

Consortium InS³pect

Ingénierie **S**ystème de **S**ervices **S**écurisés pour objets
connectés

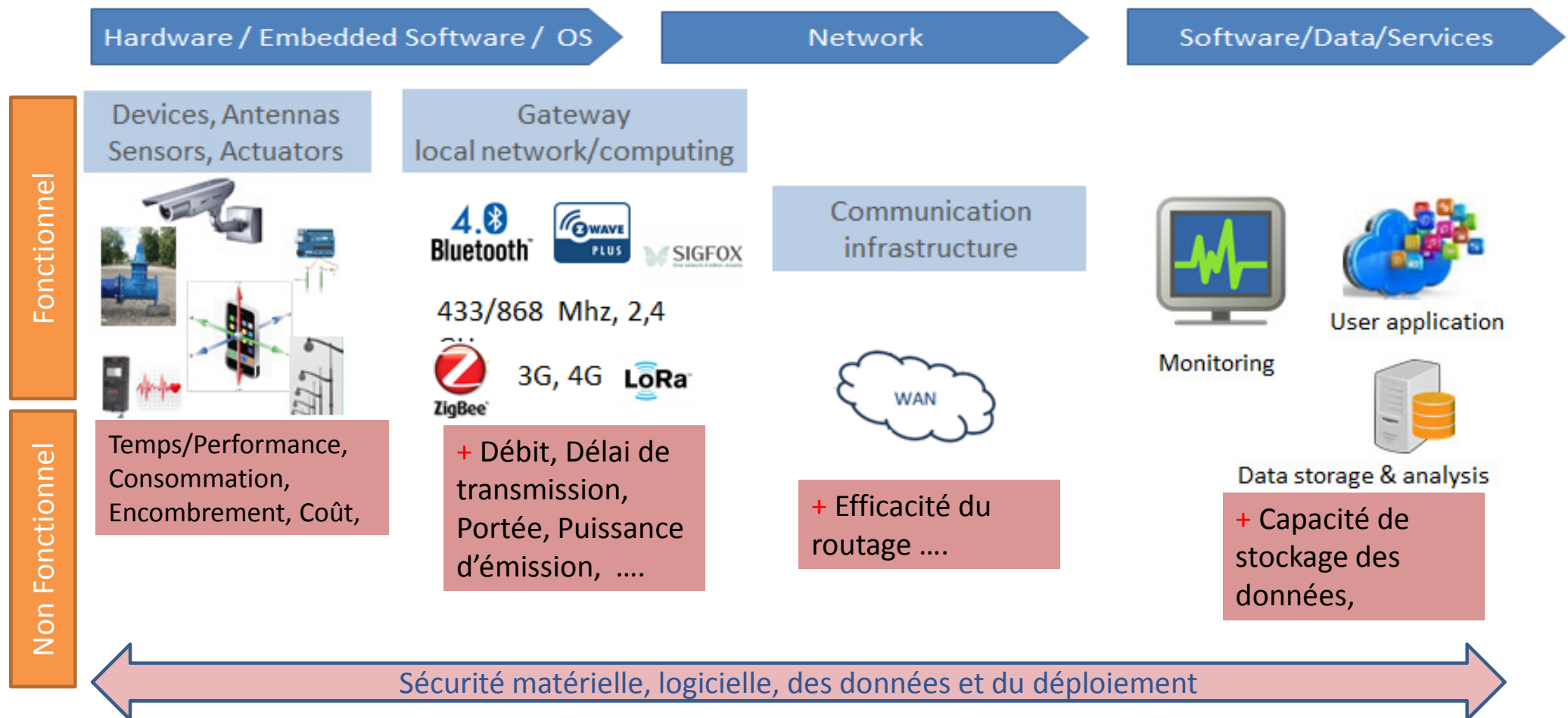
F. Mallet - M.A. Peraldi-Frati



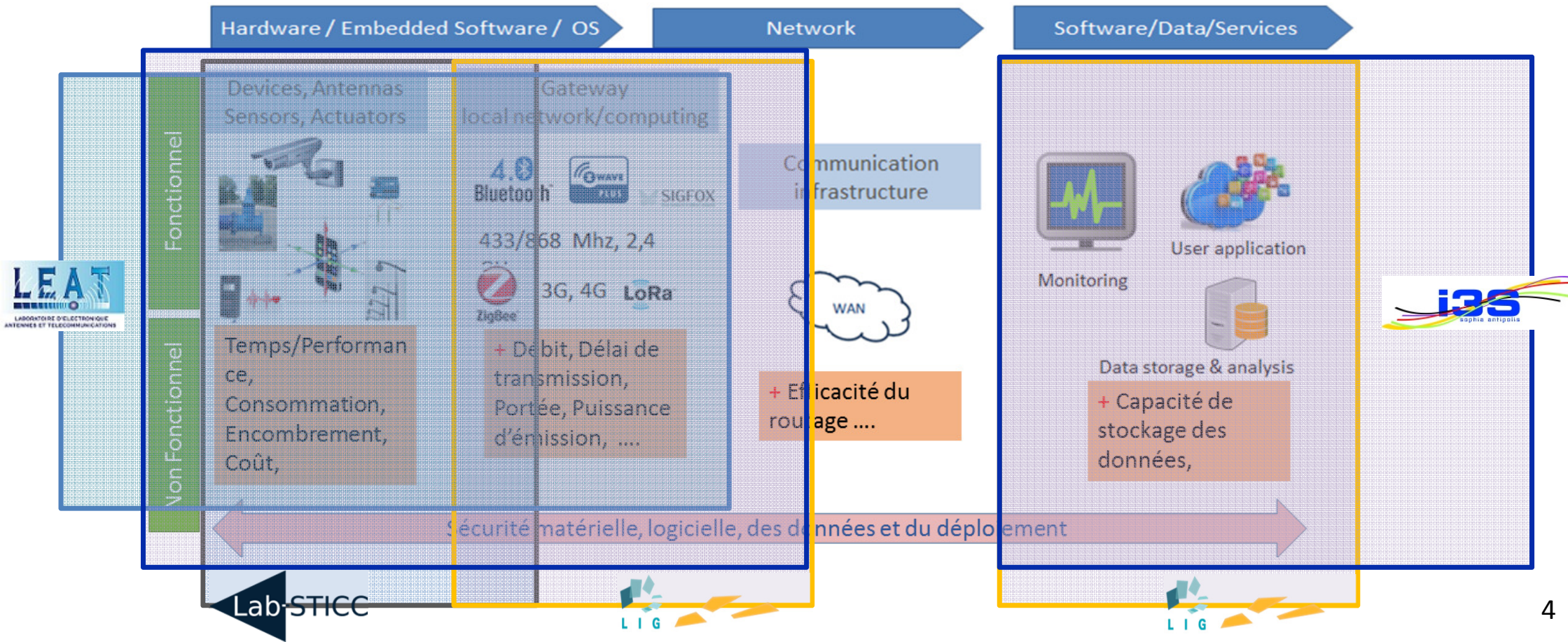
Contexte

- **Problématique : Approche système** (haut niveau) **pour**
 - La **conception de services** autour des Objets Connectés (aspects fonctionnels)
 - **Prise en compte** des contraintes (non fonctionnelles)
 - performance & consommation, plate-forme d'exécution
 - sécurité de bout en bout
 - **Validation/vérification** des systèmes
- **Projet PEPS** financé sur appel à projet exploratoire CNRS-INS2I – 2017
 - Cartographie des équipes de recherche sur le sujet (consortium ouvert)
- **Domaines** de déploiement de ces services :
 - **Industrie 4.0**: détection de courants de défaut (CC) dans réseaux électriques, suivi qualité de l'eau par réseaux de capteurs, maintenance prédictive
=> parfois avec mise en sécurité d'équipements, de personnes => **Systèmes Cyber Physiques**
 - **E-santé/Sociétal** : télémédecine préventive suivi de patient : remontée de données physio, analyse du comportement de patients, ...
 - **Automobile** : Voitures connectées, du XbyWire à la Sécurité/Fiabilité des voitures autonomes

Chaîne de valeurs des Objets Communicants Sécurisés



Couverture du consortium sur la Chaîne de valeurs des SOC's

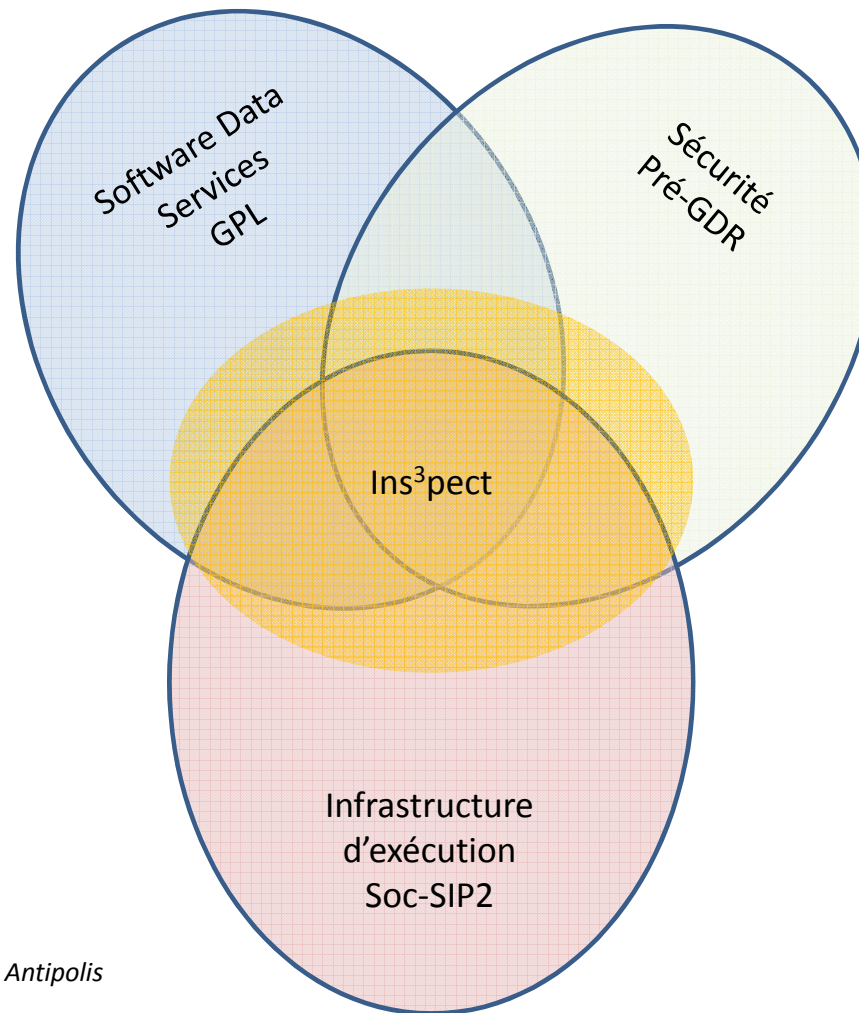


Positionnement du consortium

Domaines différents

Objets communicants sécurisés

- **CPS** /Intégration 
- **IoT**  
- **Smart grid** 
- **Usine 4.0** 



Ingénierie système :

- Ingénierie système
- Approche par modèles
- Vérification, Validation, Test

Objectifs du Workshop

1. Organisation en 3 sessions

Session3: Modélisation et Ingénierie des systèmes pour OC

- Intégration des exigences
- Simulation & analyse des options de conception
- Génération de solutions

2. Compétences transversales

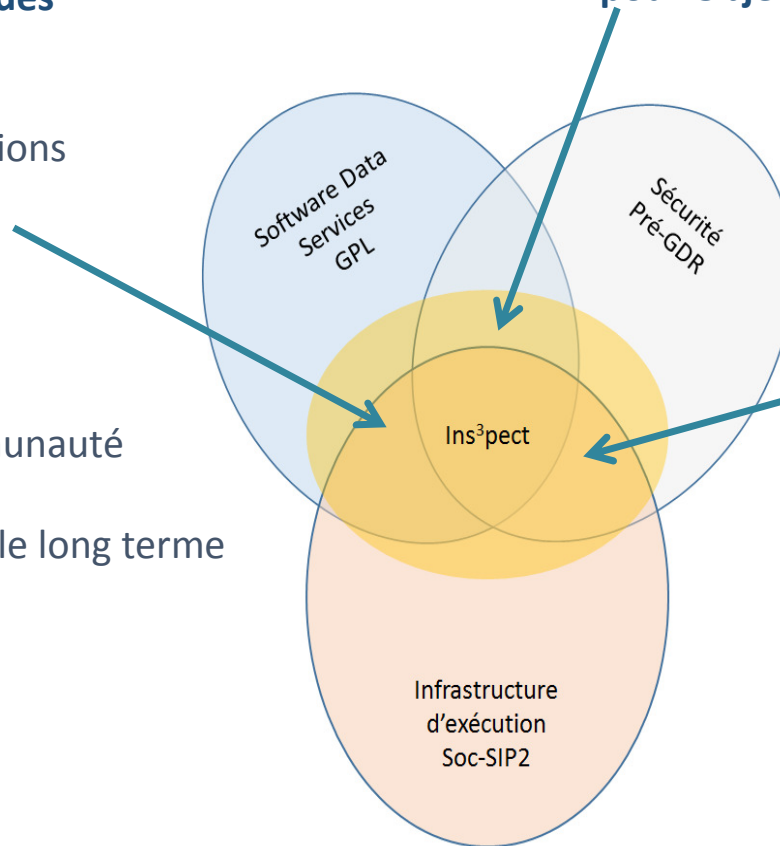
- Mesurer l'intérêt de la communauté académique et industrielle,
- Initier des collaborations sur le long terme

Session1: Sécurité des applications et services pour Objets Communicants

- Contraintes applicatives et des domaines
- Attaques /vulnérabilités applicatives

Session2: Sécurité des infrastructures de communication et d'exécution d'OC

- Sécurité firmware, protocoles
- Attaques /vulnérabilité du hardware & infrastructures
- Vérification et tests



Objectifs du Workshop

1. Organisation en 3 sessions

Session3: Modélisation et Ingénierie des systèmes pour OC

- Intégration des exigences
- Simulation & analyse des options de conception
- Génération de solutions

2. Compétences transversales

- Mesurer l'intérêt de la communauté académique et industrielle,
- Initier des collaborations sur le long terme

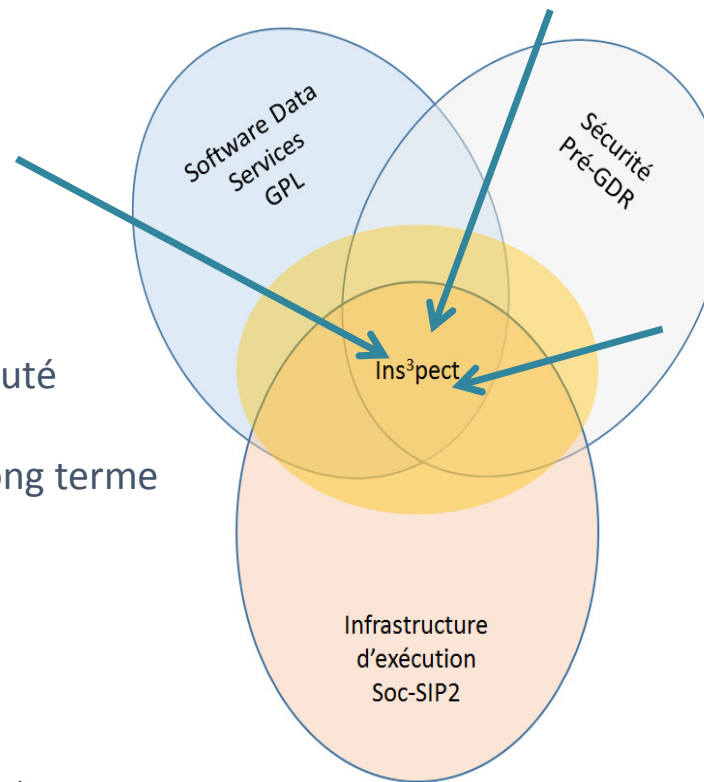
3. Rapprochement des compétences

Session1: Sécurité des applications et services pour Objets Communicants

- Contraintes applicatives et des domaines
- Attaques /vulnérabilités applicatives

Session2: Sécurité des infrastructures de communication et d'exécution d'OC

- Sécurité firmware, protocoles
- Attaques /vulnérabilité du hardware & infrastructures
- Vérification et tests





Enjoy the meeting !