Setting the Standard for Automation™

ISA France

ARAMIS : Un cloisonnement robuste par design pour les infrastructures critiques

Pascal Sitbon (Seclab, Cofondateur),
François Pébay-Peyroula (Atos Worldgrid Directeur de programme R&D)

En partenariat avec

WATERFALL Stronger Than Firewalls

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

SOGETI High Tech

HIMA SAFETY NONSTOP

ANSYS

sentryo

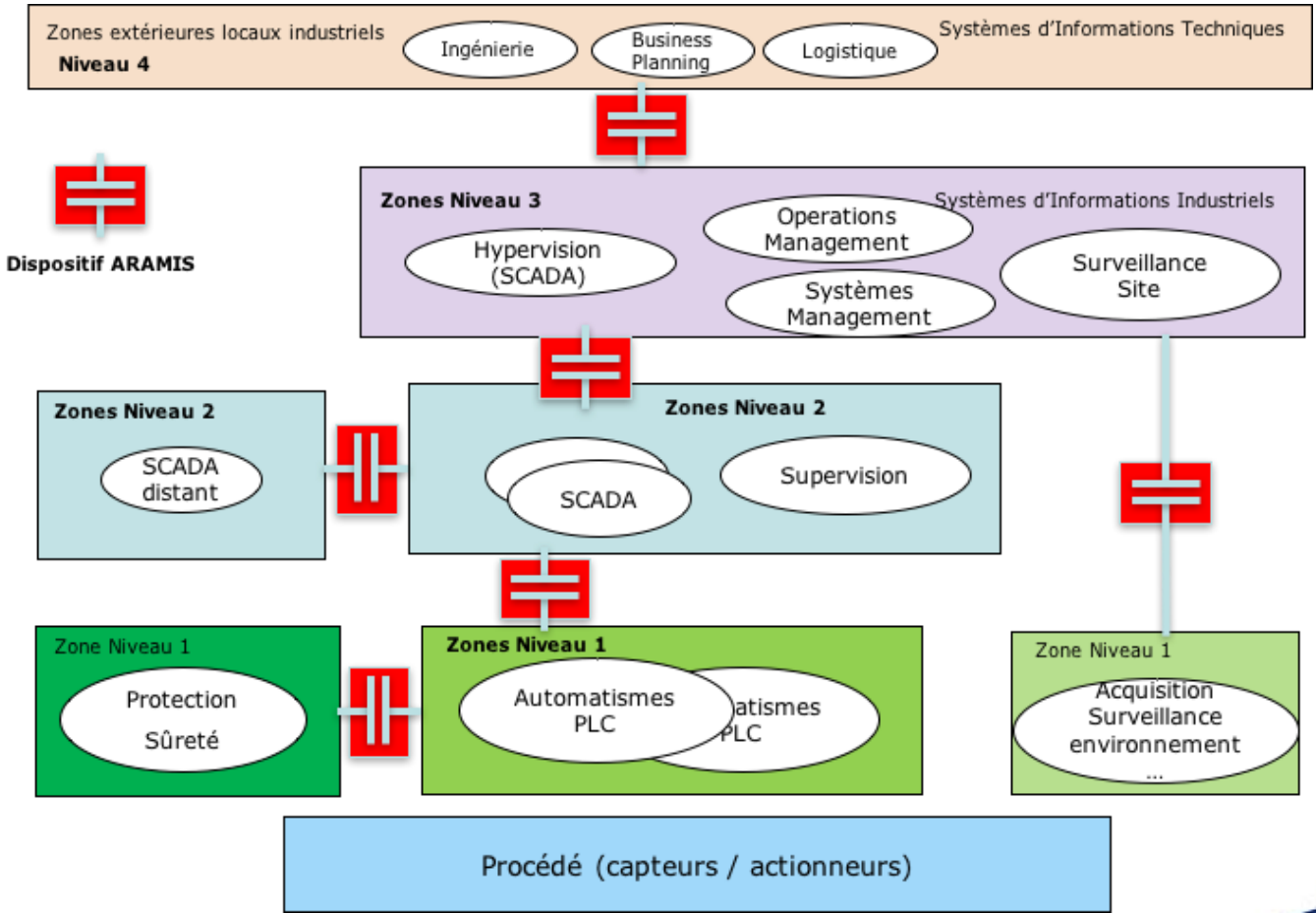
Cybersécurité et sûreté de fonctionnement
Villeurbanne –18 et 19 octobre 2016

Présentation consortium projet R&D ARAMIS

- Le consortium ARAMIS « Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles »
  - **Seclab** société innovante qui conçoit et commercialise une technologie unique de cloisonnement des réseaux
  - **Universités de Grenoble Alpes** pour l' expertise dans la cyber-sécurité (chiffrement, analyse vulnérabilités, preuves sécurité)
  - **CEA-Leti** comme référent sur les ancres de confiance et pour sa certification CESTI pour les composants
  - **Atos Worldgrid**, intégrateur de solutions de gestion intelligente de l'énergie, systèmes ICS / SCADA pour les Opérateurs d'Importance Vitale (OIV)
- Soutenu par l'ANSSI dans le cadre du Programme d'Investissements d'Avenir.

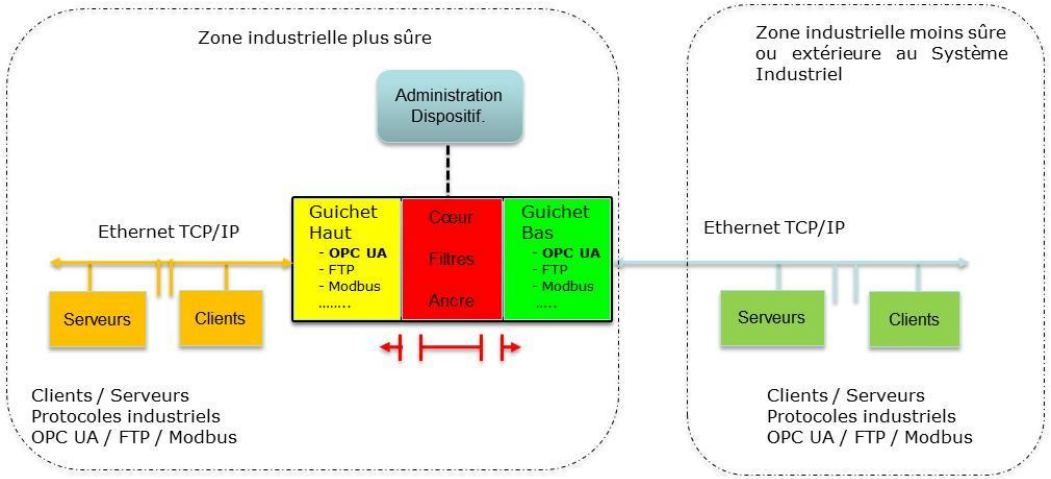
Positionnement ARAMIS dans architecture de systèmes industriels

- ARAMIS : dispositif d'isolation par rupture permettant l'échange filtrée d'informations entre réseaux de niveau de sécurité différents
- Prototype industriel mi 2017



Principe d'ARAMIS

- Différents dispositifs d'isolation :
  - Pare-feu : solution logicielle de filtrage de trafic réseau, difficile de faire du filtrage très sélectif dans le domaine industriel
  - Diode réseau : autorise physiquement la circulation d'information dans un seul sens, mais pas d'acquit des envois, ne protège qu'un sens et qu'une propriété (confidentialité ou intégrité)
  - Rupture de protocole : flux bidirectionnel, copie contrôlée =>
- **ARAMIS : intrinsèquement sûr par conception**
  - Multi protocoles
    - OPC UA, FTP(S)..
  - Cœur :
    - Isolation physique et logique en rupture
    - Filtrage niveau métier
    - Ancre de confiance



Présentation Gamme de produits SECLAB

Enjeu : cloisonner de manière déterministe en protégeant confidentialité, intégrité et disponibilité de chaque zone

DENELIS : Passerelle d'échanges - solution d'infrastructures

Cloisonnement strict via un système de sas tout en assurant l'échange contrôlé. Rupture physique entre zones non connectées permettant l'échange d'information contrôlée en immunisant contre les attaques réseau.

SCOOP : solution mobile de protection contre les attaques USB

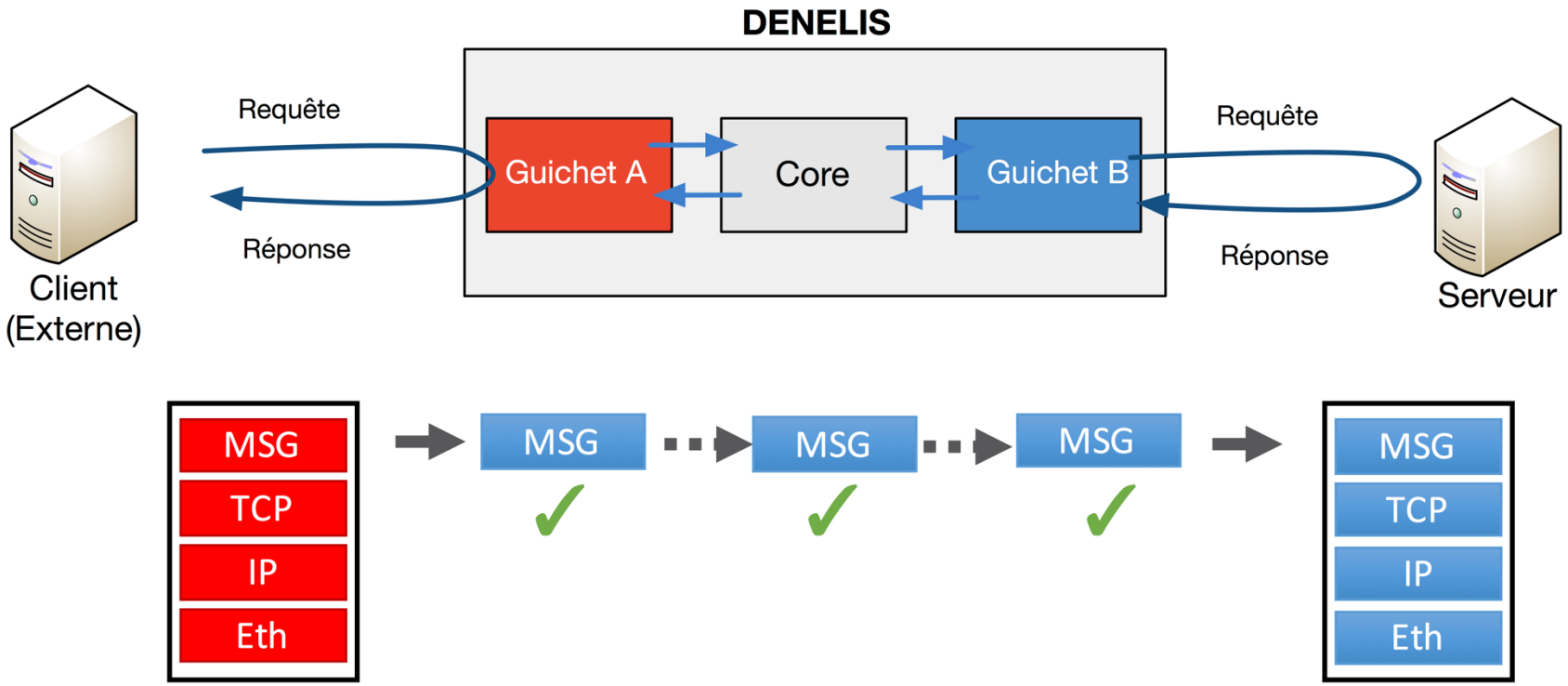
Filtre matériel destiné aux attaques USB. Rupture physique USB immunisant un poste contre les attaques USB sophistiquées (e.g. BadUSB, attaques HID, etc.).

BORNE DE DECONTAMINATION USB : Borne d'analyse antimalware immune à toutes les attaques USB bas-niveau. Solution autonome de décontamination de supports de stockage USB combinant sécurité hardware et software. La borne garantie l'innocuité du support de sortie, quel que soit l'état du support d'entrée.

Solution en partenariat avec Quarkslab.

- ✓ Protection des connectivités réseau et USB
- ✓ Protection déterministe (figé dans l'électronique)
- ✓ Breveté, 3 produits sont CSPN

Principe de fonctionnement du Denelis



Industrialisation de ARAMIS

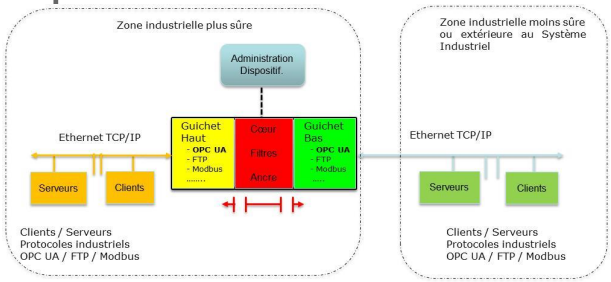
Des produits complémentaires partageant une base technologique avec Denelis

- Support de protocoles complexes et chiffrés (OPC UA)
- Filtrage métier paramétrable par l'administrateur
- Point unique de configuration sur le cœur
- Authentification forte des administrateurs
- Renforcement de la sécurité physique par une ancre de confiance
- Evaluation CSPN en cible

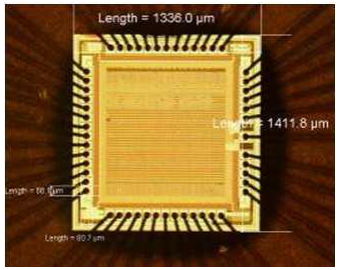
Points innovants / différenciant (1/2)

- Filtres métiers bidirectionnels configurables offline par une spécialisation du langage Python, ex :

```
MySrv  = OpcUaServer("10.0.0.1")
MyCli  = OpcUaClient("10.1.0.2 ")
MyFlux = OpcUaChannel(MySrv, Mycli)
MyFlux.enableRead().enableWrite (MyVar1)
```



- Chargement sécurisé de la configuration « compilée et vérifiée » dans le cœur, principe de liste blanche (autorisation explicite)
- Tout le logiciel est embarqué dans les 3 composants électroniques : le cœur et 2 guichets
- Ancre de confiance basée sur une approche hybride composants sécurisés / composants classiques
  - Pour un compromis sécurité/performances optimal
  - Coffre fort de secrets (certificats, clés privées)
  - Support des algorithmes de crypto asymétriques
  - Interfacée selon PKCS11 avec mode multi utilisateurs



Points innovants / différenciant (2/2)

- Cryptographie : support des mécanismes standards AES, RSA, ECC
  - Symétrique pour les échanges temps réel
  - Asymétrique pour les hand checks
  - Niveau de sécurité élevé des clés

- Identification, authentification forte
  - Par certificats X.509 pour une sécurité à base de PKI (Public Key Infrastructure)
- Chaine totalement sécurisée de bout en bout
  - Entre clients et serveurs via les guichets d'ARAMIS
  - Echanges OPC UA, FTP sécurisés, seul le cœur voit les informations métiers en clair pour les filtrer.
- Un bastion imprenable et fail secure :
  - Défense en profondeur : cœur derrière les guichets
  - Secrets et intégrité du cœur protégé par l'ancre de confiance
  - Cœur ferme le dispositif si risque de compromission

Conclusion : dilemme de concilier sécurité et sûreté dans un contexte industriel

- Disponibilité (ne pas arrêter) versus sûreté (fail safe)
- Liste blanche (autoriser) versus liste noire (interdire)
  - *Les solutions sont dans la configuration du boitier*

- Sécurité difficile à installer / opérer / maintenir (gestion des certificats)
  - *Il n'y a pas de renforcement de sécurité gratuit mais cela se procédure et s'automatise en partie*

- Difficulté de « certifier sûreté » les mécanismes crypto
  - *RGS 2.0, ANSSI, mais démonstration complexe pour des niveaux de sûreté SILx*
- Attention aux « single point of failure » (e.g. LDAP, PKI centralisée)
  - *Sécuriser l'architecture ICS, pas seulement le boitier*

- Que faire si problème ? Fail Safe => débrayage manuel => pas sécure

Merci de votre attention

Plus d'information :

- http://www.seclab-solutions.com (produits Seclab)
- https://atos.net/fr/2015/communiques-de-presse/communiques-generaux_2015_05_28/pr-2015_05_28_01 (communiqué de presse ARAMIS)

- Pascal Sitbon (Seclab) : psitbon@seclab-solutions.com
- François Pébay-Peyroula (Atos Worldgrid) : francois.pebaypeyroula@atos.net