Sûreté de Fonctionnement

Ou comment s'assurer qu'un système est « sûr »

B. Monsuez
ENSTA PT

Qu'entendons nous par SdF ?

- **Le niveau de confiance** que nous pouvons avoir dans un **système**.

- Opposition entre deux grandeurs
  - Une subjective : est ce que je suis dans un véhicule « sûr » ?
  - Une objective et quantifiable : la probabilité que cet évènement se passe est de x% !

- Attention
  - Un système subjectivement sûr n'est pas un système objectivement sûr et vice versa.

Emergence de la SdF

- Apparition concomitante avec la révolution industrielle (250 ans)
  - Industrie chimique & métallurgique
  - Transports
- Puis avec le développement de la médecine
  - Apparition de la notion coût/bénéfice
  - Evaluation statistique du risque
- Et enfin avec l'automatisation
  - Automatisation & autonomie décisionnelle des systèmes

Le cadre de la SdF aujourd'hui

- Ensemble de règles métiers
  - Règles de conception
  - Règles d'exploitation
  - Règles de démantèlement
- Ensemble de normes
  - Définition des attendus en terme de conceptions, d'exploitation et de démantèlement
- Ensemble de loi
  - Définition des procédures de qualification/certification, autorisations et autres agréments

Le cadre de la SdF (suite)

- Vision « métier » des règles
  - ISO26262 dans l'automobile
  - EN50126, EN50128 EN50129 dans le ferroviaire
  - DO254, DO178 dans l'aviation
- Pratique « nationale » ou « internationale »
  - ISO, DO : normes à portée internationales
  - EN : normes européennes
- Attention
  - Une norme peut-être « internationale » mais son interprétation nationale

Le cadre de la SdF (suite)

- Multiplicité des normes applicables
  - Normes relatives à la conception
    - ISO 26262 mais EN pour les aspects électriques
  - Normes relatives à la fabrication
    - IEC pour les aspects automatisation de la fabrication, EN pour les aspects électriques, …
  - Normes relatives à l'exploitation
    - EN + Nationales

La « sûreté » en terme d'objectifs

- La question « fondamentale » est :

  How safe is safe enough ?

- Deux visions de la gestion de risque :
  - Une vision « individualiste » : le risque qu'un individu décède ou soit blessé.
  - Une vision « sociétale » : le risque pour la société suite à un dysfonctionnement

La « sûreté » en terme d'objectifs

- Plusieurs notions d'acceptation
  - Une notion « sociétale » : la perception du risque est acceptable pour les individus et la société.
  - Une notion « économique » : le risque est économiquement supportables.
  - Une notion « bénéfice » : le risque existe mais les avantages sont tels que le risque est ignoré.

La qualification/certification

- Soit déclarative
  - Le constructeur fournit l'ensemble des procédures et résultats de test pour la validation
- Soit suite à audit
  - Un audit par des experts indépendant est réalisé.
- Soit par une instruction administrative du dossier
  - Evaluation des risques sur dossier

La SdF et les Systèmes Complexes

Un système complexe critique est un système dont :

- Le niveau de sûreté et de sécurité ne peut pas être démontré uniquement par du test
- La logique de fonctionnement est délicate à appréhender
- Un dysfonctionnement peut mettre en péril la sécurité des biens et des personnes

Le Véhicule Electrique est un Système Complexe Critique

- Recours à une électronique de gestion de l'énergie
- Recours à une électronique de pilotage
- Problématique de la sûreté
  - Sûreté des batteries et de la chaîne électrotechnique
  - Sûreté des fonctions véhicules

Quelques exemples de sous-systèmes critiques

- Le freinage par récupération d'énergie
- Le différentiel électronique
- Le drive-by-wire
- Le circuit de charge

La problématique particulière des systèmes complexes critiques

Nombre de fonctions

- Chaîne de contrôle entre un ensemble de capteurs et d'actionneurs
- Problème de la ségrégation des fonctions ?
- Problème de la distribution des fonctions ?
- Problème de la gestion des modes communs
- Problème des défaillance des fonctions

La problématique particulière des systèmes complexes critiques

Nombre d'états

- Problème de l'explosion combinatoire.
  - 2 capteurs, 2 valeurs : 4 états
  - 6 capteurs, 10 valeurs : $6^{10} = 60466176$

- Problème du test exhaustif
  - Impossibilité d'énumérer l'ensemble des états

- Problème des cas de défaillance
  - Augmenter encore le nombre d'état

La problématique particulière des systèmes complexes critiques

Le comportement discret

- Passage d'un état à un autre état topologiquement différent
  - ABS : régulation de l'état « freine » à l'état « ne freine pas »
- Difficulté de mise en place de marge de sécurité
  - En mécanique : **surdimensionnement** de x% de la structure
  - En commande : prise d'une marge pour ne pas être aux frontières de stabilité
- Une ligne d'un programme code permet de passer d'un état à l'autre ?
  - Comment assurer la stabilité dans une telle situation ?

La problématique particulière des systèmes complexes critiques

Le couplage « systèmes continus » et « systèmes discret »

- Les fonctions sont « continues »
- La commande est « discrète »

Comment modéliser un système à la fois « continu » et « discret » ?

- Problématique des démonstrations mathématiques
- Cf. la tartine beurrée

La problématique particulière des systèmes complexes critiques

Le temps-réel

- Existence d'un délai de traitement
- Garantir la décision dans le temps imparti

- Temps-réel dur : action obligatoire dans le temps imparti
- Temps-réel mou : si l'action n'est pas effectuée dans le temps imparti, on passe à la suivante

La problématique particulière des systèmes complexes critiques

La gestion des défaillances

- Détecter une défaillance
- Prendre les actions nécessaires
  - Mettre le système en sécurité
  - Mettre le système dans un état où il est possible de continuer la mission

La protection contre les intrusions

- S'assurer que le code n'est pas modifié
- S'assurer qu'une attaque par saturation n'est pas possible

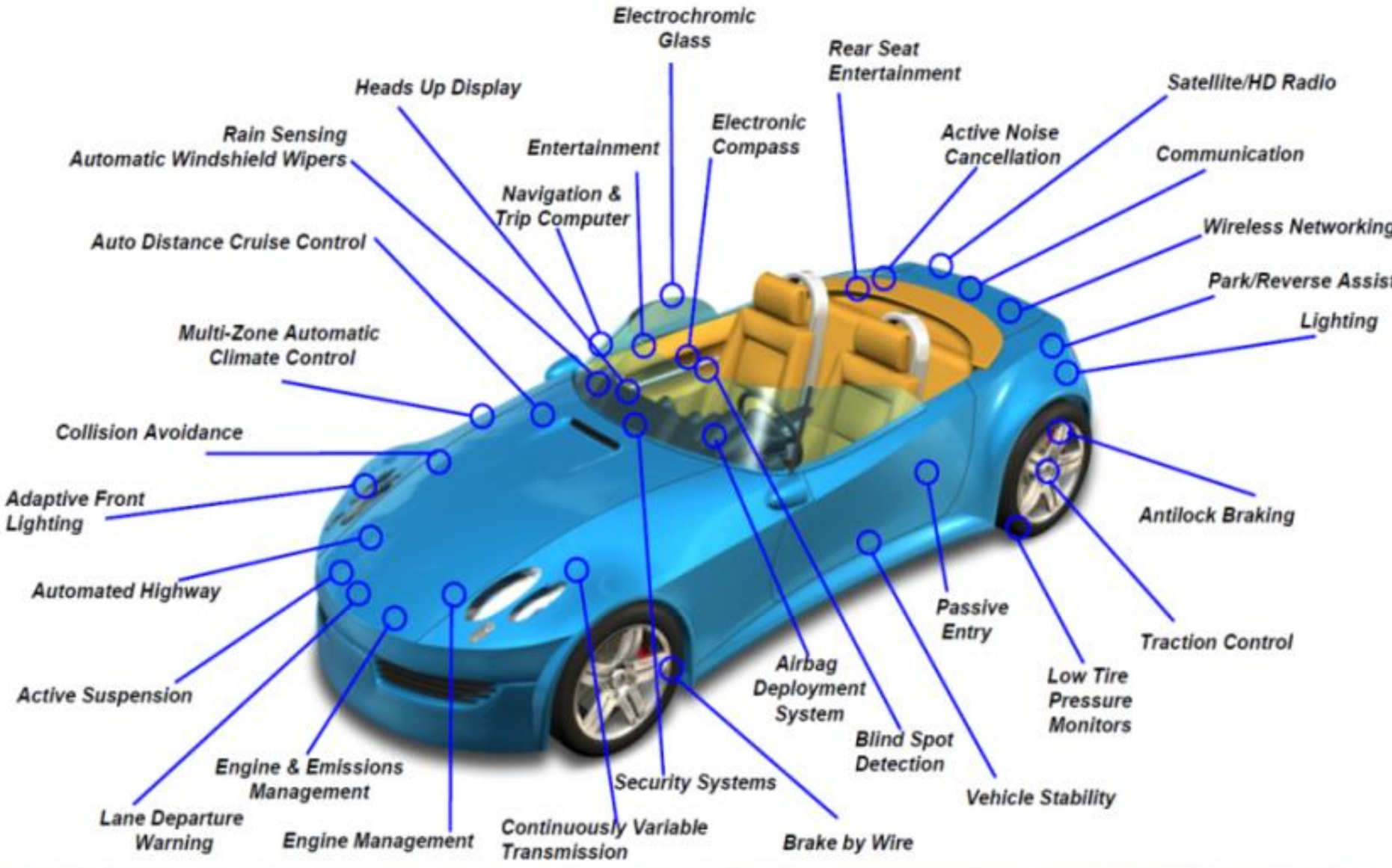
La problématique particulière des systèmes complexes critiques

La gestion des configurations

- Véhicule électrique pouvant recevoir les options suivantes
  - Batterie
  - Générateur
  - Super-Capacité
- Souhait : une seule plateforme pouvant être configurée pour les différentes options.

La SdF et l'automobile

- Problématique de l'automobile :
  - minimiser les coûts
  - grand volume
  - déclinaison des modèles
  - absence de culture de la sûreté
- Prise de conscience relativement « récente » de l'industrie automobile
  - Souhait de faire émerger une norme ad hoc « ISO 26262 »


Electrochromic Glass
Rear Seat Entertainment
Satellite/HD Radio
Heads Up Display
Electronic Compass
Active Noise Cancellation
Rain Sensing Automatic Windshield Wipers
Entertainment
Communication
Navigation & Trip Computer
Wireless Networking
Auto Distance Cruise Control
Park/Reverse Assist
Lighting
Multi-Zone Automatic Climate Control
Collision Avoidance
Adaptive Front Lighting
Antilock Braking
Automated Highway
Passive Entry
Traction Control
Airbag Deployment System
Low Tire Pressure Monitors
Active Suspension
Blind Spot Detection
Engine & Emissions Management
Vehicle Stability
Security Systems
Lane Departure Warning
Engine Management
Continuously Variable Transmission
Brake by Wire

La SdF et l'automobile

Expertise actuelle

- Aéronautique & Ferroviaire
- Solution coûteuse et onéreuse peu compatible

Idée : construire une culture de la SdF propre à l'automobile

- **Problème** : recours à des solutions peu onéreuses mais ne garantissant pas grand-chose : CAN par exemple. Emergence de nouvelles variétés **FD-CAN** & **TT-CAN**

Que recouvre la notion de système sûr ?

confiance justifiée que l'on peut placer dans un système, se caractérise par les 6 attributs suivants :

- **Availability ("readiness for correct service"),**
- **Reliability ("continuity of correct service"),**
- **Integrity ("maintaining the consistency of data"),**
- **Maintainability ("ability for a process to undergo modifications and repairs"),**
- **Safety ("absence of catastrophic consequences on the users and the environment")**
- **Security ("prevention of unauthorized disclosure of information").**

Positionnement du cours

- Sensibilisation à la culture de la SdF
  - Concepts et méthodes de prise en compte de la SdF au niveau de la conception du système
  - Concepts d'estimation et de vérification du niveau de sûreté des systèmes

- Sensibilisation aux problématiques propres de la SdF dans le Véhicule Electrique
  - Application à des exemples propres au VE.