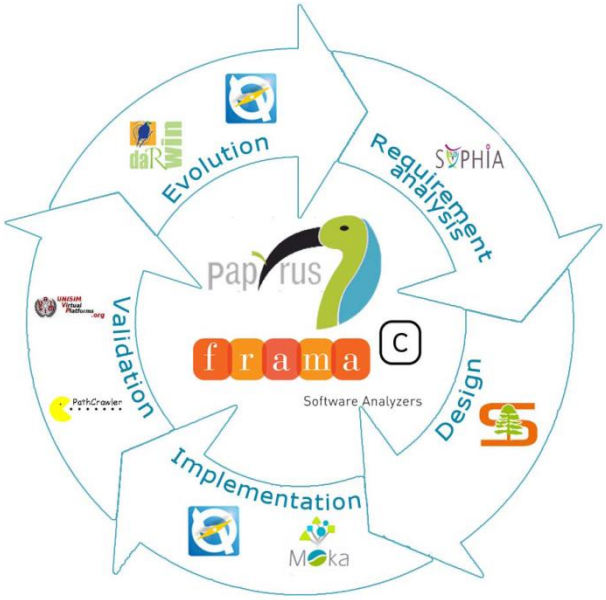


RAMS AND (CYBER)SECURITY IN MODEL-BASED FRAMEWORK

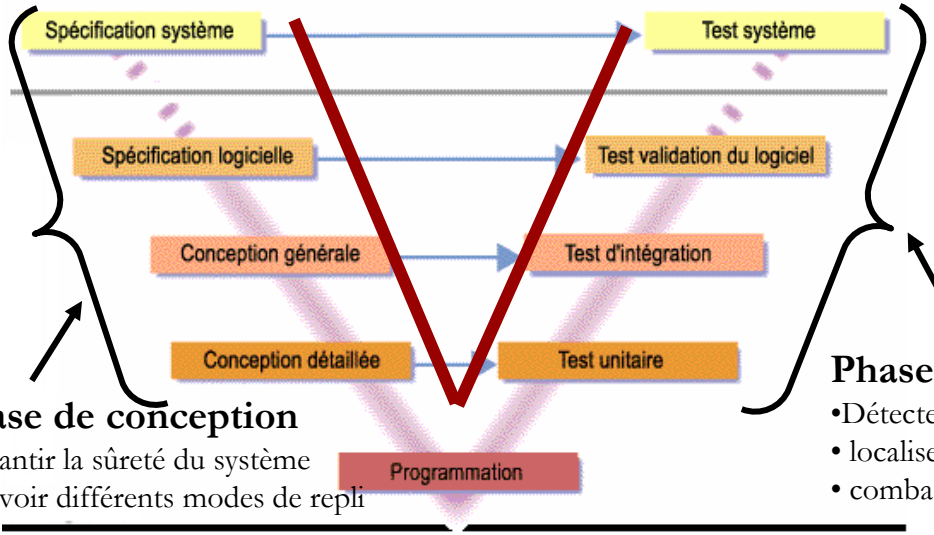
System requirements and compliance team

Morayo ADEDJOUMA

CONTEXTE ET OBJECTIFS

- **Complexité croissante et contraintes commerciales pour les CPS**

Fonctionnel, fiabilité, sûreté, coût développement et production…



Phase de conception

•Garantir la sûreté du système

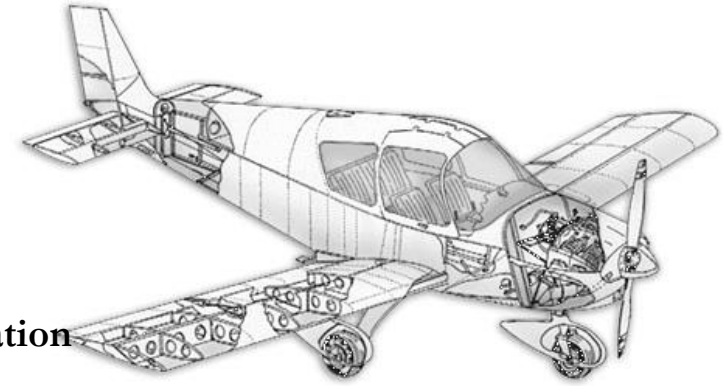
• prévoir différents modes de repli

Phase d'exploitation

•Détecter un défaut

• localiser le défaut

• combattre ses effets



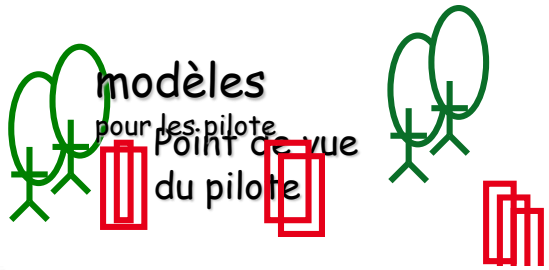
NORMES

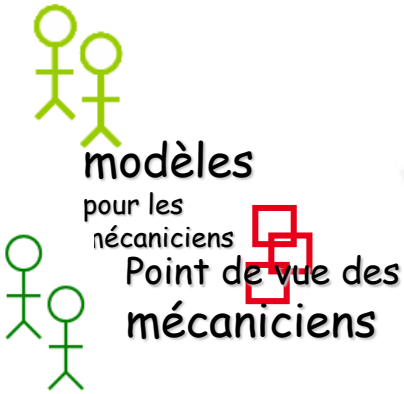
Équipes d'ingénieurs de sûreté

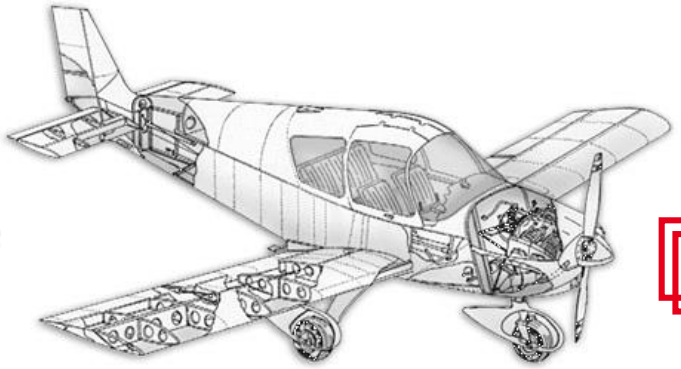
Équipes d'ingénieurs logiciels

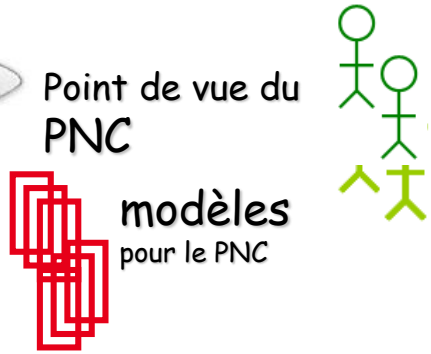
Un processus d'ingénierie basé sur les modèles

Séparations des préoccupations







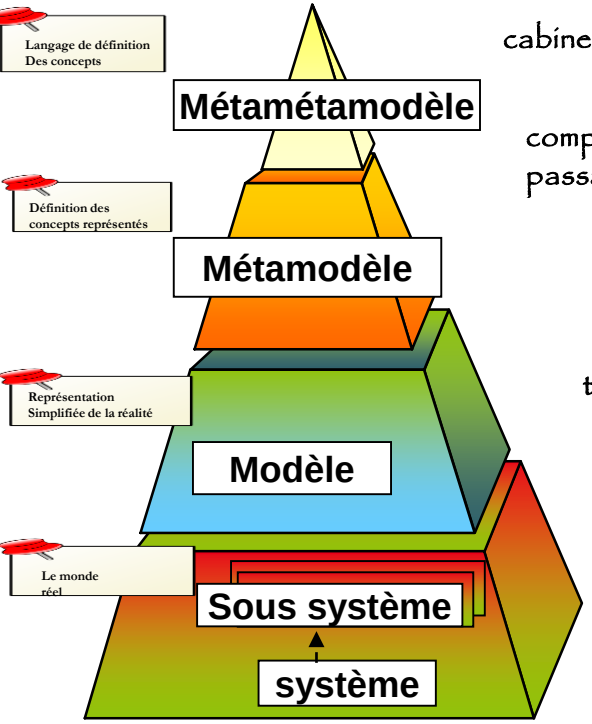


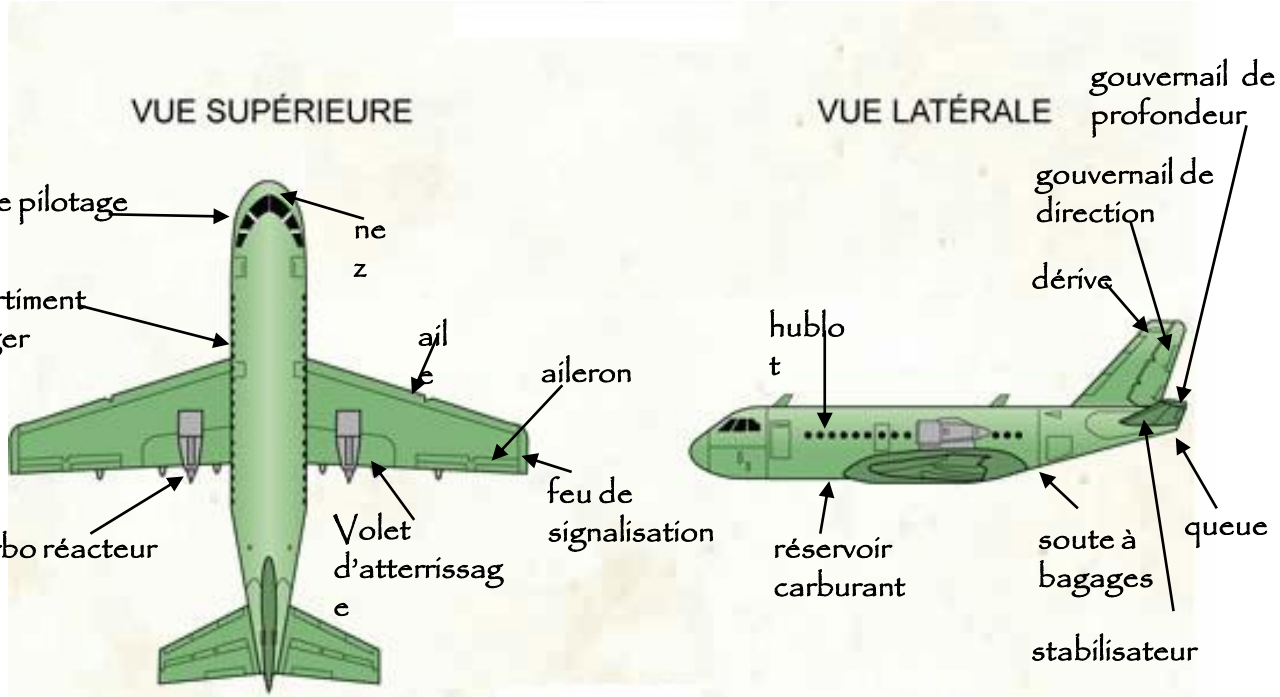
Multiples modèles d'un même système

Approche basée modèle

- Approche générative
- Conception, développement, validation
- Propriétés fonctionnelles et non fonctionnelles

Principes et concepts de l'IDM





Avion de ligne: appareil de transport aérien plus lourd que l'air, comportant des ailes et des moteurs.
Dérive: dispositif empêchant un avion de dériver.
Gouvernail de direction: appareil servant à donner la direction à l'avion.
Queue: partie arrière du fuselage allant en diminuant.
Stabilisateur: dispositif qui corrige automatiquement les erreurs et les écarts et qui assure la stabilité de l'avion.
Gouvernail de profondeur: dispositif servant à régler la hauteur de l'avion.
Compartiment passagers: section où les usagers du transport aérien voyagent.
Réservoir de carburant: contenant où est gardé le carburant en réserve.
Aileron: pièce mobile placée à l'arrière de l'aile de l'avion qui, commandée par le manche à balai, permet à l'avion de virer.
Feu de signalisation: lumière de gabarit.
Aileron compensateur: pièce auxiliaire mobile placée à l'arrière de l'aile de l'avion qui lui permet de virer.
Volet d'atterrissage: pièce mobile placée à l'arrière de l'aile de l'avion qui permet de modifier les conditions de vol.
Soute à bagages: compartiment où l'on range les bagages.
Nez: partie antérieure de l'avion.
Cabine de pilotage: cubicule réservé au maniement de l'avion.
Hublot: petite fenêtre ronde et étanche.
Turboréacteur: moteur de turbine à gaz qui fonctionne par réaction directe dans l'atmosphère.
Aile: chacun des deux plans latéraux d'un avion qui servent à le maintenir en équilibre.

Caractéristiques de la sûreté de fonctionnement

SdF: « la propriété qui permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur délivre » **[JC Laprie]**

Aspects : Évaluer la sûreté

- Disposer des performances fonctionnelles
- Ne pas engendrer de risques majeurs

Paramètres

- **FMDS : Fiabilité, Maintenabilité, Disponibilité, Sécurité-innocuité (*safety*)**
- **Testabilité, sécurité-immunité (*security*), confidentialité, intégrité, *privacy***

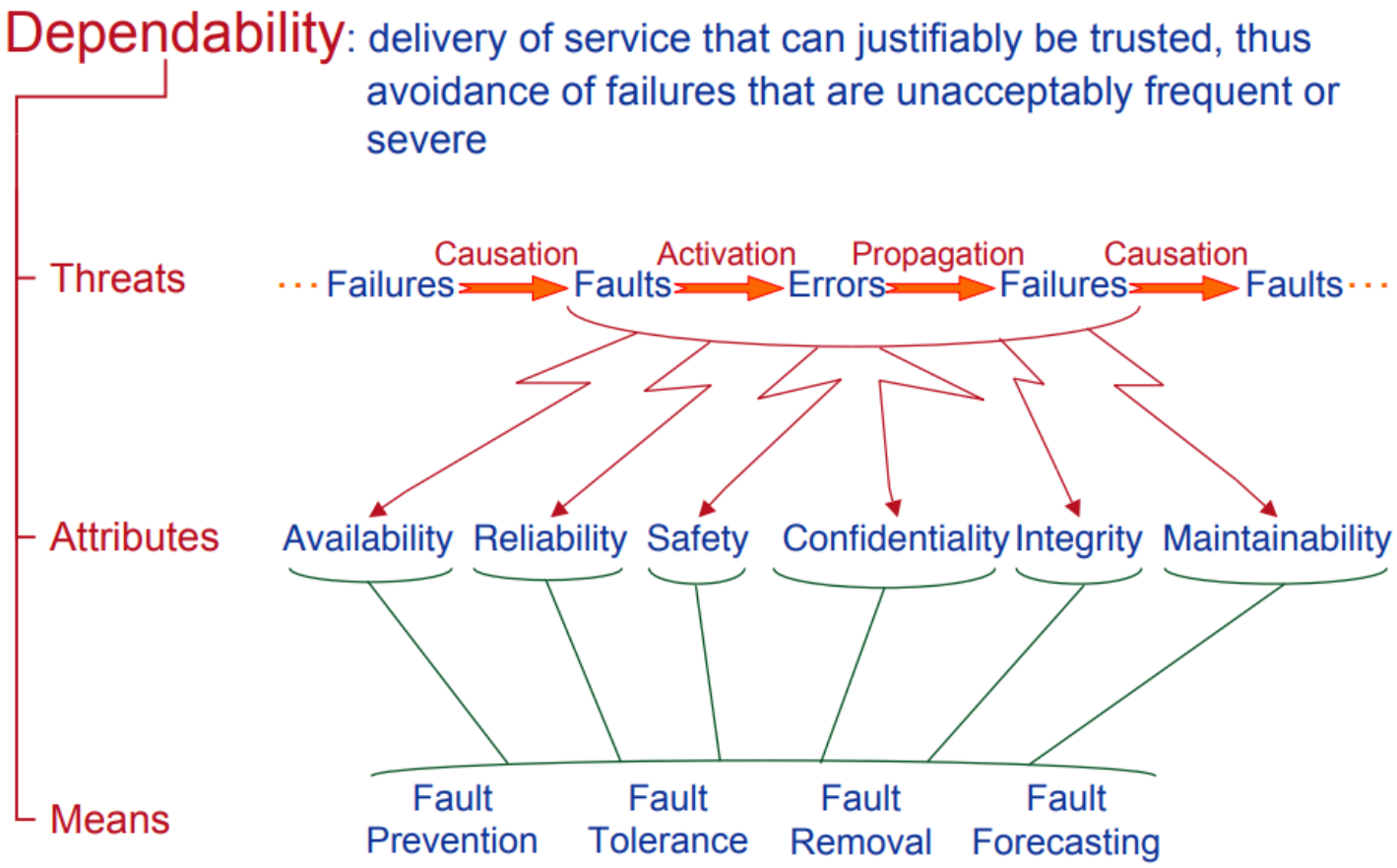
Entraves

Moyens

- **Prévention des fautes**
- **Tolérance aux fautes**
- **Élimination des fautes**
- **Prévision des fautes**

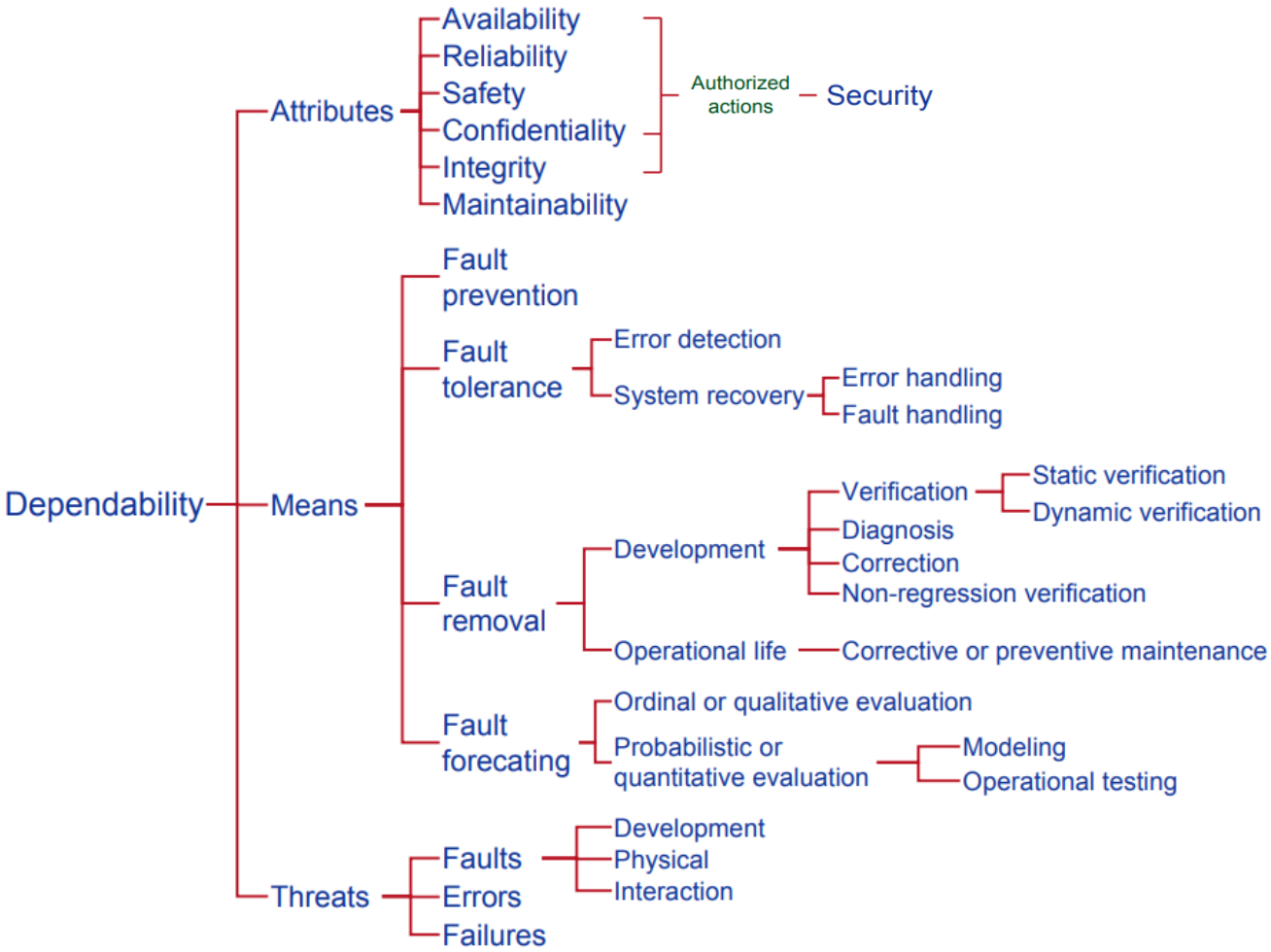
Caractéristiques de la sûreté de fonctionnement

SdF: « la propriété qui permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur délivre » **[JC Laprie]**



Caractéristiques de la sûreté de fonctionnement

SdF: « la propriété qui permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur délivre » **[JC Laprie]**



MÉTHODES ET STANDARDS POUR LA SDF

Méthodes

- Quantitative ou qualitative
- Inductive ou déductive
- Statique ou dynamique

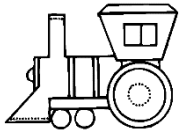
APR

AMDEC

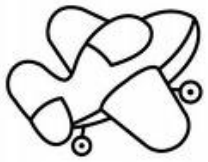
RDP

Standards

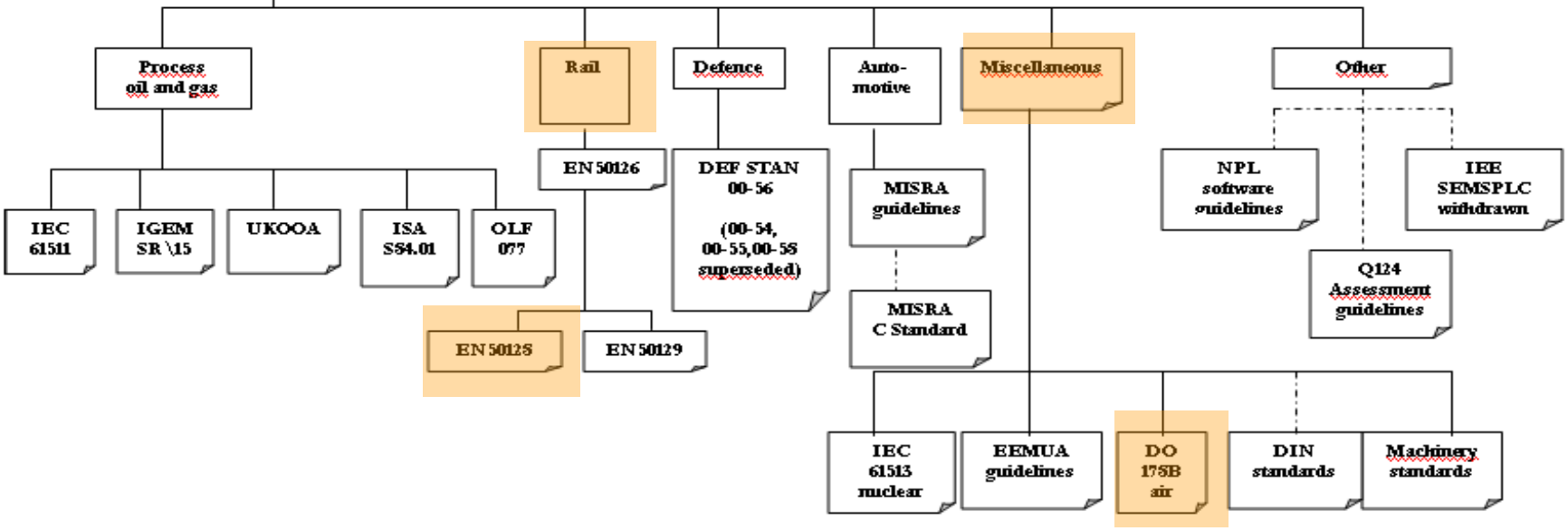
EN 50128



DO 178B



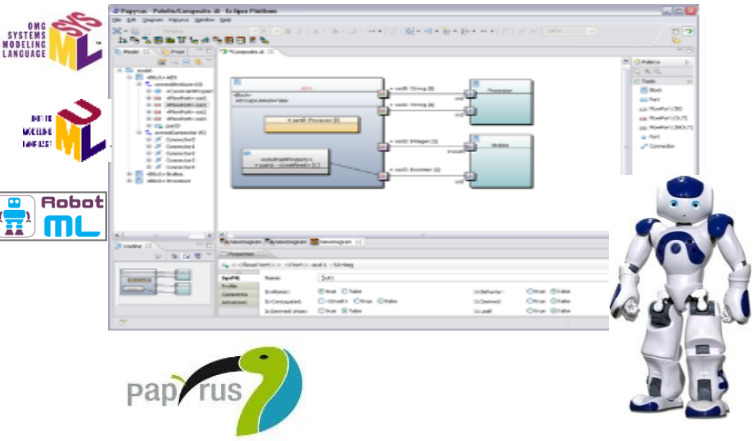
ISO 26262



CURRENT PRACTICE

System Engineering

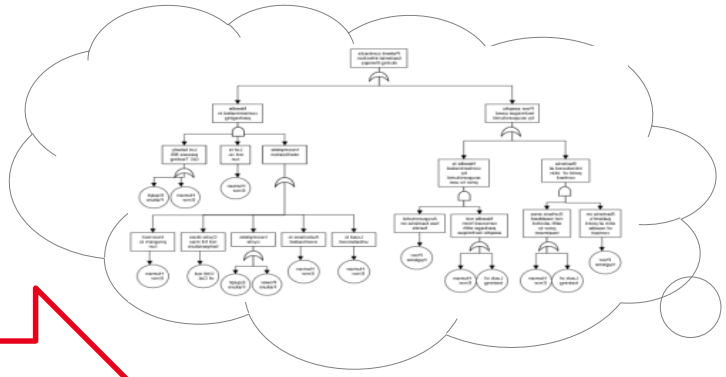
- Large usage of **Model-Based** approaches and techniques
- Complete description of the system architecture

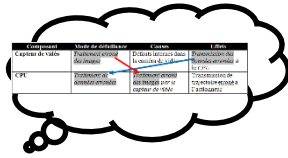


Design Engineer

CLASSICAL RAMS & (CYBER)SECURITY ANALYSIS

- Performed mostly manually
- Time consuming, costly, high probability of errors
- No strong links between system engineering and safety/security analysis





Safety/Security Engineer

Complexité

CONTEXTE ET ENJEUX

- **Evolution des systèmes et des normes**
  - Complexité accrue des systèmes

    ➔ Evolution des méthodes de conception (MBSE)
    ➔ Contraintes de coûts et délais très fortes

  - Augmentation de la complexité des activités des ingénieurs Safety

    ➔ Analyses de risques, limites de complexité atteintes sans soutien outillé
    ➔ Argumentation de la justification longue et difficile à établir sans aide outillée
    ➔ Comment réduire et capitaliser l'effort de conception sûre et de justification

  - Domaines soumis à certification plus nombreux (automobile, santé, robotique,)

    ➔ Industriels mal armés pour établir des dossiers de sécurité
    ➔ Méthodes non instrumentées (à base de tableurs) et difficiles à mettre en œuvre
    ➔ Méthodes formelles développées par les grands acteurs industriels historiques des systèmes critiques mal adaptées pour un usage direct par les nouveaux acteurs industriels

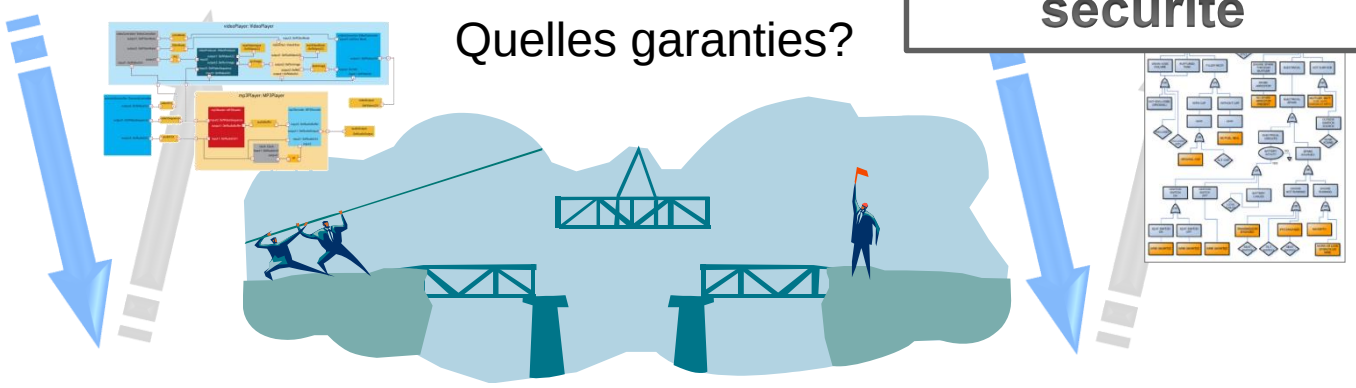
CONTEXTE ET ENJEUX

Aujourd'hui

Environnement de conception

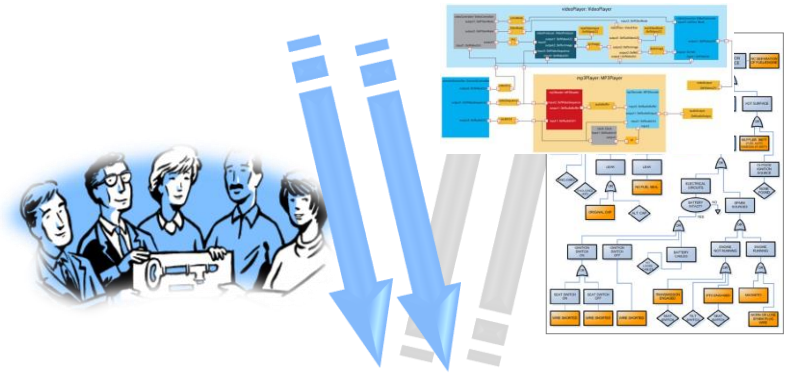
Quels Liens?
Quelles garanties?

Environment d'analyse de sécurité



Demain

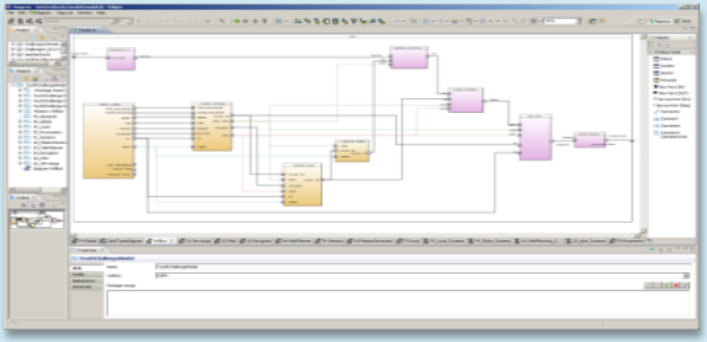
Environnement Intégré



- *Communication facilitée*
- *Garantie de cohérence des modèles*
- *Réduction des coûts de devpt.*
- *Gestion de systèmes plus complexes*

OUR METHODOLOGY

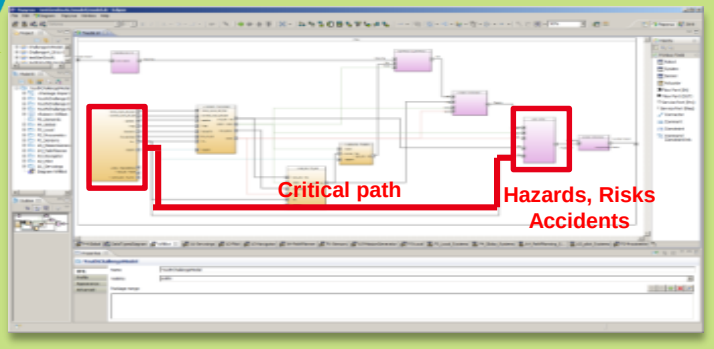
DESIGN MODEL



System architecture and behavior

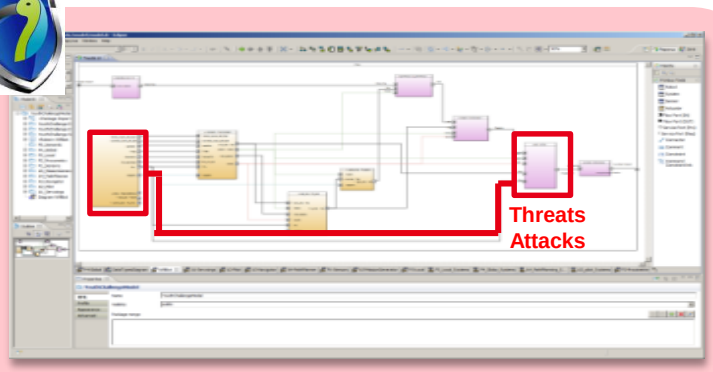
Dedicated Profile application

RAMS MODEL VIEW



Limit accidental risks!

SECURITY MODEL VIEW



Limit malicious risks!

Own dedicated models BUT consistent & aligned with system architecture models

SYSTEM LIFE-CYCLE METHODOLOGY

NORMS

Security

ISO27001/ISO27005
Generic standard on security (EBIOS methodology)

ED 202-203/ D0-356
Aerospace security practice

ISO 15408
SI security requirements

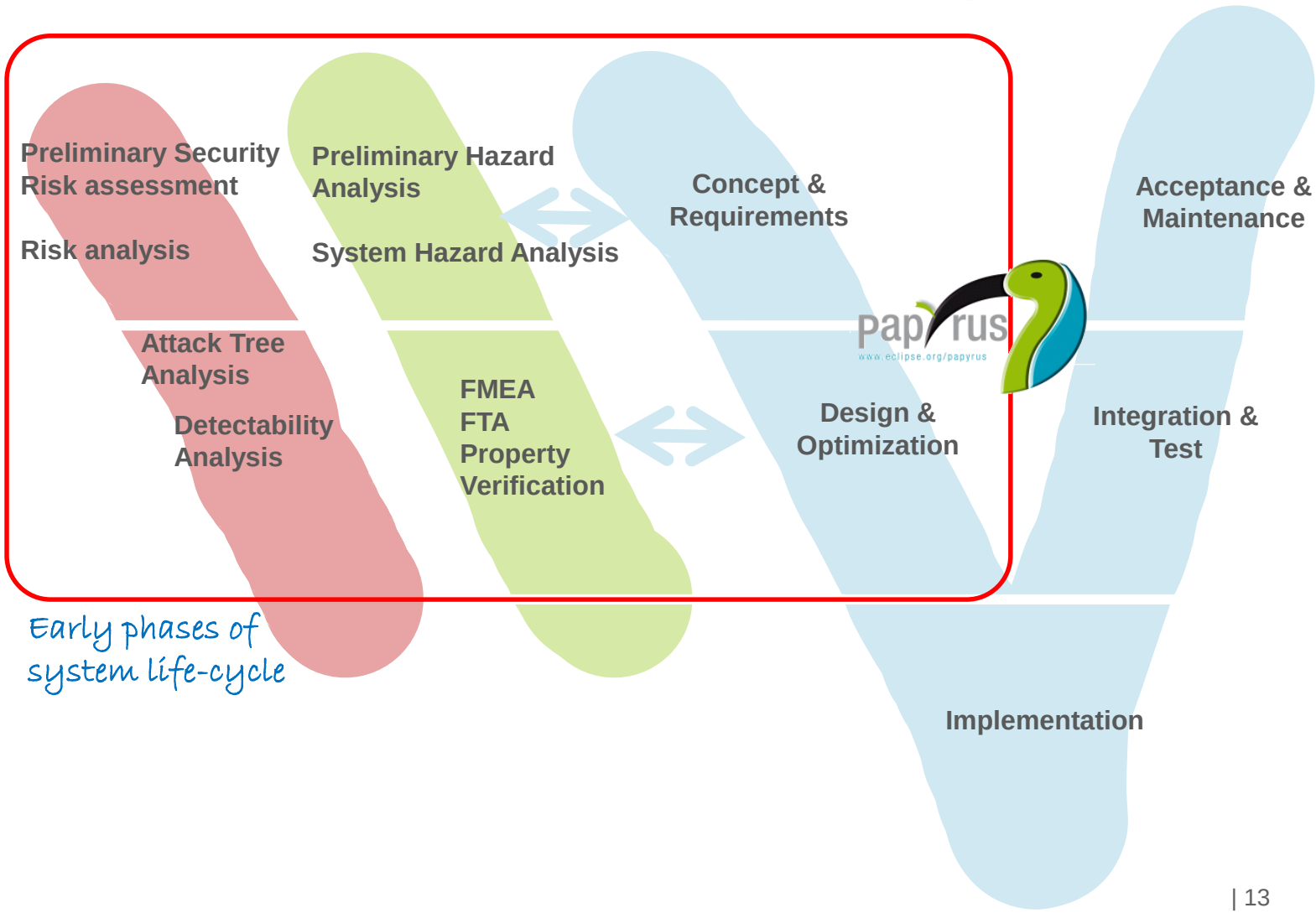
Safety

IEC 61508
Generic standard on functional safety

ISO/DIS 13482
Safety standard for personal care robots

ISO 26262
Road vehicles – Functional safety

ARP 4754/4761
Aeropspace Recommed Practice



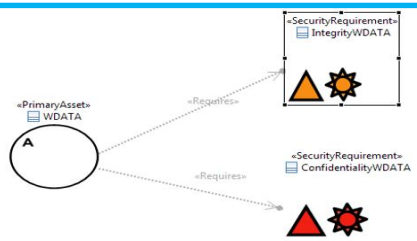
OUR TOOL FOR CYBERSECURITY: ARES

1. Context analysis and parameters configuration

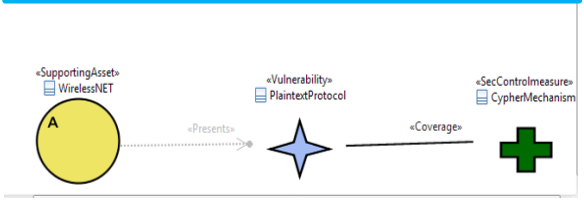
ebiosmodel.di

	Minimal	Negligible	Possible	Certain	Imminent
Critical	Important	Important	Unbearable	Unbearable	Unbearable
Very Important	Significant	Significant	Important	Unbearable	Unbearable
Important	Significant	Significant	Significant	Important	Important
Limited	Negligible	Negligible	Significant	Significant	Significant
Negligible	Negligible	Negligible	Negligible	Negligible	Negligible

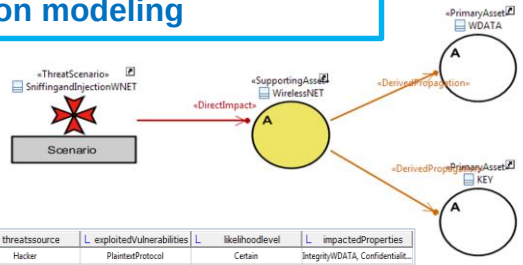
2. Primary assets identification, Feared Events modeling



3. Supporting assets identification, their vulnerabilities and existing countermeasures

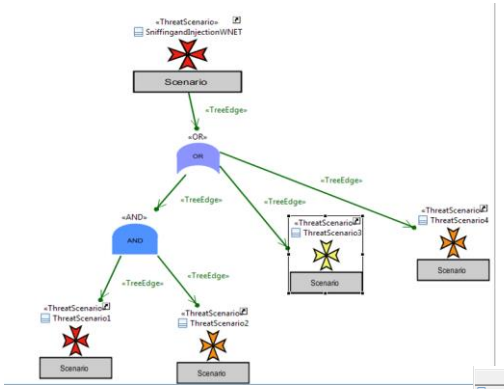


4. Threat scenarios and threats propagation modeling



	operationalImpacts	threatssource	exploitedVulnerabilities	likelihoodlevel	impactedProperties
SniffingandInjectionWNET	wior and loss of contro...	Hacker	PlaintextProtocol	Certain	IntegrityWDATA, Confidentialit...
ThreatScenario1			PlaintextProtocol	Certain	IntegrityWDATA, Confidentialit...
ThreatScenario2			PlaintextProtocol	Possible	IntegrityWDATA, Confidentialit...
ThreatScenario3			PlaintextProtocol	Negligible	IntegrityWDATA, Confidentialit...
ThreatScenario4			PlaintextProtocol	Possible	IntegrityWDATA, Confidentialit...

5. Attack trees analysis



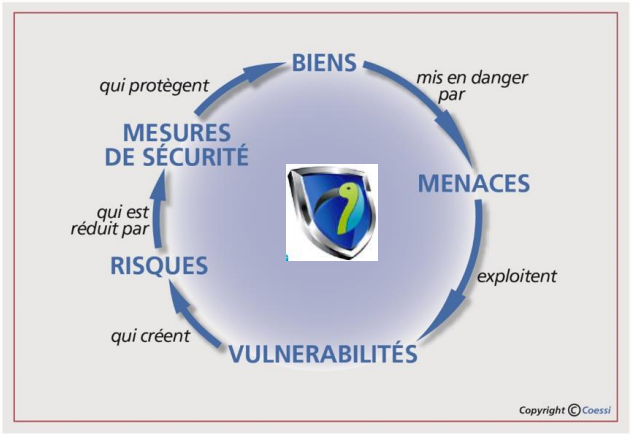
6. Risks Assessment: likelihood of threat scenarios vs. Severity of attacks

ebiosmodel.di

	likelihood	severity	Risk
Risk_SniffingandInjection...	Certain	Very Important	Unbearable
Risk_ThreatScenario1	Certain	Very Important	Unbearable
Risk_ThreatScenario2	Possible	Very Important	Important
Risk_ThreatScenario3	Negligible	Very Important	Significant
Risk_ThreatScenario4	Possible	Very Important	Important

ebiosmodel.di

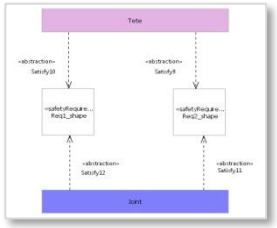
	likelihood	severity	Risk
Risk_IntegrityWDATA	Certain	Important	Important
Risk_ConfidentialityWDATA	Certain	Very Important	Unbearable
Risk_IntegrityKEY	Certain	Important	Important
Risk_ConfidentialityKEY	Certain	Very Important	Unbearable



OUR TOOL FOR RAMS: SOPHIA

Build accident scenarios

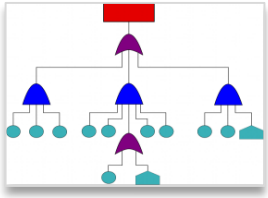
Requirement classification,
Report generation,
Import/Export to ReqIF



Preliminary Hazard Analysis

Requirement Engineering

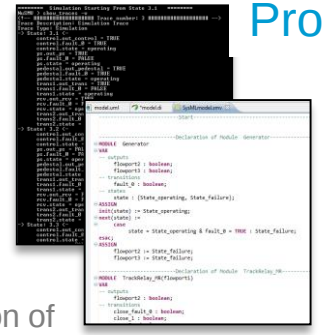
System Hazard Analysis



Analyze functional causes of accidents

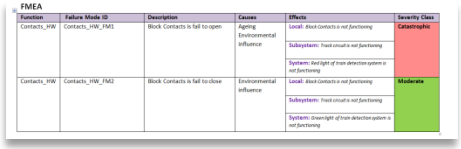
SOPHIA

Property Verification



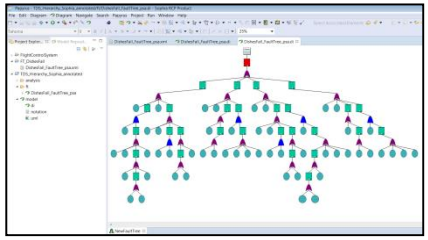
Verification of safety properties,
Reachability analysis

Failure Mode & Effects Analysis



FME(C)A tables,
Report generation

Fault Tree Analysis



Fault tree generation, minimal cut sets, probabilistic calculations

SOME APPLICATION DOMAINS

Energy, Smart Grids

Projects

MOSARIS

SESAM-Grids

Principal Partners

CoESSI

COFELY INEO GDF SUEZ

TRIALOG

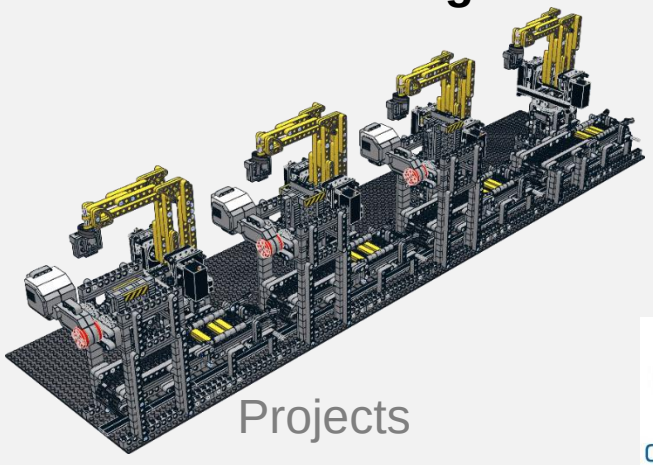
CentraleSupélec

Robotics

ALDEBARAN Robotics

P-RC2

Manufacturing



Projects

COMAU

Transportation
Automotive
Railways

Projects

Build-IT Safe

RISC

Imofis

openETCS

PERFECT

Principal Partners

tecnalia Corporación Tecnológica

ALL4TEC

RENAULT

ALSTOM

DB

SIEMENS