Projet InS^{3}pect

Ingénierie **S**ystème de **S**ervices **S**écurisés **p**our objets connéc**t**és

Marie-Agnès Peraldi-Frati* – Robert de Simone**
*Université de Nice – Laboratoire I3S
**INRIA Sophia Antipolis
Equipe Projet I3S-INRIA KAIROS e

Contexte des Services Sécurisés pour Objets Connéctés (SOCs)

- **O**bjet **C**onnecté : dispositif mécanique et électronique à base de capteurs/actionneurs et de code informatique embarqué sur une plate-forme d'exécution communicante.
- Exemple de **S**ervices pour objets connectés :
- Industrie: détection de courants de défaut (CC) dans réseau électrique, suivi qualité de l'eau par réseaux de capteurs, repérage de fuite usines (capteurs radioactivité, caméra thermiques…), Maintenance prédictive,
  => parfois avec mise en sécurité de périmètres, d'équipements, de personnes => Systèmes Cyber Physiques
- E-santé: Outils de télémédecine préventive : remontée de données physio, analyse de comportement de patients maladie Alzheimer, …
- Sociétal: maintien à domicile des personnes âgées : détection de situations anormales en liens avec les aidants,…

Chaîne de valeurs des SOCs

Hardware / Embedded Software / OS → Network → Software/Data/Services

Fonctionnel

Non Fonctionnel

Devices, Antennas Sensors, Actuators

Temps/Performance, Consommation, Encombrement, Coût,

Gateway local network/computing

Bluetooth 4.0 · Z-WAVE PLUS · SIGFOX

433/868 Mhz, 2,4

ZigBee · 3G, 4G · LoRa

\+ Débit, Délai de transmission, Portée, Puissance d'émission, ….

Communication infrastructure

WAN

\+ Efficacité du routage ….

Software/Data/Services

Monitoring

User application

Data storage & analysis

\+ Capacité de stockage des données,

Sécurité matérielle, logicielle, des données et du déploiement

Sécurité matérielle, logicielle des données du déploiement

Sécurité par conception

- Objectifs de sécurité
- Analyse de menaces
- Mise en place de contre-mesures

Sécurité du matériel

- Attaques par réseaux cachés
- Attaques en fautes
- Attaques en cache
- Logiciel malveillant

Sécurité de l'infrastructure

- Usurpation d'identité : Authentification
- Attaques du contrôle d'accès
- Trous de sécurité : mise à jour du firmware

Sécurité des communications

- Sécurité des flots d'information
- Injection de trames : detection de signatures de trames
- Mécanismes de Cryptographie

Contextualisation du modèle de sécurité
Adaptation des solutions de sécurité aux menaces

Approche système des SOCs

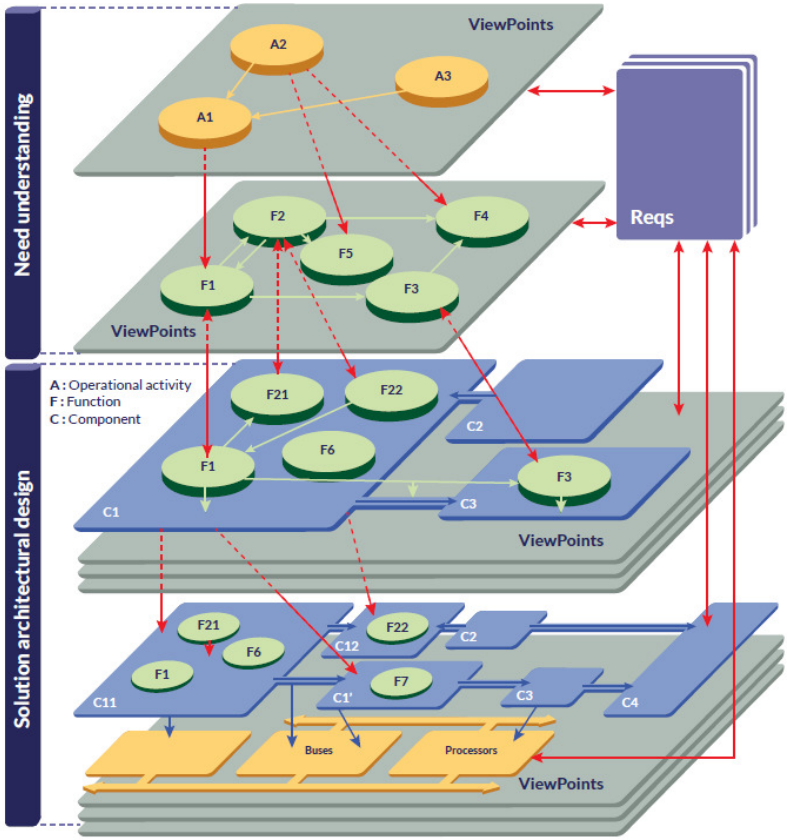
Approche d'ingénierie système

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

Quoi

Comment

Quel est le bon niveau d'abstraction au niveau système ?



MBSE Arcadia : Source thalès

Identification des Exigences

- Fonctionnelles
- Non fonctionnelles

Spécification fonctionnelles

- Dépendances
- Concurrence
- Raffinement

Spécification d'architecture

- Plate-forme d'exécution
- Mémoires, communication

Points de vue

- Propriétés non fonctionnelles
- Temps consommation, sécurité

Adéquation / Décision

- Allocation/mapping/
- Spatial + temporel (scheduling)

Verrous identifiés 1/4

Modélisation systèmes multi niveau des objets /services

- Architecture hiérarchique type *SCADA* ou systèmes ouverts
- Intégration aspects non-fonctionnels : *Performance*, *consommation, débit, sécurité*
  - Modélisation systèmes embarqués HW/SW, partitionnement/cloisonnement d'applications ***SysML, MARTE***
  - Modèle d'exigences sécurité, modèles d'attaques : ***SysML-sec***
  - Modèle de conception : contrôle d'accès aux données/ressources, boot sécurisé, ***SecureUML***
- Co-modélisation à partir de ces modèles hétérogènes
  - Format commun de description de MOCC =>modèle de langages exécutables
  - Modélisation de patterns de coordination ***Gemoc***

Verrous identifiés 2/4

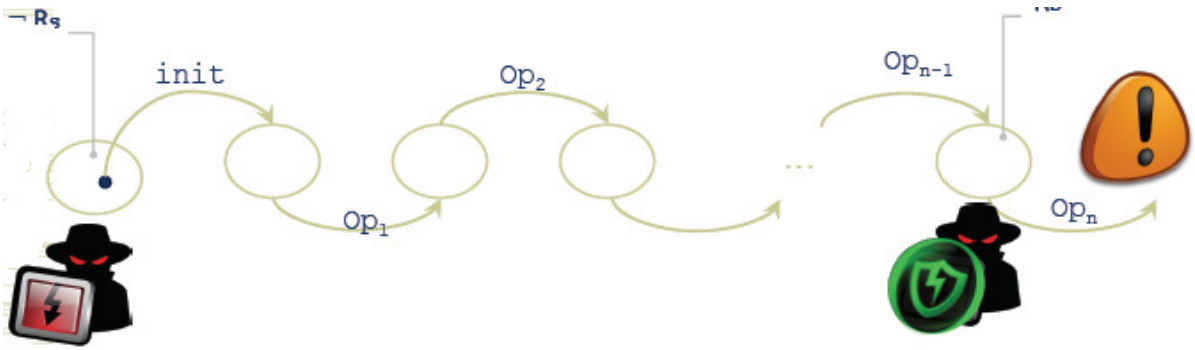
Exploration des alternatives de solutions de sécurité

- AAA^{++} : Adéquation Application Architecture
  - Calcul de solutions étendue aux modèles de sécurité.
- Calcul d'alternatives d'architectures
  - *Outil Timesquare* calcul d'ordonnancement basé sur le langage de contraintes d'horloges *CCSL*
  - *Outil PREESM* de prototypage rapide basé sur du Synchronous Data flow (modèles/algorithmes)

Verrous 3/4

Simulation et validation globale au niveau système

- Modèles exécutable/simulables => sémantique comportementale
- Vérification de la consistance entre les points de vues
- Analyse statique des modèles : USE , Secure MOVA
- Analyse comportementale : B4MSecure, GenISIS atteignabilité état
- Vérification de conformance de traces vs la spécification



Source figure Akram Idani - LIG

Verrous 4/4

Instanciation de l'approche pour domaine spécifique

- Adaptation des langages spécifiques aux domaines (notion de DSL - Domain Specific Language)
  - DSML : Definition de la syntaxe abstraite + notion d'état + tissage de règles comportementales
  - MoccML : modèle de concurrence et de temps (contraint le DSA)
  - DSA/MOCCML : Langage de contraintes basé sur des évènements
  - Génération de l'ensemble des ordonnancements (représentation symbolique) conformes aux règles sémantiques

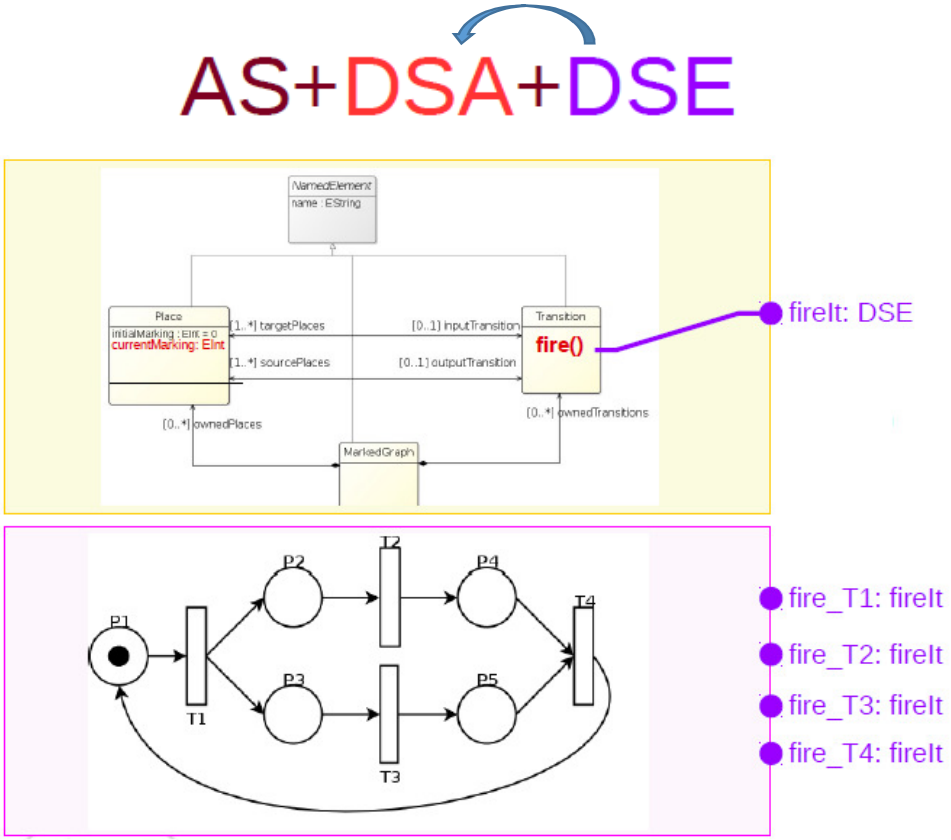
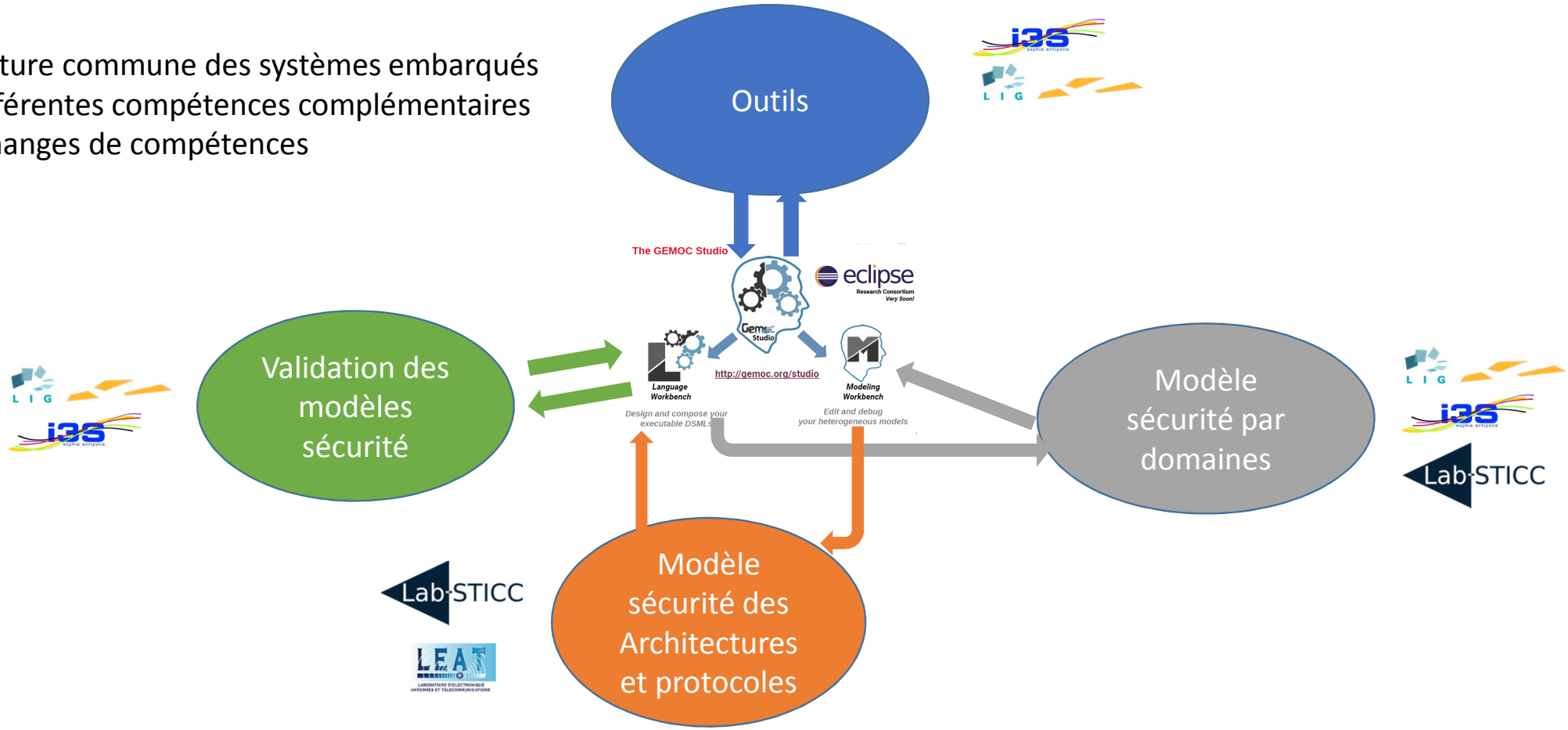


Figure Julien Deantoni – I3S

Complémentarité des partenaires

- Culture commune des systèmes embarqués
- Différentes compétences complémentaires
- Echanges de compétences



Conclusion

- Ins3pect
  - Modélisation/Simulation/Validation des Objets connéctés et leur sécurité
  - Consortium PEPS multi compétences, ouvert
  - Interactions avec GTs des GDRs (GPL, SOC^2, Sécu)

- Travaux en cours
  - Raffinement des verrous
  - Identification d'équipes intéressées de travailler sur ce
  - Organisation d'un workshop début décembre à Sophia pour :
    - Présenter les résultats des GT,
    - Mesurer l'intérêt de la communauté er des industriels,
    - Initier des collaborations plus long terme

Questions ?

- Contact
  map@i3s.unice.fr ou fmallet@unice.fr
- Web
  http://www.i3s.unice.fr/ins3pect/