GROUPE SERMA TECHNOLOGIES

SERMA INGENIERIE

Sûreté de Fonctionnement des Systèmes et Logiciels Critiques
État des lieux normatif et évolutions récentes

SERMA INGENIERIE

Plan

- Présentation du groupe SERMA
- Contexte du développement critique
- Pourquoi prendre en compte la SdF dans les développements
- Les normes de Sûreté de Fonctionnement
- Évolutions récentes normatives
- Conclusion

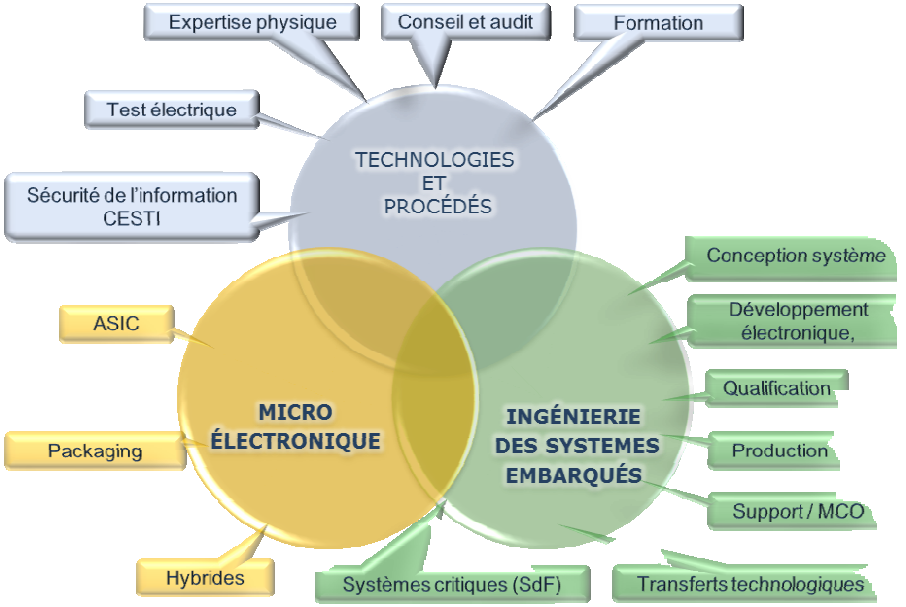
Présentation du Groupe Serma

SERMA INGENIERIE

SERMA TECHNOLOGIES | SERMA INGENIERIE | ID MOS | HCM.SYSTREL | SERMA INTERNATIONAL سارما آلدولية | SERMA GmbH

800 pers.

~80 M€ CA



Membre de 6 "Pôles de compétitivité"

- Sûreté de Fonctionnement des **systèmes critiques à forte composante logicielle**
- Maîtrise des normes CEI 61508, CEI 62304, ISO 26262, EN 50126/128/129, CEI 61513, DO 178B,…
- Des prestations adaptées : **Conseil/accompagnement - Etudes – Evaluation – Expertise – Formation**
- Des **experts reconnus** par des organismes de certification (CERTIFER, TÜV Rheinland)

Contexte du développement critique

SERMA INGENIERIE

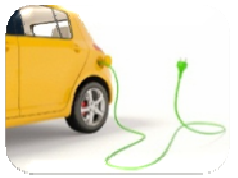
Fiabilité

Disponibilité

Médical

Aéronautique

Spatial



Automobile

L'électronique et le Logiciel au cœur des Systèmes Critiques

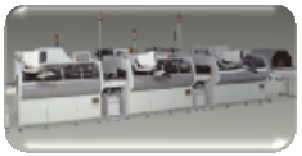
Défense

Ferroviaire

Maintenabilité

Energie

Pétrole & gaz



Industriel

Sécurité

Pourquoi prendre en compte la SdF dans les développements ?

- Pour réaliser un Produit sain c'est-à-dire fiable, maintenable et sûr de fonctionnement dans le temps
- Pour accéder à de nouveaux marchés
- Pour répondre à l'existence de marchés où la certification / évaluation de conformité est obligatoire

☛ Évaluation / Certification SdF = indicateur pour le client de la qualité/sécurité du produit

Pourquoi prendre en compte la SdF dans les développements ?
Impact des erreurs Logicielles

SERMA INGENIERIE

- Technique
  - Fonctionnel
  - Sécurité
  - Disponibilité
- Délai
  - retard pour la mise en production / exploitation
- Image :
  - Perte de confiance
  - Dégradation de l'image de la société

- Coûts :
  - Correction et mise à jour
  - Pénalités
  - Dédommagements (cas extrême : valeurs de remplacement - 100M€ pour certains satellites)

Coûts de correction des erreurs provenant

exigences et spécification :	56%
conception :	24%
codage :	10%
autres :	10%

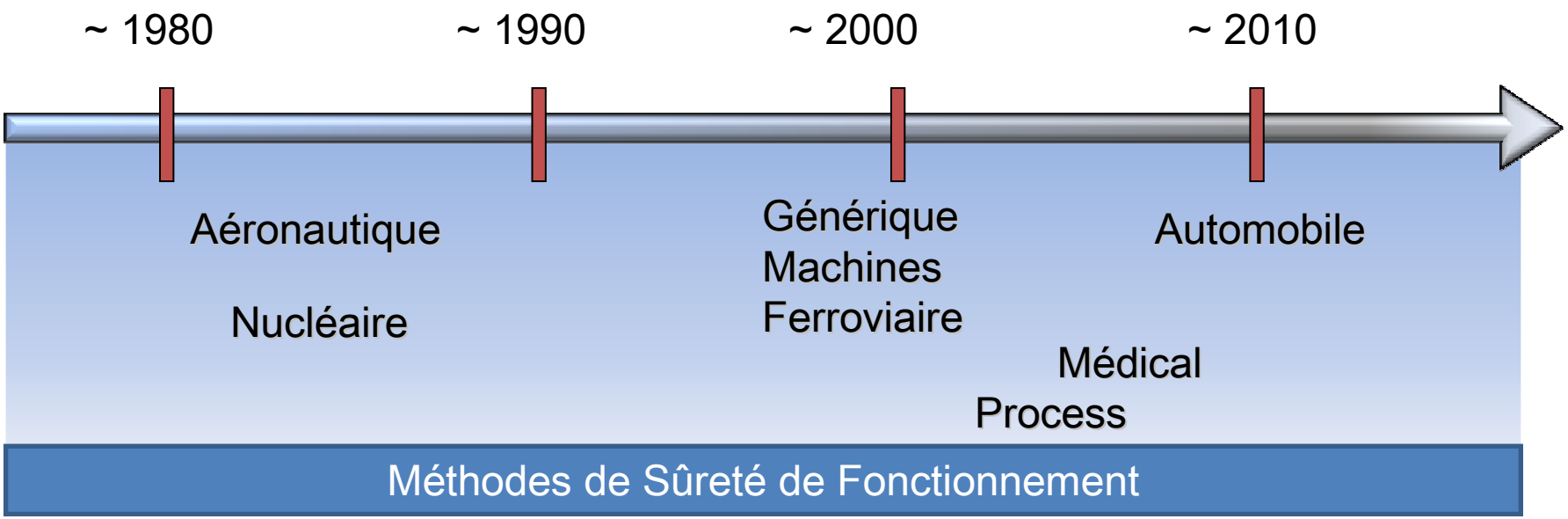
Coût de correction des défauts du logiciel

- Spécification	1
- Architecture	2
- Conception	5
- Codage	10
- Tests unitaires	15
- Tests d'intégration	22
- Tests validation / système	50
- Exploitation	100

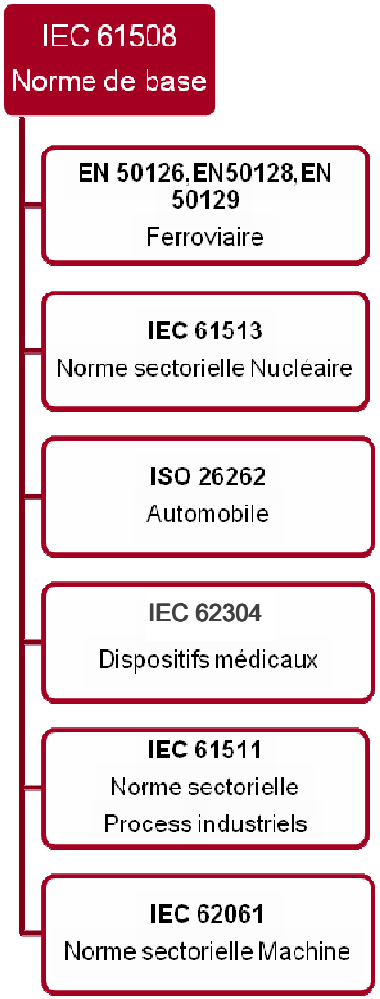
Des outils pour faciliter ces développements : Les normes

Utilisation de plus en plus importante de l'électronique et du logiciel pour assurer ou participer à des fonctions critiques pouvant impacter la sécurité

➔ Développement de référentiels intégrant la composante logicielle dans les différents secteurs industriels



La normalisation



- Norme de base : CEI 61508 (1998)
- Déploiement des normes de sécurité fonctionnelle dans les différents secteurs d'activités
- Présente une approche générique de toutes les activités liées au cycle de vie de sécurité (système, matériel et logiciel)
- Définit des niveaux SIL (Safety Integrity Level)
- D'autres normes similaires existent.
  Ex. : domaine aéronautique (DO-178)

Pratiques de développement critique : Une approche globale (1/3)

- Définir le processus de gestion de la sécurité (analyse de risque, PAQ, …) conformément à la norme suivie et l'appliquer

- Mettre en place une organisation adaptée selon le niveau de criticité (indépendance)

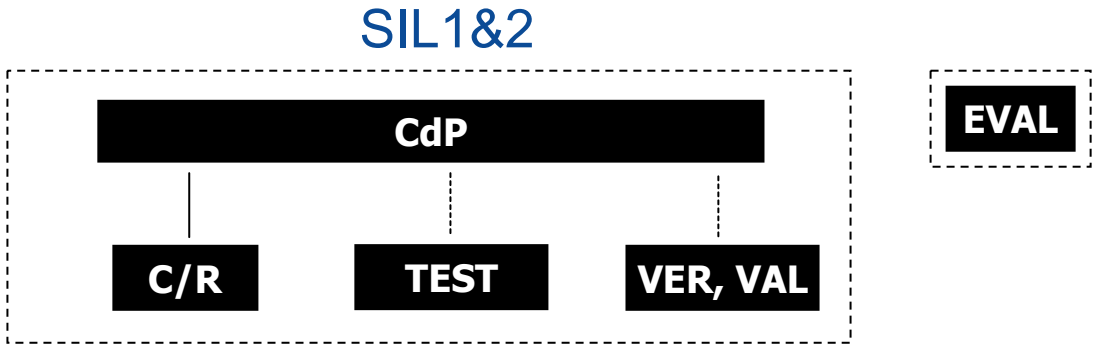


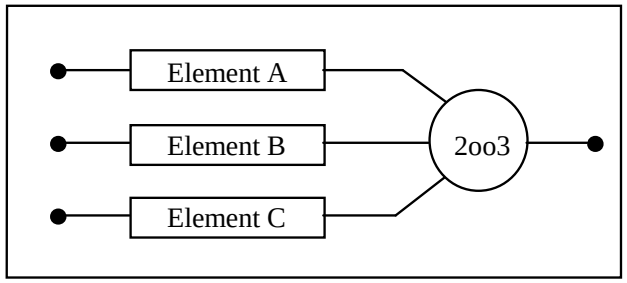
Schéma de l'EN 50128 v2011

- Démontrer la compétence du personnel

Pratiques de développement critique : Une approche globale (2/3)

- Définir le besoin sous forme d'exigence et réaliser la traçabilité des exigences (besoin Système)
- Démontrer la maîtrise et l'implémentation des exigences de sécurité (dossier de sécurité)
- Mettre en place une architecture appropriée selon la criticité (stratégie de robustesse)

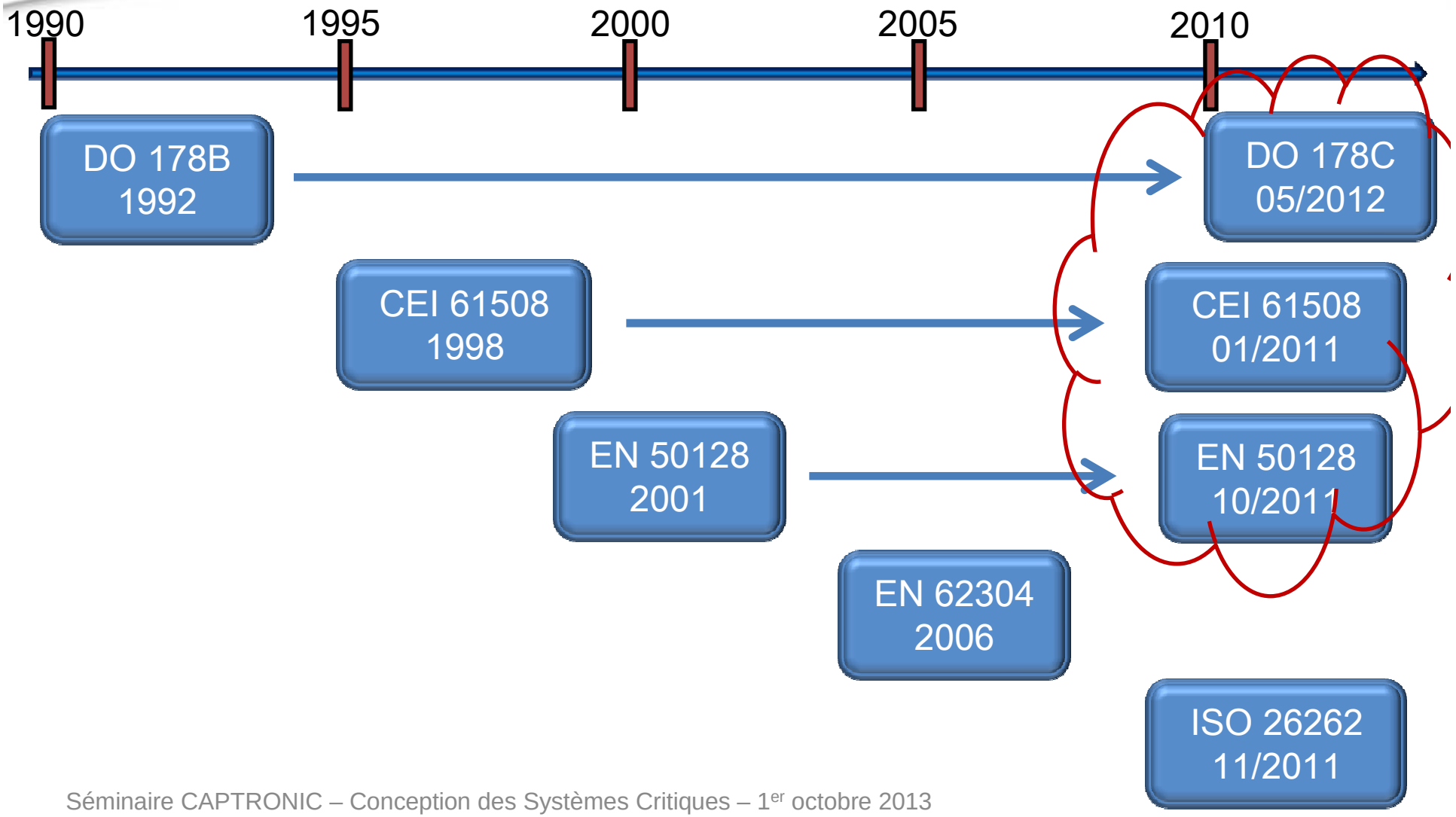
Ex : 2/3 de sécurité/disponibilité (CEI 61508 partie 6, chapitre B.2.4.5)



Pratiques de développement critique : Une approche globale (3/3)

- Mettre en place les techniques de conception adaptées (surveillance, détection, mise en position de repli…)
- Mettre en œuvre les méthodes de démonstration de la sécurité (AMDEC, Arbres de défaillances, règles de programmation, analyse statique/dynamique, …)
- Utiliser des outils qualifiés / éprouvés
- Formaliser les activités de tests (TU, TI, TV) et vérification (relecture, ….)
- …

Évolutions normatives



Évolutions normatives : Exemple de la norme EN 50128

Les évolutions de l'EN50128 v2011 (Ferroviaire) concernent notamment :

- la gestion et l'organisation du développement du logiciel
- l'indépendance des rôles avec la définition des rôles et des compétences associées
- ajout de techniques concernant le niveau SSIL0
- les activités de développement du logiciel
- le déploiement du logiciel et la maintenance des logiciels
- l'ajout d'exigences aux outils logiciels
- les systèmes configurés par des données d'application

SERMA INGENIERIE

Évolutions normatives : Exemple de la norme DO-178 C

La norme DO-178 C (aéronautique) comprend 4 suppléments techniques concernant :

- la programmation orientée objets
- le développement orienté modèles
- la place des méthodes formelles dans la certification (DO-333)
- la qualification des outils

Le document central reste inchangé sur le fond (modification éditoriale)

SERMA INGENIERIE

Conclusion

- Les normes constituent un état de l'art et une très bonne base pour le développement de systèmes critiques

- Nécessité de mise en place de processus, d'organisation et d'activités adaptés au niveau de criticité pour développer un Système critique

- Un développement critique est nécessairement plus long et plus couteux qu'un développement non contraint

SERMA INGENIERIE

Merci pour votre attention

Michel DUFRESNE

Responsable Développement activités Sûreté de Fonctionnement

Portable : +33 (0)6 72 77 59 06

Email: m.dufresne@serma.com