SystemX

Accélérateur de la Transformation Numérique

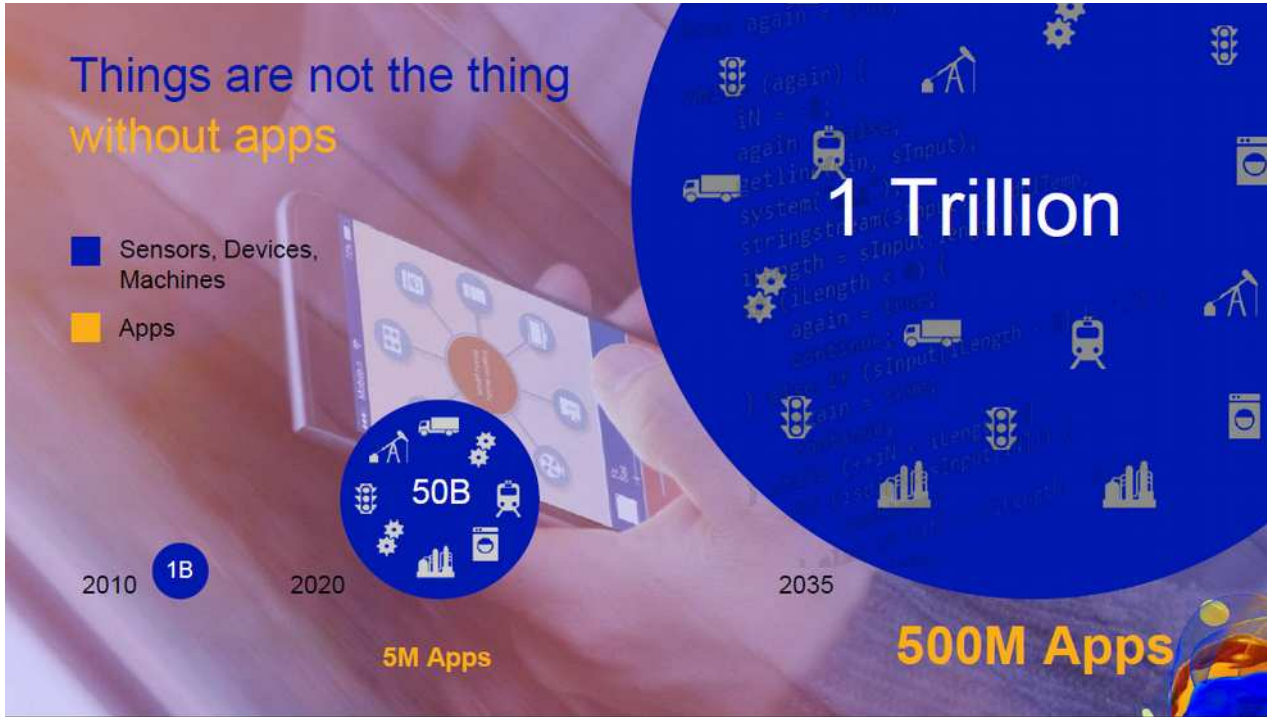
La recherche en ingénierie numérique de systèmes complexes

Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité

Cybersécurité - IoT et systèmes embarqués – Ivry, jeudi 9 juin 2016

Vers l'Internet du n'importe quoi ?

- Big Data : The past
- M2M : The present
- Internet of Everything: The future



EIC: Environnement d'Intégration et Interopérabilité en Cybersécurité

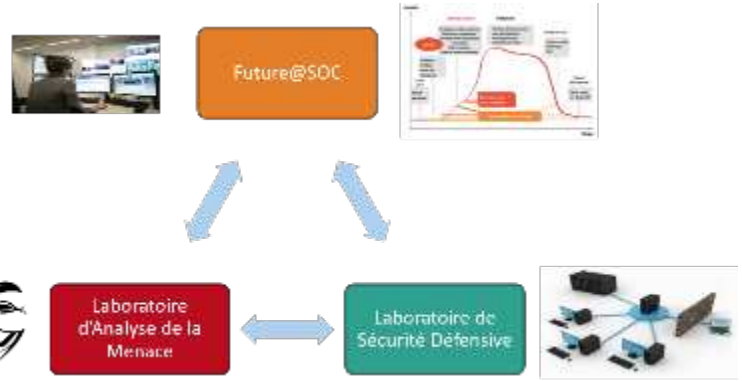
Contexte, Objectifs du projet

- Connaître et anticiper la menace en se dotant d'une plateforme d'outillages coordonnés et de capacités d'analyses automatisées ;
- Évaluer la robustesse des contre-mesures mises en œuvre dans des cas d'usages innovants et réalistes ;
- Répondre aux exigences de supervision des attaques au travers d'une gestion opérationnelle intégrée qui proposera des capacités de supervision innovantes.

Verrous technologiques

- Security By Design
- Sécurisation des architectures massives
- Supervision des systèmes de systèmes hyperconnectés
- Respect de la vie privée

Synthèse du projet



Partenaires industriels

Partenaires académiques

EIC: Environnement d'Intégration et Interopérabilité en Cybersécurité

Ingénierie Systèmes

Transport Autonome

Territoires Intelligents

Internet de Confiance

Axes majeurs et Espaces de recherche

Future@SOC : SOC du Futur

Gestion Opérationnelle

Jeux de données

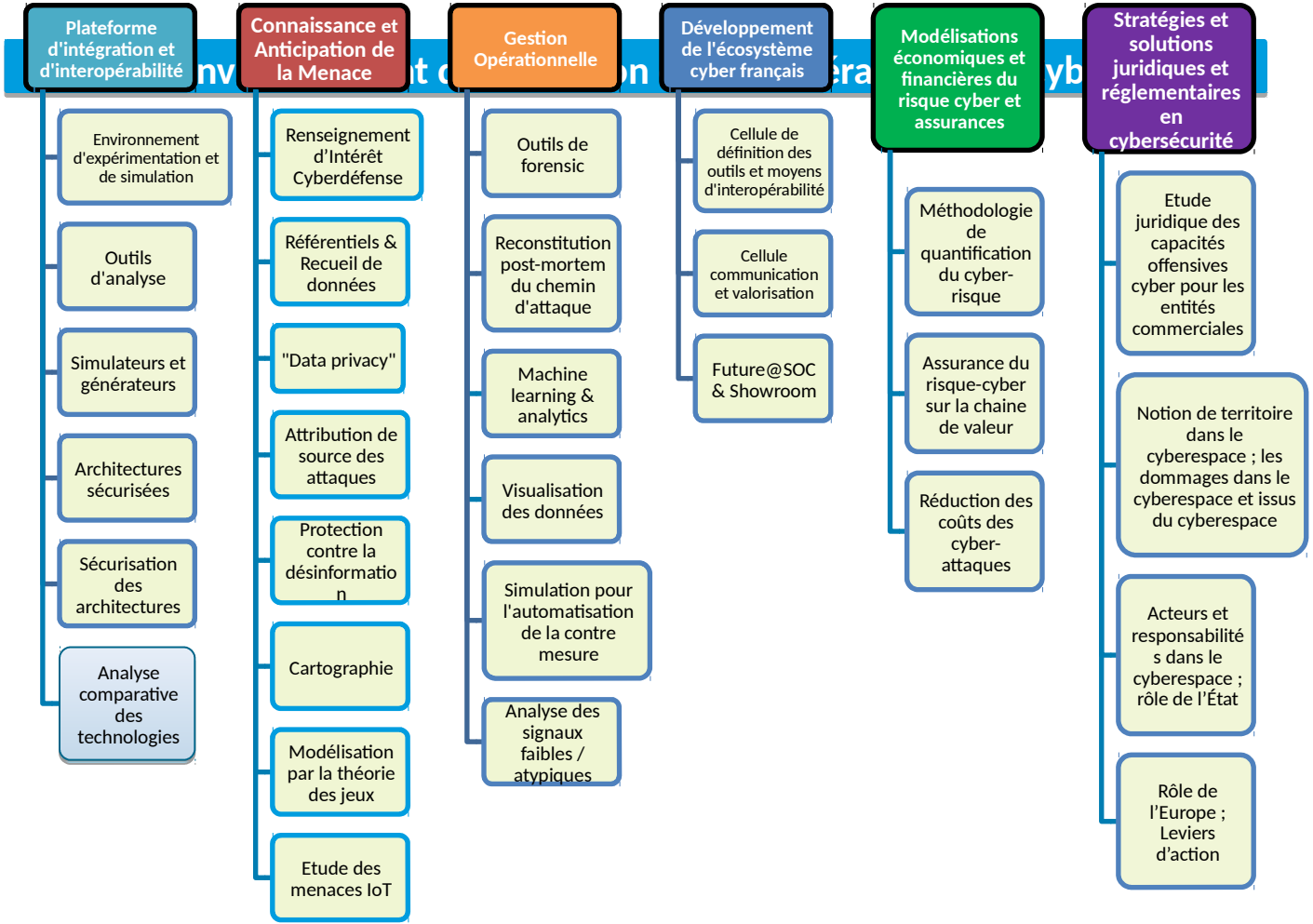
Connaissance et Anticipation de la Menace

Sécurité Défensive

Laboratoire de Connaissance et d'Anticipation de la Menace

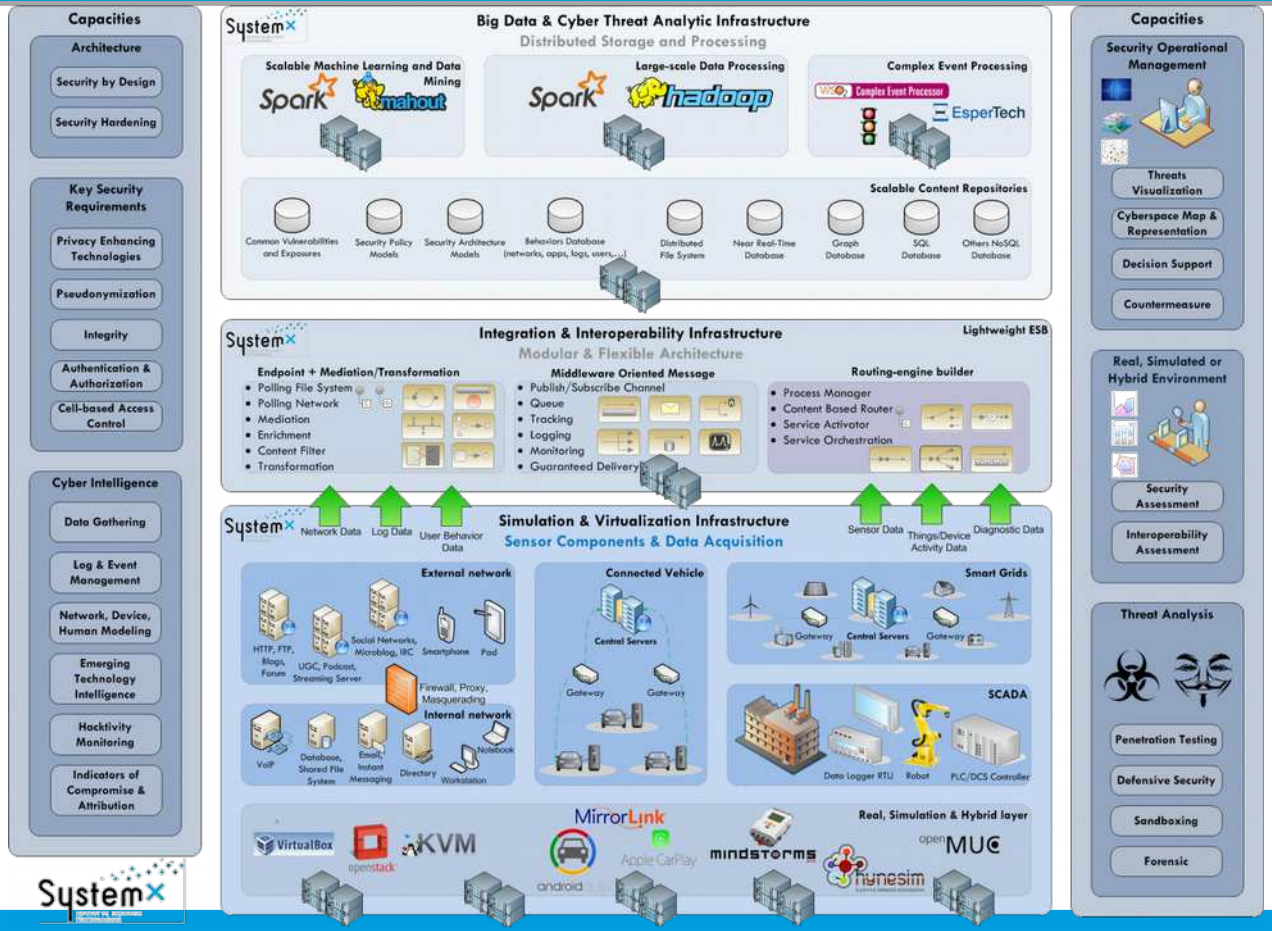
Laboratoire de Sécurité Défensive

Tâches


Plateforme d'intégration et d'interopérabilité
Environnement d'expérimentation et de simulation
Outils d'analyse
Simulateurs et générateurs
Architectures sécurisées
Sécurisation des architectures
Analyse comparative des technologies
Connaissance et Anticipation de la Menace
Renseignement d'Intérêt Cyberdéfense
Référentiels & Recueil de données
"Data privacy"
Attribution de source des attaques
Protection contre la désinformation
Cartographie
Modélisation par la théorie des jeux
Etude des menaces IoT
Gestion Opérationnelle
Outils de forensic
Reconstitution post-mortem du chemin d'attaque
Machine learning & analytics
Visualisation des données
Simulation pour l'automatisation de la contre mesure
Analyse des signaux faibles / atypiques
Développement de l'écosystème cyber français
Cellule de définition des outils et moyens d'interopérabilité
Cellule communication et valorisation
Future@SOC & Showroom
Modélisations économiques et financières du risque cyber et assurances
Méthodologie de quantification du cyber-risque
Assurance du risque-cyber sur la chaine de valeur
Réduction des coûts des cyber-attaques
Stratégies et solutions juridiques et réglementaires en cybersécurité
Etude juridique des capacités offensives cyber pour les entités commerciales
Notion de territoire dans le cyberespace ; les dommages dans le cyberespace et issus du cyberespace
Acteurs et responsabilités dans le cyberespace ; rôle de l'État
Rôle de l'Europe ; Leviers d'action

Architecture de la plate-forme CHESS

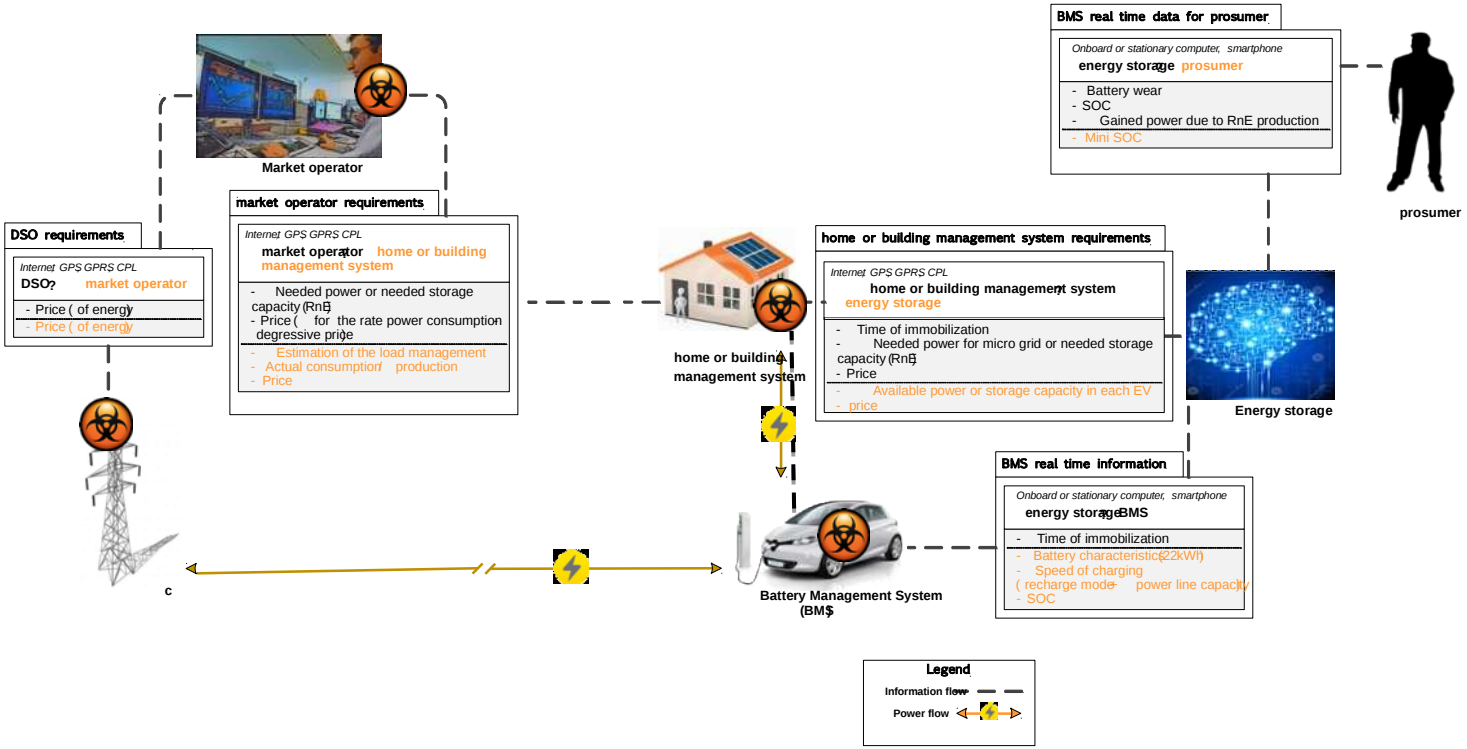
Cybersecurity Hardening Environment for Systems of Systems



- **Les Smart Grids**
  - Les futurs Réseaux d'énergie numérisés et intelligents
- **Le Véhicule Connecté & son Environnement**
  - Le transport connecté et autonome
- **L'Usine du Futur**
  - Des SCADA à l'Usine 4.0 reposant sur l'Internet Industriel des Objets
- **Les Systèmes d'Information d'Entreprise, la gestion de la mobilité et les nouveaux services associés**
  - L'Internet des Objets (IoT/M2M) et les menaces émergentes

Cas d'usage : « Smart Grids » & la « Voiture connectée »

Etude en cours de 85 cas d'usage autour du « Smart Grids » (projet ITEA2 SEAS) fournis par ENGIE et IMT



Feuille de route suivie à partir des cas d'usage

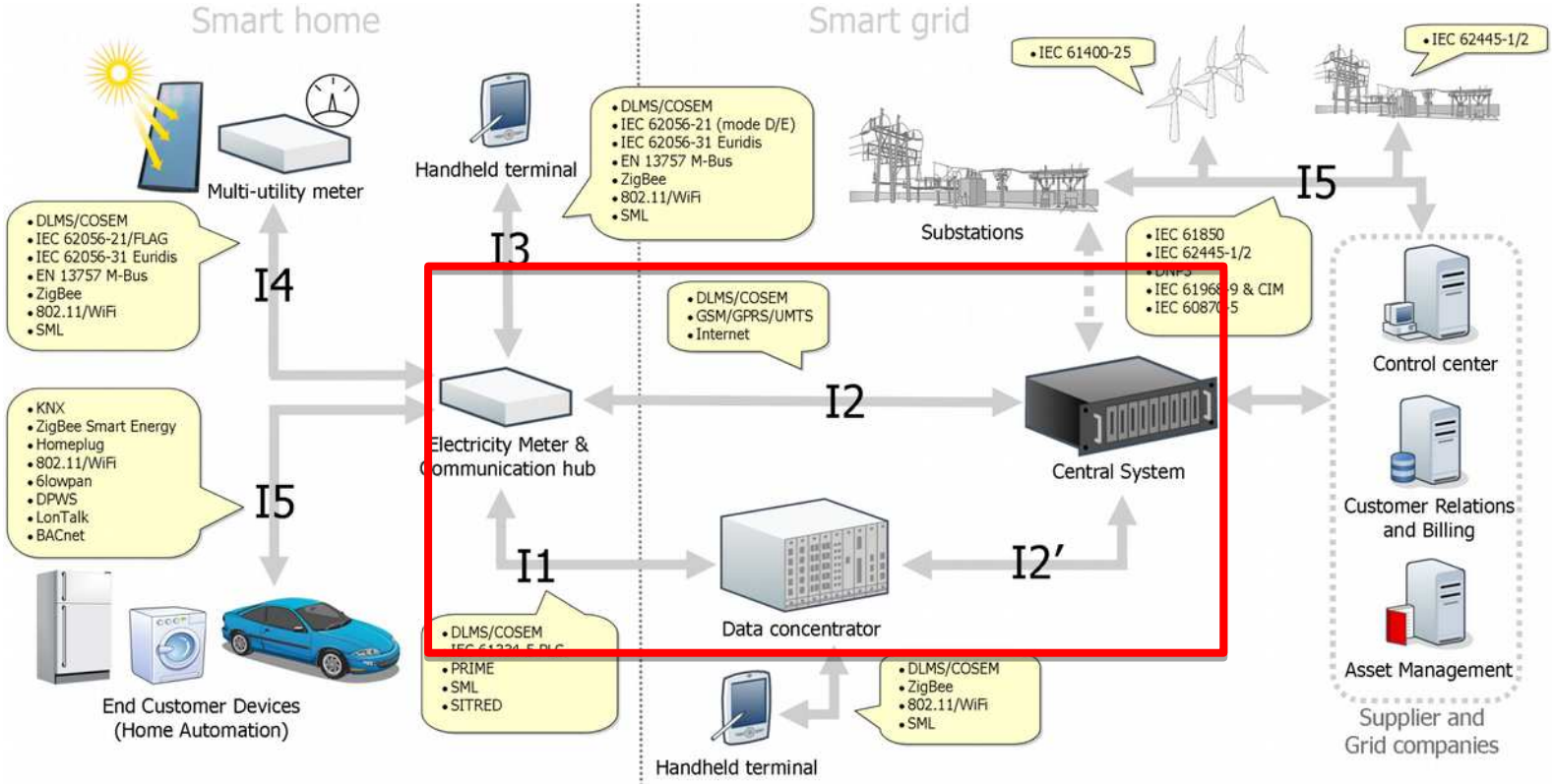
Architectures sécurisées

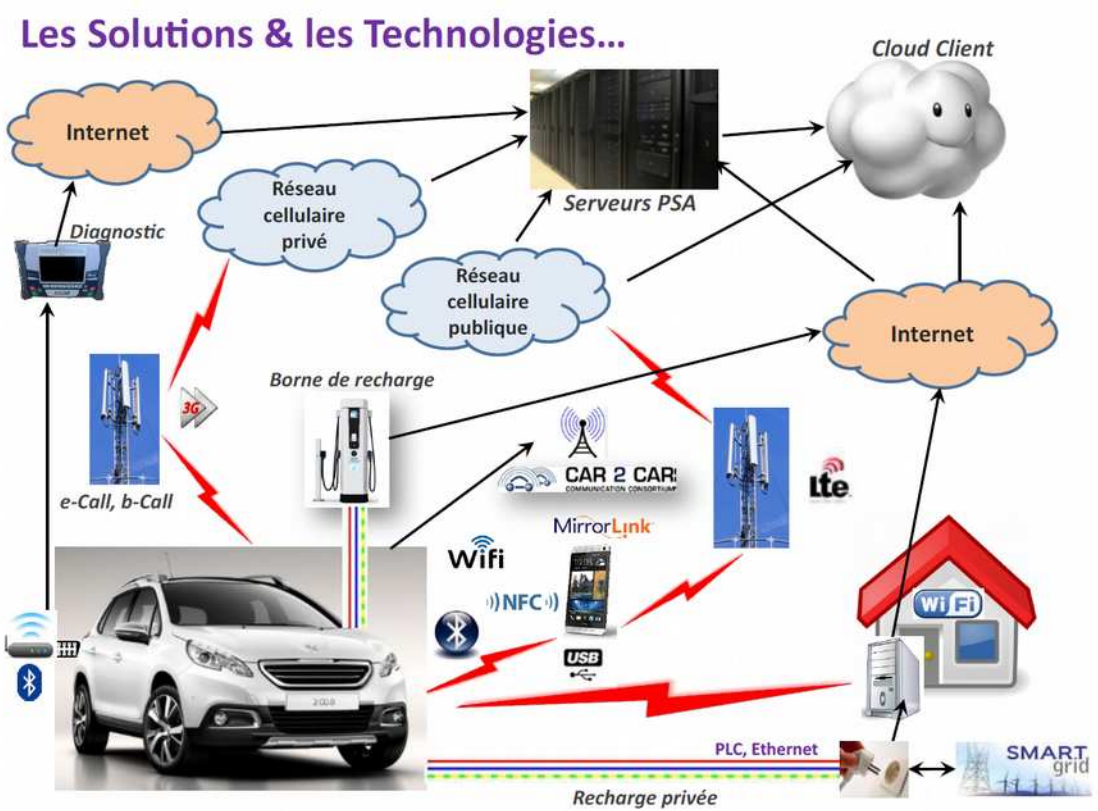
et/ou durcissement

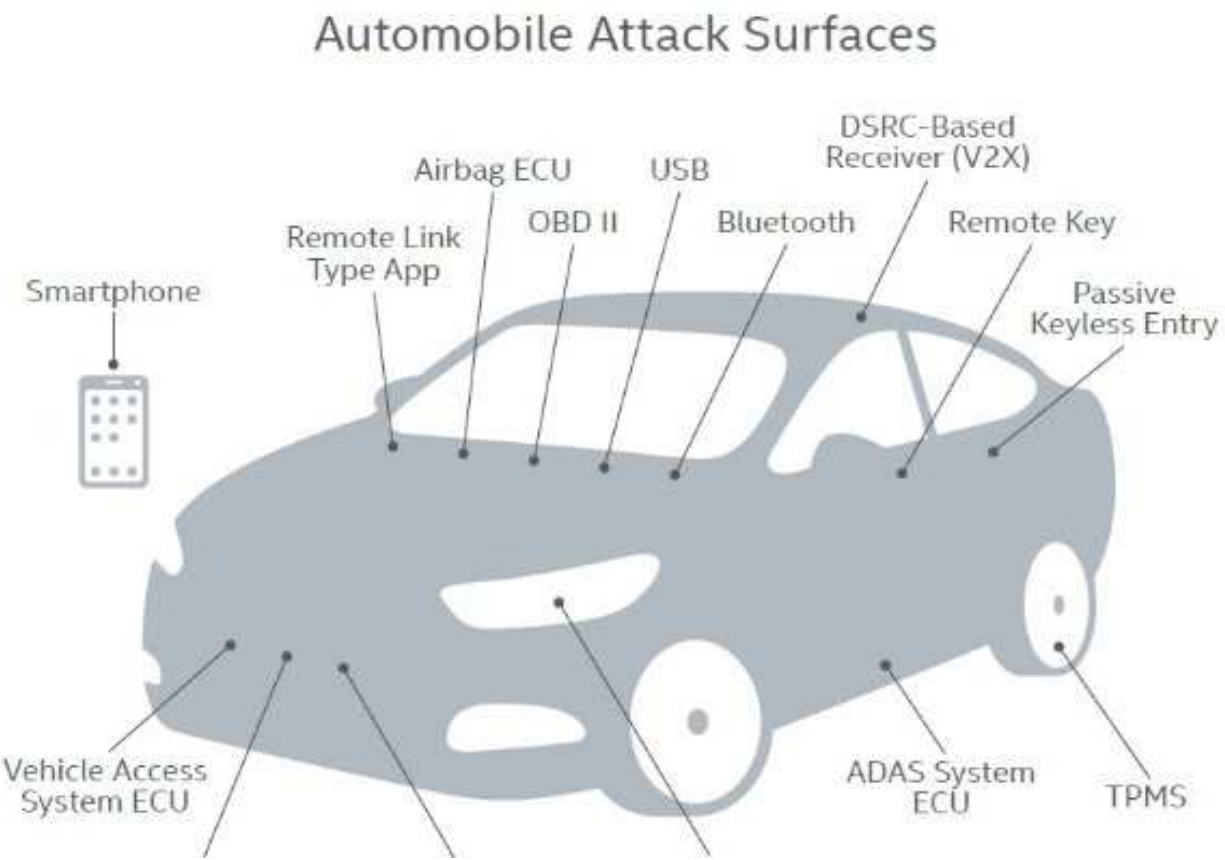
Recherche de vulnérabilité/faille

Reproduction de l'architecture cible

Standards et protocoles de communication




Les Solutions & les Technologies…
Cloud Client
Internet
Serveurs PSA
Réseau cellulaire privé
Diagnostic
Réseau cellulaire publique
Internet
Borne de recharge
3G
e-Call, b-Call
CAR 2 CAR
lte
MirrorLink
WiFi
NFC
USB
Wi Fi
PLC, Ethernet
SMART grid
Recharge privée


Automobile Attack Surfaces
DSRC-Based Receiver (V2X)
Airbag ECU
USB
Remote Link Type App
OBD II
Bluetooth
Remote Key
Smartphone
Passive Keyless Entry
Vehicle Access System ECU
ADAS System ECU
TPMS

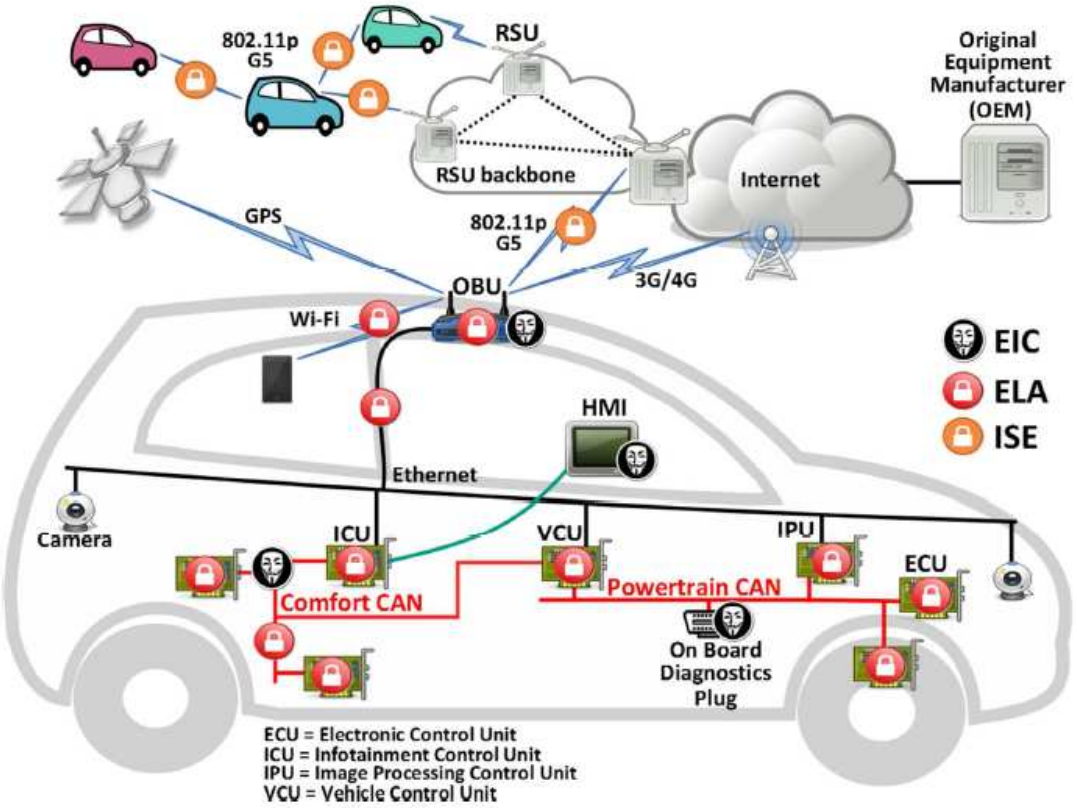
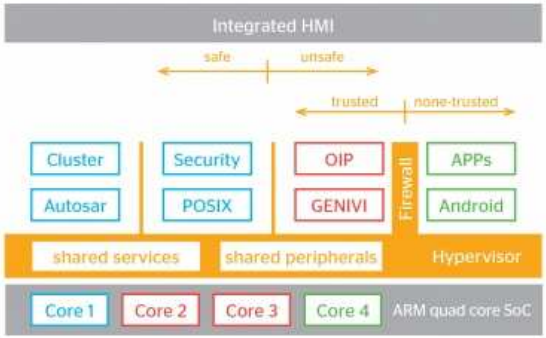
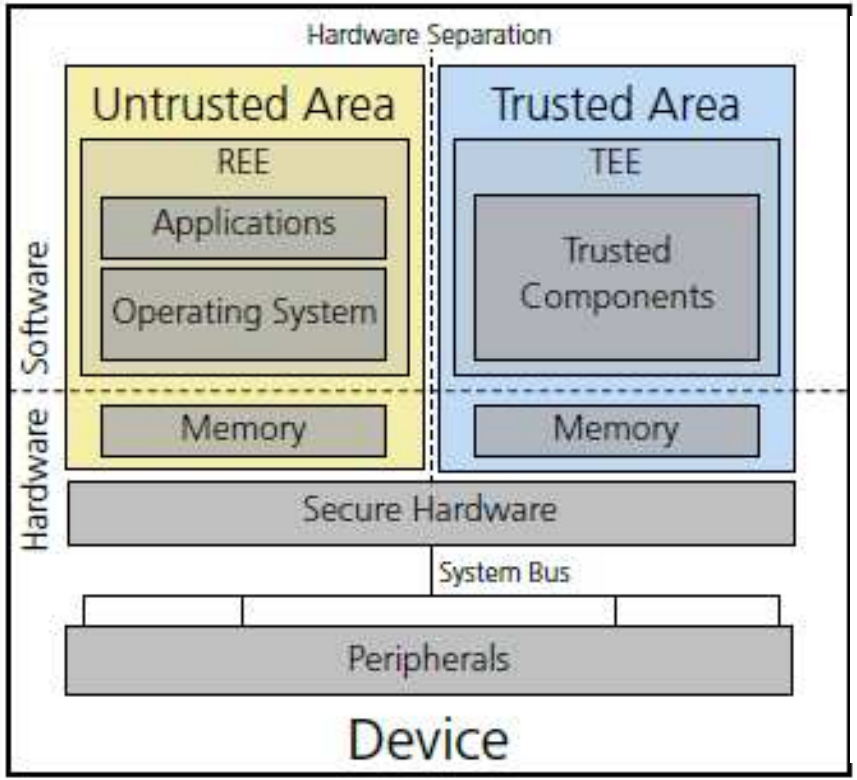


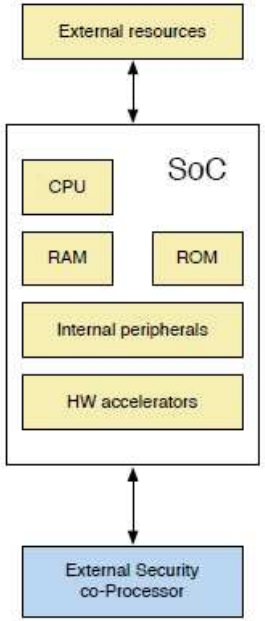
Figure 1 : Interaction des programmes sur le véhicule connecté.

Sécurité des systèmes de type « Voiture connectée »

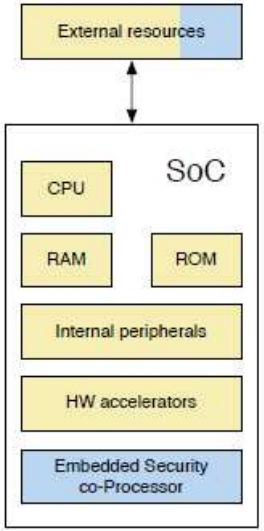
- **Problématique**
  - Passage d'un monde cloisonné à un monde connecté
- **Axes d'effort pour la cyberprotection la « Voiture connectée »**
  - Pare-feu, Antivirus, Antimalware, Hyperviseur, Sas de décontamination ?



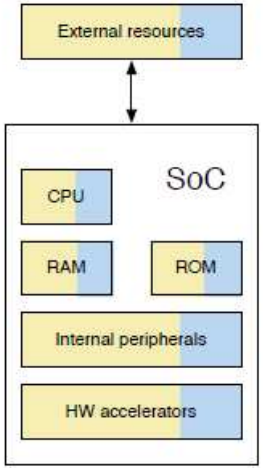




External Security co-Processor



Embedded Security co-Processor



Processor Secure Environment

Summary

- Key manager has:
  - Knowledge of pk and sk.
  - But no access to bio. data.
- Access control devices have:
  - Knowledge of sk.
  - Access to calc. results (dist.).
  - But, no access to bio. data.
- Employer (auth. server) has:
  - No knowledge of sk.
  - Hence, no access to bio. data.
  - Hence, no access to calc. results.
- Employee has:
  - To trust that the key manager will not collude with its employer.

Access control devices

Sto
FHE

HSM

HSM

HSM

HSM

Sends

oyee @ home

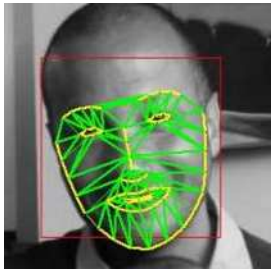
Owns bio. ref.

Employer

ABACHE : Démonstrateur opérationnel

Contrôle d'accès à double facteur :

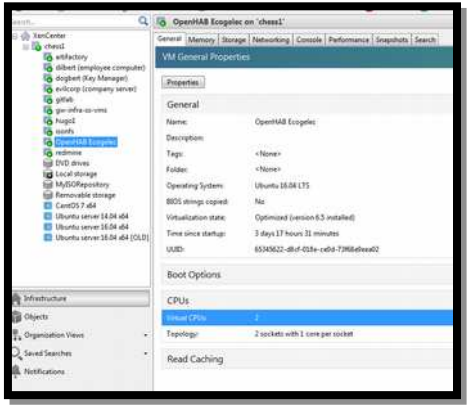
Couplage Biométrie + cryptographie homomorphe + token RFID, carte NFC Smartphone NFC

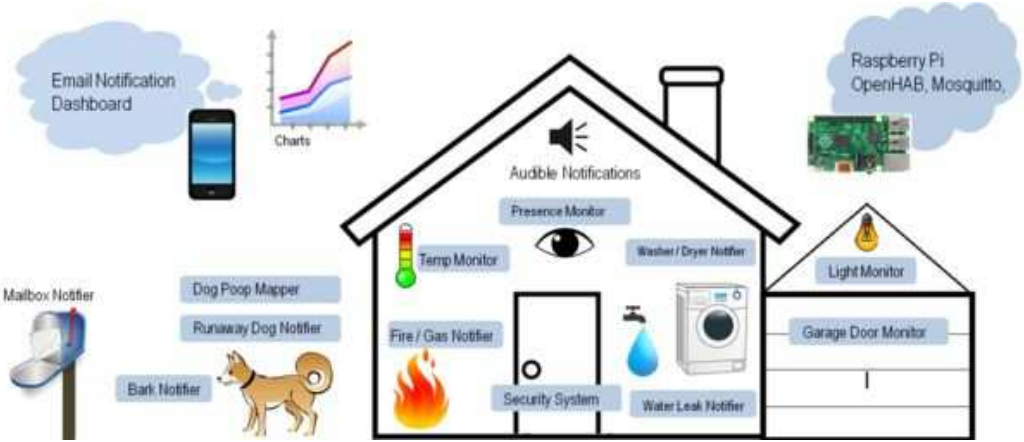


NFC + RFID à puce sans contact
Lecteur & Graveur

Lecteur de Proximité ID Carte Clé
RFID 125KHz

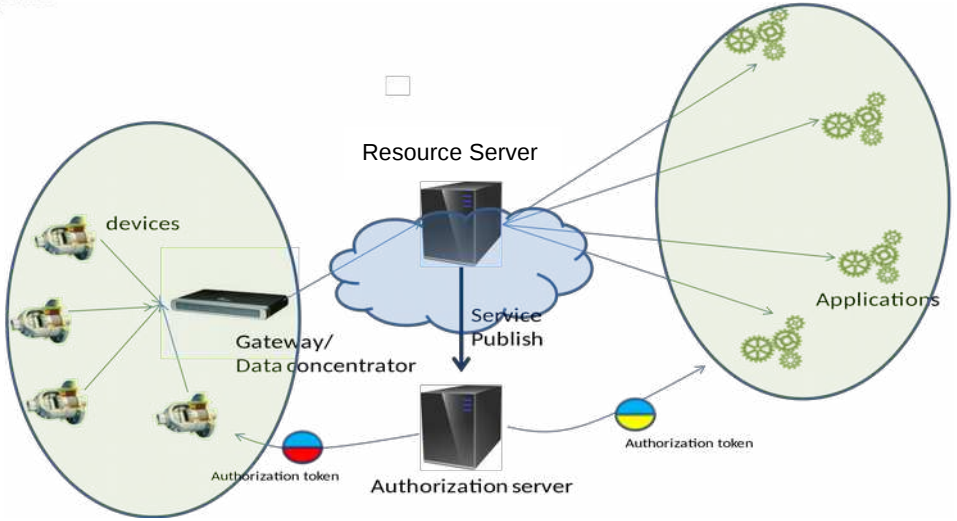
Maison connectée





Serveur d'autorisation pour l'IoT et le M2M

Architecture de référence



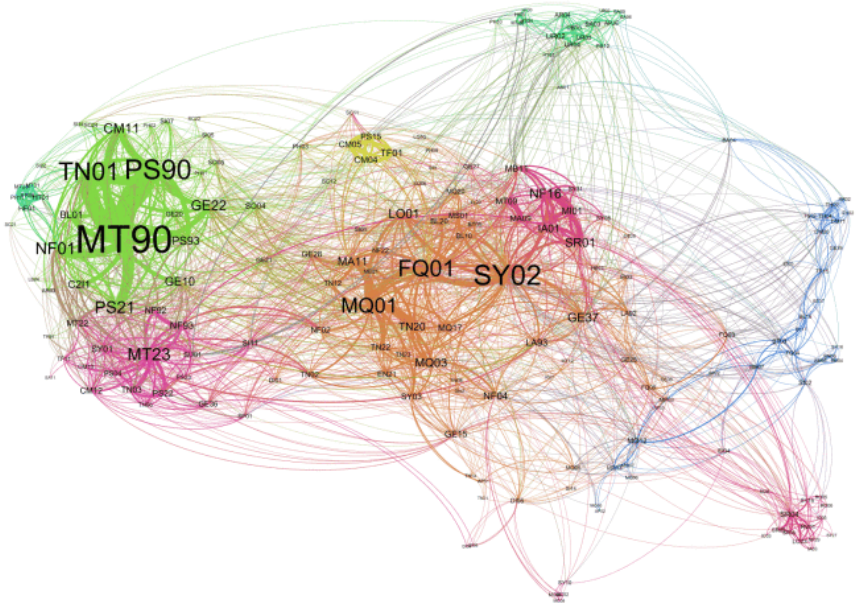
Le terme de « ressource » désigne tout ce dont l'accès peut être contrôlé

Exemples :

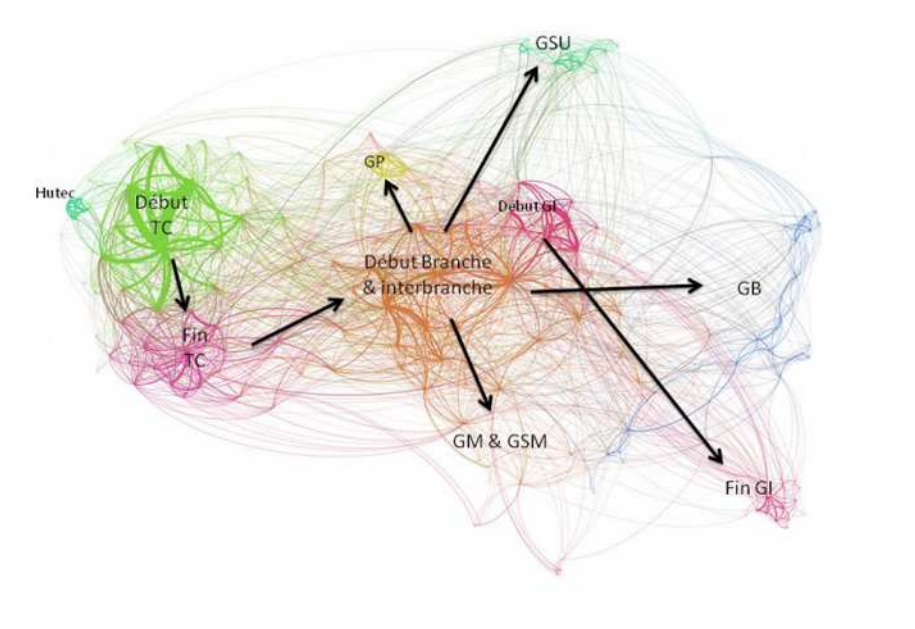
- Table dans une base de données
- Image dans un album photo
- Sujet (topic) d'un serveur MQTT
- etc

- **Le serveur d'autorisation gère les politiques d'accès aux « ressources », les droits étant matérialisés par des « tokens » de formes diverses.**
- **MQTT :**
  - Protocole de « publish/subscribe », développé par IBM, standardisé par OASIS
  - Permet d'éviter de définir explicitement « qui parle à qui »
  - L'utilisation de protocoles « publish/subscribe » est très populaire dans le monde de l'IoT

Visualisation des données de sécurité



Données brutes

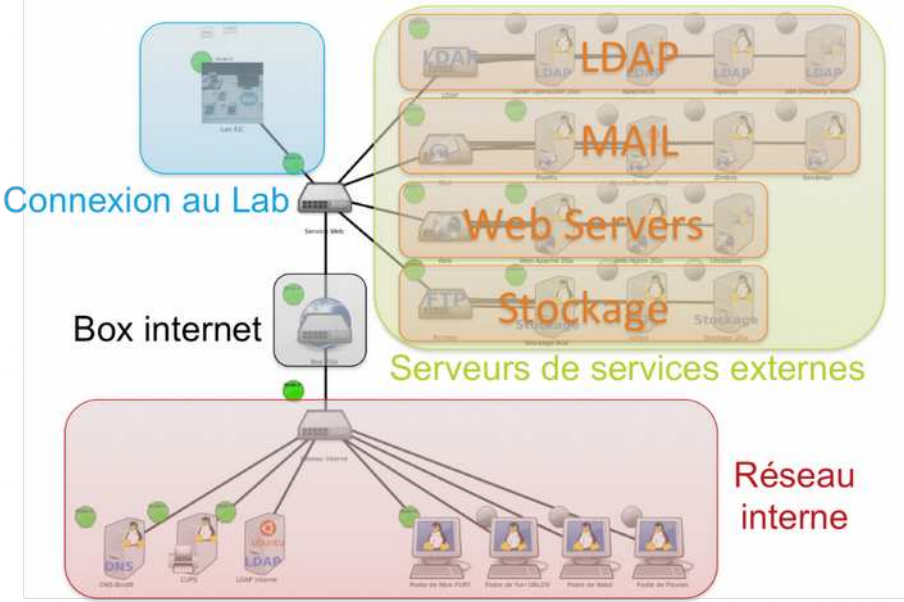


Données interprétées

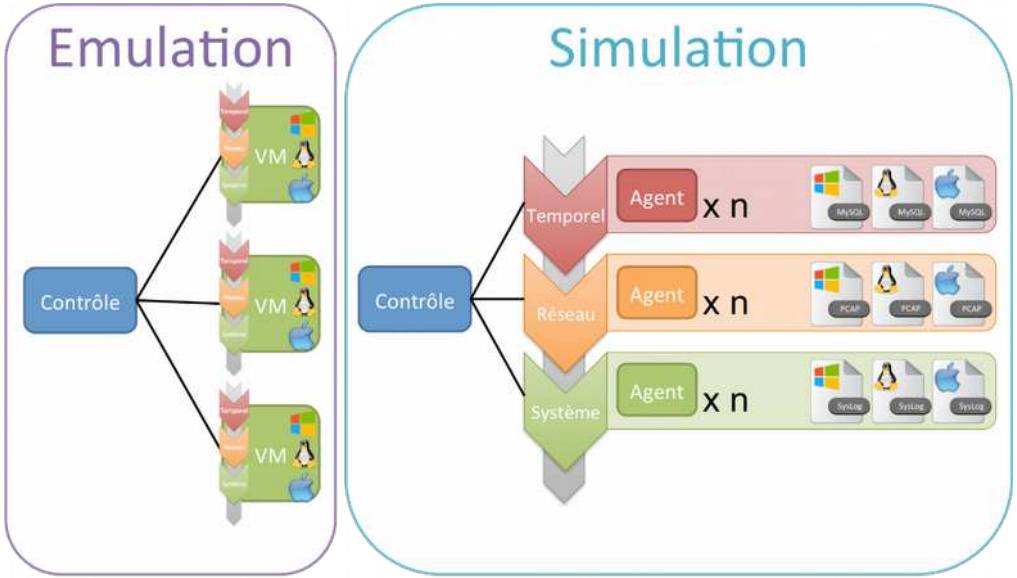
Crédit : Arnoud Vanhuele, Jean-Côme Douteau et Victor Baconneau, UTC

- **Objectif de la thèse :**
  - Simuler le SI d'une entreprise pour étudier des comportements normaux et d'attaques

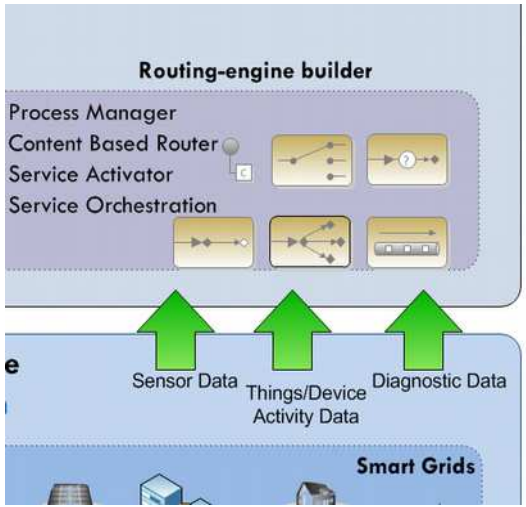
- **Architecture de SI choisie :**
  - SI de PME avec :
    - des utilisateurs
      admin, commerciaux, normaux…
    - des services internes
      LDAP, DNS, Imprimante…
    - des services externes
      Mail, Site web, Stockage…

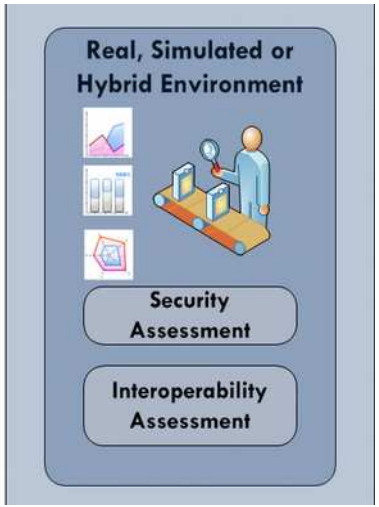


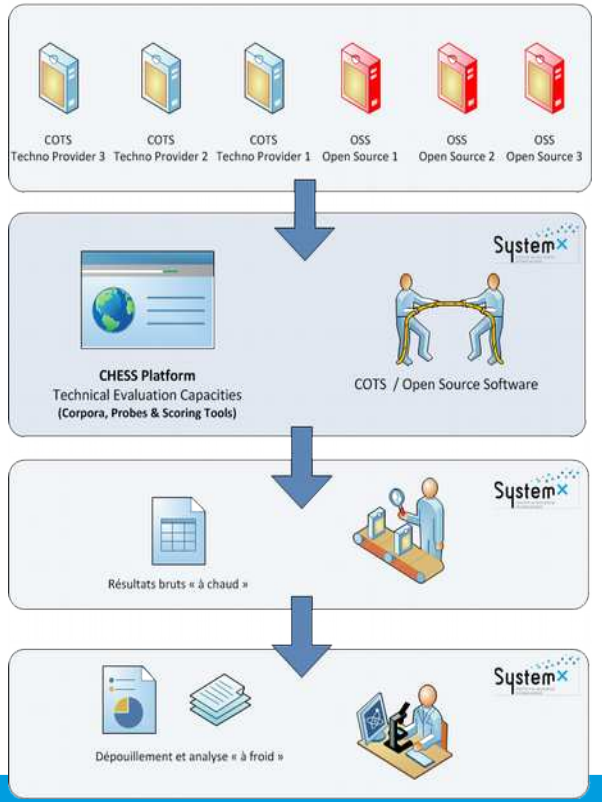
- **Emulation & Simulation**
  - Emulation
    - composée de VMs
    - des agents polyvalents
    - ne passe pas à l'échelle
    - générer les données de la simulation
  - Simulation
    - composition des agents variables *(threads, multiplexage de service,…)*
    - agents spécialisés
    - passage à l'échelle
    - se base sur les données de l'émulation



- **Nouvelles capacités visées**







Merci de votre attention

Philippe.wolf@irt-systemx.fr
Tel 01 69 08 06 42 – 06 31 67 41 50

www.irt-systemx.fr
Twitter: @IRTSystemX