RTX RC Italy

Blockchain technologies integration for aerospace supply chain – Experiences from H2020-COLLABS project

Davide Martintoni – UTRC Italy
davide.martintoni@utrc.utc.com

Raytheon Technologies

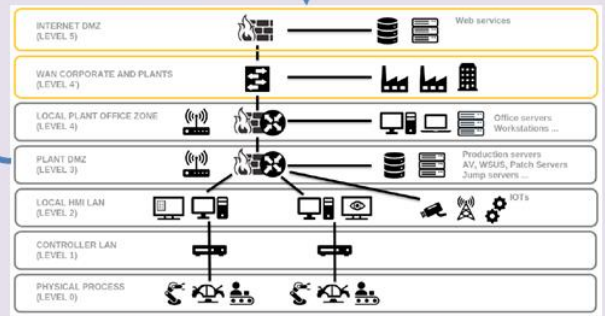
This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 871578

Agenda

- COLLABS intro
- Aerospace supply chain concept
- Supply chain mapping to HLF concepts
- Distributed environment for demonstration
- Future steps

COLLABS Objectives & Technology Overview

Collaborative Manufacturing Scope



Digital Manufacturing Infrastructures

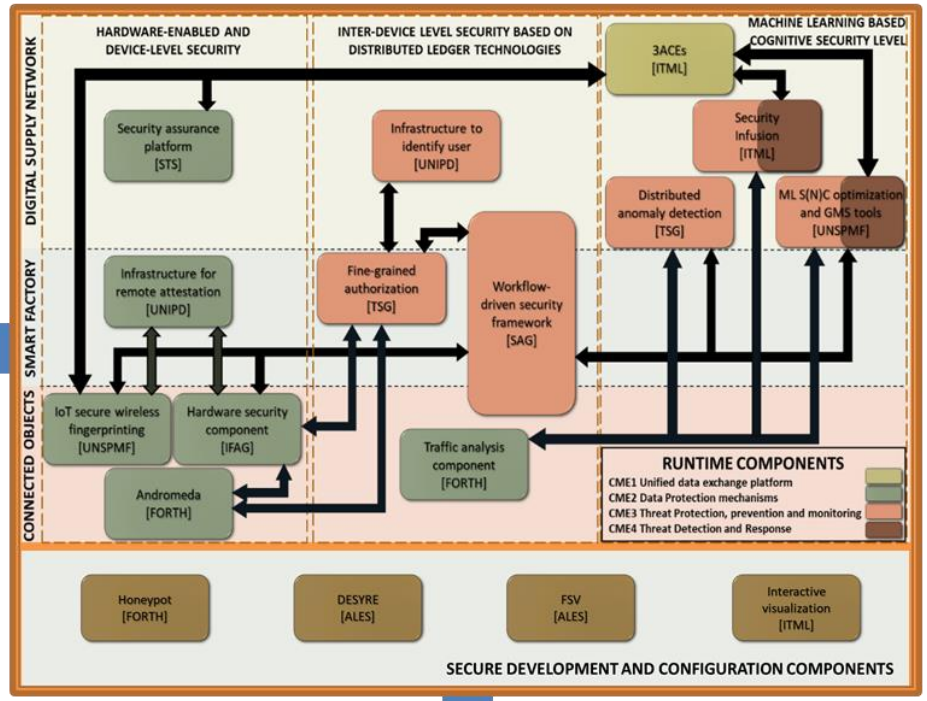
RENAULT · Pratt & Whitney · PHILIPS · AEROSPACE · AUTOMOTIVE · CONSUMER ELECTRONICS

3 Industrial Use Cases

COLLABS

- Unified Data Sharing
- Data Protection
- Threat Protection, Monitoring & Prevention
- Threat Detection, Mitigation and Response

Multi-layer cybersecurity solution



cea · FORTH · THALES · SIEMENS Ingenuity for life · infineon · ITML · HAROKOPIO UNIVERSITY · Raytheon Technologies

COLLABS comprehensive cybersecurity framework for collaborative manufacturing enables the secure data exchange across the digital supply chain while providing high degree of resilience, reliability, accountability and trustworthiness, and addresses threat prevention, detection, mitigation, and real-time response.

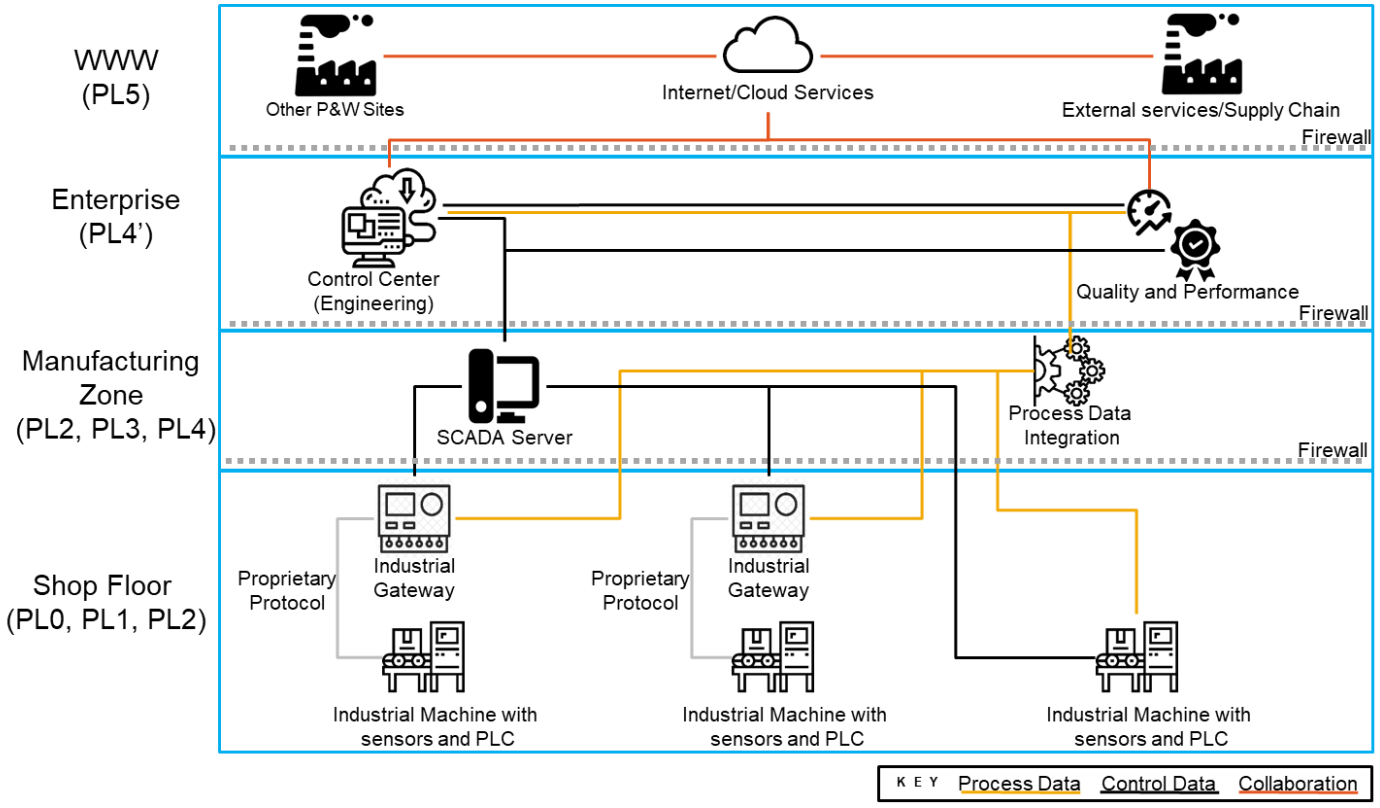
Raytheon Technologies

COLLABS Scenarios

RTX RC (P&W Inspired) Scenarios:

1. *Controlled and secure remote maintenance*
   - **Objective:** reduce as much as possible physical access to PW facilities for maintenance by enabling secure remote access from external companies, with data protection and strict access control guarantees
2. *Controlled Share of Compliance Data*
   - **Objective:** secure collection, storage and sharing of production compliance data (e.g. for quality checks) within P&W and 3rd-party service providers, with strong confidentiality, access control and data protection guarantees
3. *Trusted compliance data share across the supply chain*
   - **Objective:** secure collection, storage and sharing of production compliance data across the supply-chain, to support certification and auditing, with strong confidentiality, accountability and data protection guarantee
4. *Analysis of manufacturing performance at a global scale*
   - **Objective:** secure collection, storage and sharing of production performance data at global scale, for production optimization, with strong access control guarantees

(Simplified) Reference Architecture



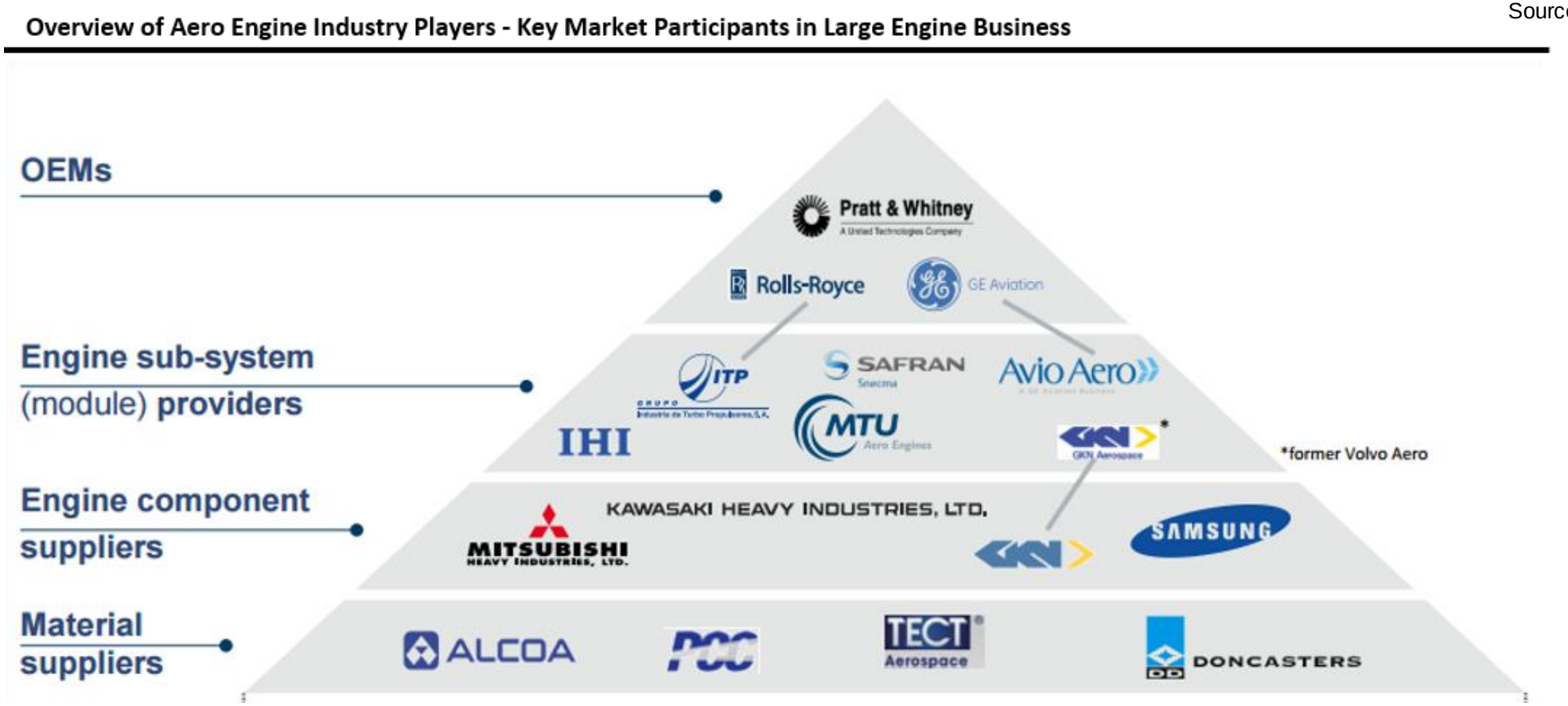
Initial scenario analysis:

- Security risk assessment
- List of minimum security requirements (a.k.a objectives)
  - Mapping to *NIST 800-171* and IEC 62443 family

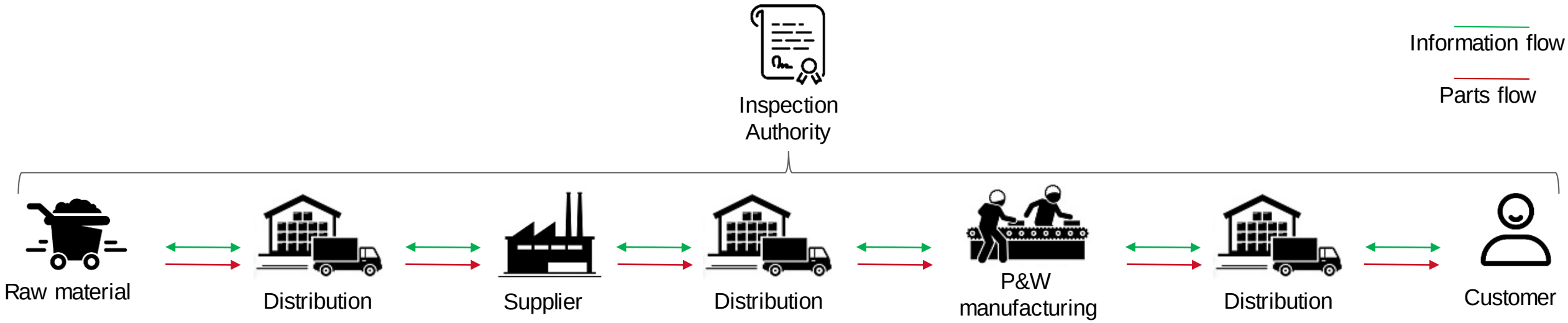
Raytheon Technologies

Supply Chain in Aero engine business

Source: seekingalpha.com



Supply Chain in Aero engine business



Raw material industry: provides primal matter. It receives an order from the supplier and provides the product with attached data

Distributor: provides logistic services. Receives orders to move goods from another company and provides details about it (e.g. tracking)

Supplier: provides parts to PW. It operates according to a request/contract and furnish detailed data about properties and production

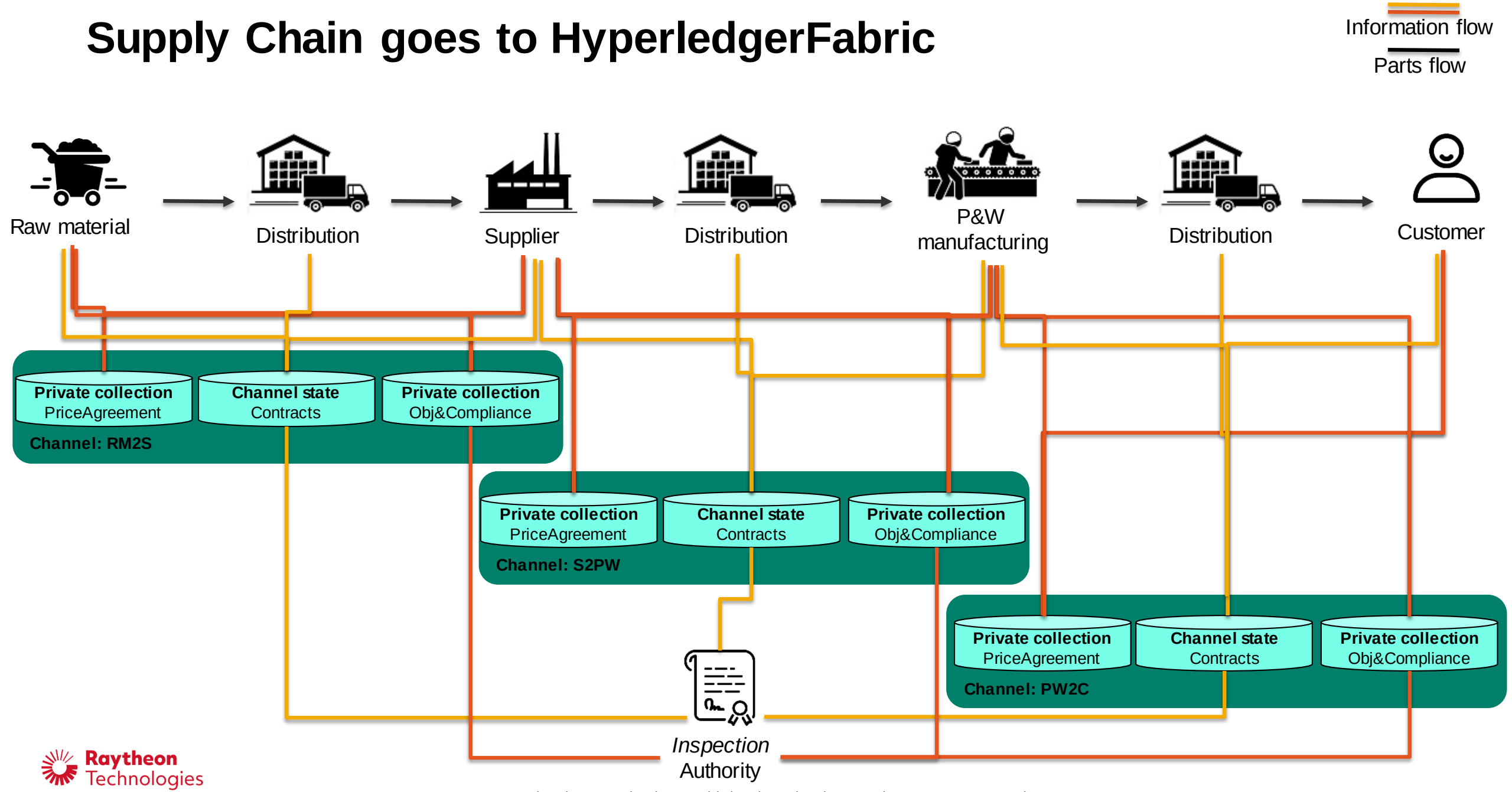
Pratt & Whitney: given orders from the clients, requests parts from supplier and manufacture a finished product which has attached conformity data

Customer: final user of the technology produced by the supply chain. It sign a contract and expect all the agreed requirements to be satisfied

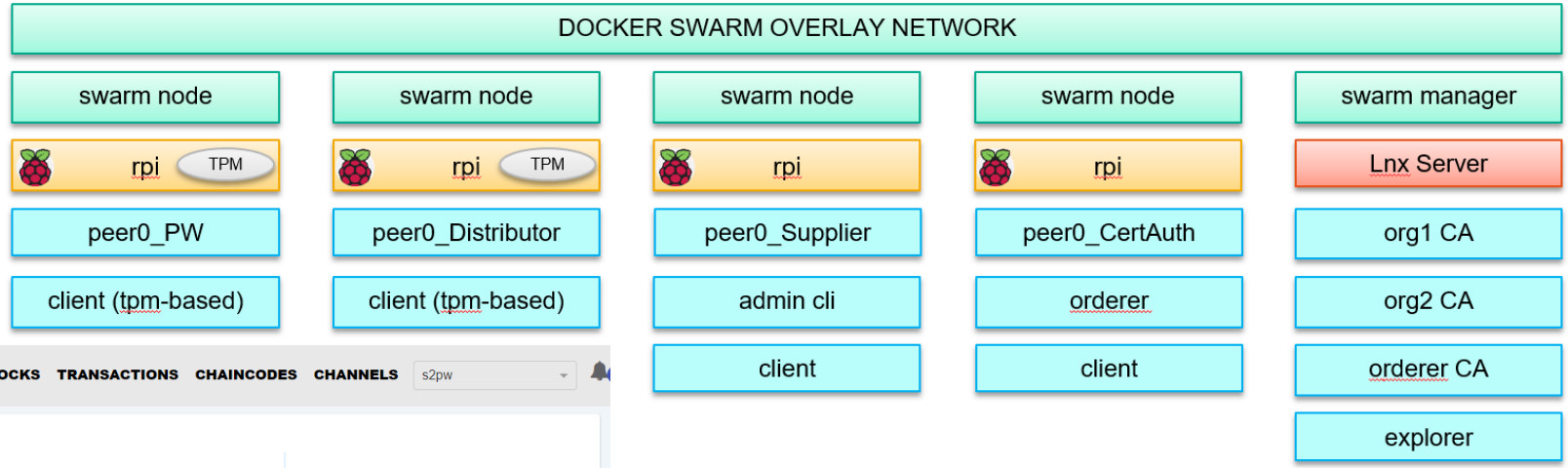
Inspection Authority: in the aerospace industry all the manufactured parts must be certified and respect strict safety requirements. The authority requires to inspect quality assurance data throughout the entire supply chain

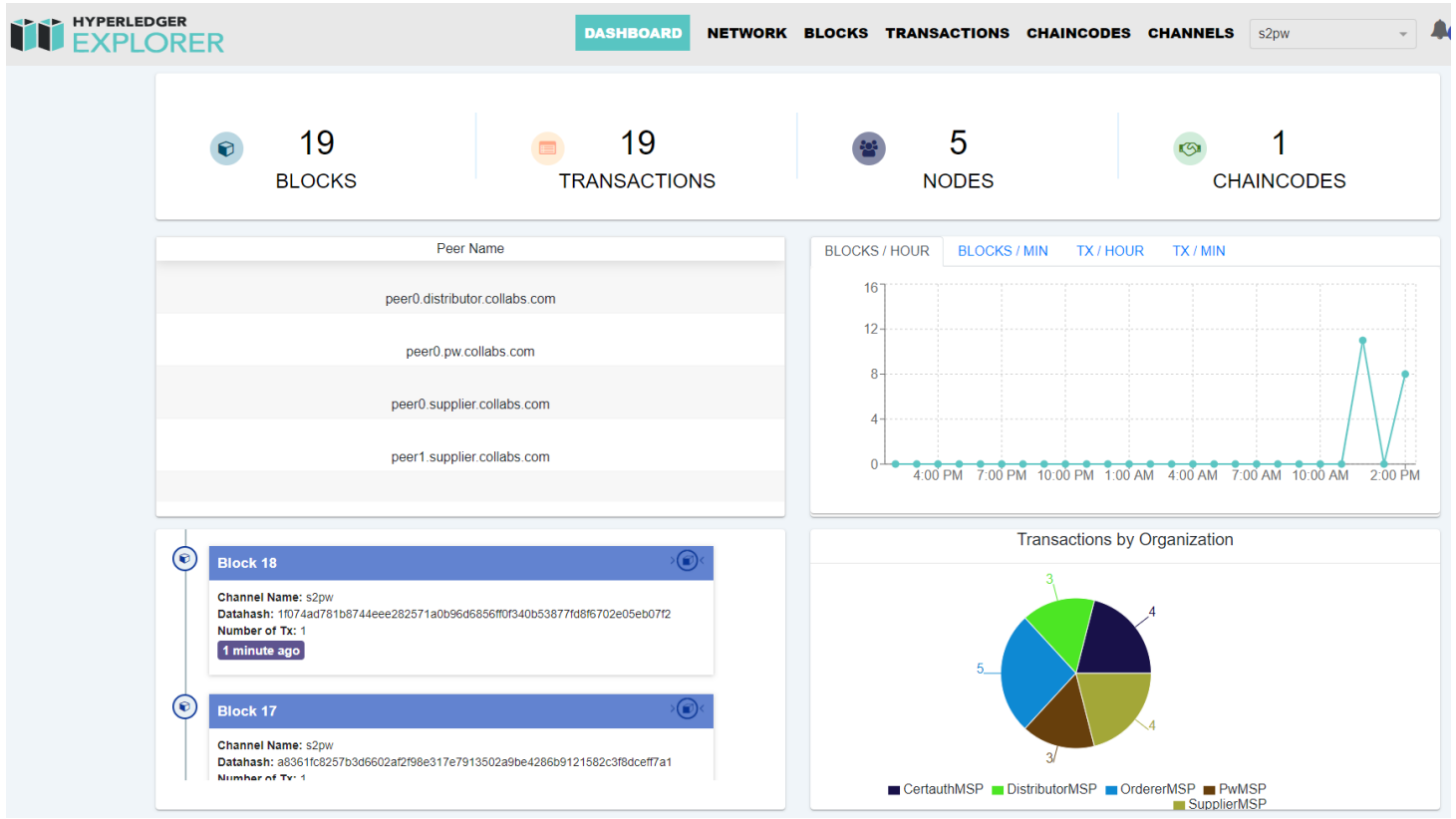
Raytheon Technologies

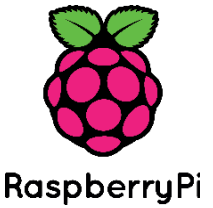
Supply Chain goes to HyperledgerFabric



Current setup





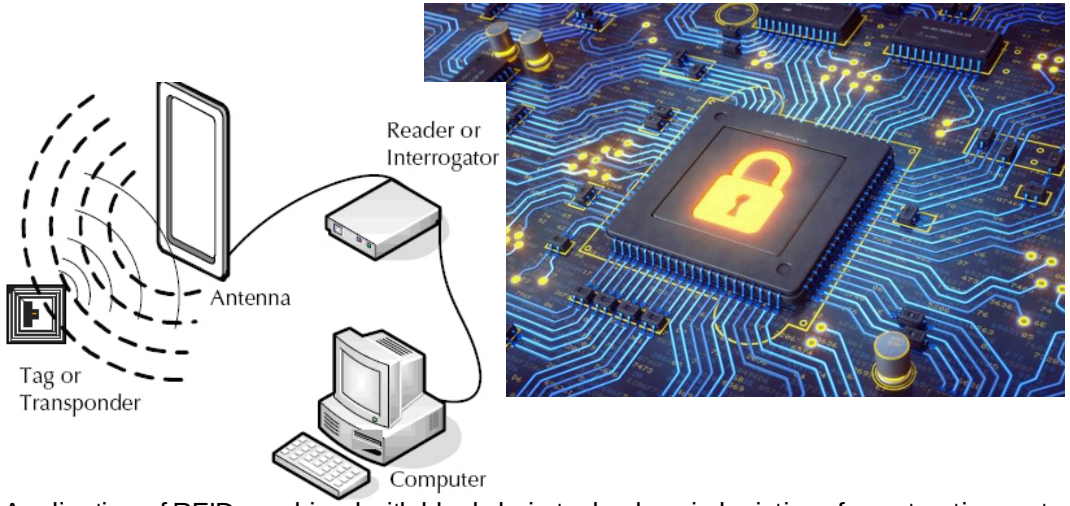


Raytheon Technologies

Future steps

Hardware security integration

- Stronger link between physical and digital world (e.g RFID/NFC tag) [1]
- Trusted computing integration with distributed ledger (e.g TPM as Root of Trust) [2][3][4]



[1] Application of RFID combined with blockchain technology in logistics of construction materials- Link
[2] Truxen: A Trusted Computing Enhanced Blockchain – Link
[3] Distributed IoT Attestation via Blockchain - Link
[4] Decentralized Trusted Computing Base for Blockchain Infrastructure Security - Link

Formal verification for Smart Contracts [1][2][3][4]

- Security properties
- Correctness
- Well-structured
- Concurrent guarantees

[1] Formal Verification of Smart Contracts ShortPaper – Link
[2] Formal verification of smart contracts based on users and blockchain behaviors models - Link
[3] Formal Verification of Workflow Policies for Smart Contracts in Azure Blockchain - Link
[4] A Concurrent Perspective on Smart Contracts - Link

Raytheon Technologies

Images Source: medium.com, wikipedia.com

Contact us

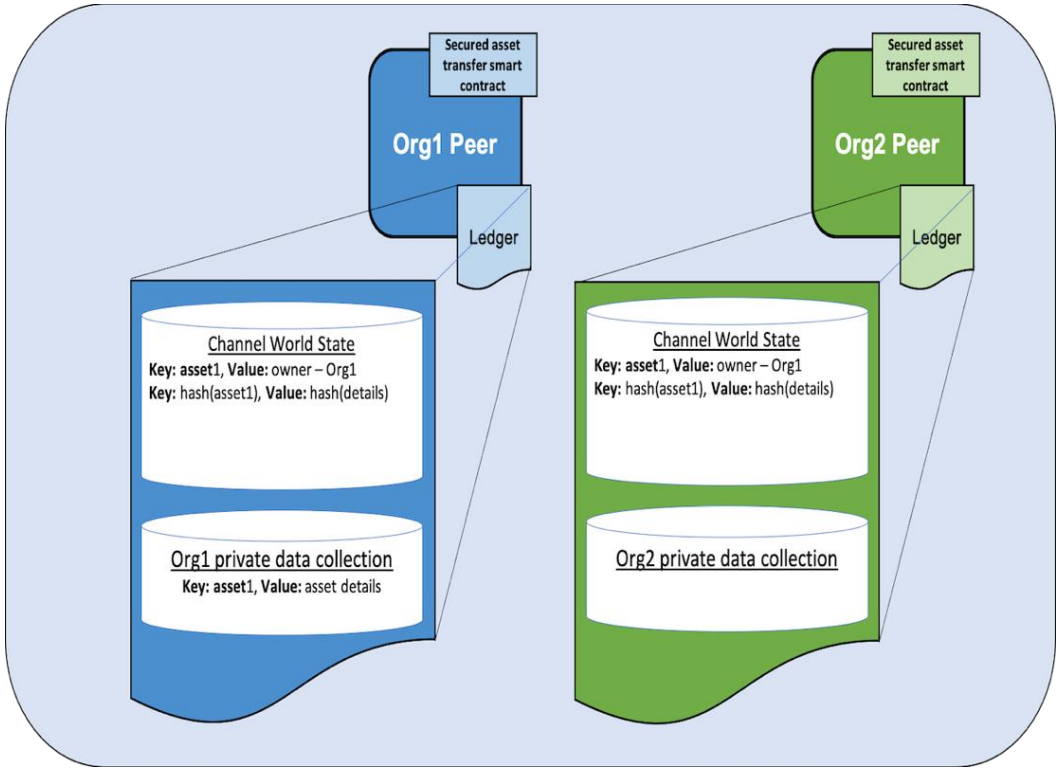
If you are interested in our projects and want to know more, please reach out to us we will happily talk with you!

davide.martintoni@rtx.com
valerio.senni@rtx.com

https://www.rtx.com/
https://www.collabs-project.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 871578

Channel vs PrivateData



Private data: it allows for use cases in which you want all channel participants to see a transaction while keeping a portion of the data private.

When to use a collection within a channel vs. a separate channel

- Use **Channels** when entire ledger must be kept confidential within a set of organizations (channel members)
- Use **PrivateData** when transactions must be shared among a set of organizations, but when only a subset of those organizations should have access to some (or all) of the data within a transaction

Raytheon Technologies

COLLABS Use Cases Overview

Raytheon Technologies

Pratt & Whitney

PHILIPS

RENAULT

Business	***defence***, ***aviation*** and ***aerospace***	***health technology*** and consumer/ ***household appliances***	***car*** manufacturer
Main objectives	Tools and approaches enabling sensitive data protection, cross-organizational access to assets and information sharing	Develop and evaluate tools and approaches for the detection and prevention of attacks against the manufacturing IT/OT network	Evaluate tools and security architectures supporting cloud-based Industrial IoT/Industry 4.0 use cases
Scenarios	1. Secure remote maintenance 2. Secure data sharing 3. Secure cloud-based data analytics	1. Shop floor threat detection and prevention 2. Secure data sharing	1. Secure remote maintenance 2. Secure cloud-based data analytics 3. Asset management and threat detection and prevention
Real-world test beds	Lab environment & evaluation with Pratt & Whitney Kalisz (PL) and the Italian site of the Research Center	Lab environment and Philips site in Drachten (NL)	Industry 4.0 Experimentation Lab with the option to evaluate in plants (FR)

Key requirements

Ensuring ***integrity*** and ***availability*** of assets (data and components), ***confidentiality*** of data as well as ***non-repudiation of activities*** in collaborative, cross-organisational workflows were identified as common key requirements. **8+ demonstration scenarios, 20+ system-level cybersecurity requirements**, sectorial best-practices and regulations included in the validation criteria.

Raytheon Technologies