INSTITUT
Mines-Télécom

Projet SecureFACTORY

Contribution IMT

MINES Albi-Carmaux · MINES Alès · MINES Douai · MINES Nantes · MINES ParisTech · Ecole Nationale Supérieure des Mines Saint-Etienne · TELECOM Bretagne · TELECOM Ecole de Management · TELECOM ParisTech · TELECOM SudParis · EURECOM · TELECOM Lille · MINESnancy

Pourquoi le projet SecureFACTORY ?

La cyber est au cœur de la transformation numérique

La cyber est au cœur de la stratégie des entreprises

Pourquoi le projet SecureFACTORY ?

Les cyber attaques contre les systèmes industriels sont une réalité

Constats

- **Les systèmes de contrôle industriels sont de plus en plus connectés au cyberespace**
- **Cette connexion au cyberespace a créé de nouvelles vulnérabilités**
- **Les tentatives de cyber attaques contre les systèmes industriels sont inévitables**
- **Ces cyber attaques peuvent avoir des impacts dévastateurs**
- **Les systèmes industriels n'ont pas été conçus pour faire face à ces cyber attaques**

Objectifs globaux du projet

- **Objectif 1**
  - Cyber résilience
  - Conception d'usines cyber résilientes
  - « Resilience by design »

- **Objectif 2**
  - Faire le lien entre cyber résilience et sûreté de fonctionnement
  - Gestion dynamique de risque combinant défaillance (accidentelle) et agression (malveillante)
  - Gestion de crise et scénarii de réaction

- **Objectif 3**
  - Usines « fail safe » et « fail secure »
  - Gestion contextuelle et prise en compte de l'environnement

- **Objectif 4**
  - Certification et homologation

- **Objectif 5**
  - Plateformes et expérimentations

Cyber securité : définition

- **3 dimensions**

- **Cyber protection**
  - Mesures techniques, physiques et organisationnelles mises en place pour bâtir des architectures les plus robustes possibles face aux menaces portant sur la disponibilité, la confidentialité et l'intégrité des informations ou des services

- **Cyber défense**
  - Mesures techniques ou organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face à des attaques.

- **Cyber résilience**
  - **Capacité des systèmes à continuer à fonctionner éventuellement en mode dégradé lorsqu'ils sont soumis à des agressions**

Sûreté de fonctionnement

- **Aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données**
- **En général 4 dimensions :**
  - Fiabilité
  - Maintenabilité
  - Disponibilité
  - Sécurité
- **Dans la suite :**
  - Sureté de fonctionnement : gestion des fautes accidentelles
  - Cyber résilience : gestion des agressions malveillantes

Fail safety et Fail security

- **Fail safety**
  - Dire d'un système qu'il est "fail-safe" ne signifie pas que la défaillance est impossible ou improbable
  - En revanche, la conception de ce système prévient ou réduit les conséquences néfastes de telles défaillances
  - Donc, lorsqu'un système "fail safe" est sujet à une défaillance, alors il demeure "safe" ou du moins il n'est pas moins "safe" qu'il ne l'était lorsqu'il fonctionnait correctement
- **Fail security**
  - Dire d'un système qu'il est « fail secure » ne signifie pas que des agressions intentionnelles sont impossibles ou improbables
  - En revanche, la conception du système « fail secure », réduit les conséquences d'insécurité résultant de ces agressions
  - Donc, un système « fail secure » fournit les moyens de concevoir des systèmes résilients
- **Gestion des conflits**
  - Il est possible que les deux dimensions suggèrent des solutions totalement opposées

Exemple simple de scénario

- **Système Fail safe**
  - En cas de défaillance électrique, ouverture des portes
- **Systèmes Fail secure**
  - En cas de défaillance électrique, fermeture des portes
- **Remarques**
  - Les systèmes industriels ont été conçus pour être « fail safe »
  - Besoins de les faire évoluer pour être aussi « fail secure »

Description des travaux

- **Tâche 1 : L'usine cyber résiliente**
  - Tâche 1.a : Système cyber résilient
  - Tâche 1.b : Composant cyber résilient
  - Tâche 1.c : Resilience by design
- **Tâche 2 : Cyber résilience et Sureté de fonctionnement**
  - Tâche 2.a : Analyse et gestion dynamique des risques
  - Tâche 2.b : Gestion des incidents
  - Tâche 2.c : Maintien en condition de sécurité
- **Tâche 3 : Usine fail safe et fail secure**
  - Tâche 3.a : Composants « fail safe » et « fail secure »
  - Tâche 3.b : Gestion contextuelle et prise en compte de l'environnement
  - Tâche 3.c : Conception du système de contrôle
  - Tâche 3.d : Vérification formelle

Description des travaux

- **Tâche 4 : Certification et homologation**
  - Tâche 4.a : Certification des composants
  - Tâche 4.b : Homologation des composants
  - Tâche 4.c : Certification du système de contrôle

- **Tâche 5 : Expérimentations**
  - Tâche 5.a : Déploiement des plateformes de tests et d'intégration
  - Tâche 5.b : Intégration
  - Tâche 5.c : Tests et validation

Contribution de l'IMT

- Étude / conception de l'architecture matérielle/logicielle
- Etude / conception des composants logiciels
- Outils de développement spécifiques du processeur sécurisé
- Vérification logicielle/matérielle
- Modélisation et analyse des risques de sécurité
- Etude et conception de protocoles de sécurité

Budget et consortium

- **Grands groupes**
  - Airbus Defense & Space Cybersécurité
  - EDF
  - Sopra – Steria
  - La Poste
  - Orange
- **PME**
  - Amossys
  - Secure IC
  - Montimage
- **Académiques**
  - IMT
  - CEA

- **Budget**
  - 8 M€