INSA

VAL DE LOIRE

SURETE DE FONCTIONNEMENT (SDF)

Principales notions et son management

dans les entreprises et les projets

Le rôle du conseil

*

Jean-François BARBET

Année scolaire 2021-2022

SECTOR : 12 avenue du Québec B.P. 636 Villebon sur Yvette F-91965 COURTABOEUF CEDEX
Tél. (33) 1 69 59 27 27 Fax (33) 1 69 59 27 28 E-mail : sector@sector-group.net Site WEB : www.sector-group.net
S.A. au capital de 421735 Euros R.C.S. Evry B 353 762 230 SIRET 353 762 230 00038 Code APE 7112B

- SECTOR: société indépendante créée en 1990
- > 130 consultants
- Métiers
  - Maîtrise des Risques
  - Sûreté de Fonctionnement (matériel, logiciel)
  - Qualité Produit/Process
  - Ingénierie de la Maintenance/Soutien Logistique Intégré
  - Gestion des Risques Projets
  - Gestion de crise et Plans de Continuité d'Activité
  - Amélioration des performances et réduction des coûts
- Principaux secteurs d'activité : Ferroviaire, Automobile, Energie, Aéronautique -Défense,

Bureaux : Région parisienne : Courtaboeuf (91)
Bordeaux, Lyon, Marseille, Nantes, Toulouse,
MONTREAL, CASABLANCA
Tél. : (33) 1 69 59 27 27 – Fax : (33) 1 69 59 27 28
Email : sector@sector-group.net - Web site : www.sector-group.net

OBJECTIFS DE LA SDF

BESOINS DES SOCIETES MODERNES

CHOIX TECHNOLOGIQUES

RISQUES IMPORTANTS

Page 3

OBJECTIFS DE LA SDF

- **Produire de grandes quantités d'énergie concentrée**
- **Envoyer dans l'espace d'importantes charges utiles**
- **Disposer d'armements puissants**
- **Produire à cadences élevées**
- **Traiter et transmettre de grandes quantités d'informations**

Page 4

OBJECTIFS DE LA SDF

RISQUES IMPORTANTS
COMPLEXITE DES REALISATIONS
NOUVEAUTE DES TECHNOLOGIES
EXIGENCE CROISSANTE CLIENTELE

⇩

INSUFFISANCE DES REGLES
DE L'ART ET DE L'EXPERIENCE

⇩

CRAINTES

Page 5

OBJECTIFS DE LA SDF

Jusqu'à une période relativement récente (vers 1960) :

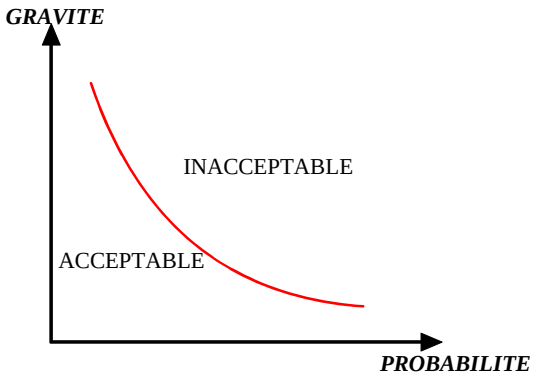
- Techniques classiques
- Evolution lente de la conception
- Effet des défaillances limité (réaction clientèle/concurrence)
  - Savoir faire de l'artisanat
  - Règles de l 'art
  - Réglementation
  - Sur-qualité en général

Et toujours à présent dans une certaine mesure !

Page 6

OBJECTIFS DE LA SDF

OBJECTIFS DE RISQUES



Page 7

OBJECTIFS DE LA SDF

- **ATTENTION**

PROBABILITE / **OBJECTIVITE**

GRAVITE / **SUBJECTIVITE**

FACTEUR D 'AVERSION

Page 8

sector

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

OBJECTIFS DE LA SDF

EXEMPLE

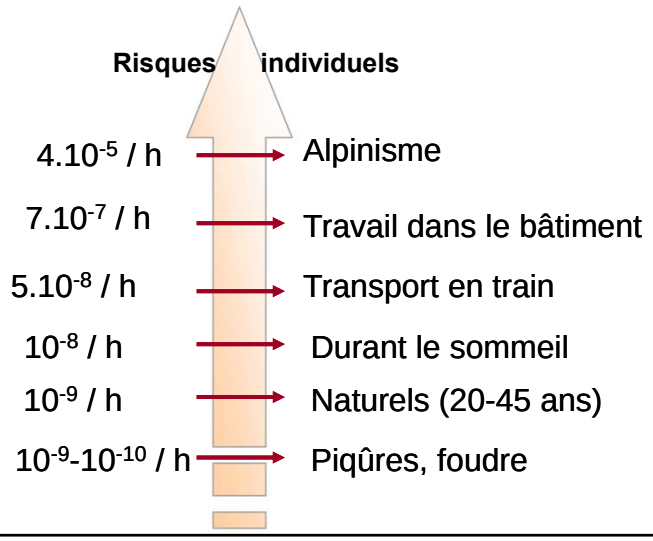
PROBABILITES / CONSEQUENCES	10^{-3} /h FREQUENT OU PEU FREQUENT	10^{-5} /h RARE	10^{-7} /h EXTREMEMENT RARE	10^{-9} /h EXTREMEMENT IMPROBABLE
MINEURES				
SIGNIFICATIVES				
CRITIQUES				
CATASTROPHIQUES				

Page 9

sector

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

OBJECTIFS DE LA SDF



Page 10

OBJECTIFS DE LA SDF

Que serait votre vie quotidienne si on se contentait d'une fiabilité de 99,9% ?

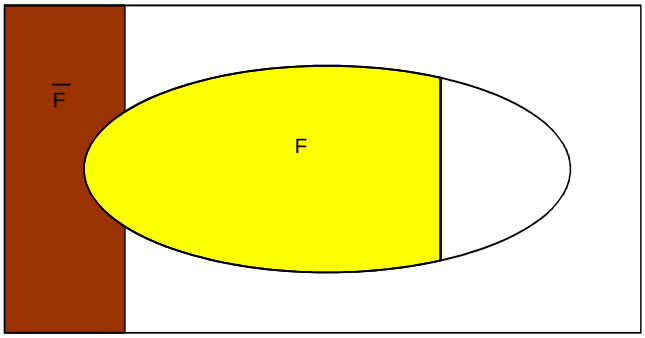
- **Chaque mois l 'eau du robinet ne serait pas potable pendant 45 minutes**
- **Chaque heure 15 000 chèques seraient débités sur de mauvais comptes**

Page 11

OBJECTIFS DE LA SDF

F = DOMAINE DE FONCTIONNEMENT

$\overline{F}$ = DOMAINE DE DYSFONCTIONNEMENT

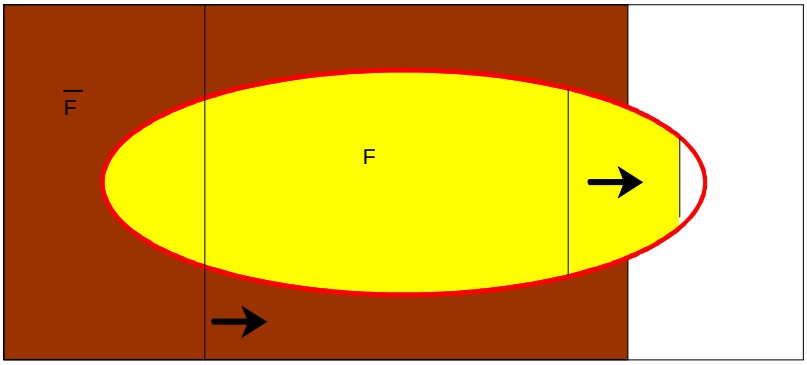


Page 12

OBJECTIFS DE LA SDF

F = DOMAINE DE FONCTIONNEMENT

$\bar{F}$ = DOMAINE DE DYSFONCTIONNEMENT



Page 13

OBJECTIFS DE LA SDF

SÛRETE DE FONCTIONNEMENT
(à partir des années 90) :
2 VOLETS

ATTEINDRE
LA MAITRISE DES RISQUES :
PERFORMANCE
(comme une autre)

APPLIQUER
UNE DEMARCHE

CONSEQUENCES ➔ ETRE EN MESURE DE FOURNIR LA PREUVE

« Dossier justificatif »

Page 14

OBJECTIFS DE LA SDF

• BESOIN POUR UNE CONFIANCE

NIVEAU A EVALUER

• NIVEAU DE CONFIANCE DANS

LA SATISFACTION DU BESOIN

= *FOURNITURE DE LA PREUVE*

Page 15

OBJECTIFS DE LA SDF

◆ **UNE DEMARCHE : - GLOBALE**

- RIGOUREUSE

- TRACEE

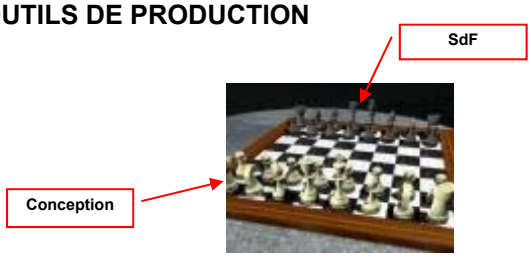
Page 16

OBJECTIFS DE LA SDF

- **UNE DEMARCHE DUALE DU PROCESSUS DE CONCEPTION**

  - PRODUIT

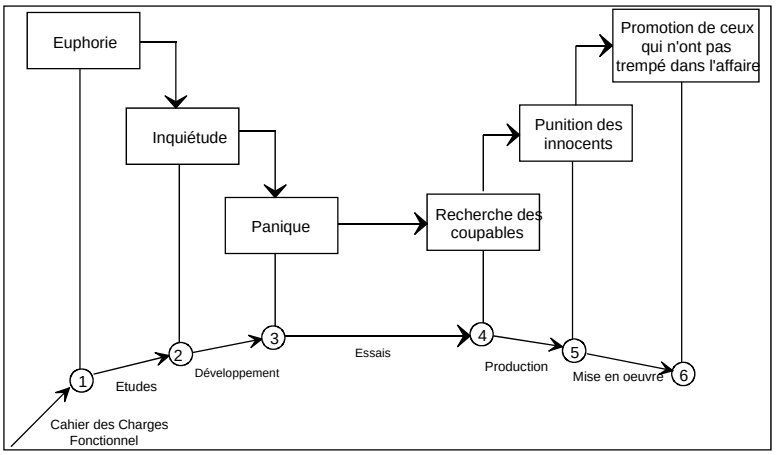
  - OUTILS DE PRODUCTION



Page 17

CONCEPTS - DEFINITIONS

PLAN DE DEVELOPPEMENT DE PROJET



Page 18

CONCEPTS - DEFINITIONS

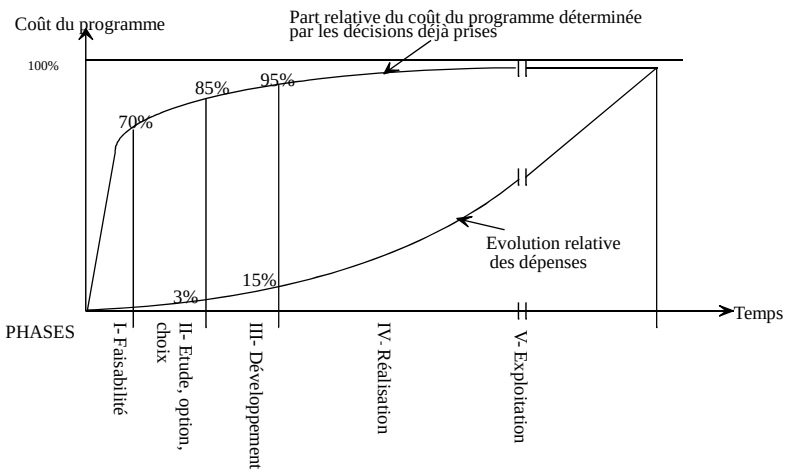
Présence de la Sûreté de Fonctionnement dans toutes les phases du projet

- Avance de phase
- Expression du besoin client
- Conception
- Développement
- Qualification - Expérimentation
- Production
- Utilisation
- Entretien – Après-vente (Maintenance)
- Fin de vie - Recyclage

Page 19

CONCEPTS - DEFINITIONS

ENGAGEMENT DES COUTS



Page 20

CONCEPTS - DEFINITIONS

- **DU SYSTEME**

AU COMPOSANT

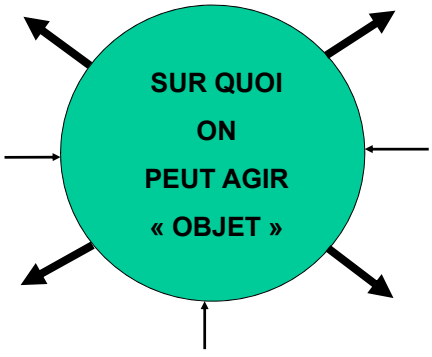
- **DU CONSTRUCTEUR-MAITRE D 'OUVRAGE (ŒUVRE)**

A L 'EQUIPEMENTIER

Page 21

CONCEPTS - DEFINITIONS

- Il est nécessaire de clairement définir le périmètre de chaque étude
- Les interfaces entre 2 ss-systèmes de niveau N gérées au niveau N+1 : garantir l'exhaustivité de l'étude des interfaces



CE QU 'IL FAUT SUBIR

« ENVIRONNEMENT »

Page 22

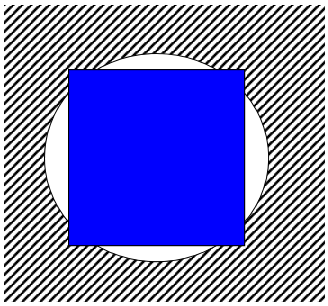
CONCEPTS - DEFINITIONS

Sûreté de Fonctionnement

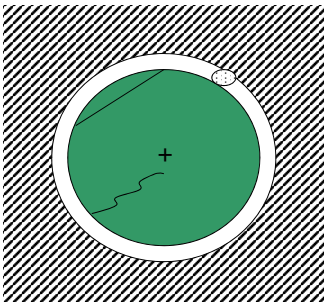
- **"Science" des défaillances : leur identification, leur description, leur évaluation, leur prévision, leur mesure et leur maîtrise.**
- **Aptitude d'une entité à remplir une ou plusieurs fonctions requises dans des conditions données. Elle comprend les concepts suivants :**
  - **Fiabilité,**
  - **Maintenabilité,**
  - **Disponibilité,**
  - **Sécurité.**

Page 23

CONCEPTS - DEFINITIONS



CONCEPTION



SURETE DE FONCTIONNEMENT (?)

Page 24

CONCEPTS - DEFINITIONS

SECURITE - INTRINSEQUE
(INOCUITE)

- DEPENDANTE DE : F
M
D

(A PRIORI NE SE NEGOCIE PAS)

CONCEPTS - DEFINITIONS

2 GRANDES CATEGORIES DE PERFORMANCES

- **CAPABILITE (PUISSANCE, CONSOMMATION, ...)**
- **SDF**

sector

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

CONCEPTS - DEFINITIONS

EXTRAIT
de l 'Allocution de Monsieur Carlos GHOSN
Directeur Général Adjoint - RENAULT
Journée Industrielle « La voiture de demain » à l 'Ecole des Mines de Paris
le 11 mars 1999

Nous plaçons la compétitivité à la base de notre croissance

Je considère que l 'innovation est une des sources de la compétitivité d 'une entreprise.

Dans l 'environnement concurrentiel qui est le nôtre, il faut à la fois être innovant pour être compétitif et l 'innovation elle-même doit répondre aux critères de compétitivité. Le challenge c 'est d 'être toujours plus innovant tout en continuant à améliorer notre compétitivité.

En qualité les exigences vis à vis des innovations sont les mêmes que pour des systèmes éprouvés. Les premiers clients ne sont pas des « dévermineurs ». Autrement dit, la phase de validation incombe pleinement au constructeur. Nous n 'avons pas le droit de mettre autre chose qu'une copie parfaite sur le marché.

Derrière la boutade, il y a un ensemble de processus dits de Sûreté de Fonctionnement, que nous mettons en place systématiquement pour les prestations innovantes et sur tous nos projets futurs[...]
l'idée est bien de fiabiliser les produits et les process nouveaux avec la même efficacité que pour l 'ensemble du véhicule, par une analyse préalable de risques.

On peut ainsi se permettre d'offrir plus d 'innovation tout en garantissant la disponibilité, la durabilité et la sécurité que le client est en droit d 'attendre.

Page 27

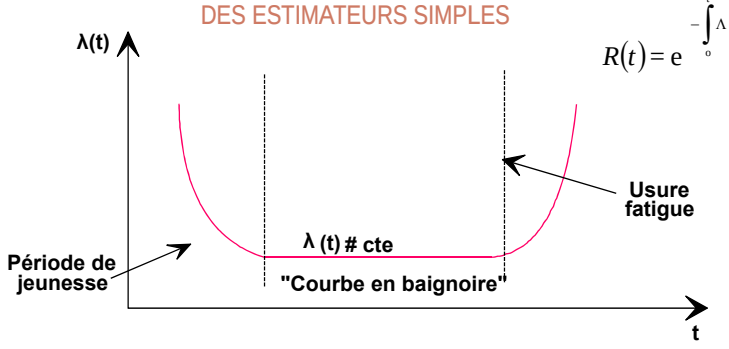
sector

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

CONCEPTS - DEFINITIONS

DES ESTIMATEURS SIMPLES

$$R(t) = e^{-\int_0^t \Lambda(u)\,du}$$



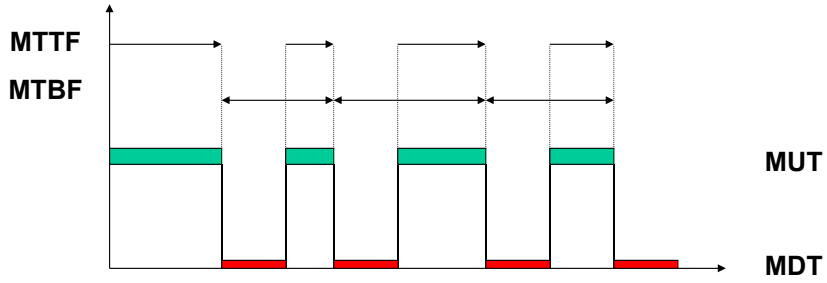
Taux de défaillance : λ # 1 / MTBF (MTTF)

λ # cte
λ . T << 1

Probabilité de défaillance : P(Bi) # λ . T

Page 28

CONCEPTS - DEFINITIONS



MTBF : Mean Time Between Failure

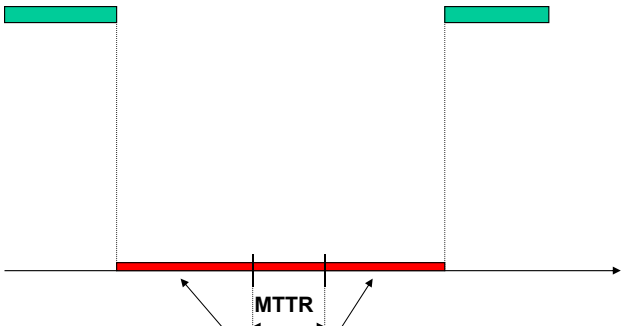
MTTF : Mean Time To Failure

MUT : Mean Up Time

MDT : Mean Down Time

Page 29

CONCEPTS - DEFINITIONS



MTTR = Mean Time To Repair

Temps « logistiques »

Page 30

CONCEPTS - DEFINITIONS

$$\text{Taux de réparation} = \mu = \frac{1}{\text{MTTR}} = \left(\frac{1}{\text{MDT}}\right)$$

$$D = \frac{MTBF}{MTBF+MTTR} \qquad \overline{D} = 1 - D = \frac{MTTR}{MTBF+MTTR}$$

Page 31

CONCEPTS - DEFINITIONS

LES DONNEES

"Do it yourself"

- Retour d'expérience
- Essais
- Méthode "Delphi"

Page 32

CONCEPTS - DEFINITIONS

LES DONNEES

"Banques"

- CNET RdF 93 rév. 02/95
- MIL HDBK 217 F notice 2
- NPRD 95
- OREDA
- EIREDA
- ...

- FIDES 2009

CONCEPTS - DEFINITIONS

Edition septembre 2010

Guide FIDES 2009

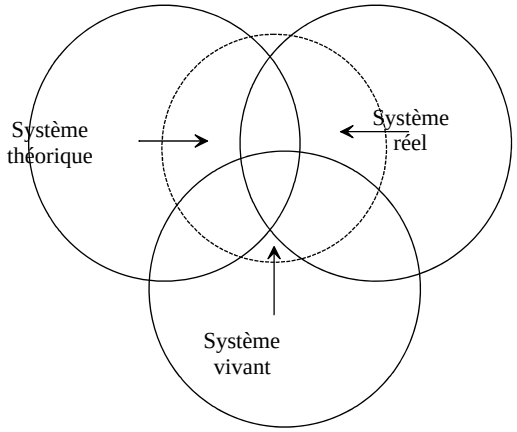
Initiative DGA avec AIRBUS, EUROCOPTER, GIAT, MBDA,THALES

- **Pour**
  - composants EEE: électronique, électrique,électromécanique
  - COTS

  Civils et milit.
- **Basé sur :**
  - REX
  - essais
  - phénomènes physiques
  - profils de mission
- **Prise en compte de:**
  - dévelop., production, exploitation, maintenance
  - fournisseurs

CONCEPTS - DEFINITIONS

La SdF et le Cycle de vie



Page 35

CONCEPTS - DEFINITIONS

La SdF et le Cycle de vie

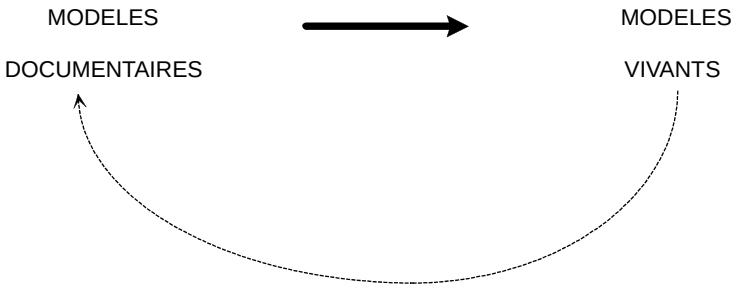
RETOUR D'EXPERIENCE

- **Données**
  - **Qualitatives**
  - **Quantitatives**
- **Validation**
  - **« Sémantique »**
  - **Statistique**

Page 36

CONCEPTS - DEFINITIONS

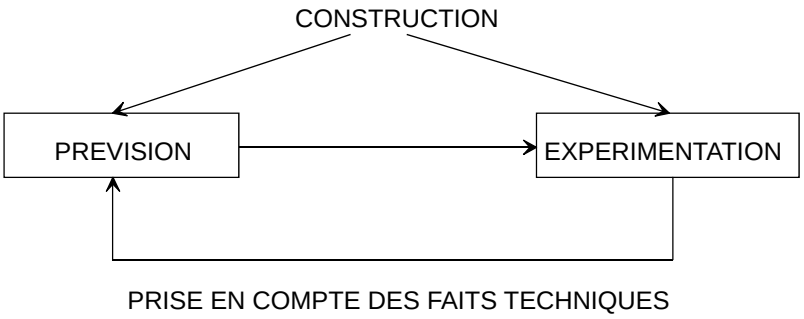
RETOUR D'EXPERIENCE



Page 37

CONCEPTS - DEFINITIONS

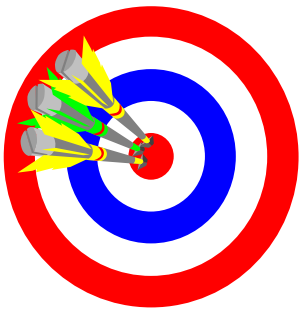
Croissance de la SdF



Page 38

DEMARCHE DE SDF

PRINCIPES DE LA METHODOLOGIE



⇒ **Identifier**

⇒ **Modéliser**

⇒ **Valoriser**

Page 39

DEMARCHE DE SDF

- **APPROCHE**
  - **INDUCTIVE/DEDUCTIVE**
  - **ITERATIVE**
- **TRACABILITE**
- **HYPOTHESES**

Page 40

DEMARCHE DE SDF

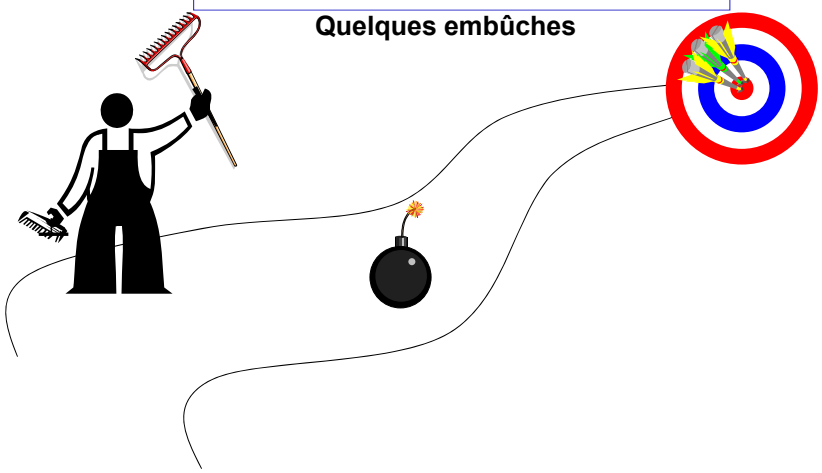
PRINCIPALES METHODES UTILISABLES

- (Analyse Fonctionnelle)
- Analyse Préliminaire des Risques (APR)
- AMDE(C)
- HAZOP(HAZard and OPerability study)
- Diagramme de fiabilité
- Arbre de Défaillance
- Graphe d 'états
- Réseau de Pétri

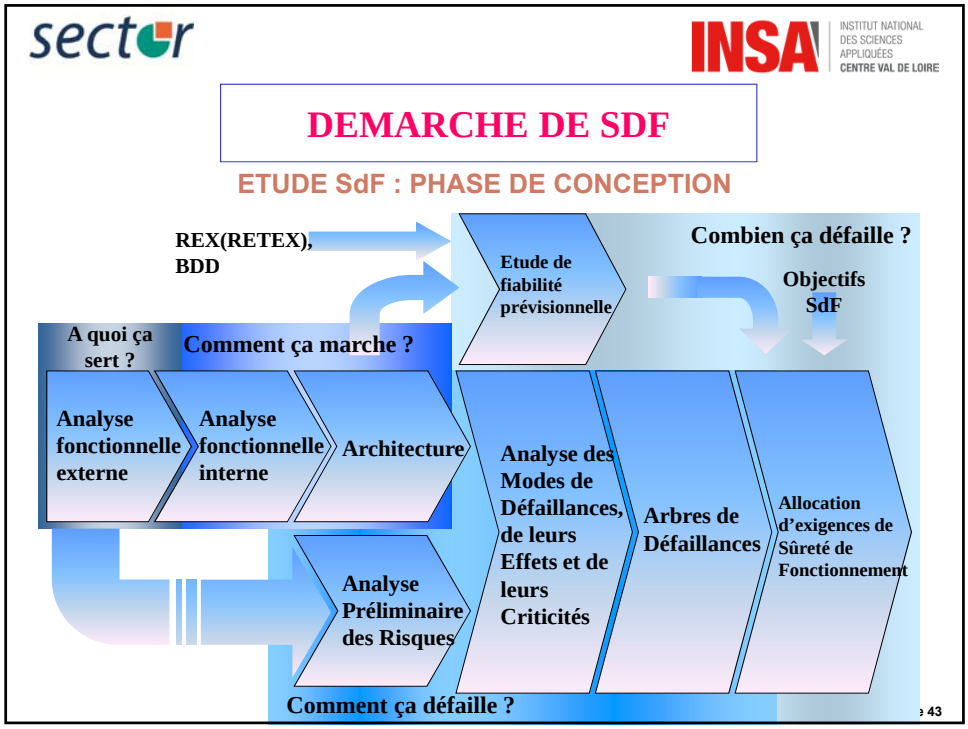
Page 41

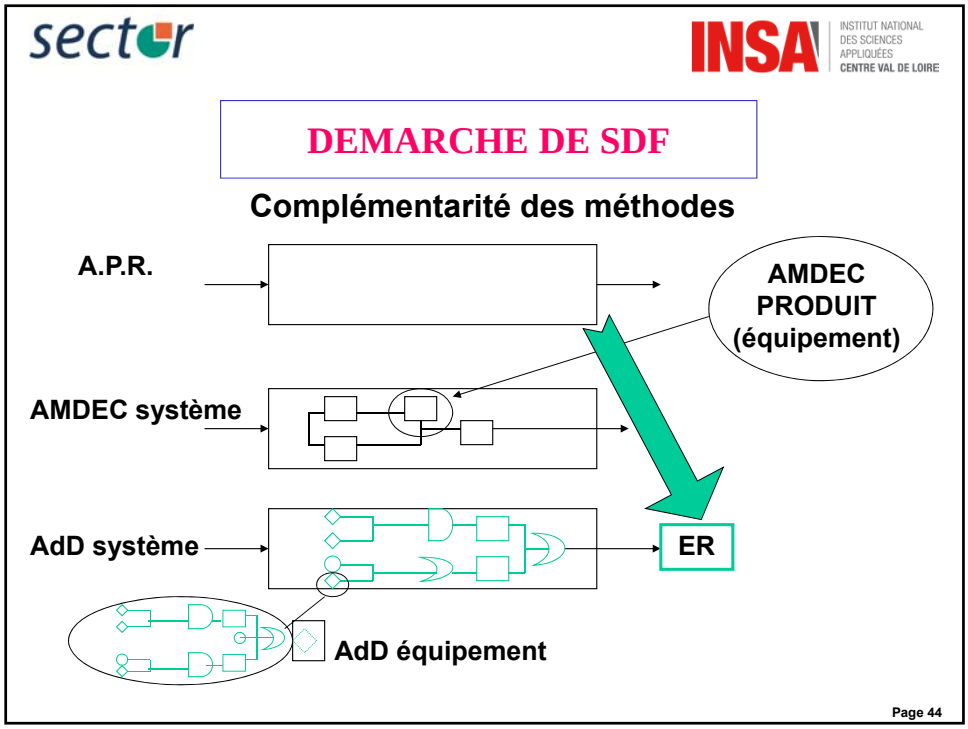
DEMARCHE DE SDF

Quelques embûches



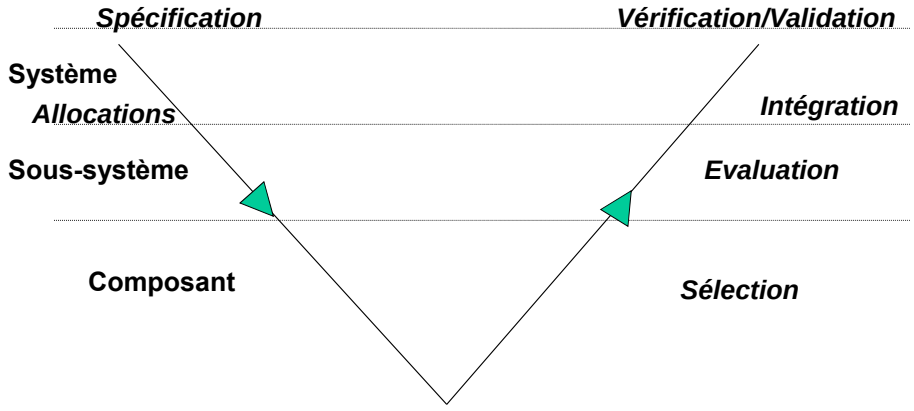
Page 42


sector
INSA
INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE
DEMARCHE DE SDF
ETUDE SdF : PHASE DE CONCEPTION
REX(RETEX), BDD
Etude de fiabilité prévisionnelle
Combien ça défaille ?
Objectifs SdF
A quoi ça sert ?
Comment ça marche ?
Analyse fonctionnelle externe
Analyse fonctionnelle interne
Architecture
Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticités
Arbres de Défaillances
Allocation d'exigences de Sûreté de Fonctionnement
Analyse Préliminaire des Risques
Comment ça défaille ?
43


sector
INSA
INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE
DEMARCHE DE SDF
Complémentarité des méthodes
A.P.R.
AMDEC PRODUIT (équipement)
AMDEC système
AdD système
ER
AdD équipement
Page 44

DEMARCHE DE SDF

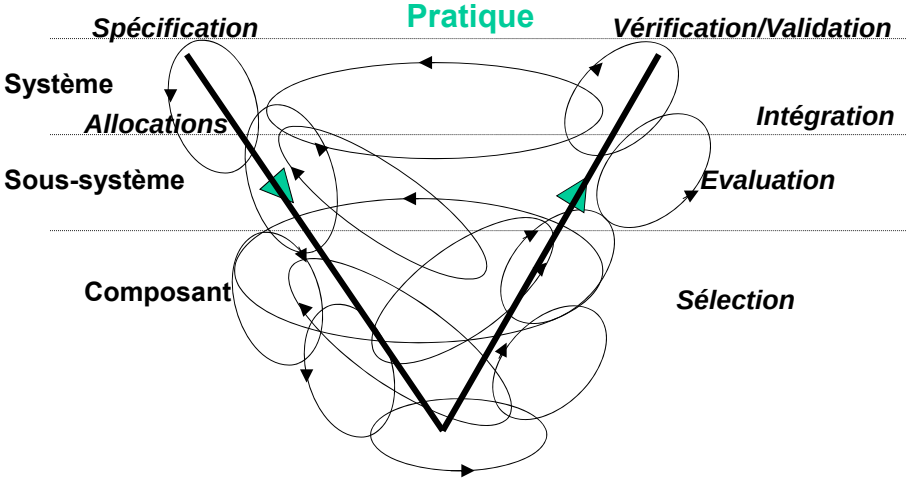
Théorie



Page 45

DEMARCHE DE SDF

Pratique



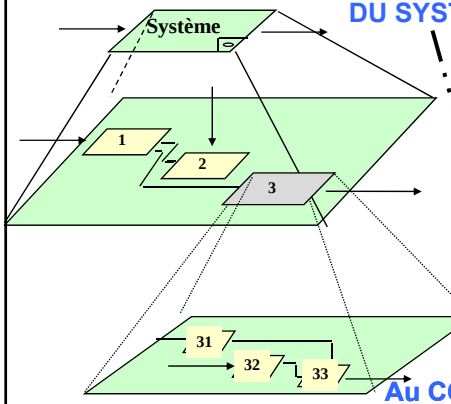
Page 46

DEMARCHE DE SDF

CONSTRUCTION DE LA SdF
PAR LES DIFFERENTS ACTEURS

DU SYSTEME

DU CONSTRUCTEUR



Au CONSTITUANT,
…A LA PIECE

A L 'EQUIPEMENTIER

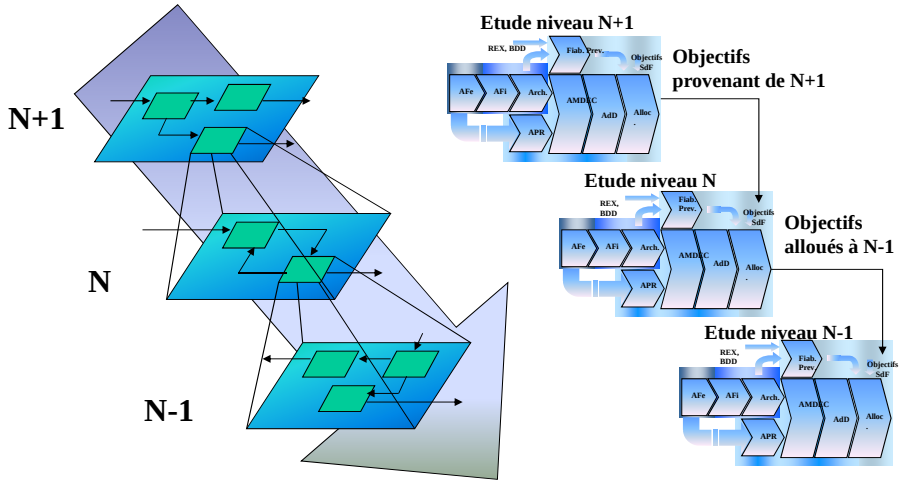
DEMARCHE DE SDF

- Pour chaque niveau :
  - ✓ on identifie les objectifs issus du niveau supérieur
  - ✓ on identifie les risques liés aux défaillances des éléments du niveau inférieur
  - ✓ on alloue des objectifs aux éléments du niveau inférieur afin de garantir la tenue des objectifs alloués au niveau étudié
  - ✓ on vérifie l'atteinte des objectifs par le niveau inférieur

sector

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

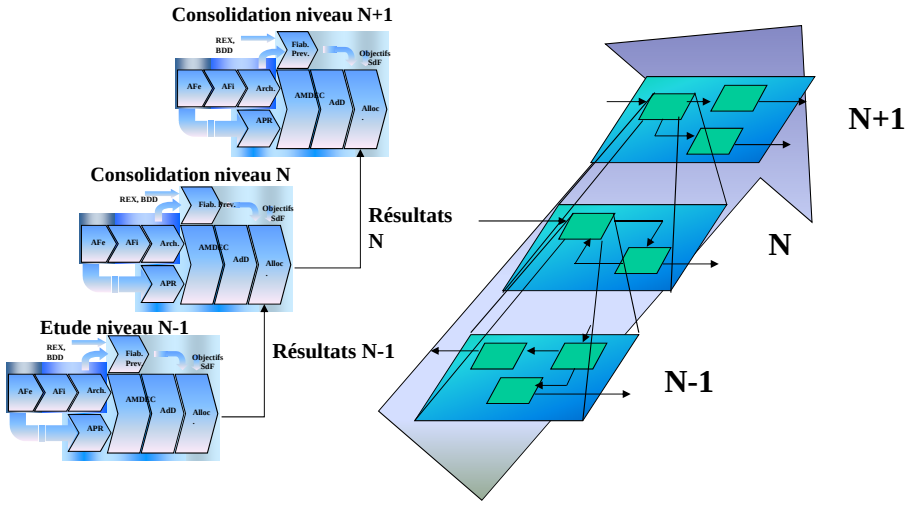
DEMARCHE DE SDF



sector

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

DEMARCHE DE SDF



DEMARCHE DE SDF

ETUDE SdF : PHASE DE CONCEPTION

Se réalise en // de la conception et :
- **Conclut la phase de conception**
- **Valide avant la réalisation de l'outil de production**

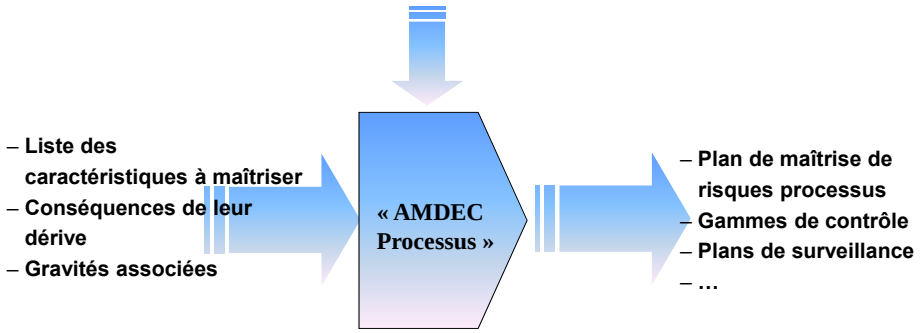
- Attendus de l'étude SdF en phase de conception :
  - Plan de maîtrise des risques de conception
  - Listes des caractéristiques du produit à maîtriser par le biais du processus, conséquences de leur dérive et gravités associées
  - Plan de validation
  - Synthèse des résultats obtenus

Page 51

DEMARCHE DE SDF

ETUDE SdF : PHASE D'INDUSTRIALISATION

– Description du processus de production



Page 52

Mise en œuvre de la SdF

via les normes de sécurité fonctionnelle

La norme CEI 61508

La norme CEI 61508 (1)

- La norme CEI 61508 présente une approche générique de toutes les activités liées au cycle de vie de sécurité de systèmes Électriques/Électroniques/Électroniques Programmables (E/E/EP) utilisés pour réaliser des fonctions de sécurité
- Dans la plupart des cas, la sécurité est obtenue néanmoins par plusieurs systèmes de diverses technologies (mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable)

La norme CEI 61508 (2)

- La stratégie de sécurité doit prendre en compte tous les éléments contribuant à la sécurité. Ainsi la CEI 61508 fournit un cadre qui s'applique à des systèmes relatifs à la sécurité basée sur d'autres technologies, puis traite spécifiquement des systèmes à base d'électronique
- Du fait de la grande variété des applications E/E/EP à des degrés de complexité très divers, la nature exacte des mesures de sécurité dépend de facteurs propres à l'application (pas de règles générales mais des méthodes d'analyse)

Page 55

Points importants de la norme CEI 61508 (1)

1. Elle concerne toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service)
2. Elle fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes relatifs à la sécurité
3. Elle définit des niveaux d'intégrité de sécurité (SIL) des systèmes E/E/EP relatifs à la sécurité
4. Elle décrit une approche basée sur l'analyse de risques pour déterminer les niveaux d'intégrité de sécurité (SIL) à atteindre pour un risque donné

Page 56

Points importants de la norme CEI 61508 (2)

5. Elle fixe des objectifs quantitatifs de défaillances dangereuses des systèmes de sécurité en fonction des niveaux d'intégrité de sécurité - SIL (Safety Integrity Level) :

Les exigences pour chaque fonction de sécurité assurée par un système E/E/EP doivent être spécifiées en termes de niveau d'intégrité et doivent indiquer si l'objectif chiffré de défaillance est, soit :

- la probabilité moyenne de défaillance dangereuse de la fonction de sécurité en cas de sollicitation, (PFDavg), pour un mode de fonctionnement à faible sollicitation (cf. Tableau 2)
- la fréquence moyenne de défaillance dangereuse de la fonction de sécurité [h^{-1}], (PFH), pour un mode de fonctionnement à sollicitation élevée ou pour un mode de fonctionnement continu (cf. Tableau 3).

Page 57

Points importants de la norme CEI 61508 (3)

Tableau 2 – Niveaux d'intégrité de sécurité – objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à faible sollicitation

Niveau d'intégrité de sécurité (SIL)	Probabilité moyenne de défaillance dangereuse en cas de sollicitation de la fonction de sécurité (PFD_{avg})
4	$\geq 10^{-5}$ à $< 10^{-4}$
3	$\geq 10^{-4}$ à $< 10^{-3}$
2	$\geq 10^{-3}$ à $< 10^{-2}$
1	$\geq 10^{-2}$ à $< 10^{-1}$

Tableau 3 – Niveaux d'intégrité de sécurité – objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à sollicitation élevée ou en mode de fonctionnement continu

Niveau d'intégrité de sécurité (SIL)	Fréquence moyenne de défaillance dangereuse de la fonction de sécurité [h^{-1}] (PFH)
4	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$

Page 58

Points importants de la norme CEI 61508 (4)

6. Elle décrit les principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/EP relatifs à la sécurité, mais n'utilise pas le concept de sécurité intrinsèque, adapté à des systèmes peu complexes dont les modes de défaillances sont connus

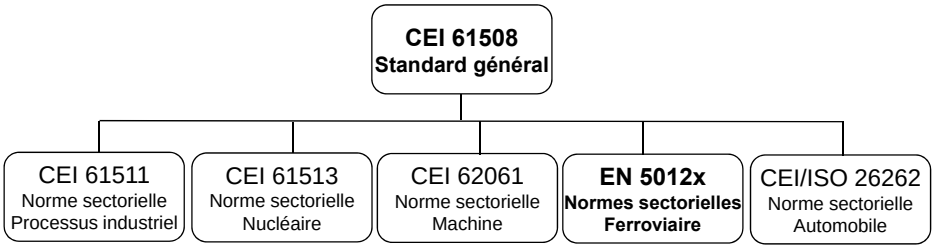
Exemples de sécurité intrinsèque dans le ferroviaire :
- **relais de signalisation**
- **TVM (Transmission Voie Machine) --> TVM 300 et TVM 430**

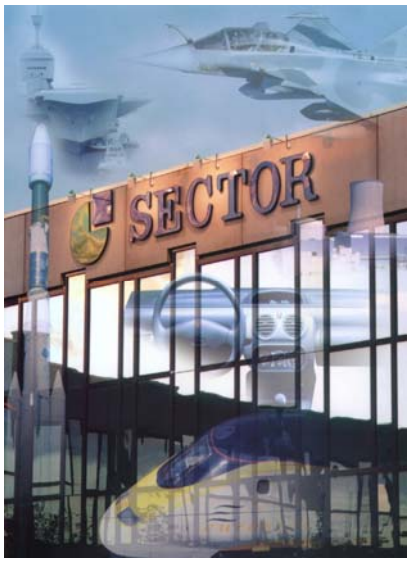
Points importants de la norme CEI 61508 (5)

Défaillances aléatoires / systématiques

- La norme distingue deux types de défaillances à maîtriser
  - Les défaillances **aléatoires** matérielles
    - Conséquence de la perte d'un composant E/E/EP
  - Les défaillances **systématiques**
    - Violation d'une exigence de sécurité par suite d'une erreur de spécification, de conception, de codage, de fabrication, dans des conditions reproductibles
- La démarche est différenciée pour les deux types de défaillances
  - Les défaillances aléatoires sont couvertes par des analyses de sécurité
  - Les défaillances systématiques sont traitées par un processus de conception rigoureux
- La norme couvre l'ensemble du cycle de vie du produit
  - Du développement jusqu'au retrait
    - Y compris l'allocation et la vérification des exigences vers l'APV, industriel, ou l'utilisateur (ex. : exigences mentionnées dans le manuel utilisateur)

Déclinaison de la norme CEI 61508





12 avenue du Québec
BP 636 Villebon sur Yvette
91965 Courtaboeuf Cedex
Phone: (33) 1 69 59 27 27
Fax: (33) 1 69 59 27 28
Email: sector@sector-group.net
Web site: www.sector-group.net

SA au capital de 421 735 €
RCS Evry B 353 762 230
SIRET 353 762 230 000 38
Code APE 7112 B