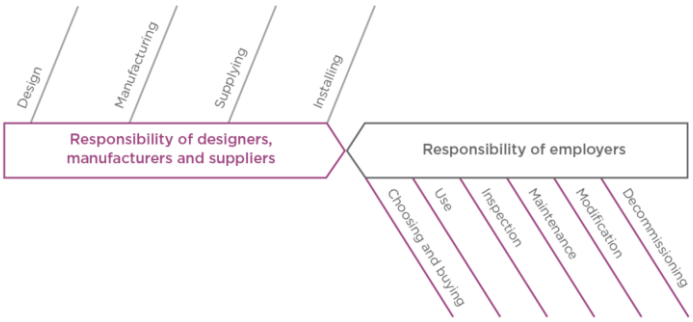
Résumé SecuFS

Cours 1 - Introduction

Responsabilités dans la fabrication d'un appareil

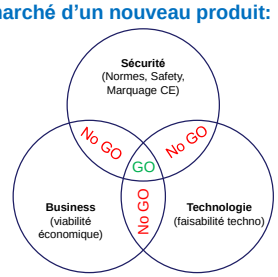


Comment est classifié le risque ?

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

SIL niveau de protection pour composant électronique
Approche de l'analyse de risque : 1) identification + définir SIL requit 2) réduire risque et voir si le SIL requit est atteint 3) Sinon réduire encore jusqu'à un risque résiduel pour l'atteindre

Mise sur le marché d'un nouveau produit:



Niveau de danger à définir individuellement -> danger perçu individuellement

Le risque : lien entre criticité d'événement et probabilité d'occurrence

Cours 2 – Certification CE

Marquage CE :
Tout produit venu en Europe doit avoir le marquage CE, norme harmonisée (reconnue par société). 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.
Norme CE felxible pour que les produits puissent être développés tout en garantissant un maximum de sécurité
Etapes :

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

24 directives du CE cours2, s10
Toujours vérifier les 24 directives s'assurer que le produit les respecte bien

Chaque directive décrit les exigences essentielles (très générales) auxquelles doivent répondre le produit.

Exigence directive machine cours2, s15 et s18

Intégration de la sécurité

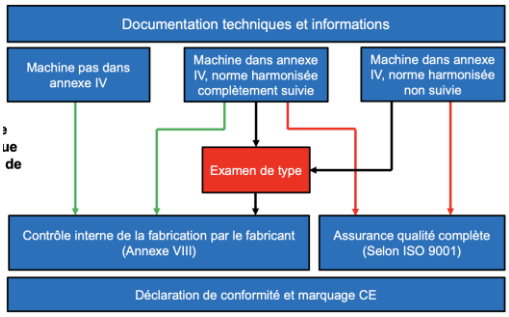
1. **Fonctionnement, réglage, entretien sans risque pour des personnes**
2. **Mesure de réduction des risques : éliminer/réduire risques – ajout de protections nécessaires pour éliminer risque – informer l'utilisateur et prévoir EPI**
3. **Construire de telle façon qu'elle ne soit pas utilisée de façon anormale**
4. **Construit en tenant compte des contraintes de l'utilisateur**
5. **Doit être livrée avec tous les équipements et accessoires spéciaux -> garantir entretien et utilisation sécurisée**

Type de normes :
1. A : norme de sécurité de base, termes de base et aspect généraux appliqués aux machines ISO12100
2. B : Traite des aspects de sécurité : B1 pour une série de machine, ISO 13849/13855 B2 pour dispositif de protection spécifique ISO 13851/14120
3. Norme de sécurité des machines : exigence de sécurité détaillé pour un type de machine précis ISO 16092/EN415/EN12409

Tableau d'application des différents types de norme : cours2, s21

Norme pour les machines
- ISO 12100 : principes généraux de conception, appréciation et réduction du risque
- ISO 12420 : Prescription pour la conception des protecteurs fixes et mobiles
- ISO 13857 : Distance de sécurité membres sup et inf, pour les 14+
- ISO 13849 : Pour les systèmes à logique programmable, système commande relatif à la sécurité
- IEC 60204 : équipement électrique des machines, sécurité câblage+équipement élec

Pour les machines dangereuses, un audit est requis (ON) pour obtenir la certification CE
Liste machine dangereuse annexe IV, cours2, s30



Comment obtenir le CE

- Module d'évaluation pour s'assurer que le produit répond aux exigences essentielles
- **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)

->2 approches : 1) contrôle de qualité par le fabricant 2) Évaluation conformité par un ON

1) Une entreprise peut faire elle-même l'évaluation de de conformité si elle a le matériel nécessaire -> peu coûteux
2) Le fabricant peut demander une évaluation par un ON, mais reste à la fin le responsable de conformité + exigences essentielles de l'UE

Certification CE : étapes typiques :

- 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.

Dossier de conformité
Le dossier démontre que la machine est conforme aux exigences de la directive
Couvre : conception, fabrication, fonctionnement, mesure pour évaluation conformité
Doit être établi dans plusieurs langue (dépend du pays de commercialisation)

Déclaration de conformité (1page et fait ref au dossier de conformité), elle contient :

- Qui on est
- Pour quel produit est la déclaration
- Quelles directives concernées
- Quelles normes sont suivies
- Où trouver les résultats des essais
- Qui est responsable dans l'entreprise

Cours 3 – ISO 12100, analyse de risque

Généralités (1)

Directive machine : le fabricant doit déterminer les exigences essentielles de santé et sécurité s'appliquant à la machine et pour lesquelles il doit prendre des mesures

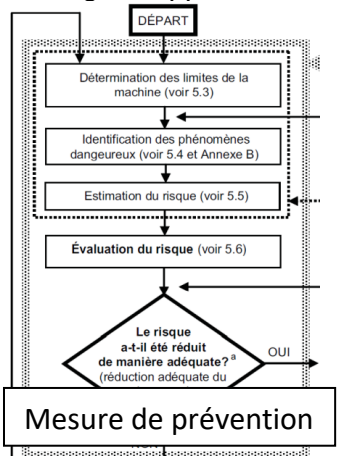
Obligation de l'employeur : doit veiller a prendre les mesures nécessaires afin que les équipements de travail soient adapté au travail à réaliser, assurant sécurité et santé

Structure de la norme 12100 : généralité-appréciation du risque-réduction du risque-documentation -> cours 3, s16

Objectif de la 12100 : 1) approche systématique 2) identifier les dangers liés à la machine, 3) évaluer et estimer les risques potentiels 4) déterminer les systèmes de sécurité requis

Définissions :
Fiabilité (reliable) : aptitude de la machine/composant à accomplir une tache sans défaillance dans un environnement donné et durant un certain temps
Phénomène dangereux : source de phénomène dangereux – soit présent en permanence lors de l'utilisation de la machine (exp déplacement) – soit peut apparaître de manière inattendue (exp explosion)
Dommage : blessure physique, atteinte à la santé
Situation dangereuse : utilisateur exposé à un danger
Risque : combinaison probabilité de dommage et gravité du dommage
Risque résiduel : risque restant après l'application des mesures de prévention
Estimation du risque : définition de la gravité probable d'un dommage + sa proba
Analyse du risque : détermination limite machine + identification phénomène dangereux + estimation risque
Evaluation du risque : à partir analyse de risque, définir si objectif de réduction est atteint
Réduction adéquate du risque : réduction risque répondant au moins aux exigences légales

Stratégie d'appréciation du risque



Facteur d'appréciation du risque :
1) Sécurité de la machine durant toutes phases de son cycle de vie
2) Aptitude de la machine à accomplir sa fonction
3) Commodité d'emploi
4) Coût réalisation-utilisation-démantèlement

Il faut connaître commun la machine sera exploitée, historique accident, santé….

Attention, la conception acceptable d'une machine peut tout d'un coup ne plus l'être avec l'évolution de la technologie

L'appréciation du risque couvre :

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

Prend en compte toutes les personnes utilisant la machine ainsi que l'utilisation normale et les mauvais usages prévisibles
Combinaison mesures concepteur-utilisateur -> réduction du risque en **4 étapes**, cours3,S25

Appréciation du risque (2)

1. Limite d'utilisation : mode de fonctionnement, exigence, formation, exposition d'autres personnes aux phénomènes dangereux (danger de la machine), connaît pas les règles de sécurité
2. Limite dans l'espace : amplitude mvt machine, place pour les opérateurs, source énergie, interaction homme-machine
3. Limite dans le temps : frequ. Entretien, durée vie machine
4. Autres limites : matériaux, environnement, propreté

Phénomènes dangereux

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…

Pour la machine :
Phénomènes peuvent en fonctionnement normal ou en disfonctionnement
En disfonctionnement, peut être du à perturbation externe, var dimension matériau travaillé, perturbation d'alimentation…

Pour l'opérateur :
Peuvent apparaitre si : perte de contrôle de la machine, mauvais comportement (déconcentration, moindre effort, sur utilisation, personnes inappropriée (enfant))

Phénomène dangereux exemple cours3, s36

Dommages dus aux phénomènes dangereux:
Mécanique : Fracture, coupure, amputation, perforation, écorchure, irritation, brûlure, blessure, décès
Electrique : brulure, choc, décès
Thermique : brulure, hypothermie
Bruit : détérioration acuité auditive, stress
Vibration, rayonnement, contamination, ergonomie (cours3, s43)

Estimation : gravité : G1(lésion légère, exp écorchure), G2(lésion grave, irréversible souvent)
Fréquence : F1(rare à assez fréquent/courte durée), F2(fréquent à continu/longue durée)
Proba d'occurrence : O1(très faible, technologie stable), O2(faible >= 1bris/100'000h ou entrainé par qqn de qualifié), O3(élevée >= 1bris/1000h ou entrainé qqn sans expérience)
Possibilité évitement : P1(possible dans certaines conditions), P2(impossible ou presque)

Evaluation des risques réalisée après estimation pour si possible de réduire les risques
Si réduction nécessaire -> 12100 en 3 étapes. Attention à ne pas créer de nouveaux risques

Réduction risque (3)
3 critères : efficacité, faisabilité et coût
Réduction en 3 étapes : 1) Modif de conception (design) 2) application mesure protection 3)information à l'utilisateur

Hiérarchie de suppression des risques, reprend les 3 étapes : 1) Elimination/substitution risque, 2) technologie de protection (butée, barrière, verrouillage…) 3) Mesure d'information (éclairage, klaxon, étiquette, signalisation…) 4) Format/procédure (formation, inspection matériel, procédure)
5) EPI

Documentation d'appréciation du risque (4)

- 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

Structure de la 12100

Structure de la norme:

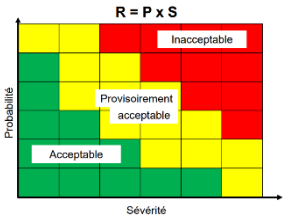
1. Domaine d'application 2. Références normatives 3. Termes et définitions 4. Stratégie d'appréciation du risque	**1. Généralités**
5. Appréciation du risque 2. Information pour l'appréciation du risque 3. Détermination des limites de la machine 4. Identification des phénomènes dangereux 5. Estimation 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**

Cours 4 – ISO 12100 partie 2

Avant analyse de risque : identifier : opérateur, personnel nettoyage/maintenance, équipements, produit et environnement
Pour chaque source : définir le niveau de risque acceptable
sélectionner la méthode d'analyse

2 méthodes : Méthode déductive : approche top-down avec arbre de déffaillance : Hypothèse de départ événement final puis on remonte la chaine
Méthode inductive : approche bottom-up, partira de la défaillance d'un composant/élément et comprendre qu'il est susceptible d'engendrer
-> Matrice risque
-> graphe des risque
-> Indice de criticité

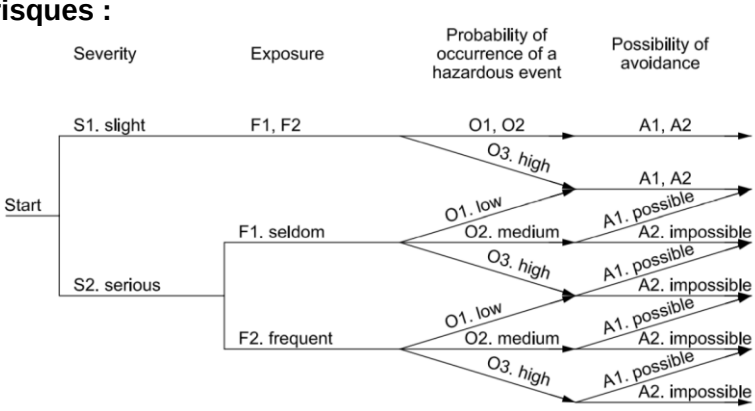
Matrice des risques :
R = P x S (proba * sévérité)



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

Castatrophique -> mort ou infirmité permanente, grave -> blessure mais pourra reprendre l'activité

Graphe des risques :



Acceptable 1-2

Justifiable/tolérable 3-4

Inacceptable 5-6

S1 : Blessure légère (réversible9, **S2** : Blessure grave (potentiellement irréversible)

F1 : 2x durant par période ou <15min dans une journée **F2** : >2x et >15min /période travail

O1 : Technologie reconnue et robuste, **O2** : défaillance technique remarquée, action inadéquate prévisible par qqn de formé (protecteur abimé/incomplet), **O3** : défaillance technique régulière , action inadéquate prévisible par qqn de non formé (exp protecteur manquant)

A1 : possible sous certaines condition d'éviter le danger, **A2** : impossible

Cours 5 – Sécurité des systèmes techniques : Réduction du risque

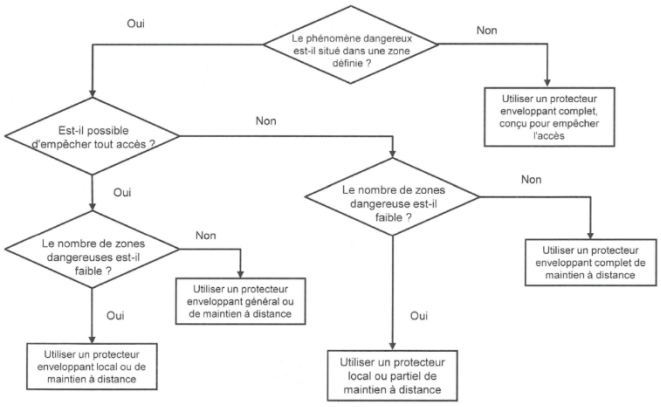
Réduction du risque avec les protecteurs maniques, en plus des risques mécaniques, aussi **risque par le bruit :** protection supplémentaire : enceintes/écran/silencieux, et aussi les **vibrations :** protection supp : dispositif s'amortissement,(support élastique, suspension)
Emission substance dangereuse : protection supp : confinement machine, rinçage, ventilation
Rayonnement : protection supp : filtrage/absorbation, écran atténuateur

ISO 14120 normes relatives à la protection mécanique,
prescription générale pour la fabrication des protecteur fixes et mobiles

Définit les protecteurs : fixes, enveloppants, de maintenance à distance, … s9, cours5

Selon annexe A, protecteur fixe à ne pas utiliser si : accès nécessaire à la zone dangereuse, opération de maintenance dans la zone plus que 1x/mois
Protecteur fixe pas suffisant si : risque protecteur non remonté, si maintenance nécessite le fonctionnement de la machine

En général : protecteur robuste, résistant aux impacts, fixation sûr, taille permettant une manutention aisée
Pour les protecteurs mobiles, ne devrait pas se fermer si qqn se trouve dans la zone dangereuse, sinon besoin 2ème protecteur



Pour les matériaux, prendre en compte les arcs élec, étincelle, fumée, projection
Souvent on met un écran de protection supplémentaire et une ventilation

Protecteur à mettre en jaune -> bien visible et délimite bien la zone dangereuse
Esthétique et facilité d'entretien peuvent influencer le type de matériaux

Outil noyé/fermé exemple poinçonneuse-> aucun accès, sinon max 6mm de jeu mais besoin protection supplémentaire → grande protection ! mais utilisation limité, forme matériau tjs la même par exp.

Protecteur fixe : facile à adapter/installer, maintenance minimum mais peut limiter la visibilité, limité le type d'opération et les réparations demandent des fois leur démontage complet

Protecteur interverrouillage : si ouverture protecteur-> machine arrêtée/déclenchée (elec, pneumatique, hydraulique…), machine ne redémarre qu'après fermeture !
Protection max, accès à la machine rapide, mais peut facilement être désactivé

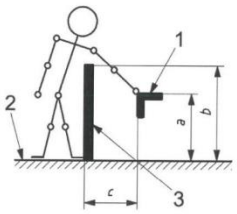
Protecteur ajustable : peuvent être ajustés en fonction de l'opération à réaliser
Permet une variation de la taille de la matière à travailler, mais les mains pourraient entrer dans la zone de danger, l'opérateur peut retirer la protection, peut limiter la visibilité

Protecteur auto-ajustable : le protecteur s'adapte seul en fonction du matériel usiné, quand elle est enlevée, le protecteur se referme
Ajustable et prêt à l'emploi, mais pas tjs protection max, limite la visibilité

Hauteur d'une zone dangereuse a
Hauteur d'une structure de protection b
Distance horizontale jusqu'au danger c

Zone dangereuse (point le plus proche) 1
Plan de référence 2
Structure de protection 3

Distance de sécurité selon iso 13857 :
Tableau risque faible s31, cours5, risque élevé s32, cours5



Bonnes pratiques : protecteurs fixés solidement, protègent des éjections, émanations, protecteur mobile, si défaillance d'un élément, doit empêcher le démarrage

ISO 14120 – exigences :
Système fixation reste solidaire à la machine au démontage
Évite : que les protecteurs ne soient pas remis en place, qu'ils soient partiellement fixés ou mal fixé avec des fixations non adaptées

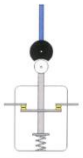
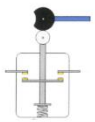
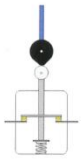
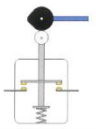
Composants de sécurité : permet d'appliquer adéquatement les principes de sécurité
Permettant des fois d'apporter plus de flexibilité que les protecteurs mécaniques

Définition : - sert à assurer une fonction de protection, - vendu indépendamment, - Dont la défaillance peut présenter un danger, - pas indispensable au fonctionnement de la machine ; peut être remplacé par des composants normaux
Liste de composants de sécurité : s38, cours 5

Certification : certains composants de sécurité apparaissent dans l'annexe 4 de la directive des machines : besoin du soutien d'un organisme notifié pour la certification

Différence protecteur/dispositif protection : barrière matérielle de protection/moyen de protection autre qu'un protecteur

Dispositif de verrouillage :
Dispositif mécanique, électrique ou autre destiné à empêcher la machine de fonctionner dans certaines conditions, par exemple si le protecteur n'est pas fermé
Fonction : si ouverture protecteur, la machine s'arrête ou la machine ne démarre pas si protecteur ouvert, exemple protecteur s45, cours5
Les dispositifs ne doivent pas être utilisés comme butée, doit être fiables

Action mécanique	Protecteur fermé	Protecteur non fermé
directe		
non directe		

Dispositif verrouillage type 1 : direct : position initiale fermé, indirect : position init ouvert
Direct : si rupture ressort, système ouvert, indirect : si rupture ressort, système fermé
Enfoncé circuit fermé-> indirect, enfoncé circuit ouvert-> direct
Exemple dispositif s52, cours5,
Force max autorisée s62, cours5

Dispositif d'interverrouillage :
Si temps de mise de à l'arrêt de la machine > au temps d'accès à la zone dangereuse, besoin du dispositif d'interverrouillage, exemple inertie machine tournante
Autorise les fonctions dangereuses que lorsqu'il est enclenché + verrouillé
Résister mécaniquement, exp empêcher l'ouverture d'un protecteur, position verrouillée surveillée par le système, conseil de verrouillage quand tension nul et déverrouillage sous tension. Exemple : clé A à utiliser pour déverrouiller clé B qui permettra d'ouvrir le protecteur

Barrières immatérielles :
Utilisé si besoin d'accéder souvent à la zone dangereuse, convient aucun risque d'éjection
Constitué d'un émetteur-récepteur, faisceau lumineux (max 10° divergence), résolution minimum 14mm
Selon ISO 13855, S=KxT + C (S=distance minimum entre barrière et phénomène dangereux K=vitesse approche m/s, T=temps d'arrêt s, C=distance sup potentiellement requise

Potentielle inhibition de la barrière, par exemple le temps qu'un matériel passe, doit être conçu pour que le personnel ne trompe pas la protection
L'inhibition doit s'arrêter direct après le passage du matériel, doit être automatique

Possible aussi de l'occultation, programmée pour que certains faisceau soient occulté
Occultation fixe :faisceau prédéterminé, occultation flottante :nombre faisceaux déterminé

Tapis sensible à la pression :

Protège d'une zone dangereuse, si une pression est appliquée, arrêt de la machine
2 types, normalement ouvert -> si pression, courant passe / normalement fermé -> si pression courant coupé

Commande bimanuelle :
Protège un opérateur. L'oblige à activer la machine avec ses deux mains
Type 1 : actionnement simultané des 2 boutons pour démarrer, si l'un est lâché-> arrêt
Type 2 : Type 1 + demande de relâcher les 2 boutons pour réarmement
Type 3 : Type 2 + délai max de <0,5 s pour enfoncer les 2 boutons, sinon tout relâcher
Type selon PL s77, cours5

Scanner de sécurité :
Scanner balayant une zone de distance de sécurité, si on entre, d'abord avertissement (zone d'alerte) puis arrêt (zone de protection)

Autre :
Interrupteur d'arrêt télescopique : interrupteur de fin de course
Bande sensible : si surpression dans bande, arrêt de l'action, exp fermeture des portes

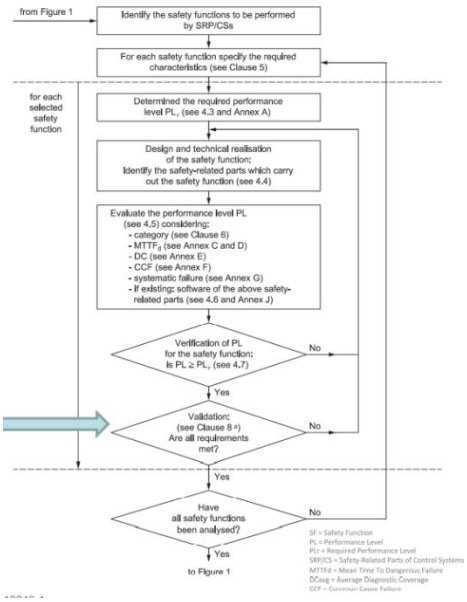
Arrêt d'urgence : ISO 13850
Catégorie 0 : Arrêt par la suppression de l'alimentation (non contrôlé)
Catégorie 1 : Arrêt contrôlé, alimentation coupé que lorsque tout est arrêté
Dispositif **supplémentaire** qui ne remplace pas les protections

Si actionné, doit resté actif tant qu'il n'est pas déverouillé
Réarmement uniquement manuel

Autre type d'arrêt s87, cours5
Couleur s88, cours5

Résumé avantage/limite/application des protecteurs s90, cours5

Cours 6 - ISO13849 – norme de type B



Traite des parties du système de commande relative à la sécurité
Applicable partout : électrique, hydraulique, pneumatique…

Probabilité de défaillance lié à : architecture, défaillances systématiques, fiabilité composants, défaillance de cause commune, couverture de diagnostique

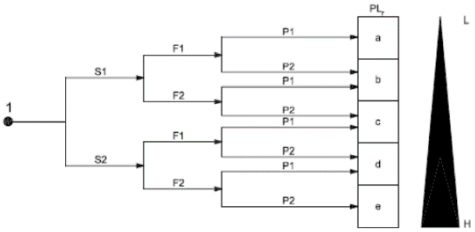
L'analyse de risque 13849 a un design itératif →→→→→

Niveau de sécurité selon domaine :

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

SRP-CS ? partie d'un système de contrôle répondant à des entrées de signaux de contrôle et qui génèrent des sortie sécurisées relatives à ces entrées

PLr ? Niveau de performance pour chaque fonction de sécurité
S1 : blessure sans complication, S2 : avec complication
F1 : rare que qqn soit exposé au danger, F2 : fréquent/continuel
P1 : si chance que danger/risque soit limité, P2 : inévitable



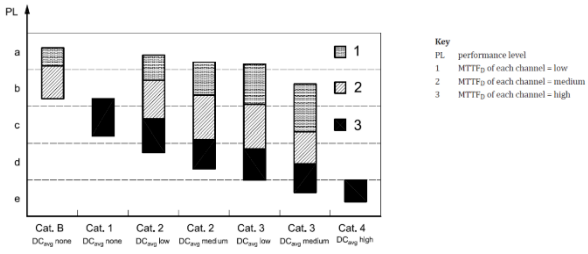
2 types de défaillance (erreur) :
Aléatoire : imprévisible, souvent due à une dégradation dans le matériel
Systématique : du à une erreur humaine/de design->erreur conception/production/installation
L'annexe G donne des mesures permettant de détecter et corriger des défaillances

Calcul du taux de défaillance PLr grâce au PFH, proba 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 $< 10^{-7}$

Etude simplifiée du niveau de PL atteint par un système :

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 covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e



Category : catégorie d'architecture
DC_{avg} : couverture de diagnostique
MTTF : temps moyen avant un problème (mean time to failure)

S'ajoute à ça les défaillances systématiques et le taux de défaillance commune β

Architecture : catégories :
B : composant logique avec un input et un output, pas de diagnostic, MTTF bas/moyen
1 : comme B avec un MTTF haut

2 : comme B avec diagnostic sur la partie logique, 100 diagnostics pour une sollicitation
Si problème, sortie OTE génère signal d'alerte(PL C ou inférieur),un état de sécurité PL D
3 : comme B mais avec système redondant DCav moyen
4 : comme 3 mais MTTFd et DCav haut

DC<60% nul, 60<DC<90% faible, 90<DC<99 moyen, 99<DC élevé
Calcul : $DC = \frac{somme\ \lambda_{dd}}{somme\ \lambda_{dd} + somme\ \lambda_{du}}$ λdd = faute dangereuse détectée, λdu= non détectée

3<MTTFd<10 ans : faible, 10<MTTFd<30 ans : moyen, 30<MTTFd<100 ans : élevé

Calcul : $MTTFd = \frac{B10d}{0.1\ x\ n_{op}}$ $avec\ n_{op} = \frac{\left(d_{op}\ x\ h_{op}\ x\ 3600\frac{s}{h}\right)}{t_{cycle}}$
dop =nbre moyen de jour d'utilisation par an
hop =nbre moyen d'heure d'utilisation par jour
tcycle = temps moyen entre le démarrage successif de 2 cycle (en s)

Calcul du β s40, cours6

Eléments en chaîne : somme des PFHd

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.			

Si on ne connait pas les PFH, utiliser ce tableau, prendre tjs le PL le plus bas (a le plus faible)

Résumé des PL a, b, c, d, e s47, cours6

IEC 62061 VS ISO 13849 Toutes deux des normes harmonisées

Conversion :

PL (ISO13849)	SIL (IEC62061)	PFH
a	Pas de correspondance	$\geq 10^{-5} \ldots < 10^{-4}$
b	1	$\geq 3x10^{-6} \ldots < 10^{-5}$
c	1	$\geq 10^{-6} \ldots < 3x10^{-6}$
d	2	$\geq 10^{-7} \ldots < 10^{-6}$
e	3	$\geq 10^{-8} \ldots < 10^{-7}$

ISO13849 suit une architecture spécifique, IEC62061 plus adapté aux systèmes complexes (pas d'architecture spécifique)
13849 et 62061 sont combinables, par exemple un sous module dans 62061 peuvent être validé par 13849

Ratio de défaillance sans impact sur le système par rapport au total des impacts :

SFF = (ΣʎS + ΣʎDD) /(ΣʎS + ΣʎD)
ʎS est le taux de défaillance de la sécurité
ʎDD est le taux de défaillance dangereuse qui est détecté par la fonction de diagnostic
ʎD est le taux de défaillance dangereuse.

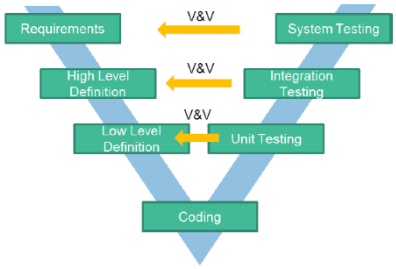
Calcul du PFH -> estimer fiabilité système
Sans redondance, égal au MTTFd
Avec redondance, à calculer avec DC et β -> calcul pour valider 62061

B estimable selon s59, cours6

Cours 8 – Processus de développement des systèmes techniques (1)

-> Gestion du risque, besoin, contrainte, maintenance, partie prenante
Cause des échecs les plus répandues : manque input utilisateur, exigences/specs incomplets, changement d'exigence et specs durant le développement

But processus : réunir les différentes équipes de développement pour réduire le risque que le projet soit affecté
But entreprise : trouver solution la plus économique et performante répondant aux besoins des différentes parties prenantes



Modèle de développement couramment utilisé
Basé sur ISO 26262

Cycle de vie système : Planification, analyse, conception, développement, vérification/validation, implémentation, maintenance

Exigences : contraintes et condition selon le besoin des utilisateurs
-> trouver un juste milieu entre contrainte, définition du problème, produit possible et acceptable

Besoin de s'assurer que le client a bien exposé son problème et ses besoins, que l'équipe d'exigence a compris le client, que l'exigence système correspond au besoin, que l'équipe d'ingénieurs a compris l'exigence du système -> supprimer toute ambiguïté
-> utiliser bon verbe, pas d'adverbe, pas de négation, chaque élément est défini précisément, exemple couleur-> donner le RAL
Les fonctions sont décrites par un verbe.

Exigence atomique (1 exigence=1 besoin), complète, consistante(pas de contradiction), non redondante, vérifiable, implémentable, non ambiguë

Vérification/Validation système : **vérification du pt de vue concepteur** : test et comparaison si résultat correspond au exigence du système
Validation du pt de vue client : le système correspond aux attentes

Type VV : informel(audit, revue de projet), test statique, dynamique, formel

Ingénierie basée sur des modèles (MBSE) : approche visuelle méthodologique des systèmes
Améliore : communication, productivité, qualité, complexité, réutilisabilité

MBSE trois piliers : méthodologie, langage, outils
trois vues : structure, comportement, exigence (et lien entre les éléments)
(Amène : création compétence des employés)

Système : 1) ensemble d'éléments interagissant ensemble selon des principes ou règles Déterminé par sa frontière, sa mission, ses interactions avec son environnement, ses fonctions, ses sources 2) Assemblage/collection organisée ayant une structure: forme une entité et en relation avec le milieu extérieur pour remplir une ou plusieurs fonctions

Un système répond à une finalité et un environnement : IN : entrées, exigences/contraintes/ressources, OUT : sortie
(exp freinage IN Force, vitesse, élec, OUT : press.frein)

Exigences : 1)fonctionnelle 2)de performance 3)opérationnelle

Black-box : système vu de l'extérieur, -> système et environnement définissable
A définir : Contexte structurel : interaction avec environnement (pas d'aspect fonctionnel)
Contexte opérationnel : cas d'utilisation (aspect focntionel)

White-box : analyse des fonctions du systèmes et les sous-systèmes
A définir : sous-systèmes, leurs interactions entre eux et avec l'extérieur, fonctions du systèmes et leur allocation avec les sous-systèmes

Système peut être considéré comme boite noire ou blanche, chaque sous système à définir
Les sous-systèmes sont des boites noires

Cours 9 – Processus de développement des systèmes techniques (2)

Décomposition système : Fonction : toutes les activités, opérations, transformations réalisées par le système (pas de lien avec la forme du système)
Fonction = processus + opérande (qui opère, agit)
Comprendre système -> identifier fonction principale (émergence)

Forme = objet + structure (différents objets mis ensemble selon une structure donnent une forme)

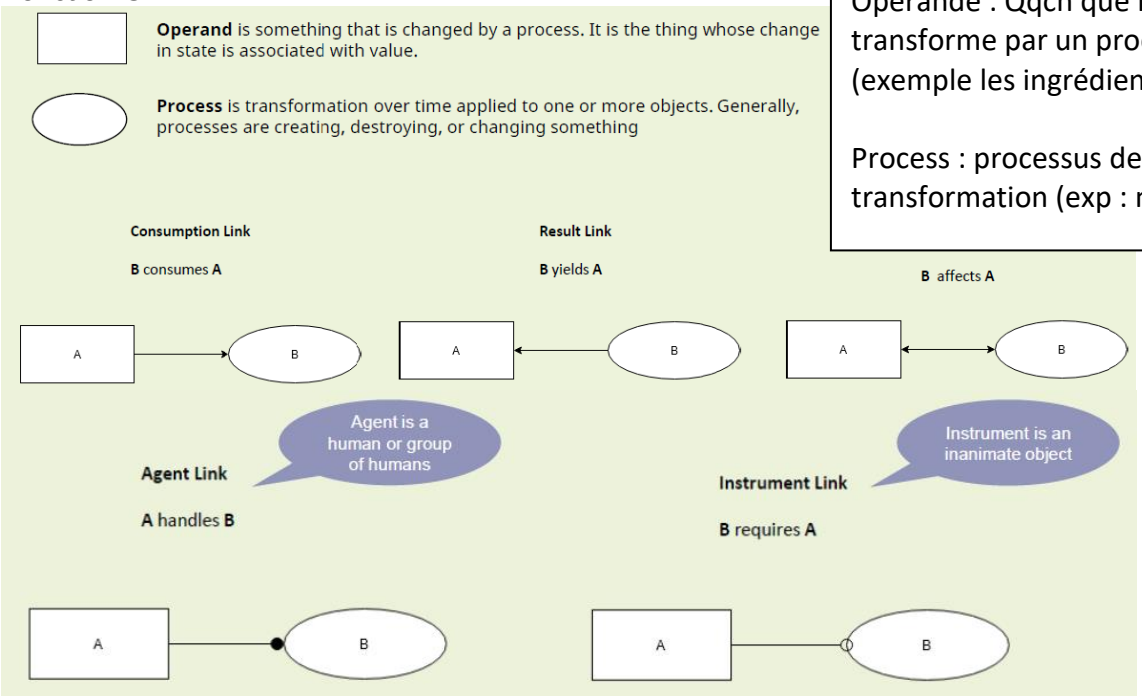
Méthode (pilier MBSE) : Différents méthode d'approche d'un problème: Mathworks (matlab), SysML, UML, OPL, ARCADIA, OPM …

Approche OPM :
L'ensemble du produit comprend le produit/système et les systèmes accompagnant
L'ensemble du produit se trouve dans un contexte d'utilisation, inclus aussi objets normalement présent mais non nécessaire au fonctionnement du système
L'ensemble du produit est généralement indépendant
Le produit/système interagit seulement avec les éléments dans l'ensemble du produit

Fonction OPM :

Opérande : Qqch que l'on transforme par un processus (exemple les ingrédients)

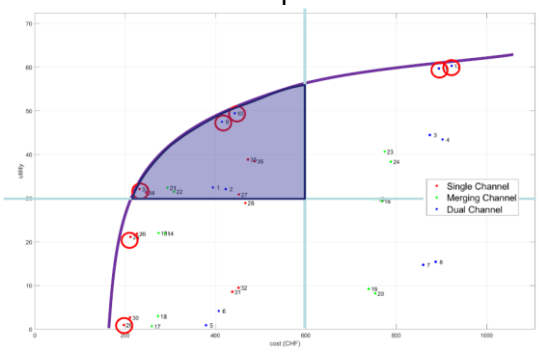
Process : processus de transformation (exp : mixer)



Safety Environnement : Simulation avec fautes : injecter des fautes dans la simulation pour voir comment se comporte le système et si besoin, l'améliorer (processus et design)
Aller en profondeur, exemple tester de court-circuiter une résistance

Robotic description
Modèle d'optimisation de développement, réduction 5 à 10x temps de développement

Configuration management
Team techinque + business travaillent en même temps -> par simulation, trouver meilleure solution entre technique et côté financier



Cours 11 – Fiabilité des systèmes techniques, niveau composant

Fiabilité : étude des défaillances d'un système, système fiable si la probabilité de remplir sa mission sur une durée donné correspond au cahier des charges

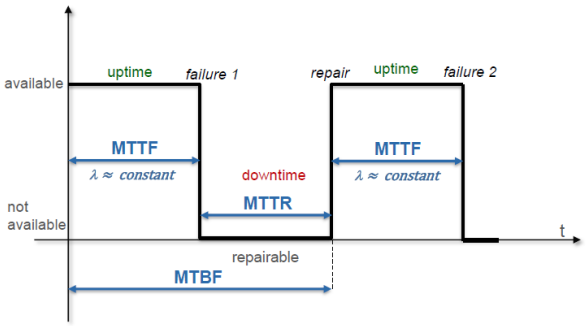
Durabilité : aptitude à répondre à un besoin durant un certain espace-temps

Hazard rate (hasard): $H = \frac{n_c}{N}$ ou $H(\Delta t) = \frac{\Delta n_c}{\Delta t * n_s}$ $avec\ N = n_c + n_s$ nc = pièces cassées, ns = pièce survie, N = nombre de pièces

Probabilité de défaillance : $F(t) = \frac{n_c(t)}{N}$ F(0)=0 et F(infini)=1, avec le temps toutes les pièces finissent par être cassées

Probabilité survie : inverse de F(t), $1 = F(t) + R(t)$, $R(t) = \frac{n_s(t)}{N}$

Espérance de vie MTTF (mean time to fail),
$MTTF = \int_0^{infini} R(t)$



MTBF = MTTF + MTTR
MTBF(mean time between failure),
MTTR(mean time to repear)

Densité de défaillance : $f(t) = \frac{dF(t)}{dt} = -\frac{dF(t)}{dt}$
F(0) = f(infini) = 0 (à la fin, tout est cassé)
Probabilité qu'une erreur arrive à un instant t (en heure !!)

Taux de défaillance : $h(t) = \frac{f(t)}{R(t)} = \lambda(t)$

	Probabilité de défaillance Probability of Failure $F(t)$	Probabilité de survie Probability of Survival $R(t)$	Densité de défaillance Hazard Density $f(t)$	Taux de défaillance Failure Rate $h(t) = \lambda(t)$
$F(t)$		$1 - R(t)$	$\int_0^t f(\tau)d\tau$	$1 - e^{\left(-\int_0^t h(\tau)d\tau\right)}$
$R(t)$	$1 - F(t)$		$\int_t^\infty f(\tau)d\tau$	$e^{\left(-\int_0^t h(\tau)d\tau\right)}$
$f(t)$	$\frac{d\,F(t)}{dt}$	$-\frac{d\,R(t)}{dt}$		$h(t) * e^{\left(-\int_0^t h(\tau)d\tau\right)}$
$h(t) = \lambda(t)$	$\frac{1}{1-F(t)} * \frac{d\,F(t)}{dt}$	$-\frac{1}{R(t)} * \frac{d\,R(t)}{dt}$	$\frac{f(t)}{\int_t^\infty f(\tau)d\tau}$	

Unité : pour les erreur, unité très répandue : 1 FIT = 10^{-9} /h

Courbe baignoire, très répandue dans l'ingénieurie :
Erreur de Rodage (diminue) – erreur aléatoire (cte) – vieillesse (erreur augmente, croit continuellement avec le temps)
-> jeunesse (early life) – utile (useful life) – vieillissement (wearout life)

Répartition de vie : décrit distribution statistiques utilisées en fiabilité et analyse de vie
Distribution décrite par f(t)

5 types : linéaire : s22 cours 11
Rectangulaire : s23, cours 11
Exponentielle : s25, cours 11
Exponentielle : décalée s28, cours 11
Weibull : s29, cours 11
Normale (gauss) : s31, cours 11

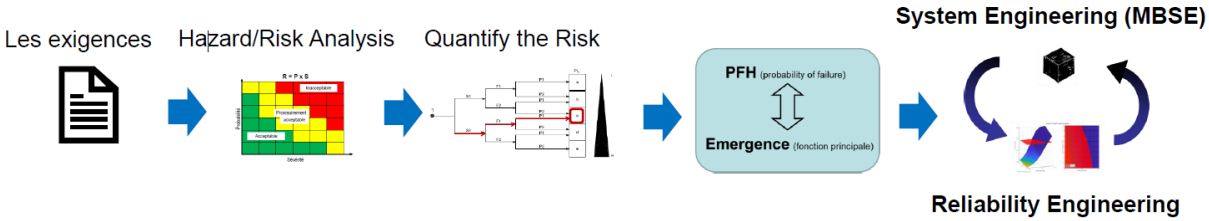
Cours 12 – Fiabilité des systèmes techniques, niveau systèmes

RAMS : Reliability (fiabilité) – Safety (sécurité)– Availbility(A) (disponibilité) – Maintenabilité

Reliability (MTTF) et Safety -> au moment du defaut
Availbility et Maintenabilité (MTTR) -> au moment de la réapration

$$A = \frac{MTTF}{MTTF + MTTR} = f(\lambda, \mu)$$

Développement système : fil rouge

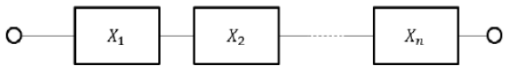


Analyse de fiabilité niveau système

Reliability block diagramm RBD :
Fonctionne comme un interrupteur : ouvert : système en faute, fermé : système opérationnel

Deux possibilité : success tree (STA), fault tree (FTA) FTA = NON(STA)
But : traverser la chaine de bloc, si un bloc ouvert, toute la chaine est interrompue

Série :

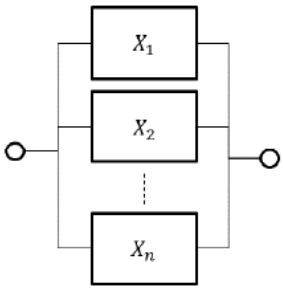


$$R_s = R(X_1 \cap X_2 \cap \ldots \cap X_n) \qquad Rs = \prod_{i=1}^{n} Ri$$

Fs = 1-Rs

Rs=R1*R2*R3*… avec X1=R1, X2=R2, …

Parallèle :



$$F_s = F(X_1 \cap X_2 \cap \ldots \cap X_n) \qquad Fs = \prod_{i=1}^{n} Fi$$

Rs =1-Fs

$$Rs = 1 - Fs = 1 - \prod_{i=1}^{n} Fi = 1 - \prod_{i=1}^{n} (1 - Ri)$$

R=1-Fs=1 - [(1-R1)* (1-R2)* (1-R3)*…]
Avec 1-R1 = X1, 1-R2=X2, …

$$Rs = \prod_{i=1}^{n} Ri = \prod_{i=1}^{n} e^{-\lambda t} = e^{-\lambda_1 t} * e^{-\lambda_1 t} * \ldots * e^{-\lambda_n t} = e^{-(\lambda_1+\lambda_2+\cdots+\lambda_n)t} = e^{-(\sum_{i=1}^{n} \lambda_i)\, t}$$

Calcul du MTTF : $MTTF = \int_0^{infini} R_s \, dt = \frac{1}{\lambda_{sys}}$ (à calculer avec $e^{\lambda nt}$)

Ingénierie système, prendre en compte l'environnement -> analyse Life Stress Models
Impact le system ingineering (MBSE)

Température : Elle a un impact clair sur les composants, par exemple ceux en silicium

Se présente sous la forme d'un facteur accélération AF

$$AF = \frac{R(Ts)}{R(To)} = e^{\frac{Ea}{kb}\cdot\left(\frac{1}{To}-\frac{1}{Ts}\right)} \qquad \lambda_s = \lambda_o \cdot AF \qquad MTTF = \frac{1}{\lambda_s}$$

AF	Acceleration Factor
Ea	Activation Energy (eV)
AF	Boltzmann's constant $(8.62 \cdot 10^{-5} eV/K)$
To	Temperature d'opération normale (Kelvin)
Ts	Temperature de stress (Kelvin)

Impact sur le MTTF : ----------→

Règles:

$Ts < To \rightarrow AF \downarrow \rightarrow \lambda_s \downarrow \rightarrow MTTF \uparrow$

$Ts = To \rightarrow AF = 1 \rightarrow \lambda_s = \lambda_o$

$Ts > To \rightarrow AF \uparrow \rightarrow \lambda_s \uparrow \rightarrow MTTF \downarrow$