Table K.1 — Numerical representation of Figure 5**

| MTTF$_D$ for each channel years | Average probability of a dangerous failure per hour, PFH$_D$ (1/h) and corresponding performance level (PL) | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Cat. B | PL | Cat. 1 | PL | Cat. 2 | PL | Cat. 2 | PL | Cat. 3 | PL | Cat. 3 | PL | Cat. 4 | PL |
| | DC$_{avg}$ = none | | DC$_{avg}$ = none | | DC$_{avg}$ = low | | DC$_{avg}$ = medium | | DC$_{avg}$ = low | | DC$_{avg}$ = medium | | DC$_{avg}$ = high | |
| 3 | $3{,}80 \times 10^{-5}$ | a | | | $2{,}58 \times 10^{-5}$ | a | $1{,}99 \times 10^{-5}$ | a | $1{,}26 \times 10^{-5}$ | a | $6{,}09 \times 10^{-6}$ | b | | |
| 3,3 | $3{,}46 \times 10^{-5}$ | a | | | $2{,}33 \times 10^{-5}$ | a | $1{,}79 \times 10^{-5}$ | a | $1{,}13 \times 10^{-5}$ | a | $5{,}41 \times 10^{-6}$ | b | | |
| 3,6 | $3{,}17 \times 10^{-5}$ | a | | | $2{,}13 \times 10^{-5}$ | a | $1{,}62 \times 10^{-5}$ | a | $1{,}03 \times 10^{-5}$ | a | $4{,}86 \times 10^{-6}$ | b | | |
| 3,9 | $2{,}93 \times 10^{-5}$ | a | | | $1{,}95 \times 10^{-5}$ | a | $1{,}48 \times 10^{-5}$ | a | $9{,}37 \times 10^{-6}$ | b | $4{,}40 \times 10^{-6}$ | b | | |
| 4,3 | $2{,}65 \times 10^{-5}$ | a | | | $1{,}76 \times 10^{-5}$ | a | $1{,}33 \times 10^{-5}$ | a | $8{,}39 \times 10^{-6}$ | b | $3{,}89 \times 10^{-6}$ | b | | |
| 4,7 | $2{,}43 \times 10^{-5}$ | a | | | $1{,}60 \times 10^{-5}$ | a | $1{,}20 \times 10^{-5}$ | a | $7{,}58 \times 10^{-6}$ | b | $3{,}48 \times 10^{-6}$ | b | | |
| 5,1 | $2{,}24 \times 10^{-5}$ | a | | | $1{,}47 \times 10^{-5}$ | a | $1{,}10 \times 10^{-5}$ | a | $6{,}91 \times 10^{-6}$ | b | $3{,}15 \times 10^{-6}$ | b | | |
| 5,6 | $2{,}04 \times 10^{-5}$ | a | | | $1{,}33 \times 10^{-5}$ | a | $9{,}87 \times 10^{-6}$ | b | $6{,}21 \times 10^{-6}$ | b | $2{,}80 \times 10^{-6}$ | c | | |
| 6,2 | $1{,}84 \times 10^{-5}$ | a | | | $1{,}19 \times 10^{-5}$ | a | $8{,}80 \times 10^{-6}$ | b | $5{,}53 \times 10^{-6}$ | b | $2{,}47 \times 10^{-6}$ | c | | |
| 6,8 | $1{,}68 \times 10^{-5}$ | a | | | $1{,}08 \times 10^{-5}$ | a | $7{,}93 \times 10^{-6}$ | b | $4{,}98 \times 10^{-6}$ | b | $2{,}20 \times 10^{-6}$ | c | | |
| 7,5 | $1{,}52 \times 10^{-5}$ | a | | | $9{,}75 \times 10^{-6}$ | b | $7{,}10 \times 10^{-6}$ | b | $4{,}45 \times 10^{-6}$ | b | $1{,}95 \times 10^{-6}$ | c | | |
| 8,2 | $1{,}39 \times 10^{-5}$ | a | | | $8{,}87 \times 10^{-6}$ | b | $6{,}43 \times 10^{-6}$ | b | $4{,}02 \times 10^{-6}$ | b | $1{,}74 \times 10^{-6}$ | c | | |
| 9,1 | $1{,}25 \times 10^{-5}$ | a | | | $7{,}94 \times 10^{-6}$ | b | $5{,}71 \times 10^{-6}$ | b | $3{,}57 \times 10^{-6}$ | b | $1{,}53 \times 10^{-6}$ | c | | |
| 10 | $1{,}14 \times 10^{-5}$ | a | | | $7{,}18 \times 10^{-6}$ | b | $5{,}14 \times 10^{-6}$ | b | $3{,}21 \times 10^{-6}$ | b | $1{,}36 \times 10^{-6}$ | c | | |
| 11 | $1{,}04 \times 10^{-5}$ | a | | | $6{,}44 \times 10^{-6}$ | b | $4{,}53 \times 10^{-6}$ | b | $2{,}81 \times 10^{-6}$ | c | $1{,}18 \times 10^{-6}$ | c | | |
| 12 | $9{,}51 \times 10^{-6}$ | b | | | $5{,}84 \times 10^{-6}$ | b | $4{,}04 \times 10^{-6}$ | b | $2{,}49 \times 10^{-6}$ | c | $1{,}04 \times 10^{-6}$ | c | | |
| 13 | $8{,}78 \times 10^{-6}$ | b | | | $5{,}33 \times 10^{-6}$ | b | $3{,}64 \times 10^{-6}$ | b | $2{,}23 \times 10^{-6}$ | c | $9{,}21 \times 10^{-7}$ | d | | |
| 15 | $7{,}61 \times 10^{-6}$ | b | | | $4{,}53 \times 10^{-6}$ | b | $3{,}01 \times 10^{-6}$ | b | $1{,}82 \times 10^{-6}$ | c | $7{,}44 \times 10^{-7}$ | d | | |
| 16 | $7{,}13 \times 10^{-6}$ | b | | | $4{,}21 \times 10^{-6}$ | b | $2{,}77 \times 10^{-6}$ | c | $1{,}67 \times 10^{-6}$ | c | $6{,}76 \times 10^{-7}$ | d | | |
| 18 | $6{,}34 \times 10^{-6}$ | b | | | $3{,}68 \times 10^{-6}$ | b | $2{,}37 \times 10^{-6}$ | c | $1{,}41 \times 10^{-6}$ | c | $5{,}67 \times 10^{-7}$ | d | | |
| 20 | $5{,}71 \times 10^{-6}$ | b | | | $3{,}26 \times 10^{-6}$ | b | $2{,}06 \times 10^{-6}$ | c | $1{,}22 \times 10^{-6}$ | c | $4{,}85 \times 10^{-7}$ | d | | |
| 22 | $5{,}19 \times 10^{-6}$ | b | | | $2{,}93 \times 10^{-6}$ | c | $1{,}82 \times 10^{-6}$ | c | $1{,}07 \times 10^{-6}$ | c | $4{,}21 \times 10^{-7}$ | d | | |

Licensed to ROCHE Center Auvergne Rhône Alpes (Marcy l'Etoile) (rochecarlos@gmail.com)

# Les paramètres requis valider le PL atteint (2)

Ce graphique peut être simplifié dans ce tableau de correspondance:

| Category | B | 1 | 2 | 2 | 3 | 3 | 4 |
|---|---|---|---|---|---|---|---|
| $DC_{avg}$ | none | none | low | medium | low | medium | high |
| $MTTF_D$ of each channel | | | | | | | |
| Low | a | Not cov-ered | a | b | b | c | Not cov-ered |
| Medium | b | Not cov-ered | b | c | c | d | Not cov-ered |
| High | Not cov-ered | c | c | d | d | d | e |


Sources: ISO 13849-1

# Les paramètres requis valider le PL atteint (3)

Les paramètres requis sont donc:

- La catégorie d'architecture utilisé (Category)
- La couverture de diagnostique ($DC_{avg}$)
- Le $MTTF_D$ de chaque canal

Vient s'additionner à ça deux facteurs indépendants qui sont:

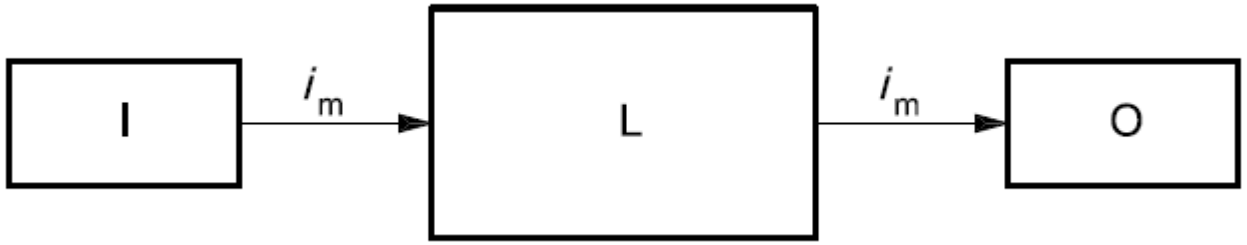
- Le développement selon le cycle de vie de la norme (défaillance systématiques)
- Les défaillances de causes communes (β)



Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie B

| Category | Summary of requirements | System behaviour | Principle used to achieve safety | $MTTF_D$ of each channel | $DC_{avg}$ | CCF |
|---|---|---|---|---|---|---|
| B (see 6.2.3) | SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used. | The occurrence of a fault can lead to the loss of the safety function. | Mainly characterized by selection of components | Low to medium | None | Not relevant |




**Key**

$i_m$ interconnecting means

I input device, e.g. sensor

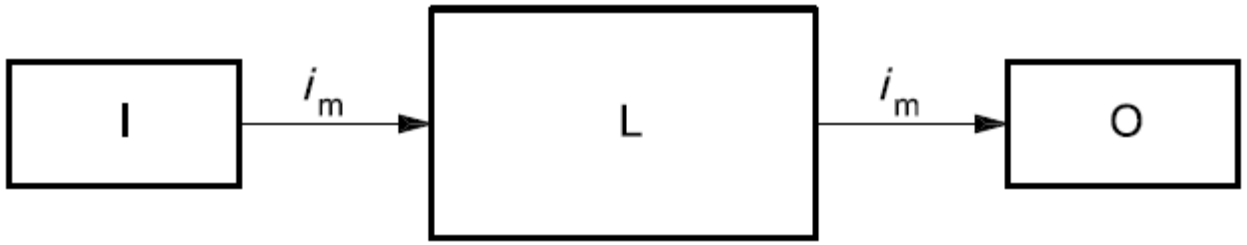
L logic

O output device, e.g. main contactor


Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 1

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 (see 6.2.4) | Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used. | The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B. | Mainly characterized by selection of components | High | None | Not relevant |




**Key**

$i_m$ interconnecting means

I input device, e.g. sensor

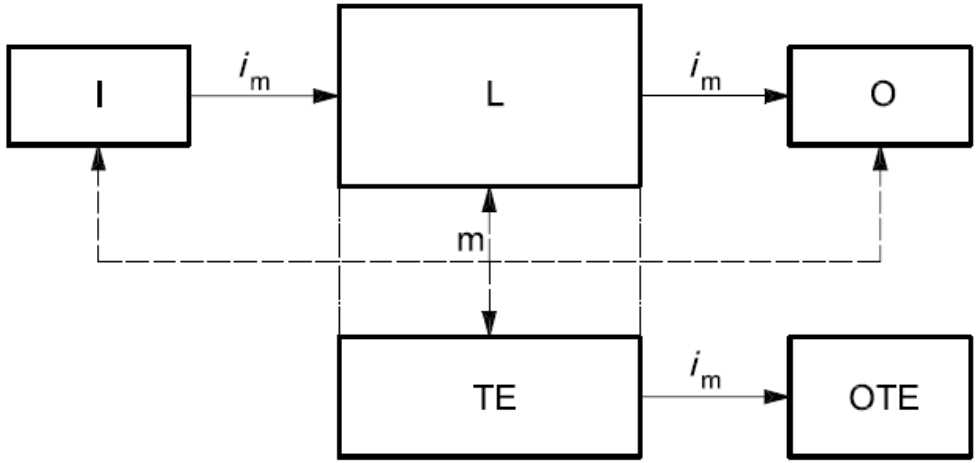
L logic

O output device, e.g. main contactor


Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 2

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 (see 6.2.5) | Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system (see 4.5.4). | The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check. | Mainly characterized by structure | Low to high | Low to medium | See Annex F |




**Key**

| | |
|---|---|
| $i_m$ | interconnecting means |
| I | input device, e.g. sensor |
| L | logic |
| m | monitoring |
| O | output device, e.g. main contactor |
| TE | test equipment |
| OTE | output of TE |

Dashed lines represent reasonably practicable fault detection.


Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 2, hypothèses

Des dispositions additionnelles sont applicables afin d'atteindre les objectifs de la catégorie 2:

- L'intervalle de contrôle suppose un taux de test supérieur à 100x le taux de sollicitation de la fonction

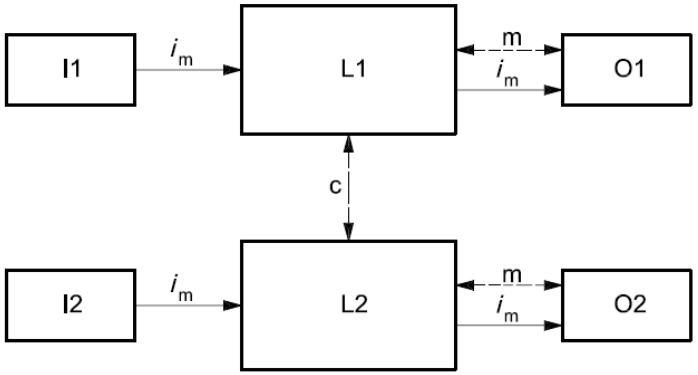
- En alternative, un test peut conduire une réaction immédiate lors de la sollicitation de la fonction entraînant la machine dans une condition non-dangereuse (toujours actif)
- Dans ce cas, la sortie OTE doit générer un état de sécurité. Ceci est également requis lorsque la Cat. 2 est utilisée pour atteindre un $PL_r$ D.
- Pour un $PL_r$ inférieur ou égal à C, il est suffisant que la sortie OTE génère un signal d'alerte



Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 3

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 (see 6.2.6) | Requirements of B and the use of well-tried safety principles shall apply.<br>Safety-related parts shall be designed, so that<br>— a single fault in any of these parts does not lead to the loss of the safety function, and<br>— whenever reasonably practicable, the single fault is detected. | When a single fault occurs, the safety function is always performed.<br>Some, but not all, faults will be detected.<br>Accumulation of undetected faults can lead to the loss of the safety function. | Mainly characterized by structure | Low to high | Low to medium | See Annex F |




**Key**

| | |
|---|---|
| $i_m$ | interconnecting means |
| c | cross monitoring |
| I1, I2 | input device, e.g. sensor |
| L1, L2 | logic |
| m | monitoring |
| O1, $O_2$ | output device, e.g. main contactor |

Dashed lines represent reasonably practicable fault detection.

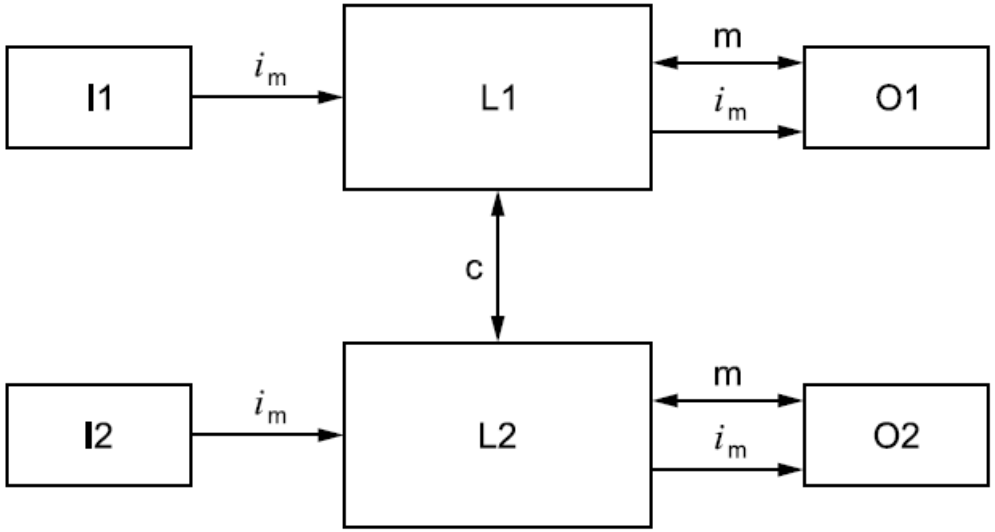

Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 4

| | | | | | | |
|---|---|---|---|---|---|---|
| 4<br>(see 6.2.7) | Requirements of B and the use of well-tried safety principles shall apply.<br>Safety-related parts shall be designed, so that<br>— a single fault in any of these parts does not lead to a loss of the safety function, and<br>— the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function. | When a single fault occurs the safety function is always performed.<br>Detection of accumulated faults reduces the probability of the loss of the safety function (high DC).<br>The faults will be detected in time to prevent the loss of the safety function. | Mainly characterized by structure | High | High including accumulation of faults | See Annex F |


Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 4 (2)




**Key**

| | |
|---|---|
| $i_m$ | interconnecting means |
| c | cross monitoring |
| I1, I2 | input device, e.g. sensor |
| L1, L2 | logic |
| m | monitoring |
| O1, $O_2$ | output device, e.g. main contactor |

Solid lines represent diagnostic coverage higher than in the Cat.3 architecture


Sources: ISO 13849-1

# Le paramètre DC

| DC | |
|---|---|
| **Indice** | **Gamme** |
| Nulle | DC < 60 % |
| Faible | 60 % ≤ DC < 90 % |
| Moyenne | 90 % ≤ DC < 99 % |
| Élevée | 99 % ≤ DC |

NOTE 1 Pour les SRP/CS constituées de plusieurs parties, la présente partie de l'ISO 13849 utilise une valeur moyenne $DC_{avg}$, voir Figure 5, Article 6 et E.2.

NOTE Le choix d'une gamme de DC est basée sur les valeurs clés de 60 %, 90 % et 99 % qu'on peut déjà trouver dans d'autres normes (par exemple la série IEC 61508) traitant des tests de couverture de diagnostic. Des recherches montrent que (1-DC) plutôt que DC lui-même est une mesure caractéristique pour déterminer l'efficacité du test. (1-DC) pour les valeurs clés de 60 %, 90 % et 99 % forme une sorte d'échelle logarithmique en cohérence avec l'échelle logarithmique du PL. Une valeur de DC de moins de 60 % a une faible incidence sur la fiabilité du système soumis à essai et est de ce fait qualifiée de «nulle». Une valeur de DC supérieure à 99 % pour des systèmes complexes est très difficile à obtenir. Pour des raisons pratiques, le nombre de gammes a été restreint à quatre. Les valeurs limites données dans ce tableau sont présumées être précises à 5 %.


Sources: ISO 13849-1

# Le paramètre DC – Calcul

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}}$$

Le DC représente le ratio de fautes dangereuses détectées par rapport à la somme de la totalité des fautes dangereuses du système.

Des exemples de DC se trouvent dans l'annexe E de l'ISO 13849-1


Sources: ISO 13849-1

# DC - Annexe E

| 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. | 99 % |
| Surveillance croisée des entrées sans test dynamique | 0 % à 99 %, 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 % |
| Surveillance croisée des entrées et des résultats intermédiaires internes à la logique (L) et moniteur de logiciel temporel et logique du programme et détection de défauts statiques et des courts-circuits (pour I/O multiples) | 99 % |
| Surveillance indirecte (par exemple par commutateur de pression, surveillance de position électrique des actionneurs) | 90 % à 99 %, dépendant de l'application |
| Surveillance directe (par exemple surveillance de position électrique des distributeurs de commande, surveillance des dispositifs électro-mécaniques par éléments de contact mécaniquement liés) | 99 % |
| Détection des défauts par le procédé | 0 % à 99 %, dépendant de l'application; cette mesure toute seule n'est pas suffisante pour un niveau requis de performance «e» ! |
| Surveillance de quelques caractéristiques du capteur (temps de réponse, gamme des signaux analogiques, par exemple résistance électrique, capacité) | 60 % |
| **Logique** | |
| Surveillance indirecte (par exemple surveillance par commutateur de pression, surveillance de position électrique des actionneurs) | 90 % à 99 %, dépendant de l'application |
| Surveillance directe (par exemple surveillance de position électrique des distributeurs de commande, surveillance des dispositifs électro-mécaniques par éléments de contact mécaniquement liés) | 99 % |
| Surveillance temporelle simple de la logique (par exemple: temporisateur comme chien de garde, lorsque les points de déclenchement se situent dans le programme de la logique) | 60 % |
| Surveillance temporelle et logique de la logique par chien de garde, lorsque l'équipement d'essai réalise des contrôles de vraisemblance du comportement de la logique | 90 % |
| Auto-tests à la mise en marche pour détecter les défauts latents dans | 90 % (dépendant de la technique d'essai) |

# Le paramètre $MTTF_D$

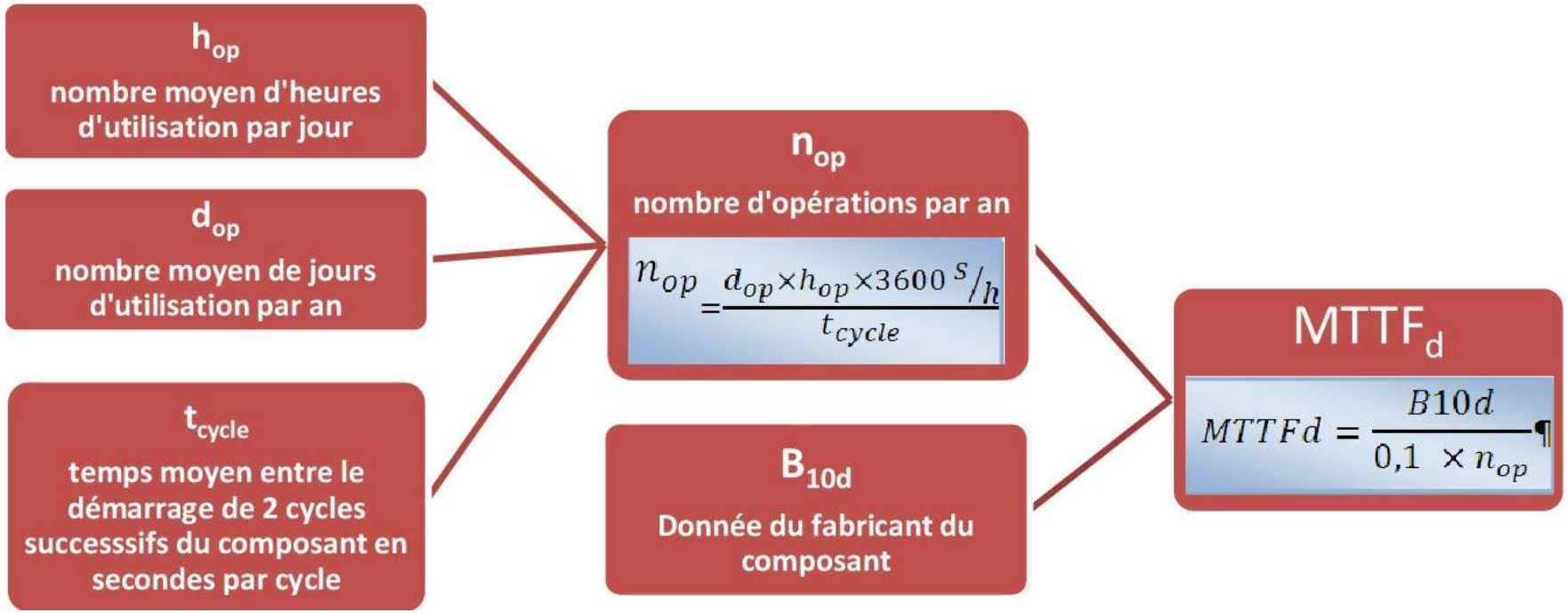
| $MTTF_D$ | |
|---|---|
| **Indice pour chaque canal** | **Gamme pour chaque canal** |
| Faible | 3 ans $\leqslant MTTF_D <$ 10 ans |
| Moyen | 10 ans $\leqslant MTTF_D <$ 30 ans |
| Élevé | 30 ans $\leqslant MTTF_D \leqslant$ 100 ans |

NOTE 1 Le choix d'une gamme de $MTTF_D$ pour chaque canal est basé sur les taux de défaillance trouvés dans l'état de l'art du domaine formant une échelle logarithmique cohérente avec l'échelle logarithmique des PL. Une valeur de $MTTF_D$ pour chaque canal inférieure à 3 années n'est pas supposée être trouvée pour des SRP/CS réels dans la mesure où cela signifierait qu'après une année, 30 % de l'ensemble des systèmes du marché seraient défaillants et susceptibles d'être remplacés. Une valeur de $MTTF_D$ pour chaque canal supérieure à 100 années n'est pas acceptable dans la mesure où une SRP/CS traitant d'un risque élevé ne devrait pas dépendre uniquement de la fiabilité des composants. Afin de renforcer les SRP/CS contre les défaillances systématiques et aléatoires, il convient que des moyens additionnels tels que redondance et essais soient requis. Pour des raisons pratiques, le nombre de gammes a été restreint à trois. La limitation du $MTTF_D$ pour chaque canal à une valeur maximale de 100 années se réfère aux SRP/CS à canal unique qui réalisent la fonction de sécurité. Des valeurs plus élevées de $MTTF_D$ peuvent être utilisées pour des composants simples (voir Tableau D.1).

NOTE 2 Les valeurs limites données dans ce tableau sont présumées être précises à 5 %.


Sources: ISO 13849-1

# Le paramètre $MTTF_D$ – Calcul




Lorsque le fabricant n'est pas capable de fournir les donnée afin de calculer le MTTF, alors il est possible d'utiliser des bases de données de fiabilité, certains exemples sont aussi données dans l'annexe C de l'ISO 13849-1. Si le composant n'est vraiment pas disponible, alors, 10 ans est parfois utilisé par défaut.

# Le paramètre β – Défaillances de cause commune

Pour certaines catégories d'architecture, un indice β supérieur à 65 est demandé. Celui-ci est calculé en additionnant les valeurs de la table ci-dessous lorsque les mesures sont respectées:

| No. | Measure against CCF | Score |
|---|---|---|
| 1 | **Separation/ Segregation** | |
| | Physical separation between signal paths, for example:<br>— separation in wiring/piping;<br>— detection of short circuits and open circuits in cables by dynamic test;<br>— separate shielding for the signal path of each channel;<br>— sufficient clearances and creepage distances on printed-circuit boards. | **15** |
| 2 | **Diversity** | |
| | Different technologies/design or physical principles are used, for example:<br>— first channel electronic or programmable electronic and second channel electromechanical hardwired,<br>— different initiation of safety function for each channel (e.g. position, pressure, temperature),<br>and/or<br>digital and analog measurement of variables (e.g. distance, pressure or temperature)<br>and/or<br>Components of different manufactures. | **20** |

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.


Sources: ISO 13849-1

# Le paramètre β – Défaillances de cause commune (2)

| No. | Measure against CCF | Score |
|---|---|---|
| **3** | **Design/application/experience** | |
| 3.1 | Protection against over-voltage, over-pressure, over-current, over-temperature, etc. | **15** |
| 3.2 | Components used are well-tried. | **5** |
| **4** | **Assessment/analysis** | |
| | For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design. | **5** |
| **5** | **Competence/training** | |
| | Training of designers to understand the causes and consequences of common cause failures. | **5** |
| **6** | **Environmental** | |
| 6.1 | For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1).<br>Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium.<br>NOTE For combined fluidic and electric systems, both aspects should be considered. | **25** |
| 6.2 | Other influences<br>Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards). | **10** |
| | **Total** | **[max. achievable 100]** |

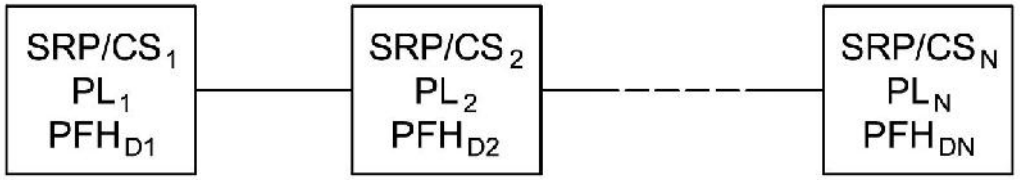
| Total score | Measures for avoiding CCF[a] |
|---|---|
| 65 or better | Meets the requirements |
| Less than 65 | Process failed ⇒ choose additional measures |

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

Sources: ISO 13849-1

# Combinaison des SRP/CS pour atteindre un PL global

On considère qu'il existe N $SRP/CS_i$ distinctes dans une combinaison en série, qui réalisent ensemble une fonction de sécurité. Pour chaque $SRP/CS_i$, un $PL_i$ a déjà été évalué. Si les valeurs de $PFH_D$ de toutes les $SRP/CS_i$ sont connues, la $PFH_D$ de la SRP/CS combinée est égale à la somme de toutes les valeurs de $PFH_D$ des N $SRP/CS_i$ individuelles.




**SRP/CS**

PL

$$PFH_D = PFH_{D1} + PFH_{D2} + \ldots + PFH_{DN}$$

# Combinaison des SRP/CS pour atteindre un PL global

Si les valeurs de PFHD de toutes les SRP/CSi individuelles ne sont pas connues, on peut appliquer une autre solution de la façon suivante:

- Identifier le PLi le plus faible, appelé PLlow.
- Identifier le nombre N low ≤ N du SRP/CSi avec PLi = PLlow.
- Déterminer le PL dans le Tableau 11.

**Table 11 — Calculation of PL for series alignment of SRP/CS**

| $PL_{low}$ | $N_{low}$ | ⇒ | PL |
|---|---|---|---|
| a | > 3 | ⇒ | None, not allowed |
| | ≤ 3 | ⇒ | a |
| b | > 2 | ⇒ | a |
| | ≤ 2 | ⇒ | b |
| c | > 2 | ⇒ | b |
| | ≤ 2 | ⇒ | c |
| d | > 3 | ⇒ | c |
| | ≤ 3 | ⇒ | d |
| e | > 3 | ⇒ | d |
| | ≤ 3 | ⇒ | e |

NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

# Exemple 1

**Table 11 — Calculation of PL for series alignment of SRP/CS**

| $PL_{low}$ | $N_{low}$ | ⇒ | PL |
|---|---|---|---|
| a | > 3 | ⇒ | None, not allowed |
| | ≤ 3 | ⇒ | a |
| b | > 2 | ⇒ | a |
| | ≤ 2 | ⇒ | b |
| c | > 2 | ⇒ | b |
| | ≤ 2 | ⇒ | c |
| d | > 3 | ⇒ | c |
| | ≤ 3 | ⇒ | d |
| e | > 3 | ⇒ | d |
| | ≤ 3 | ⇒ | e |

NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

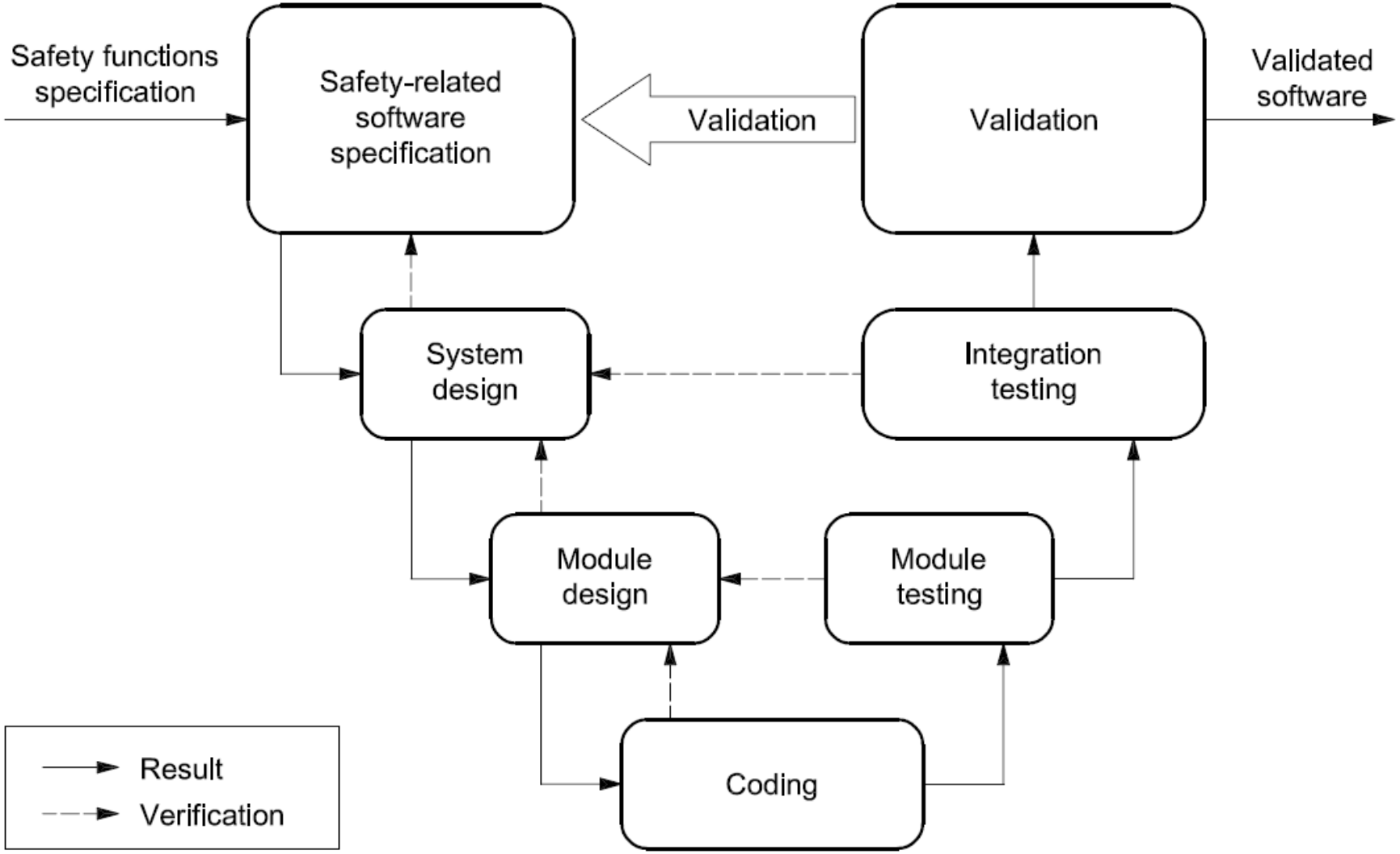
# Exemple 2

**Table 11 — Calculation of PL for series alignment of SRP/CS**

| $PL_{low}$ | $N_{low}$ | ⇒ | PL |
|---|---|---|---|
| a | > 3 | ⇒ | None, not allowed |
| | ≤ 3 | ⇒ | a |
| b | > 2 | ⇒ | a |
| | ≤ 2 | ⇒ | b |
| c | > 2 | ⇒ | b |
| | ≤ 2 | ⇒ | c |
| d | > 3 | ⇒ | c |
| | ≤ 3 | ⇒ | d |
| e | > 3 | ⇒ | d |
| | ≤ 3 | ⇒ | e |

NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

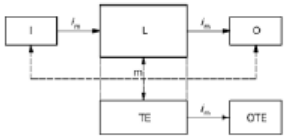
# Le développement software

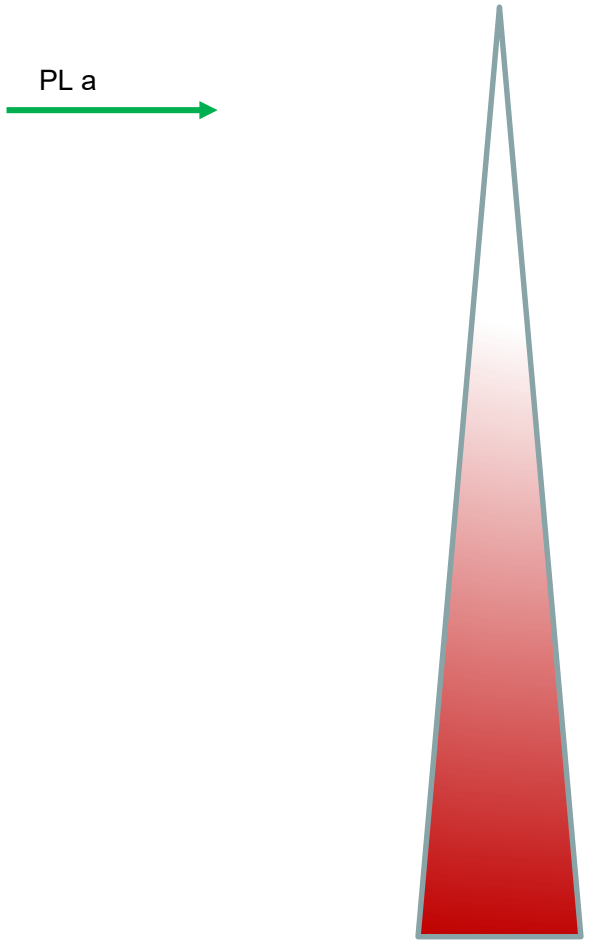




Sources: ISO 13849-1

# Récapitulatif des catégories selon le PLr – PL a

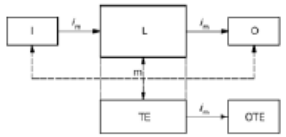
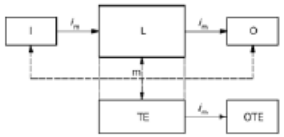
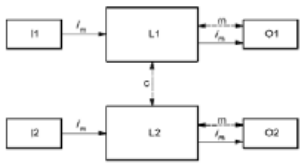
| Catégories autorisées | Cat B<br>*§ 6.2.3* | Cat 2<br>*§ 6.2.5* |
|---|---|---|
| **Respect autre catégorie** | | Respect exigences de Cat B |
| **$MTTF_d$ par canal fonct.**<br>***§ 4.5.2*** | 3 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Faible ») | 3 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Faible ») |
| **$DC_{avg}$ mini**<br>***§ 4.5.3 et Annexe E*** | $DC_{avg}$ ≥ 0<br>($DC_{avg}$ ≥ « Nulle ») | $DC_{avg}$ ≥ 60%<br>(donc $DC_{avg}$ ≥ « Faible ») |
| **CCF**<br>***Annexe F*** | Sans objet | Score ≥ 65 |
| **Spécificités** | Composants aptes à la fonction | - Composants et principes de sécurité éprouvés (§ 6.2.4)<br>- $MTTF_{d,TE}$ à considérer (§ 4.5.4) |
| **Contrôle des fonctions - périodicité** | Sans objet | Démarrage machine,<br>et périodiquement (automatique ou manuel),<br>et taux de demande ≤ 1/100 du taux d'essais |
| **Contrôle des fonctions - réaction** | Sans objet | Si défaut détecté :<br>Conduire à état sûr (arrêt)<br>ou avertissement de danger |
| **Architecture désignée** | |  |
| **Fautes systématiques** | Annexe G | Annexe G |



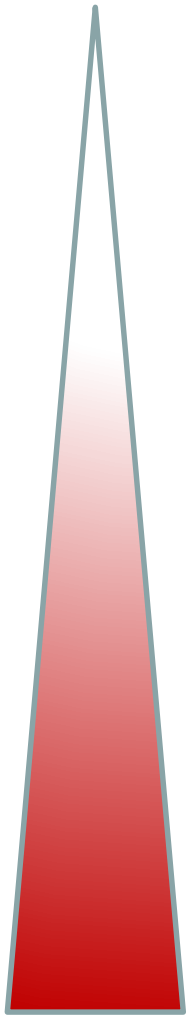


Sources: ISO 13849-1 & IEC 62061

# Récapitulatif des catégories selon le PLr – PL b

| Catégories autorisées | Cat B<br>*§ 6.2.3* | Cat 2<br>*§ 6.2.5* | Cat 2<br>*§ 6.2.5* | Cat 3<br>*§ 6.2.6* |
|---|---|---|---|---|
| Respect autre catégorie | | Respect exigences de Cat B | Respect exigences de Cat B | Respect exigences de Cat B |
| $MTTF_d$ par canal fonct.<br>*§ 4.5.2* | 10 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Moyen ») | 10 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Moyen ») | 3 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Faible ») | 3 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Faible ») |
| $DC_{avg}$ mini<br>*§ 4.5.3 et Annexe E* | $DC_{avg}$ ≥ 0<br>($DC_{avg}$ ≥ « Nulle ») | $DC_{avg}$ ≥ 60 %<br>(donc $DC_{avg}$ ≥ « Faible ») | $DC_{avg}$ ≥ 90 %<br>(donc $DC_{avg}$ ≥ « Moyenne ») | $DC_{avg}$ ≥ 60 %<br>(donc $DC_{avg}$ ≥ « Faible ») |
| CCF<br>*Annexe F* | Sans objet | Score ≥ 65 | Score ≥ 65 | Score ≥ 65 |
| Spécificités | Composants aptes à la fonction | - Composants et principes de sécurité éprouvés (§ 6.2.4)<br>- $MTTF_{d,TE}$ à considérer (§ 4.5.4) | - Composants et principes de sécurité éprouvés (§ 6.2.4)<br>- $MTTF_{d,TE}$ à considérer (§ 4.5.4) | - Composant et principes de sécurité éprouvés (§ 6.2.4)<br>- Défaut unique = état sûr |
| Contrôle des fonctions - périodicité | Sans objet | Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais | Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais | Si possible, dès ou avant prochaine sollicitation |
| Contrôle des fonctions - réaction | | Si défaut détecté :<br>Conduire à état sûr (arrêt) ou avertissement de danger | Si défaut détecté :<br>Conduire à état sûr (arrêt) ou avertissement de danger | Si défaut détecté :<br>Conduire à état sûr (arrêt) |
| Architecture désignée | |  |  |  |
| Fautes systématiques | Annexe G | Annexe G | Annexe G | Annexe G |

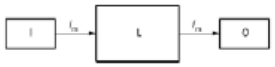
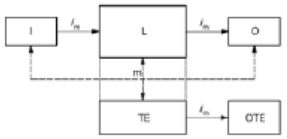
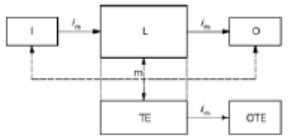
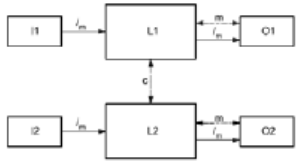
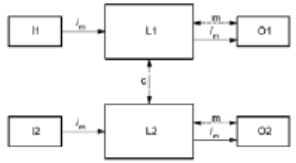
PL b

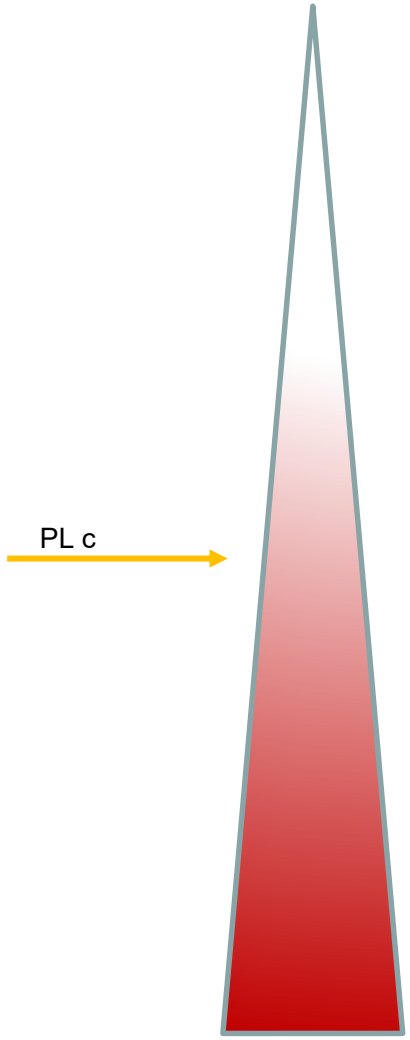




Sources: ISO 13849-1 & IEC 62061

# Récapitulatif des catégories selon le PLr – PL c

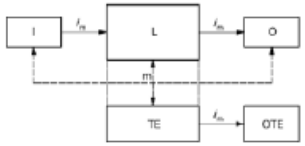
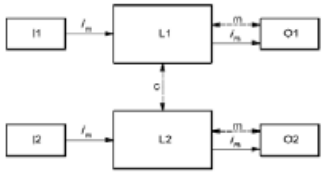
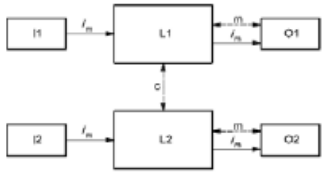
| Catégories autorisées | Cat 1<br>*§ 6.2.4* | Cat 2<br>*§ 6.2.5* | Cat 2<br>*§ 6.2.5* | Cat 3<br>*§ 6.2.6* | Cat 3<br>*§ 6.2.6* |
|---|---|---|---|---|---|
| **Respect autre catégorie** | Respect exigences de Cat B | Respect exigences de Cat B | Respect exigences de Cat B | Respect exigences de Cat B | Respect exigences de Cat B |
| **$MTTF_d$ par canal fonct.** *§ 4.5.2* | 30 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ = « Elevé ») | 30 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ = « Elevé ») | 10 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Moyen ») | 10 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Moyen ») | 3 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF^d$ ≥ « Faible ») |
| **$DC_{avg}$ mini** *§ 4.5.3 et Annexe E* | $DC_{avg}$ ≥ 0<br>($DC_{avg}$ ≥ « Nulle ») | $DC_{avg}$ ≥ 60 %<br>(donc $DC_{avg}$ ≥ « Faible ») | $DC_{avg}$ ≥ 90 %<br>(donc $DC_{avg}$ ≥ « Moyenne ») | $DC_{avg}$ ≥ 60 %<br>(donc $DC_{avg}$ ≥ « Faible ») | $DC_{avg}$ ≥ 90 %<br>(donc $DC_{avg}$ ≥ « Moyenne ») |
| **CCF** *Annexe F* | Sans objet | Score ≥ 65 | Score ≥ 65 | Score ≥ 65 | Score ≥ 65 |
| **Spécificités** | Composant et principes de sécurité éprouvés | - Composants et principes de sécurité éprouvés (§ 6.2.4)<br>- $MTTF_{d,TE}$ à considérer (§ 4.5.4) | - Composants et principes de sécurité éprouvés (§ 6.2.4)<br>- $MTTF_{d,TE}$ à considérer (§ 4.5.4) | - Composant et principes de sécurité éprouvés (§ 6.2.4)<br>- Défaut unique = état sûr | - Composant et principes de sécurité éprouvés (§ 6.2.4)<br>- Défaut unique = état sûr |
| **Contrôle des fonctions - périodicité** | Sans objet | Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais | Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais | Si possible, dès ou avant prochaine sollicitation | Si possible, dès ou avant prochaine sollicitation |
| **Contrôle des fonctions - réaction** | | Si défaut détecté :<br>Conduire à état sûr (arrêt) ou avertissement de danger | Si défaut détecté :<br>Conduire à état sûr (arrêt) ou avertissement de danger | Si défaut détecté :<br>Conduire à état sûr (arrêt) | Si défaut détecté :<br>Conduire à état sûr (arrêt) |
| **Architecture désignée** |  |  |  |  |  |
| **Fautes systématiques** | Annexe G | Annexe G | Annexe G | Annexe G | Annexe G |

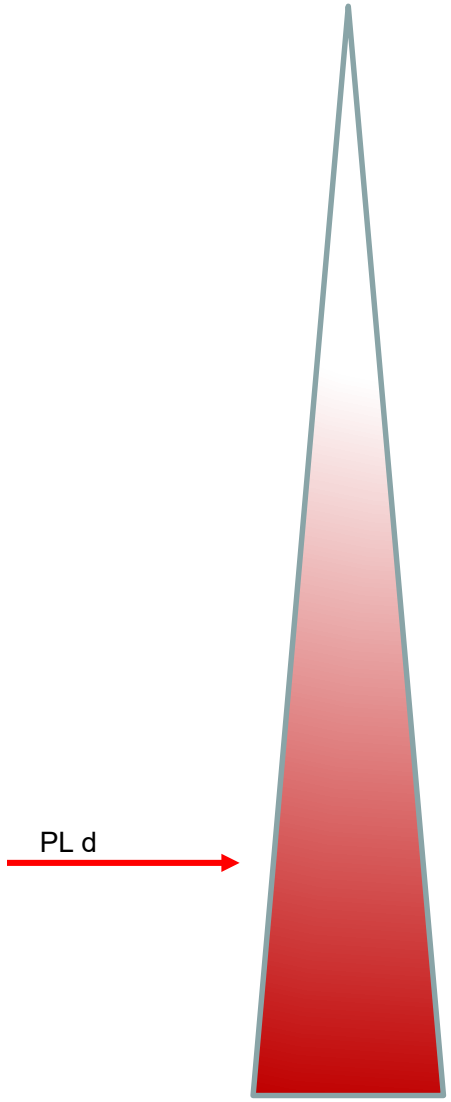




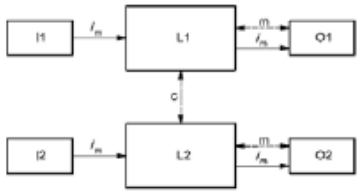
Sources: ISO 13849-1 & IEC 62061

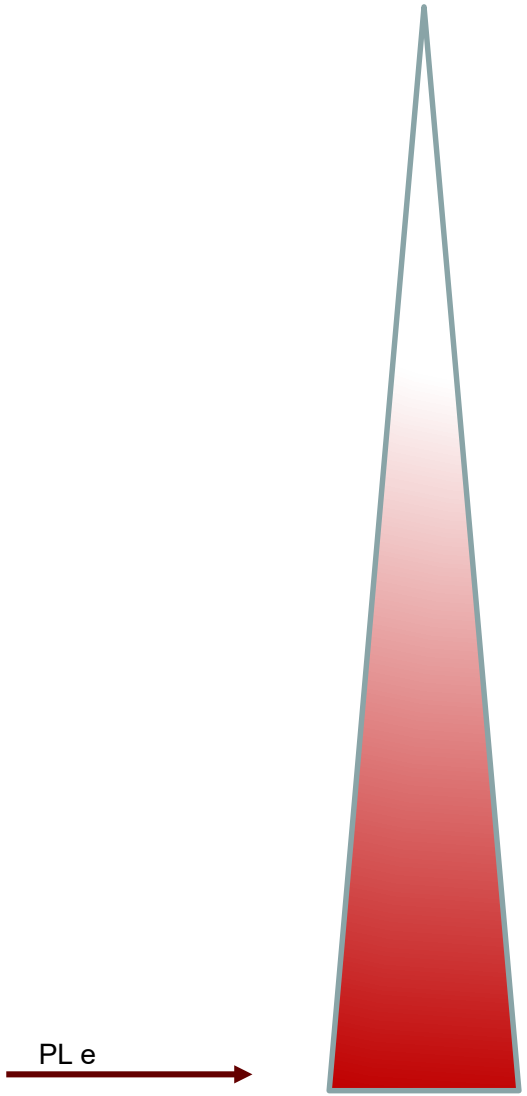
# Récapitulatif des catégories selon le PLr – PL d

| Catégories autorisées | Cat 2<br>*§ 6.2.5* | Cat 3<br>*§ 6.2.6* | Cat 3<br>*§ 6.2.6* |
|---|---|---|---|
| Respect autre catégorie | Respect exigences de Cat B | Respect exigences de Cat B | Respect exigences de Cat B |
| $MTTF_d$ par canal fonct.<br>*§ 4.5.2* | 30 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ = « Elevé ») | 30 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ = « Elevé ») | 10 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ ≥ « Moyen ») |
| $DC_{avg}$ mini<br>*§ 4.5.3 et Annexe E* | $DC_{avg}$ ≥ 90%<br>(donc $DC_{avg}$ ≥ « Moyenne ») | $DC_{avg}$ ≥ 60 %<br>(donc $DC_{avg}$ ≥ « Faible ») | $DC_{avg}$ ≥ 90 %<br>(donc $DC_{avg}$ ≥ « Moyenne ») |
| CCF<br>*Annexe F* | Score ≥ 65 | Score ≥ 65 | Score ≥ 65 |
| Spécificités | - Composants et principes de sécurité éprouvés (§ 6.2.4)<br>- $MTTF_{d.TE}$ à considérer (§ 4.5.4) | - Composant et principes de sécurité éprouvés (§ 6.2.4)<br>- Défaut unique = état sûr | - Composant et principes de sécurité éprouvés (§ 6.2.4)<br>- Défaut unique = état sûr |
| Contrôle des fonctions - périodicité | Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais | Si possible, dès ou avant prochaine sollicitation | Si possible, dès ou avant prochaine sollicitation |
| Contrôle des fonctions - réaction | Si défaut détecté :<br>Conduire à état sûr (arrêt) ou avertissement de danger | Si défaut détecté :<br>Conduire à état sûr (arrêt) | Si défaut détecté :<br>Conduire à état sûr (arrêt) |
| Architecture désignée |  |  |  |
| Fautes systématiques | Annexe G | Annexe G | Annexe G |



# Récapitulatif des catégories selon le PLr – PL d

| | |
|---|---|
| **Catégories autorisées** | **Cat 4**<br>*§ 6.2.7* |
| **Respect autre catégorie** | Respect exigences de Cat B |
| **$MTTF_d$ par canal fonct.**<br>***§ 4.5.2*** | 30 ans ≤ $MTTF_d$ ≤ 100 ans<br>(donc $MTTF_d$ = « Elevé ») |
| **$DC_{avg}$ mini**<br>***§ 4.5.3 et Annexe E*** | $DC_{avg}$ ≥ 99 %<br>(donc $DC_{avg}$ = « Elevée ») |
| **CCF**<br>***Annexe F*** | Annexe F (CCF ≥ 65) |
| **Spécificités** | - Composant et principes de sécurité éprouvés (§ 6.2.4)<br>- Défaut unique = état sûr |
| **Contrôle des fonctions - périodicité** | Dès ou avant prochaine sollicitation |
| **Contrôle des fonctions - réaction** | Défaut détecté :<br>Conduire à état sûr (arrêt) |
| **Architecture désignée** |  |
| **Fautes systématiques** | Annexe G |





Sources: ISO 13849-1 & IEC 62061

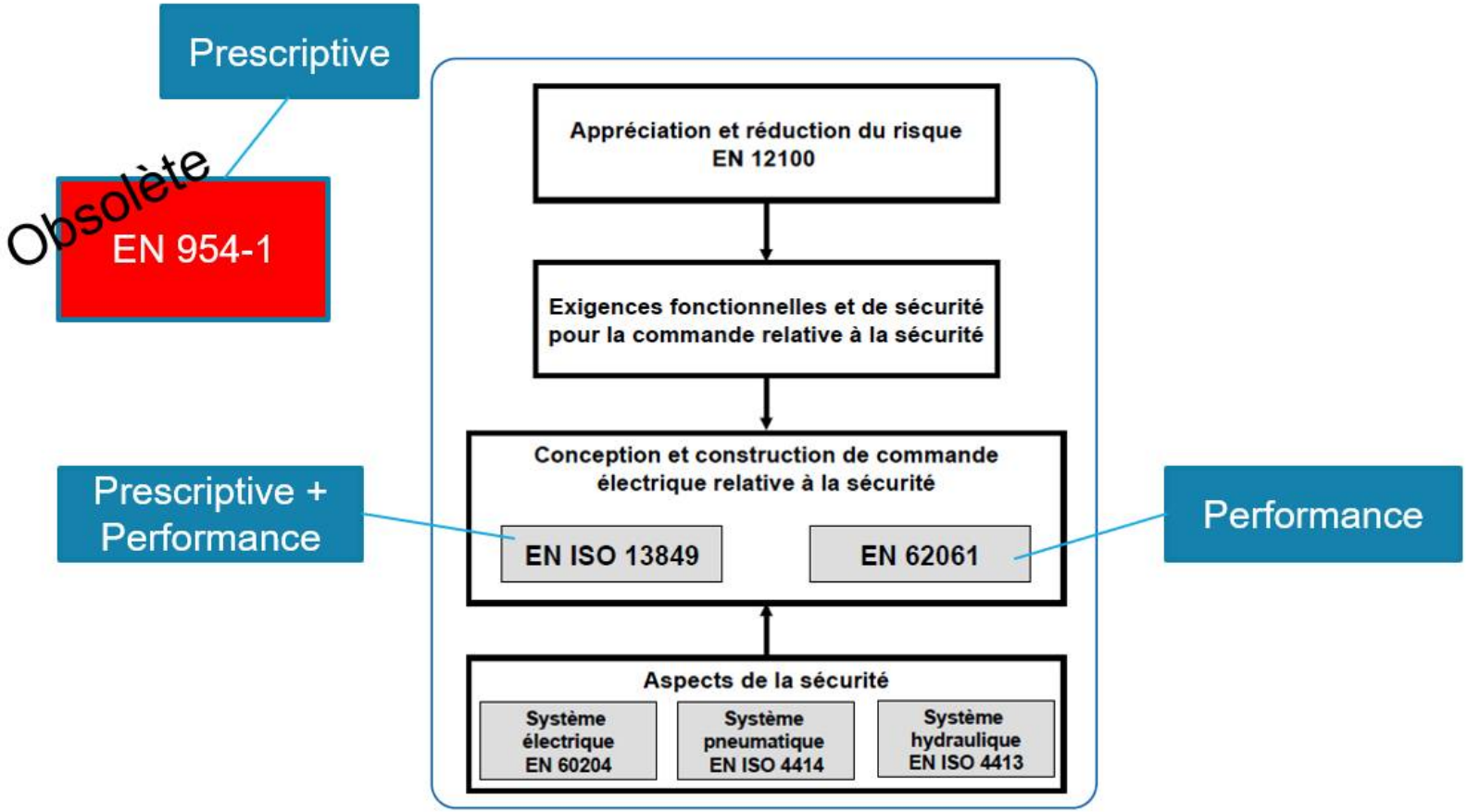
# IEC 62061 vs ISO 13849 – Légalement

Au niveau législatif, les deux normes sont reconnues comme «normes harmonisées» par la communauté européenne. Ce qui implique qu'ils sont tous les deux utilisables afin de valider la sécurité d'un SRP-CS

| | | | | | | |
|---|---|---|---|---|---|---|
| 2006/42/EC | CEN | EN ISO 13849-1:2008,<br>EN ISO 13849-1:2008/AC:2009 | Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006) | B | 29/12/2009 | OJ C 214 - 08/09/2009 |
| 2006/42/EC | Cenelec | EN 62061:2005,<br>EN 62061:2005/AC:2010,<br>EN 62061:2005/A1:2013,<br>EN 62061:2005/A2:2015 | Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems | B | 15/01/2016 | OJ C 014 - 15/01/2016 |

Sources: ISO 13849-1 & IEC 62061

# IEC 62061 vs ISO 13849 - Structure



# IEC 62061 vs ISO 13849 – Les niveaux de sécurité

Les deux standard définissent un niveau de sécurité. Dans l'ISO 13849, il est appelé PL (Performance Level) dans l'IEC62061, SIL (Safety Integrity Level). Ils sont tous deux directement transposables d'une norme à l'autre.

| PL (ISO13849) | SIL (IEC62061) | PFH |
|---|---|---|
| a | Pas de correspondance | $\geq 10^{-5}$ … $< 10^{-4}$ |
| b | 1 | $\geq 3 \times 10^{-6}$ … $< 10^{-5}$ |
| c | 1 | $\geq 10^{-6}$ … $< 3 \times 10^{-6}$ |
| d | 2 | $\geq 10^{-7}$ … $< 10^{-6}$ |
| e | 3 | $\geq 10^{-8}$ … $< 10^{-7}$ |

Sources: ISO 13849-1 & IEC 62061

# IEC 62061 vs ISO 13849 – La technologie utilisée

- La norme ISO 13849 couvre la validation de systèmes non électriques comme les systèmes pneumatiques, ou hydrauliques par exemple. Ceux-ci ne sont pas couverts par l'IEC62061 qui ne couvre que les composante électriques, électroniques et électronique programmable.
- La norme IEC 62061 est plus adaptée aux systèmes ayant une architecture complexe. En effet, l'ISO 13849 demande de suivre des architectures spécifiques afin d'atteindre ses objectifs.
- Si un système devait contenir des sous-modules pneumatiques par exemple, il est possible de valider le système selon l'IEC62061 en évaluant les sous module selon l'ISO 13849 et en utilisant les résultats dans le système complet.
- Dans l'industrie de transformation, comme le monde de la chimie par exemple, l'IEC 62061 est plus souvent utilisée car elle utilise les niveaux SIL tout comme l'IEC 61511 régissant cette industrie.
- Pour un système contenant du SW complexe, l'IEC 61508 peut être utilisée comme support pour la validation du software.


Sources: ISO 13849-1 & IEC 62061

# IEC 62061 vs ISO 13849 – L'architecture

La norme IEC 62061 ne définit pas d'architecture spécifiques. Cependant, celles-ci sont implicitement requises lors du calcul du paramètre SFF (Safe Failure Fraction) qui est requis par ce standard. Ce SFF représente le ratio de défaillances n'ayant pas d'impact sur le système par rapport au total des défaillances possibles

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

$\lambda_S$ is the rate of safe failure
$\lambda_{DD}$ is the rate of dangerous failure which is detected by the diagnostic function
$\lambda_D$ is the rate of dangerous failure

Afin de calculer cet indice SFF, il faudra très souvent avoir recourt à des méthodes plus complexes que celles utilisées dans l'ISO 13849, comme les FMEA/FMEDA, FTA…

La liberté aquise dans l'architecture a donc un prix et demande plus de travail dans les analyses du système.


Sources: ISO 13849-1 & IEC 62061

# IEC 62061 vs ISO 13849 – Les paramètres du SIL

Une fois la SFF calculée, le niveau SIL atteint par le système peuvent être définis en suivant le tableau ci-dessous. Le deuxième paramètre requis est la HFT (Hardware Fault Tolerance) et il représente la redondance de notre système.

| Safe failure fraction | Hardware fault tolerance (see Note 1) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | Not allowed (for exceptions see Note 3) | SIL1 | SIL2 |
| 60 % – < 90 % | SIL1 | SIL2 | SIL3 |
| 90 % – < 99 % | SIL2 | SIL3 | SIL3 (see Note 2) |
| ≥ 99 % | SIL3 | SIL3 (see Note 2) | SIL3 (see Note 2) |

NOTE 1 A hardware fault tolerance of $N$ means that $N$+1 faults could cause a loss of the safety-related control function.

NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.

NOTE 3 See 6.7.6.4 or for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see 6.7.7.

Sources: ISO 13849-1 & IEC 62061

# IEC 62061 vs ISO 13849 – Le taux de défaillance

Dans le développement selon l'IEC 62061, le PFH est utilisé pour estimer la fiabilité du système. Il devra donc être calculé. Lorsque notre système ne contient pas de canal redondant, il est très similaire au $MTTF_D$ calculé dans l'ISO 13849-1.

Lorsque le système contient de la redondance, les paramètres de DC, β et l'intervalle de test entrent dans le calcul du PFH et le complexifient légèrement.

Nous voyons donc qu'aucun tableau ne permet de valider une architecture selon IEC 62061 mais des équations et des calculs.


Sources: ISO 13849-1 & IEC 62061

# IEC 62061 vs ISO 13849 – β (CCF)

Pour les défaillances de cause commune, comme mentionné dans le slide précédent, la valeur de β sera utilisée dans le calcul du PFH, il faut donc l'estimer en suivant un tableau similaire à celui de l'ISO 13849. Selon le score obtenu, nous dérivons β et nous l'intégrons dans le calcul du PFH.

| Item | Reference | Score |
|---|---|---|
| Separation/segregation | | |
| Are SRECS signal cables for the individual channels routed separately from other channels at all positions or sufficiently shielded? | 1a | 5 |
| Where information encoding/decoding is used, is it sufficient for the detection of signal transmission errors? | 1b | 10 |
| Are SRECS signal and electrical energy power cables separate at all positions or sufficiently shielded? | 2 | 5 |
| If subsystem elements can contribute to a CCF, are they provided as physically separate devices in their local enclosures? | 3 | 5 |
| Diversity/redundancy | | |
| Does the subsystem employ different electrical technologies for example, one electronic or programmable electronic and the other an electromechanical relay? | 4 | 8 |
| Does the subsystem employ elements that use different physical principles (e.g. sensing elements at a guard door that use mechanical and magnetic sensing techniques)? | 5 | 10 |
| Does the subsystem employ elements with temporal differences in functional operation and/or failure modes? | 6 | 10 |
| Do the subsystem elements have a diagnostic test interval of <1 min? | 7 | 10 |
| Complexity/design/application | | |
| Is cross-connection between channels of the subsystem prevented with the exception of that used for diagnostic testing purposes? | 8 | 2 |
| Assessment/analysis | | |
| Have the results of the failure modes and effects analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design? | 9 | 9 |
| Are field failures analysed with feedback into the design? | 10 | 9 |
| Competence/training | | |
| Do subsystem designers understand the causes and consequences of common cause failures? | 11 | 4 |
| Environmental control | | |
| Are the subsystem elements likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc. over which it has been tested, without the use of external environmental control? | 12 | 9 |
| Is the subsystem immune to adverse influences from electromagnetic interference up to and including the limits specified in IEC 61326-3-1? | 13 | 9 |

NOTE An alternative item (e.g. references 1a and 1b) is given in Table F.1 where it is intended that a claim can be made for a contribution towards avoidance of CCF from only the most relevant item.

| Overall score | Common cause failure factor (β) |
|---|---|
| ≤ 35 | 10 % (0,1) |
| 36 – 65 | 5 % (0,05) |
| 66 – 85 | 2 % (0,02) |
| 86 – 100 | 1 % (0,01) |

Sources: ISO 13849-1 & IEC 62061

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

1. Kasinathan Sumanan – Remontés Mécaniques
2. Mathieu Rimet – Sécurité domaine chimie
3. Nathanaël Jaquet - Mesure acoustique de machines
4. Alexandre Murisier - ISO 13851
5. Juliette McMichael – Consignation (Lockout Tagout)
6. Mattéo Meister – ISO/PRF 22916 – Dispositifs microfluidiques
7. Harjeet Nagi - Norme de sécurité électrique et régimes de neutres
8. Shukri Ramadani - Les EPI
9. Quentin Müller – ISO 13857 les distances de sécurité
10. César Michaud – Les jouets radioactifs
11. Philippe Gaêl Dubuis – Chariots de Manutention
12. Julien Pernet – Retour sur l'ISO 12100
13. Anuraag Pothula – Redondance
14. Pescatore Gabriele – CEM
15. Forestal Maël – ISO 13856-2
16. Adrien Périchon – ISO 14120
17. Monia Baouab – ISO 13731-1
18. Xavier Giuntini – L'utilisation des couleurs dans la sécurité des machies
19. Thierry Fracheboud – Directive CFST 6512
20. Joris Ferroni – Explication des termes MTTF,MTBF,MTTR
21. Fabrice Seppey – Directives des installations de tir en suisse
22. ??

# Questions ?

Sécurité et fiabilité des systèmes (SecuFS)

# 08 – Processus de développement des systèmes techniques – Partie 1

Frédéric Schenker

15.11.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | 31.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours

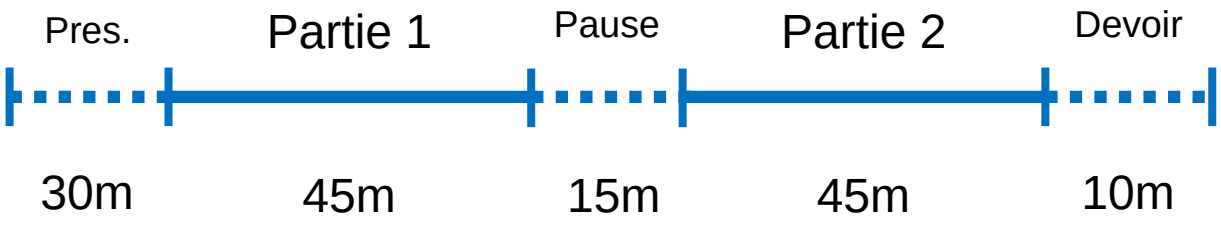
**Structure du cours:**

**Partie 1** : 15 novembre 2021
Objectif général : Introduction à l’ingénierie système et ces processus

**Partie 2** : 22 novembre 2021
Objectifs : L’ingénierie système basée sur les modèles et son application

**Partie 3** : 29 novembre 2021
Objectifs : Workshop

# Format du cours




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

| | | |
|---|---|---|
| 23 | Celso Cippà | Le concept de fail-safe |
| 24 | Thibault Vadon | Dosimétrie et radioprotection |
| 25 | Macherel Rémy | Les phénomènes dangereux, exemple pour une machine |
| 26 | Mansour Ghomashi | Sécurité dans les centrales électriques ( haute tension ) |
| 27 | Roux Pierre-Aloïs | Comment fonctionne la surveillance du marché |

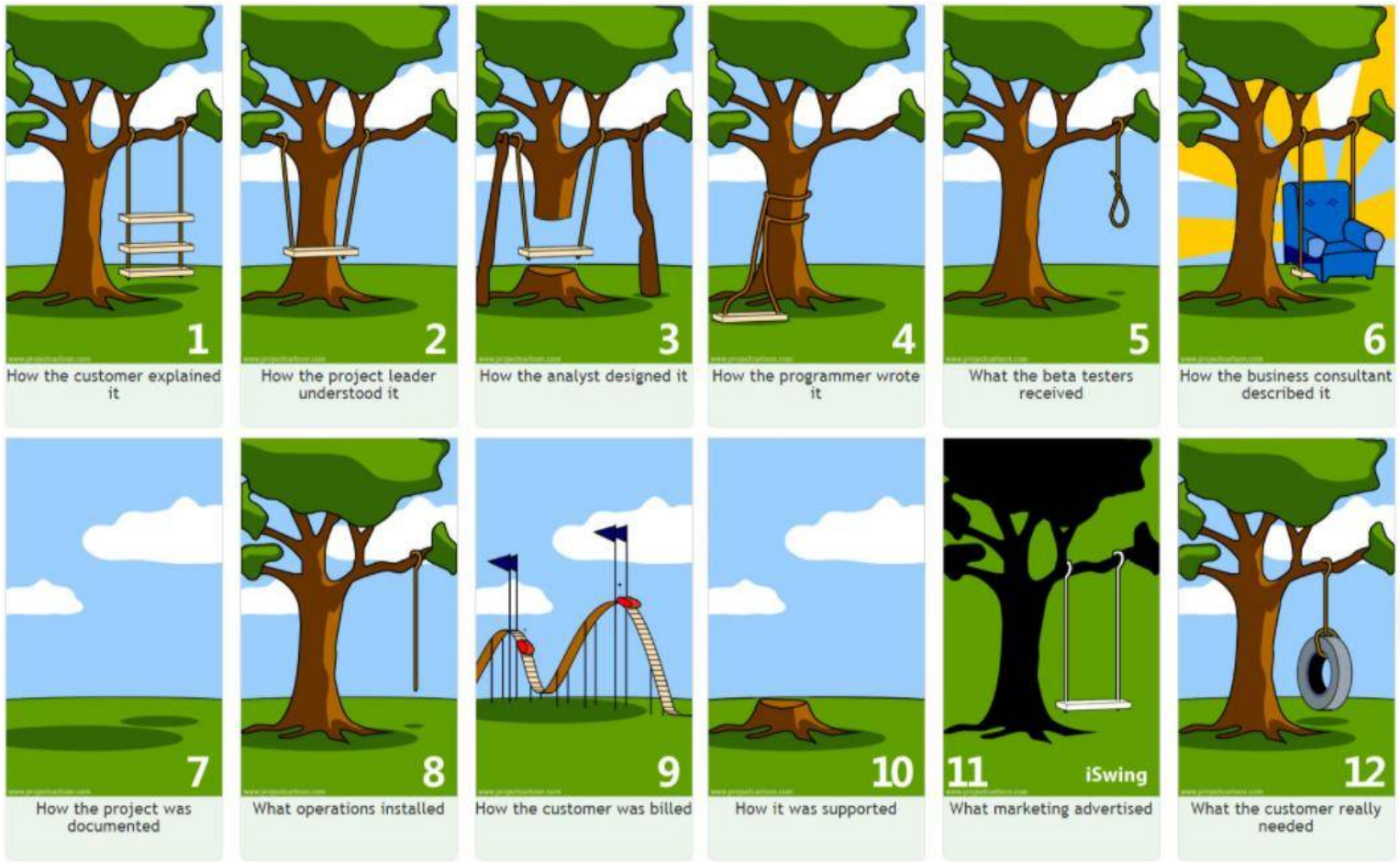
Tableau des présentations

# Objectifs du cours

- Introduction à l’ingénierie des systèmes
- Les processus de l’ingénierie système
- Quelques clés pour le développement de système
  - Les exigences
  - La vérification et la validation
- L’ingénierie des systèmes basée sur le modèle (MBSE)
- Les systèmes

# Introduction à l’ingénierie des systèmes

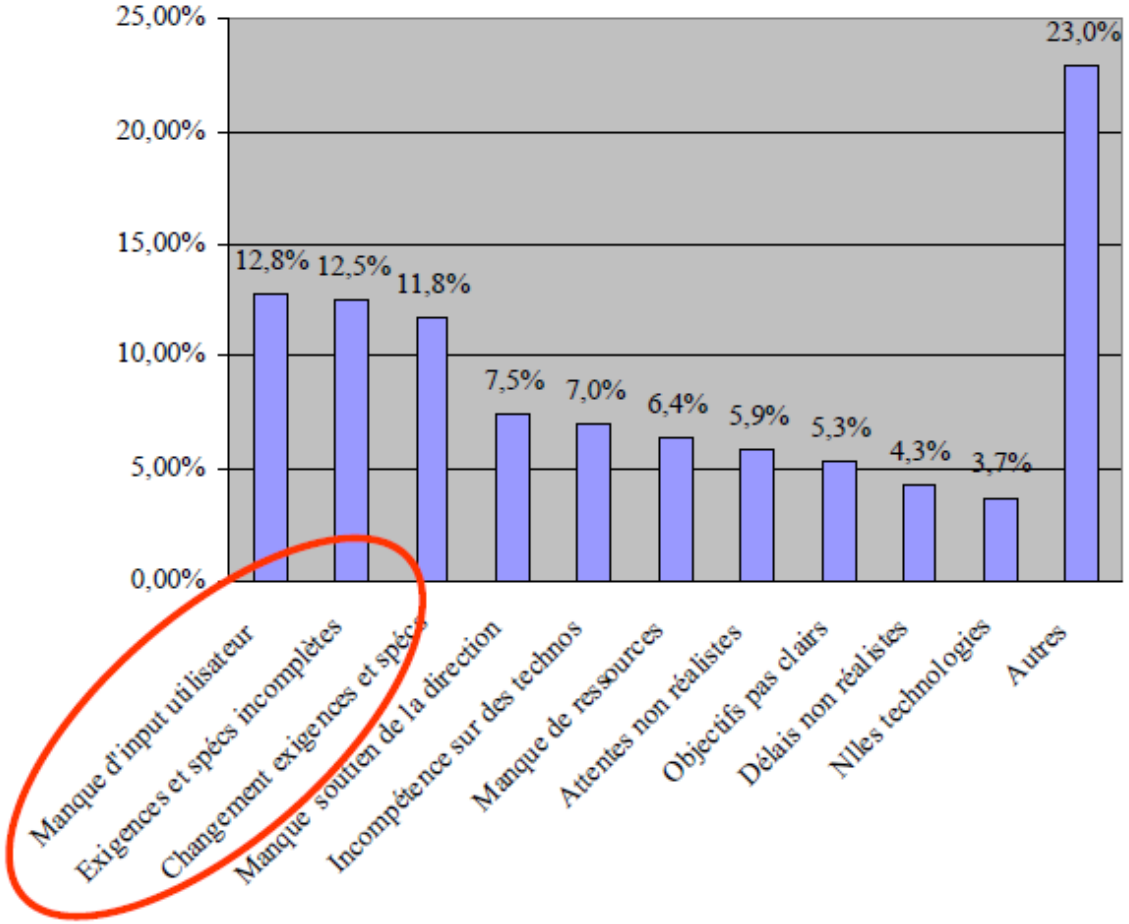
# Introduction – Ingénierie des systèmes




- Gestion des risques
- Gestion des besoins
- Gestion des contraintes
- Gestion des parties prenantes
- Gestion de la maintenance
- Gestion du rendu
- …

Sources: https://www.zentao.pm/share/trees-wing-project-management-cartoon-97.html

# Causes des échecs d'un développement




Sources: D. Luzeaux DGA

# Ingénierie des système - Définition

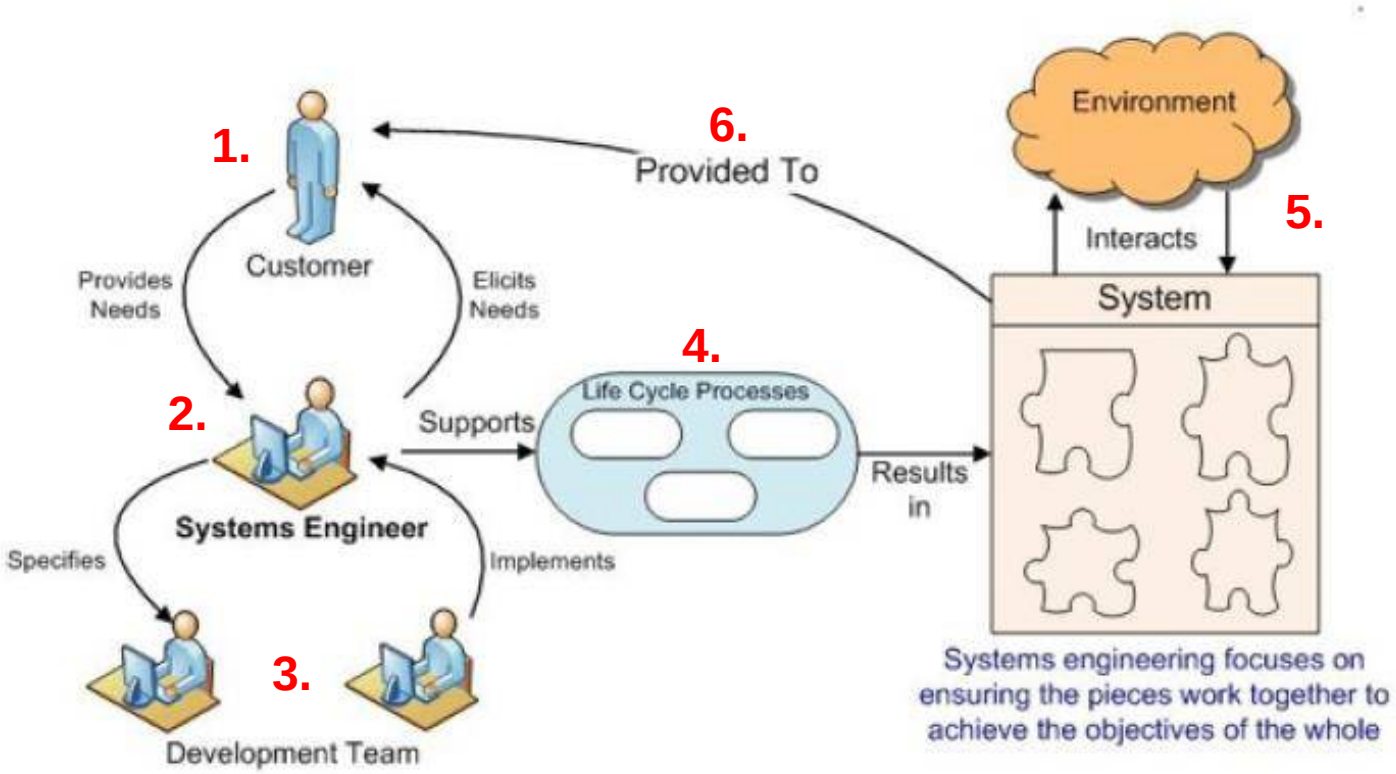
Approche transdisciplinaire (inter-métier) appliquée au cycle de développement des systèmes incluant des processus de management et technique.

Objectifs :

- Répondre aux besoins des parties prenantes d'un système en développement.
- Réunir toutes les équipes de développement (ingénieurs, manager, vendeur, …) autour d'un même objectif.
- Réduire les risques pouvant affecter le succès d'un projet.

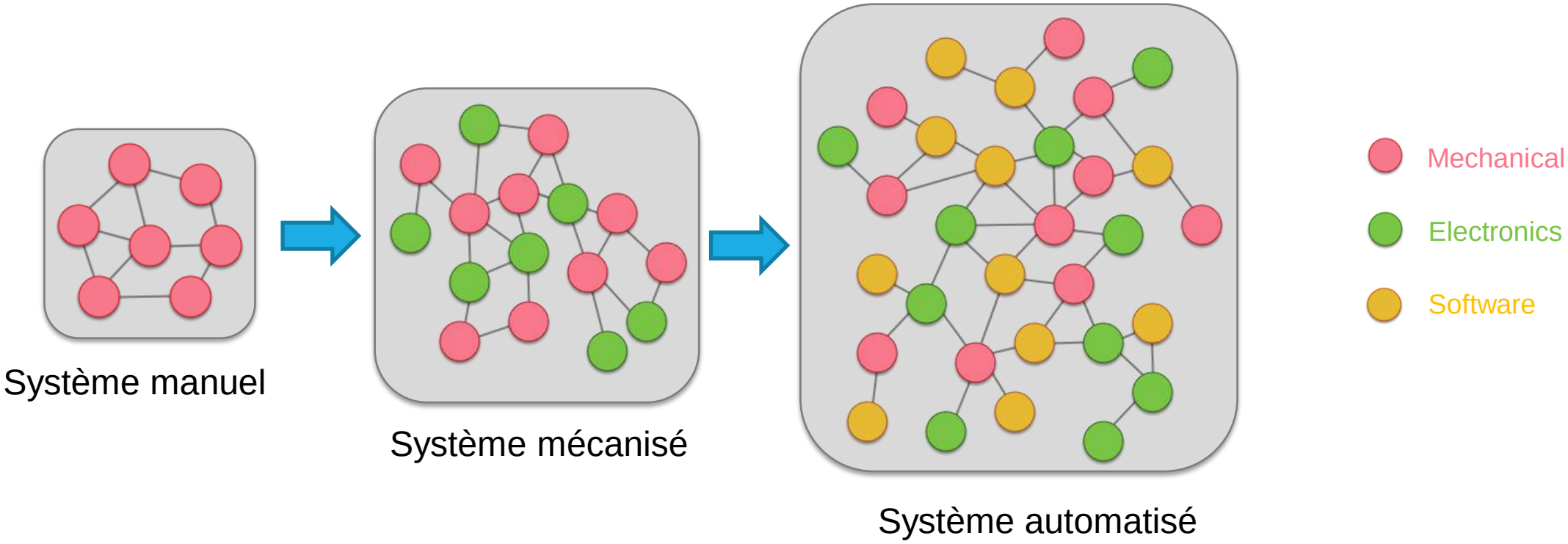
Sources: Practical Guide to SysML - The Systems Modeling Language (3rd Edition) – S. Friedenthal

# Ingénierie des système - Définition




Sources: Practical Guide to SysML - The Systems Modeling Language (3rd Edition) – S. Friedenthal

# Evolution de la complexité



# Evolution de la complexité (1)

Example : le store à lamelles

**Système manuel :**
L'utilisateur utilise une manivelle pour actionner le store lorsqu'il le souhaite

**Système mécanisé :**
L'utilisateur utilise un bouton mural pour actionner le store lorsqu'il le souhaite.

**Système automatisé :**
Le store actionne automatiquement le store lorsqu'il détecte que le soleil est présent.

# Evolution de la complexité (2)

Example : direction d'une voiture

**Système manuel :**
L'utilisateur tourne son volant pour agir sur la direction que prend son véhicule.

**Système mécanisé :**
L'utilisateur tourne son volant pour agir sur la direction que prend son véhicule. Le véhicule assiste l'utilisateur dans son action (direction assistée).

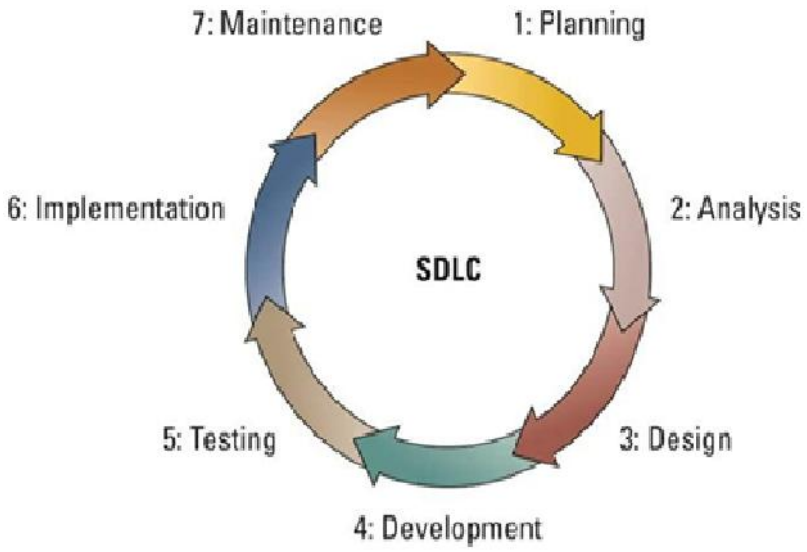
**Système automatisé :**
Le véhicule peut agir directement sur sa direction en prenant le contrôle (lane assist).

# Les processus de l’ingénierie système

# Le cycle de vie d'un système

Ensemble des méthodes qui englobent les activités pour :

- **Planification**
- **Analyse**
- **Conception**
- **Développement**
- **Vérification/Validation**
- **Implémentation**
- **Maintenance**

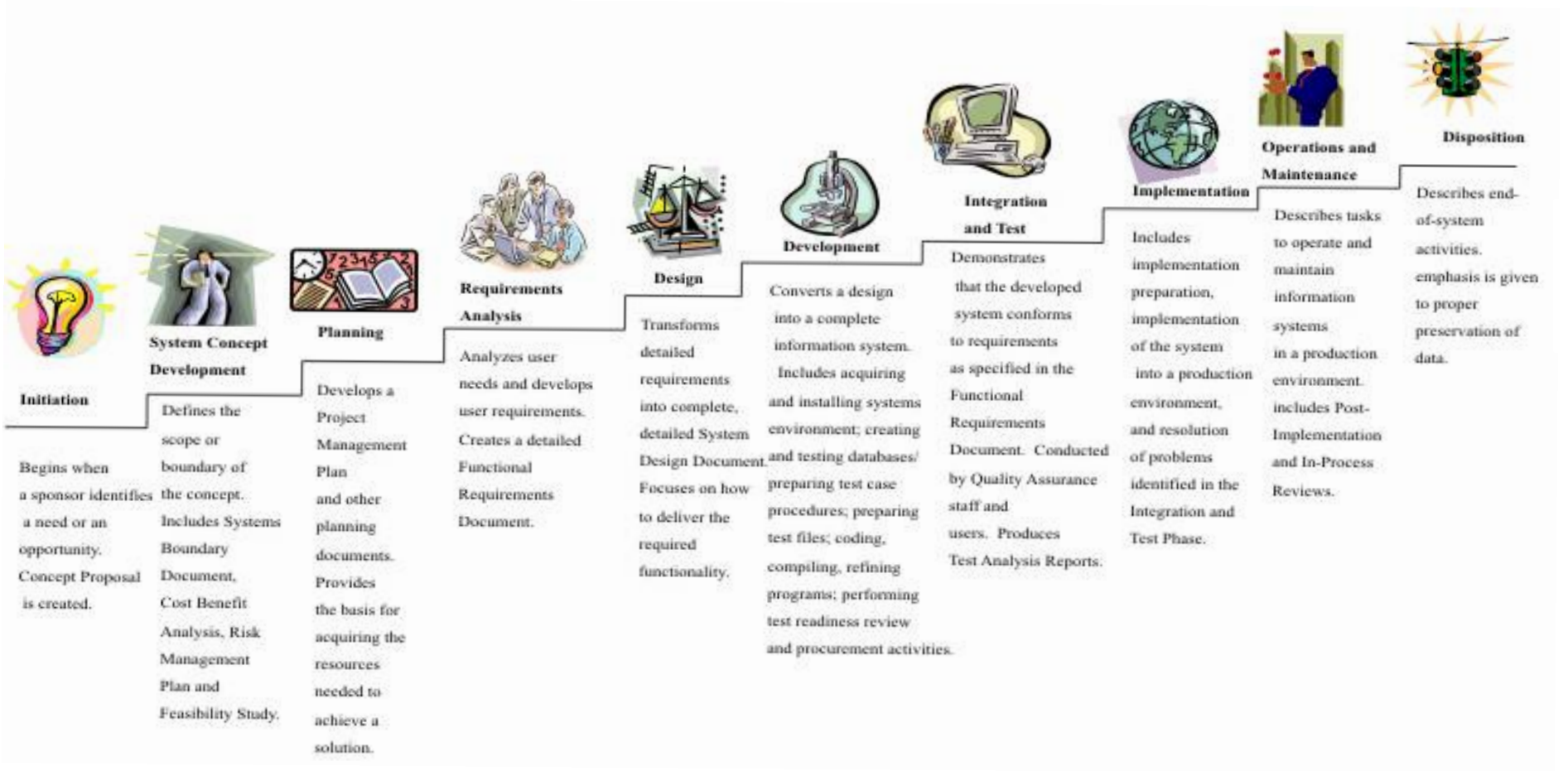



*System Development Life Cycle

Objectif entreprise : trouver la solution la plus économique et performante qui répondra aux besoins des différentes parties prenantes

Sources: http://study-aids.co.uk/dissertation-blog/system-development-life-cycle-sdlc/

# Le cycle de vie d’un produit

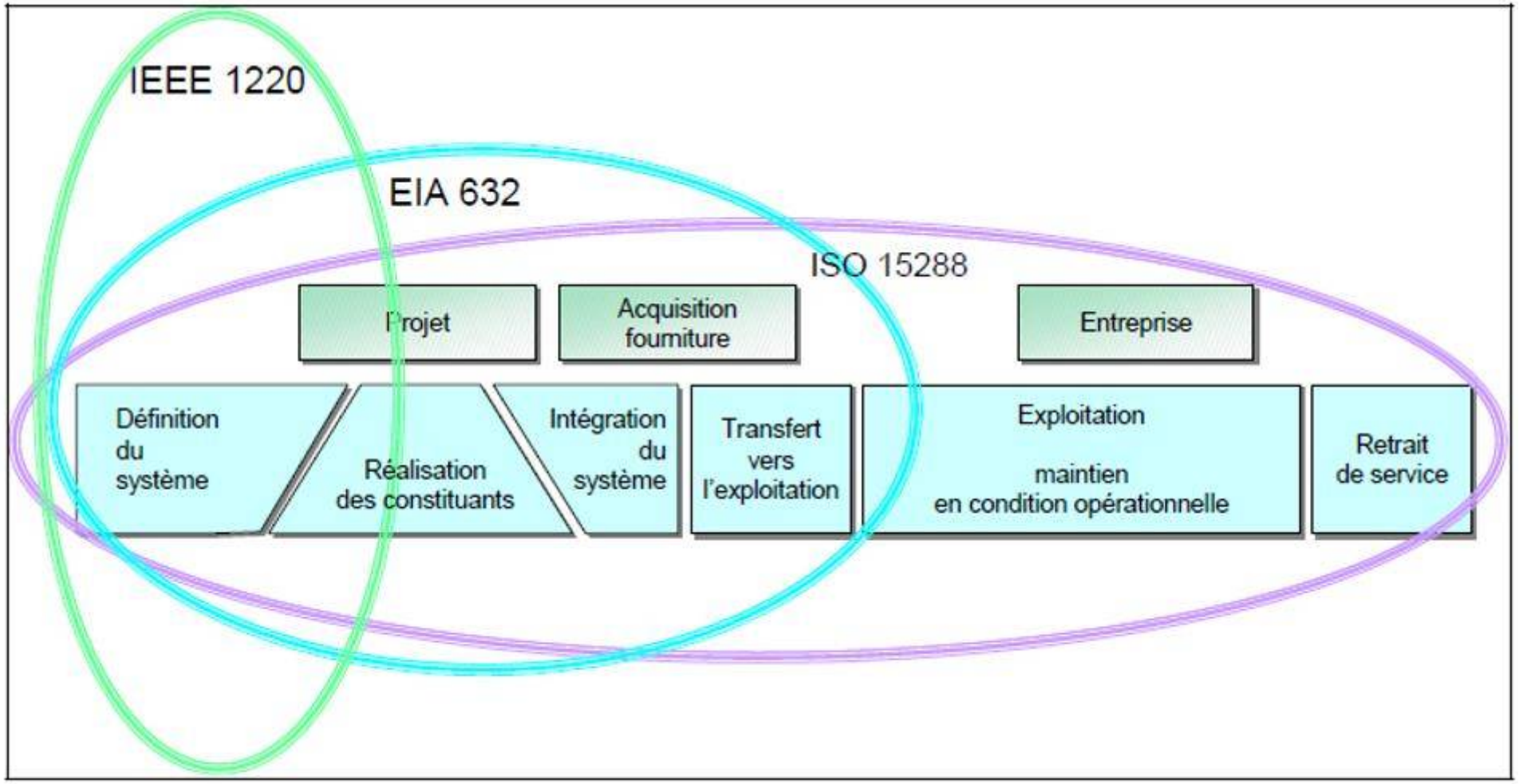



..

Disposal/retirement

Sources: https://www.justice.gov/archive/jmd/irm/lifecycle/ch1.htm#para1.2

# Normes de l'IS

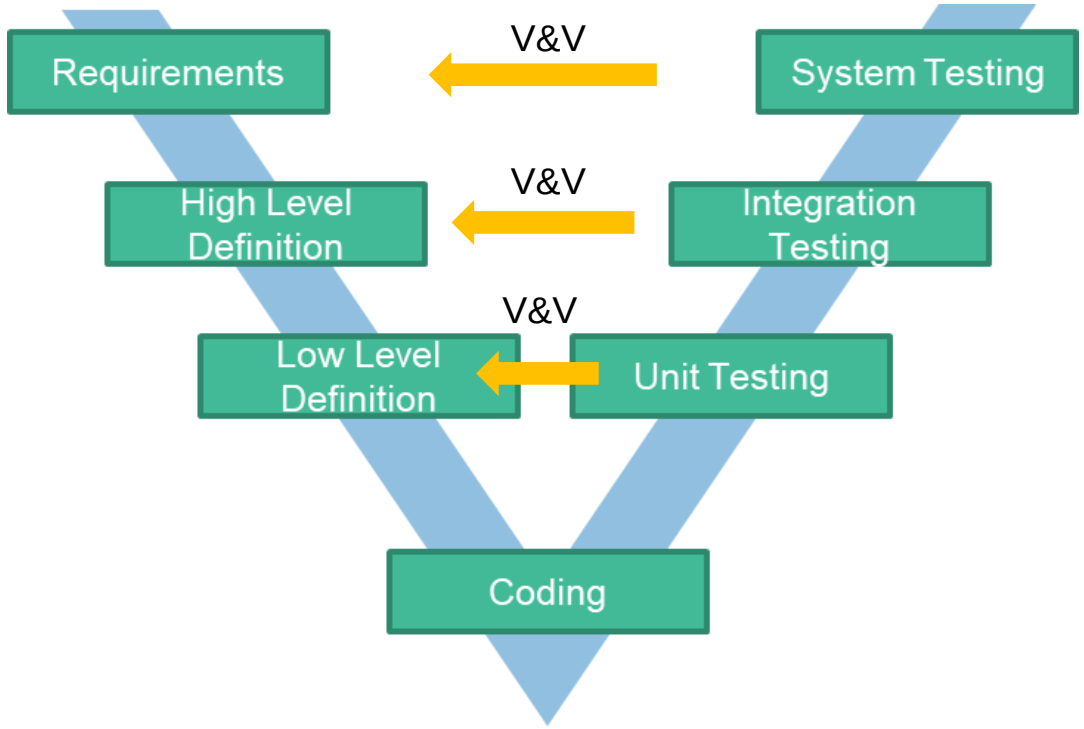



Sources: HAAG – Ingénierie Système 2015

# Processus exemple

Le modèle en V : modèle de développement couramment utilisé dans l'industrie.

p.ex. : Base dans le processus de l'ISO 26262 (norme automobile)

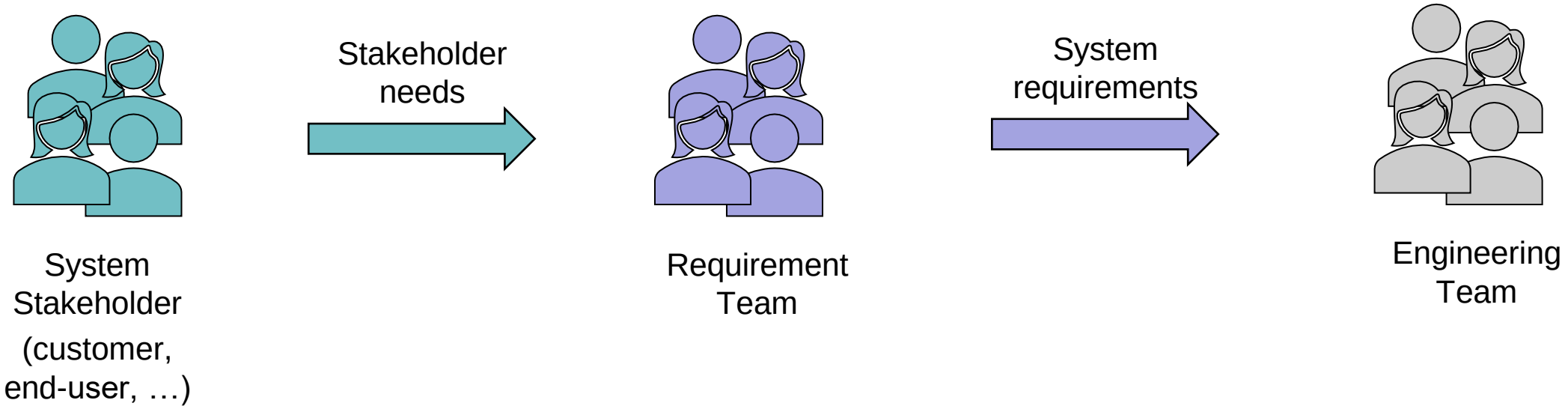


# Quelques aspects clés

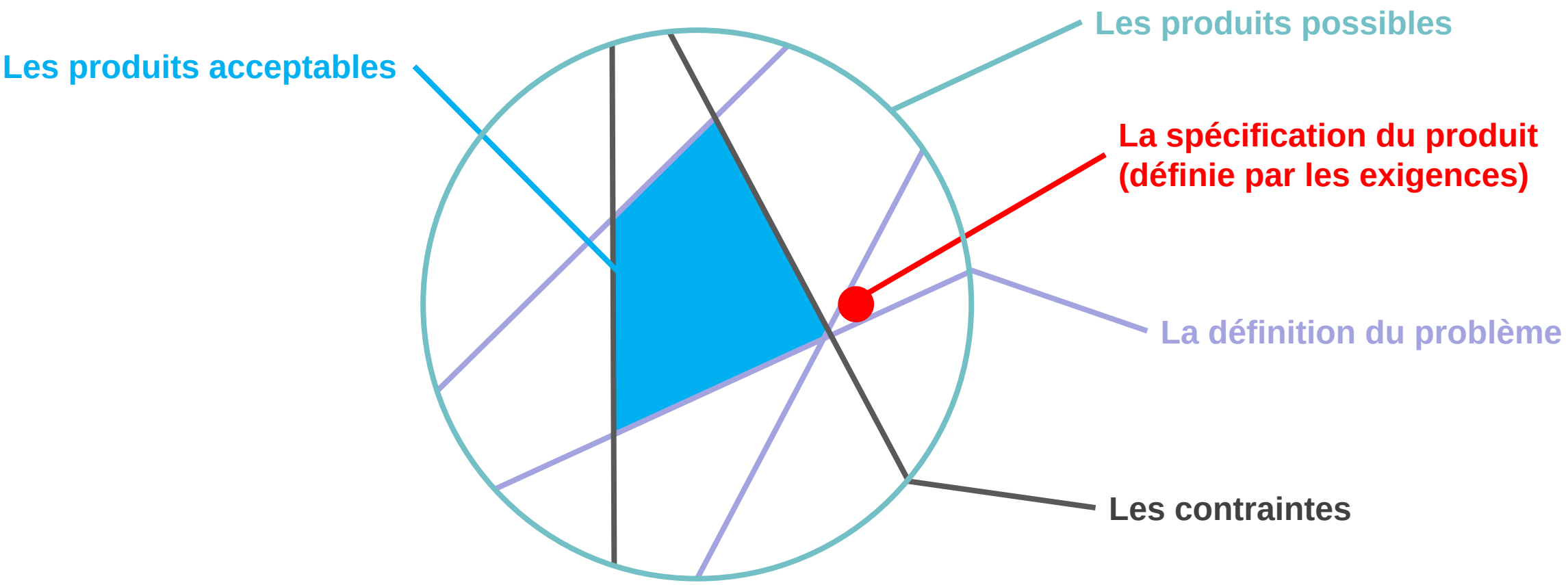
# Les exigences - Définition

Définition (ISO 29148) :

*statement that translates or expresses a need and its associated constraints and conditions*



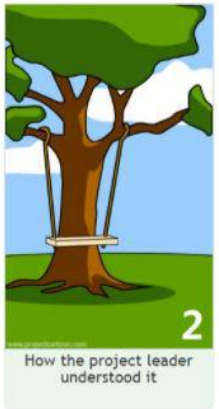
# Les exigences - Problématique




Sources: Requirement Best Practices - Jama software - Webinar

# Les exigences – Les problèmes liés

- Comment s’assurer que le client a exposé son problème correctement ?
- Comment s’assurer que le client a exposé ses besoins correctement ?
- Comment s’assurer que l’équipe exigences a compris le client correctement ?
- Comment s’assurer que l’exigence système correspond aux besoins clients ?
- Comment s’assurer que l’équipe d’ingénieurs comprend l’exigence système correctement ?
- …



# Les exigences – Ecrire une bonne exigence

- Eviter les ambiguïtés

Exemple :
La voiture doit être bleu → que veut dire bleu ?
La voiture doit être bleu ciel [#7BAFD4]

- Utiliser un bon verbe

  !! Préférer la forme ‘shall’ !!

Exemple (Anglais) :
- The car shall be sky blue [#7BAFD4]
- The car should be sky blue [#7BAFD4]
- The car can be sky blue [#7BAFD4]

- Eviter les adverbes peu clairs

Exemple :
- Le système doit faire **raisonnablement …**
- Le système doit faire **aussi vite que possible ...**
- Le système doit améliorer **considérablement** …
- …

→ Mesurable ? Vérifiable ? Testable ?

- Eviter les négations

Exemple :
Le système ne doit pas fournir pas plus de 4MB → NOK
Le système doit fournir plus 4MB → OK

Sources: Requirement Best Practices - Jama software - Webinar

# Les exigences – Les propriétés

- Atomique → Une exigence inclut un seul besoin
- Complète → Eviter les abstractions, les «c'est logique que …»
- Consistante → Eviter les conflits d'idée ou les contradictions
- Pas ambiguë
- Non redondante
- Vérifiable
- Implémentable

Ce n'est pas le rôle de l'équipe des exigences de fixer des contraintes.

Sources: Requirement Management training – Steven Adamson

# Les exigences – La forme

| [Trigger] | [Precondition] | Actor | Action | [Object] |
|---|---|---|---|---|
| When a collision is detected | and the passenger airbag switch is on | the system | SHALL detonate | the passenger airbags |

Sources: Requirement Best Practices - Jama software - Webinar

# Vérification et Validation (V&V)

Présentation de M. Beltus de la semaine prochaine

# L’ingénierie des systèmes basée sur les modèles

Model-Based Systems Engineering (MBSE)

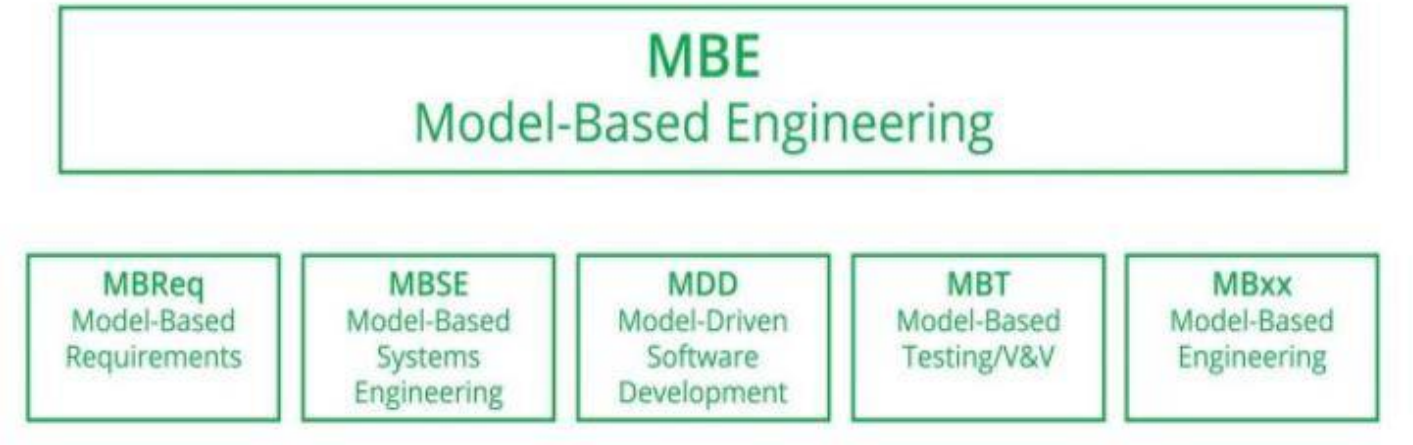
# MBSE - Définition

- Le Model BasedSystems Engineering (MBSE) est une approche ou méthodologie se basant sur des représentations visuelles des systèmes (plutôt que textuelle) visant à simplifier les processus de conception et de production d'outils technologiques.

  → https://blog.lesjeudis.com/cest-quoi-le-mbse

- "Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases."

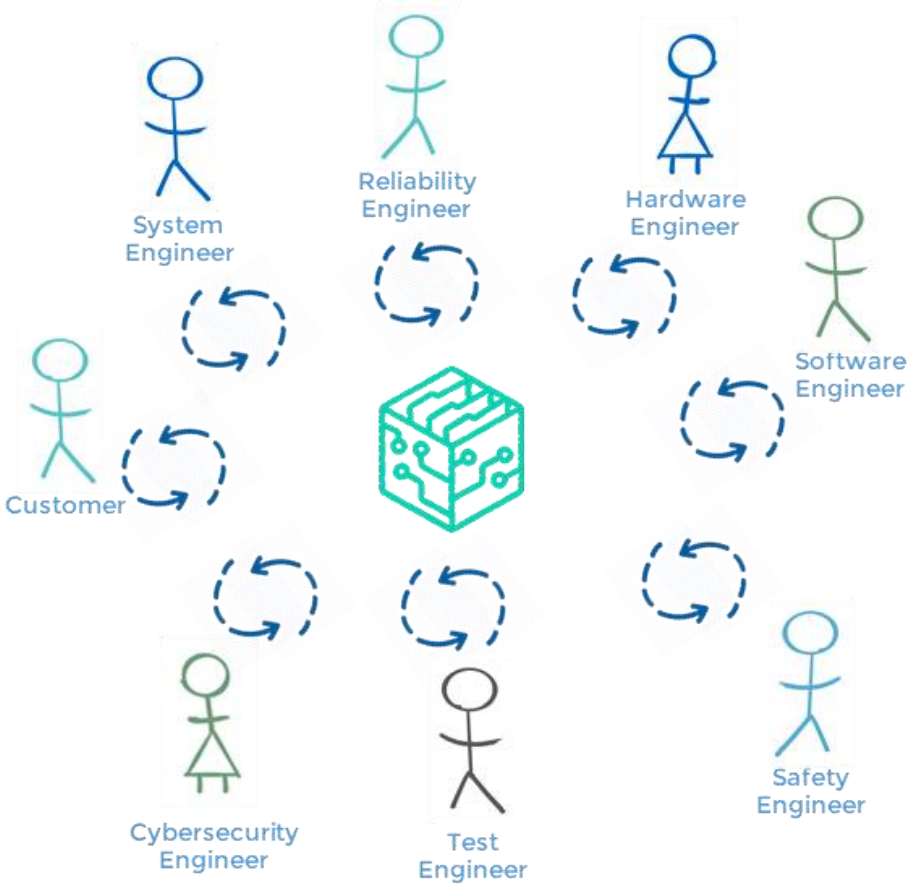
  → INCOSE SE Vision 2020 -2007




Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

# Pourquoi MBSE ? (1)

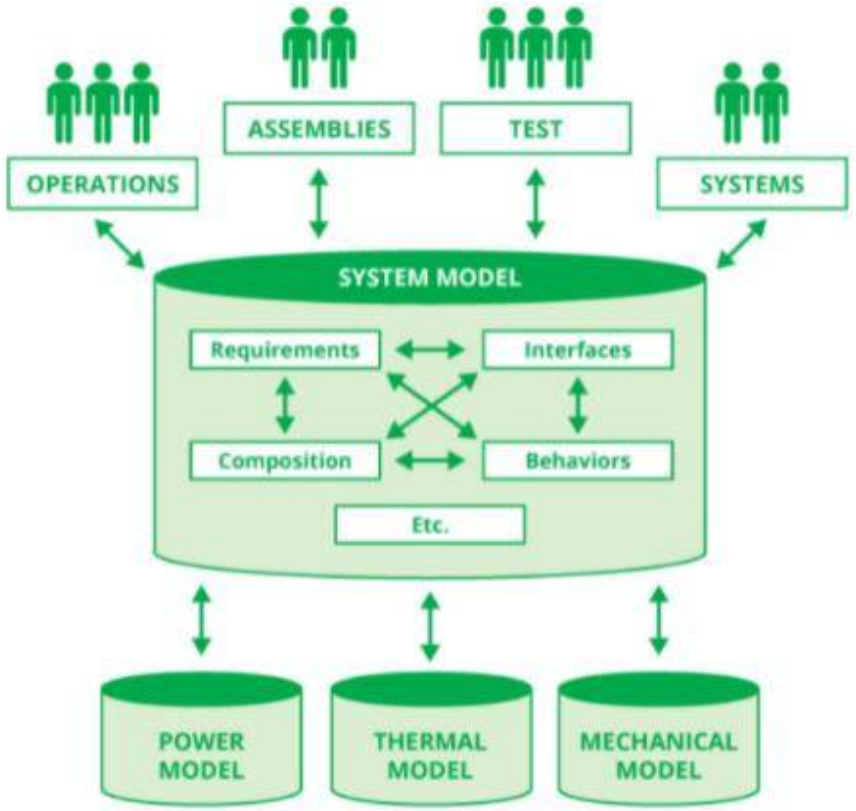
Un modèle est utilisé comme source unique pour toutes les parties prenantes afin de décrire l'évolution de la conception du système tout au long du cycle de vie du produit.

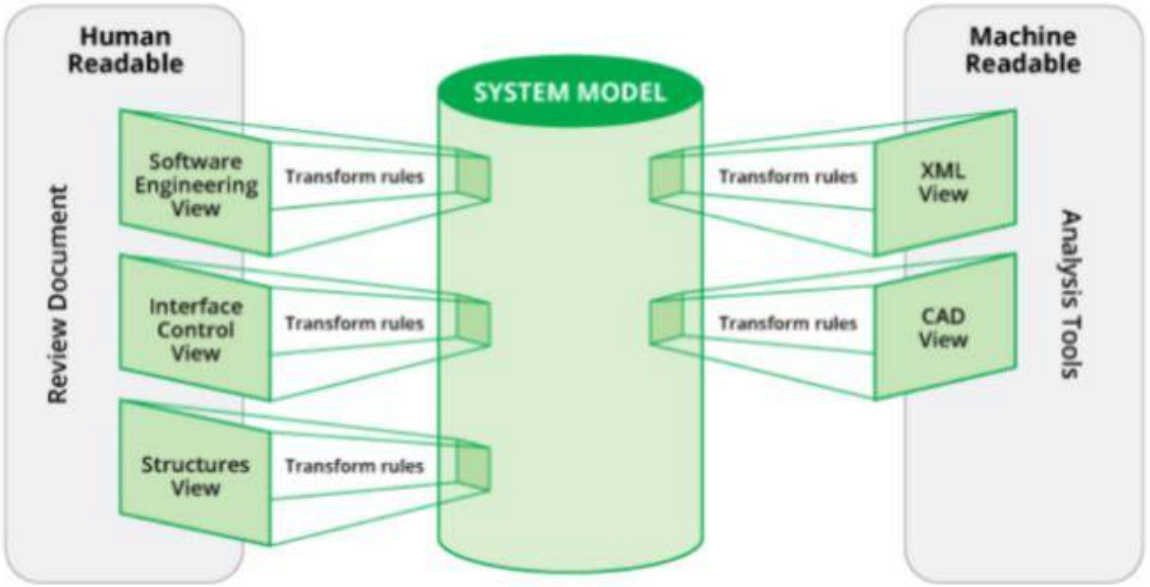



- + **Améliore la communication inter-métier**
- + **Améliore la productivité**
- + **Améliore la qualité**
- + **Support à l'intégration**
- + **Gère la compléxité**
- + **Facilite la réutilisabilité**

Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

# Pourquoi MBSE ? (2)




Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

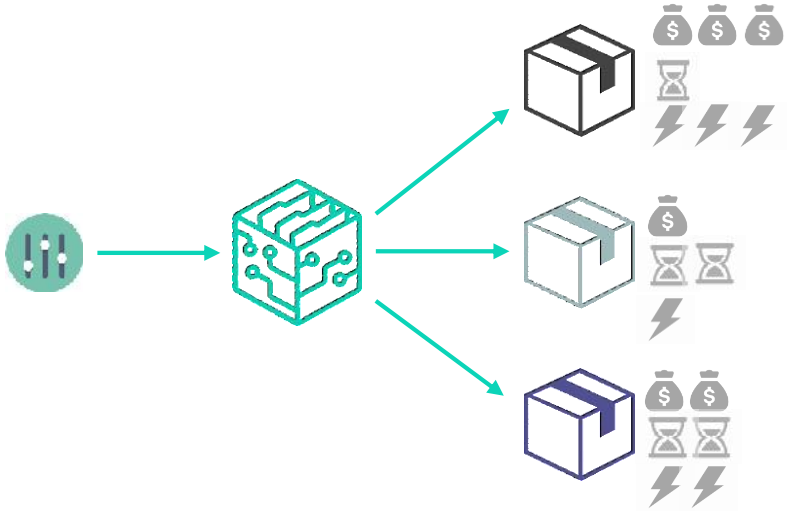
# Cas concret (1)

## Model as a support for decision making

A model allowed us to store in a single location several system configurations.

It comprised of a dozen sub-components. This setup enables the insertion of new configurations.

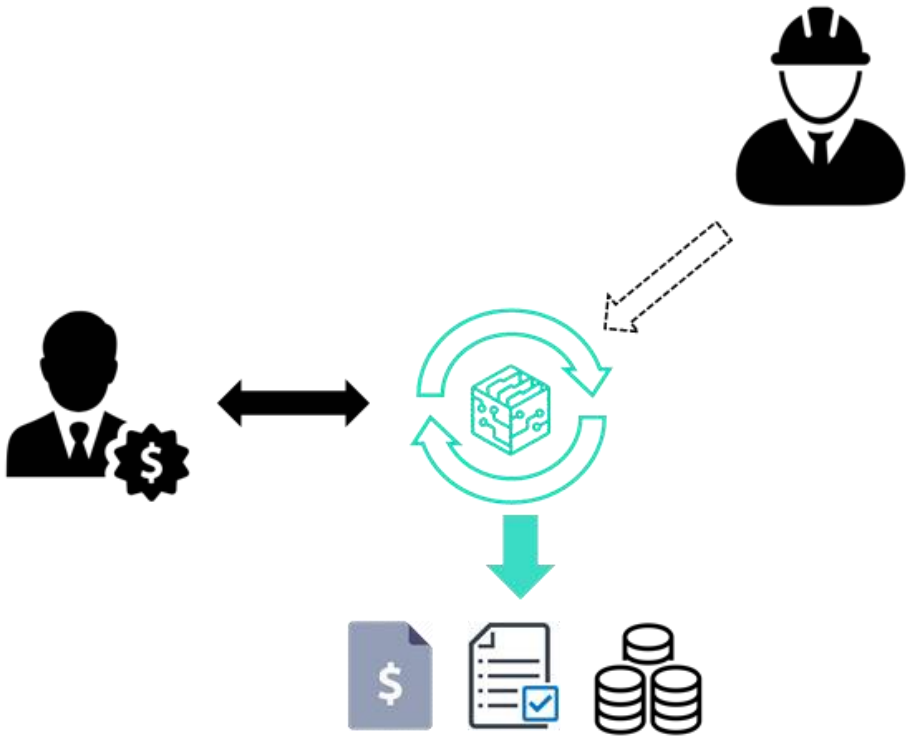
Simulation between all configuration through the model enables the owner to find trade-off based on selected criteria and achieve the best solution.



# Cas concret (2)

## Model as a support for sales

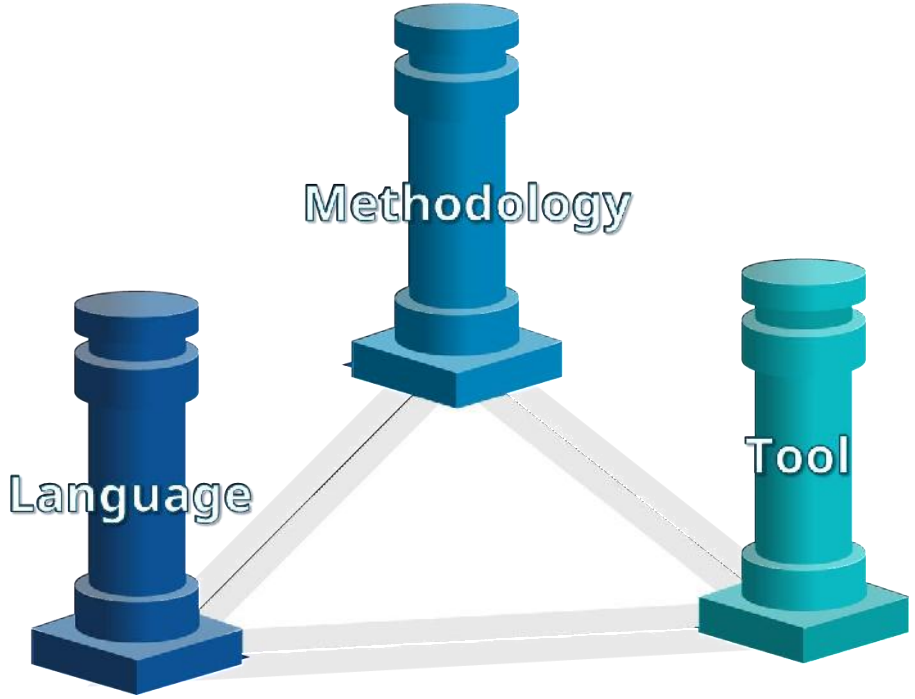
- Allow sellers to make more detailed offers
- To guarantee the feasibility of the offers from a technical point of view
- Acquire  up to date and useful external data
- Automatic document generation and digitization of information



# MBSE – Concept clés (1)

MBSE est basé sur trois piliers :

1. Méthodologie
2. Language
3. Outils

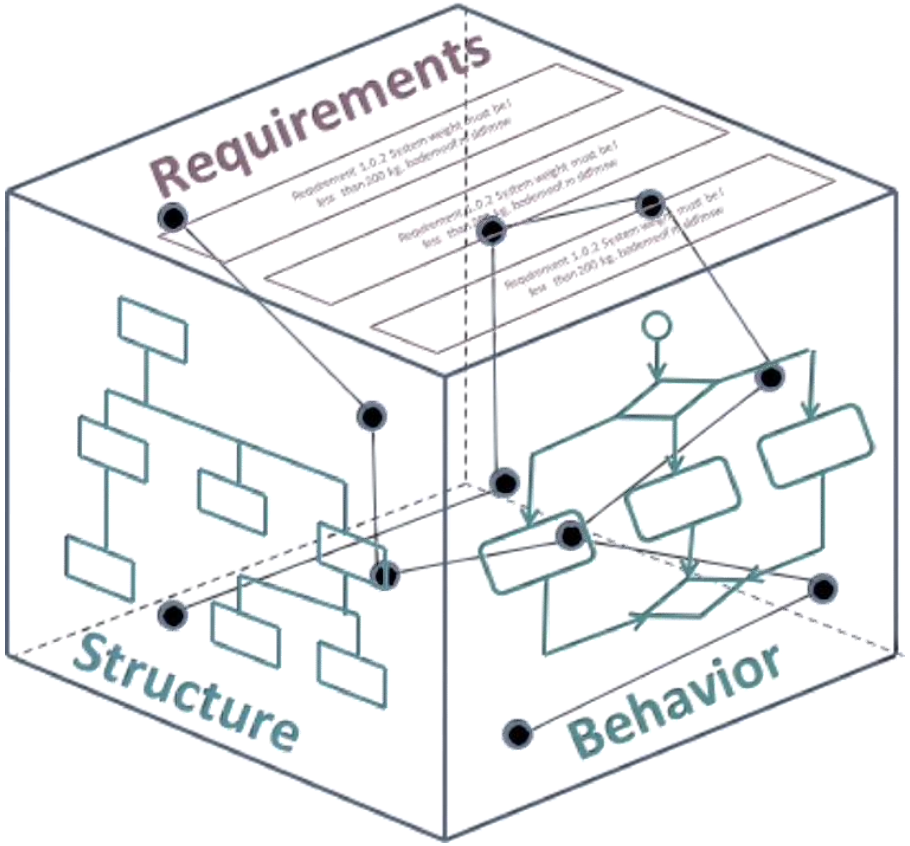


# MBSE – Concept clés (2)

Selon MBSE, un modèle doit représenter trois «vues»

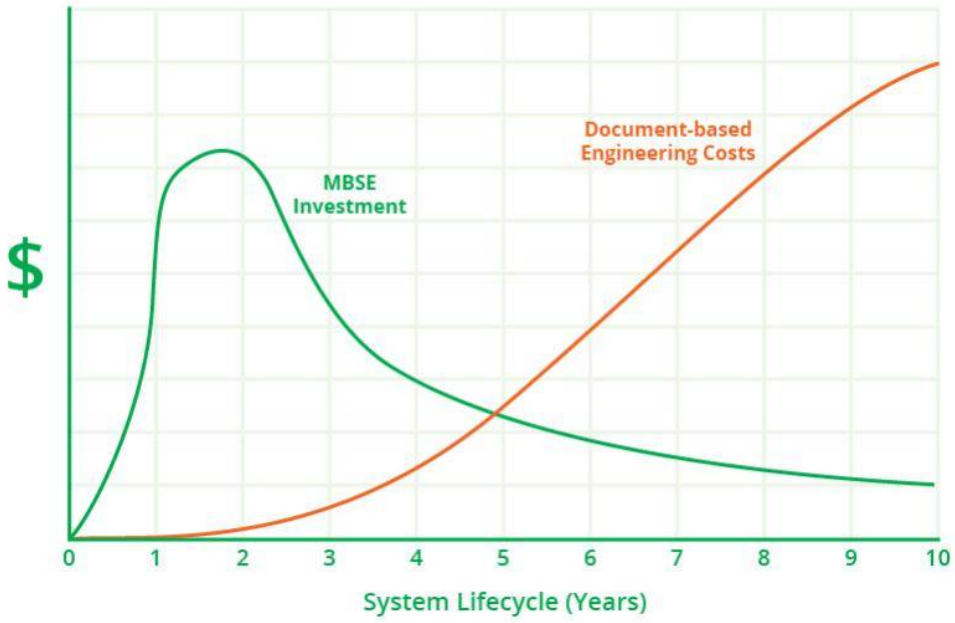
1. La structure
2. Le comportement
3. Les exigences

!! Mais également les liens entre ces éléments par le principe d'allocation.



# MBSE Challenges and Benefits

- Intégration de l'existant dans les modèles
- Quantité de données à traiter par le modèle
- Investissement pour l'implémentation d'une approche MBSE
- Création de la compétences auprès des employés
- Définition et adoption des processus dans les différentes équipes.
- Formation au processus, languages et outils MBSE




Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

# Les systèmes

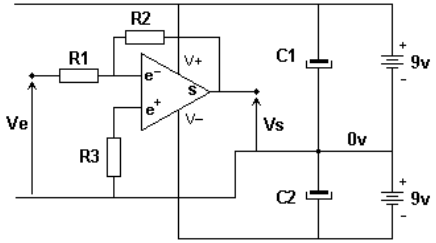
# Les systèmes - Définition

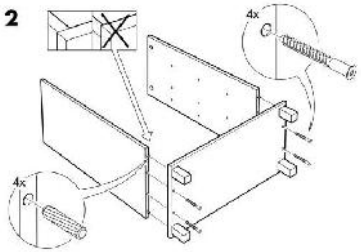
1. *Un système est un ensemble d'éléments interagissant entre eux selon certains principes ou règles. Un système est déterminé par sa frontière, sa mission, ses interactions avec son environnement, ses fonctions, ses ressources* (Wikipedia)

2. *Un assemblage ou collection organisée (possédant une structure) d'objets reliés les uns aux autres, de façon à former une entité et en relation avec le milieu extérieur dans le but de remplir une ou plusieurs fonctions.* (Analyse des systèmes – Giroux)

*3. A system is an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. (INCOSE)*

# Les systèmes - Définition

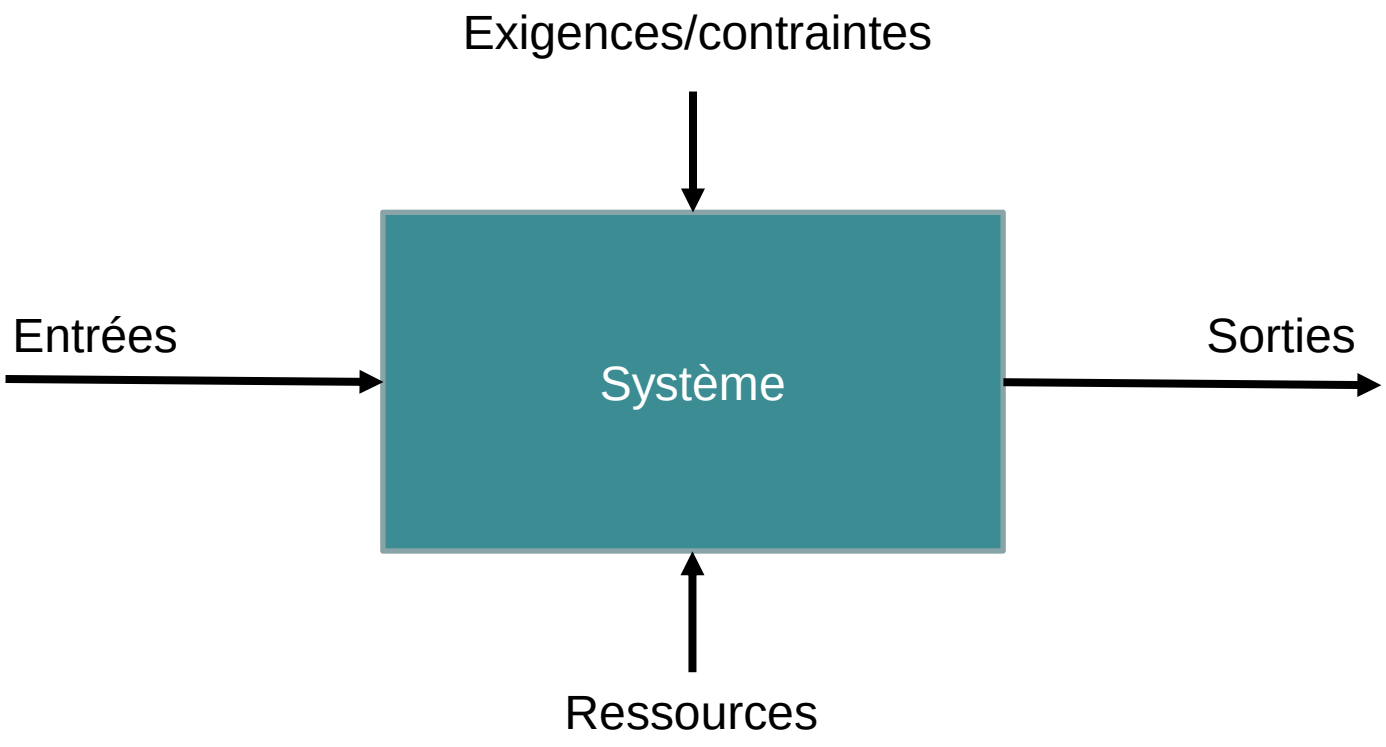




# Les systèmes - Définition

Un système est un objet qui répond à une finalité dans un environnement donné.

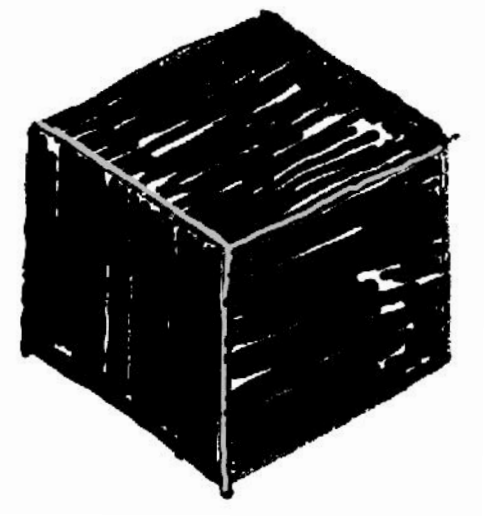
- Flux sortant
- Flux entrant



# Les systèmes – Représentation Black-Box

En «black-box», le système est considéré comme vu depuis l'**extérieur** uniquement.

Seuls les systèmes et son environnement peuvent être appréhendés.

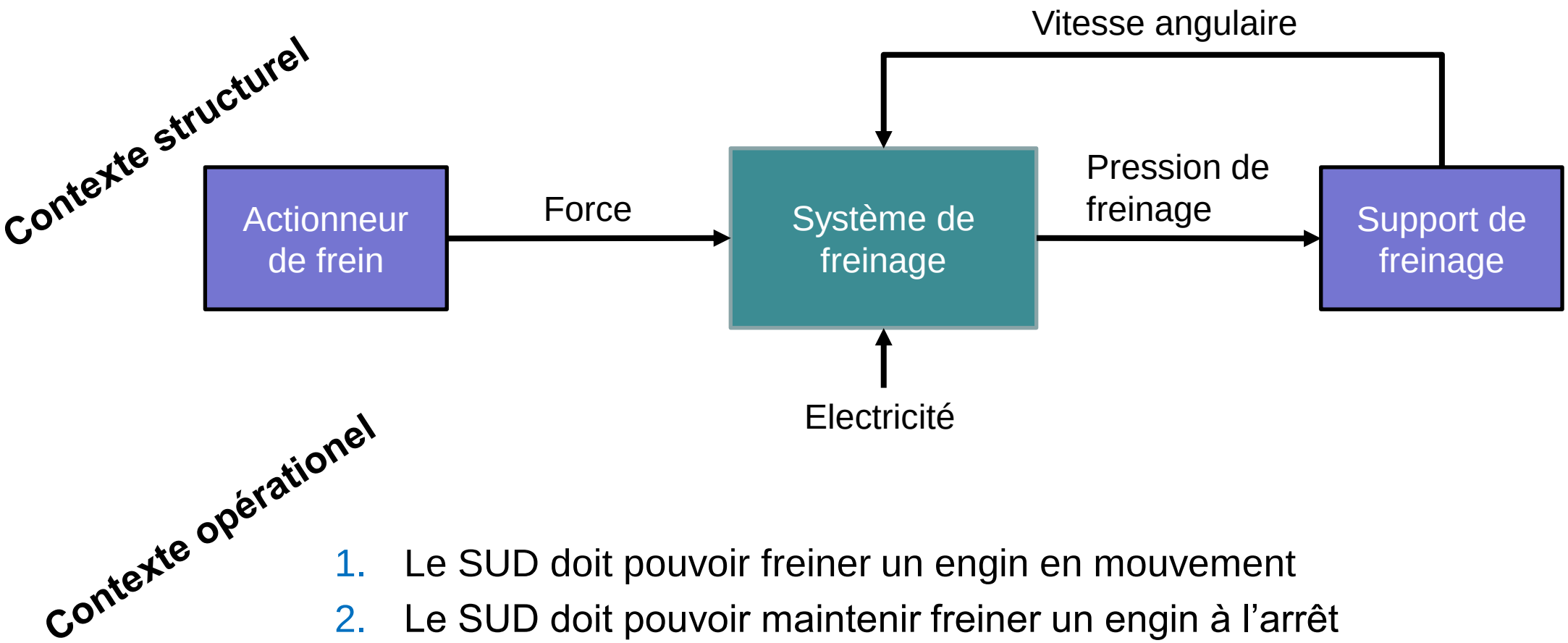


À définir :

- Le contexte structurel (les interactions avec l'environnement)
- Le contexte opérationnel (les cas d'utilisation)

# Les systèmes – Représentation Black-Box – Exemple

Exemple : Un système de freinage

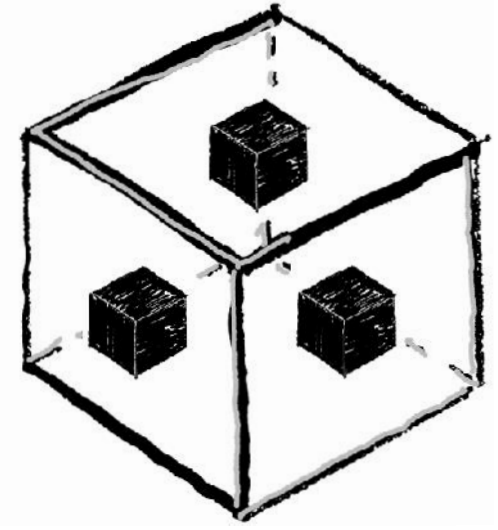



1. Le SUD doit pouvoir freiner un engin en mouvement
2. Le SUD doit pouvoir maintenir freiner un engin à l'arrêt

# Les systèmes – Représentation White-Box

En «white-box», le système est considéré comme vu depuis l'intérieur uniquement.

L'analyse white-box considère les fonctions du système ainsi que les sous-systèmes.

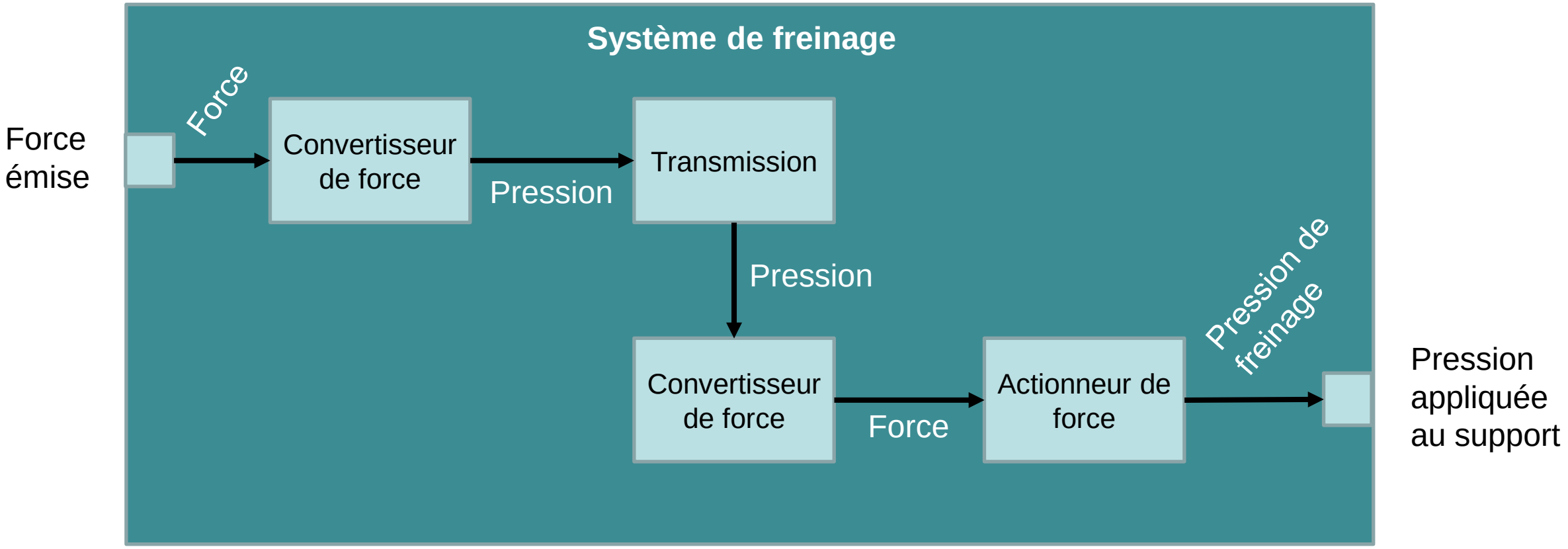


À définir :

- Les sous-systèmes
- Les interactions entre les sous-systèmes
- Les interactions des sous-systèmes avec l'extérieur
- Les fonctions du système et leur allocation aux sous-systèmes

# Les systèmes – Représentation White-box – Exemple

Exemple : Un système de freinage hydraulique



# Les systèmes – Représentation White-box – Exemple (2)

Exemple : Un système de freinage hydraulique

1. Fonction 1 – Le SUD doit convertir la force d'actionnement en pression hydraulique
   → Allouée au convertisseur de force d'entrée

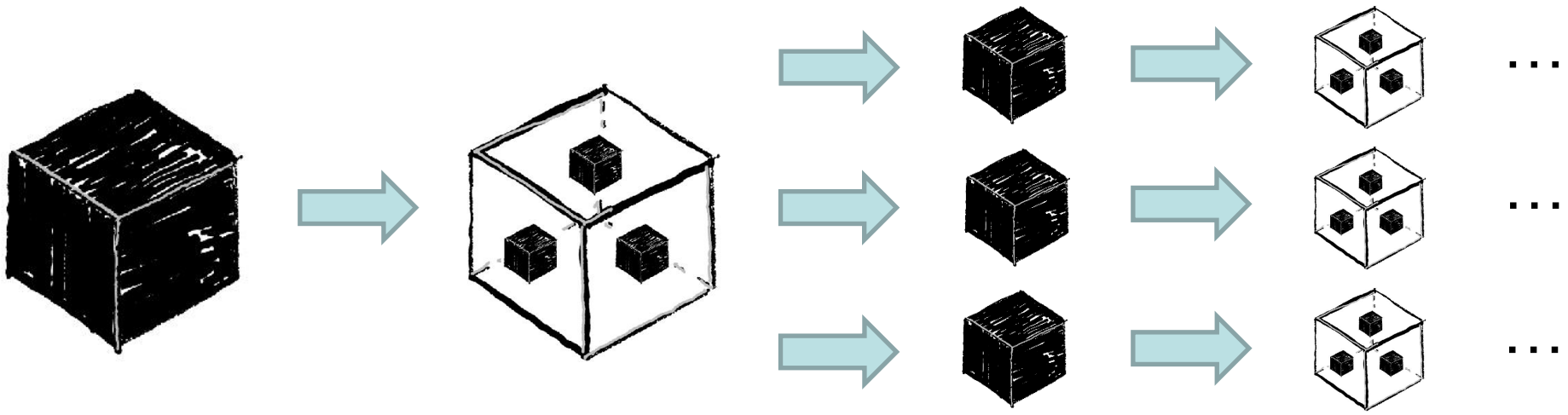
2. Fonction 2 – Le SUD doit transférer la pression
   → Allouée au block de transmission

3. Fonction 3 – Le SUD doit convertir la pression hydraulique en force de freinage
   → Allouée au convertisseur de force de sortie

4. Fonction 4 – Le SUD doit appliquer une pression sur le support de freinage
   → Allouée à l'actionneur de force

# Les systèmes – Représentation itérative

- Un système peut être considéré comme une boite noire.
- Un système peut être considéré comme une boite blanche. Les sous-systèmes sont définis.
- Ces sous-systèmes sont considérés comme boite noire à ce niveau.



# Exercice

- Réalisez une analyse Black/White-box d’un système de votre choix.

- Système : de votre choix (travail de bachelor, travail en cours, autre).
- Niveau d’abstraction : au moins 1
- Méthode : de votre choix

# Exercice pour le 21.11.2021

Compléter l’exercice commencé en classe et le rendre jusqu’à dimanche 21.11.2021 – 23h59 sur le dépôt d’exercice ouvert sur Moodle.

Vous pouvez commencer tout de suite

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

| | | |
|---|---|---|
| 28 | Luc Riedhauser | ISO 4210 Sécurité des bicyclettes |
| 29 | Beltus Mbanjei | Vérification et validation ? Différence et signification |
| 30 | | Les méthodes de verification et validation |
| 31 | | Les types d'exigence |
| 32 | | Les méthodes, outils et language du MBSE |

Tableau des présentations

# Merci pour votre attention

Questions ou remarques: frederic.schenker@hefr.ch ou via Teams

Sécurité et fiabilité des systèmes (SecuFS)

# 09 – Processus de développement des systèmes techniques – Partie 2

Frédéric Schenker

22.11.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | 31.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours

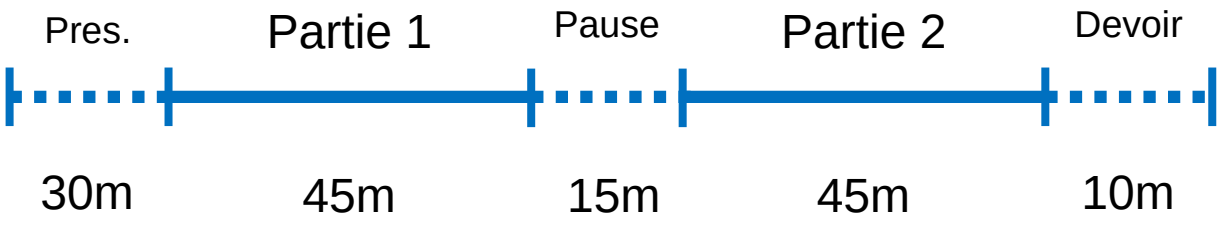
**Structure du cours:**

**Partie 1** : 15 novembre 2021
Objectif général : Introduction à l’ingénierie système et ces processus

**Partie 2** : 22 novembre 2021
Objectifs : L’ingénierie système basée sur les modèles et son application

**Partie 3** : 29 novembre 2021
Objectifs : Workshop

# Format du cours




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

| | | |
|---|---|---|
| 28 | Luc Riedhauser | ISO 4210 Sécurité des bicyclettes |
| 29 | Beltus Mbanjei | Vérification et validation ? Différence et signification |
| 30 | | Les méthodes de verification et validation |
| 31 | Sébastien Deriaz | La sécurité dans l'escalade |
| 32 | | Les méthodes, outils et language du MBSE |

Tableau des présentations

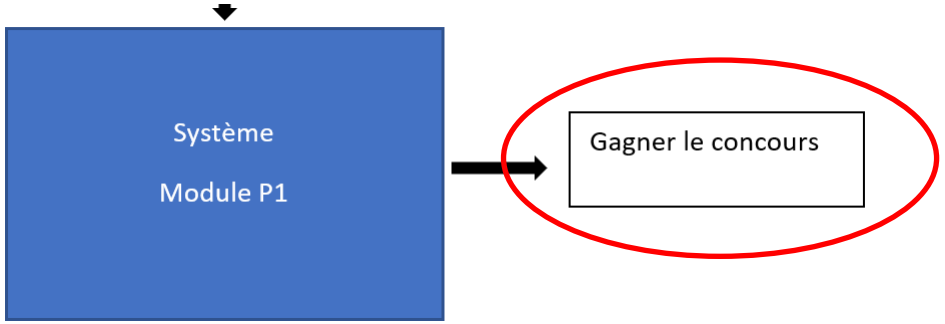
# Retour sur l'exercice (1)

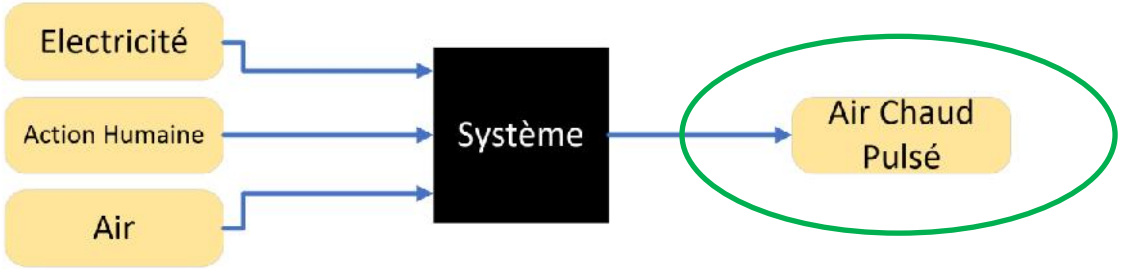
- Rester générique

3. Mesure de l'état de charge de la batterie (leds)

Mesurer l'état de charge de la batterie
→ Allouer au ruban de leds

- Ne pas confondre objectif et sortie de système



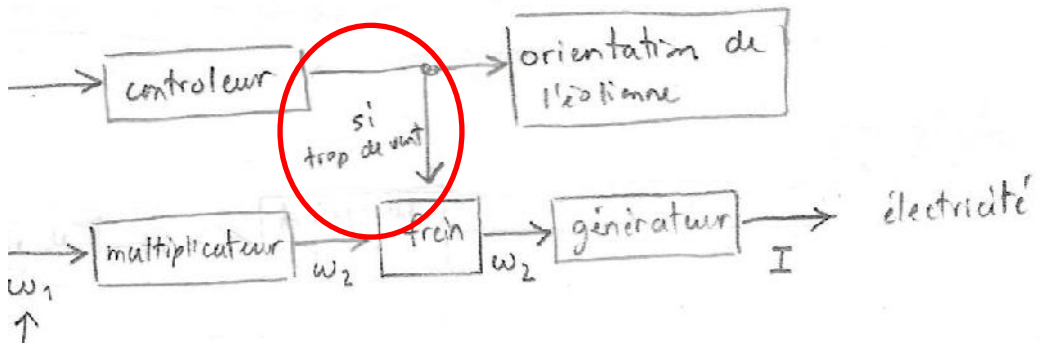

- Choix des mots : une fonction doit être décrite par un verbe.

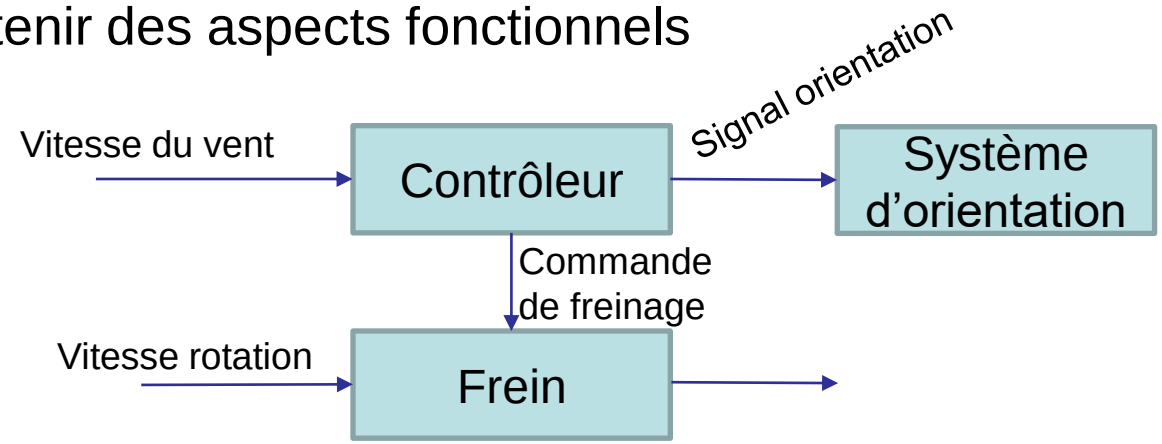
1. Gestion de la charge : Régulation de la tension d'entrée pour l'adapter à une charge de batterie
2. Gestion de la décharge : Adaptation de la tension de batterie pour la rendre utilisable
3. Surveillance de la température : Protection du système dans le cas ou la batterie serait défaillante (ou si elle est soumise à des températures trop élevées)

Fonction 1 : **Gérer la charge (de la batterie)**
Description : Régulation de la tension d'entrée pour l'adapter à une charge de batterie.

# Retour sur l'exercice (2)

- Une représentation structurelle ne doit pas contenir des aspects fonctionnels




- Contexte opérationnel vs contexte fonctionnel

Operational Context:

1. The filter system shall receive and work with sea water from a pump.
2. The filter system shall accept filter disks for sampling the sea water of microplastics.
3. The filter system shall eject the sea water once it is processed.
4. The filter system shall transfer the processed microplastic sample into a storage unit.

**Exigences**
Le système de filtrage doit recevoir de l'eau de mer depuis une pompe.

**Fonction**
Recevoir de l'eau de mer

**Opération**
Lorsque de l'eau de mer est reçu, le système de filtrage doit se mettre en activité

# Retour sur l’exercice (3)

**Exigence fonctionnelle**

L’élément doit pouvoir être localisé

**Exigence de performance**

La localisation doit avoir une précision d’au moins 5 mètre

**Exigence opérationnelle**

Lorsqu’ils sont en marche, la position de chaque élément appartenant au contexte doit être monitoré.

# Objectifs du cours

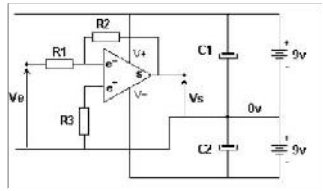
- La décomposition d’un système
- Les piliers du MBSE
- System Thinking par OPM
- L’ingénierie des systèmes basée sur le modèle (MBSE)
- Les systèmes

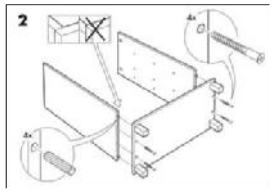
# La décomposition d’un système

# Le système - Rappel

**Définition**

*A system is an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. (INCOSE)*





Un système est défini par sa **fonction** et par sa **forme**.

# La fonction du système (1)

**La fonction** du système est toutes les activités, opérations et transformations que le system produit. C'est les actions pour lesquels le système existe or pour lequel il est employé. Il n'y a aucun lien avec la forme du système.

**«What the system does»**

**Fonction = Process + Operands**

Pour comprendre un système, il faut identifier sa fonction principale ou son «emergence»

**Un vélo ou une voiture ont la fonction d'être des moyens de transport.**

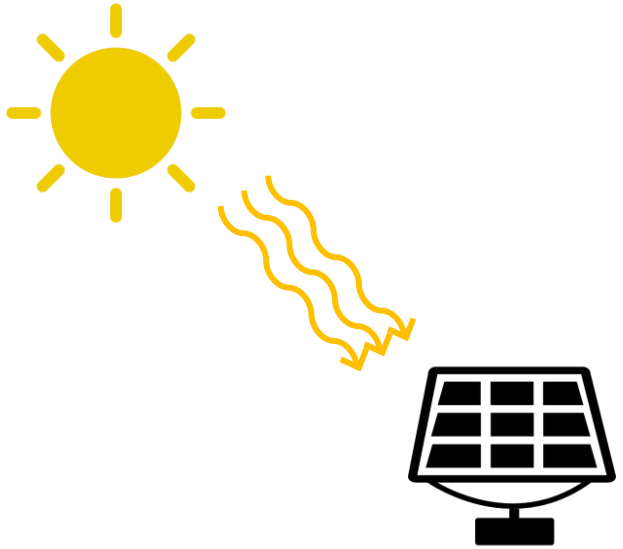
Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

# La fonction du système (2)

**La fonction** du système est toutes les activités, opérations et transformations que le system produit. C'est les actions pour lesquels le système existe or pour lequel il est employé. Il n'y a aucun lien avec la forme du système.

**«What the system does»**

**Fonction = Process + Operands**



| Produce energy | = | Photon | + | Atomic Transforming |
|---|---|---|---|---|

Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

# La fonction du système (3)

Que pensez-vous d'un briquet ? Quelle est l'emergence ici ?

L'emergence du briquet est de produire un flamme.

Décapsuler une bière, illuminer un espace ou allumer un feu de camping sont des fonctions secondaires. Elles sont apparues grâce à l'évolution de la forme du briquet.

1823 - DÖBEREINER'S LAMP

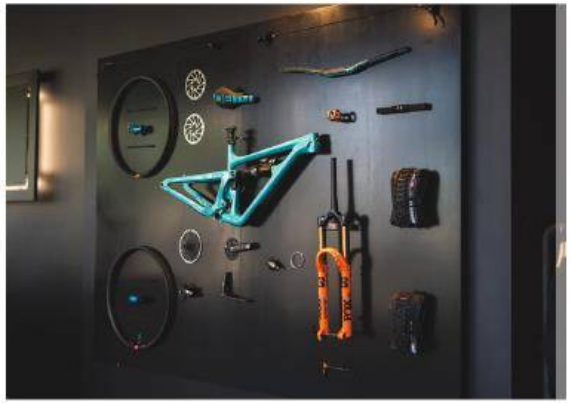
1973 - THE BIC DISPOSABLE LIGHTER

# Forme du système

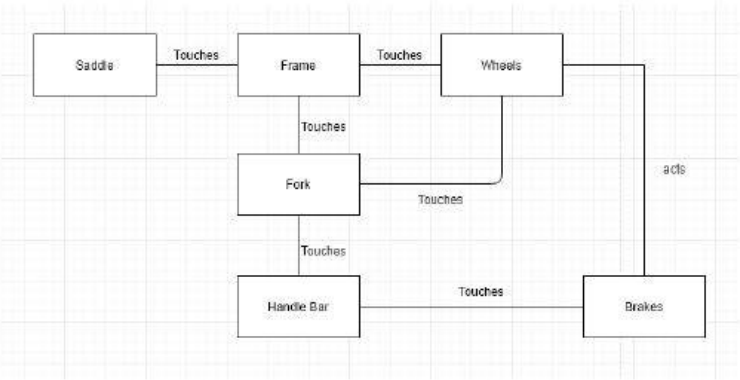
**La forme**, un instrument de la fonction, est un attribut du système qui incarne un élément physique ou informel qui existe ou a le potentiel d'exister. La Forme peut être décomposé en objet, et ces objets peuvent avoir des relations ou une structure.

**«What the system is»**

**Forme = Object + Structure**



+



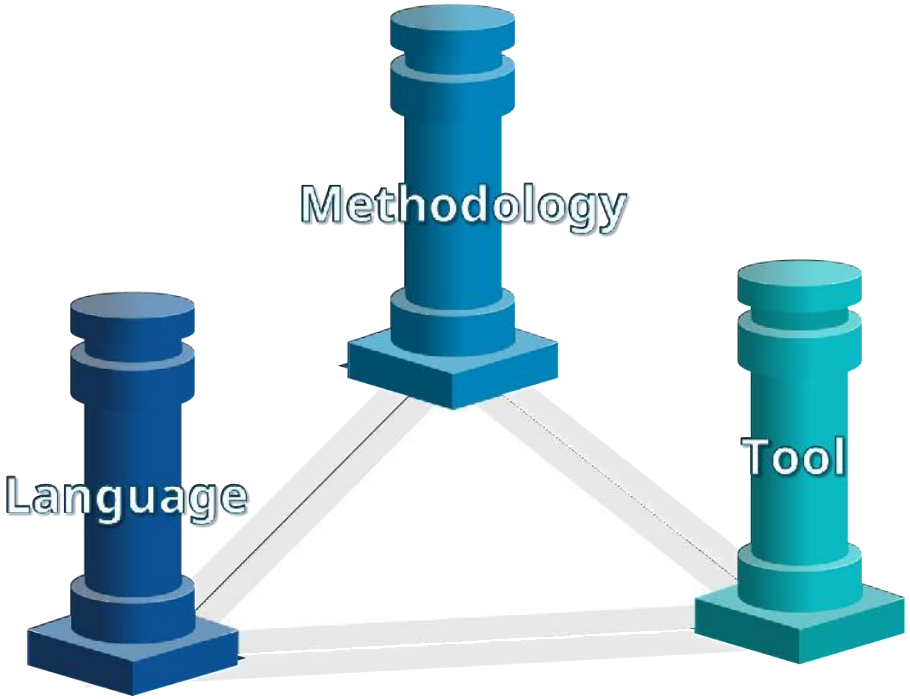

=

# Les piliers de MBSE

# MBSE – Concept Clés

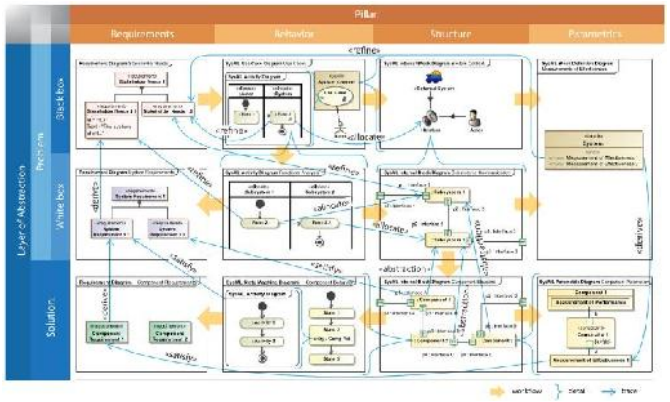
MBSE est basé sur trois piliers :

1. Méthodologie
2. Language
3. Outils

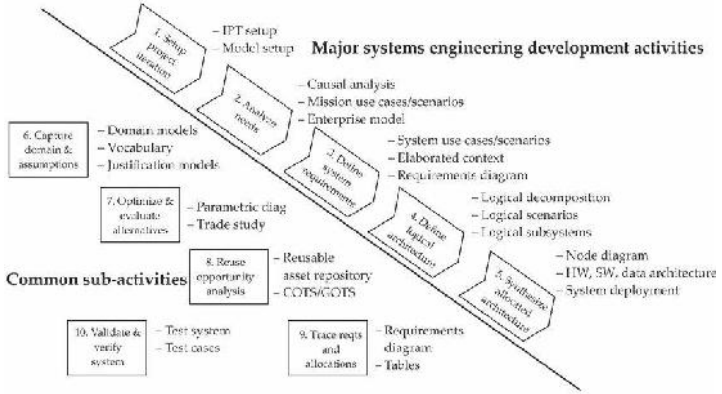


# Les méthodes

Architecture, Analysis & Design Integrated Approach

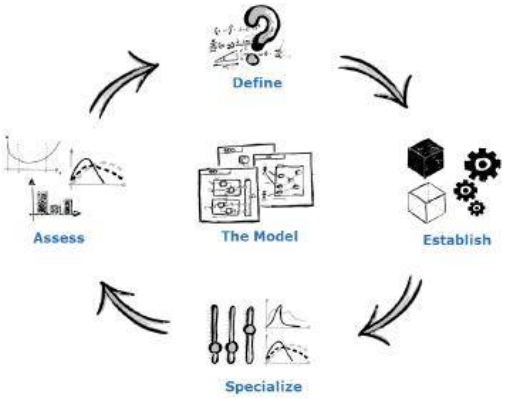


MagicGrid




Object-Oriented Systems Engineering Method (OOSEM)

Object Process Methodology (OPM)




ROSAS Methodology

# Les langages

ARCADIA

Architecture, Analysis & Design Integrated Approach

Architecture Analysis and Design Language (AADL)

System Modeling Language (SysML)

Object-Process Methodology ISO 19450

Object Process Language / Object Process Diagam (OPL/OPD)

Unified Modeling Language (UML)

MathWorks

MathWorks Environment

# Les outils

Eclipse Papyrus

IBM Rational Rhapsody

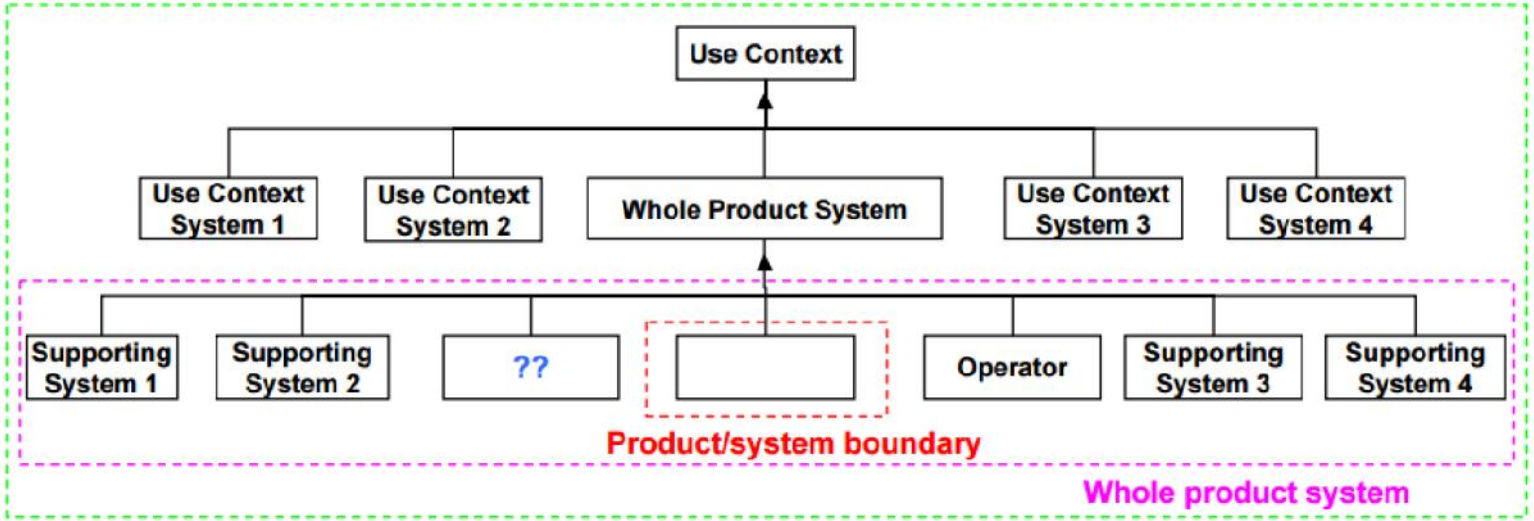
DrawIO

MathWorks Environment

MagicDraw

# System Thinking par OPM

# System Thinking – Approche Structurelle (1)



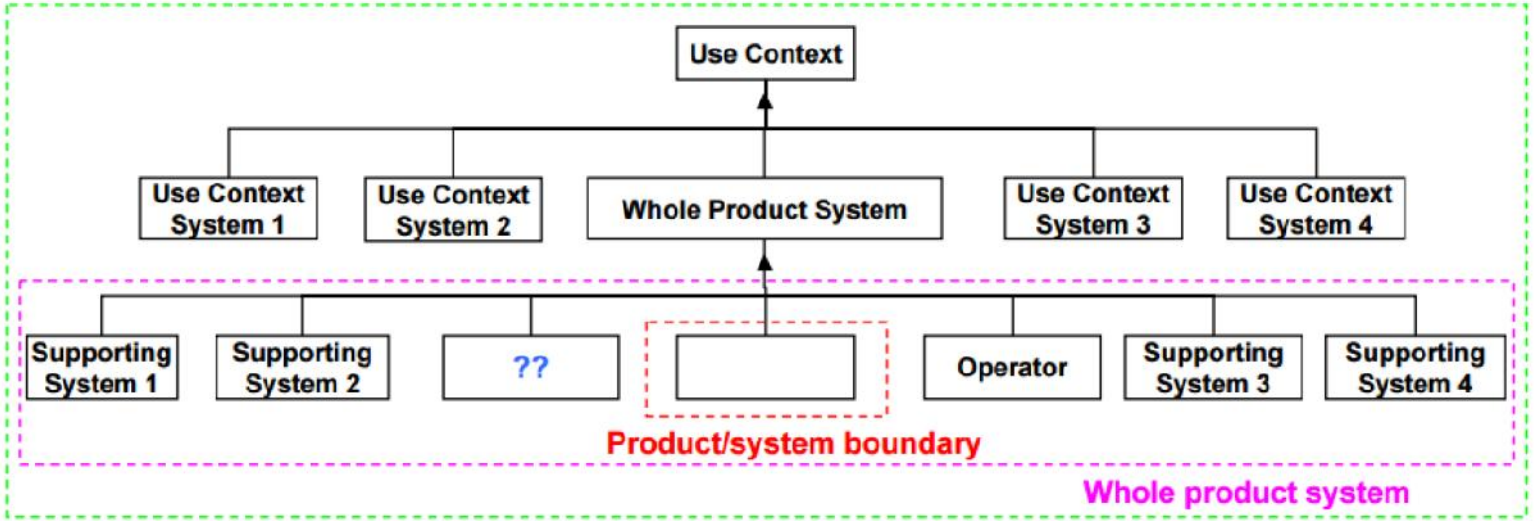

L'ensemble du produit comprend le produit/Système et les systèmes accompagnants

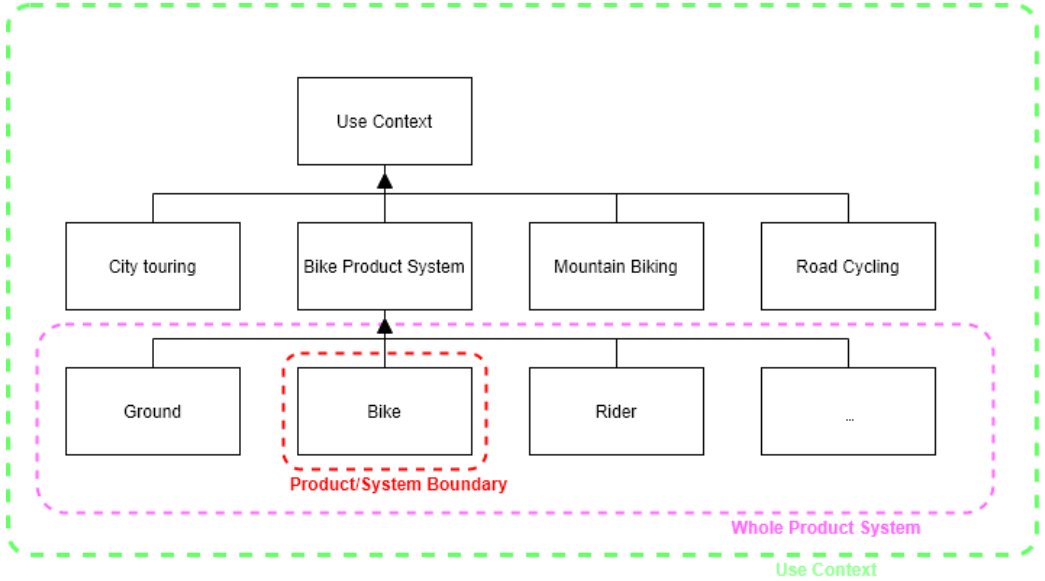
L'ensemble du produit figure dans un contexte d'utilisation, qui inclut les objets normalement présents quand le système opère, mais qui ne sont pas nécessaire pour que le système fonctionne.

Le produit/system interface avec les objets dans l'ensemble du produit, mais pas avec les objets du contexte d'utilisation.
L'ensemble du produit est généralement indépendant tandis que le contexte d'utilisation est dépendent du contexte.

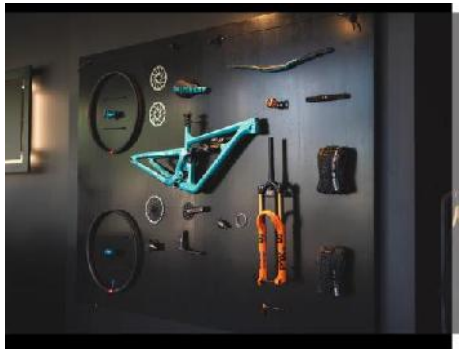
Sources: Architecture and Systems Engineering : Models and Methods to Manage Complex Systems, Massachusetts Institute of Technology xPRO, Professional Certificate Program, Bruce Cameron

# System Thinking – Approche Structurelle (2)

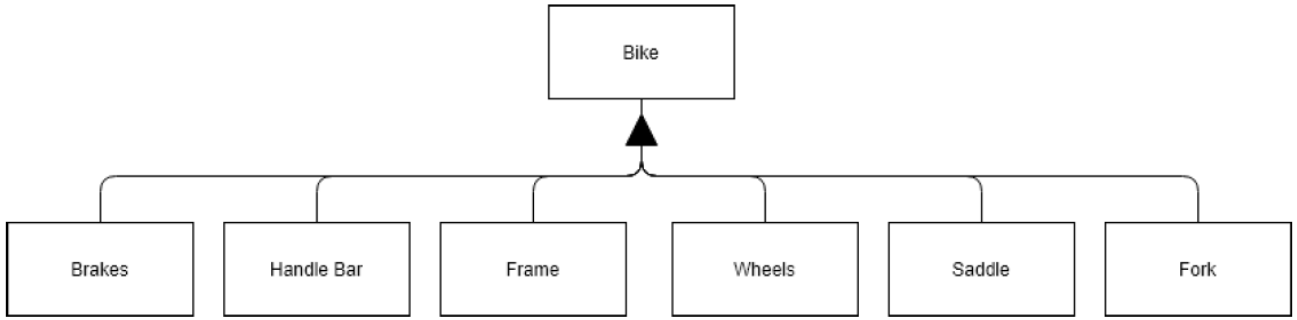


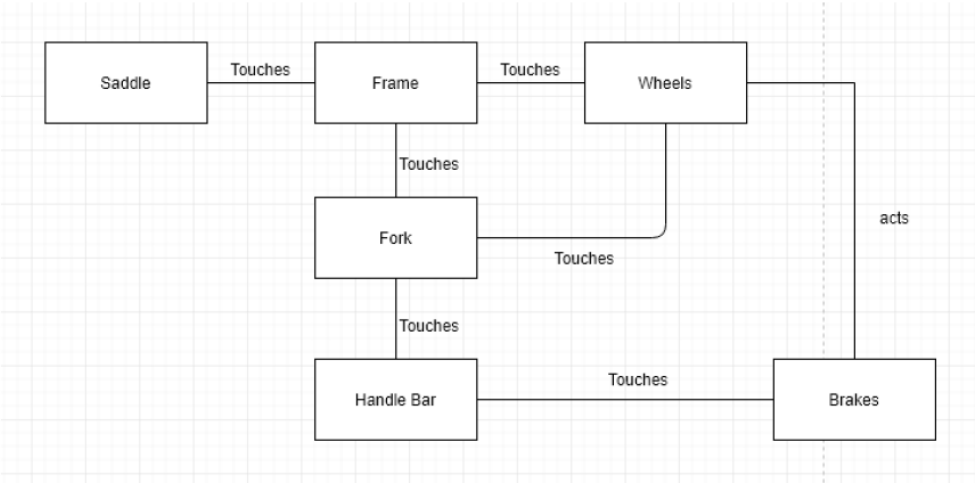


# System Thinking – Approche Structurelle - Example



Structure par OPM :



# System Thinking – Approche Fonctionnelle (1)

Décrire la fonction par OPM

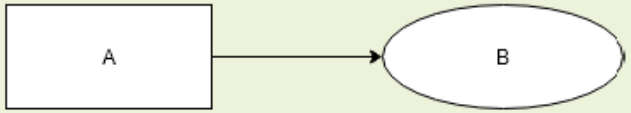
**OPM** (Object Process Methodology)

**Operand** is something that is changed by a process. It is the thing whose change in state is associated with value.

**Process** is transformation over time applied to one or more objects. Generally, processes are creating, destroying, or changing something

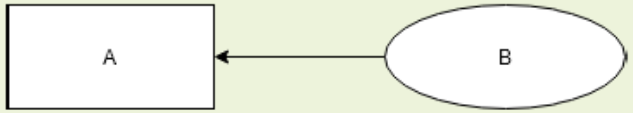
**Consumption Link**

**B** consumes **A**



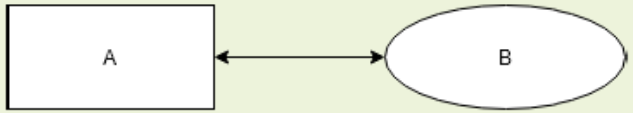

**Result Link**

**B** yields **A**




**Effect Link**

**B** affects **A**




Sources: OPM, Object Process Methodology, Wikipedia
Model-Based Systems Engineering with OPM and SysML, Dov Dori, Springer

# System Thinking – Approche Fonctionnelle (2)

Lier la fonction à la forme par OPM (allocation)

**OPM** (Object Process Methodology)

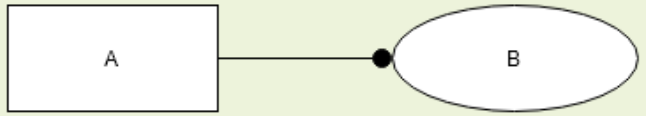
**Operand** is something that is changed by a process. It is the thing whose change in state is associated with value.

**Process** is transformation over time applied to one or more objects. Generally, processes are creating, destroying, or changing something

Agent is a human or group of humans

**Agent Link**

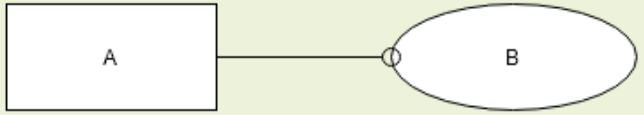
**A** handles **B**




Instrument is an inanimate object

**Instrument Link**

**B** requires **A**

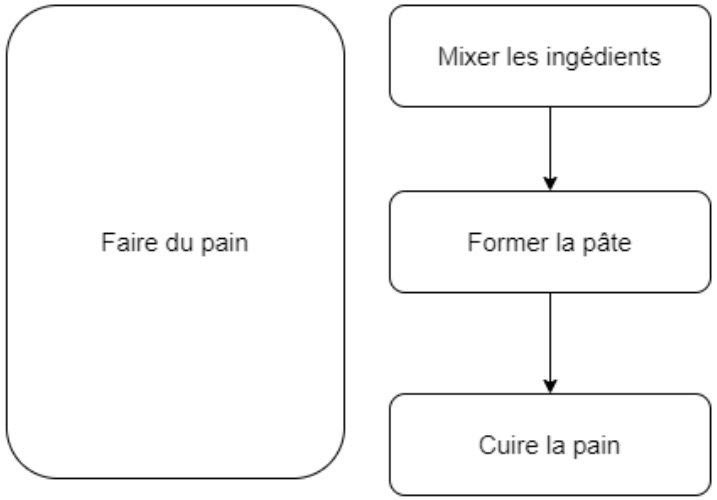



Sources: OPM, Object Process Methodology, Wikipedia
Model-Based Systems Engineering with OPM and SysML, Dov Dori, Springer

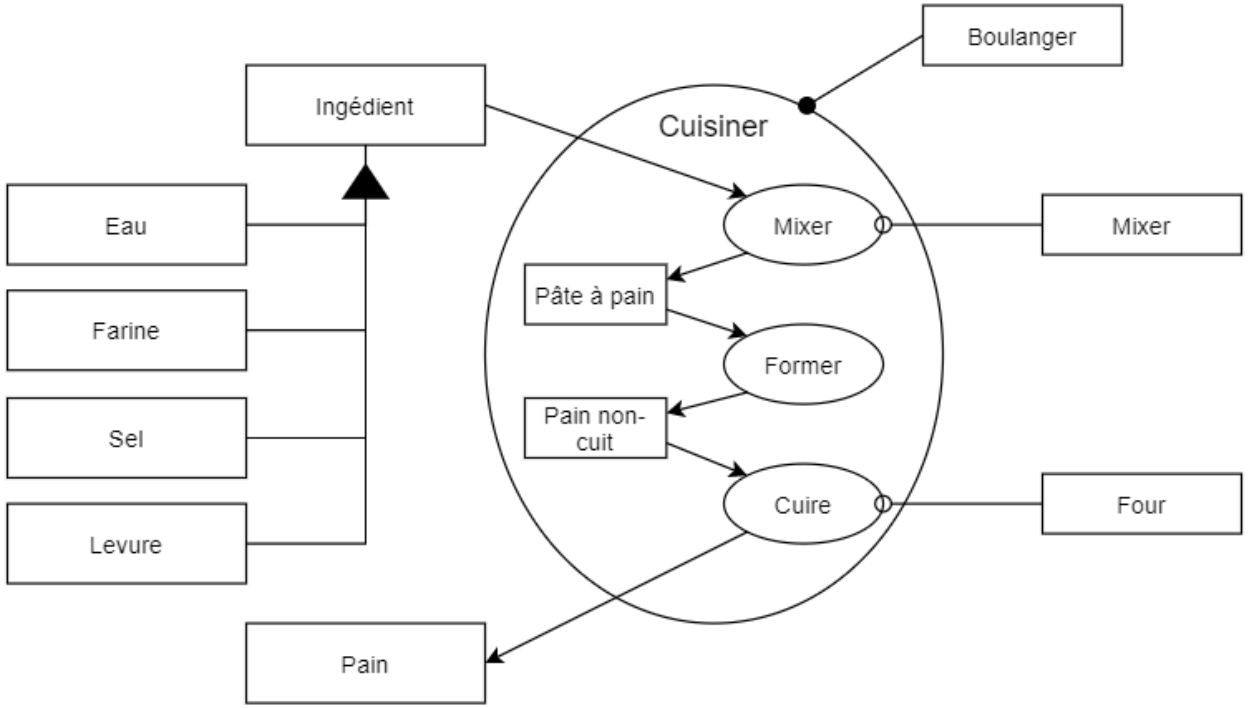
# System Thinking – Approche Fonctionnelle - Example

Faire du pain (simplifier !)

Vue fonctionnelle




Vue Process/Attributs

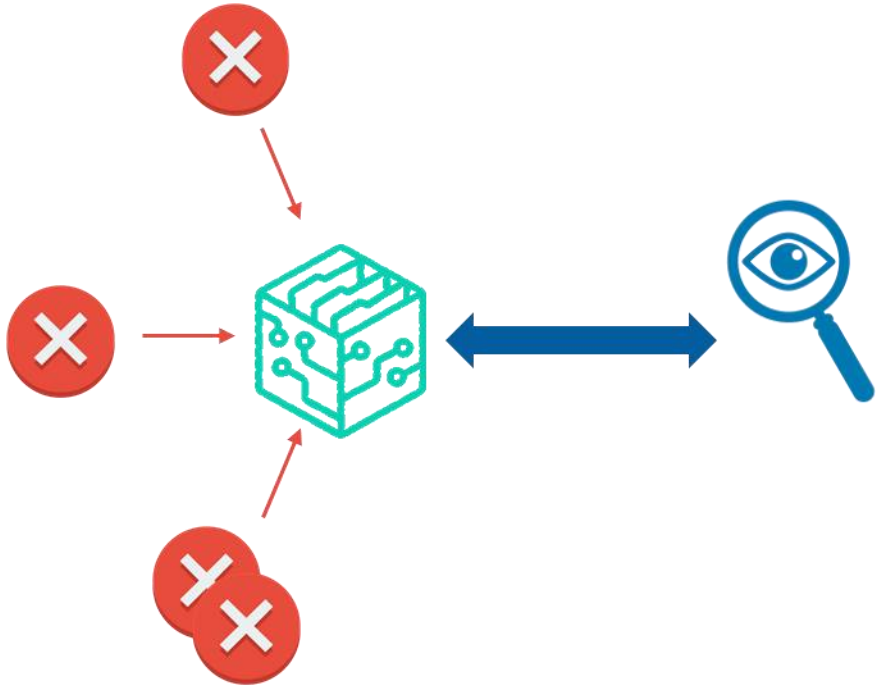


# Quelques applications concrètes du MBSE

# Safety Environment (1)

**Model as fault simulator**

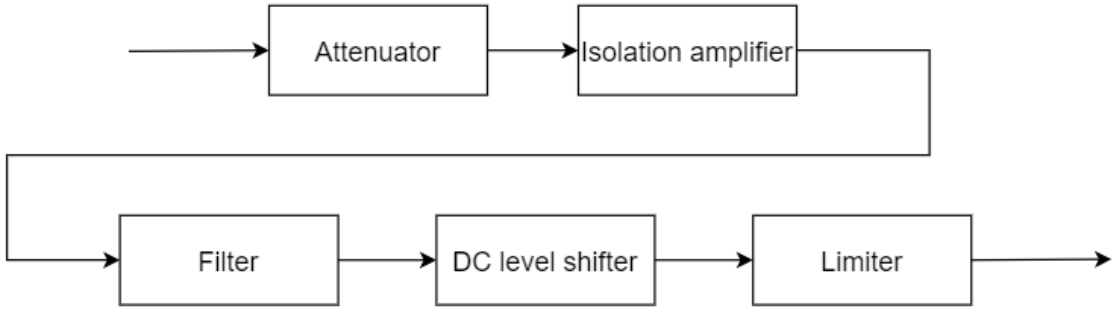
- Simulation of the nominal behavior of a system.
- Fault injection within the simulation of this model allows us to observe its reliability and to improve its design and operating processes.
- In addition, the generation of safety artifacts such as Failure Rate Calculation (FIT) becomes possible.



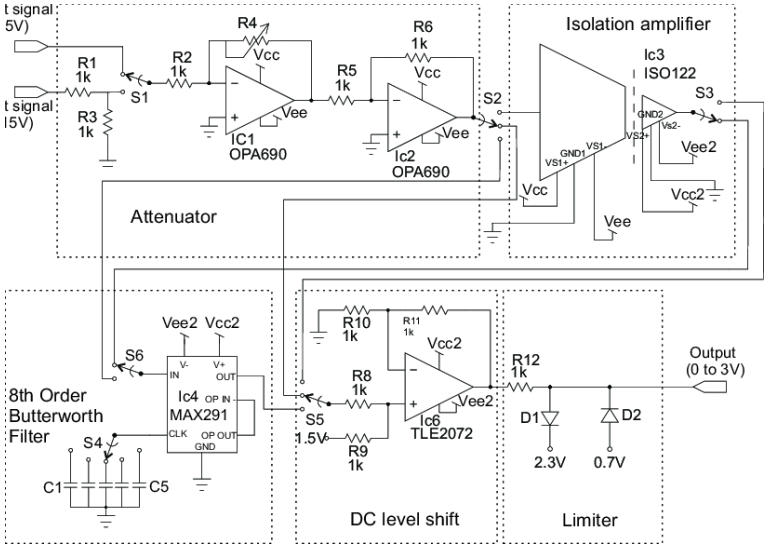
# Safety Environment (2)

## 1st granularity level

## 2nd granularity level

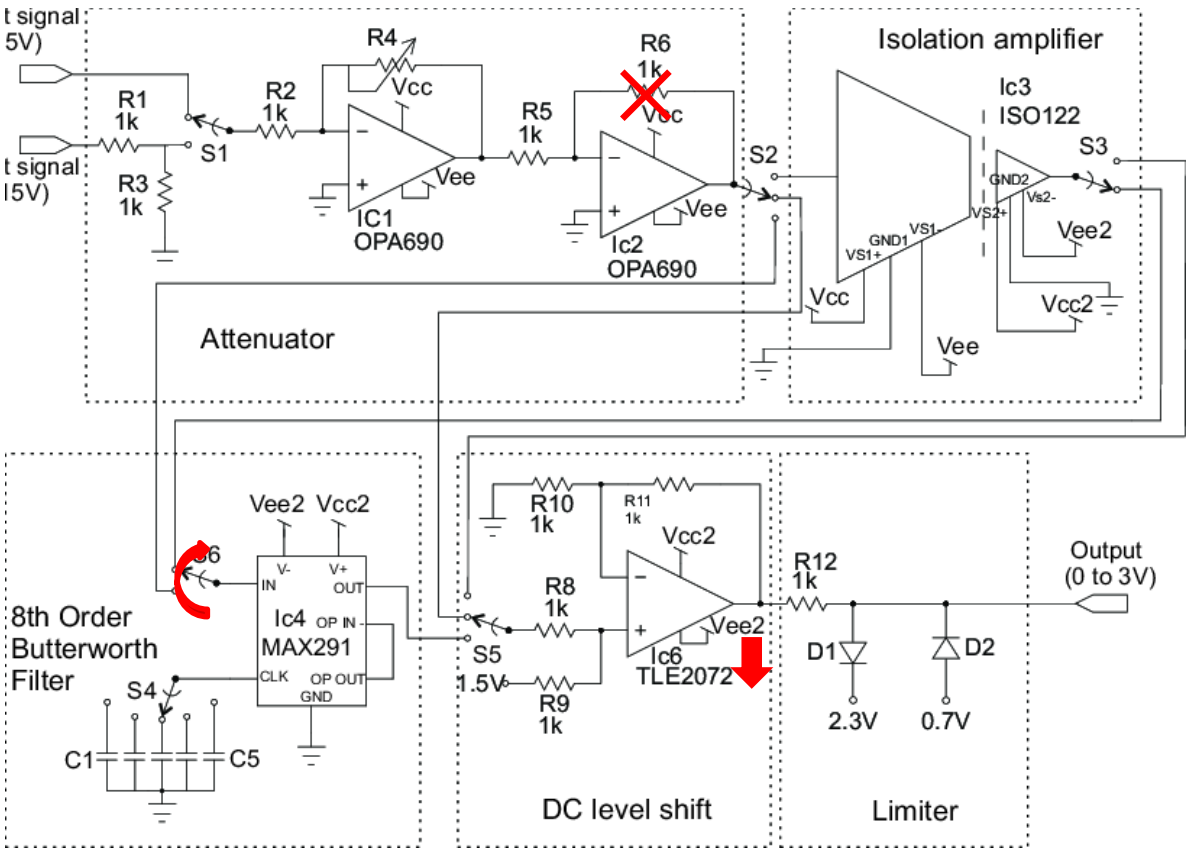



## 3rd granularity level




Sources: Diaz-Diaz, Irwin & Cervantes, Ilse. (2013). Design of a Flexible Analog Signal Conditioning Circuit for DSP-Based Systems. Procedia Technology. 7. 231-237. 10.1016/j.protcy.2013.04.029.

# Safety Environment (3)




Quelles est la cause de la perte de la résistance R6 (Open-circuit) ?

→ Au niveau de l'atténuateur

→ Au niveau du circuit de conditionnement

Quelles est la cause du blocage sur switch S6 (Stuck at …) ?

→ Au niveau du filtre

→ Au niveau du circuit de conditionnement

Quelles est la cause d'un abaissement de l'alimentation Vee2 (Drift) ?

→ Au niveau du filtre

→ Au niveau du circuit de conditionnement

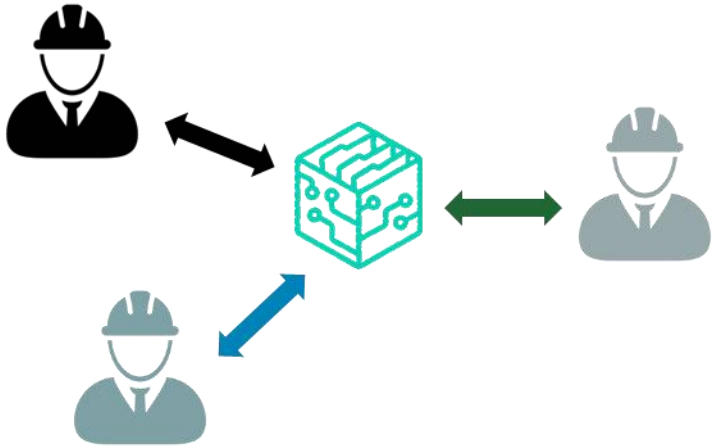
# Robotics description

**Model as a support for the design of a new robot**

The use of a model allowed us to optimize the understanding as well as the resolution of the mechatronic problems for one of our customers.

Our approach demonstrates that it is possible to reduce the engineering development time for the basic design by a factor 5 to 10.

Furthermore, the model has facilitated exchanges between the various stakeholders and the project has been better structured.



# Configuration Management (1)

**Model as a support for decision-making**

A model allowed us to store in a single location several system configurations.

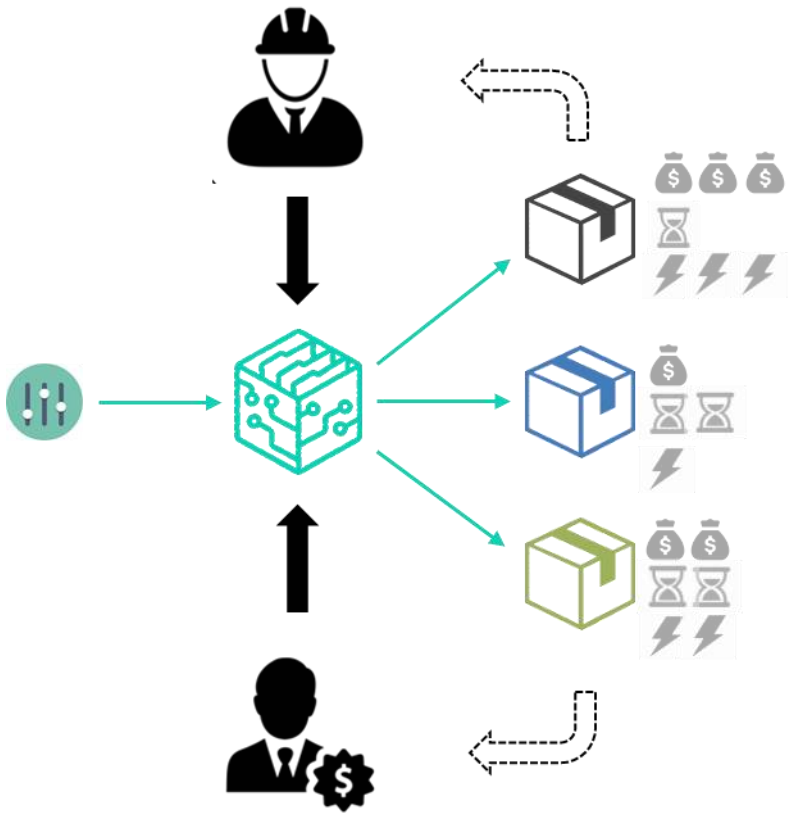
→ **Complexity management**

Both technical and business teams work on the same model.

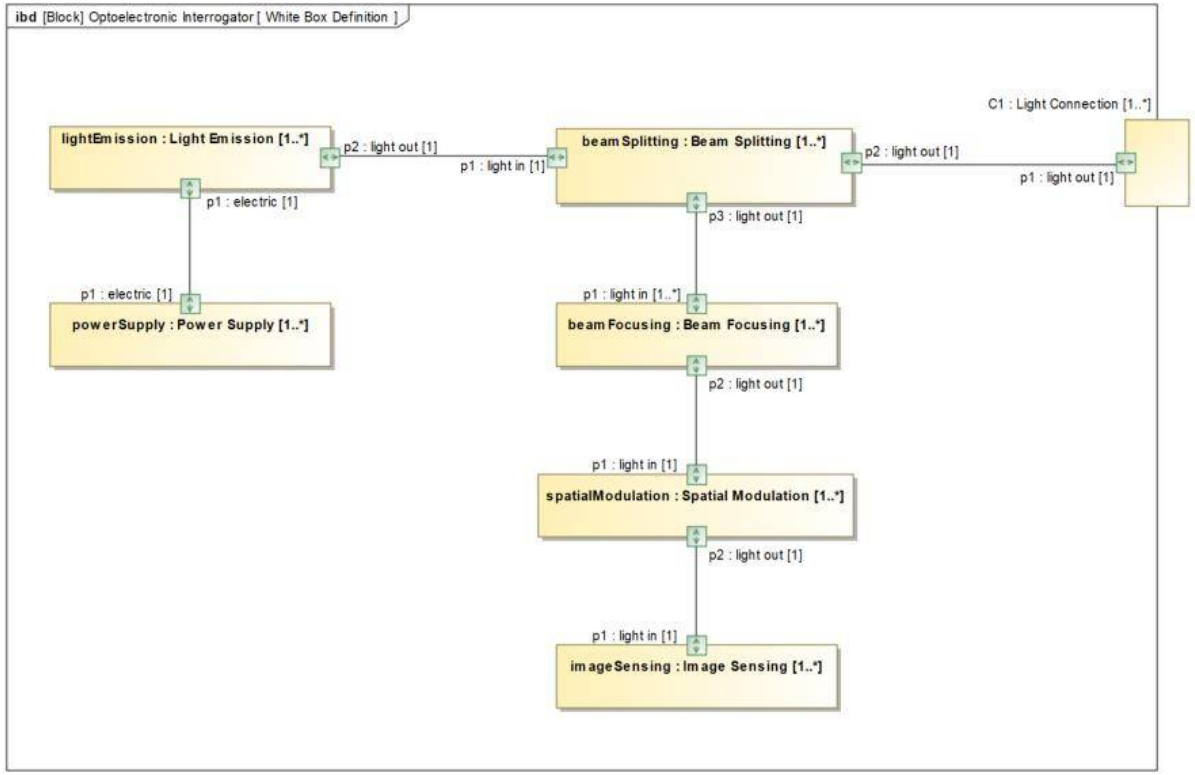
→ **Technical and business teams reconnection**

Simulation between all configuration through the model enables the owner to find a trade-off based on selected criteria and achieve the best solution.

→ **Industrialization process enhancement**



# Configuration Management – Model Design




Different components with their own parameters (cost, performance) :

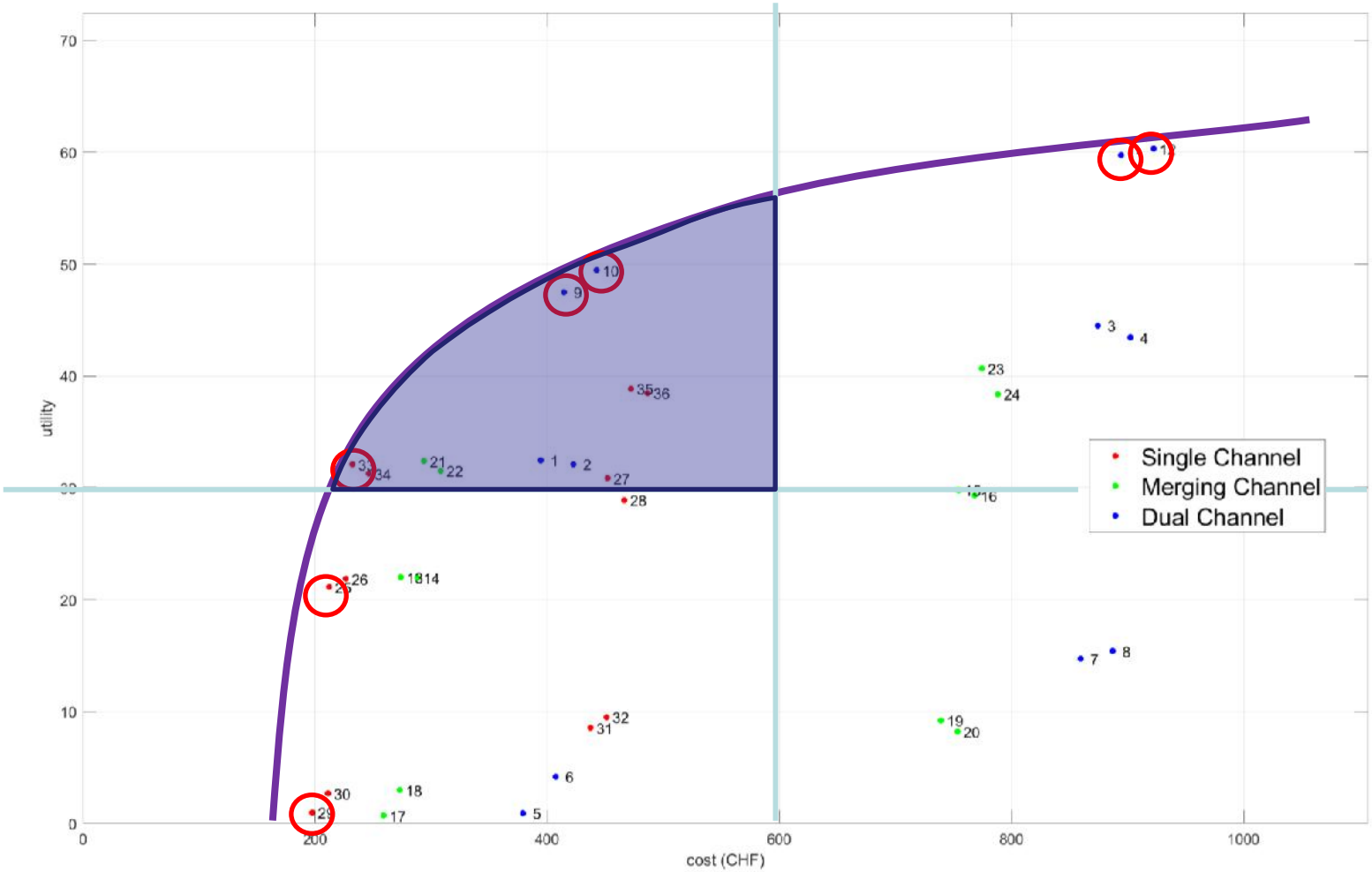
- 3 Power supply possibilities
- 2 Light source possibilities
- 1 Beam splitter possibility
- 1 Light Connector possibility
- 1 Mirror possibility
- 1 Wedge possibility
- 2 Image sensor possibilities

3 different potential architectures

- Single Channel
- Mirror Merging Channel
- Dual Channel

# Configuration Management - Assessment

Attribute : Cost → Better is lower
SNR → Better is higher (utility variable)




1. Determine Pareto Frontier

2. Identify the most pertinent points on the Pareto Frontier

3. Fix limits in the attributes

4. Select the potential points
   - Architecture 9 (Dual)
   - Architecture 10 (Dual)
   - Architecture 33 (Single)

# Exercice

- Réalisez une analyse OPM sur le système choisi en première session. Cette analyse doit être fonctionnelle et structurelle.

- Système : de votre choix (travail de bachelor, travail en cours, autre).
- Niveau d’abstraction : au moins 1
- Méthode : OPM

Conseil : Télécharger l’application DrawIO

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

| | | |
|---|---|---|
| 33 | | Les accidents provoqués par des erreur d'IS |
| 34 | | Les types d'exigence |
| 35 | | Qu'elles sont les possibilités simuler ? Différence ? et utilitée? |
| 36 | | Le «Software-in-the-Loop», qu'est-ce que c'est ? |
| 37 | | Le «Hardware-in-the-Loop», qu'est-ce que c'est ? |

Tableau des présentations

# Exercice pour le 28.11.2021

Compléter l’exercice commencé en classe et le rendre jusqu’à dimanche 28.11.2021 – 23h59 sur le dépôt d’exercice ouvert sur Moodle.

Vous pouvez commencer tout de suite

# Merci pour votre attention

Questions ou remarques: frederic.schenker@hefr.ch ou via Teams

Sécurité et fiabilité des systèmes (SecuFS)

# 10 – Processus de développement des systèmes techniques – Workshop

Frédéric Schenker

29.11.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | 31.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours

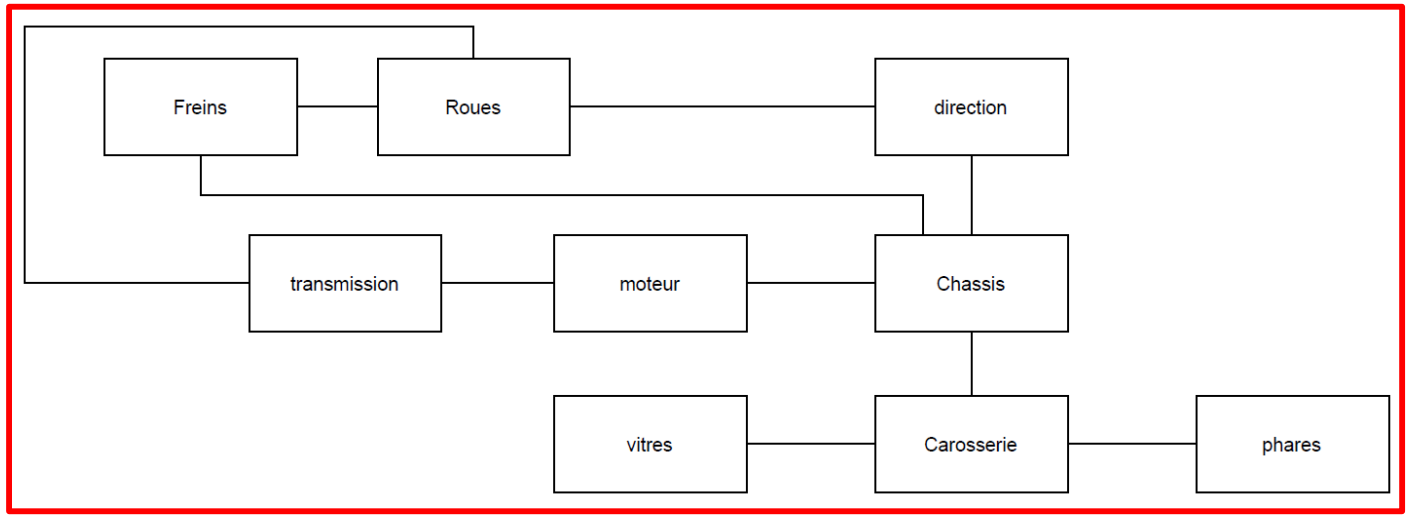
**Structure du cours:**

**Partie 1** : 15 novembre 2021
Objectif général : Introduction à l’ingénierie système et ces processus

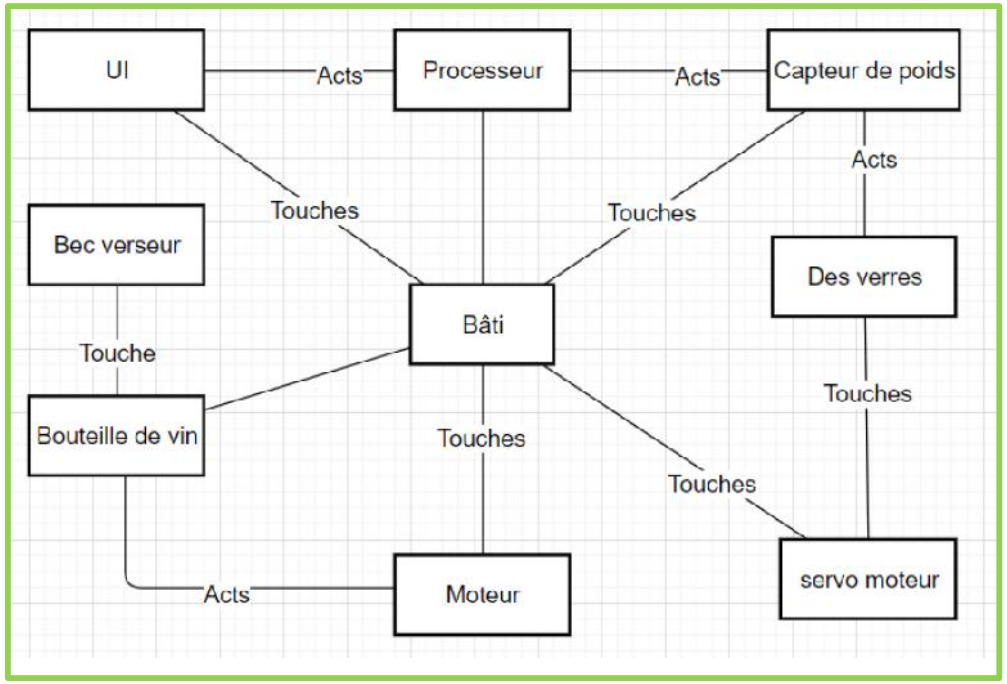
**Partie 2** : 22 novembre 2021
Objectifs : L’ingénierie système basée sur les modèles et son application

**Partie 3** : 29 novembre 2021
Objectifs : Workshop

# Retour sur l'exercice (1)

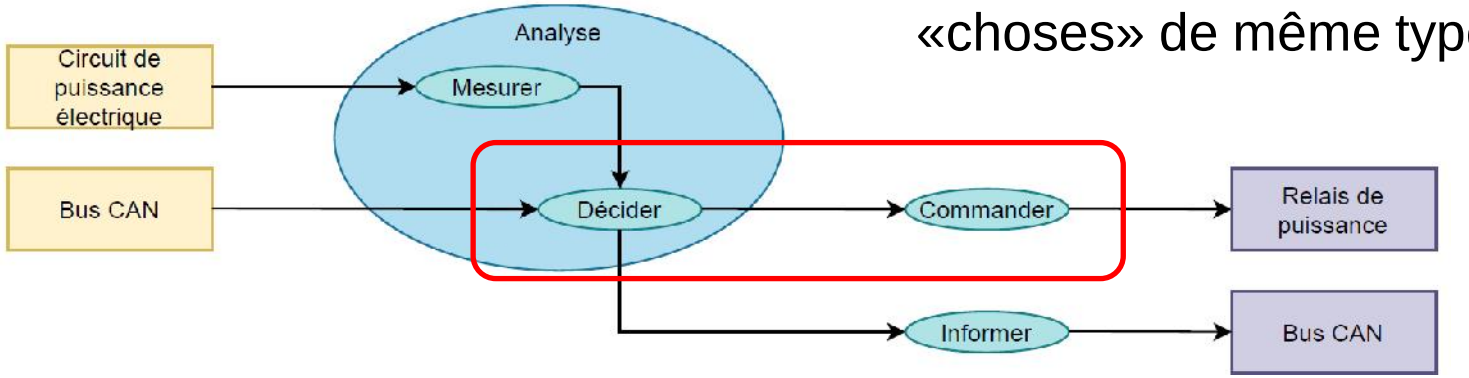


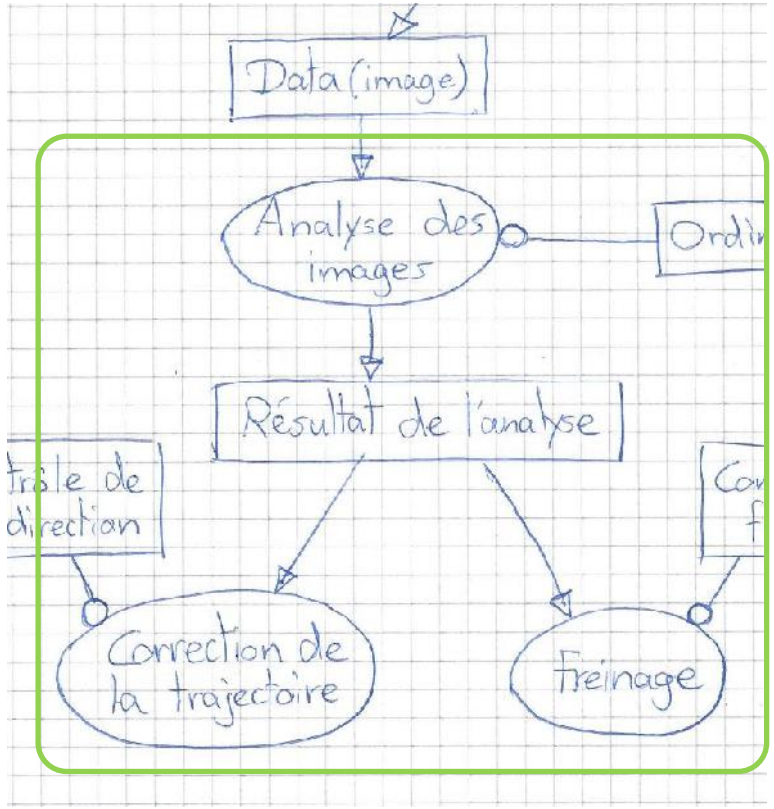

Indiquer le type de lien, ce qui permet la liaison d'un bloc à un autre.



# Retour sur l'exercice (2)

Eviter le lien de résultat, consommation, .. Pour des «choses» de même type



# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

| | | |
|---|---|---|
| 33 | | Les accidents provoqués par des erreur d'IS |
| 34 | Taylor Samson | ISO 14119 - Les dispositifs de verrouillage |
| 35 | | Le «Software-in-the-Loop», qu'est-ce que c'est ? |
| 36 | Arnaud Yersin | Le «Hardware-in-the-Loop», qu'est-ce que c'est ? |
| 37 | Sébastien Mader | Certificat X.509 |

Tableau des présentations

# Présentations individuelles

Chaque semaine, 5 étudiants préparent une présentation de 5 minutes qu'ils exposent à leurs camarades la semaine suivante.

Les thèmes basés sur le contenu du cours du jour seront définis à la fin de la session et présentés la fois suivante.

Toutes les présentations seront ensuite placées sur le Moodle du cours afin que tout le monde puisse en profiter.

| | | |
|---|---|---|
| 33 | Celso Cippà | Le concept de fail-safe |
| 34 | | Sécurité fonctionnelle / Cyber-Sécurité, quelle est la différence? |
| 35 | | Niveau TRL, qu'est-ce que c'est? |
| 36 | | Introduction aux norme ECSS |
| 37 | | Les accidents provoqués par des erreur d'IS |

Tableau des présentations

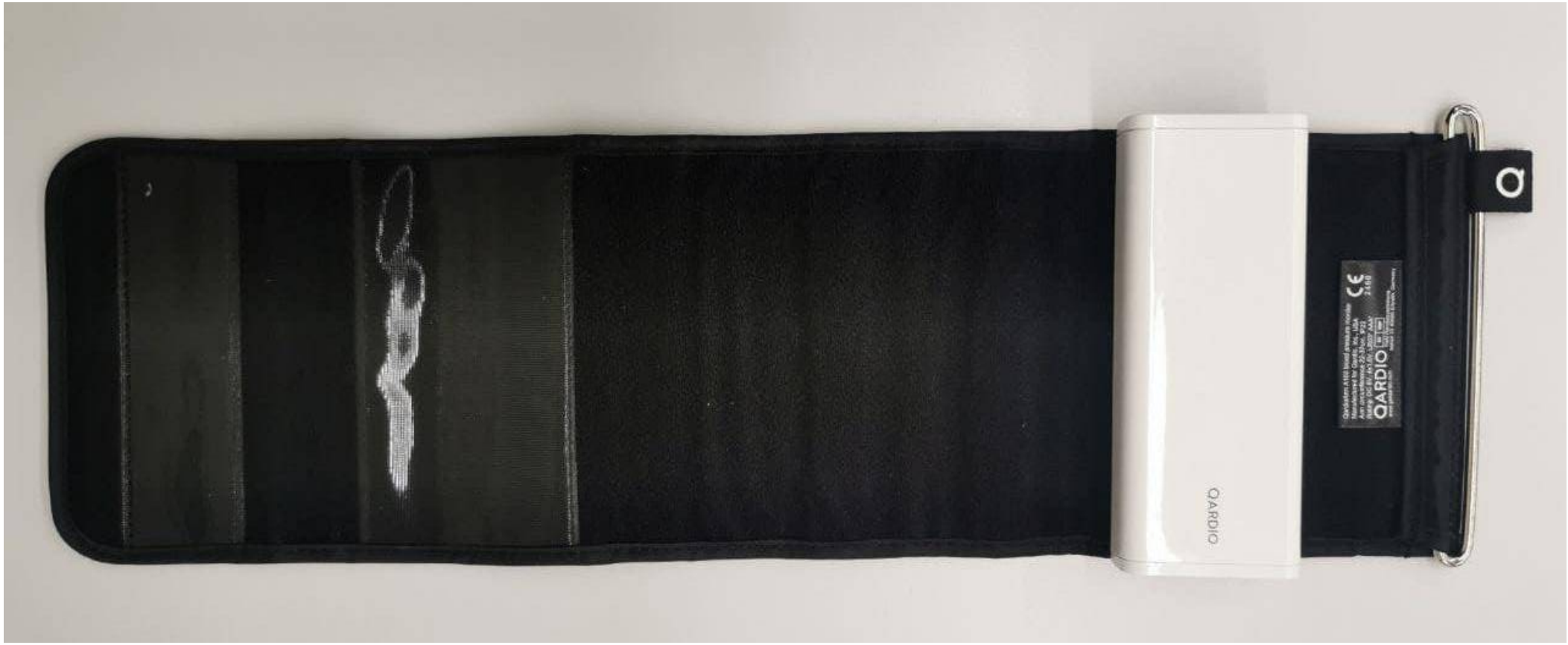
# Workshop

# Objectifs du Workshop

- Analyse «System Thinking» d'un tensiomètre de bras» (sphygmomanomètre)

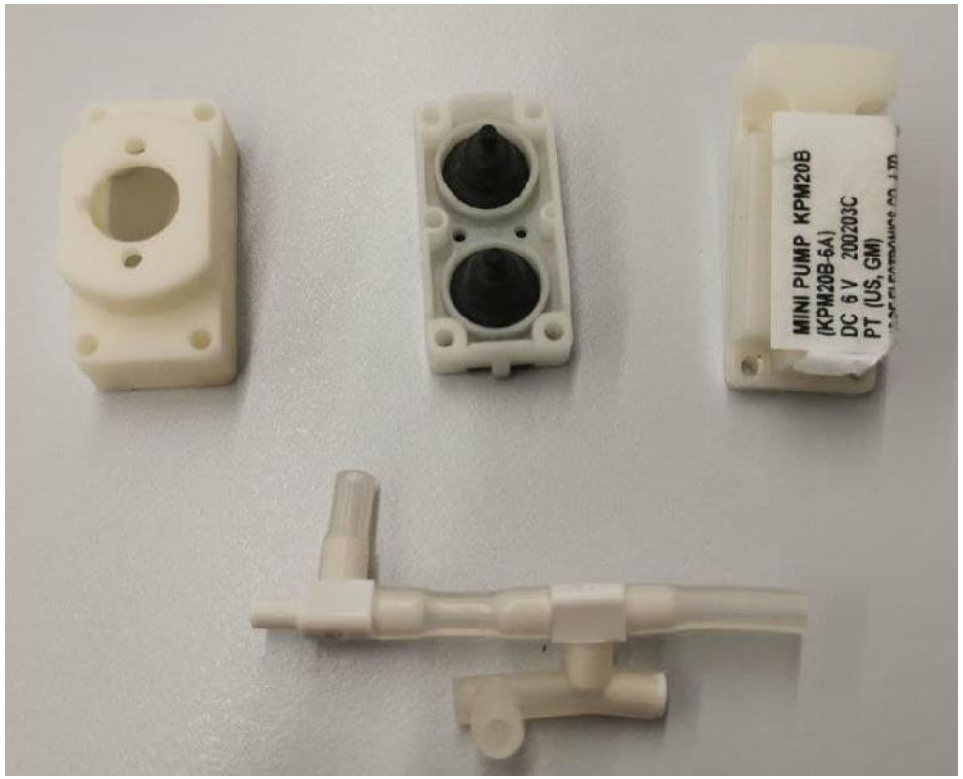
https://www.qardio.com/

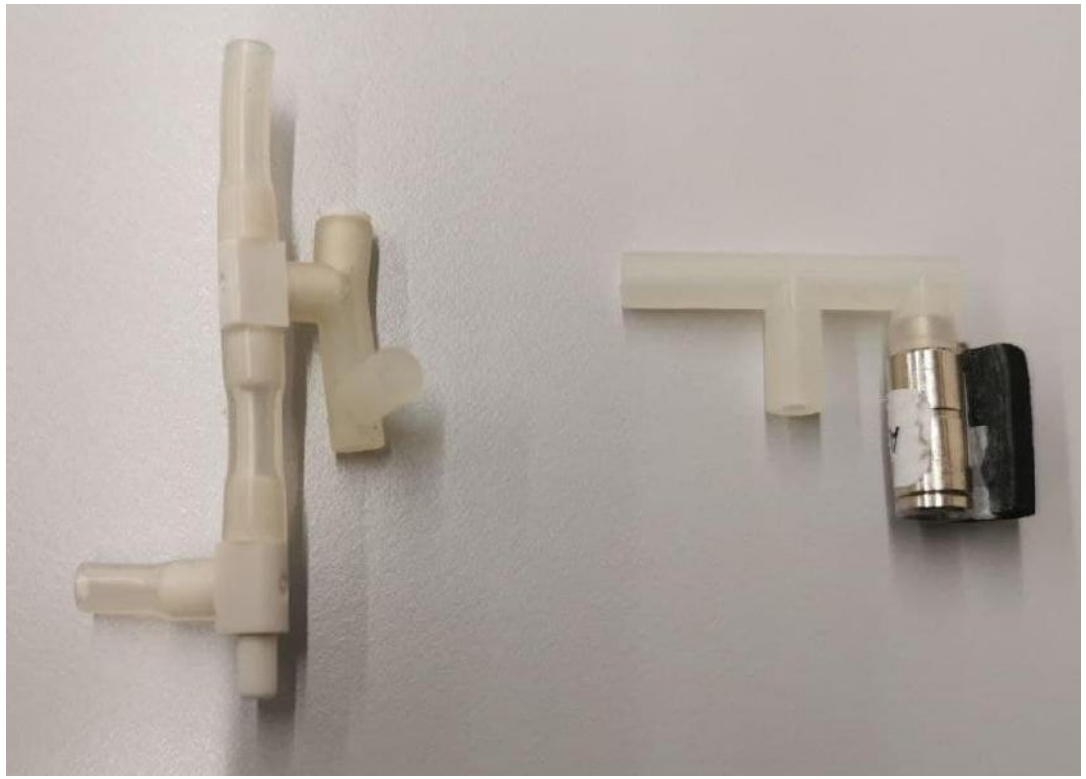
# Tensiomètre (1)



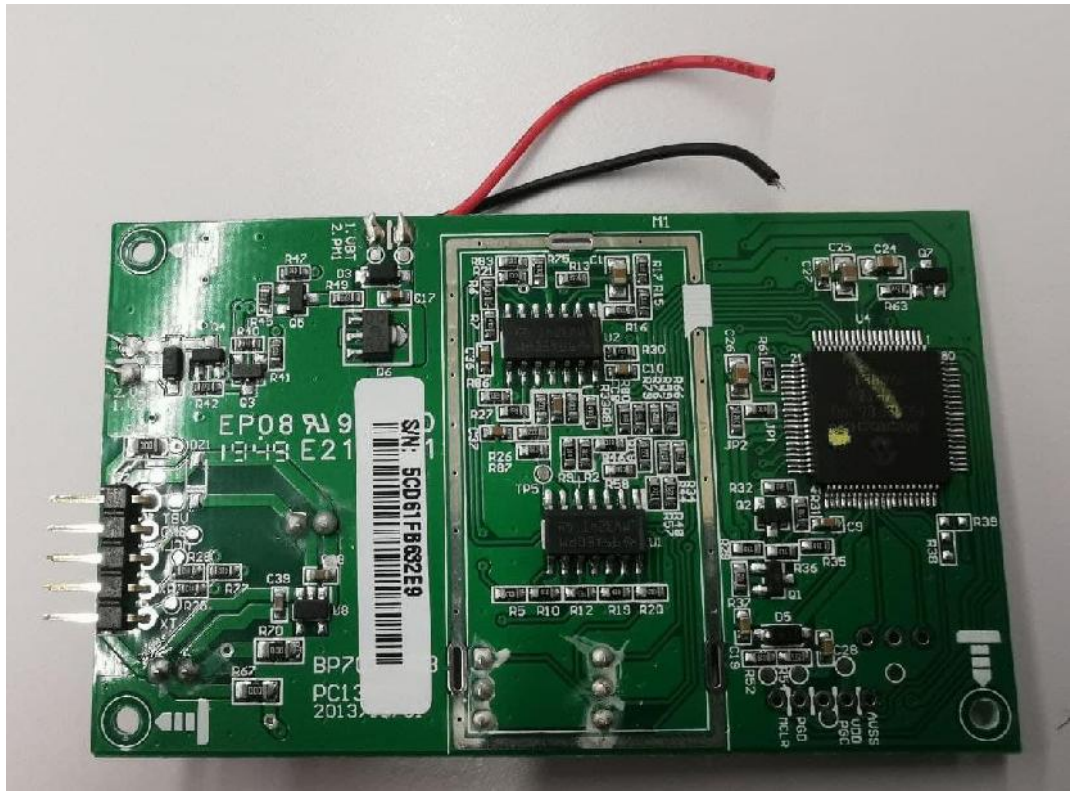
# Tensiomètre (2)

# Tensiomètre (3)



# Tensiomètre (4)



# Tensiomètre (5)

# Tensiomètre (5)

# Merci pour votre attention

Questions ou remarques: frederic.schenker@hefr.ch ou via Teams

Sécurité et fiabilité des systèmes (SecuFS)

# 10 – Processus de développement des systèmes techniques – Workshop - Correction

Frédéric Schenker

29.11.2021

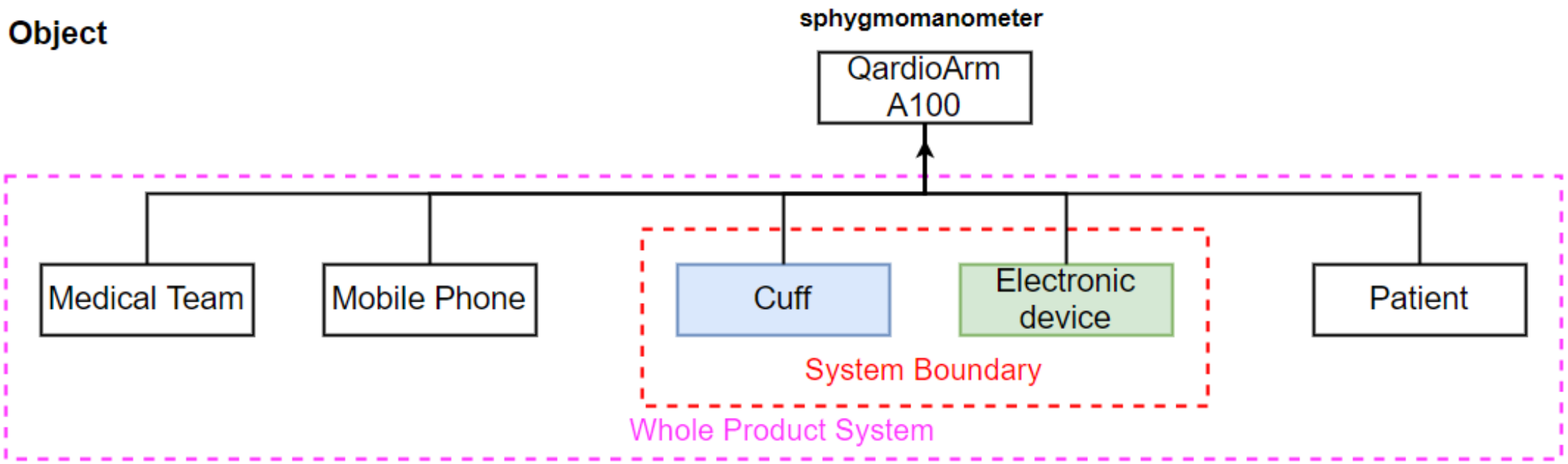
# Workshop

# Objectifs du Workshop

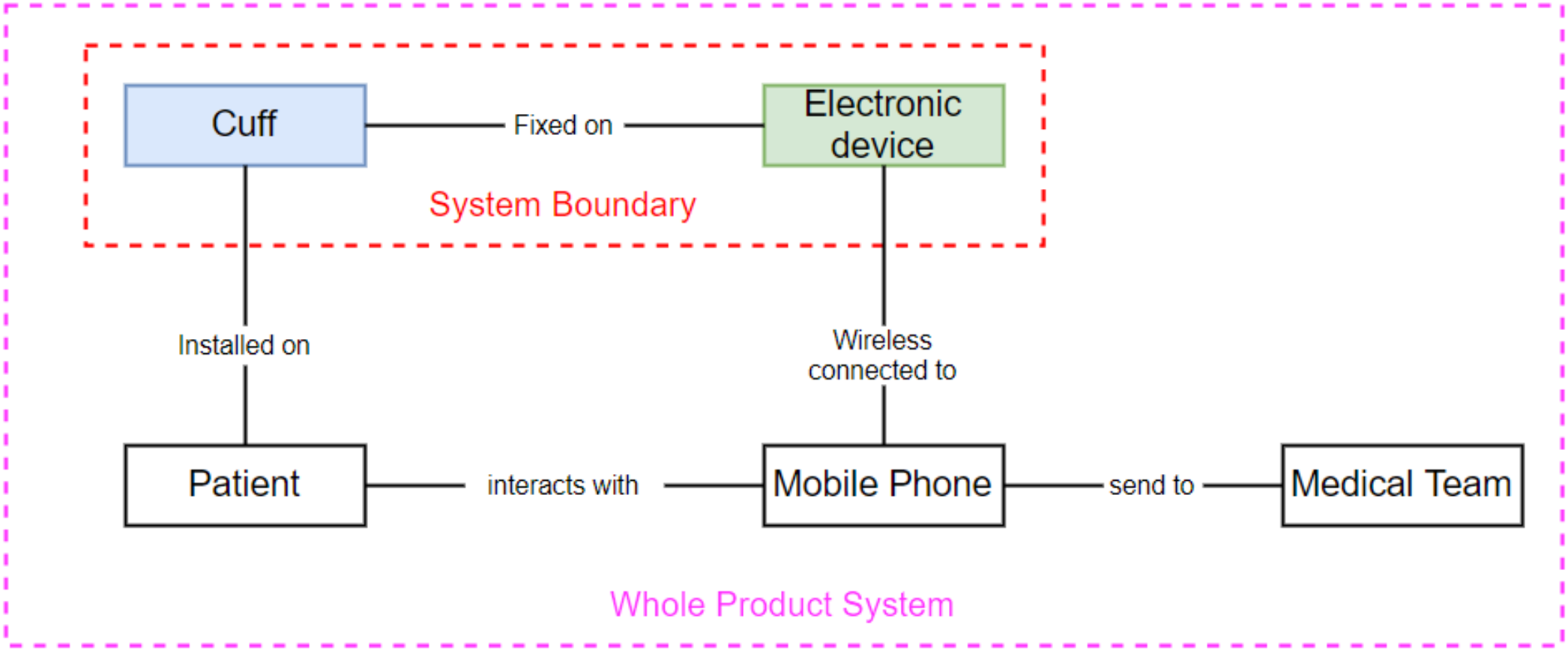
- Analyse «System Thinking» d'un tensiomètre de bras» (sphygmomanomètre)

https://www.qardio.com/

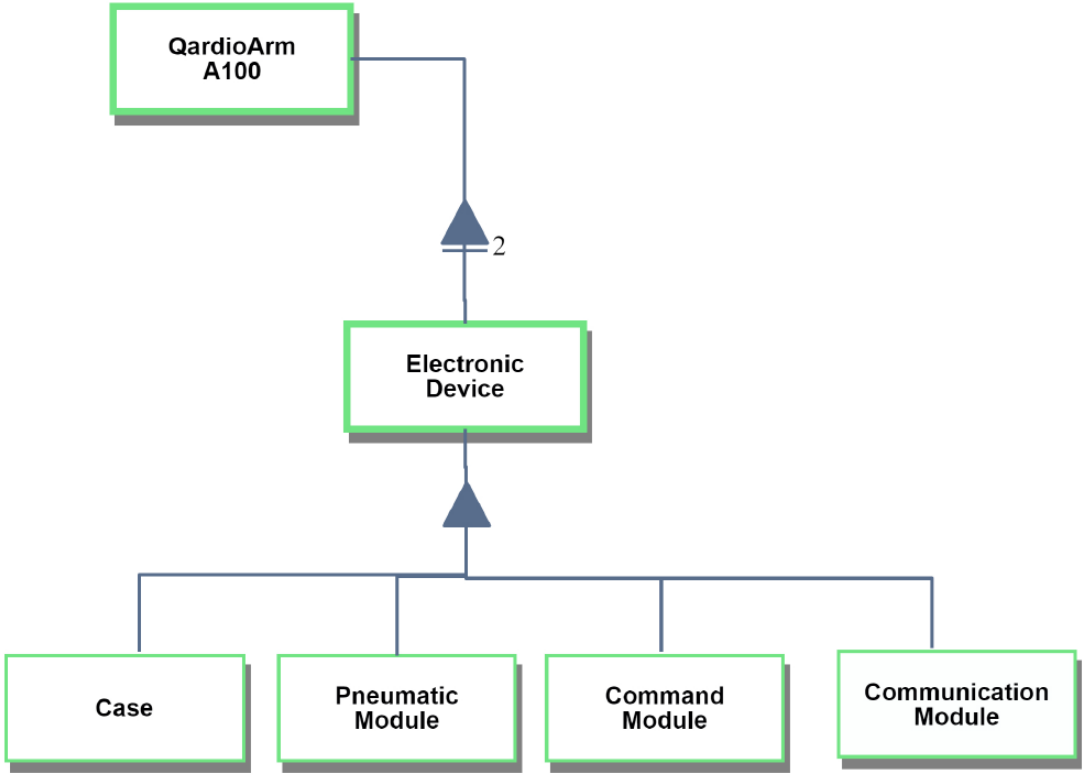
# Object


Object
sphygmomanometer
QardioArm A100
Medical Team
Mobile Phone
Cuff
Electronic device
Patient
System Boundary
Whole Product System

# Structure


Cuff
Fixed on
Electronic device
System Boundary
Installed on
Wireless connected to
Patient
interacts with
Mobile Phone
send to
Medical Team
Whole Product System

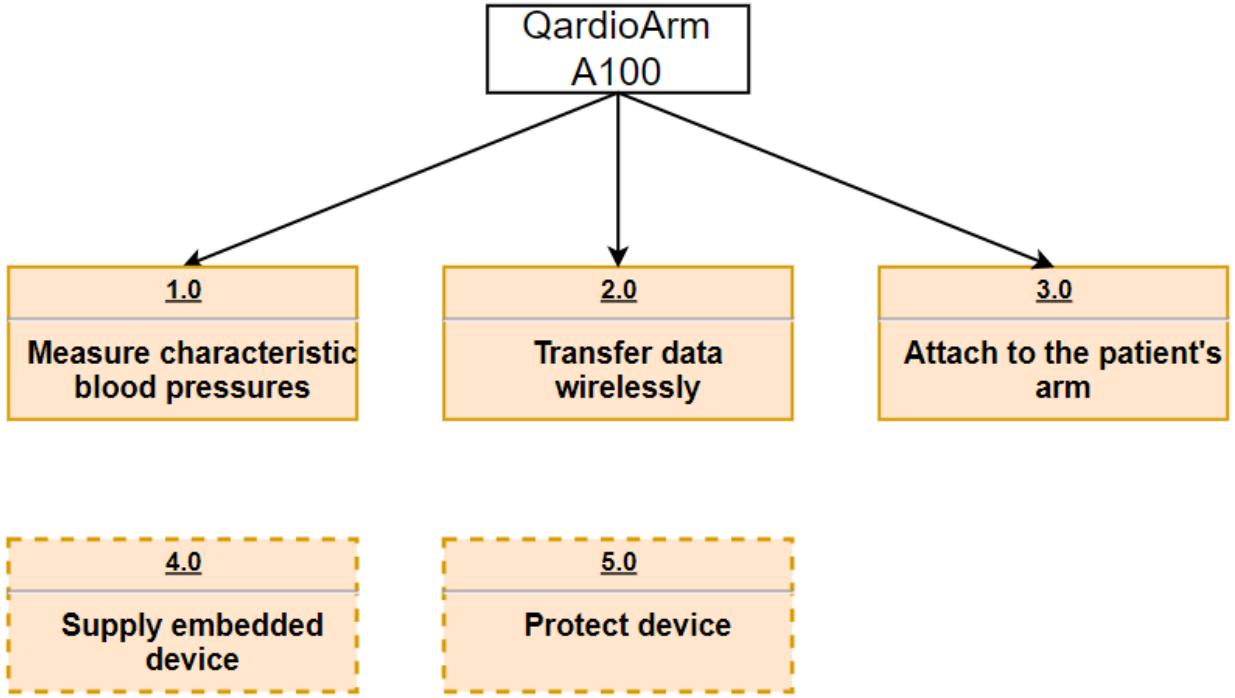
# Object – Electronic Device



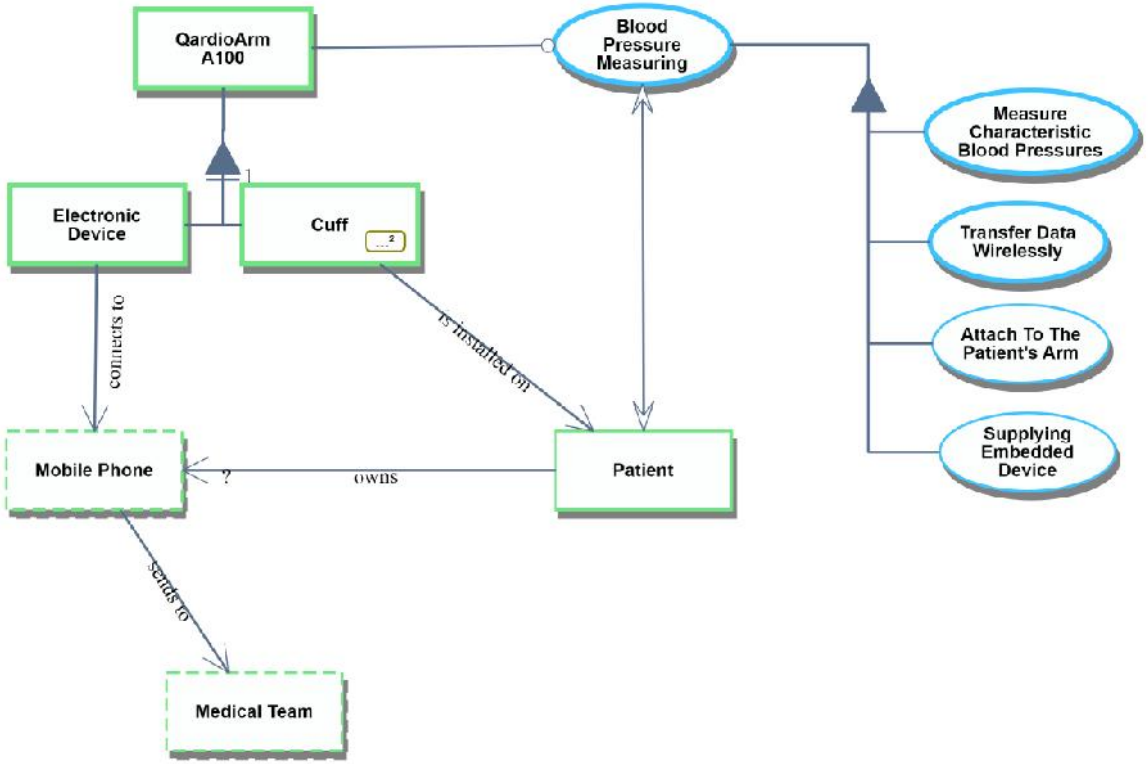

1. Electronic Device consists of Case, Command Module, Communication Module and Pneumatic Module.
2. QardioArm A100 consists of Electronic Device and two more parts.

# Functions

System Functions

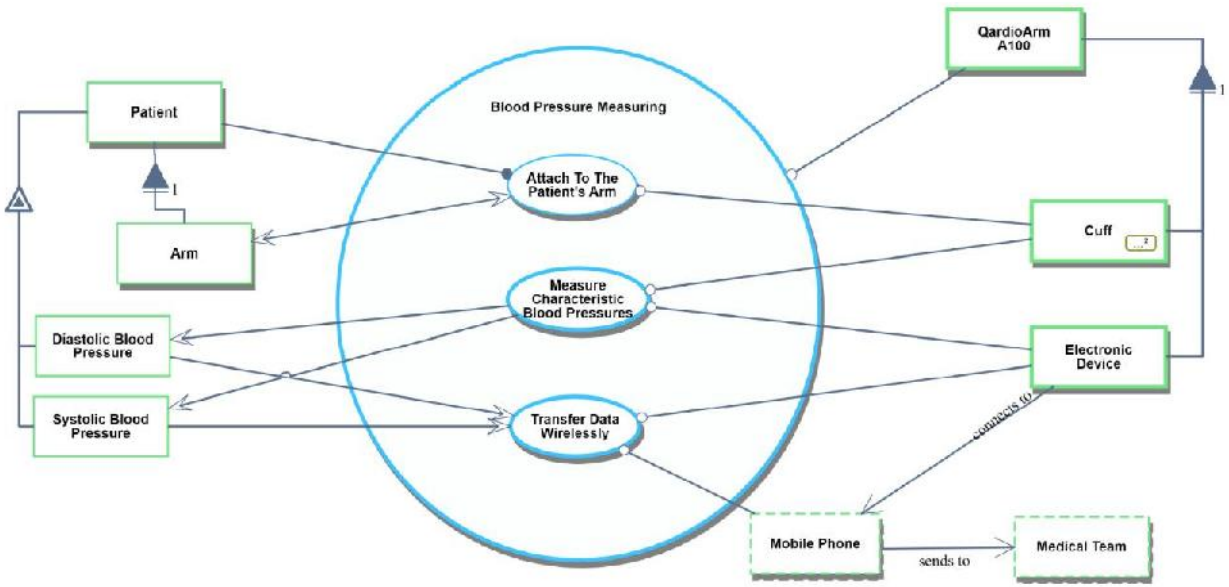


# Process + Attribues (1)




1. Mobile Phone is environmental.
2. Medical Team is environmental.
3. Cuff is stateful.
4. Patient owns an optional Mobile Phone.
5. QardioArm A100 consists of Cuff, Electronic Device and one more part.
6. Blood Pressure Measuring consists of Attach To The Patient's Arm, Measure Characteristic Blood Pressures, Supplying Embedded Device and Transfer Data Wirelessly.
7. Mobile Phone sends to Medical Team.
8. Electronic Device connects to Mobile Phone.
9. Cuff is installed on Patient.
10. Blood Pressure Measuring requires QardioArm A100.
11. Blood Pressure Measuring affects Patient.

# Process + Attribues (2)




1. Blood Pressure Measuring from SD zooms in SD1 into Attach To The Patient's Arm, Measure Characteristic Blood Pressures, and Transfer Data Wirelessly, which occur in that time sequence .
2. Cuff is stateful.
3. Diastolic Blood Pressure of Patient is informatical.
4. Systolic Blood Pressure of Patient is informatical.
5. Mobile Phone is environmental.
6. Medical Team is environmental.
7. Patient exhibits Diastolic Blood Pressure and Systolic Blood Pressure.
8. Patient consists of Arm and one more part.
9. QardioArm A100 consists of Cuff, Electronic Device and one more part.
10. Electronic Device connects to Mobile Phone.
11. Mobile Phone sends to Medical Team.
12. Blood Pressure Measuring requires QardioArm A100.
13. Patient handles Attach To The Patient's Arm.
14. Attach To The Patient's Arm requires Cuff.
15. Attach To The Patient's Arm affects Arm.
16. Measure Characteristic Blood Pressures requires Cuff and Electronic Device.
17. Measure Characteristic Blood Pressures yields Diastolic Blood Pressure of Patient and Systolic Blood Pressure of Patient.
18. Transfer Data Wirelessly requires Electronic Device and Mobile Phone.
19. Transfer Data Wirelessly consumes Diastolic Blood Pressure of Patient and Systolic Blood Pressure of Patient.

# Merci pour votre attention

Questions ou remarques: frederic.schenker@hefr.ch ou via Teams

Sécurité et fiabilité des systèmes (SecuFS)

# 11 –Fiabilité des systèmes techniques - Niveau composants

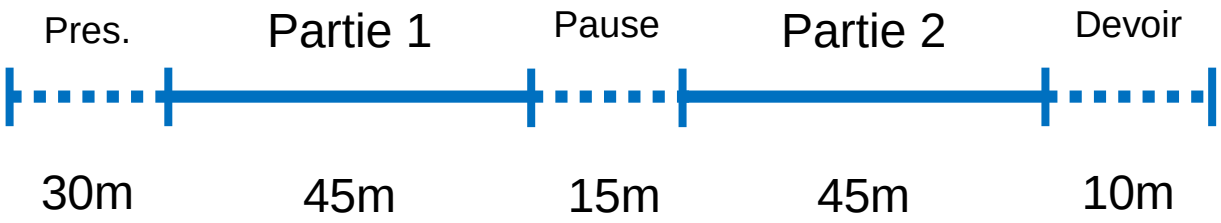
Jonathan Hendriks

06.12.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | Workshop «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | 31.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Définition(s):

**Fiabilité** :

La fiabilité est l'étude des défaillances des systèmes. Un système est dit « fiable » lorsque la probabilité de remplir sa mission sur une durée donnée correspond à celle spécifiée dans le cahier des charges.

L'Union technique de l'électricité (UTE), sur recommandation de la Commission électrotechnique internationale, a proposé la définition suivante :

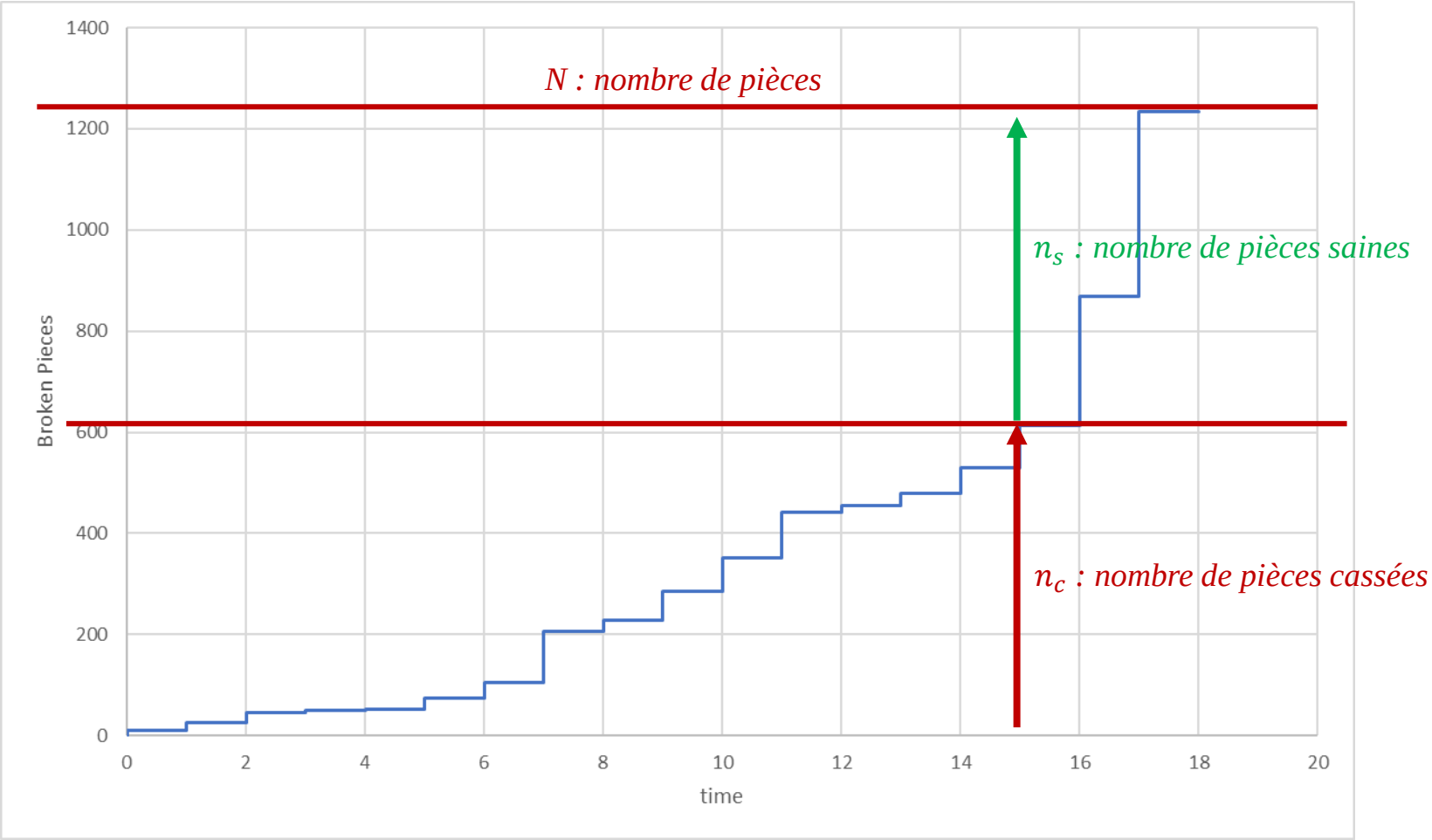
*«La fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise dans des conditions données pour une période de temps donnée [1].»*

**Durabilité** :

Qualité de ce qui est durable. Dans le domaine de la sécurité fonctionnel, c'est l'aptitude de répondre/satisfaire à un besoin durant un espace de temps.[2]

Sources:
[1] Pierre Chapouille, La fiabilité, Que sais-je ?; Commission électrotechnique internationale, Vocabulaire électrotechnique international 191-01-24
[2] Larousse, https://www.larousse.fr/dictionnaires/francais/durabilit%C3%A9/27024#definition

# Hazard Rate – H(t)




$$N = n_c + n_s$$

where

$n_c$ = les pièces cassées

$N$ = le nombre des pièces

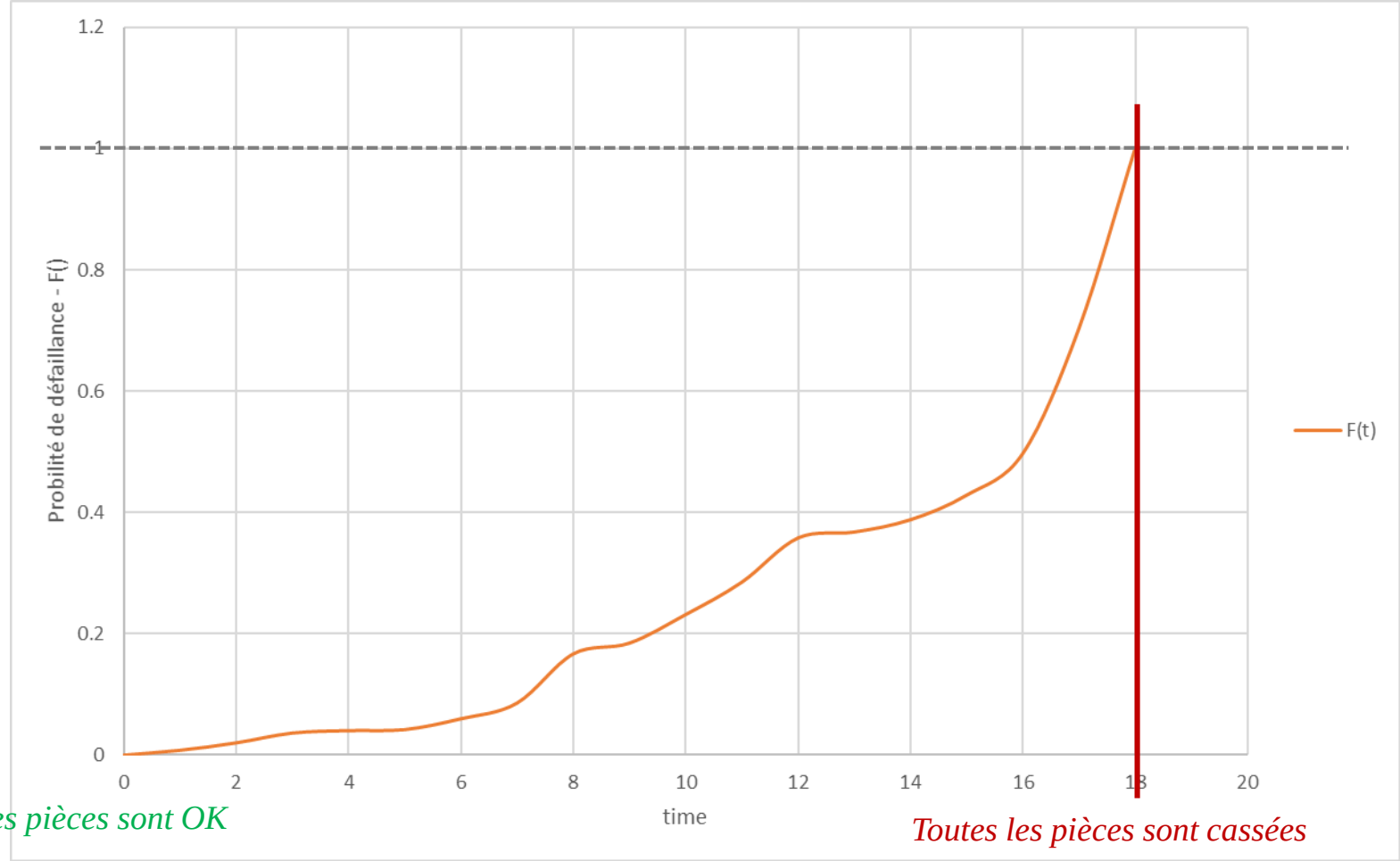
$n_s$ = les pièces survies

Hazard Rate:

$$H = \frac{n_c}{N}$$

$$H(\Delta t) = \frac{1 * \Delta n_c}{n_s * \Delta t}$$

# Probabilité de défaillance – F(t)




$$N = n_c + n_s$$

where

$n_c$ = les pièces cassées

$N$ = le nombre des pièces

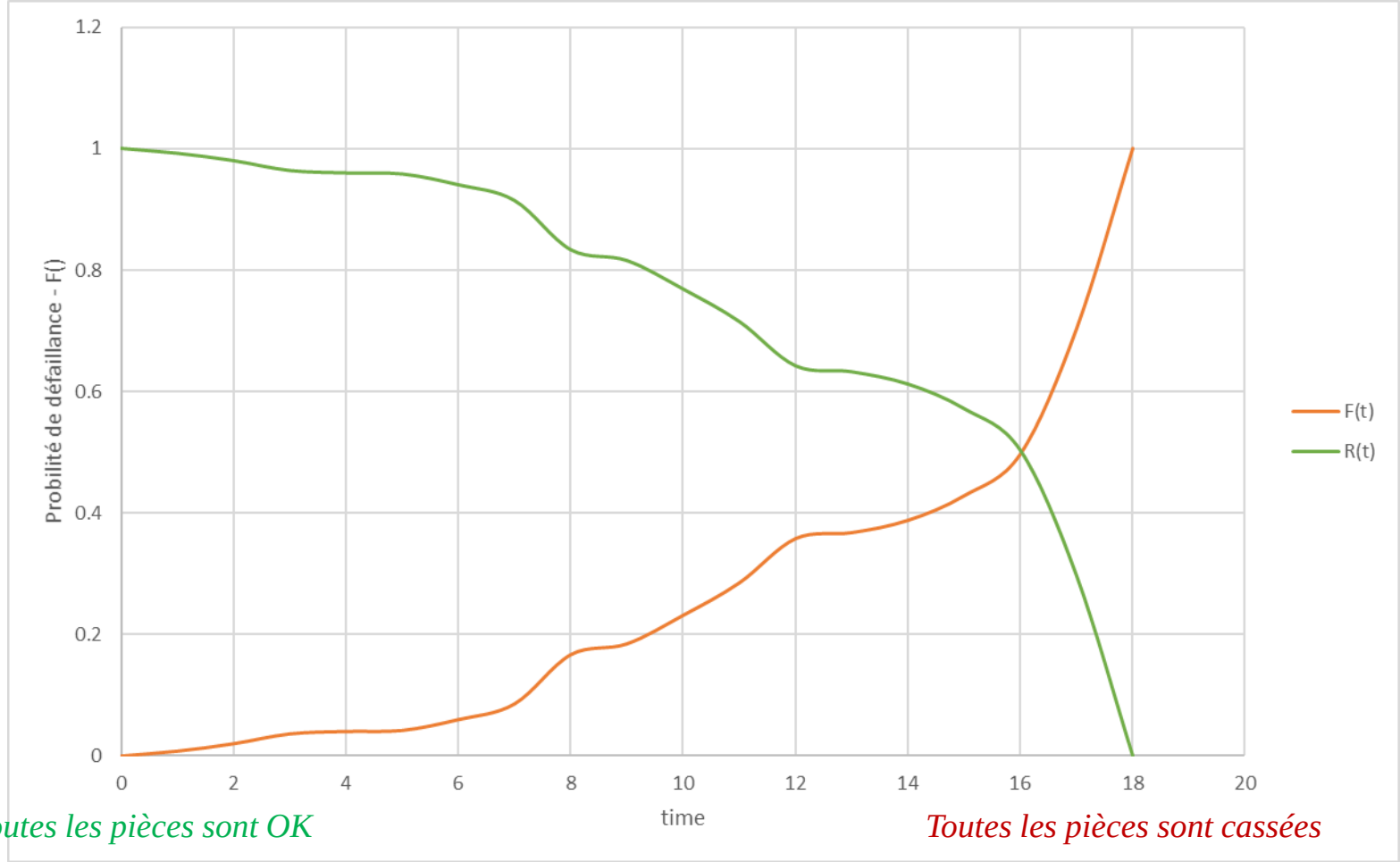
$n_s$ = les pièces survies

Failure Rate – F(t):

$$F(t) = \frac{n_c(t)}{N}$$

$$F(0) = 0$$
$$F(\infty) = 1$$

# Probabilité de survie – R(t)




Failure Rate – F(t):

$$F(t) = \frac{n_c}{N}$$

Survival Rate – R(t):

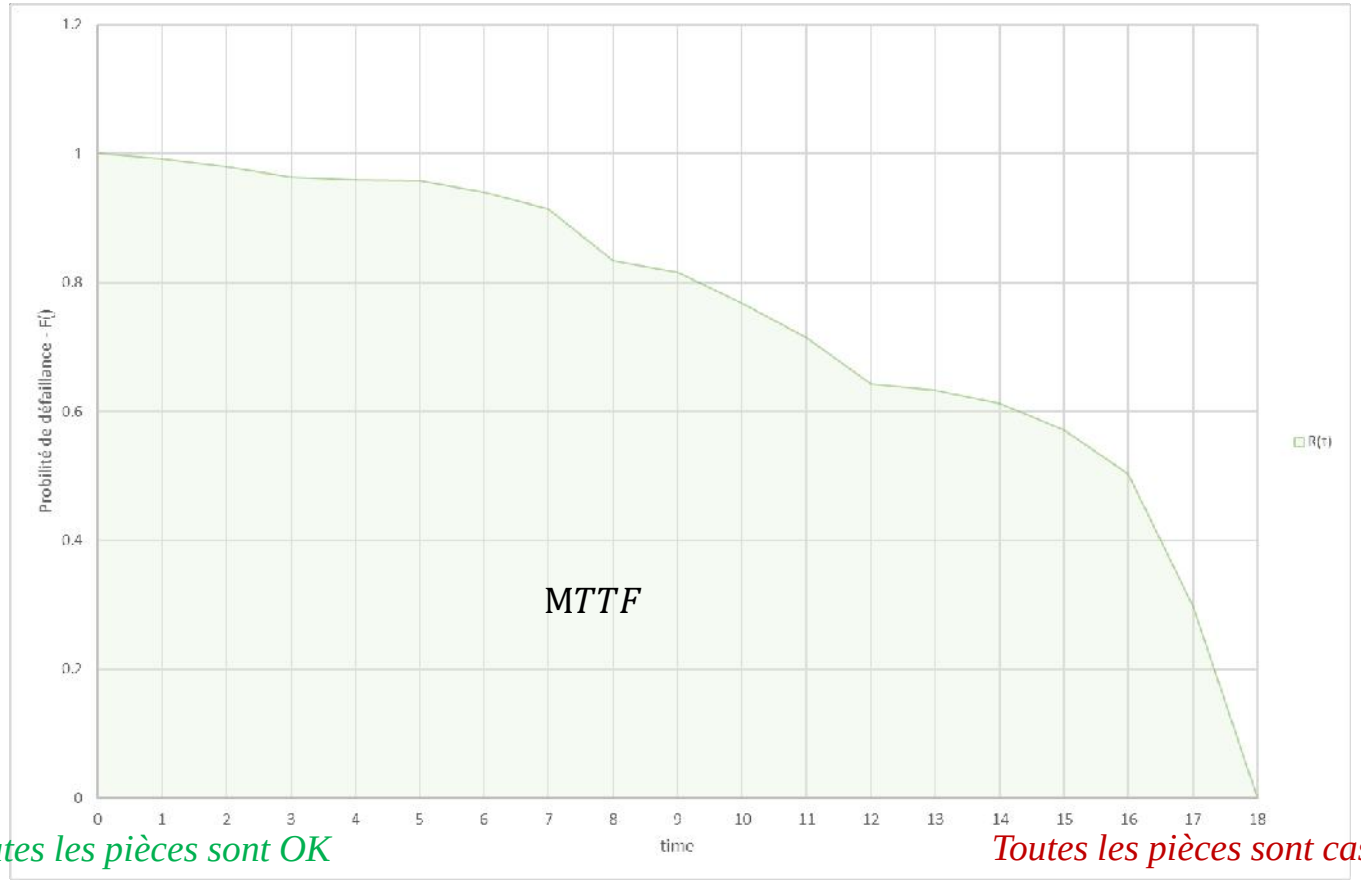
$$F(t) = 1 - R(t)$$

$$1 = F(t) + R(t)$$

$$R(t) = \frac{n_s(t)}{N}$$

# Espérance de vie – MTTF (système non réparable)

Mean Time To Failure (MTTF) mesure la valeur moyenne de temps qu'un système non-reparable peut fonctionner avant d'être en panne.




*Toutes les pièces sont OK*

*Toutes les pièces sont cassées*

Survival Rate – R(t):

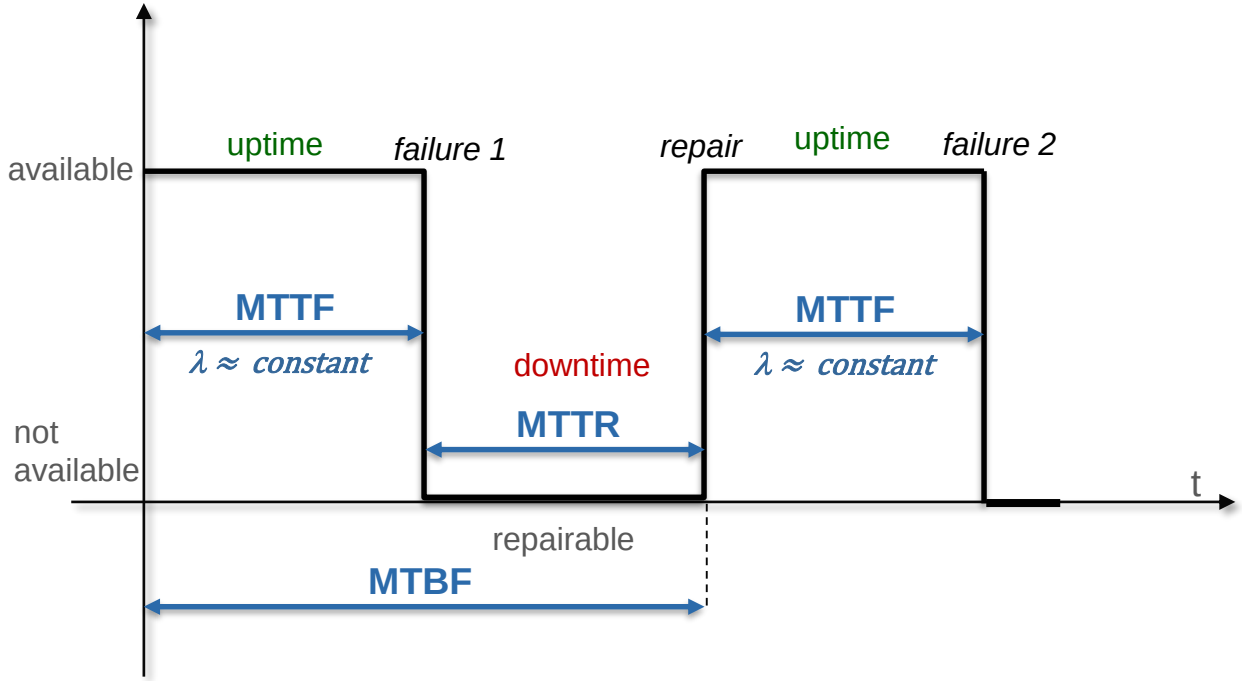
$$R(t) = \frac{n_s(t)}{N}$$

Mean Time To Failure – MTTF:

$$MTTF = \int_0^{\infty} R(t)dt$$

# Espérance de vie (1)

| | | |
|---|---|---|
| Mean Time To Failure | (MTTF) | mesure la valeur moyenne de temps qu'un système non-réparable peut fonctionner avant d'être en panne. |
| Mean Time Between Failure | (MTBF) | mesure la valeur moyenne de temps qu'un système met pour un cycle panne/restoré. |
| Mean Time To Repair | (MTTR) | mesure la valeur moyenne de temps de réparation sur un système |




$$MTBF = MTTF + MTTR$$

Système Non-Réparable :

$MTTR = 0$

$MTBF = MTTF$

# Espérance de vie (2)

Integration par partie:

$$\int v\frac{du}{dt}dt = vu - \int u\frac{dv}{dt}dt$$

Explication:

$$MTTF = \int_0^\infty t f(t)\,dt = -\int_0^\infty t\frac{dR(t)}{dt}dt = -\left(\boxed{[t\cdot R(t)]_0^\infty} - \int_0^\infty R(t)dt\right) = \int_0^\infty R(t)dt$$

**= 0**

Avec:

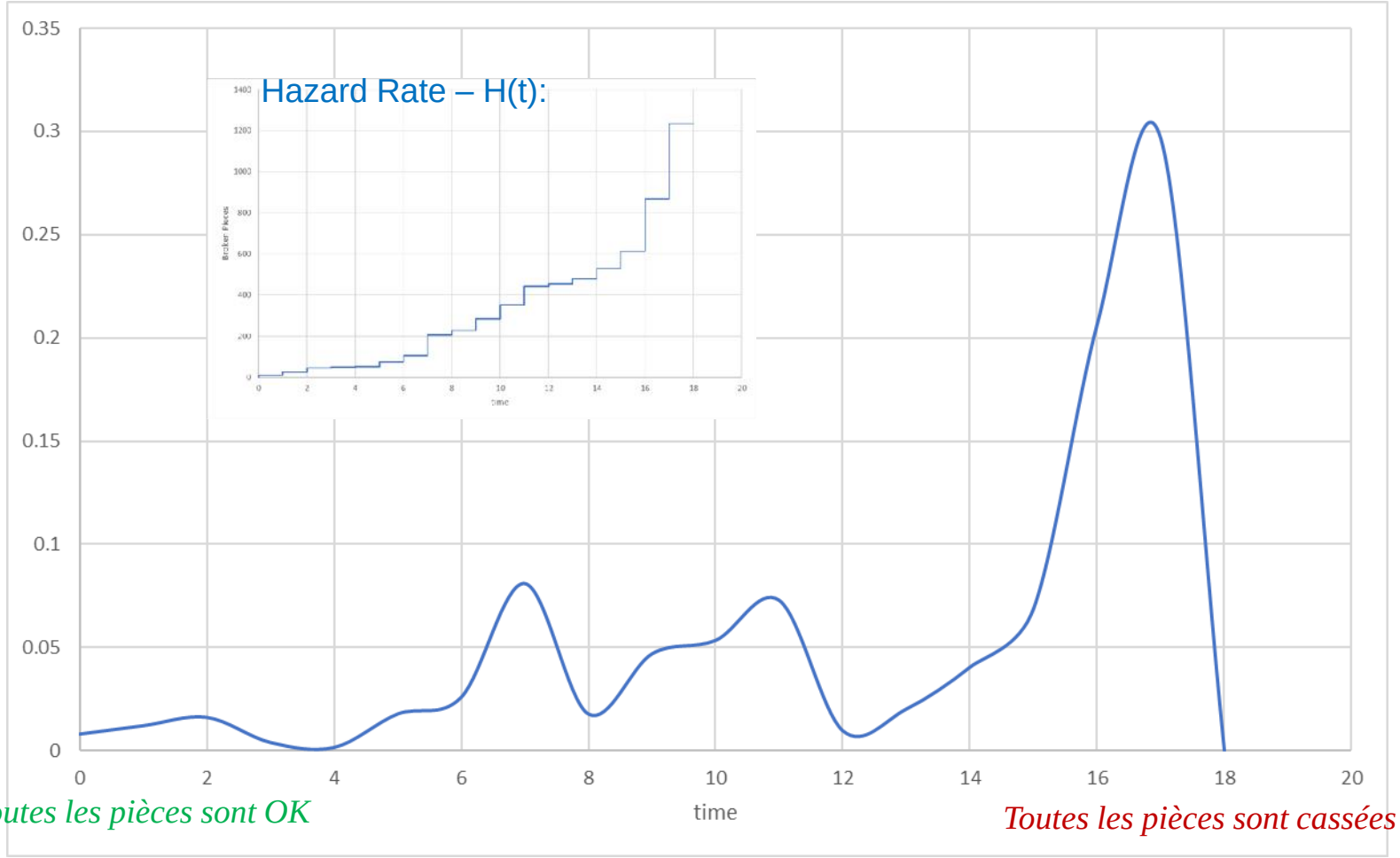
$$f(t) = \frac{dF(t)}{dt} = \frac{-dR(t)}{dt}$$

Avec:

$$R(\infty) \cong 0$$

$$R(0) = 1$$

# Densité de défaillance – f(t)




La densité de défaillance d'un composant ou système correspond a la probabilité qu'une erreur apparait à l'instant t.

Failure Density – f(t):

$$f(t) = \frac{d\,F(t)}{dt} = -\frac{d\,R(t)}{dt}$$

$$f(0) = 0$$
$$f(\infty) = 0$$

Sources:
[1] Failure Rate Analysis, Fatemeh Afsharnia, https://www.intechopen.com/chapters/58187

# Taux de défaillance – h(t)

Dans l'industrie, c'est important de pouvoir caractériser, combien de pieces, qui ont survie jusqu'à l'instant $t$, peuvent tomber en panne dans l'interval $t$ et $t + \Delta t$.

C'est la probabilité conditionnelle de F sous la condition qu'au moment $t$, les éléments ont survies et que le composant/système a fonctionné de $t = 0$ à $t_1$

$$H(\Delta t) = \frac{1 * \Delta n_c}{n_s * \Delta t}$$

$$\mathrm{h}(t) = \frac{1 * dn_c(t)}{n_s * dt} = \frac{1 * dF(t) * N}{R(t) * N * dt} = \frac{1 * dF(t)}{R(t) * dt} = \frac{1}{R(t)} * \frac{dF(t)}{dt} = \frac{f(t)}{R(t)}$$

Failure Rate – ʎ(t):

$$\boxed{\mathrm{h}(t) = \frac{f(t)}{R(t)} = \lambda(t)}$$

Avec : $f(t) = \frac{dF(t)}{dt} = \frac{-dR(t)}{dt}$

$$\mathrm{h}(t) = \frac{1 * dF(t)}{R(t) * dt} = \frac{1 * (-dR(t))}{R(t) * dt} = \frac{-1}{R(t)} * \frac{dR(t)}{dt} = \frac{f(t)}{R(t)}$$

Sources:
[1] Failure Rate Analysis, Fatemeh Afsharnia, https://www.intechopen.com/chapters/58187

# Fiabilité – Tableau Récapitulatif

| | Probabilité de défaillance<br>Probability of Failure<br>$F(t)$ | Probabilité de survie<br>Probability of Survival<br>$\mathrm{R}(t)$ | Densité de défaillance<br>Hazard Density<br>$f(t)$ | Taux de défaillance<br>Failure Rate<br>$h(t) = \lambda(t)$ |
|---|---|---|---|---|
| $F(t)$ | | $1 - R(t)$ | $\int_0^t f(\tau)d\tau$ | $1 - e^{\left(-\int_0^t h(\tau)d\tau\right)}$ |
| $\mathrm{R}(t)$ | $1 - F(t)$ | | $\int_t^\infty f(\tau)d\tau$ | $e^{\left(-\int_0^t h(\tau)d\tau\right)}$ |
| $f(t)$ | $\frac{d\,F(t)}{dt}$ | $-\frac{d\,R(t)}{dt}$ | | $h(t) * e^{\left(-\int_0^t h(\tau)d\tau\right)}$ |
| $h(t) = \lambda(t)$ | $\frac{1}{1 - F(t)} * \frac{d\,F(t)}{dt}$ | $-\frac{1}{R(t)} * \frac{d\,R(t)}{dt}$ | $\frac{f(t)}{\int_t^\infty f(\tau)d\tau}$ | |

# Exercise 1

Dans un essaie, nous mesurons 316 pièces jusqu'ils sont tous tombés en panne

| intervalle [h] | pièces cassés | $n_c$ | Δt [h] | F(t) | R(t) | $\Delta n_c/\Delta t$ | f(t) [1/h] | h(t) [1/h] = | Surface sous f(t) |
|---|---|---|---|---|---|---|---|---|---|
| 0-2 | 82 | | | | | | | | |
| 2-4 | 22 | | | | | | | | |
| 4-6 | 24 | | | | | | | | |
| 6-8 | 20 | | | | | | | | |
| 8-10 | 23 | | | | | | | | |
| 10-12 | 32 | | | | | | | | |
| 12-14 | 25 | | | | | | | | |
| 14-16 | 27 | | | | | | | | |
| 16-18 | 20 | | | | | | | | |
| 18-20 | 15 | | | | | | | | |
| 20-22 | 10 | | | | | | | | |
| 22-24 | 2 | | | | | | | | |
| 24-87 | 14 | | | | | | | | |

Valeur espérance de vie moyenne = ?

# Solution

| intervalle [h] | pièces cassés | $n_c$ | Δt [h] | F(t) = nc/316 | R(t) = 1-F(t) | $\Delta n_c/\Delta t$ = a | f(t) [1/h] =F'(t) = a/316 | h(t) [1/h] = f(t)/R(t) | Surface sous f(t) Δt * f(t) | MTTFi |
|---|---|---|---|---|---|---|---|---|---|---|
| 0-2 | 82 | 82 | 2 | 0.259 | 0.741 | 41.000 | 0.1297 | 0.1752 | 0.2595 | 1.481013 |
| 2-4 | 22 | 104 | 2 | 0.329 | 0.671 | 11.000 | 0.0348 | 0.0519 | 0.0696 | 1.341772 |
| 4-6 | 24 | 128 | 2 | 0.405 | 0.595 | 12.000 | 0.0380 | 0.0638 | 0.0759 | 1.189873 |
| 6-8 | 20 | 148 | 2 | 0.468 | 0.532 | 10.000 | 0.0316 | 0.0595 | 0.0633 | 1.063291 |
| 8-10 | 23 | 171 | 2 | 0.541 | 0.459 | 11.500 | 0.0364 | 0.0793 | 0.0728 | 0.917722 |
| 10-12 | 32 | 203 | 2 | 0.642 | 0.358 | 16.000 | 0.0506 | 0.1416 | 0.1013 | 0.71519 |
| 12-14 | 25 | 228 | 2 | 0.722 | 0.278 | 12.500 | 0.0396 | 0.1420 | 0.0791 | 0.556962 |
| 14-16 | 27 | 255 | 2 | 0.807 | 0.193 | 13.500 | 0.0427 | 0.2213 | 0.0854 | 0.386076 |
| 16-18 | 20 | 275 | 2 | 0.870 | 0.130 | 10.000 | 0.0316 | 0.2439 | 0.0633 | 0.259494 |
| 18-20 | 15 | 290 | 2 | 0.918 | 0.082 | 7.500 | 0.0237 | 0.2885 | 0.0475 | 0.164557 |
| 20-22 | 10 | 300 | 2 | 0.949 | 0.051 | 5.000 | 0.0158 | 0.3125 | 0.0316 | 0.101266 |
| 22-24 | 2 | 302 | 2 | 0.956 | 0.044 | 1.000 | 0.0032 | 0.0714 | 0.0063 | 0.088608 |
| 24-87 | 14 | 316 | 63 | 1.000 | 0.000 | 0.222 | 0.0007 | #DIV/0! | 0.0443 | 0 |

MTTF 8.266 h

Valeur espérance de vie moyenne = $\int R(t)\,dt = 2*0.7405 + 2*\ 0.6709 + ..... = 8.26\ \mathrm{h}$

# Unité

- Le Taux de défaillance peut être exprimé dans n'importe quelle unite de temps (Seconds, milli-second, jours, mois , année,…)

  Cependant, les heures sont le plus commun.

- Le Taux de défaillance est très souvent exprimé en failure per million, ou $10^{-6}$.

- Une unité/terme très répendu dans le monde de la sécurité fonctionnelle et la fiabilité est **Failures In Time** (**FIT**) qui est défini par le taux de défaillance d'un composant sur 1 billion d'heure composant ($10^9$)(ex. 1000 composants pour 1 million d'heures, or 1 million composants pour 1000 heure).

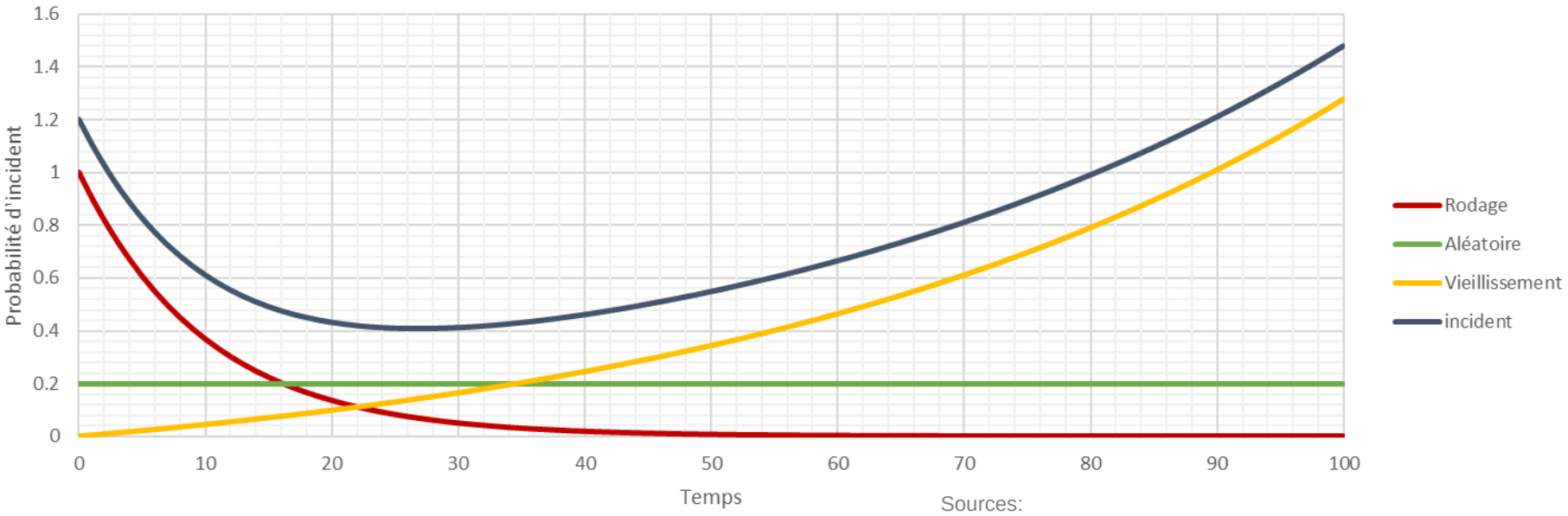
$$\boxed{1\ FIT = 10^{-9}/h}$$

Sources:
[1] Failure Rate, Wikipedia, https://en.wikipedia.org/wiki/Failure_rate

# Courbe de baignoire (1)

En ingénierie la **courbe en baignoire** est une représentation classique de la probabilité d'incidents pour des systèmes. La courbe en baignoire est la somme de trois composantes :

- courbe des incidents liés au rodage du système, qui commence à un niveau élevé puis décroit avec le temps ;
- courbe des incidents aléatoires qui est indépendante de l'âge du système ;
- courbe des incidents liés au vieillissement du système qui débute à des niveaux faibles mais croît de façon continue avec le temps.

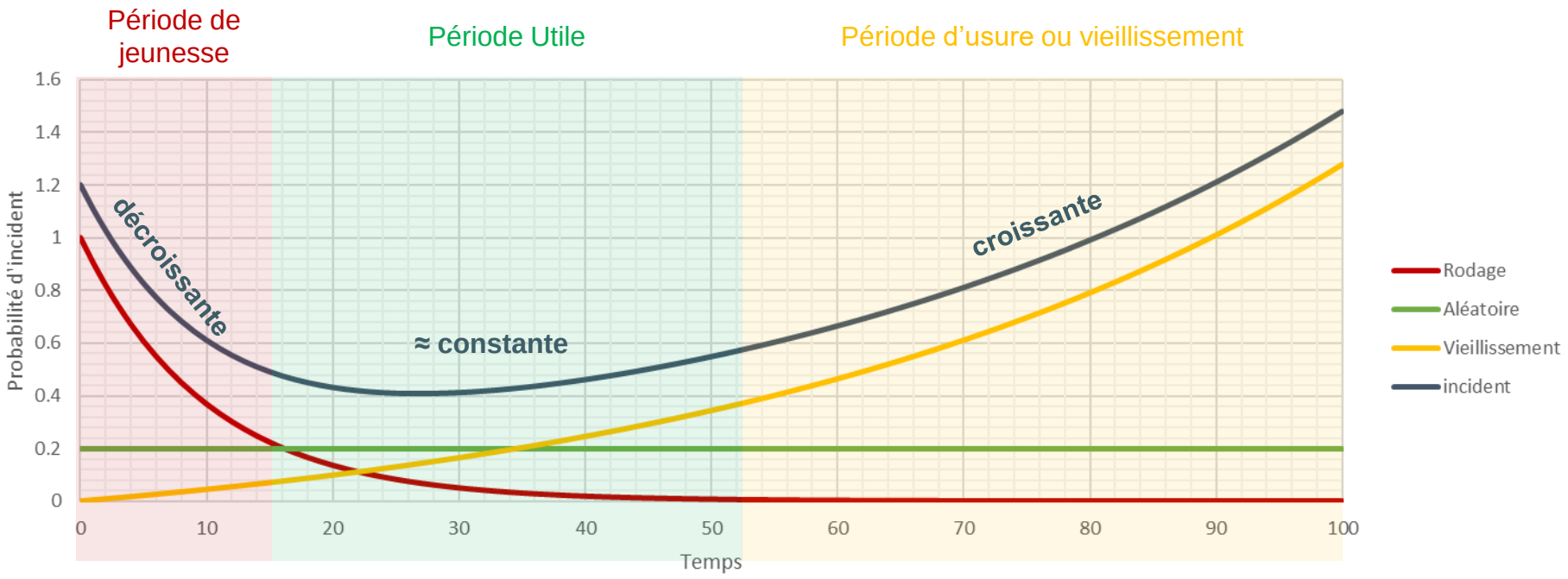



Sources:
[1] Courbe de baignoire, https://fr.wikipedia.org/wiki/Courbe_en_baignoire

# Courbe de baignoire (2)

La **courbe en baignoire** est aussi décrite en 3 périodes (très liés aux courbes décrites ultériement):

- Période Jeunesse (Early Life)
- Période Utile (Useful Life), qui commence à un niveau élevé puis décroit avec le temps ;
- Période d'usure ou vieillissement (Wearout Life)





Sources:
[1] Courbe de baignore, https://fr.wikipedia.org/wiki/Courbe_en_baignoire
[2] Life Data Analysis Reference, https://reliawiki.org/index.php/Life_Data_Analysis_Reference_Book

# Répartition de vie (Life Distribution) (1)

Qu’est-ce qu’une répartition de vie (Life Distribution)?

Une répartition de vie décrit les distributions statistiques qui sont utilisée en fiabilité et en analyse de vie.

Une distribution est décrite par la densité de défaillance $f(t)$ (probability density function : pdf).

Sources:
[1] Life Distributions, Reliawiki, https://reliawiki.org/index.php/Life_Distributions

# Répartition de vie (Life Distribution) (2)

- Exponential Distribution
- Shifted Exponential Distribution
- Normal and Lognormal Distribution
- Phase-Type Distribution
- Gamma Distribution, Erlangian Distribution and Chi-Square Distribution
- Log-Logistic Distribution
- Bernouilli Distribution
- Mass at Origin, Geometric Distribution
- Defective Distribution
- Uniform Distribution
- Binomial Distribution
- Hypergeometric Distribution

Pour le cours:

- Linear Distribution
- Rectangular Distribution
- Exponential Distribution
- Normal and Lognormal Distribution
- Weibull Distribution

Sources:
[1] Life Distributions, Reliawiki, https://reliawiki.org/index.php/Life_Distributions

# Distribution Linéaire

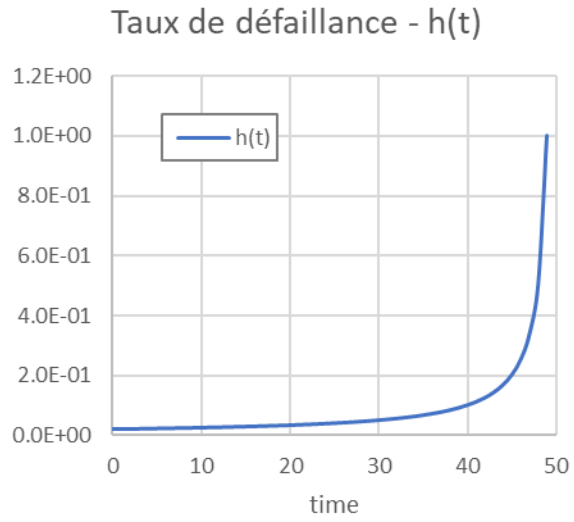
$$F(t) = kt, \text{ pour } (t = 0..\ 50h),\ k = 0.02$$

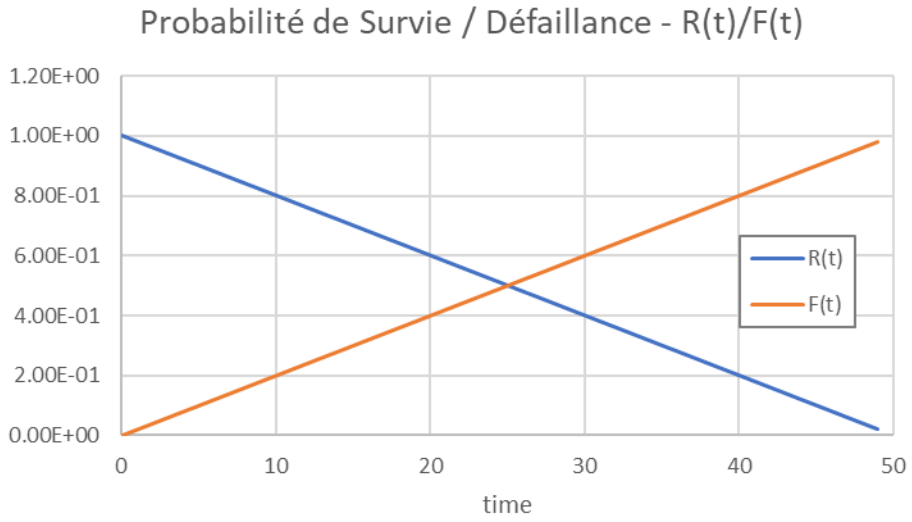
$$R(t) = 1 - kt$$

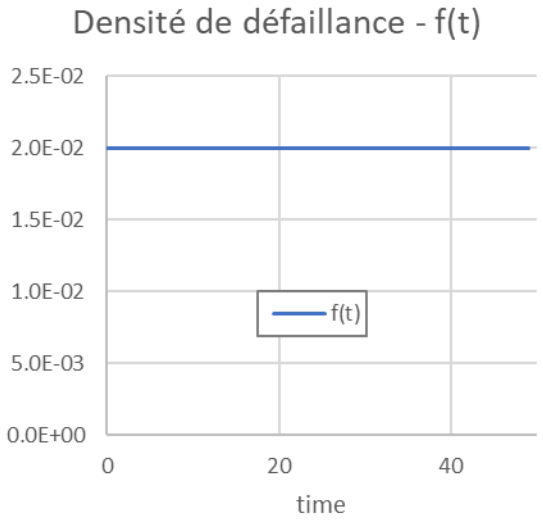
$$f(t) = k$$

$$h(t) = \frac{k}{1 - kt}$$

$$MTTF = \int_0^{\infty} t f(t)\, dt = \int_0^{50} t\, k\, dt = \left[\frac{1}{2} k t^2\right]_0^{50} = 25 - 0 = 25h$$



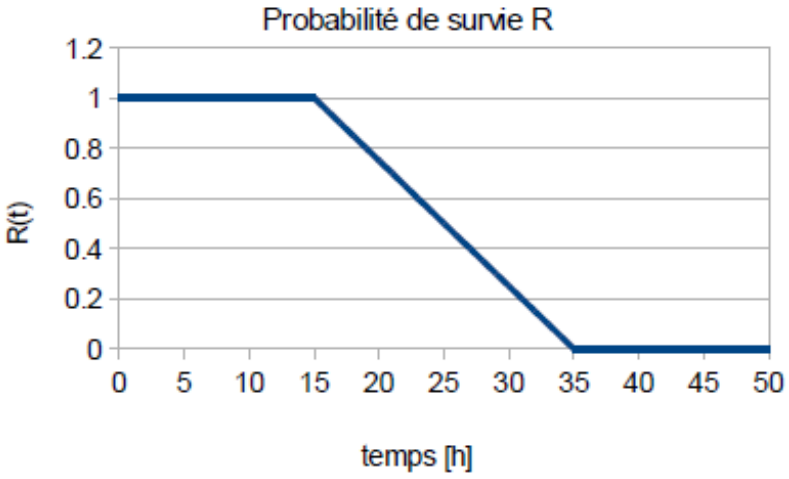
# Distribution rectangulaire (1)

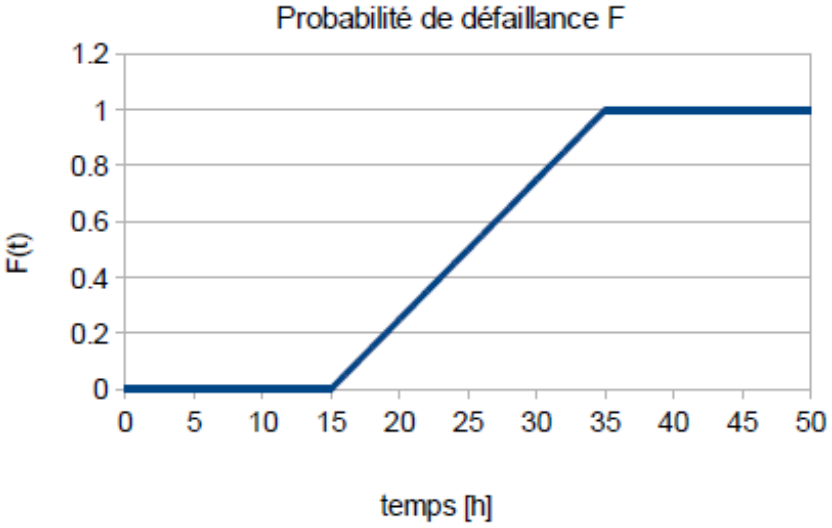
$$\mathrm{f}(t) = \begin{cases} 0 & pour\ 0 < t < a \\ 1/(b-a) & pour\ a \leq t \leq b \\ 0 & pour\ t > b \end{cases}$$

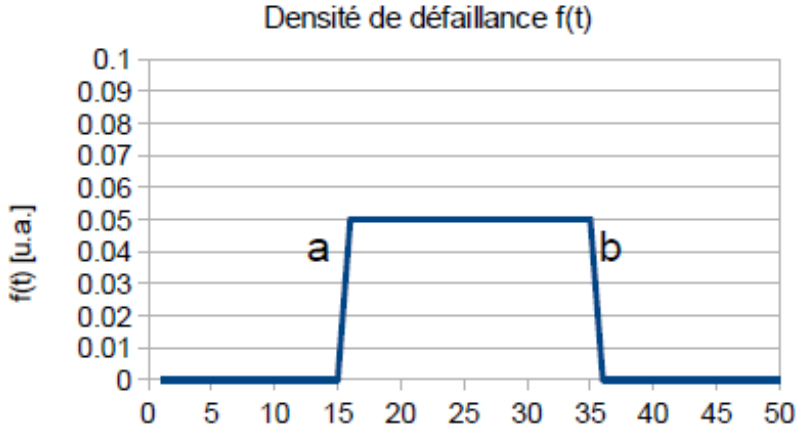
$$\mathrm{h}(t) = \begin{cases} \infty & pour\ 0 < t < a \\ 1/(b-t) & pour\ a < t < b \\ 1/(b-a) & pour\ t > b \end{cases}$$

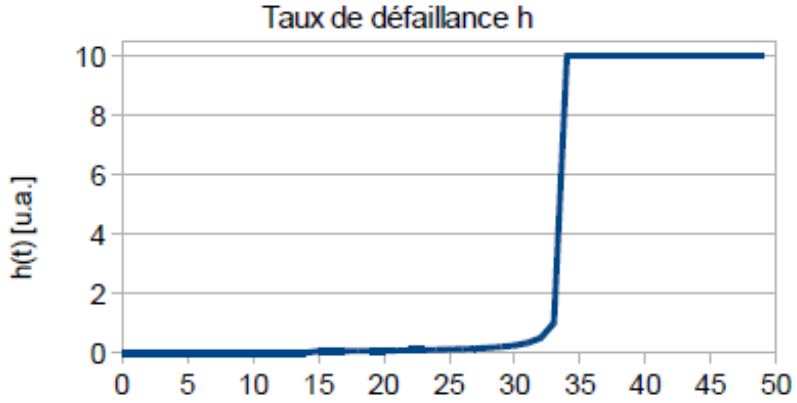
$$\mathrm{R}(t) = \begin{cases} 1 & pour\ 0 < t < a \\ (b-t)/(b-a) & pour\ a \leq t \leq b \\ 0 & pour\ t > b \end{cases}$$

# Distribution rectangulaire (2)



# Distribution Exponentielle (1)

$$F(t) = 1 - e^{-\lambda t}$$

$$R(t) = e^{-\lambda t}$$

$$f(t) = \lambda e^{-\lambda t}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^\infty t f(t)\, dt = \frac{1}{\lambda}$$

Integration par partie:

$$\int v \frac{du}{dt} dt = vu - \int u \frac{dv}{dt} dt$$

Explication:

$$MTTF = \int_0^\infty t f(t)\, dt = \left[-t \cdot e^{-\lambda t}\right]_0^\infty - \int_0^\infty 1 \cdot \left(-e^{-\lambda t}\right) dt = 0 - \left[-\frac{e^{-\lambda t}}{\lambda}\right]_0^\infty = 0 - \left(\frac{e^{-\lambda \infty}}{\lambda} - \frac{e^{-\lambda 0}}{\lambda}\right) = \frac{1}{\lambda}$$

Avec:

$$v = t \qquad du/_{dt} = \lambda e^{-\lambda t}$$

$$dv/_{dt} = 1 \qquad dv/_{dt} = -\lambda/_{\lambda} e^{-\lambda t} = -e^{-\lambda t}$$

# Distribution Exponentielle (2)

- Taux de défaillance : $h(t) = \lambda = 1FIT = (10^{-9} failure/h)$

$$1ans = 8760hours$$

$$F(t) = 1 - e^{-\lambda t}$$

$$R(t) = e^{-\lambda t}$$

$$f(t) = \lambda e^{-\lambda t}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^\infty t f(t)\, dt = \frac{1}{\lambda} = \frac{1}{1\ FIT} = \frac{1}{10^{-9}\ failure/h} = 10^9 hour/failure$$

- Pour cette distribution, 1 FIT signifie après 114155 ans, 63.2% des pieces sont en pannes.

$$R(t) = e^{-\lambda t} = e^{-\frac{1}{MTTF}t}$$

$$R(MTTF) = e^{-\frac{1}{MTTF}t} = e^{-\frac{1}{10^9}10^9} = e^{-1} = 0.367 = 36.7\%$$

$$F(MTTF) = 63.2\%$$

# Distribution Exponentielle (3)

- Taux de défaillance : $h(t) = \lambda = 1FIT = (10^{-9} failure/h)$

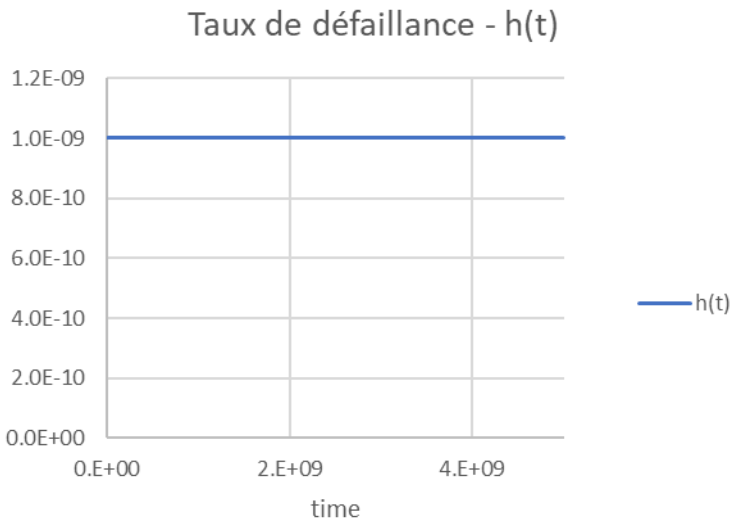
$$F(t) = 1 - e^{-\lambda t}$$

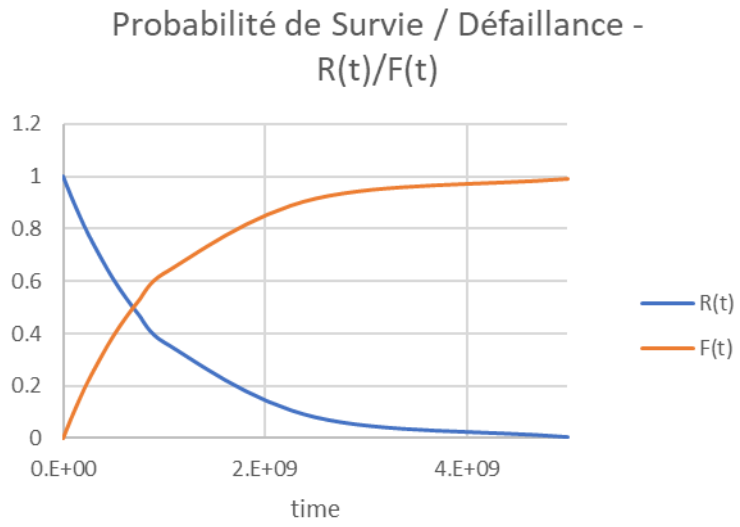
$$R(t) = e^{-\lambda t}$$

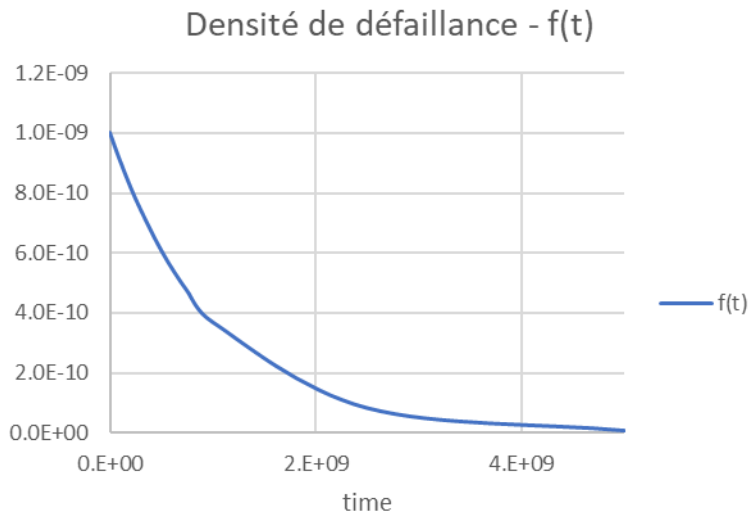
$$f(t) = \lambda e^{-\lambda t}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^{\infty} t f(t)\, dt = \frac{1}{\lambda} = \frac{1}{1\ FIT} = \frac{1}{10^{-9}\ failure/h} = 10^9 hour/failure$$



# Distribution Exponentielle décallée (1)

$$F(t) = 1 - e^{-\lambda(t-a)}$$

$$R(t) = e^{-\lambda(t-a)}$$

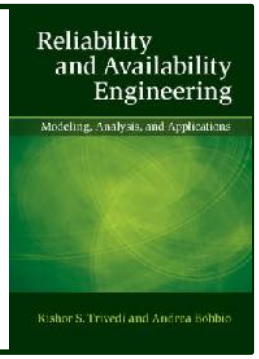
$$f(t) = \lambda e^{-\lambda(t-a)}$$

$$h(t) = \lambda$$

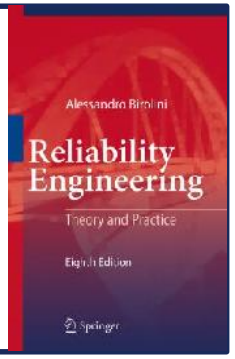
$$MTTF = \int_0^{\infty} (t-a) f(t-a)\, dt = \mathrm{a} + \frac{1}{\lambda}$$

# Distribution de Weibull (1)

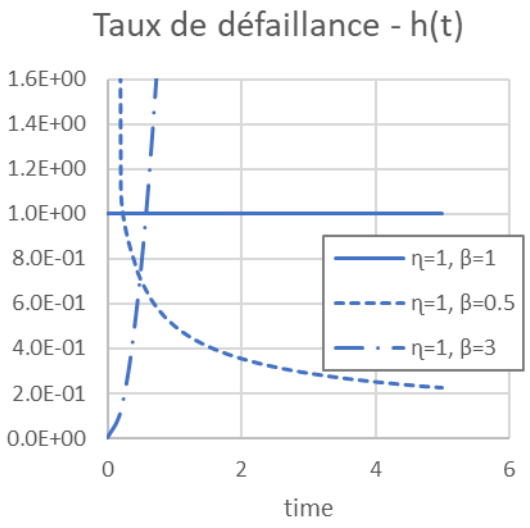
$$F(t) = 1 - e^{-(\eta t)^{\beta}}$$
$$R(t) = e^{-(t\eta)^{\beta}}$$
$$f(t) = \beta\eta \cdot (\eta t)^{\beta-1} \cdot e^{-(\eta t)^{\beta}}$$
$$h(t) = \beta\eta \cdot (\eta t)^{\beta-1}$$

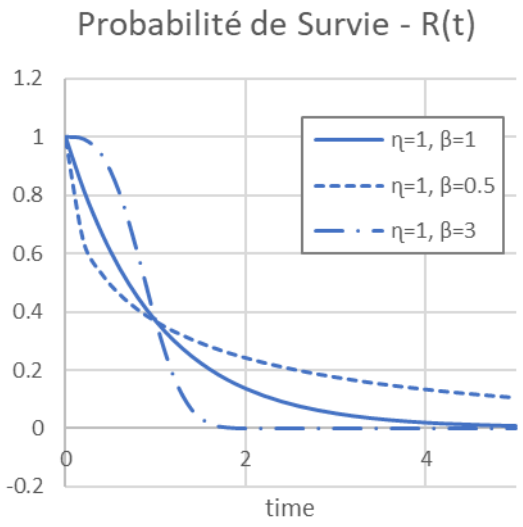


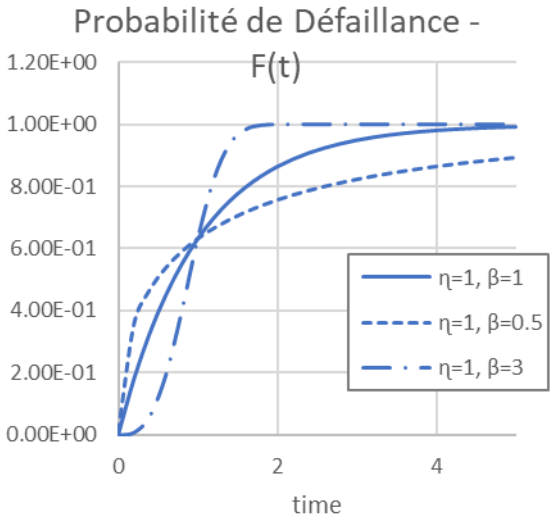

$$= 1 - e^{-(\lambda t)^{\beta}}$$
$$= e^{-(\lambda t)^{\beta}}$$
$$= \beta\lambda \cdot (\lambda t)^{\beta-1} \cdot e^{-(\lambda t)^{\beta}}$$
$$= \beta\lambda \cdot (\lambda t)^{\beta-1}$$

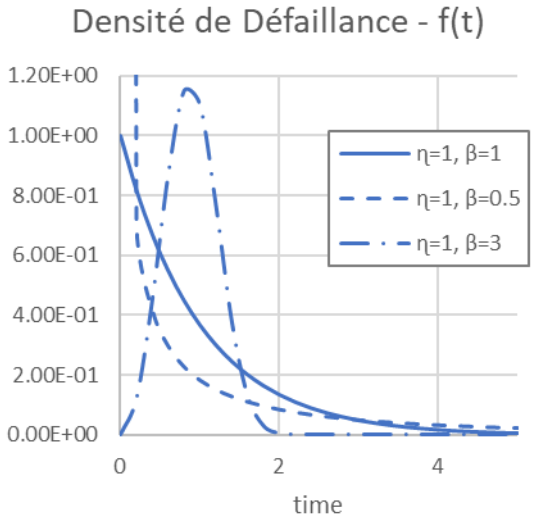



$$= 1 - e^{-(\alpha t)^{\beta}}$$
$$= e^{-(\alpha t)^{\beta}}$$
$$= \beta\alpha \cdot (\alpha t)^{\beta-1} \cdot e^{-(\alpha t)^{\beta}}$$
$$= \beta\alpha \cdot (\alpha t)^{\beta-1}$$



# Distribution de Weibull (2)

$$F(t) = 1 - e^{-(t\eta)^{\beta}}$$

$$R(t) = e^{-(t\eta)^{\beta}}$$

$$f(t) = \beta\eta \cdot (\eta t)^{\beta-1} \cdot e^{-(\eta t)^{\beta}}$$

$$h(t) = \beta\eta \cdot (\eta t)^{\beta-1}$$

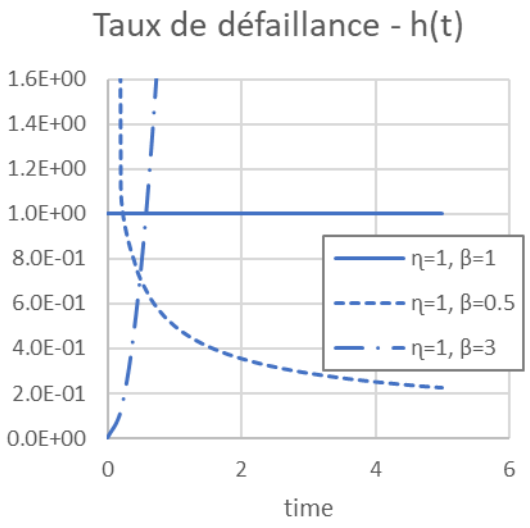
Si η = λ et β = 1, alors nous retrouvons une distribution exponentielle

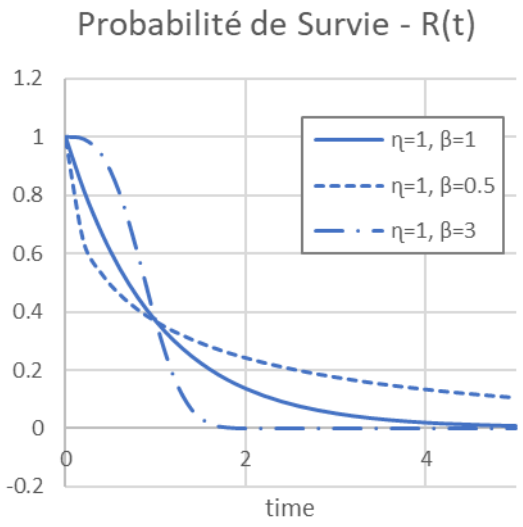
$$F(t) = 1 - e^{-(\lambda t)^{\beta}} = 1 - e^{-\lambda t}$$

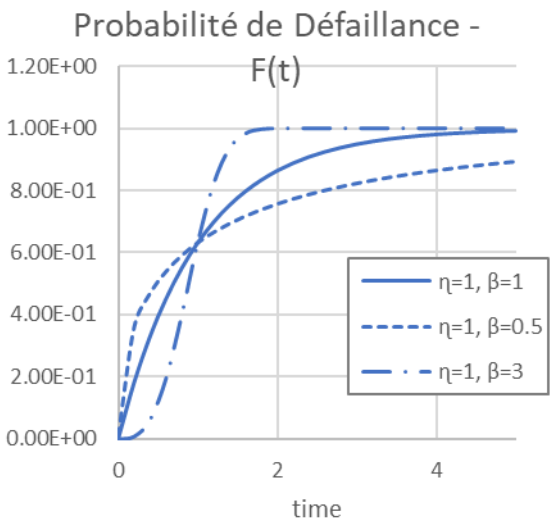
$$R(t) = e^{-(\lambda t)^{\beta}} = e^{-\lambda t}$$

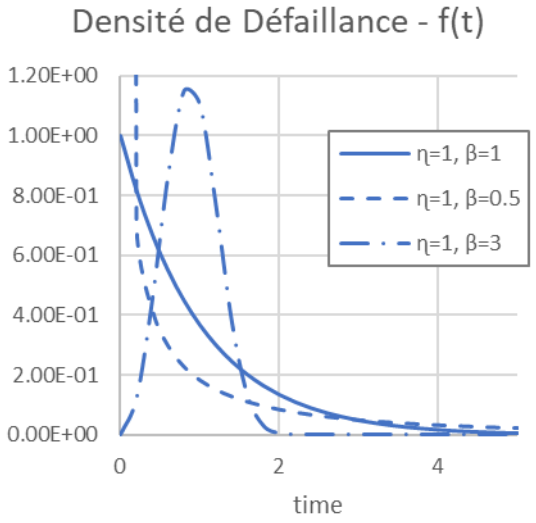
$$f(t) = \lambda \cdot (\lambda t)^{1-1} \cdot e^{-(\lambda t)^{1}} = \lambda e^{-\lambda t}$$

$$h(t) = \lambda \cdot (\lambda t)^{1-1} = \lambda$$



# Distribution Normal (Distribution de Gauss) (1)

$$F(\mathrm{x}) = \Phi\left(\frac{x-\mu}{\sigma}\right)$$

$$f(x) = \frac{1}{\sqrt{2\pi}\cdot\sigma}\cdot e^{\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)}$$

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{\left(-\frac{t^2}{2}\right)}\,dt$$

Une autre méthode est de par:

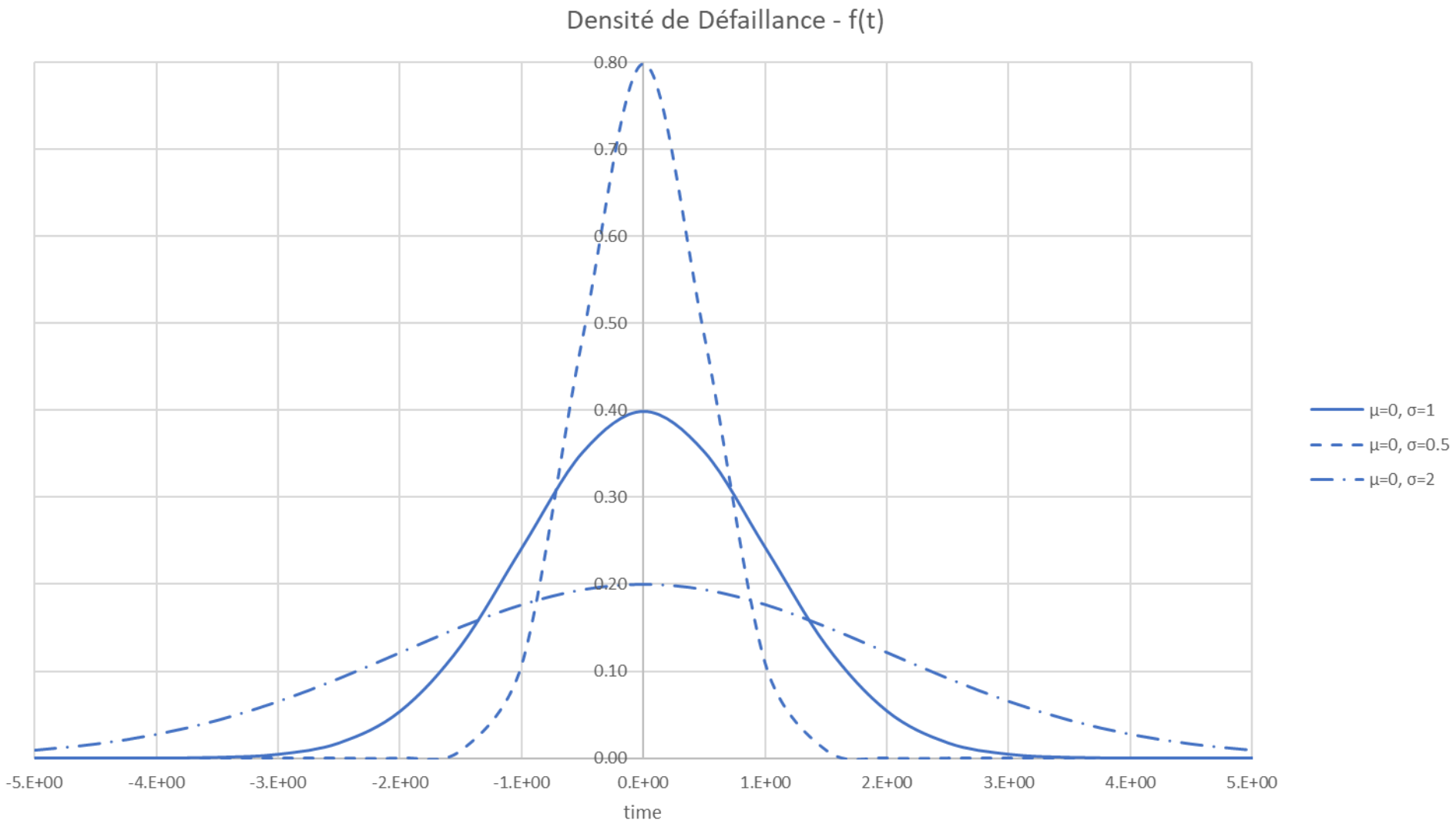
$$\Phi(x) = \frac{1}{2} + \frac{1}{\sqrt{2\pi}}e^{\left(-\frac{x^2}{2}\right)}\cdot\left[x + \frac{x^3}{3} + \frac{x^5}{3\cdot 5} + \cdots + \frac{x^{2n+1}}{(2n+1)!!}\right]$$

La double factorial n!!:

$$\mathrm{n!!} = \begin{cases} \prod_{k=1}^{\frac{n}{2}-1}(2k) = n(n-2)(n-4)\ldots. & ,for\ n > 0\ odd \\ \prod_{k=1}^{\frac{n+1}{2}}(2k-1) = n(n-2)(n-4)\ldots. & ,for\ n > 0\ even \\ 1 & ,for\ n = -1{,}0 \end{cases}$$

Sources:
[1] Double factorial, Wikipedia, https://en.wikipedia.org/wiki/Double_factorial

# Distribution Normal (Distribution de Gauss) (2)



# Exercices 2 (1)

1) Un composant dispose d'une distribution exponentielle et d'un taux de défaillance de $10^{-5}/h$.

Avec quelle probabilité vit-t-il plus que :

- 2'000 h
- 20'000 h
- 100'000 h

# Exercices 2 (2)

1) Un système technique est distribué selon Weibull avec les paramètres :
$\eta = 10^{-7}/h$
$\beta = 0.7$

a. Quelle est la probabilité que le système tombe en panne pendant la première année?
b. Quelle est la probabilité que le système tombe en panne pendant 10 ans, s'il a déjà survécu 5 ans?
c. Quelle valeur prend $\beta$, si après 2 ans 5% des systems sont tombés en panne ($\eta = 1.671 \cdot 10^{-10}(1/h)^{\beta}$
d. Quels types de défaillance peut-on trouver pour a. et c. (selon Weibull et la courbe de baignore)?

# Solution (1)

1) Un composant dispose d'une distribution exponentielle et d'un taux de défaillance de $10^{-5}/h$.

Avec quelle probabilité vit-t-il plus que :

- 2'000 h
- 20'000 h
- 100'000 h

Solution:

$R(t) = e^{-\lambda t}$

$R(2000) = e^{-10^{-5}/h*2000h} = e^{-0.02} = 0.98 \approx 98\%$

$R(20000) = e^{-10^{-5}/h*20000h} = e^{-0.2} = 0.81 \approx 81\%$

$R(100000) = e^{-10^{-5}/h*100000h} = e^{-1} = 0.367 \approx 36.7\%$

# Solution (3)

1) Un système technique est distribué selon Weibull avec les paramètres :

$\eta = 10^{-7}/h$

$\beta = 0.7$

a. Quelle est la probabilité que le système tombe en panne pendant la première année?

Solution:

$$F(t) = 1 - R(t) = 1 - e^{-(\eta t)^{\beta}} = 1 - e^{-(\alpha t)^{\beta}}$$

$$F(t) = 1 - e^{-\left(10^{-7} t\right)^{0.7}}$$

$$F(1ans) = F(8760) = 1 - e^{-\left(10^{-7} 8760h\right)^{0.7}}$$

$$F(8760) = 1 - e^{-\left(\frac{8760}{10^{7}}\right)^{0.7}} = 1 - 0.992786 = 0.007214 \approx 0.72\%$$

# Solution (4)

1) Un système technique est distribué selon Weibull avec les paramètres :

$\eta = 10^{-7}/h$

$\beta = 0.7$

b. Quelle est la probabilité que le système tombe en panne pendant 10 ans, s'il a déjà survécu 5 ans?

Solution A:

Si l'on suppose que le système a été **en service pendant 5 ans** sans défaillance et qu'il a été **maintenu ("réparé")** après **5 ans**, le système est considéré comme **"neuf"** et le calcul de la **probabilité de défaillance recommence à partir de 5 ans à "0"** ("reset").

$$F(t) = 1 - R(t) = 1 - e^{-(\eta t)^{\beta}} = 1 - e^{-(\alpha t)^{\beta}}$$

$$F(8760) = 1 - e^{-\left(\frac{(10ans - 5ans)8760}{10^7}\right)^{0.7}} = 0.022089 \approx 2.2\%$$

# Solution (5)

1) Un système technique est distribué selon Weibull avec les paramètres :

$\eta = 10^{-7}/h$

$\beta = 0.7$

b. Quelle est la probabilité que le système tombe en panne pendant 10 ans, s'il a déjà survécu 5 ans?

Solution B:

Quelle est la probabilité de défaillance pour la **période de 5 à 10 ans**, si l'on suppose que le système est **en service depuis 5 ans** sans défaillance et qu'il **n'a pas été maintenu** ("réparé") au **bout de 5 ans**, le système est considéré comme **"utilisé" en permanence** (sans «reset») et le calcul de la **probabilité de défaillance commence** en fait au temps **t=0**.

$$F(t) = 1 - R(t) = 1 - e^{-(\eta t)^{\beta}} = 1 - e^{-(\alpha t)^{\beta}}$$

$$F(10ans) - F(5ans) = 1 - e^{-\left(\frac{(10ans*8760}{10^7}\right)^{0.7}} - 1 - e^{-\left(\frac{(5ans*8760}{10^7}\right)^{0.7}} = 0.0135 \approx 1.35\%$$

# Solution (6)

Logarithm Power Rule
$\log(x^y) = y \cdot \log(x)$

1) Un système technique est distribué selon Weibull avec les paramètres :
$\eta = 10^{-7}/h$
$\beta = 0.7$

Logarithm Quotient rule
$\log(x/y) = \log(x)/\log(y)$

c. Quelle valeur prend $\beta$, si après 2 ans 5% des systems sont tombés en panne
$(\eta = 1.671 \cdot 10^{-10}(1/h)^{\beta}$

Solution:

$$R(t) = e^{-(t\eta)^{\beta}} = e^{-\left(2ans*8760*1.671*10^{-10}\right)^{\beta}} = 0.95$$

$$R = e^{-(\eta \cdot t)^{\beta}} \quad => \quad -ln(R) = (\eta \cdot t)^{\beta} \quad => \quad \ln(-\ln(R)) = \beta \cdot \ln(\eta \cdot t) \quad => \quad \beta = \frac{\ln(-\ln(R))}{\ln(\eta \cdot t)}$$

$$\beta = \frac{\ln(-\ln(R))}{\ln(\eta \cdot t)} = \frac{\ln(-\ln(0.95))}{\ln(1.671 * 10^{-10} * 2 * 8760)} = 0.233$$

Verif : $R(t) = e^{-(t\eta)^{\beta}} = e^{-\left(2ans*8760*1.671*10^{-10}\right)^{0.233}} \approx 0.95$

# Solution (7)

1) Un système technique est distribué selon Weibull avec les paramètres :

$\eta = 10^{-7}/h$

$\beta = 0.7$

d. Quels types de défaillance peut-on trouver pour a. et c. (selon Weibull et la courbe de baignore)?

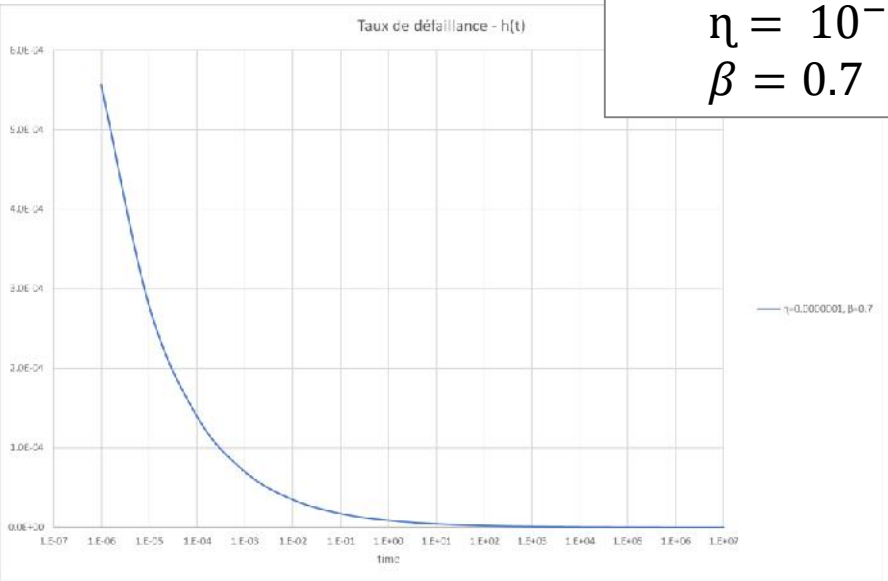
Solution:

| Pour a. | Pour c. |
|---|---|
| $\eta = 10^{-7}/h$ | $\eta = 1.671 * 10^{-10}/h$ |
| $\beta = 0.7$ | $\beta = 0.233$ |

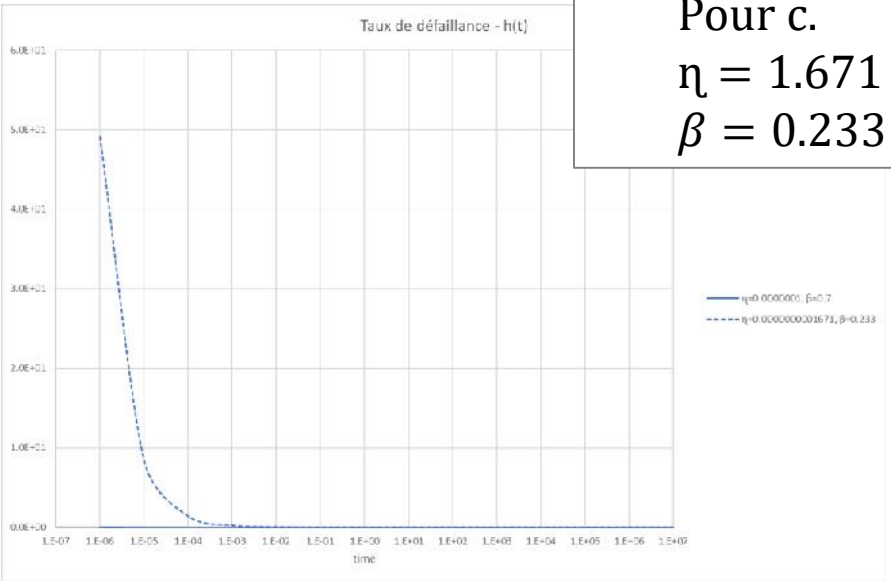
# Solution (8)

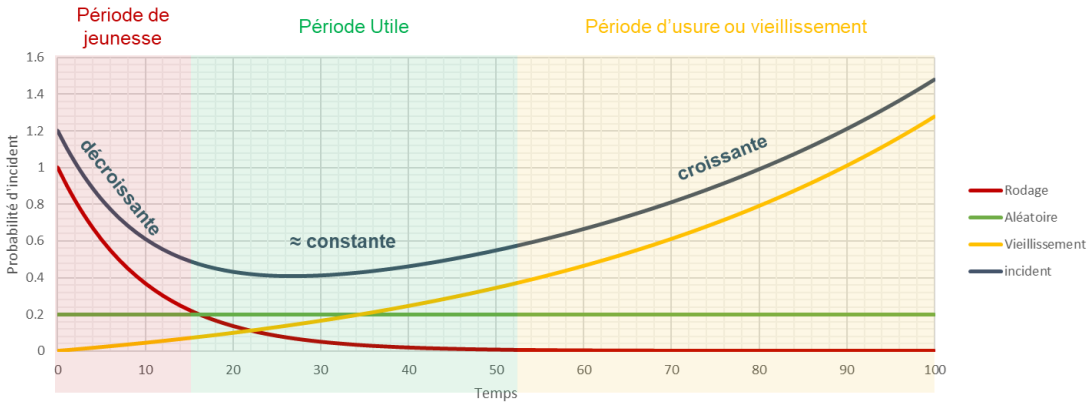
Solution:

Pour a.
$\eta = 10^{-7}/h$
$\beta = 0.7$




Pour c.
$\eta = 1.671 * 10^{-10}/h$
$\beta = 0.233$




Pour les deux courbes, nous nous trouvons dans la période de jeunesse.

# Merci pour votre attention

Questions ou remarques: jonathan.hendriks@hefr.ch ou via Teams

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et fiabilité des systèmes (SecuFS)

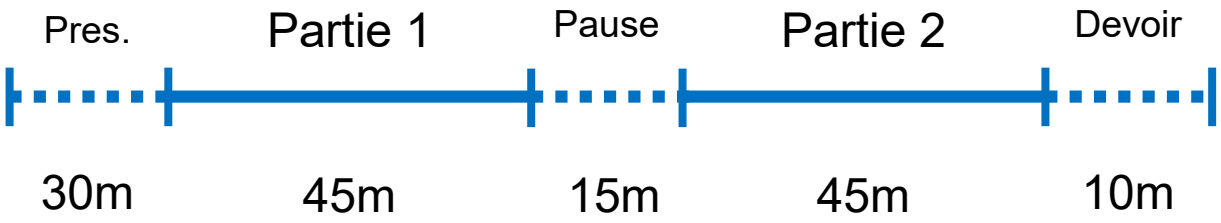
# 11 –Fiabilité des systèmes techniques - Niveau systèmes

Jonathan Hendriks
13.12.2021

# Contenu du cours

| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | Workshop «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| Examen | | 31.01.2022 | Examen écrit | |
| Total | **42** | | | |

# Structure du cours




**Structure du cours:**

17h30: Présentations individuelles
18h00: Partie 1
18h45: Pause de 15min
19h00: Partie 2
19h45: Temps à disposition pour débuter les exercices
19h55: Fin du cours

# Exercices 2 (1)

1) Un composant dispose d'une distribution exponentielle et d'un taux de défaillance de $10^{-5}/h$.

Avec quelle probabilité vit-t-il plus que :

- 2'000 h
- 20'000 h
- 100'000 h

# Exercices 2 (2)

1) Un système technique est distribué selon Weibull avec les paramètres :
$\eta = 10^{-7}/h$
$\beta = 0.7$

a. Quelle est la probabilité que le système tombe en panne pendant la première année?
b. Quelle est la probabilité que le système tombe en panne pendant 10 ans, s'il a déjà survécu 5 ans?
c. Quelle valeur prend $\beta$, si après 2 ans 5% des systems sont tombés en panne ($\eta = 1.671 \cdot 10^{-10}(1/h)^{\beta}$
d. Quels types de défaillance peut-on trouver pour a. et c. (selon Weibull et la courbe de baignore)?

# RAMS (1)

R

**Reliability**

"The ability of a technical system to perform its required functions under given conditions for a given period of time (mission time)".

A

**Availability**

"the ability of a technical system to perform a specific function at specific operational conditions at a moment in time under consideration of the system reliability and maintenance/repair activities".

M

**Maintainability**

"The feasibility that a certain maintenance measure can be executed for a system under given boundary conditions within a defined period of time, if the maintenance will be performed under defined conditions, a defined process and auxiliary materials will be used".

S

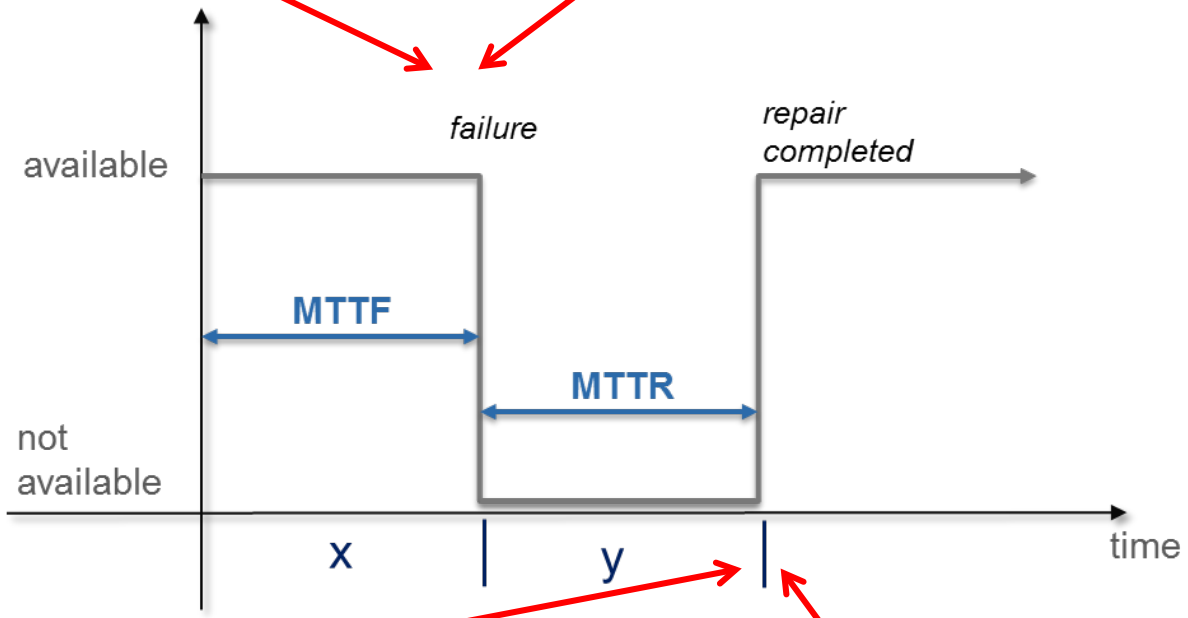
**Safety**

"the non-existence of unacceptable damage risk".

# RAMS (2)

**Reliability:**
„… the engine of a locomotive fails after “x” hours of reliable operation (MTTF);
**no safety issue** when occurring on a safe area **on ground**.”

**Safety:**
„… the engine of a locomotive fails after “x” hours of reliable operation **while the train is moving** – **safety issue!**”




**Availability:**
„… the engine of a locomotive fails after “x” hours of reliable operation, but can be repaired in “y” hours.”

**Maintainability:**
„… corrective action: the engine of a locomotive failed after “x” hours of reliable operation; to make the vehicle again available after “y” hours repair time (MTTR).”

# Analyse de Fiabilité (1)

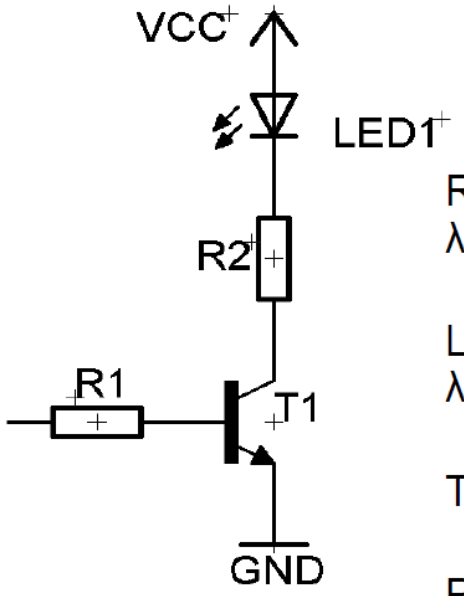
1. Reliability Block Diagram (RBD)
2. Markov Chain
3. Petri Nets

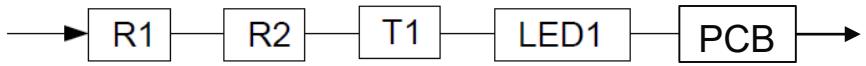
# RBD : Bloc Fonctionnel(1)

# RBD : Série(1)

# RBD : Parallèle (1)

# Un autre exemple




R1 et R2:
$\lambda_R = \lambda_b\, \pi_E\, \pi_Q\, \pi_R = 0.78 \cdot 2.4 \cdot 0.3 \cdot 1 \cdot 10^{-9} \approx 1 \cdot 10^{-9}$ /h

LED1:
$\lambda_L = \lambda_b\, \pi_T\, \pi_E\, \pi_Q = 0.65 \cdot 30 \cdot 2.4 \cdot 0.1 \cdot 10^{-9} \approx 5 \cdot 10^{-9}$ /h

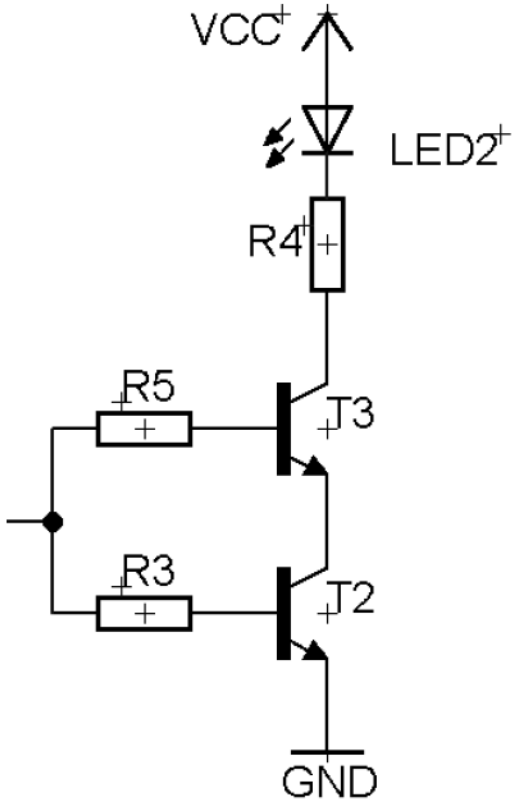
T1: $\lambda_T \approx 14 \cdot 10^{-9}$ /h

PCB + brasures: $\lambda_P \approx 2 \cdot 10^{-9}$ /h

$\lambda_S = 2 \cdot \lambda_R + \lambda_L + \lambda_T + \lambda_P \approx 23$ FIT

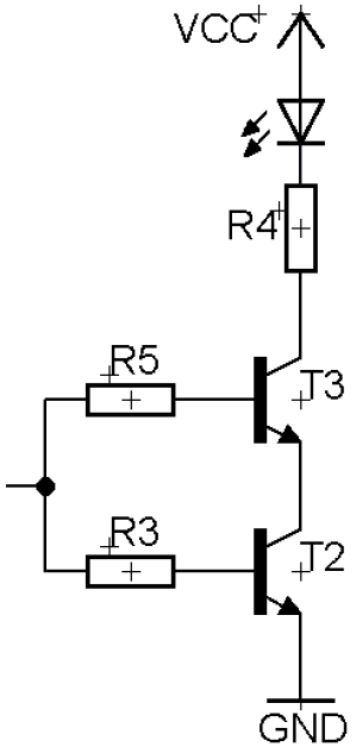
MTBF = $1/\lambda_S \approx 4.3 \cdot 10^7$ h ≈ 5000 a

# Amélioration avec une redondance

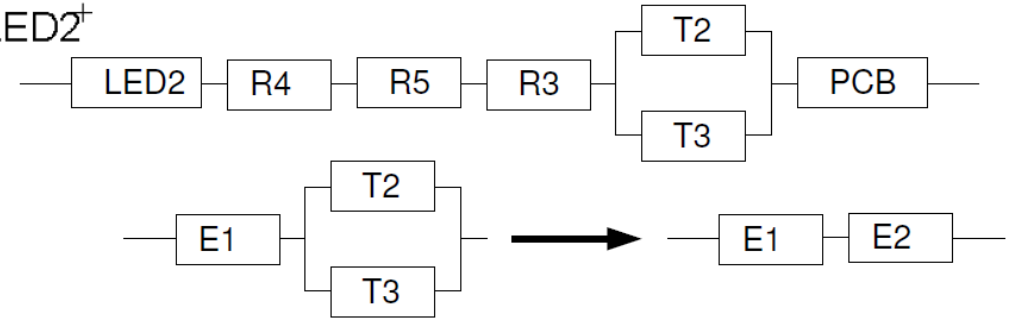



- Modes de défaillance ?
- Diagramme de bloc ?
- Calcule de MTTF ?

# Solutions de la page 42 des slides




Mode de défaillance: Court circuit




$\lambda_{E1} = \lambda_{LED} + 3 \cdot \lambda_R + \lambda_{PCB} = 10$ FIT

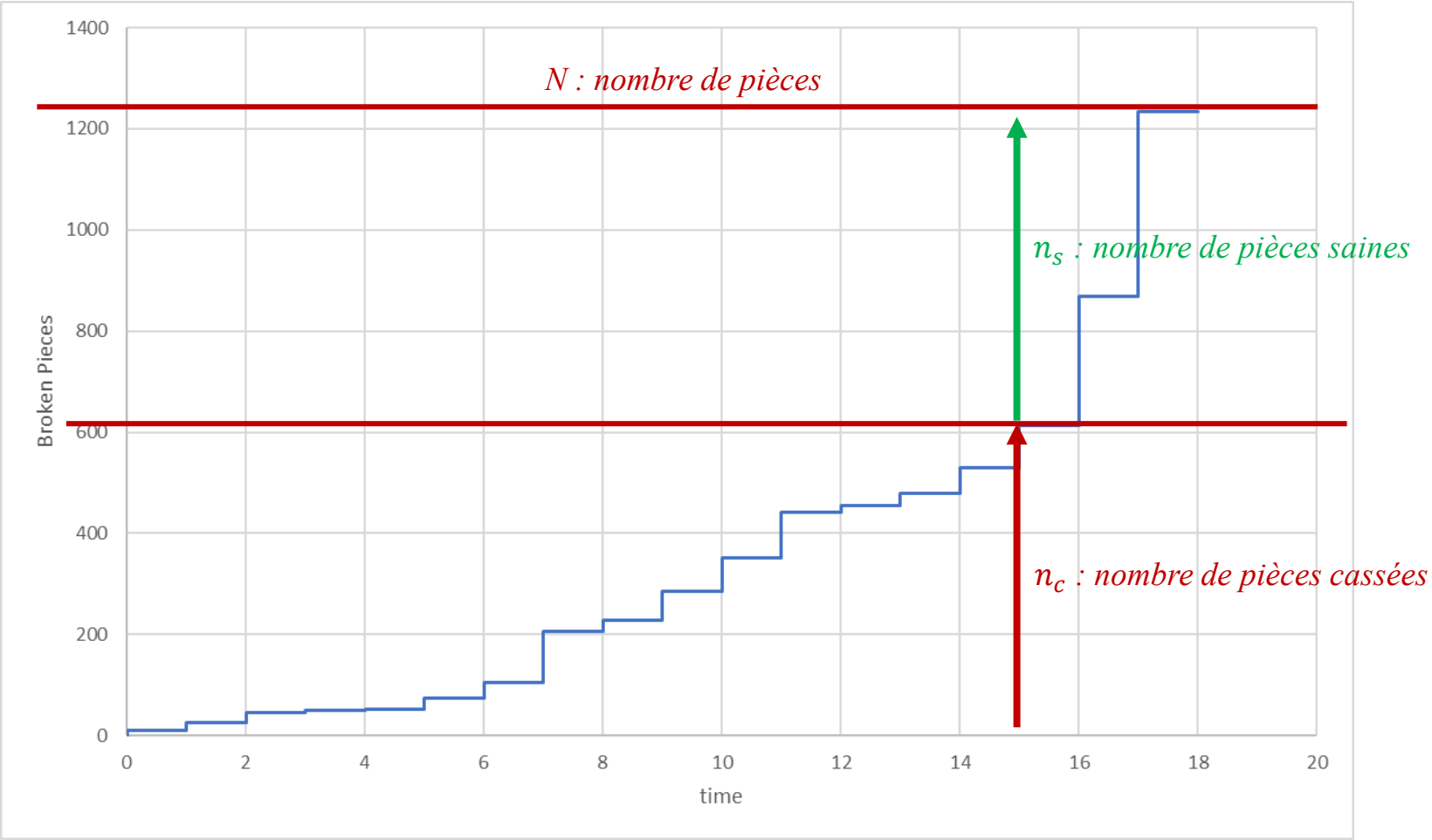
$\lambda_{E2} = 2/3 \cdot \lambda_T = 2/3 \cdot 14$ FIT $\approx 9$ FIT <= $\lambda_{T2} = \lambda_{T3}$

$\lambda_s = \lambda_{E1} + \lambda_{E2} = 19$ FIT

MTTF $= 1/\lambda_s \approx 6000$ années

après 6000 ans il y a encore 37% des circuit qui fonctionnent

# Hazard Rate – H(t)




$$N = n_c + n_s$$

where

$n_c$ = les pièces cassées

$N$ = le nombre des pièces

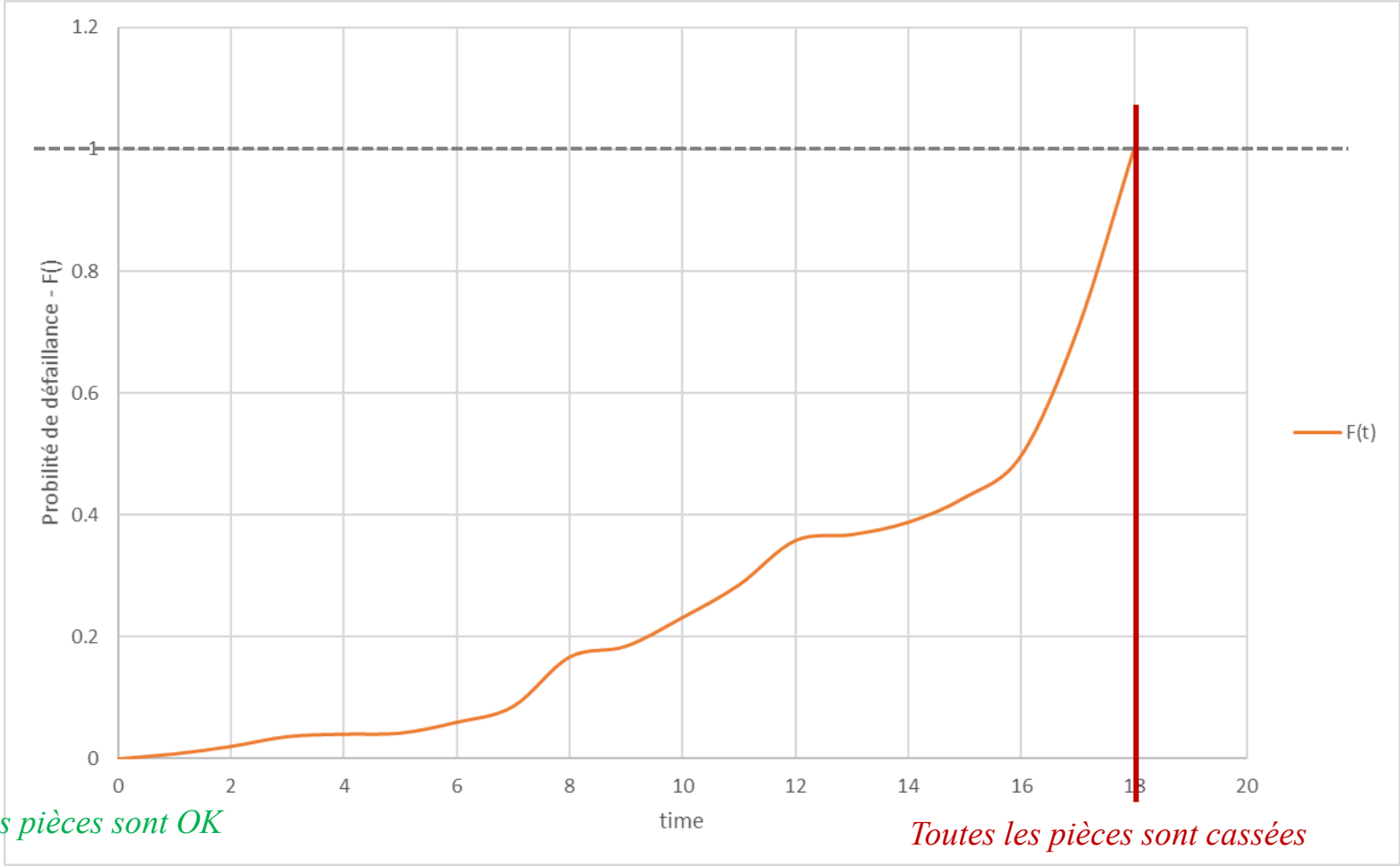
$n_s$ = les pièces survies

Hazard Rate:

$$H = \frac{n_c}{N}$$

$$H(\Delta t) = \frac{1 * \Delta n_c}{n_s * \Delta t}$$

# Probabilité de défaillance – F(t)




$$N = n_c + n_s$$

where

$n_c$ = les pièces cassées

$N$ = le nombre des pièces

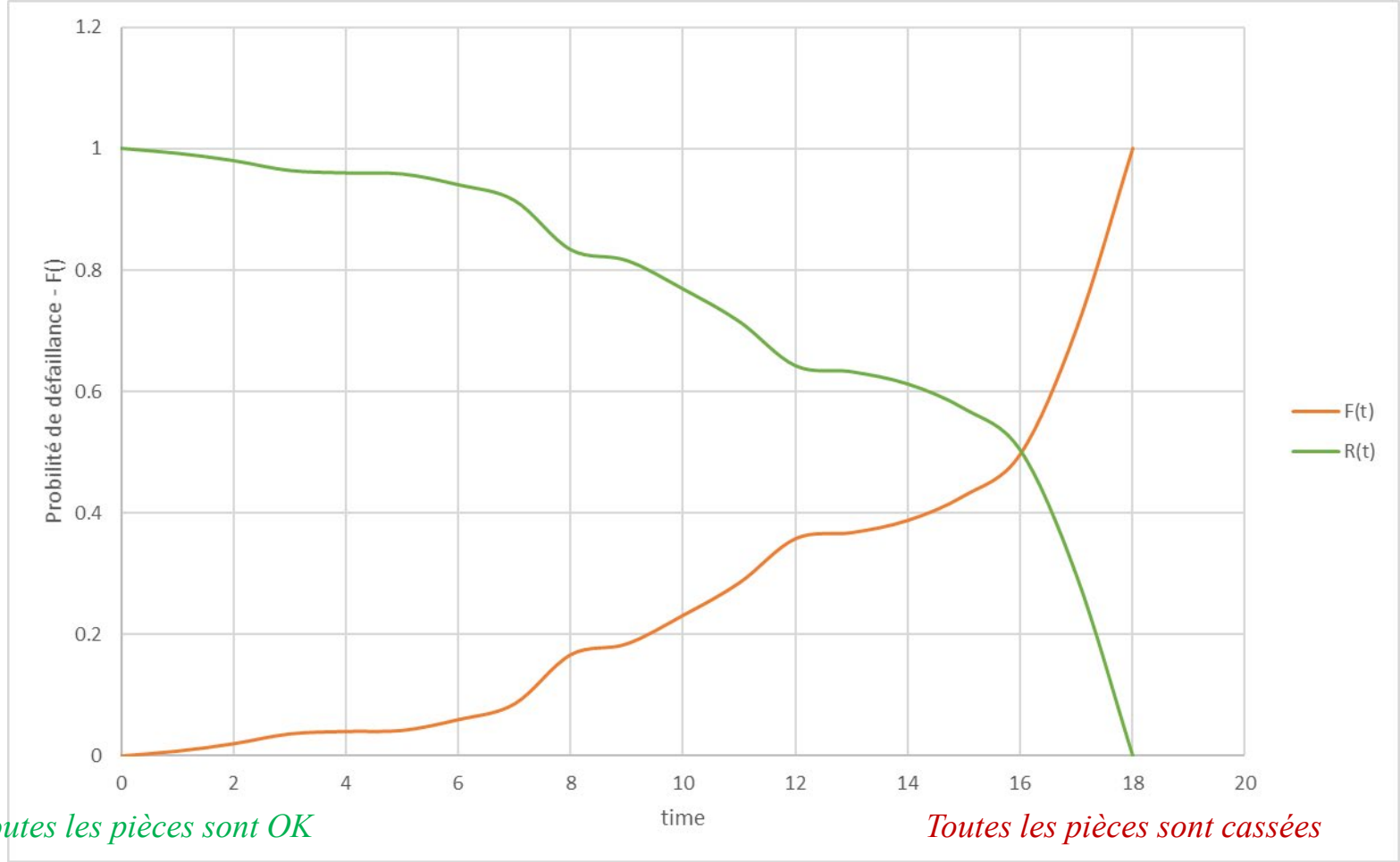
$n_s$ = les pièces survies

Failure Rate – F(t):

$$F(t) = \frac{n_c(t)}{N}$$

$$F(0) = 0$$
$$F(\infty) = 1$$

# Probabilité de survie – R(t)




Failure Rate – F(t):

$$F(t) = \frac{n_c}{N}$$

Survival Rate – R(t):

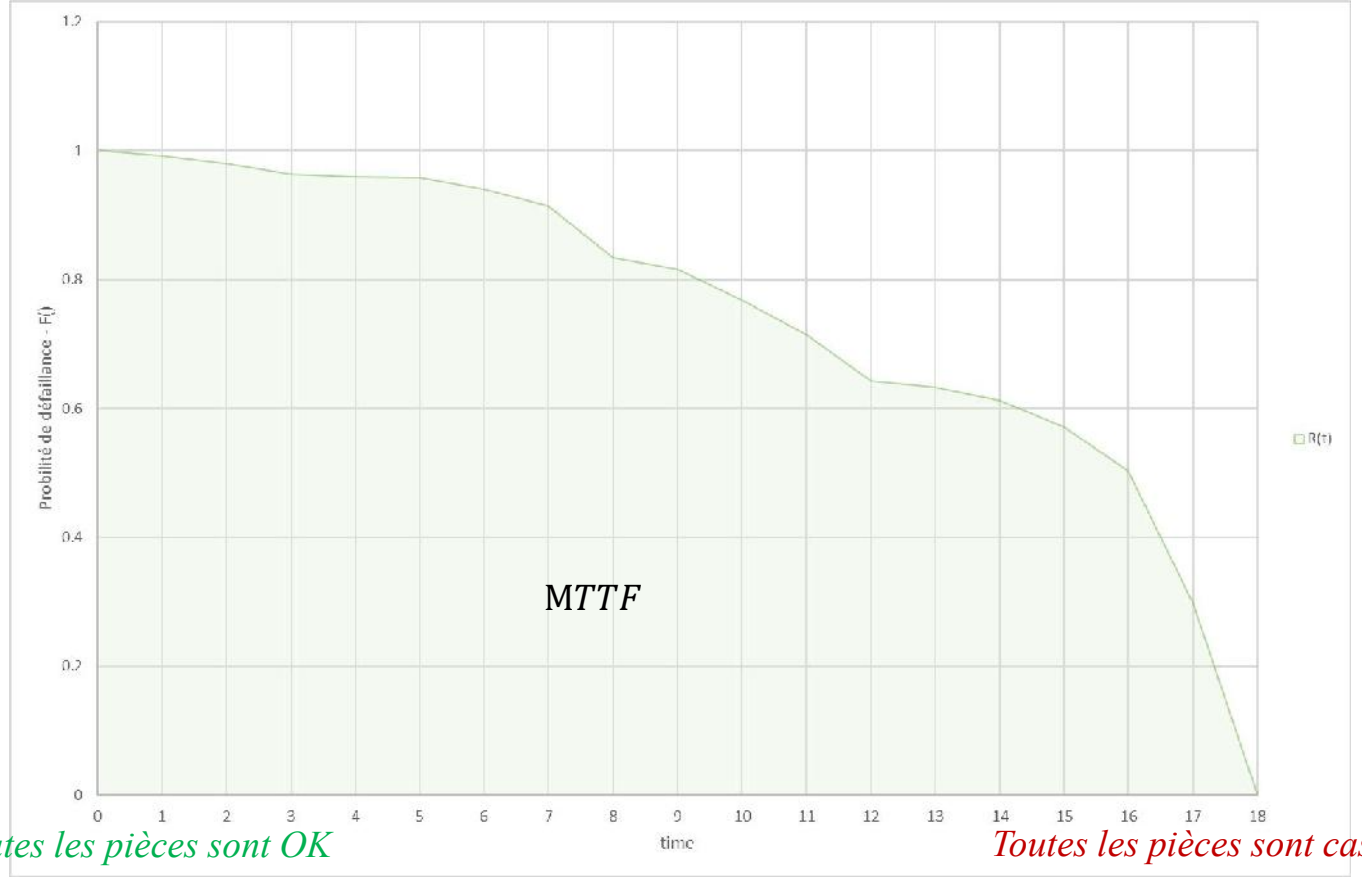
$$F(t) = 1 - R(t)$$

$$1 = F(t) + R(t)$$

$$R(t) = \frac{n_s(t)}{N}$$

# Espérance de vie – MTTF (système non réparable)

Mean Time To Failure (MTTF) mesure la valeur moyenne de temps qu'un système non-reparable peut fonctionner avant d'être en panne.




*Toutes les pièces sont OK*

*Toutes les pièces sont cassées*

Survival Rate – R(t):

$$R(t) = \frac{n_s(t)}{N}$$

Mean Time To Failure – MTTF:

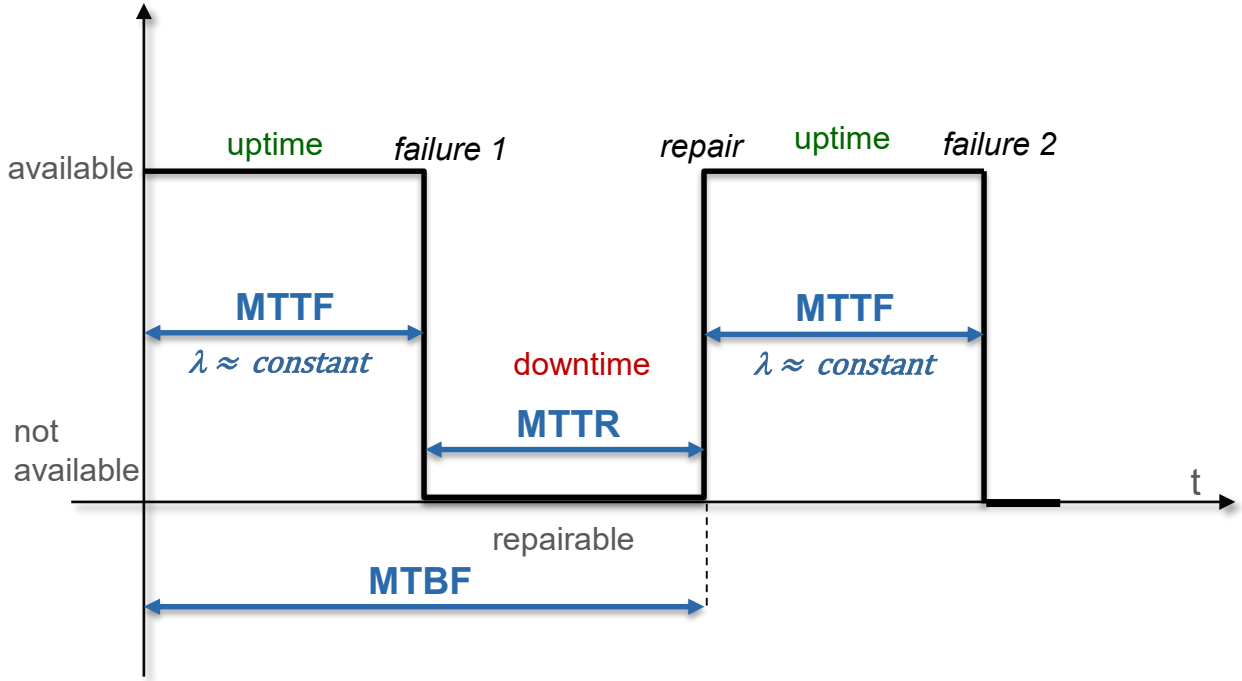
$$MTTF = \int_0^\infty R(t)dt$$

# Espérance de vie (1)

Mean Time To Failure (MTTF) mesure la valeur moyenne de temps qu'un système non-réparable peut fonctionner avant d'être en panne.

Mean Time To Failure (MTBF) mesure la valeur moyenne de temps qu'un système met pour un cycle panne/restoré.

Mean Time To Repair (MTTR) mesure la valeur moyenne de temps de réparation sur un système




$$MTBF = MTTF + MTTR$$

Système Non-Réparable :

$MTTR = 0$

$MTBF = MTTF$

# Espérance de vie (2)

Integration par partie:

$$\int v\frac{du}{dt}dt = vu - \int u\frac{dv}{dt}dt$$

Explication:

$$MTTF = \int_0^\infty t f(t)\,dt = -\int_0^\infty t\frac{dR(t)}{dt}dt = -\left(\boxed{[t\cdot R(t)]_0^\infty} - \int_0^\infty R(t)dt\right) = \int_0^\infty R(t)dt$$

**= 0**

Avec:

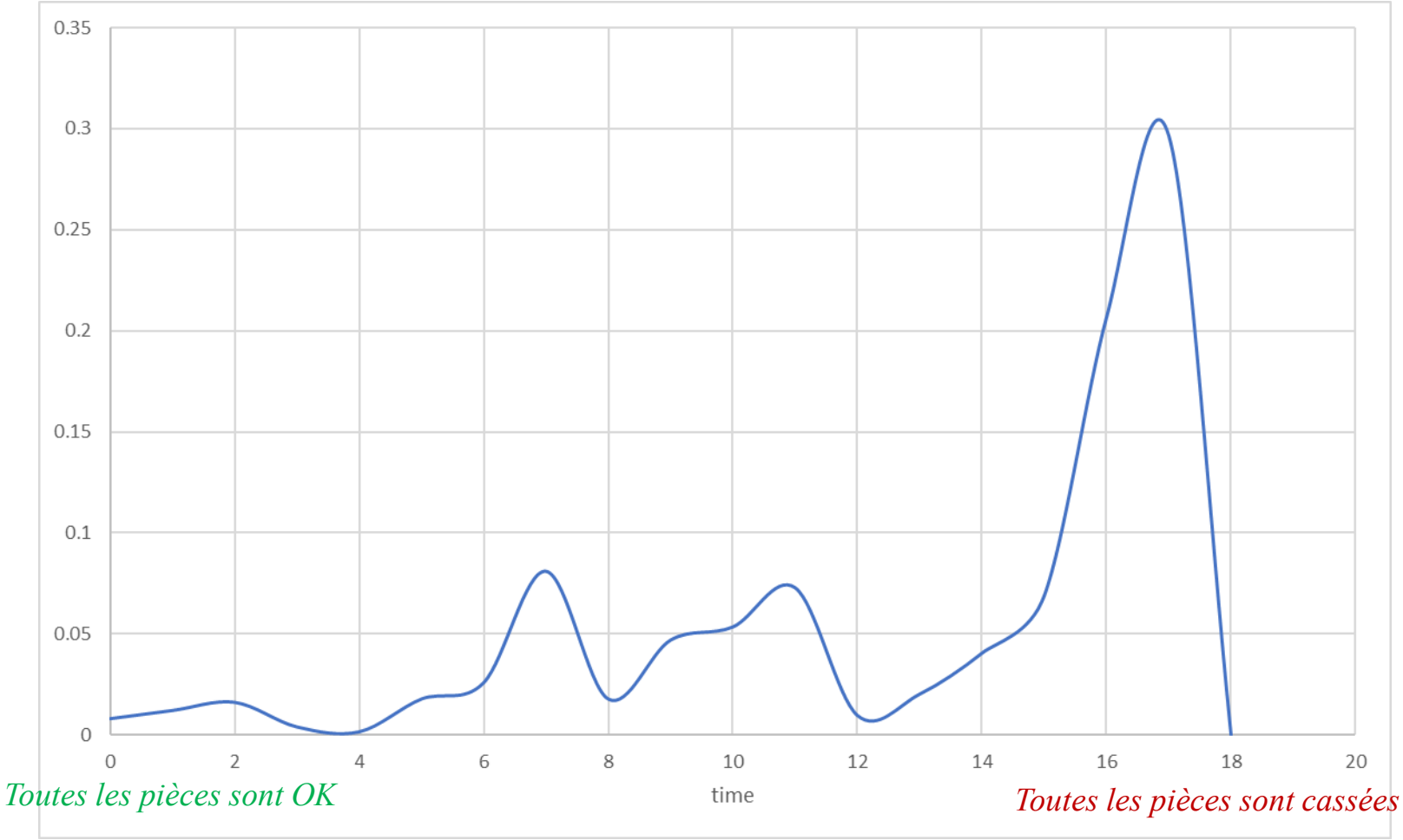
$$f(t) = \frac{dF(t)}{dt} = \frac{-dR(t)}{dt}$$

Avec:

$$R(\infty) \cong 0$$

$$R(0) = 1$$

# Densité de défaillance – f(t)




La densité de défaillance d'un composant ou système correspond a la probabilité qu'une erreur apparait à l'instant t.

Failure Density – f(t):

$$\boxed{f(t) = \frac{d\,F(t)}{dt} = -\frac{d\,R(t)}{dt}}$$

$$f(0) = 0$$
$$f(\infty) = 0$$

Sources:
[1] Failure Rate Analysis, Fatemeh Afsharnia, https://www.intechopen.com/chapters/58187

# Taux de défaillance – h(t)

Dans l'industrie, c'est important de pouvoir caractériser, combien de pieces, qui ont survie jusqu'à l'instant $t$, peuvent tomber en panne dans l'interval $t$ et $t + \Delta t$.

C'est la probabilité conditionnelle de F sous la condition qu'au moment $t$, les éléments ont survies et que le composant/système a fonctionné de $t = 0$ à $t_1$

$$H(\Delta t) = \frac{1 * \Delta n_c}{n_s * \Delta t}$$

$$\mathrm{h}(t) = \frac{1 * dn_c(t)}{n_s * dt} = \frac{1 * dF(t) * N}{R(t) * N * dt} = \frac{1 * dF(t)}{R(t) * dt} = \frac{1}{R(t)} * \frac{dF(t)}{dt} = \frac{f(t)}{R(t)}$$

Avec : $f(t) = \frac{dF(t)}{dt} = \frac{-dR(t)}{dt}$

$$\mathrm{h}(t) = \frac{1 * dF(t)}{R(t) * dt} = \frac{1 * (-dR(t))}{R(t) * dt} = \frac{-1}{R(t)} * \frac{dR(t)}{dt} = \frac{f(t)}{R(t)}$$

Failure Rate – $\lambda(t)$:

$$\boxed{\mathrm{h}(t) = \frac{f(t)}{R(t)} = \lambda(t)}$$

Sources:
[1] Failure Rate Analysis, Fatemeh Afsharnia, https://www.intechopen.com/chapters/58187

# Fiabilité – Tableau Récapitulatif

| | Probabilité de défaillance<br>Probability of Failure<br>$F(t)$ | Probabilité de survie<br>Probability of Survival<br>$\mathrm{R}(t)$ | Densité de défaillance<br>Hazard Density<br>$f(t)$ | Taux de défaillance<br>Failure Rate<br>$h(t) = \lambda(t)$ |
|---|---|---|---|---|
| $F(t)$ | | $1 - R(t)$ | $\int_0^t f(\tau)d\tau$ | $1 - e^{\left(-\int_0^t f(\tau)d\tau\right)}$ |
| $\mathrm{R}(t)$ | $1 - F(t)$ | | $\int_0^\infty f(\tau)d\tau$ | $e^{\left(-\int_0^t f(\tau)d\tau\right)}$ |
| $f(t)$ | $\frac{d\,F(t)}{dt}$ | $-\frac{d\,R(t)}{dt}$ | | $h(t) * e^{\left(-\int_0^t f(\tau)d\tau\right)}$ |
| $h(t) = \lambda(t)$ | $\frac{1}{1 - F(t)} * \frac{d\,F(t)}{dt}$ | $-\frac{1}{R(t)} * \frac{d\,R(t)}{dt}$ | $\frac{f(t)}{\int_0^\infty f(\tau)d\tau}$ | |

# Exercise 1

Dans un essaie, nous mesurons 316 pièces jusqu'ils sont tous tombés en panne

| intervalle [h] | pièces cassés | $n_c$ | Δt [h] | F(t) | R(t) | $\Delta n_c/\Delta t$ | f(t) [1/h] | h(t) [1/h] = | Surface sous f(t) |
|---|---|---|---|---|---|---|---|---|---|
| 0-2 | 82 | | | | | | | | |
| 2-4 | 22 | | | | | | | | |
| 4-6 | 24 | | | | | | | | |
| 6-8 | 20 | | | | | | | | |
| 8-10 | 23 | | | | | | | | |
| 10-12 | 32 | | | | | | | | |
| 12-14 | 25 | | | | | | | | |
| 14-16 | 27 | | | | | | | | |
| 16-18 | 20 | | | | | | | | |
| 18-20 | 15 | | | | | | | | |
| 20-22 | 10 | | | | | | | | |
| 22-24 | 2 | | | | | | | | |
| 24-87 | 14 | | | | | | | | |

Valeur espérance de vie moyenne = ?

# Solution

| intervalle [h] | pièces cassés | $n_c$ | Δt [h] | F(t) = nc/316 | R(t) = 1-F(t) | $\Delta n_c/\Delta t$ = a | f(t) [1/h] =F'(t) = a/316 | h(t) [1/h] = f(t)/R(t) | Surface sous f(t) Δt * f(t) | MTTFi |
|---|---|---|---|---|---|---|---|---|---|---|
| 0-2 | 82 | 82 | 2 | 0.259 | 0.741 | 41.000 | 0.1297 | 0.1752 | 0.2595 | 1.481013 |
| 2-4 | 22 | 104 | 2 | 0.329 | 0.671 | 11.000 | 0.0348 | 0.0519 | 0.0696 | 1.341772 |
| 4-6 | 24 | 128 | 2 | 0.405 | 0.595 | 12.000 | 0.0380 | 0.0638 | 0.0759 | 1.189873 |
| 6-8 | 20 | 148 | 2 | 0.468 | 0.532 | 10.000 | 0.0316 | 0.0595 | 0.0633 | 1.063291 |
| 8-10 | 23 | 171 | 2 | 0.541 | 0.459 | 11.500 | 0.0364 | 0.0793 | 0.0728 | 0.917722 |
| 10-12 | 32 | 203 | 2 | 0.642 | 0.358 | 16.000 | 0.0506 | 0.1416 | 0.1013 | 0.71519 |
| 12-14 | 25 | 228 | 2 | 0.722 | 0.278 | 12.500 | 0.0396 | 0.1420 | 0.0791 | 0.556962 |
| 14-16 | 27 | 255 | 2 | 0.807 | 0.193 | 13.500 | 0.0427 | 0.2213 | 0.0854 | 0.386076 |
| 16-18 | 20 | 275 | 2 | 0.870 | 0.130 | 10.000 | 0.0316 | 0.2439 | 0.0633 | 0.259494 |
| 18-20 | 15 | 290 | 2 | 0.918 | 0.082 | 7.500 | 0.0237 | 0.2885 | 0.0475 | 0.164557 |
| 20-22 | 10 | 300 | 2 | 0.949 | 0.051 | 5.000 | 0.0158 | 0.3125 | 0.0316 | 0.101266 |
| 22-24 | 2 | 302 | 2 | 0.956 | 0.044 | 1.000 | 0.0032 | 0.0714 | 0.0063 | 0.088608 |
| 24-87 | 14 | 316 | 63 | 1.000 | 0.000 | 0.222 | 0.0007 | #DIV/0! | 0.0443 | 0 |

MTTF 8.266 h

Valeur espérance de vie moyenne = $\int R(t)\,dt = 2*0.7405 + 2*\ 0.6709 + ..... = 8.26\ \mathrm{h}$

# Unité

- Le Taux de défaillance peut être exprimé dans n'importe quelle unite de temps (Seconds, milli-second, jours, mois , année,…)

  Cependant, les heures sont le plus commun.

- Le Taux de défaillance est très souvent exprimé en failure per million, ou $10^{-6}$.

- Une unité/terme très répendu dans le monde de la sécurité fonctionnelle et la fiabilité est **Failures In Time** (**FIT**) qui est défini par le taux de défaillance d'un composant sur 1 billion d'heure composant ($10^9$)(ex. 1000 composants pour 1 million d'heures, or 1 million composants pour 1000 heure).

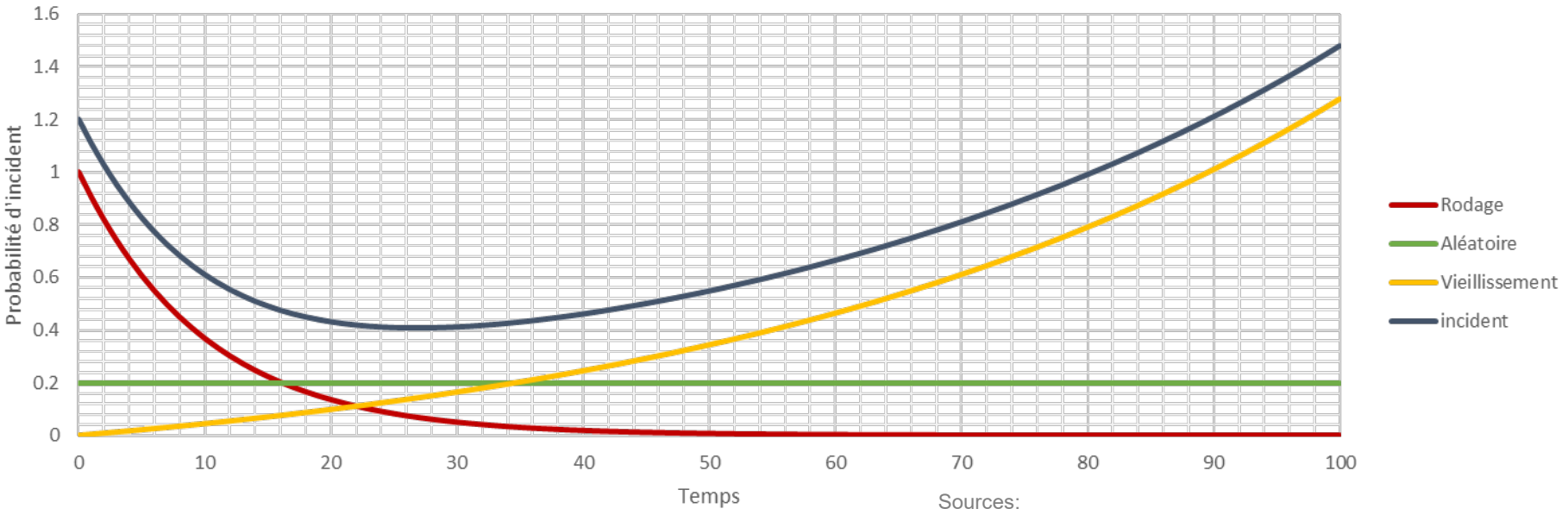
$$\boxed{1\ FIT = 10^{-9}/h}$$

Sources:
[1] Failure Rate, Wikipedia, https://en.wikipedia.org/wiki/Failure_rate

# Courbe de baignoire (1)

En ingénierie la **courbe en baignoire** est une représentation classique de la probabilité d'incidents pour des systèmes. La courbe en baignoire est la somme de trois composantes :

- courbe des incidents liés au rodage du système, qui commence à un niveau élevé puis décroit avec le temps ;
- courbe des incidents aléatoires qui est indépendante de l'âge du système ;
- courbe des incidents liés au vieillissement du système qui débute à des niveaux faibles mais croît de façon continue avec le temps.

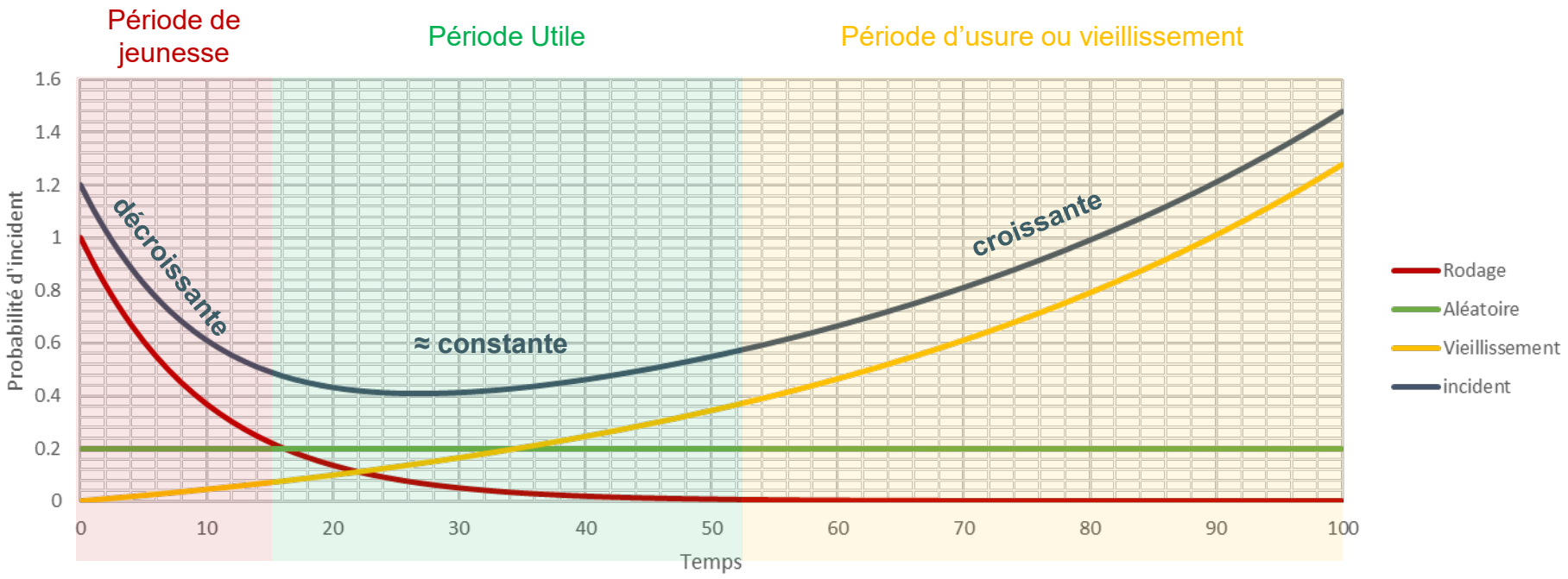



Sources:
[1] Courbe de baignoire, https://fr.wikipedia.org/wiki/Courbe_en_baignoire

# Courbe de baignoire (2)

La **courbe en baignoire** est aussi décrite en 3 périodes (très liés aux courbes décrites ultériement):

- Période Jeunesse (Early Life)
- Période Utile (Useful Life), qui commence à un niveau élevé puis décroit avec le temps ;
- Période d'usure ou vieillissement (Wearout Life)




Sources:
[1] Courbe de baignore, https://fr.wikipedia.org/wiki/Courbe_en_baignoire
[2] Life Data Analysis Reference, https://reliawiki.org/index.php/Life_Data_Analysis_Reference_Book

# Répartition de vie (Life Distribution) (1)

Qu’est-ce qu’une répartition de vie (Life Distribution)?

Une répartition de vie décrit les distributions statistiques qui sont utilisée en fiabilité et en analyse de vie.

Une distribution est décrite par la densité de défaillance $f(t)$ (probability density function : pdf).

Sources:
[1] Life Distributions, Reliawiki, https://reliawiki.org/index.php/Life_Distributions

# Répartition de vie (Life Distribution) (2)

- Exponential Distribution
- Shifted Exponential Distribution
- Normal and Lognormal Distribution
- Phase-Type Distribution
- Gamma Distribution, Erlangian Distribution and Chi-Square Distribution
- Log-Logistic Distribution
- Bernouilli Distribution
- Mass at Origin, Geometric Distribution
- Defective Distribution
- Uniform Distribution
- Binomial Distribution
- Hypergeometric Distribution

Pour le cours:

- Linear Distribution
- Rectangular Distribution
- Exponential Distribution
- Normal and Lognormal Distribution
- Weibull Distribution

Sources:
[1] Life Distributions, Reliawiki, https://reliawiki.org/index.php/Life_Distributions

# Distribution Linéaire

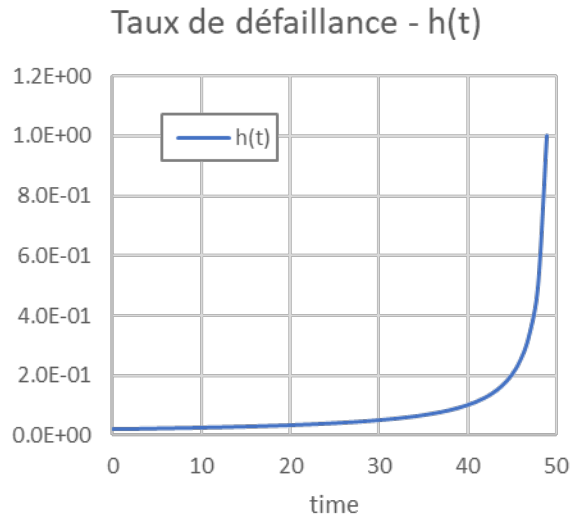
$F(t) \quad = \quad kt$, pour (t = 0.. 50h), k = 0.02

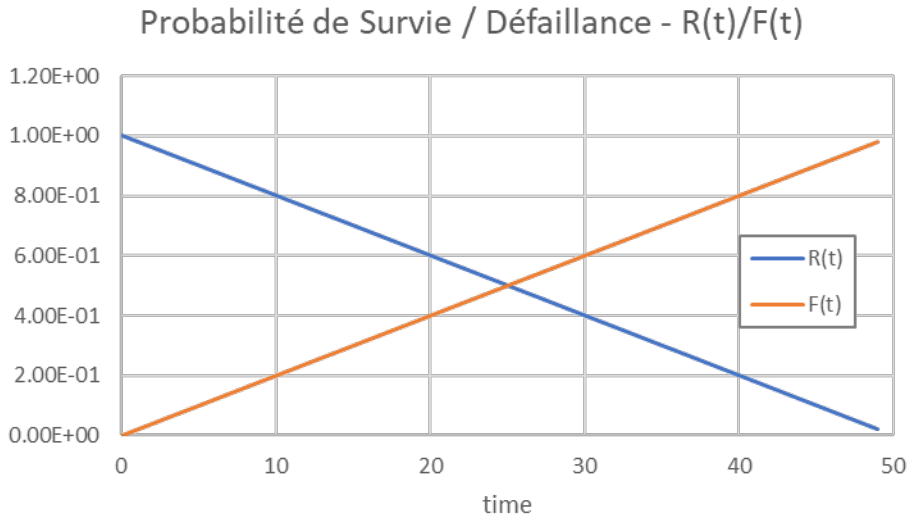
$R(t) \quad = \quad 1 - kt$

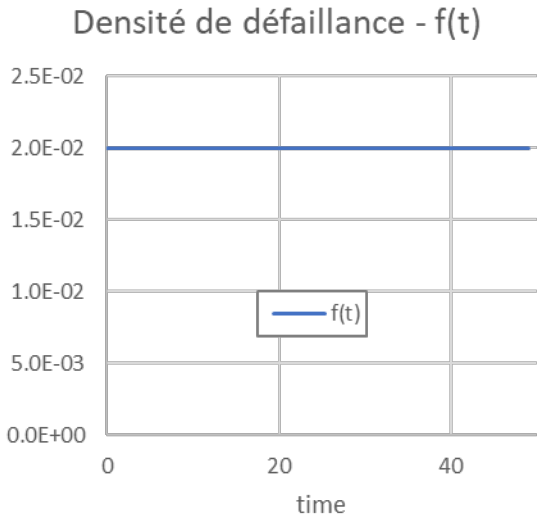
$f(t) \quad = \quad k$

$$h(t) \quad = \quad \frac{k}{1 - kt}$$

$$MTTF \quad = \quad \int_0^{\infty} t f(t)\, dt = \int_0^{50} t\, k\, dt = \left[\frac{1}{2} k t^2\right]_0^{50} = 25 - 0 = 25h$$



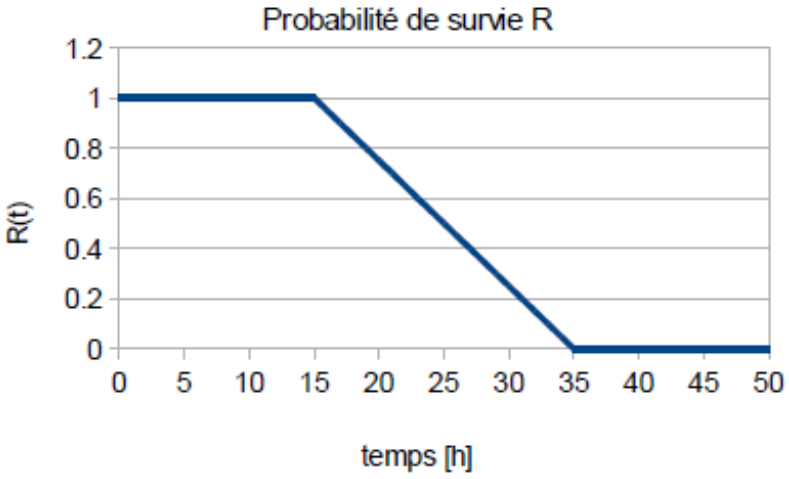
# Distribution rectangulaire (1)

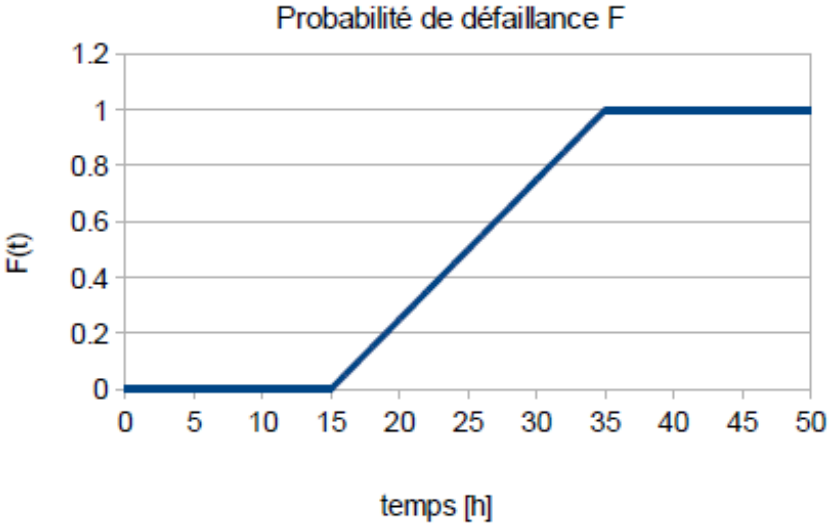
$$\mathrm{f}(t) = \begin{cases} 0 & pour\ 0 < t < a \\ 1/(b-a) & pour\ a \leq t \leq b \\ 0 & pour\ t > b \end{cases}$$

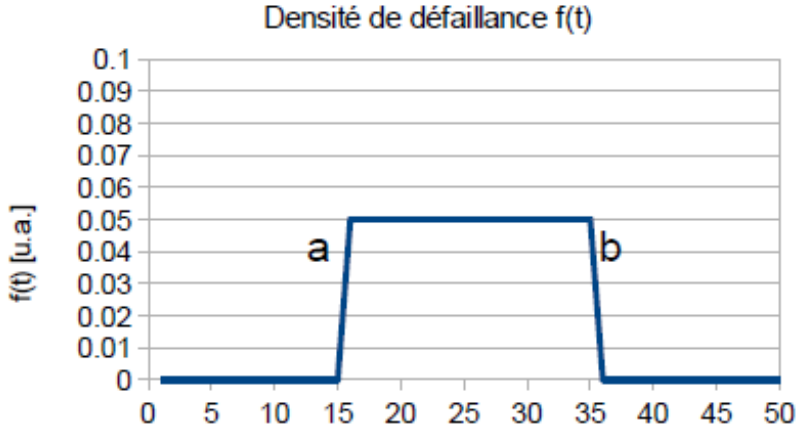
$$\mathrm{h}(t) = \begin{cases} \infty & pour\ 0 < t < a \\ 1/(b-t) & pour\ a < t < b \\ 1/(b-a) & pour\ t > b \end{cases}$$

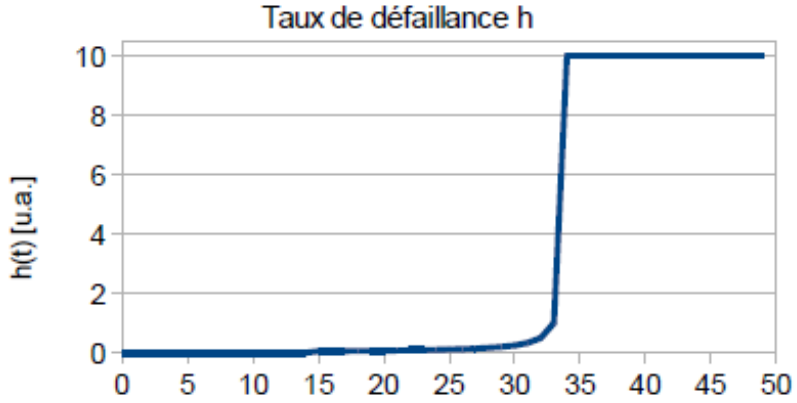
$$\mathrm{R}(t) = \begin{cases} 1 & pour\ 0 < t < a \\ (b-t)/(b-a) & pour\ a \leq t \leq b \\ 0 & pour\ t > b \end{cases}$$

# Distribution rectangulaire (2)



# Distribution Exponentielle (1)

$$F(t) = 1 - e^{-\lambda t}$$

$$R(t) = e^{-\lambda t}$$

$$f(t) = \lambda e^{-\lambda t}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^\infty t f(t)\, dt = \frac{1}{\lambda}$$

Integration par partie:

$$\int v \frac{du}{dt} dt = vu - \int u \frac{dv}{dt} dt$$

Explication:

$$MTTF = \int_0^\infty t f(t)\, dt = \left[-t \cdot e^{-\lambda t}\right]_0^\infty - \int_0^\infty 1 \cdot \left(-e^{-\lambda t}\right) dt = 0 - \left[-\frac{e^{-\lambda t}}{\lambda}\right]_0^\infty = 0 - \left(\frac{e^{-\lambda \infty}}{\lambda} - \frac{e^{-\lambda 0}}{\lambda}\right) = \frac{1}{\lambda}$$

Avec:

$$v = t \qquad du/_{dt} = \lambda e^{-\lambda t}$$

$$dv/_{dt} = 1 \qquad dv/_{dt} = -\lambda/_{\lambda} e^{-\lambda t} = -e^{-\lambda t}$$

# Distribution Exponentielle (2)

$$1ans = 8760hours$$

- Taux de défaillance : $h(t) = \lambda = 1FIT\ (10^{-9} failure/h)$

$$F(t) = 1 - e^{-\lambda t}$$

$$R(t) = e^{-\lambda t}$$

$$f(t) = \lambda e^{-\lambda t}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^\infty t f(t)\, dt = \frac{1}{\lambda} = \frac{10^{-9} failure}{h} = 1FIT$$

- Pour cette distribution, 1 FIT signifie après 114155 ans, 63.2% des pieces sont en pannes.

$$R(t) = e^{-\lambda t} = e^{-\frac{1}{MTTF}t}$$

$$R(MTTF) = e^{-\frac{1}{MTTF}t} = e^{-\frac{1}{10^9}10^9} = e^{-1} = 0.367 = 36.7\%$$

$$F(MTTF) = 63.2\%$$

# Distribution Exponentielle (3)

- Taux de défaillance : $h(t) = \lambda = 1FIT\ (10^{-9} failure/h)$

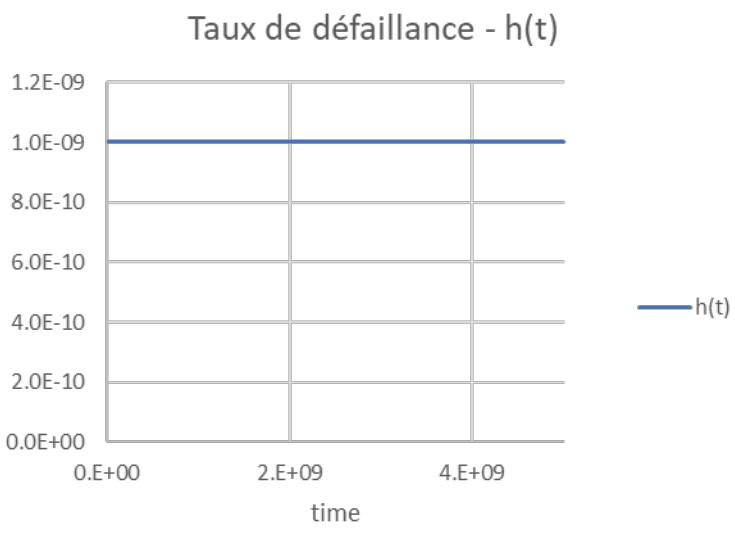
$$F(t) = 1 - e^{-\lambda t}$$

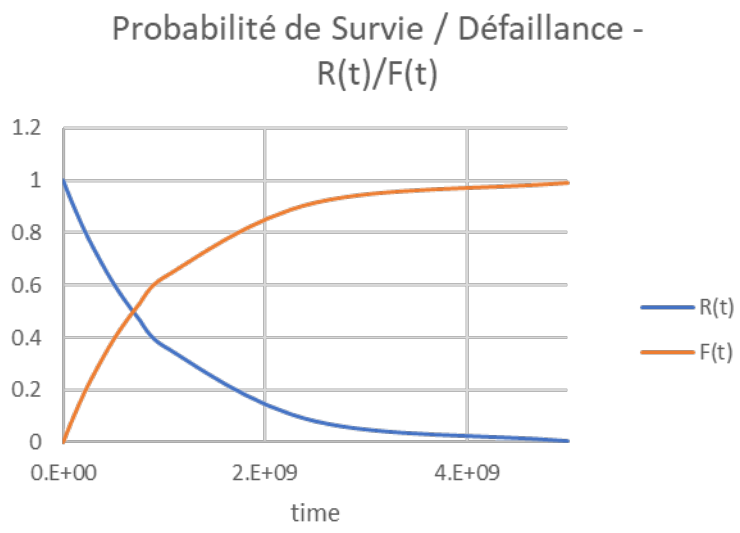
$$R(t) = e^{-\lambda t}$$

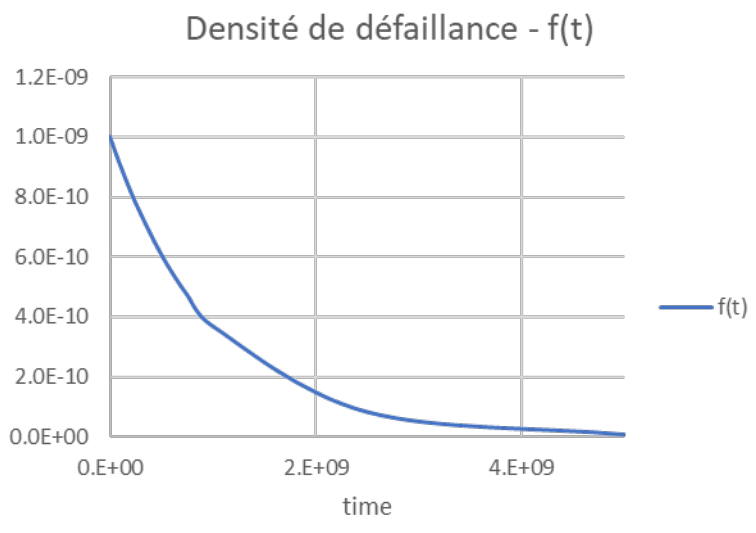
$$f(t) = \lambda e^{-\lambda t}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^{\infty} t f(t)\, dt = \frac{1}{\lambda} = \frac{10^{-9} failure}{h} = 1FIT$$



# Distribution Exponentielle décallée (1)

$$F(t) = 1 - e^{-\lambda(t-a)}$$

$$R(t) = e^{-\lambda(t-a)}$$

$$f(t) = \lambda e^{-\lambda(t-a)}$$

$$h(t) = \lambda$$

$$MTTF = \int_0^{\infty} (t-a) f(t-a)\, dt = \mathrm{a} + \frac{1}{\lambda}$$

# Distribution de Weibull (1)

$$F(t) = 1 - e^{-(\eta t)^{\beta}}$$

$$R(t) = e^{-(\eta t)^{\beta}}$$

$$f(t) = \beta\eta \cdot (\eta t)^{\beta-1} \cdot e^{-(\eta t)^{\beta}}$$

$$h(t) = \beta\eta \cdot (\eta t)^{\beta-1}$$

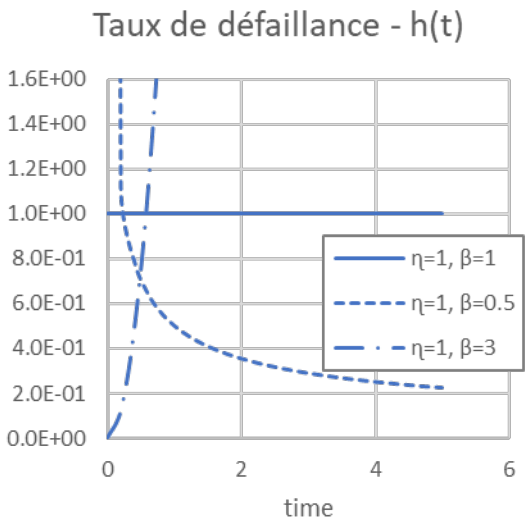
Si η = λ et β = 1, alors nous retrouvons une distribution exponentielle

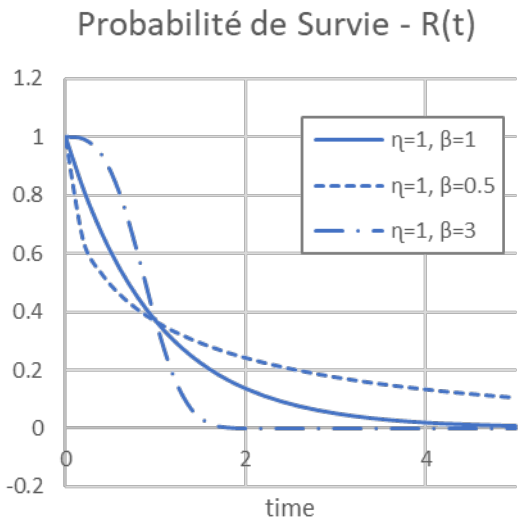
$$F(t) = 1 - e^{-(\lambda t)^{\beta}} = 1 - e^{-\lambda t}$$

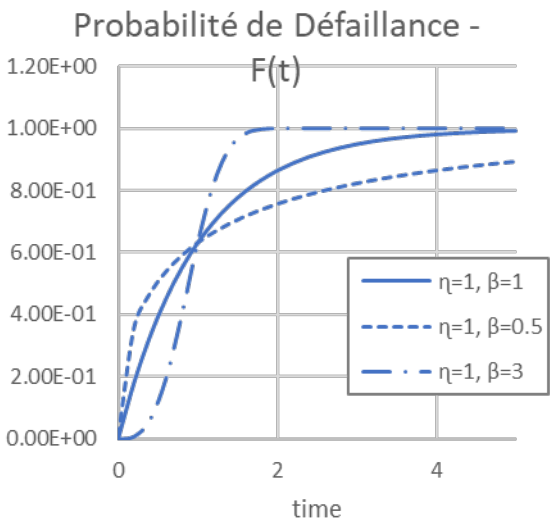
$$R(t) = e^{-(\lambda t)^{\beta}} = e^{-\lambda t}$$

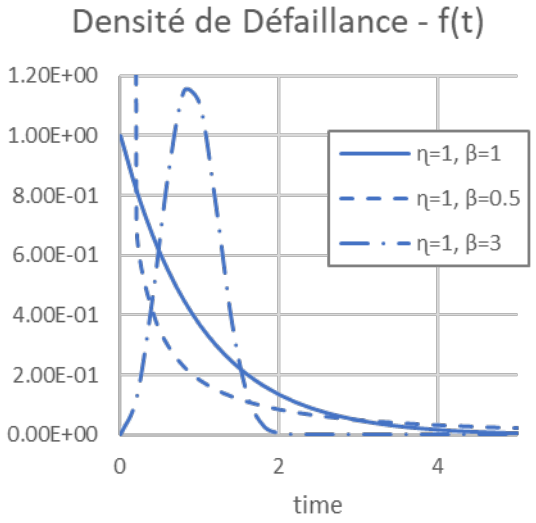
$$f(t) = \lambda \cdot (\lambda t)^{1-1} \cdot e^{-(\lambda t)^{1}} = \lambda e^{-\lambda t}$$

$$h(t) = \lambda \cdot (\lambda t)^{1-1} = \lambda$$



# Distribution Normal (Distribution de Gauss) (1)

$$F(\mathrm{x}) = \Phi\left(\frac{x-\mu}{\sigma}\right)$$

$$f(x) = \frac{1}{\sqrt{2\pi}\cdot\sigma}\cdot e^{\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)}$$

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{\left(-\frac{t^2}{2}\right)}dt$$

Une autre méthode est de par:

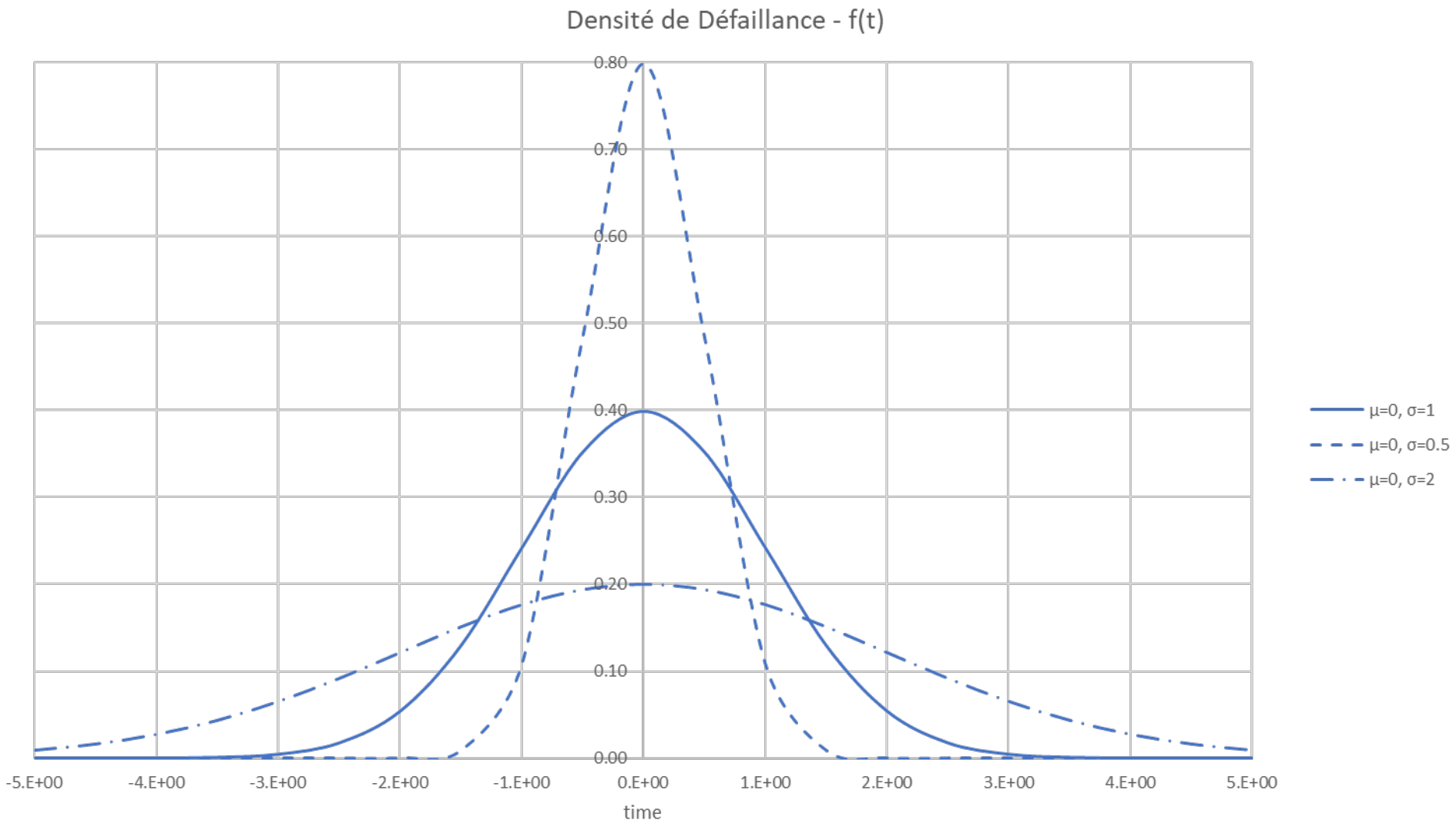
$$\Phi(x) = \frac{1}{2} + \frac{1}{\sqrt{2\pi}}e^{\left(-\frac{x^2}{2}\right)}\cdot\left[x + \frac{x^3}{3} + \frac{x^5}{3\cdot 5} + \cdots + \frac{x^{2n+1}}{(2n+1)!!}\right]$$

La double factorial n!!:

$$\mathrm{n!!} = \begin{cases} \prod_{k=1}^{\frac{n}{2}-1}(2k) = n(n-2)(n-4)\ldots. & ,for\ n > 0\ odd \\ \prod_{k=1}^{\frac{n+1}{2}}(2k-1) = n(n-2)(n-4)\ldots. & ,for\ n > 0\ even \\ 1 & ,for\ n = -1,0 \end{cases}$$

Sources:
[1] Double factorial, Wikipedia, https://en.wikipedia.org/wiki/Double_factorial

# Distribution Normal (Distribution de Gauss) (2)



# Exercices 2 (1)

1) Un composant dispose d'une distribution exponentielle et d'un taux de défaillance de $10^{-5}/h$.

Avec quelle probabilité vit-t-il plus que :

- 2'000 h
- 20'000 h
- 100'000 h

# Exercices 2 (2)

1) Un système technique est distribué selon Weibull avec les paramètres :
$\eta = 10^{-7}/h$
$\beta = 0.7$

a. Quelle est la probabilité que le système tombe en panne pendant la première année?
b. Quelle est la probabilité que le système tombe en panne pendant 10 ans, s'il a déjà survécu 5 ans?
c. Quelle valeur prend $\beta$, si après 2 ans 5% des systems sont tombés en panne ($\eta = 1.671 \cdot 10^{-10}(1/h)^{\beta}$
d. Quels types de défaillance peut-on trouver pour a. et c. (selon Weibull et la courbe de baignore)?

# Merci pour votre attention

Questions ou remarques: jonathan.hendriks@hefr.ch ou via Teams

MASTER OF SCIENCE
IN ENGINEERING

Sécurité et Automatisation (SECU)

# 13 – Récapitulatif du cours

Eric Silva
20.12.2021

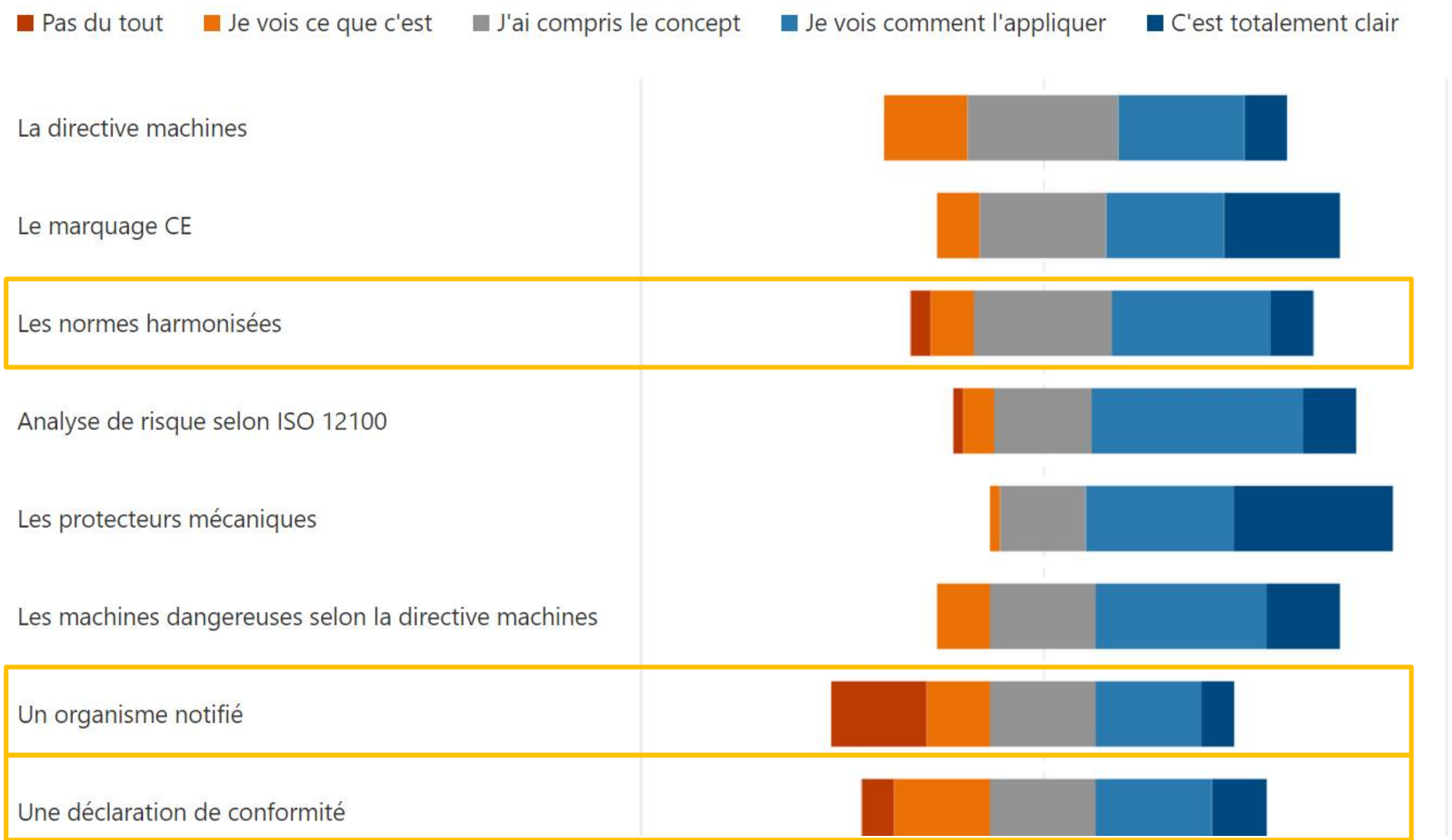
# Contenu du cours

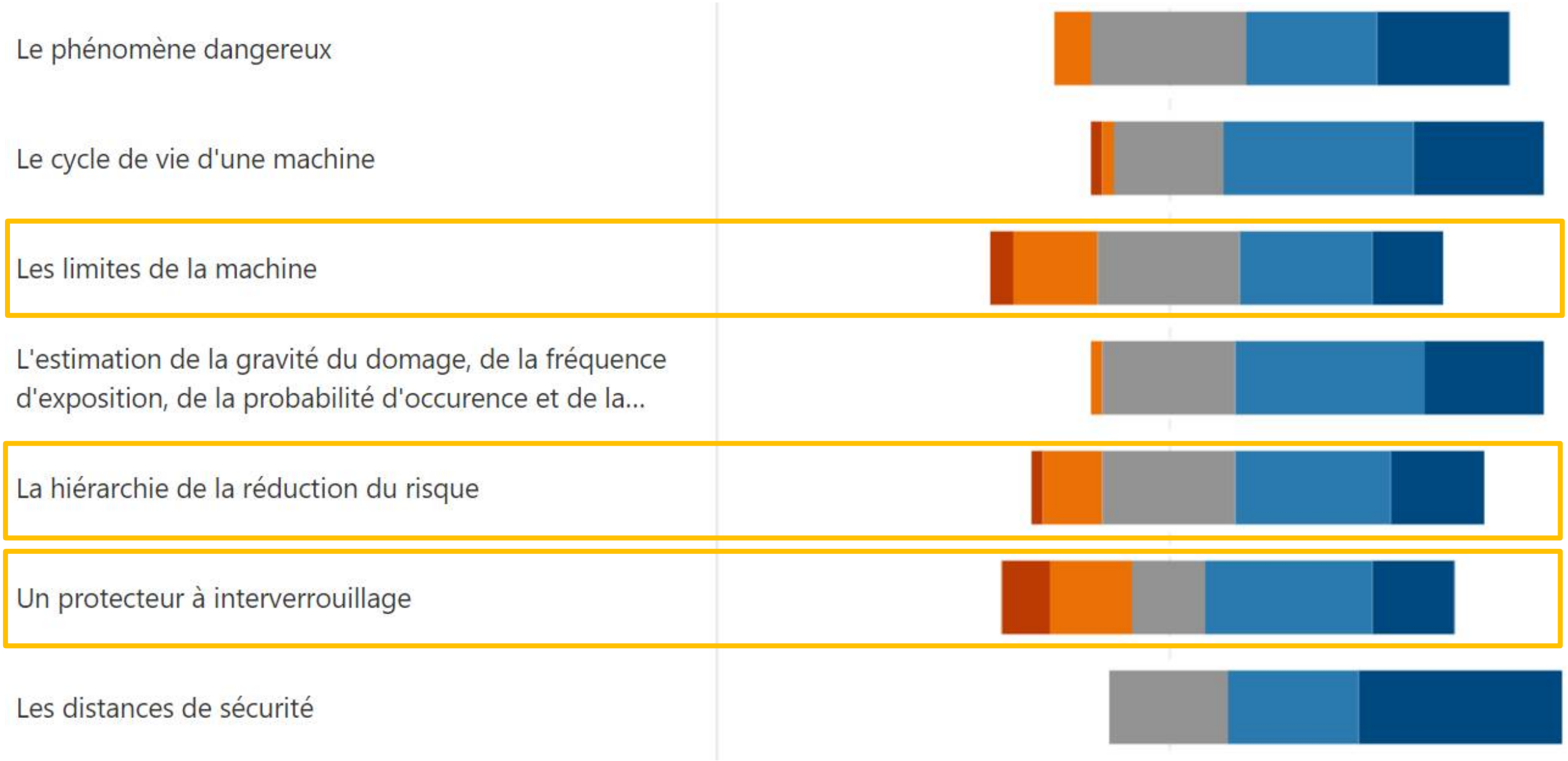
| Semaine | Périodes | Date | Thèmes | Remarques |
|---|---|---|---|---|
| SA2 | 3 | 27.09.2021 | Introduction au risque, à la sécurité et à la fiabilité en général | |
| SA3 | 3 | 04.10.2021 | Sécurité des systèmes techniques – Directives, Normes et Marquage CE | |
| SA4 | 3 | 11.10.2021 | Sécurité des systèmes techniques – Analyse de risque selon ISO 12100 | |
| SA5 | 3 | 18.10.2021 | **Workshop** «analyse de risque» | |
| SA6 | 3 | 25.10.2021 | Sécurité des systèmes techniques – Sélection de la réduction du risque | |
| SA7 | 3 | 01.11.2021 | Sécurité des systèmes techniques – Composants de sécurité et ISO13849/IEC62061 | |
| SA8 | 3 | 08.11.2021 | **Workshop** «ISO13849 et IEC62061» | |
| SA9 | 3 | 15.11.2021 | Processus de développement des systèmes techniques – Partie 1 | |
| SA10 | 3 | 22.11.2021 | Processus de développement des systèmes techniques – Partie 2 | |
| SA11 | 3 | 29.11.2021 | **Workshop** «Développement de systèmes techniques» | |
| SA12 | 3 | 06.12.2021 | Fiabilité des systèmes techniques - Niveau composants | |
| SA13 | 3 | 13.12.2021 | Fiabilité des systèmes techniques - Niveau systèmes | |
| SA14 | 3 | 20.12.2021 | Récapitulatif du cours | |
| | | 24.12.2021 - 07.01.2022 | Vacances de Noël | |
| SA14 | 3 | 10.01.2022 | Semaine de réserve | |
| **Examen** | | **31.01.2022** | **Examen écrit – 17h30 salle B2** | |
| Total | **42** | | | |

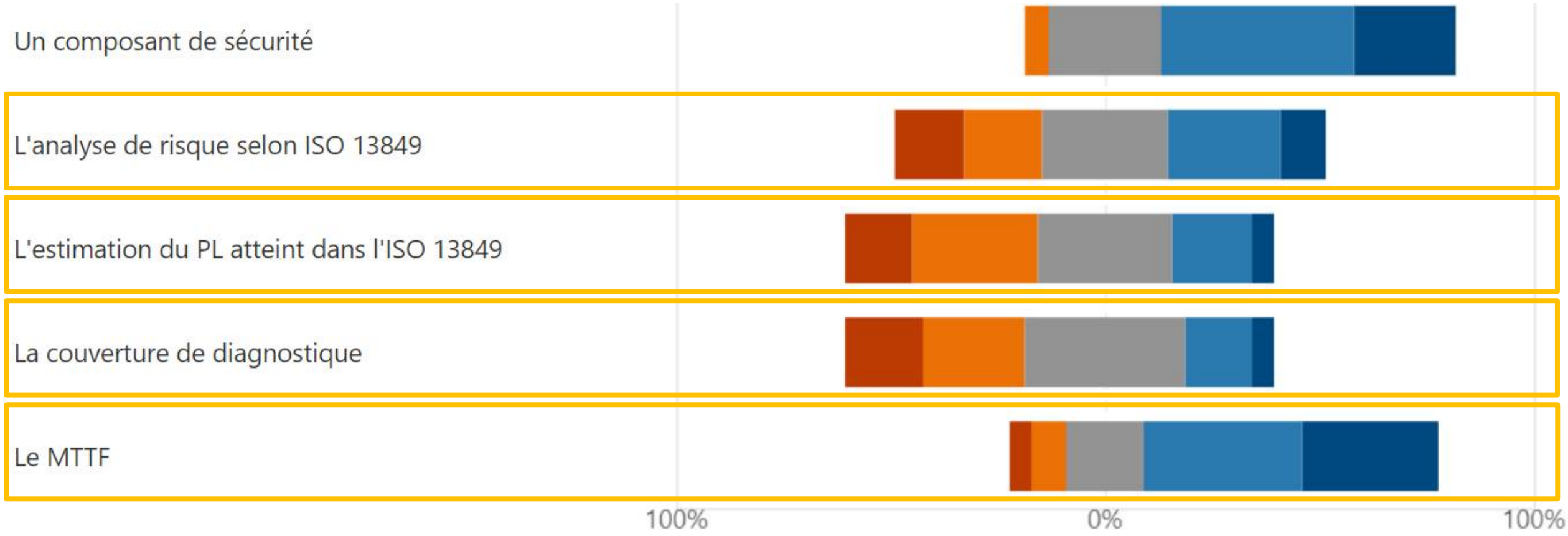
# Résumé du feedback du cours: (38 réponses)

- Les présentations individuelles ont été utiles pour 84.3% des étudiants (5.3% non)
  - Les thèmes étaient intéressants, un cadre plus strict pourrait être mis en place.

- La structure du cours convent mais en règle générale, plus d'exercices seraient les bienvenus.
- La participation des différents intervenants a été dans l'ensemble très appréciée
  - Limiter le nombre de slides et ajouter des exercices
  - Très condensé
  - Relier plus souvent la théorie et la pratique (cas concrets)
  - Faire attention à bien maintenir le fil rouge durant le cours
- Noter la présentation ou un rapport durant le cours afin de diluer la note sur deux rendus
- Cours sur l'ISO13849 était très condensé et difficile à comprendre
- 1x ce cours n'a pas d'utilité pratique, professionnelle ou personnelle


Pas du tout
Je vois ce que c'est
J'ai compris le concept
Je vois comment l'appliquer
C'est totalement clair
La directive machines
Le marquage CE
Les normes harmonisées
Analyse de risque selon ISO 12100
Les protecteurs mécaniques
Les machines dangereuses selon la directive machines
Un organisme notifié
Une déclaration de conformité


Le phénomène dangereux
Le cycle de vie d'une machine
Les limites de la machine
L'estimation de la gravité du domage, de la fréquence d'exposition, de la probabilité d'occurence et de la...
La hiérarchie de la réduction du risque
Un protecteur à interverrouillage
Les distances de sécurité


Un composant de sécurité
L'analyse de risque selon ISO 13849
L'estimation du PL atteint dans l'ISO 13849
La couverture de diagnostique
Le MTTF
100%
0%
100%

Les catégories d'architecture selon ISO 13849

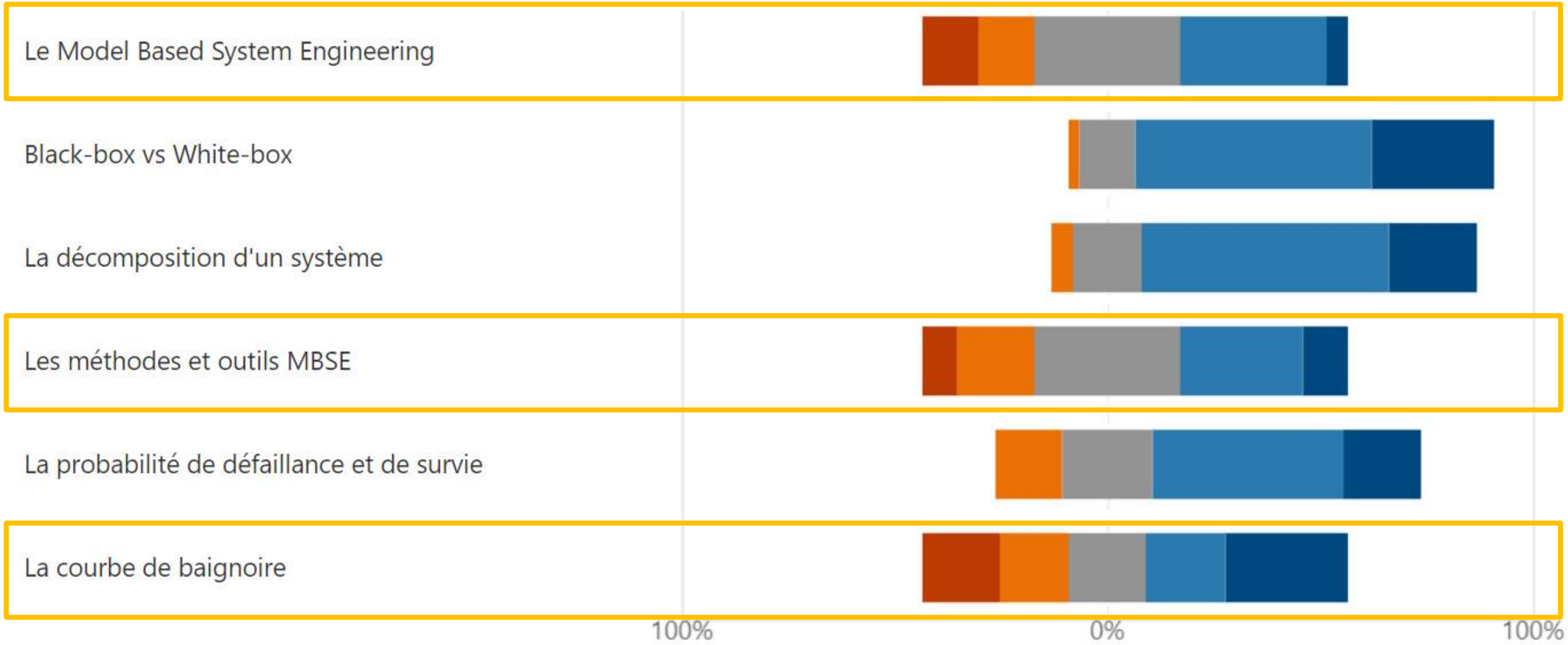
Les défaillances de cause commune

Défaillance aléatoire vs défaillance systèmatique

L'ingéniérie des systèmes

La définition des exigences

La vérification et la validation


Le Model Based System Engineering
Black-box vs White-box
La décomposition d'un système
Les méthodes et outils MBSE
La probabilité de défaillance et de survie
La courbe de baignoire
100%
0%
100%

# Modalités d’examen

Sources:
https://www.deleguescommerciaux.gc.ca/guides/133383.aspx?lang=fra/

# Forme et exigences

- Date: 31 Janvier 2020
- Heure: 17h30
- Durée: en principe 120 minutes, certainement un peu moins.
- L’examen sera écrit et se tiendra sur place
- L’examen sera «open book»

# Questions concernant l’examen?

# 01 – Introduction risque et sécurité

- Qu’est ce qu’un système «Safe», «Reliable», «Secure»
- Définition et réduction du risque
- Introduction à la norme ISO 12100

# 02 – Directives, Standards et normes applicables

- Le but du Marquage CE et les étapes pour y arriver
- Définition des directives et normes applicables
- Comment identifier les exigences essentielles et qu’est-ce que c’est
- Intégration de la sécurité
- Les types de normes et leurs rôles
- La norme utilisée pour l’analyse de risque au niveau de la machine
- Autres normes importantes pour le développement d’une machine
- Quelle procédure de marquage CE s’applique à quel produit (Examen de type ou non)
- Etapes finales pour le Marquage CE

# 03 – Analyse de risque selon la norme ISO 12100

- Les objectifs de la norme ISO12100
- Termes et définitions utilisés
- Les étapes de l'appréciation du risque
- Les facteurs d'appréciation du risque
- Les cycles de vie qui doivent être couverts
- Information nécessaire pour l'appréciation du risque
- Les phénomènes dangereux (tâches, états de la machine et opérateur)
- Les dommages pouvant être occasionnés par les phénomènes dangereux
- Estimation du risque (Gravité, Fréquence, Probabilité d'occurrence, Possibilité d'évitement)
- La réduction du risque (Critères, hiérarchie et priorisation des réductions de risque)
- Documentation de l'analyse de risque

# 05 – Méthodes de réduction du risque

- Protection contre les dangers (Mécanique, bruit, vibrations, émissions dangereuses, rayonnement
- Les types de protecteurs et leurs avantages / limitations
- Les limites des protecteurs fixes et choix du protecteur
- Exigences et matériaux pour les protecteurs
- Les distances de sécurité
- Liste des composants de sécurité

# 06 – Développement d’un composant de sécurité

- Normes applicables (ISO 13849 et IEC 62061)
- Les paramètres de sécurité selon ISO 13849
- Relation entre l’ISO 13849 et l’ISO 12100
- Définition du niveau de performance requis (graphe des risques)
- Types de défaillances
- Paramètres requis pour valider le PL atteint
- ISO 13849 et IEC 62061 différences et quand s’applique l’une plutôt que l’autre

# 8 – Processus de développement de systèmes techniques

- Les processus de l'ingénierie système
- Le cycle de vie d'un système
- Les exigences (Définition et rédaction/forme)
- Vérification et validation (différence)
- Les systèmes (définition et représentation)
- Model-Based System Engineering (concept et piliers)
- Représentation Black/White-box
- Idée générale d'une méthodologie MBSE

# 08 – Processus de développement de systèmes techniques

- Les processus de l’ingénierie système
- Le cycle de vie d’un système
- Les exigences (Définition et rédaction/forme)
- Vérification et validation (différence)
- Les systèmes (définition et représentation)
- Model-Based System Engineering (concept et piliers)
- Représentation Black/White-box
- Idée générale d'une méthodologie MBSE

# 09 – Processus de développement de systèmes techniques – Partie 2

- La décomposition d'un système
- Les piliers du MBSE (méthodes, langages, outils)
- Le System Thinking (approche structurelle et fonctionnelle)
- L'ingénierie des systèmes basée sur le modèle (MBSE)

# 11 – Fiabilité des systèmes techniques – Niveau composants

- Fiabilité et durabilité
- Probabilité et Taux de défaillance/survie
- MTTF
- Courbe de baignoire
- Différentes distributions mathématiques

# 12 – Fiabilité des systèmes techniques – Niveau système

- MTTF, MTTR, MTBF
- RAMS
- Reliability Block Diagram
- Calcul du failure rate pour un système

# Retour sur l'ISO 13849

# ISO 13849 - Introduction

- Cette norme est une norme de type B1 qui a remplacé l'EN 954-1:1996 le 31 décembre 2011.
- Elle traite des parties des systèmes de commande relatives à la sécurité (SRP-CS)
- Elle fournit des recommandations à ceux qui sont impliqués dans la conception et l'évaluation des SRP-CS
- Elle est applicable, quelle que soit la technologie ou l'énergie utilisée (électrique, hydraulique, pneumatique, mécanique…)
- Elle a été mise à jour en 2015

# EN Standards Types

**Basic safety standard**

**Type A**

| |
|---|
| **EN ISO 12100** Safety of machinery – Risk assessment and risk reduction |

**Safety group standards**

**Type B1**

| | | | |
|---|---|---|---|
| **EN ISO 13857** Safety distances | **EN ISO 13849-1** Safety-related parts of controls | **EN ISO 13855** arm/hand speeds | **EN 62061** functional safety of control systems |

**Type B2**

| | | | |
|---|---|---|---|
| **EN ISO 13850** Emergency stop devices | **EN 61496** opto-electronic protective devices | **EN 60204-1** electrical equipment | ... more |

**Safety product standard**

**Type C**

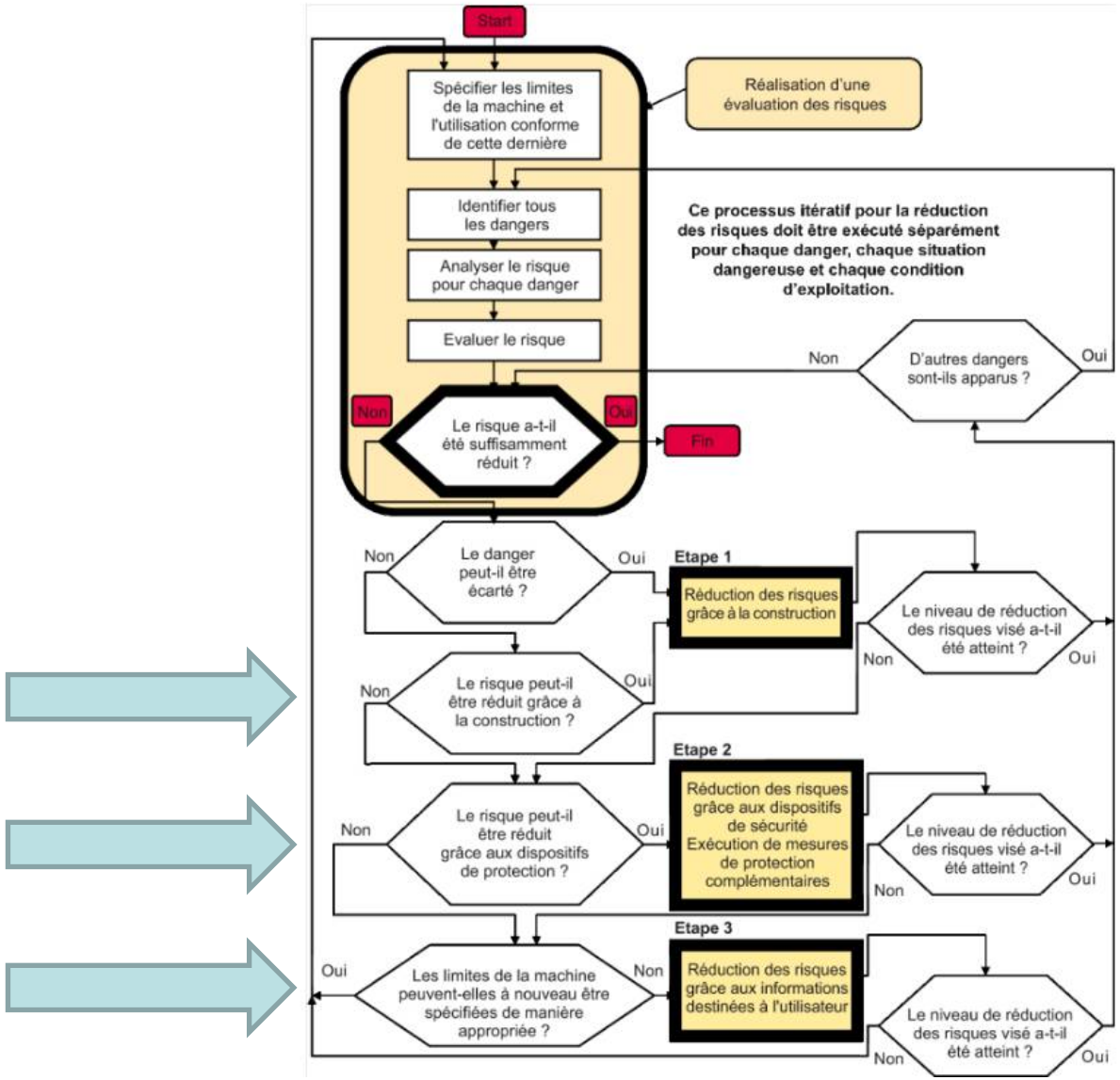
| | | | |
|---|---|---|---|
| **EN 691** Woodworking machines | **EN 10218-1** Robots | **EN 1114** Extruders | |
| **EN 692** Mechanical presses | **EN 415** Packaging machines | **EN 201** Rubber and plastics machines | ... more |
| **EN 693** Hydraulische Pressen | **EN 620** Conveyer systems | **EN 619** Continuous handling equipment piece goods | |

Une machine satisfait aux exigences de base en matière de sécurité et de protection de la santé lorsqu'elle a été construite selon ces normes harmonisées.

Les normes EN se divisent en différents types :

- ❑ Type A – norme de sécurité fondamentale
- ❑ Type B – norme de sécurité relative à un groupe
- ❑ Type C – norme de sécurité relative à un produit

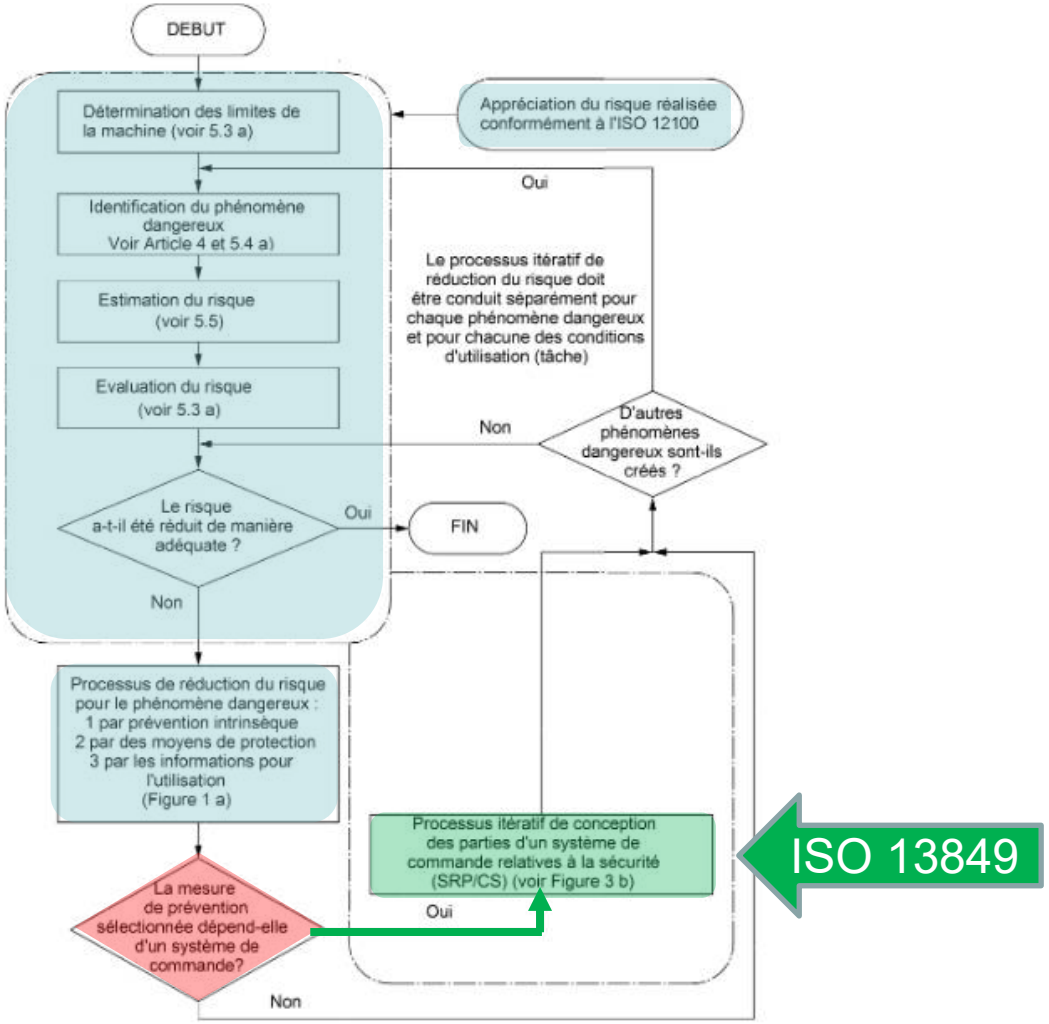
# ISO 12100 – Analyse de risque



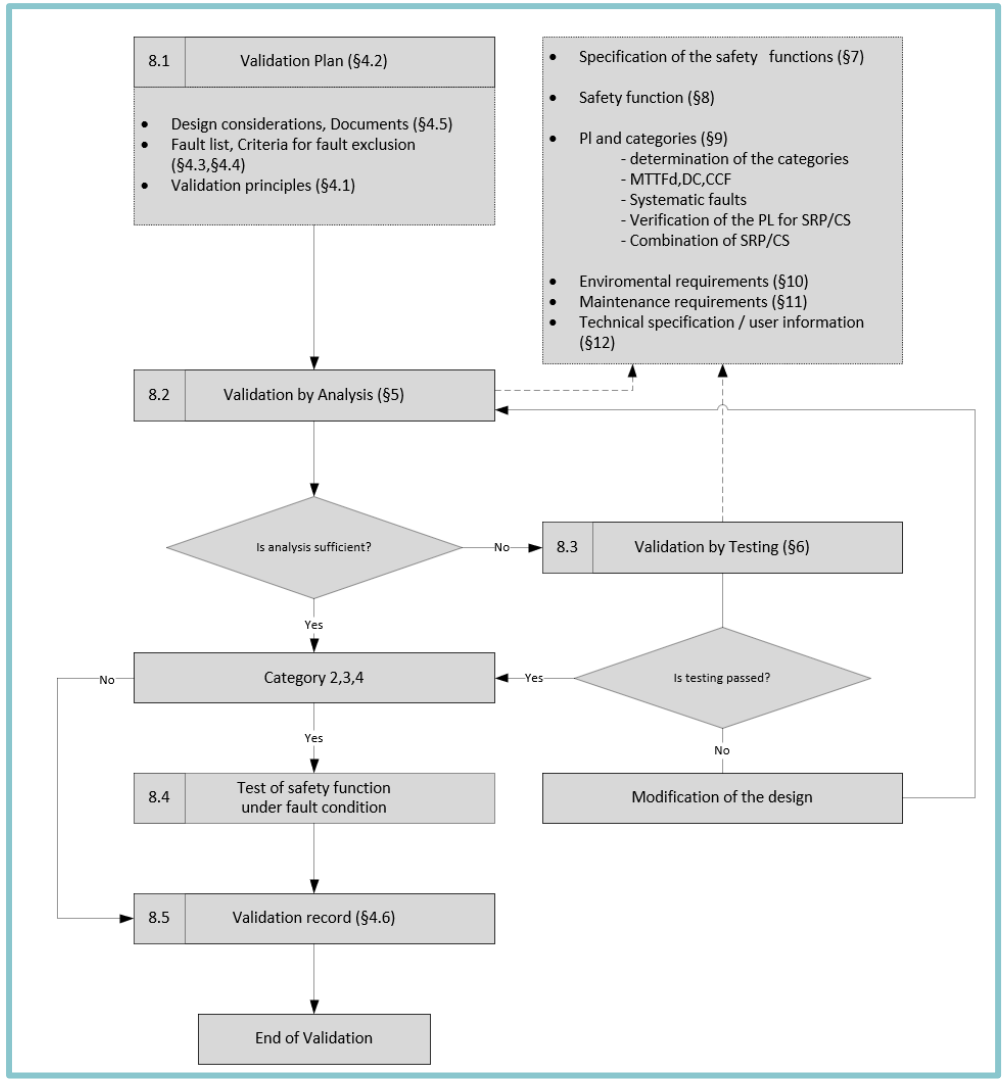


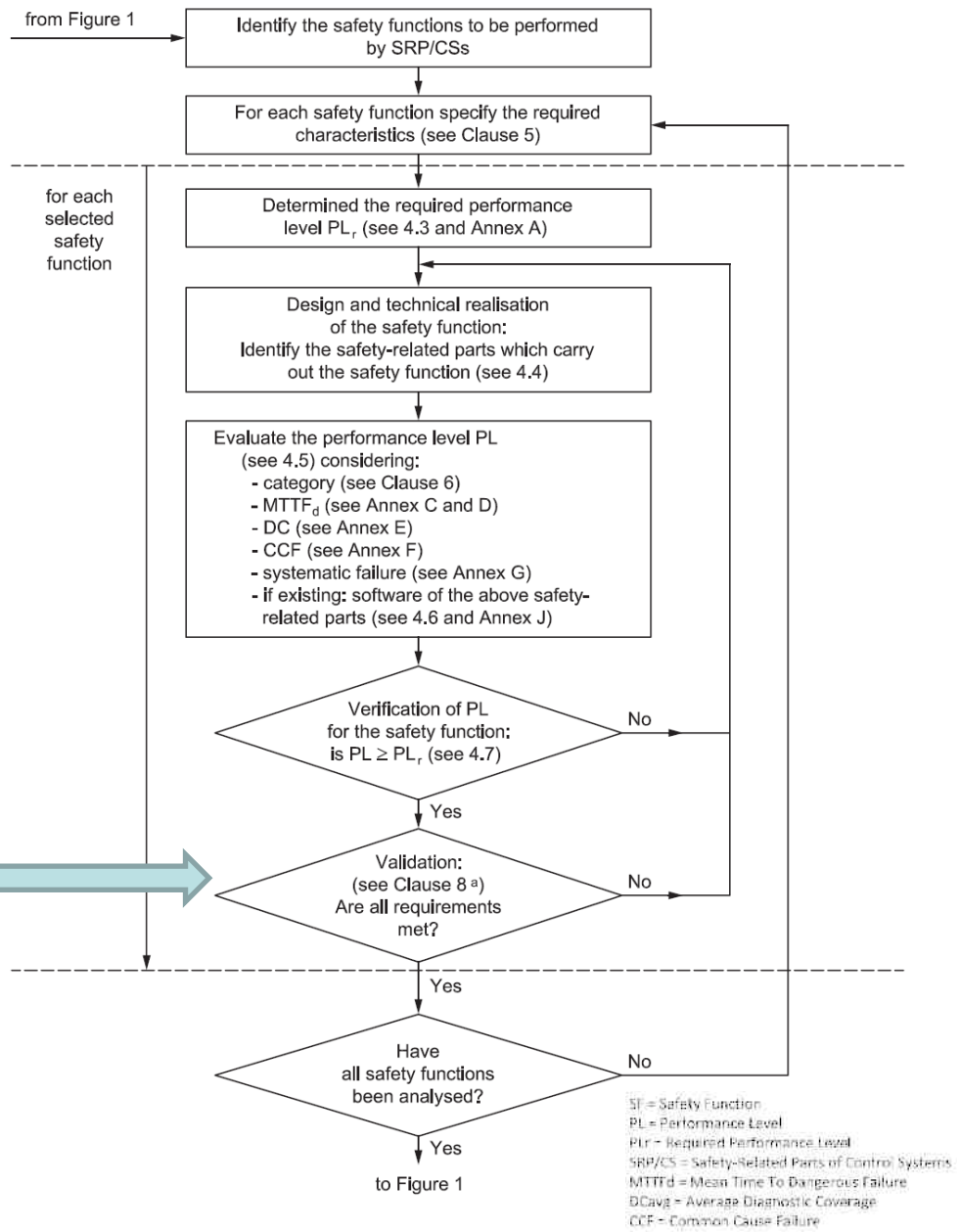

Sources: ISO 13849-1

# ISO 12100 – Analyse de risque → ISO 13849



# ISO 13849 – Design itératif

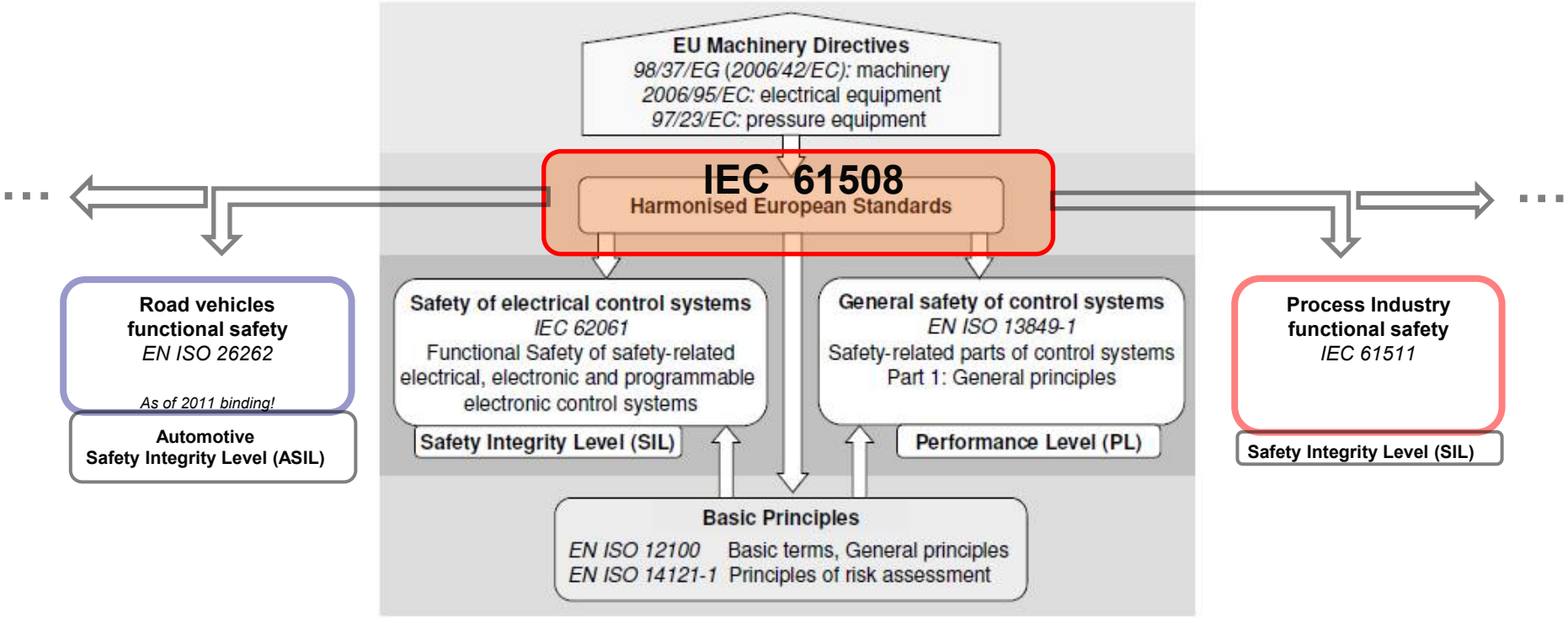





Sources: ISO 13849-1

# IEC 61508 – La sécurité fonctionnelle





Sources: Berns Engineers

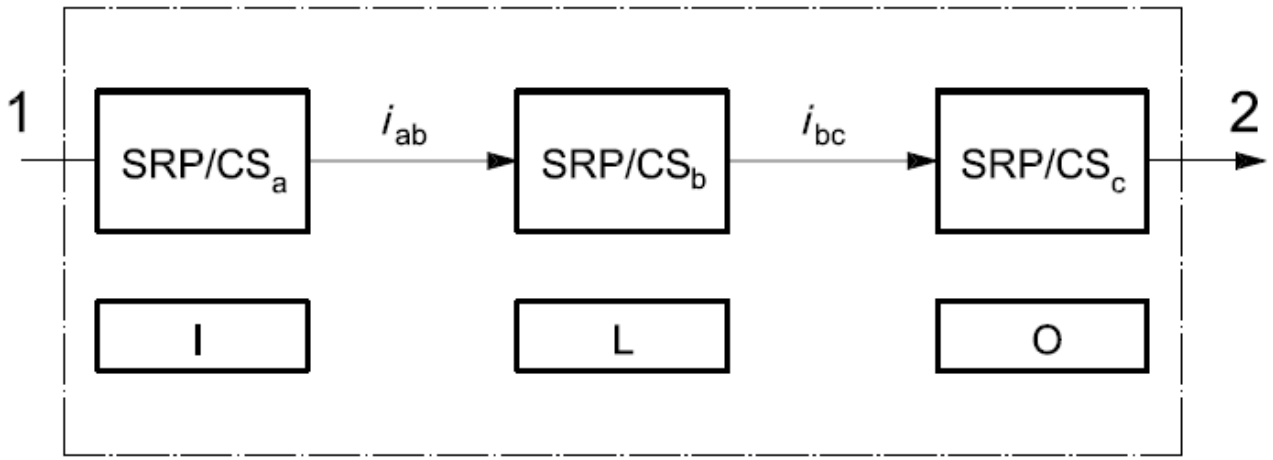
# Le niveau de sécurité selon le domaine d'application

| Industry | Domain Specific "Safety Integrity Levels" | | | | |
|---|---|---|---|---|---|
| Aerospace<br>RTCA DO254 (HW) / DO 178C (SW) | DAL E | DAL D | DAL C | DAL B | DAL A |
| General Functional Safety<br>IEC 61508 | (SIL 0) | SIL 1 | SIL 2 | SIL 3 | SIL 4 |
| Railway<br>CENELEC EN 50126 / 50128 / 50129 | (SIL 0) | SIL 1 | SIL 2 | SIL 3 | SIL 4 |
| Automotive<br>ISO EN 26262 | QM | ASIL A | ASIL B/C | ASIL D | - |
| Machinery<br>ISO 13849 | PL A | PL B/C | PL D | PL E | - |


Sources: Berns Engineers

# Qu’est-ce qu’un SRP-CS?

**safety–related part of a control system**
**SRP/CS**
part of a control system that responds to safety-related input signals and generates safety-related output signals

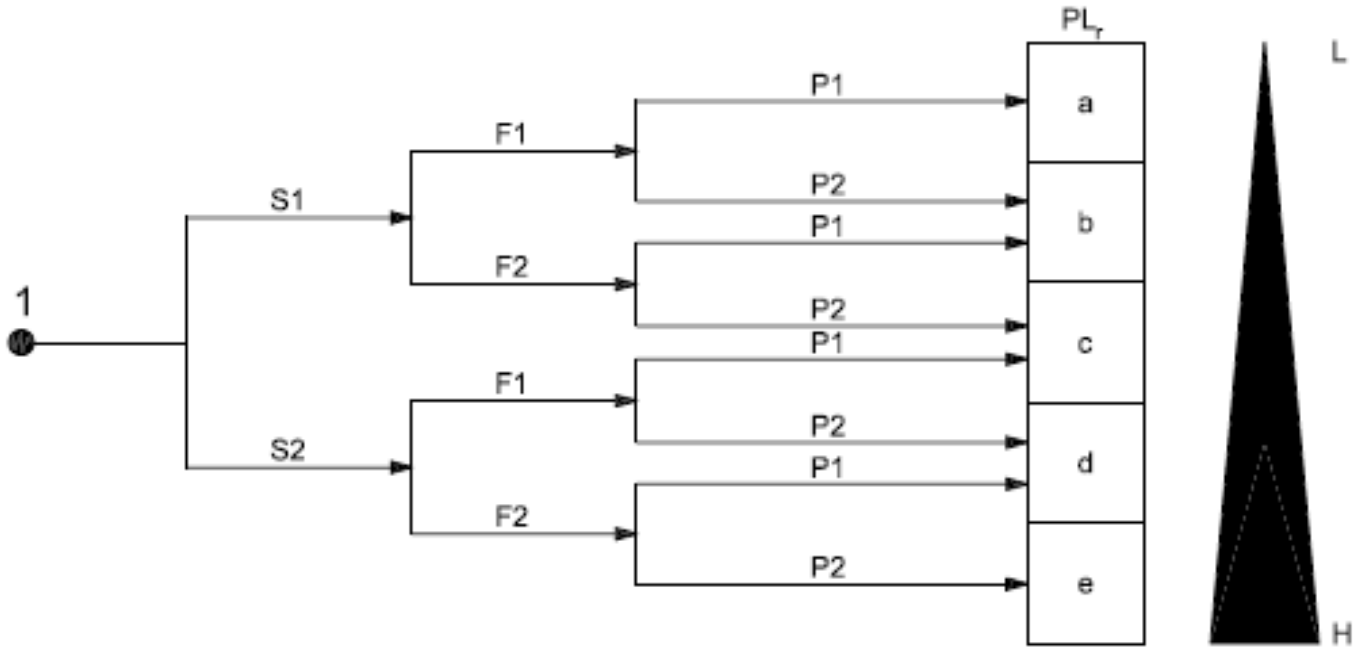



**Key**

I input (e.g. limit switch, sensor, AOPD)
L logic
O output (e.g. valve, contactor, current converter)
1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)
2 machine actuator (e.g. motor, cylinder)

# La définition du niveau de performance requis (PLr)

Toutes les fonctions de sécurité (par exemple la prévention d'un démarrage intempestif) réalisées par les SRP-CS doivent être identifiées et leurs caractéristiques, définies, y compris le niveau de performance requis $PL_r$. Pour définir ce dernier paramètre, nous pouvons utiliser l'analyse par graphe des risques :





Sources: ISO 13849-1

# Le graphe des risques – Paramètres

Tout comme pour certaines méthodes d'évaluation du risque selon la norme ISO 12100, nous devons estimer le risque en prenant en compte 3 facteurs:

La sévérité – S:

- S1 – Blessure sans complications
- S2 – Blessures avec complications (p.ex. amputation, paralysie, mort…)

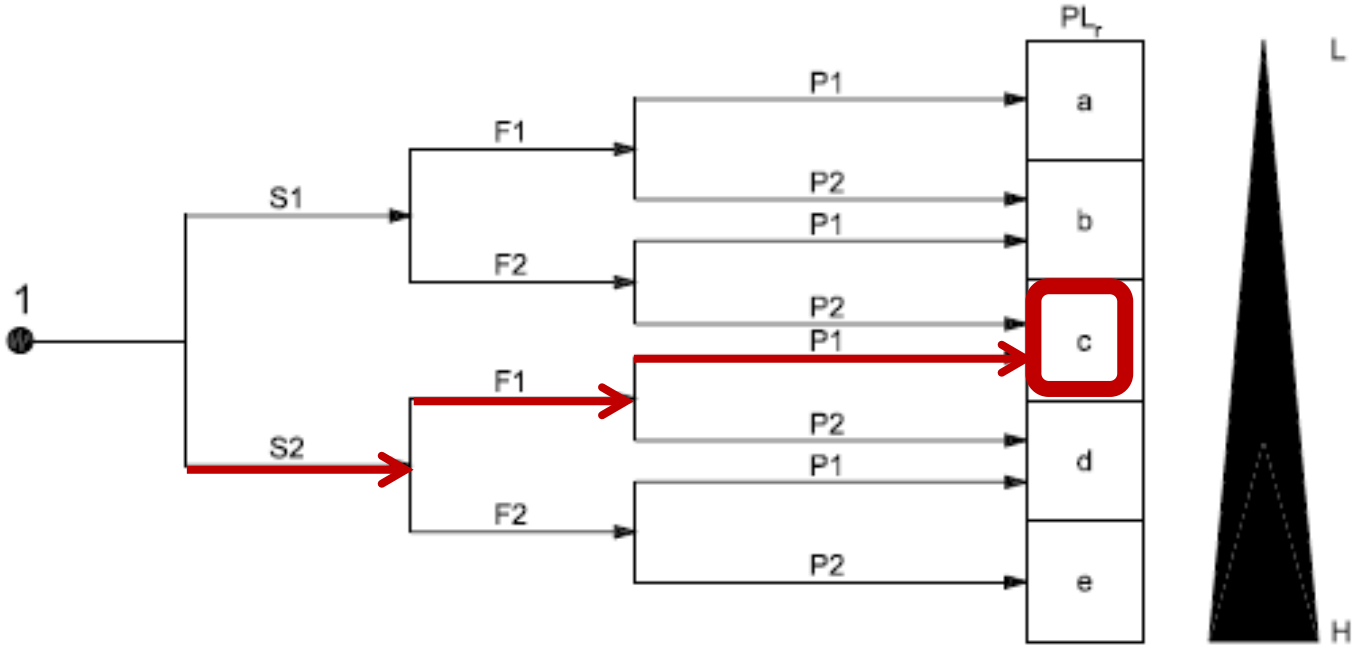
La fréquence d'exposition au danger – F:

- F1 – Il est rare qu'une personne soit exposée au danger
- F2 – Une personne est fréquemment ou continuellement exposée au danger

La possibilité d'éviter le danger – P:

- P1 – Il y a une chance réaliste que le danger soit évité ou que sont impact soit limité
- P2 – La personne en danger ne pourra pas éviter le danger

# Niveau de performance requis exemple (PLr)




**Key**

| | |
|---|---|
| 1 | starting point for evaluation of safety function's contribution to risk reduction |
| L | low contribution to risk reduction |
| H | high contribution to risk reduction |
| $PL_r$ | required performance level |

**Risk parameters:**

| | |
|---|---|
| S | severity of injury |
| S1 | slight (normally reversible injury) |
| S2 | serious (normally irreversible injury or death) |
| F | frequency and/or exposure to hazard |
| F1 | seldom-to-less-often and/or exposure time is short |
| F2 | frequent-to-continuous and/or exposure time is long |
| P | possibility of avoiding hazard or limiting harm |
| P1 | possible under specific conditions |
| P2 | scarcely possible |



Sources: ISO 13849-1

# Les types de défaillances

Lors du développement d'un système relatif à la sécurité, nous différencions deux types de défaillances possibles qui devront être couvertes:

**Les défaillances aléatoires:**

- Défaillance ne pouvant être prévue, elle est souvent due à une ou plusieurs dégradations dans le matériel. Ces défaillances peuvent être dues aux conditions dans lesquelles la machine évolue (humidité, température, vibrations…)

**Les défaillance systématiques:**

- Défaillances souvent liées à une erreur humaine ou une erreur de design
  - Mauvaise formulation des spécifications
  - Erreur de conception de la partie matérielle
  - Erreur de production
  - Erreur d'installation de la machine
  - Erreur de conception ou d'intégration du logiciel

# Prévenir les défaillance systématiques

Quelques exemples de mesures qui peuvent être mises en place pour détecter et corriger certaines erreurs systématiques se trouvent dans l'annexe G de l'ISO 13949-1.

## Annex G
(informative)

## Systematic failure

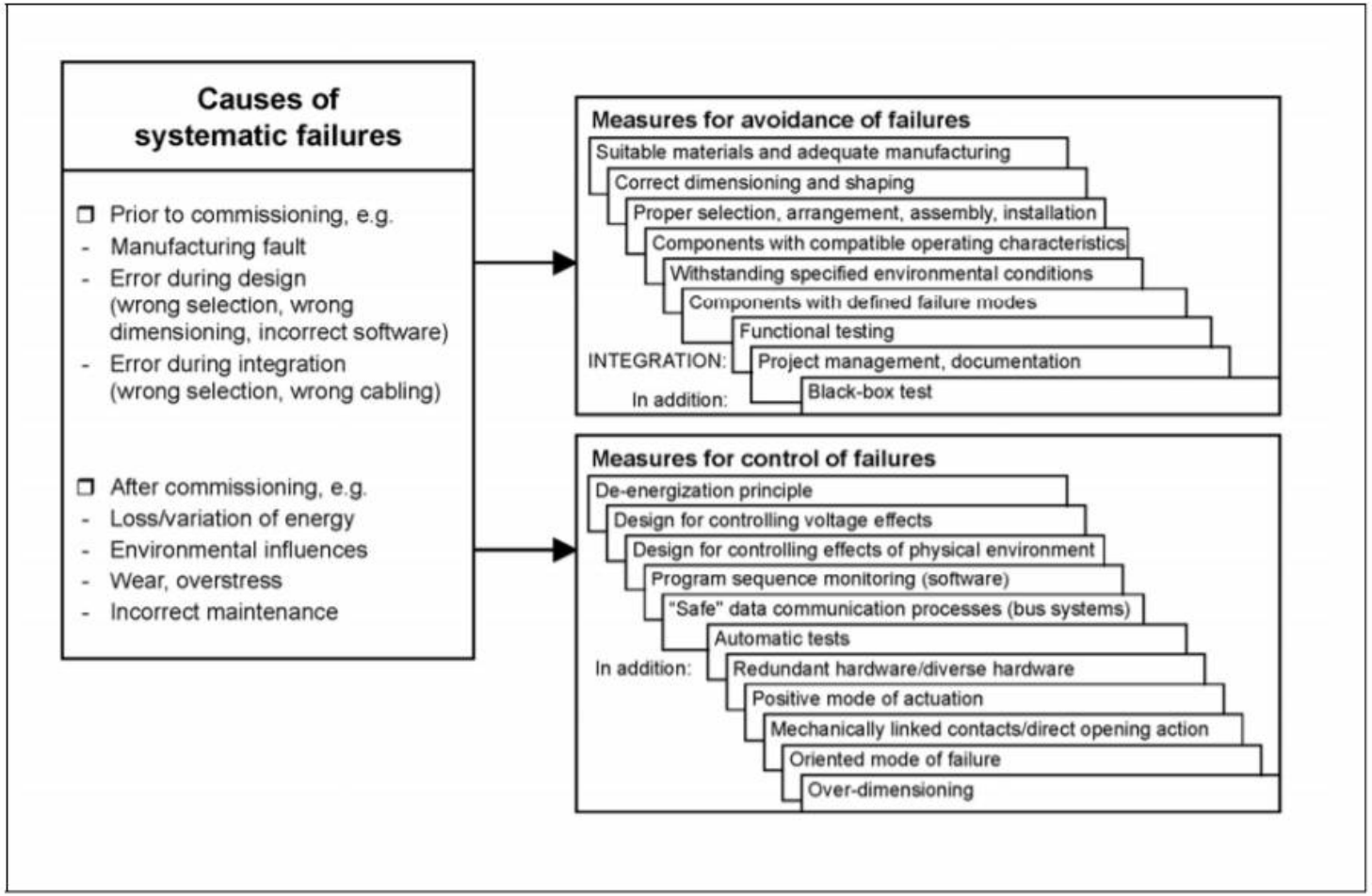
### G.1 General

ISO 13849-2 gives a comprehensive list of measures against systematic failure which should be applied, such as basic and well-tried safety principles.

### G.2 Measures for the control of systematic failures

The following measures should be applied.

# Prévenir les défaillance systématiques



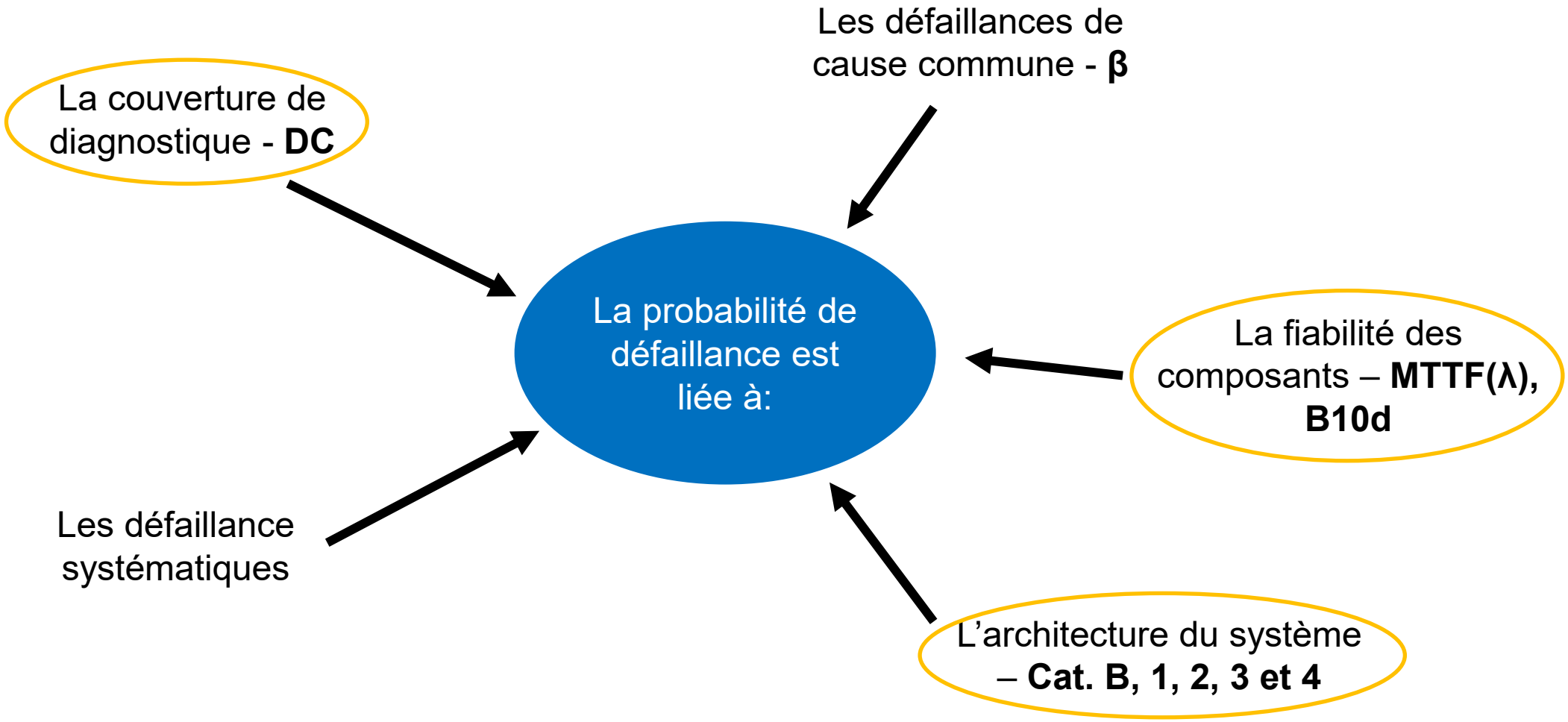
# Prévenir les défaillance aléatoires

Afin de prévenir les défaillance aléatoires, il est nécessaire de calculer le taux défaillance de notre système grâce à l'indice PFH (Probabilité de défaillance par heure)

| PL | Average probability of dangerous failure per hour ($PFH_D$) 1/h |
|---|---|
| a | $\geq 10^{-5}$ to $< 10^{-4}$ |
| b | $\geq 3 \times 10^{-6}$ to $< 10^{-5}$ |
| c | $\geq 10^{-6}$ to $< 3 \times 10^{-6}$ |
| d | $\geq 10^{-7}$ to $< 10^{-6}$ |
| e | $\geq 10^{-8}$ to $< 10^{-7}$ |

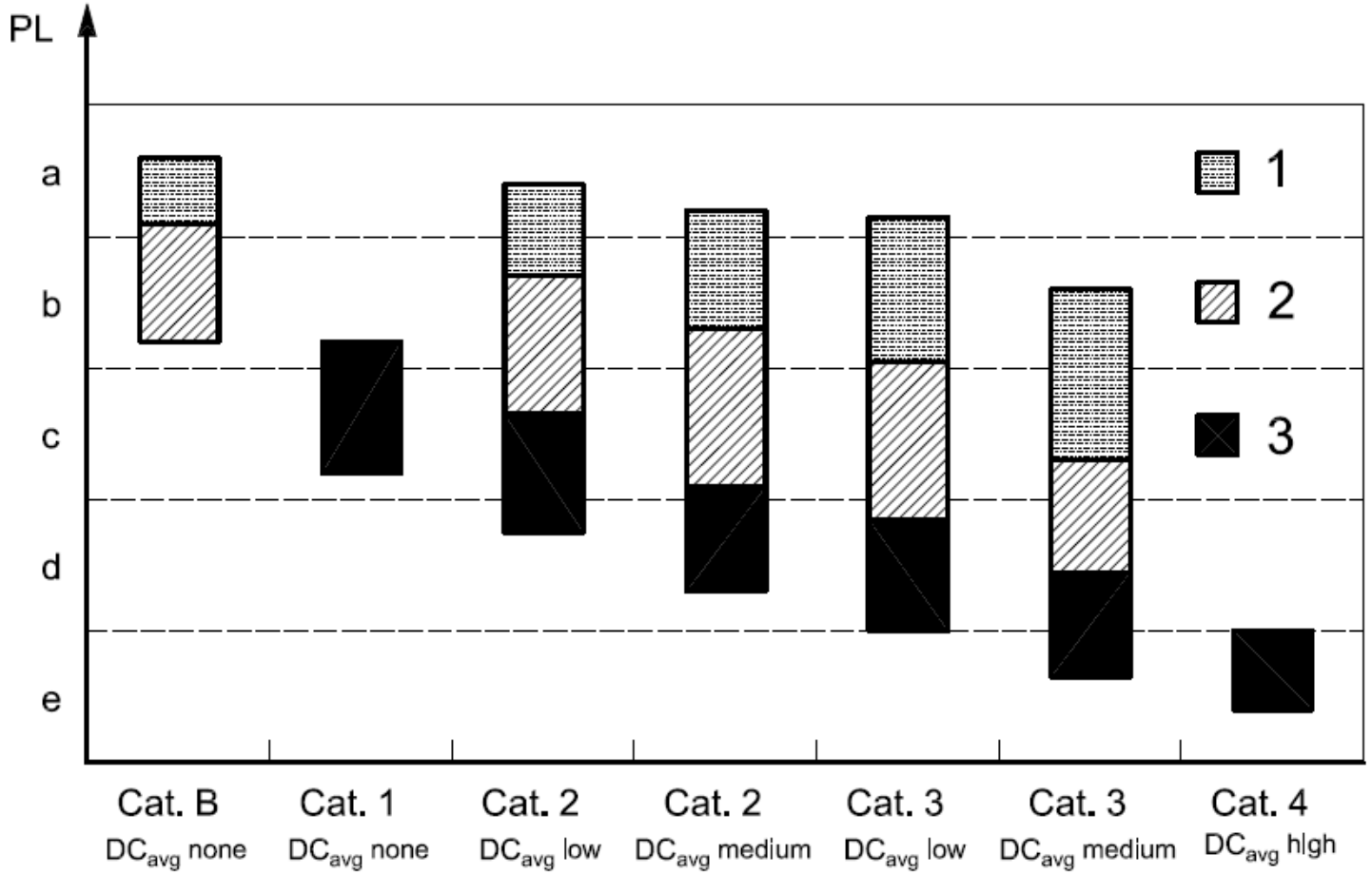

Sources: ISO 13849-1

# ISO 13849 – Les paramètres de la sécurité



# Les paramètres requis valider le PL atteint

Ce graphique propose, de manière simplifiée, l'évaluation du niveau PL atteint par un système:




**Key**

| | |
|---|---|
| PL | performance level |
| 1 | $MTTF_D$ of each channel = low |
| 2 | $MTTF_D$ of each channel = medium |
| 3 | $MTTF_D$ of each channel = high |


Sources: ISO 13849-1

# Les paramètres requis valider le PL atteint (3)

Les paramètres requis sont donc:

- La catégorie d'architecture utilisé (Category)
- La couverture de diagnostique ($DC_{avg}$)
- Le $MTTF_D$ de chaque canal

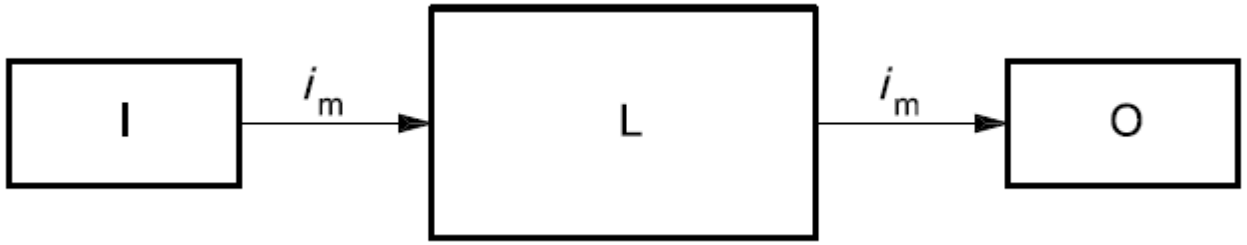
Vient s'additionner à ça deux facteurs indépendants qui sont:

- Le développement selon le cycle de vie de la norme (défaillance systématiques)
- Les défaillances de causes communes (β)

 Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie B

| Category | Summary of requirements | System behaviour | Principle used to achieve safety | $MTTF_D$ of each channel | $DC_{avg}$ | CCF |
|---|---|---|---|---|---|---|
| B (see 6.2.3) | SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used. | The occurrence of a fault can lead to the loss of the safety function. | Mainly characterized by selection of components | Low to medium | None | Not relevant |




**Key**

$i_m$ interconnecting means

I input device, e.g. sensor

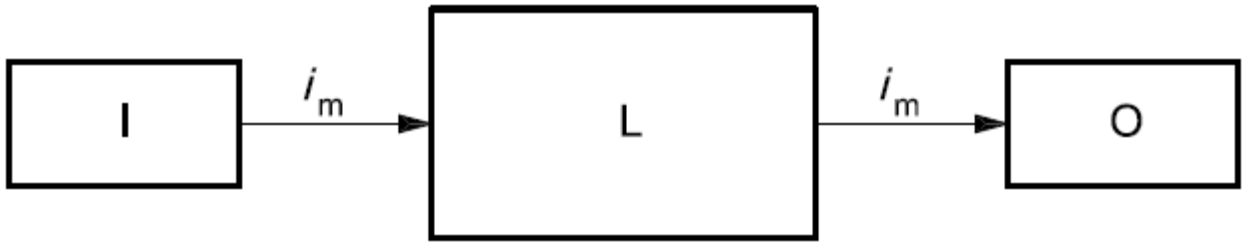
L logic

O output device, e.g. main contactor


Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 1

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 (see 6.2.4) | Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used. | The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B. | Mainly characterized by selection of components | High | None | Not relevant |




**Key**

$i_m$ interconnecting means

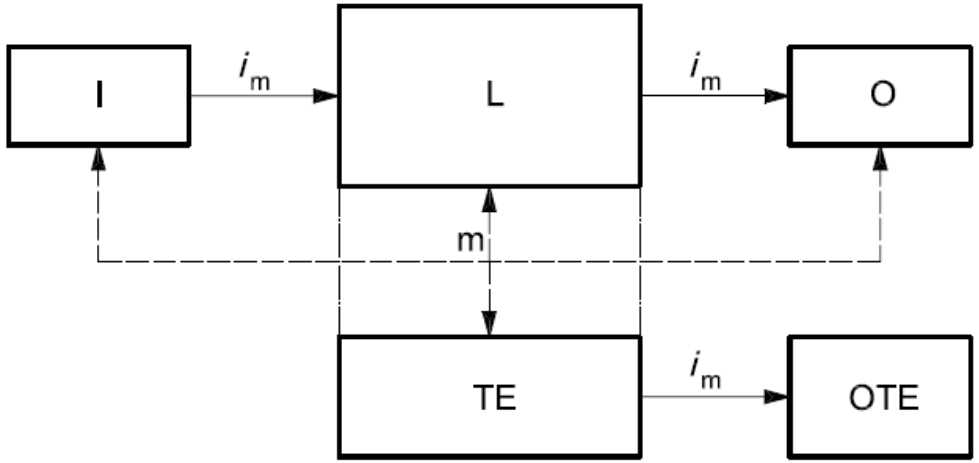
I input device, e.g. sensor

L logic

O output device, e.g. main contactor

# Les catégories d'architecture – Catégorie 2

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 (see 6.2.5) | Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system (see 4.5.4). | The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check. | Mainly characterized by structure | Low to high | Low to medium | See Annex F |



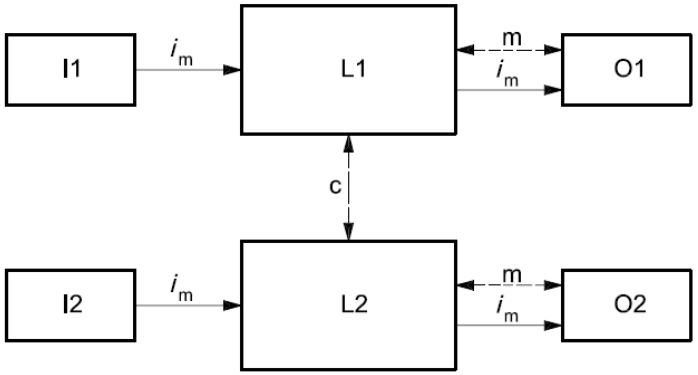

**Key**

| | |
|---|---|
| $i_m$ | interconnecting means |
| I | input device, e.g. sensor |
| L | logic |
| m | monitoring |
| O | output device, e.g. main contactor |
| TE | test equipment |
| OTE | output of TE |

Dashed lines represent reasonably practicable fault detection.

# Les catégories d'architecture – Catégorie 3

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 (see 6.2.6) | Requirements of B and the use of well-tried safety principles shall apply.<br>Safety-related parts shall be designed, so that<br>— a single fault in any of these parts does not lead to the loss of the safety function, and<br>— whenever reasonably practicable, the single fault is detected. | When a single fault occurs, the safety function is always performed.<br>Some, but not all, faults will be detected.<br>Accumulation of undetected faults can lead to the loss of the safety function. | Mainly characterized by structure | Low to high | Low to medium | See Annex F |



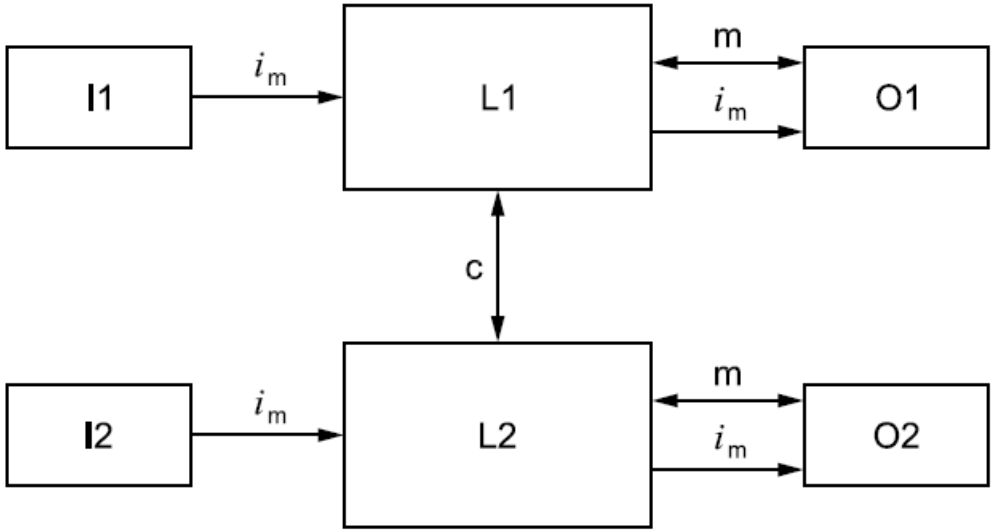

**Key**

| | |
|---|---|
| $i_m$ | interconnecting means |
| c | cross monitoring |
| I1, I2 | input device, e.g. sensor |
| L1, L2 | logic |
| m | monitoring |
| O1, $O_2$ | output device, e.g. main contactor |

Dashed lines represent reasonably practicable fault detection.


Sources: ISO 13849-1

# Les catégories d'architecture – Catégorie 4 (2)




**Key**

| | |
|---|---|
| $i_m$ | interconnecting means |
| c | cross monitoring |
| I1, I2 | input device, e.g. sensor |
| L1, L2 | logic |
| m | monitoring |
| O1, $O_2$ | output device, e.g. main contactor |

Solid lines represent diagnostic coverage higher than in the Cat.3 architecture

# Le paramètre DC

| DC | |
|---|---|
| **Indice** | **Gamme** |
| Nulle | DC < 60 % |
| Faible | 60 % ≤ DC < 90 % |
| Moyenne | 90 % ≤ DC < 99 % |
| Élevée | 99 % ≤ DC |

NOTE 1 Pour les SRP/CS constituées de plusieurs parties, la présente partie de l'ISO 13849 utilise une valeur moyenne $DC_{avg}$, voir Figure 5, Article 6 et E.2.

NOTE Le choix d'une gamme de DC est basée sur les valeurs clés de 60 %, 90 % et 99 % qu'on peut déjà trouver dans d'autres normes (par exemple la série IEC 61508) traitant des tests de couverture de diagnostic. Des recherches montrent que (1-DC) plutôt que DC lui-même est une mesure caractéristique pour déterminer l'efficacité du test. (1-DC) pour les valeurs clés de 60 %, 90 % et 99 % forme une sorte d'échelle logarithmique en cohérence avec l'échelle logarithmique du PL. Une valeur de DC de moins de 60 % a une faible incidence sur la fiabilité du système soumis à essai et est de ce fait qualifiée de «nulle». Une valeur de DC supérieure à 99 % pour des systèmes complexes est très difficile à obtenir. Pour des raisons pratiques, le nombre de gammes a été restreint à quatre. Les valeurs limites données dans ce tableau sont présumées être précises à 5 %.

# Le paramètre DC – Calcul

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}}$$

Le DC représente le ratio de fautes dangereuses détectées par rapport à la somme de la totalité des fautes dangereuses du système.

Des exemples de DC se trouvent dans l'annexe E de l'ISO 13849-1

# DC - Annexe E

| 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. | 99 % |
| Surveillance croisée des entrées sans test dynamique | 0 % à 99 %, 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 % |
| Surveillance croisée des entrées et des résultats intermédiaires internes à la logique (L) et moniteur de logiciel temporel et logique du programme et détection de défauts statiques et des courts-circuits (pour I/O multiples) | 99 % |
| Surveillance indirecte (par exemple par commutateur de pression, surveillance de position électrique des actionneurs) | 90 % à 99 %, dépendant de l'application |
| Surveillance directe (par exemple surveillance de position électrique des distributeurs de commande, surveillance des dispositifs électro-mécaniques par éléments de contact mécaniquement liés) | 99 % |
| Détection des défauts par le procédé | 0 % à 99 %, dépendant de l'application; cette mesure toute seule n'est pas suffisante pour un niveau requis de performance «e» ! |
| Surveillance de quelques caractéristiques du capteur (temps de réponse, gamme des signaux analogiques, par exemple résistance électrique, capacité) | 60 % |
| **Logique** | |
| Surveillance indirecte (par exemple surveillance par commutateur de pression, surveillance de position électrique des actionneurs) | 90 % à 99 %, dépendant de l'application |
| Surveillance directe (par exemple surveillance de position électrique des distributeurs de commande, surveillance des dispositifs électro-mécaniques par éléments de contact mécaniquement liés) | 99 % |
| Surveillance temporelle simple de la logique (par exemple: temporisateur comme chien de garde, lorsque les points de déclenchement se situent dans le programme de la logique) | 60 % |
| Surveillance temporelle et logique de la logique par chien de garde, lorsque l'équipement d'essai réalise des contrôles de vraisemblance du comportement de la logique | 90 % |
| Auto-tests à la mise en marche pour détecter les défauts latents dans | 90 % (dépendant de la technique d'essai) |

# Le paramètre $MTTF_D$

| $MTTF_D$ | |
|---|---|
| **Indice pour chaque canal** | **Gamme pour chaque canal** |
| Faible | 3 ans $\leqslant MTTF_D <$ 10 ans |
| Moyen | 10 ans $\leqslant MTTF_D <$ 30 ans |
| Élevé | 30 ans $\leqslant MTTF_D \leqslant$ 100 ans |

NOTE 1 Le choix d'une gamme de $MTTF_D$ pour chaque canal est basé sur les taux de défaillance trouvés dans l'état de l'art du domaine formant une échelle logarithmique cohérente avec l'échelle logarithmique des PL. Une valeur de $MTTF_D$ pour chaque canal inférieure à 3 années n'est pas supposée être trouvée pour des SRP/CS réels dans la mesure où cela signifierait qu'après une année, 30 % de l'ensemble des systèmes du marché seraient défaillants et susceptibles d'être remplacés. Une valeur de $MTTF_D$ pour chaque canal supérieure à 100 années n'est pas acceptable dans la mesure où une SRP/CS traitant d'un risque élevé ne devrait pas dépendre uniquement de la fiabilité des composants. Afin de renforcer les SRP/CS contre les défaillances systématiques et aléatoires, il convient que des moyens additionnels tels que redondance et essais soient requis. Pour des raisons pratiques, le nombre de gammes a été restreint à trois. La limitation du $MTTF_D$ pour chaque canal à une valeur maximale de 100 années se réfère aux SRP/CS à canal unique qui réalisent la fonction de sécurité. Des valeurs plus élevées de $MTTF_D$ peuvent être utilisées pour des composants simples (voir Tableau D.1).

NOTE 2 Les valeurs limites données dans ce tableau sont présumées être précises à 5 %.


Sources: ISO 13849-1

# Le paramètre $MTTF_D$ – Calcul

**$h_{op}$**
nombre moyen d'heures d'utilisation par jour

**$d_{op}$**
nombre moyen de jours d'utilisation par an

**$t_{cycle}$**
temps moyen entre le démarrage de 2 cycles successsifs du composant en secondes par cycle

**$n_{op}$**
nombre d'opérations par an

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ {}^{s}/_{h}}{t_{cycle}}$$

**$B_{10d}$**
Donnée du fabricant du composant

**$MTTF_d$**

$$MTTFd = \frac{B10d}{0{,}1 \times n_{op}}$$

B10d = nombre moyen de cycles jusqu'à ce que 10 % des composants soient défaillants

Lorsque le fabricant n'est pas capable de fournir les donnée afin de calculer le MTTF, alors il est possible d'utiliser des bases de données de fiabilité, certains exemples sont aussi données dans l'annexe C de l'ISO 13849-1. Si le composant n'est vraiment pas disponible, alors, 10 ans est parfois utilisé par défaut.

# Le paramètre β – Défaillances de cause commune

Pour certaines catégories d'architecture, un indice β supérieur à 65 est demandé. Celui-ci est calculé en additionnant les valeurs de la table ci-dessous lorsque les mesures sont respectées:

| No. | Measure against CCF | Score |
|---|---|---|
| 1 | **Separation/ Segregation** | |
| | Physical separation between signal paths, for example:<br>— separation in wiring/piping;<br>— detection of short circuits and open circuits in cables by dynamic test;<br>— separate shielding for the signal path of each channel;<br>— sufficient clearances and creepage distances on printed-circuit boards. | **15** |
| 2 | **Diversity** | |
| | Different technologies/design or physical principles are used, for example:<br>— first channel electronic or programmable electronic and second channel electromechanical hardwired,<br>— different initiation of safety function for each channel (e.g. position, pressure, temperature),<br>and/or<br>digital and analog measurement of variables (e.g. distance, pressure or temperature)<br>and/or<br>Components of different manufactures. | **20** |

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

# Le paramètre β – Défaillances de cause commune (2)

| No. | Measure against CCF | Score |
|---|---|---|
| 3 | **Design/application/experience** | |
| 3.1 | Protection against over-voltage, over-pressure, over-current, over-temperature, etc. | 15 |
| 3.2 | Components used are well-tried. | 5 |
| 4 | **Assessment/analysis** | |
| | For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design. | 5 |
| 5 | **Competence/training** | |
| | Training of designers to understand the causes and consequences of common cause failures. | 5 |
| 6 | **Environmental** | |
| 6.1 | For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1).<br>Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium.<br>NOTE For combined fluidic and electric systems, both aspects should be considered. | 25 |
| 6.2 | Other influences<br>Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards). | 10 |
| | **Total** | [max. achievable 100] |

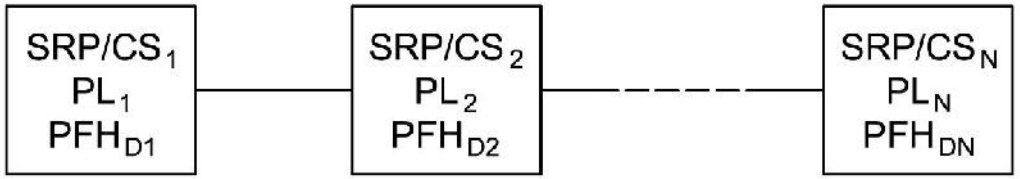
| Total score | Measures for avoiding CCF[a] |
|---|---|
| 65 or better | Meets the requirements |
| Less than 65 | Process failed ⇒ choose additional measures |

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.


Sources: ISO 13849-1

# Combinaison des SRP/CS pour atteindre un PL global

On considère qu'il existe N $SRP/CS_i$ distinctes dans une combinaison en série, qui réalisent ensemble une fonction de sécurité. Pour chaque $SRP/CS_i$, un $PL_i$ a déjà été évalué. Si les valeurs de $PFH_D$ de toutes les $SRP/CS_i$ sont connues, la $PFH_D$ de la SRP/CS combinée est égale à la somme de toutes les valeurs de $PFH_D$ des N $SRP/CS_i$ individuelles.

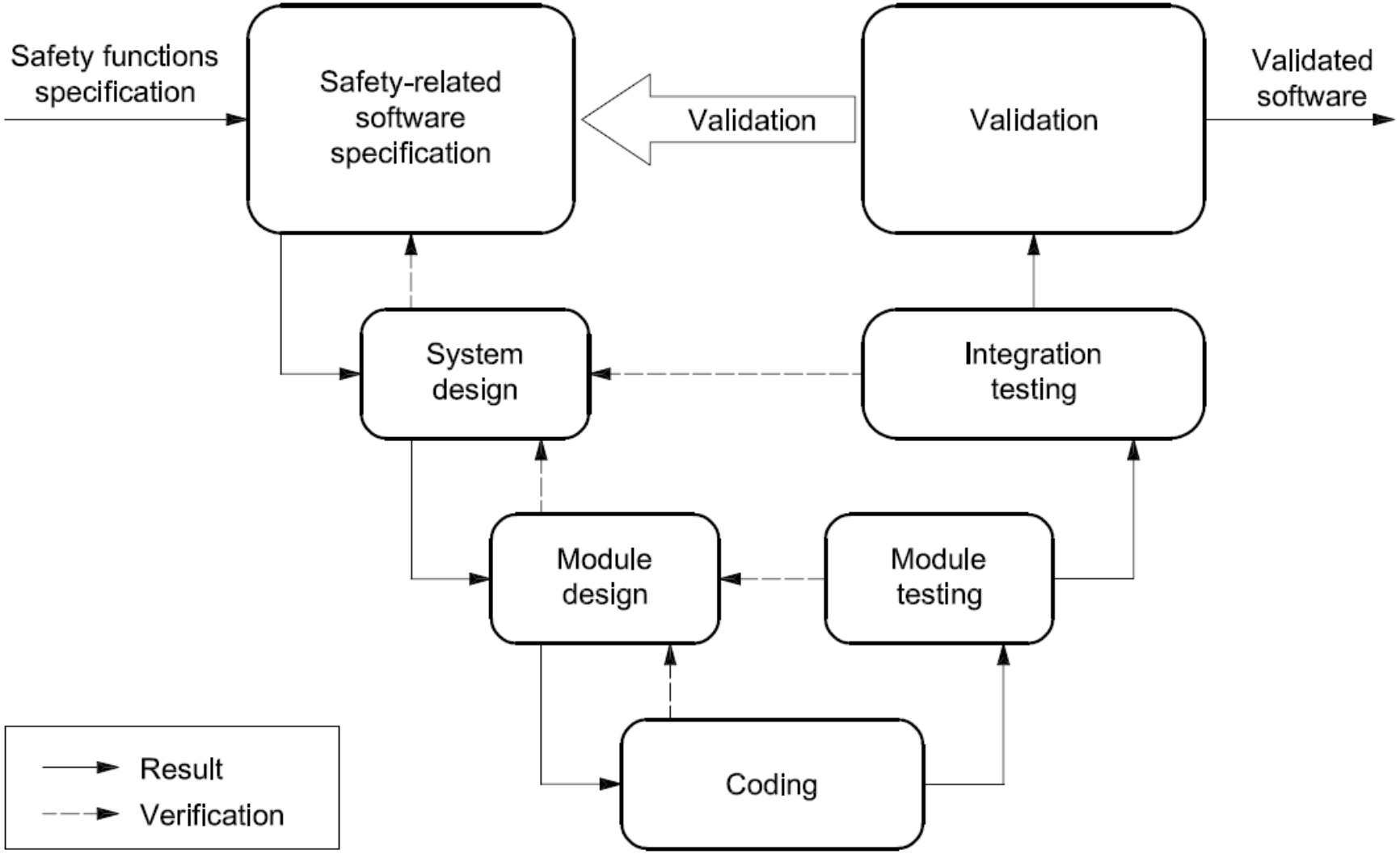



**SRP/CS**

PL

$$PFH_D = PFH_{D1} + PFH_{D2} + \ldots + PFH_{DN}$$

# Le développement software





Sources: ISO 13849-1

# Exemples de question d’examen

# Exemples :

Quelles sont les 6 étapes pour obtenir le marquage CE ?

Mentionnez 3 directives qui requièrent un marquage CE ?

Quels sont les avantages et limitations d'utilisation d'un protecteur de type «Protecteur ajustable»?

Pour une vanne pneumatique, un fabricant détermine une valeur moyenne de 50mio de cycles pour son B10d. La vanne est utilisée 8h par jour durant 260 jours par année. Le temps moyen entre le démarrage de deux commutations successives de la vanne est estimé à 6 secondes. Calculez le nombre d'opérations par année (Nop) et le MTTFd de ce système.

Quelle est la différence entre une défaillance systématique et une défaillance aléatoire ? À quoi sont dues les défaillances systématiques ?

Quels sont les 3 piliers du «Model Based System Engineering» ?

# Merci à tous pour votre participation et votre intérêt

N’hésitez pas à me contacter pour toute question avant l’examen mais aussi plus tard dans votre vie professionnelle.

Par email: eric.silva@hefr.ch
Sur LinkedIn: linkedin.com/in/-eric-silva