RESSI 2017 Autrans 18/05/2017

ARAMIS : Un cloisonnement robuste par conception pour les infrastructures critiques

- **François Pébay-Peyroula (Atos Worldgrid)**
- Xavier Facélina (Seclab)
- Jean-Louis Roch (Universités Grenoble-Alpes)
- Florian Pebay-Peyroula (CEA Leti)

Atos Worldgrid cea Université Grenoble Alpes seclāb

Consortium projet R&D ARAMIS

Une alchimie innovante entre industriels et laboratoires

- Le consortium ARAMIS « Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles »
  - **Atos Worldgrid**, intégrateur de solutions de gestion intelligente de l'énergie, systèmes ICS / SCADA pour les Opérateurs d'Importance Vitale (OIV) - leader
  - **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
- Soutenu par l'ANSSI dans le cadre du Programme d'Investissements d'Avenir
- Financé par la BPI

Atos Worldgrid cea UNIVERSITÉ Grenoble Alpes seclāb

Atos Worldgrid et cybersécurité industrielle

- Une certification ISO 27001
- Une infrastructure support (sites sûrs, programme CHESS, PKI)
- Le support d'un groupe Atos/Bull et de ses produits

  chiffreurs, PKI, HSM, CardOS smart cards

- Compréhension des métiers pour OIV (domaine nucléaire , transport, distribution électrique, O&G…)
- Application des normes : CEI 62443, CEI 62645, CEI 62351, ANSSI,..
- Une participation active aux groupes de travail cybersécurité industrielle ANSSI
- Des programmes de R&D
- Une communauté d'experts
- Des références
- Une volonté d'investissement dans le domaine cybersécurité

Atos Worldgrid cea UNIVERSITÉ Grenoble Alpes seclāb

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
- ✓ Historique EDF
- ✓ Fabrication en France
- ✓ Cible OIV / systèmes critiques

Atos Worldgrid — cea — Université Grenoble Alpes — seclāb

Univ. Grenoble-Alpes – équipe-action SCCyPhy

- SCCyPhy *Security and Cryptology for CyberPhysical systems*
  - Communauté d'experts en cybersécurité de 7 laboratoires à Grenoble (CNRS, Inria, Grenoble-INP, UGA)
    - Institut Fourier (crypto), LIG (system&network security), LJK (crypto, PKI), TIMA (hardware), Verimag (modèles et preuves), GIPSA-Lab (multimedia), Inria (privacy)
  - De la crypto au matériel en passant par attaques et preuves

- Contributions à ARAMIS :
  - Rupture protocolaire, filtrage et isolation (LIG, Verimag)
  - Cryptographie (dimensionnement, ECDLP) (IF)
  - Architecture de sécurité (certificats) (LJK)
  - Modèles d'attaques (Verimag)
  - Analyse de logs et inférence de règles (LIG)

Atos Worldgrid cea UNIVERSITÉ Grenoble Alpes seclāb

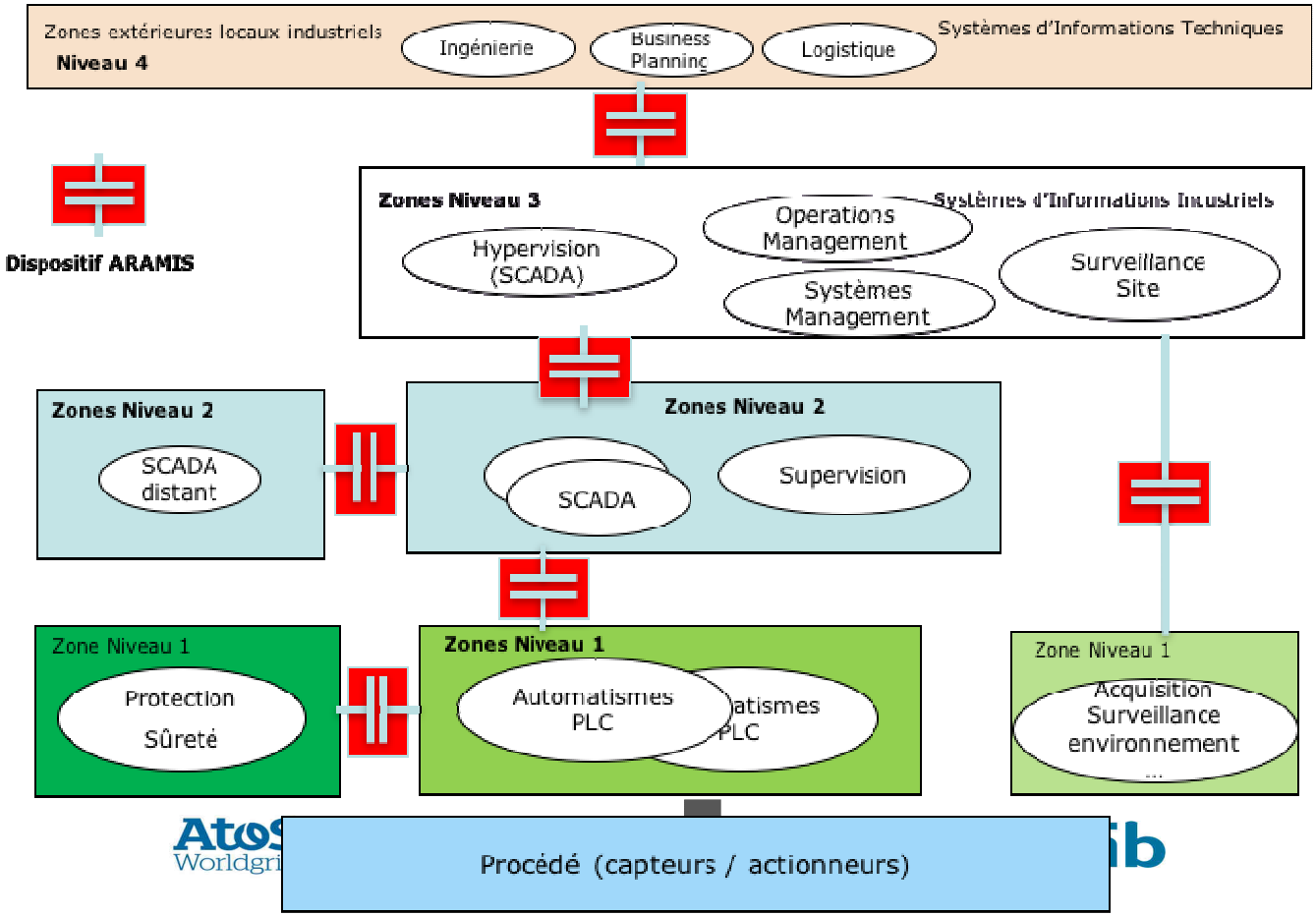
CEA-Leti

- Equipe impliquée
  - Service Sécurité des Systèmes et d'Evaluation des Composants
    - Recherche et développement en Sécurité des Objets et Systèmes cyber-Physiques
    - Evaluation et certification sécuritaires (CESTI)
- Contribution à ARAMIS
  - Ancre de Confiance de sécurité matérielle

Atos Worldgrid cea UNIVERSITÉ Grenoble Alpes seclāb

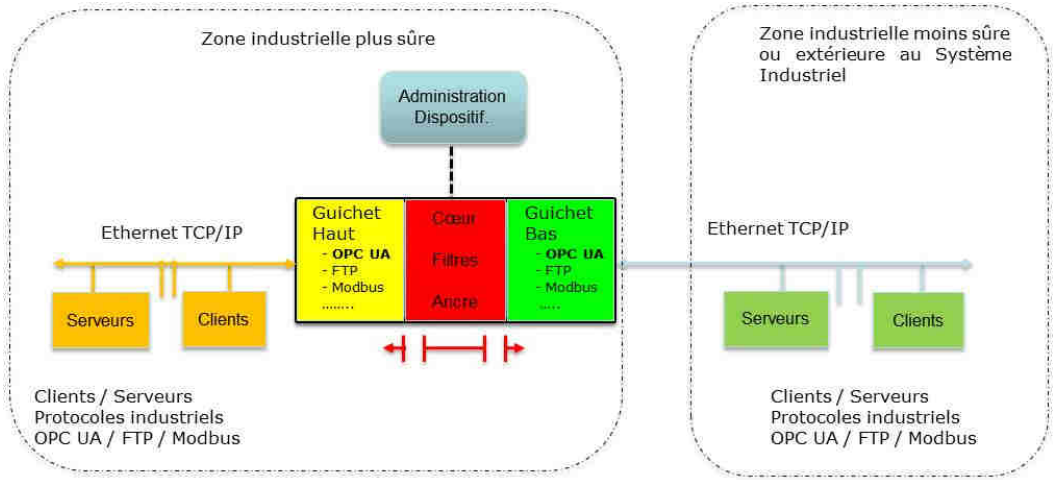
Positionnement ARAMIS dans architecture de systèmes industriels

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

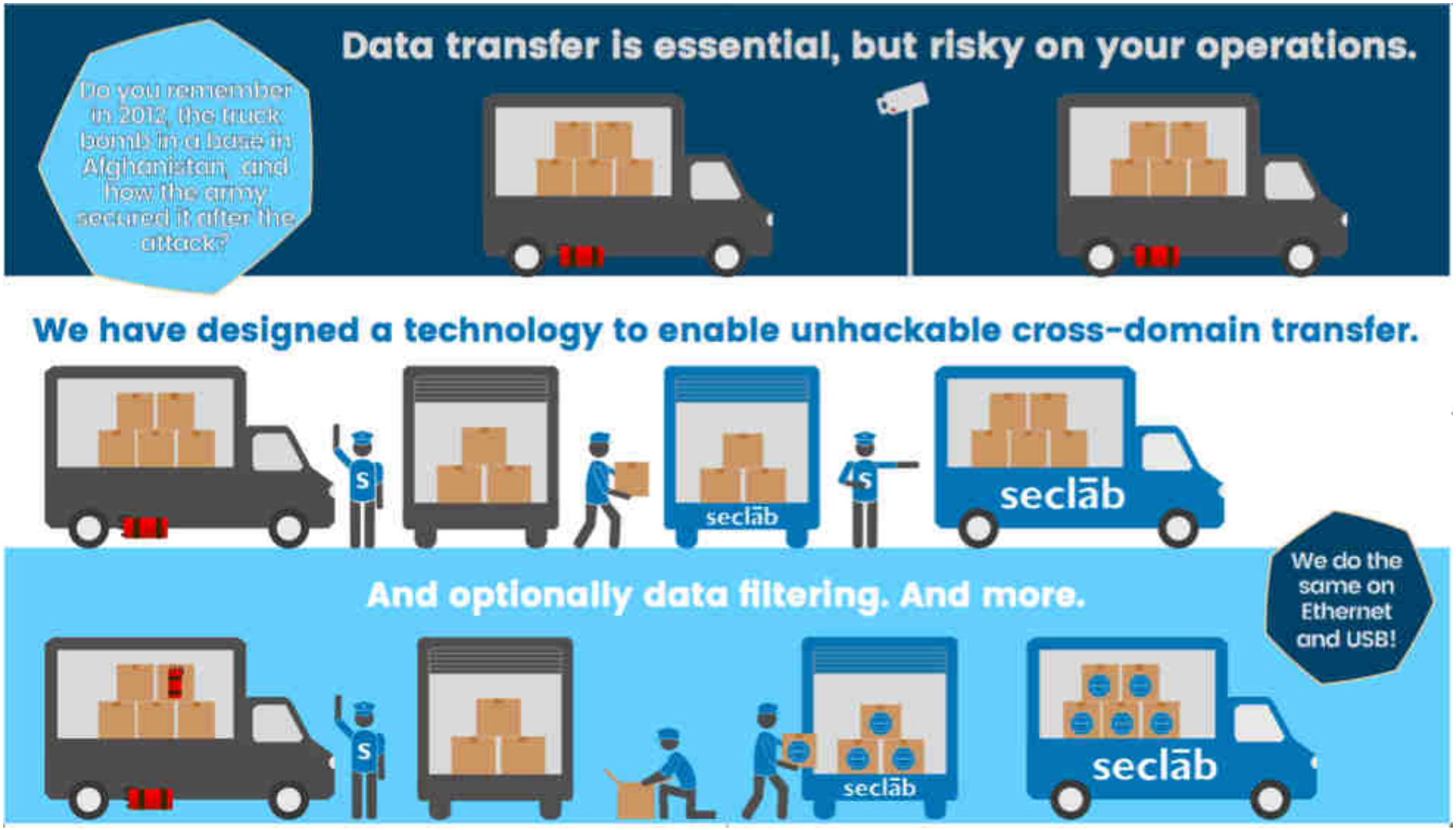


Principes d'ARAMIS

- Différents dispositifs d'isolation existants :
  - Pare-feu : solution logicielle de filtrage de trafic réseau, difficile de faire du filtrage très sélectif dans le domaine industriel, modes communs HW, OS, pile réseau
  - Diode réseau : autorise physiquement la circulation d'information dans un seul sens, mais pas d'acquit des envois, ne protège qu'un sens, mode commun pile réseau
- **ARAMIS : intrinsèquement sûr par conception**
  - Rupture physique et protocolaire avec introspection de la charge :
    - flux bidirectionnel,
    - copie contrôlée
    - Multi protocoles
      - OPC UA, FTP(S), Modbus
    - Cœur :
      - Isolation physique et logique en rupture
      - Filtrage niveau métier
      - Ancre de confiance

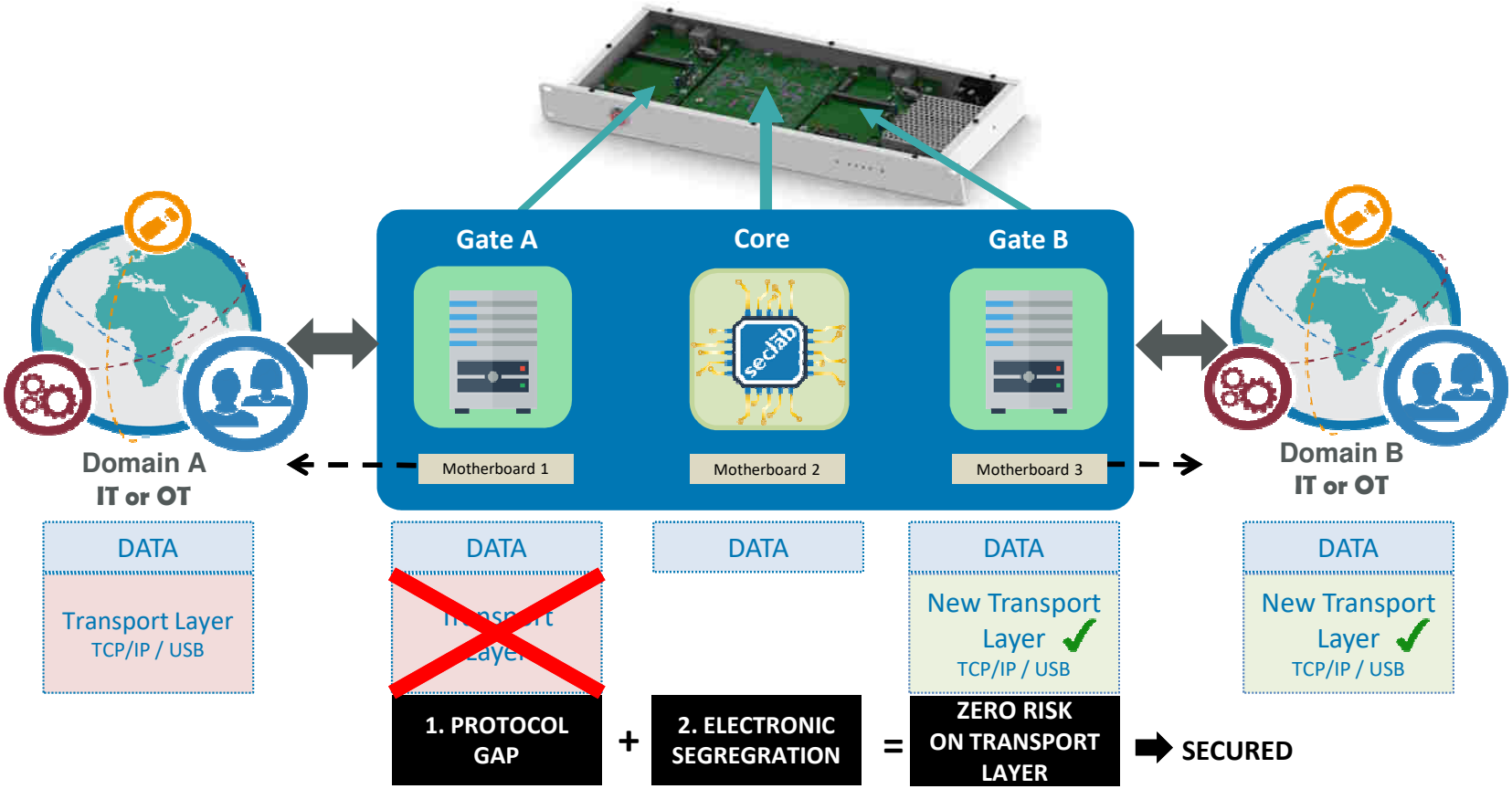


Principe de fonctionnement du Denelis (et Aramis)



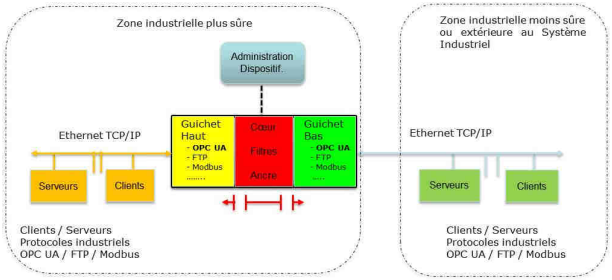
Atos Worldgrid cea Université Grenoble Alpes seclāb

Principe de fonctionnement du Denelis (et Aramis)



ARAMIS : Points innovants / différenciants (1/3)

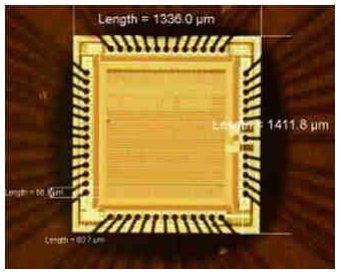
- Une architecture interne en zones matérielles / logicielles : le cœur et 2 guichets
- Une analyse technique et métier des flux
- Filtres métiers bidirectionnels configurables hors ligne par une API du langage Python, ex :




```
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)

- 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



Atos Worldgrid cea Université Grenoble Alpes seclāb

ARAMIS : Points innovants / différenciants (2/3)

- Cryptographie : support des mécanismes standards AES, RSA, ECC et spécifiques ECC
  - Symétrique pour les échanges temps réel
  - Asymétrique pour les hand checks
  - Niveau de sécurité RGS 2.0

- Identification, authentification forte
  - Par certificats X.509 pour une sécurité à base de PKI (Public Key Infrastructure)
- Chaîne 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 sécurisé et fail secure :
  - Défense en profondeur : cœur derrière les guichets
  - Secrets et intégrité du cœur protégés par l'ancre de confiance
  - Cœur ferme le dispositif si risque de compromission

Atos Worldgrid cea Université Grenoble Alpes seclāb

Points innovants / différenciants (3/3)

- Structure d'accueil pour nouveaux protocoles
- Garantie forte de l'authentification des composants logiciels, des communications et de l'intégrité des traitements
- Participation à une architecture sécurisée par l'alimentation d'un SIEM avec des logs signés/chiffrés

Atos Worldgrid cea UNIVERSITÉ Grenoble Alpes seclāb

Industrialisation/commercialisation de ARAMIS

Le passage d'un prototype R&D à un produit

- Des renforcements sécurité
- Une fiche produit
- Le nécessaire de commercialisation
- Support d'autres protocoles industriels
- Authentification forte des administrateurs
- Renforcement de la sécurité physique par une ancre de confiance
- Evaluations ANSSI en cible

Atos Worldgrid cea UNIVERSITÉ Grenoble Alpes seclāb

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)
- http://aramis.minalogic.net/ (Site Aramis sur Minalogic)

- Xavier Facélina (Seclab) : xfacelina@seclab-solutions.com
- Francois Pébay-Peyroula (Atos Worldgrid): francois.pebaypeyroula@atos.net
- Jean-Louis Roch (Grenoble Universités) Jean-Louis.Roch@imag.fr
- Florian Pebay-Peyroula (CEA Leti) florian.pebay@cea.fr