Final Presentation

PROTECT AND ALLOW EXCHANGE OF MANUFACTURING DATA

PETER HAGSTROM (NEXOVA), NATHANAEL WYBOU (LABORELEC) & MICHAEL RAISON (SABCA)

Nexova

ENGIE Laborelec

SABCA

Background

Modern manufacturing, assembly, integration and test (MAIT) for spacecraft manufacturing is increasingly more reliant on digitalization

- Industry 4.0
- Advanced manufacturing methods (e.g., additive manufacturing, cloud and distributed manufacturing, …)

Data and physical realms more exchangeable and in the focal point of threat actors

Nexova

ENGIE Laborelec

SABCA

MAIT – Industry

Specifications and Design to Cost

Mechanical Manufacturing

Electronic Manufacturing

Surface Treatment

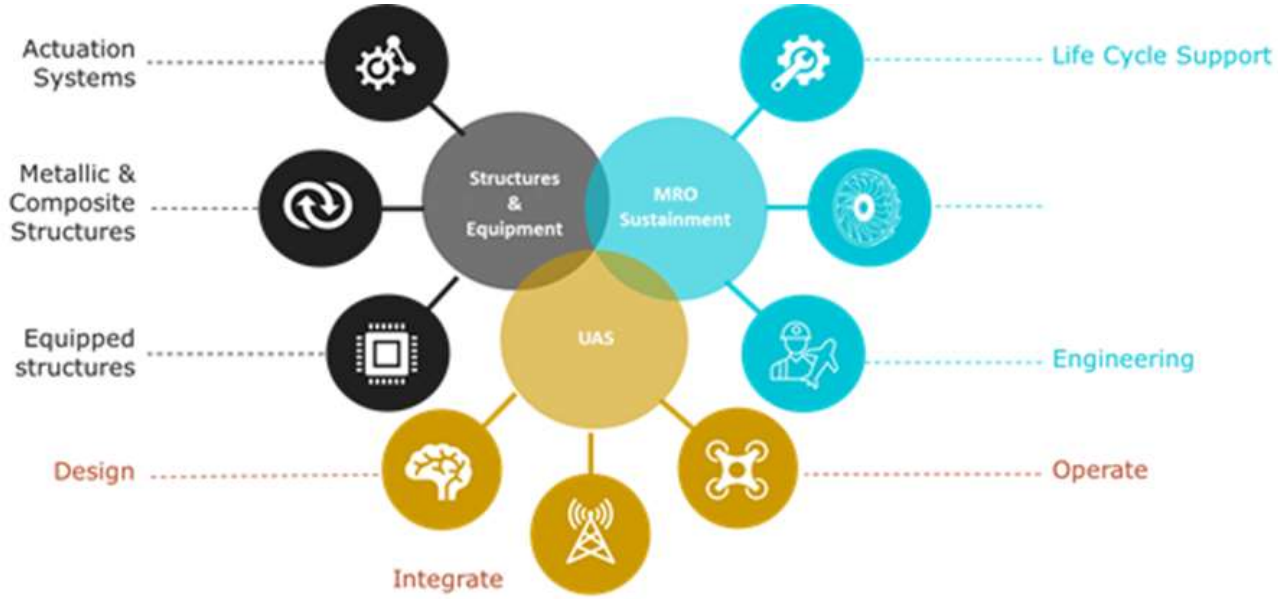
Software

Assembly

Aerostructure equipping

Testing and Qualification

Maintenance and Upgrade



Nexova

ENGIE Laborelec

SABCA

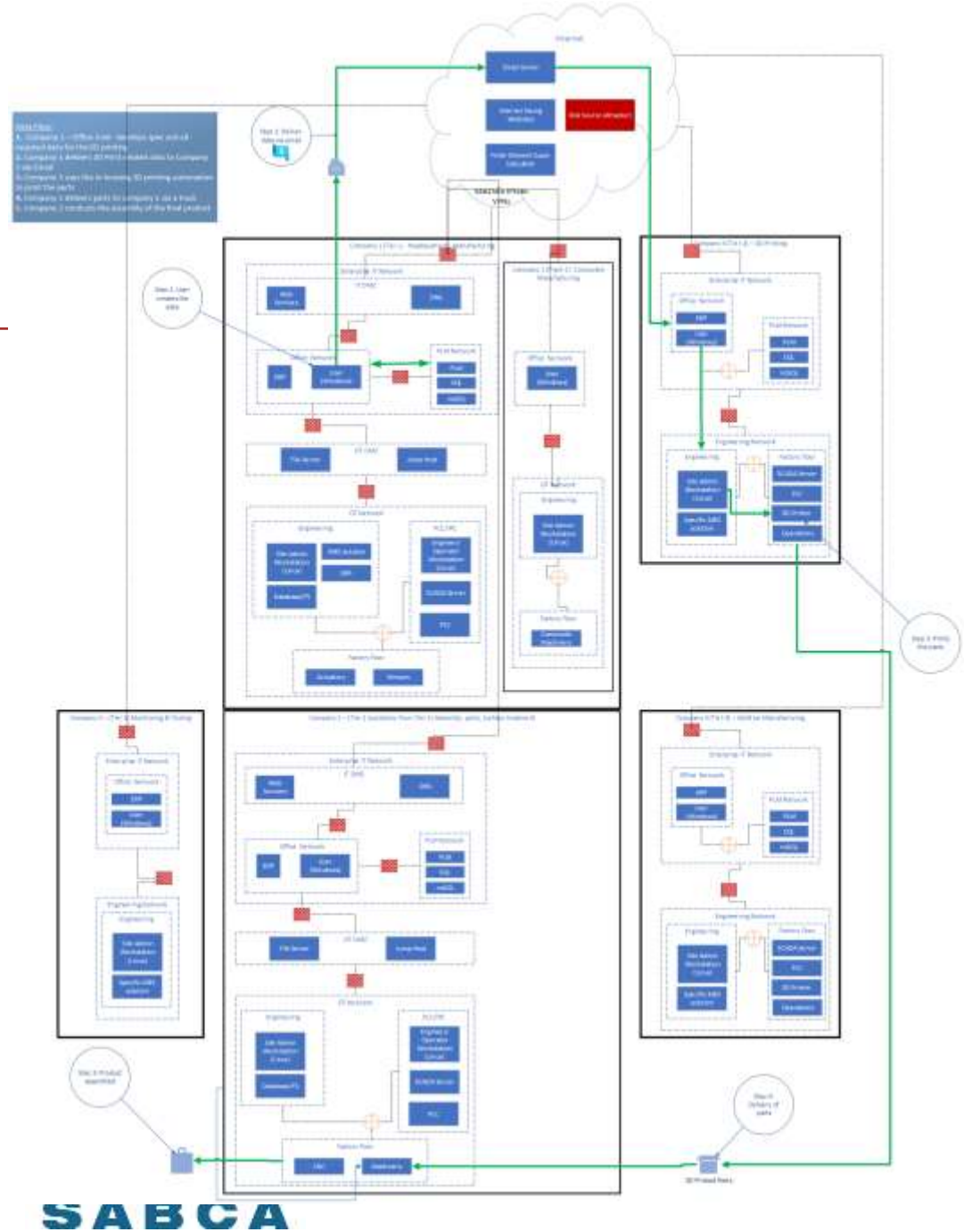
Selection Case

- *The grid fins with outsourcing of the additive manufacturing part as an example of design data to be exchanged with an external company.*
  *In this story, the Main Engine Bay / Grid Fins were produced internally at the headquarters (**M**), the assembly was done at a subsidiary (**A**) and the 3D Printing had been outsourced. The separation from the design/modelling calculation model and results, the parameters definition and the final configuration mapping showed that the zero-trust by the technology was not necessary to implement in the meaning that the data was not usable for other purpose.*

- *Main Engine Bay industrialization and manufacturing: Build-to-print with most of the parts made on numerical machines and some composite parts in another site of the company (as an example of data transfer to another in-house division/other building and other site at 70 km)*

- *Thrust Vector Actuator System development and manufacturing: design and built to spec with close cooperation with a supplier for the health monitoring system (as an example of internal and external data transfer).*

- *Surface treatment project on which the additive manufacturing was based on a matrix of points instead of a complete data lake.*



Nexova

ENGIE Laborelec

SABCA

Selection Case cont.

- *5 Distinct use cases*
  - *3D printing Processes*
  - *Introduction of ERP*
  - *Collaboration between plants*
  - *Health Monitoring Process*
  - *Additive Layer*
- *Focus on protection of data-items*

	Primary Assets
1	Product lifecycle Management Data
2	Project management, Contractual and Tendering data
3	Crisis management Data
4	Quality Assurance, Monitoring and Operational data
5	Health, Safety and Environment
6	Supporting Services Data
7	Personal Data

	Supporting Assets
1	ERP Software
2	MAIT Collaboration Platform
3	Internal Servers
4	External Servers
5	Workstations
6	Removable Media
7	Scada Systems

Nexova ENGIE Laborelec SABCA

Security Problem

Identify the most feared events

- Identify how malicious actors (Risk Origins) could reach their objective (Target Objective)
- Use of EBIOS RM

16 critical risks highlighted

- Strategic Scenarios (high level path of attack) has been identified for each risk
- Use of MITRE ATT&CK

RO/TO pair			
Risk origin	Target objective	Short name	Name
RO1 - State-related	TO1 - Sabotage for destabilisation purposes (during a complicated political context)	R1	Direct attack from a state related to sabotage PLM data for sabotage purposes
		R2	Attack through an IT provider from a state-related to sabotage PLM data for destabilisation purposes
		R3	Direct attack from a state-related to sabotage QA QC monitoring and operational data
		R4	Indirect attack from a state-related using transporters, logistics and packaging stakeholders to sabotage QA QC monitoring and operational data for destabilisation purposes
		R5	Attack through an OT provider to sabotage QA QC monitoring and operational data for destabilisation purposes
RO2 - Specialised outfits	TO2 - Theft and exploitation of data for lucrative purposes	R6	Direct attack from specialised outfits to still and exploit PLM datafor lucrative purposes
		R7	Indirect attack from specialised outfits using a European private organisation to still and exploit PLM data for lucrative purposes
		R8	Attack through an IT provider to still and exploit PLM data for lucrative purposes
RO4 - Competitor	TO3 - Theft and exploitation of data to gain commercial advantages	R9	Direct attack from a competitor to still and exploit project management contractual and tendering data for commercial advantages
		R10	Indirect attack from a competitor using transporters, logistics and packaging stakeholders to still and exploit project management, contractual and tendering data to gain commercial advantages
		R11	Attack through maintenance and cleaning services to still and exploit project management, contractual and tendering data for lucrative purposes
		R12	Direct attack from a competitor to still and exploit data to gain commercial advantages
		R13	Indirect attack from a competitor using transporters, logistics and packaging stakeholders to still and exploit data to gain commercial advantages
		R14	Attack through temporary services providers to gain commercial advantages
RO1 - State-related	TO4 - Theft and exploitation of data for spying purposes	R15	Direct attack from a state-related to still and exploit crisis management data for spying purposes
		R16	Attack through security guardians from a state-related to still and exploit crisis management data for spying purposes

Nexova

ENGIE Laborelec

SABCA

Security Problem – EBIOS RM

EBIOS Risk Manager

- Published by ANSSI, the French cybersecurity agency
- Organized around 5 workshops
  - Scope and security baseline
  - Risk origins
  - Strategic scenarios
  - Operations scenarios
  - Risk treatment
- Focus on intentional attacks

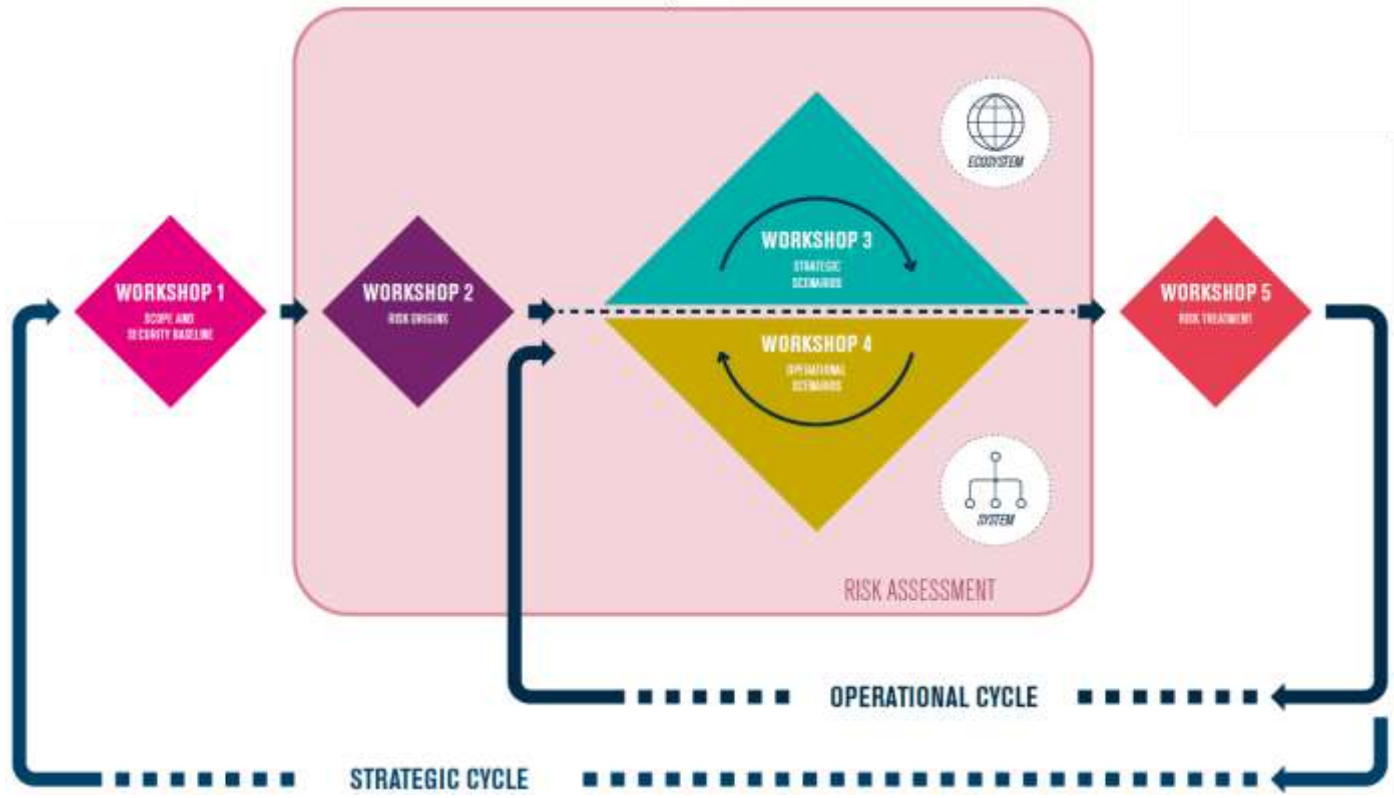


Image source & full documentation : https://cyber.gouv.fr/publications/ebios-risk-manager-method

Nexova

ENGIE Laborelec

SABCA

Security Problem – MITRE ATT&CK

MITRE ATT&CK framework

- https://attack.mitre.org/
- Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations
- 3 Matrices
  - Enterprise
  - Mobile
  - ICS

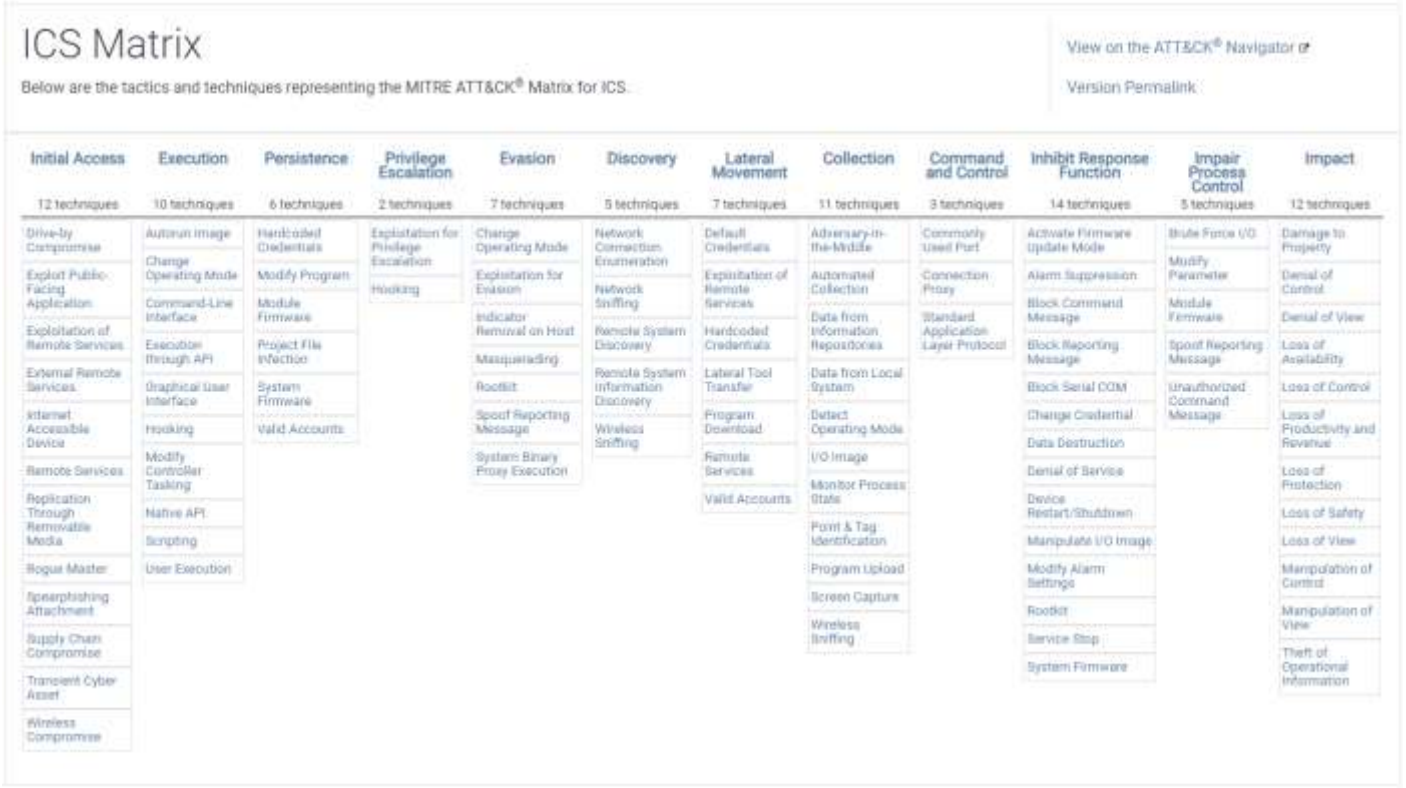


Image source: https://attack.mitre.org/matrices/ics/

Security Trends

STUXNet

Cyberattack on the control information system of an industrial plant

"Duqu" Virus

Cyberattack to obtain information that could be used to attack industrial control systems.

"Shamoon" attack

Use of a "wiper" that paralyzed storage, transport and sales of ARAMCO oil barrels for weeks.

Virus Flame

Attack aimed at infecting computers on a network in a one-by-one mode, in order to extract data of any kind.

German Metallurgical Plant

Ransomware attack: after refusing to pay the ransom, the attackers paralyzed the shutdown system of a blast furnace, damaging the plant.

Ukraine power grid attacks

2 attacks target the Ukraine power grid: one in December 2015 dubbed "Black Energy", leading to a power cut in part of the country of about 6 hours; one in 2016 targeting a transmission line

"Wannacry Ransomware"

Affecting more than 150 countries and paralyzing the production of many companies

"Triton" Malware

Industrial virus targeting safety systems, reprogramming safety controllers.

"Picanol" production halted due to ransomware

The operations of the weaving machine company Picanol stopped for 3 days in all their sites in Belgium, Hungary, and China because of a ransomware

Colonial Pipeline, United State

Ransomware struck pipeline management systems, demanding $4.4 million in bitcoin, resulting in a 5-day service disruption

During 2022 number of attacks doubled against industrial infrastructure.

In the same year, 70% of all ransomware attacks focused on manufacturing.

Source: https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Exec-Summary-2022.pdf

Nexova

ENGIE Laborelec

SABCA

Guidelines

Risk-based approach to security

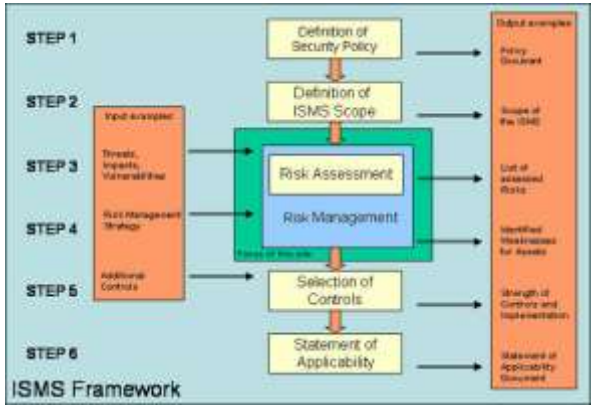
Information security and classification

Security Requirement Statement

Define Roles and Responsibilities

Monitoring

Awareness and continued Training



EBIOS RISK MANAGER

ATT&CK®

Nexova

ENGIE Laborelec

SABCA

Best Practices

Defence-In-Depth
- Multiple layers of security controls
- Network segmentation
- Access Control
- Encryption
- Detection Systems

Supply Chain Security
- Assess and establish agreements
- Secure development lifecycle practices
- Supply chain monitoring

Training
- Security Awareness Training
- Incident response training
- Compliance training

Incident Response
- Development and testing of incident response plans
- Policies

NIST SP 800-53 – Security and privacy Controls

NIST SP 800-82 – Guide to OT Security

National regulation (NIS-2, CCB – Cyber Fundamentals, …)

ISO27k1, ISA/IEC 62443…

Nexova

ENGIE Laborelec

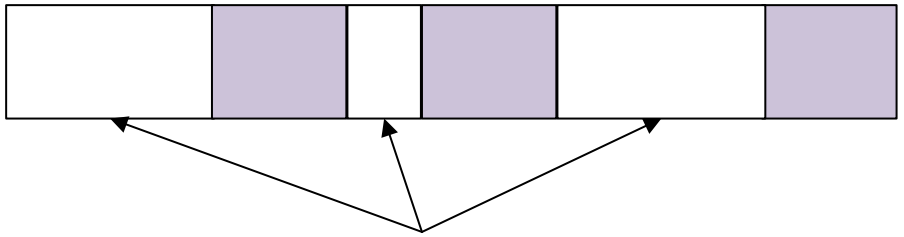
SABCA

Guidelines Conclusions

Available security frameworks, controls and guidelines are already present

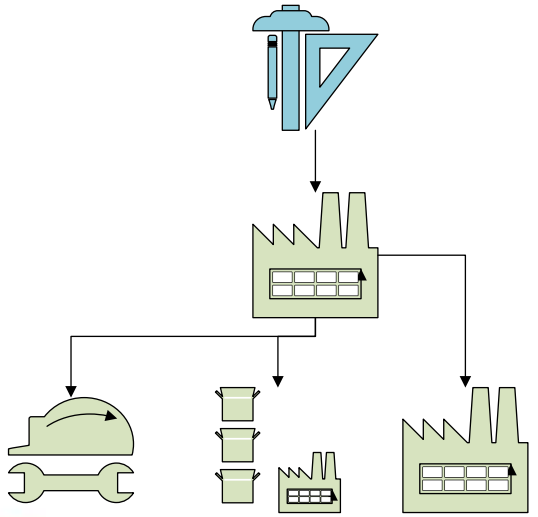
Many controls can be implemented using of-the-shelve technical solutions (encryption, account management, ..)

A risk-based approach and cyber-hygiene measures are critical



Distributed and Cloud-Manufacturing – New Security Challenges

- Automatic Request For Quotation
- Side-channel attacks
- Protection of IPR
- Unfair competition



Nexova

ENGIE Laborelec

SABCA

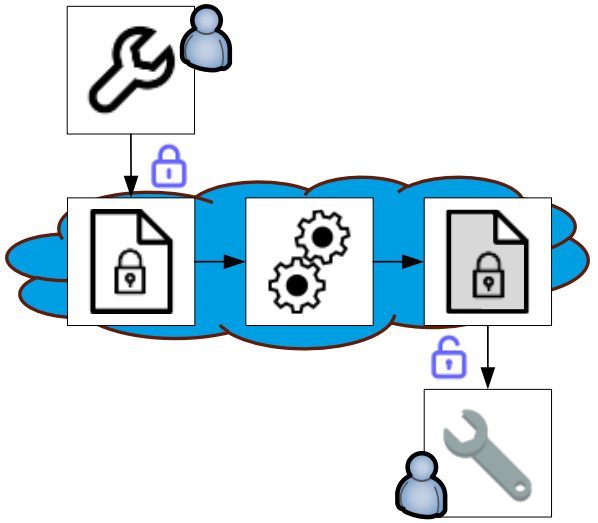
New Security Measures

Study application of 3 new cryptographic technologies:

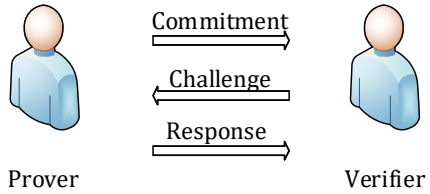
- Fully-Homomorphic Encryption
- Secure Multi-party Computation
- Zero-knowledge protocols

Three identified use-cases

- Finite-element calculation in untrusted environment
- ZKP for testing document properties
- Support for secure market-place using combination of MPC and ZKP



Fully Homomorphic Encryption



Zero Knowledge Protocol

Nexova

eNGie Laborelec

SABCA

New Security Measures - Conclusions

Finite-element calculation in unsecure environment

- Complex computation
- Overhead in the FHE model renders it meaningless

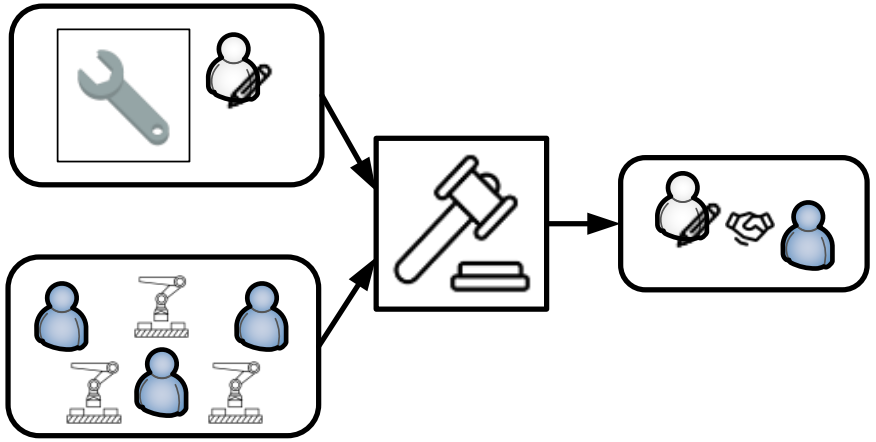
Finite Element Calculation example

ZKP for testing document properties

- Not practical, document is anyway available
- Selective disclosure using other means (encryption)

Support for secure marketplace using combination of MPC and ZKP

- Potential to use for more secure, however, needs wide adoption



Secure Marketplace concept

Nexova

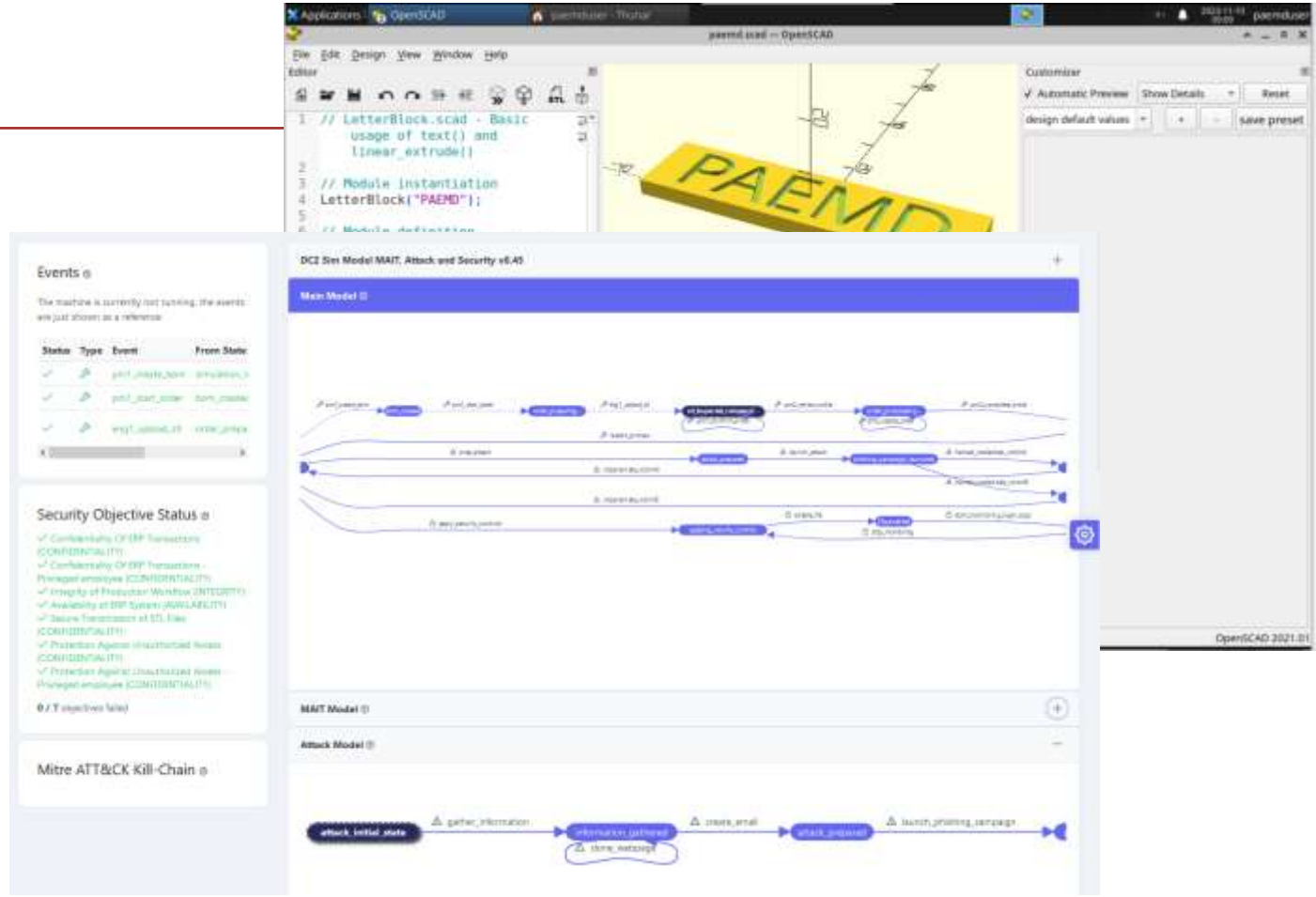
ENGIE Laborelec

SABCA

Awareness training / Security Demonstration

Demonstrator to simulate:

- Enterprise infrastructure
- MAIT Process
- Attacker Process
- Control Measures



Lightweight and fast

Strong Security Focus

Building on Operational Scenarios

Nexova

ENGIE Laborelec

SABCA

Architecture

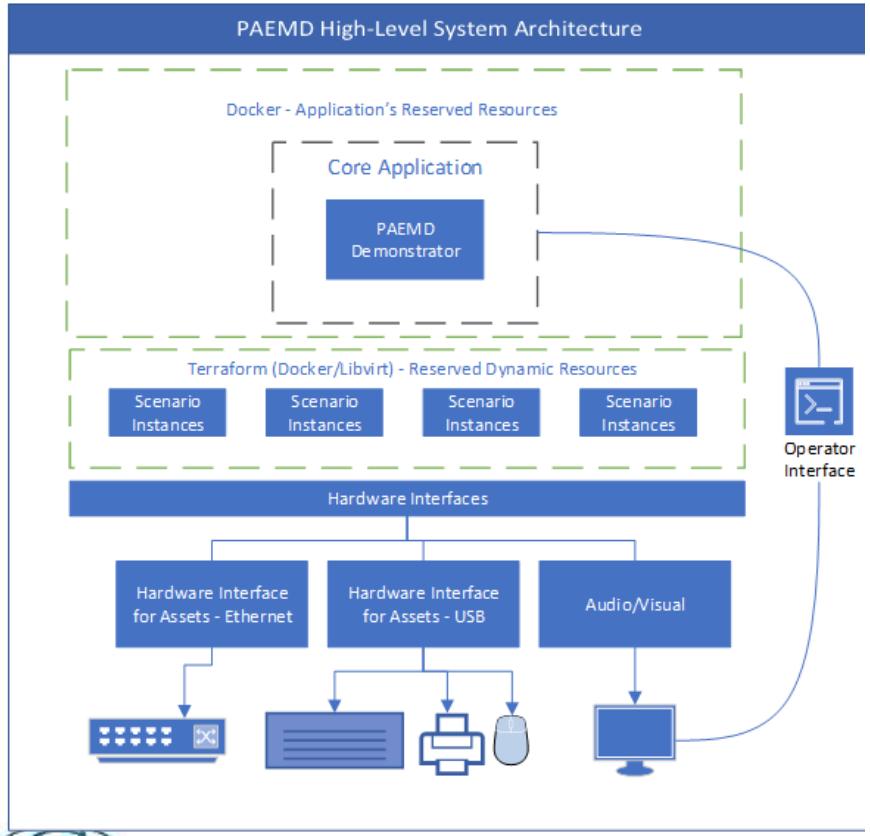
Physically based on a workstation laptop

- Scenario bridge-networking for HW-in loop

- AV and operator interface

Reserved dynamic resources provided through Terraform using containerization and virtualization

Web-application managing the process-flow and providing the operator the user-interface



Nexova

ENGIE Laborelec

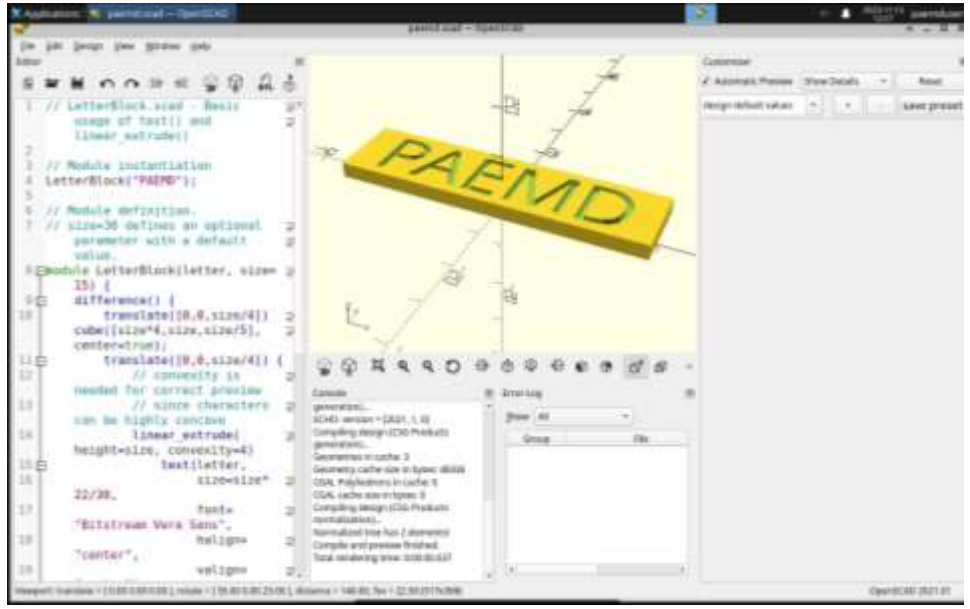
SABCA

Overview of DC1 - Printing between Company A and B

An engineering company (Company A) creates a design for a mechanical part, the design process involves rigorous testing and revisions to ensure an optimal performance.

The design is manufactured by a second company (Company B)

- **The production of the part needs to be secure to ensure that the design is not tampered with and that the finalized parts mechanical properties are as specified**



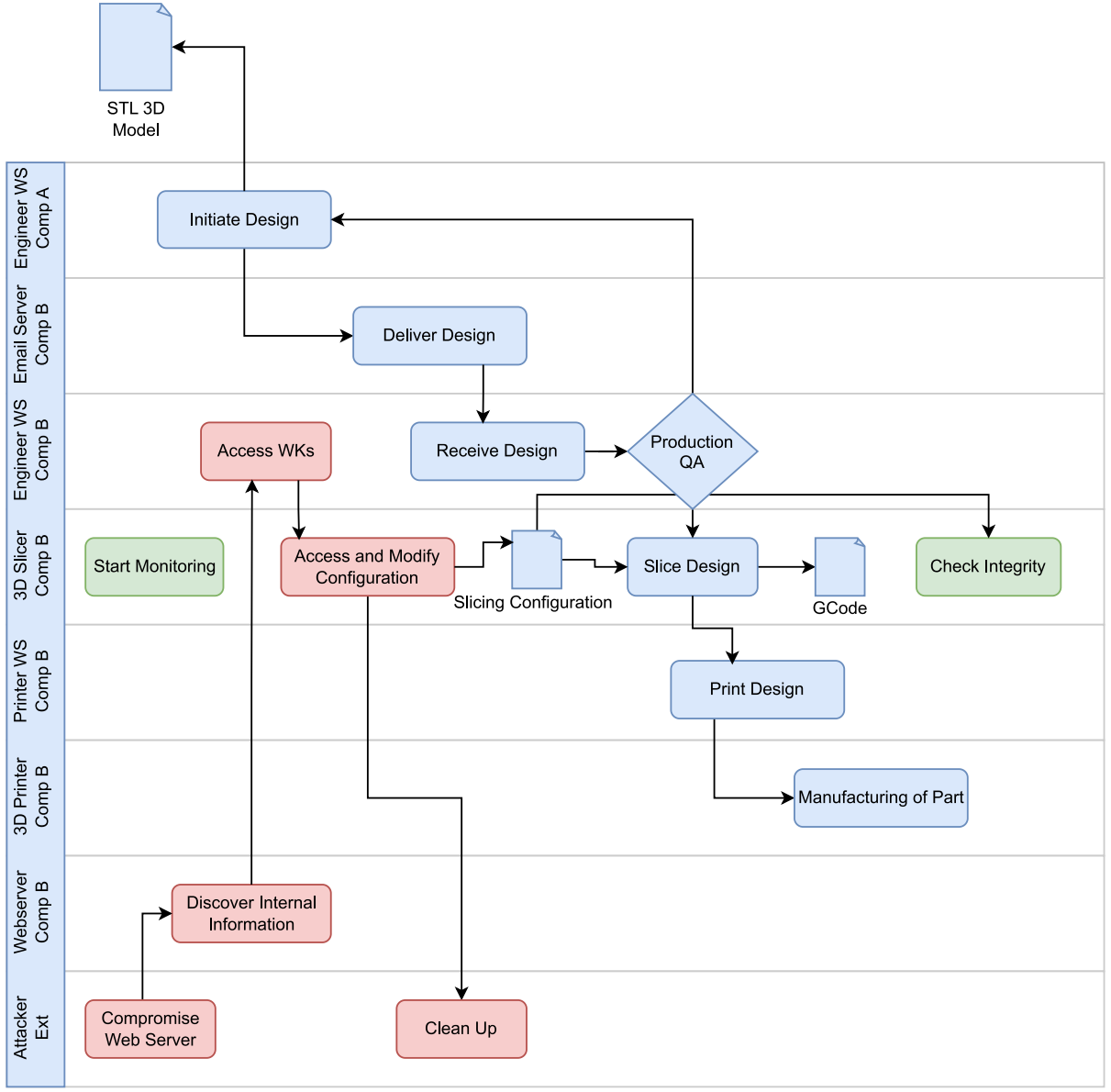
Nexova

ENGIE Laborelec

SABCA

Overview of DC1 - Printing between Company A and B

Overview of the information flow



Production of PLM-data (initiate design)

Company A produce the data using specialized and advanced CAD software to create a 3D model.

The design involves rigorous testing and revisions to ensure that the part will have the correct mechanical properties.

- It is important that the models are not tampered with since it can have both an effect on production costs as well as potentially safety risks.

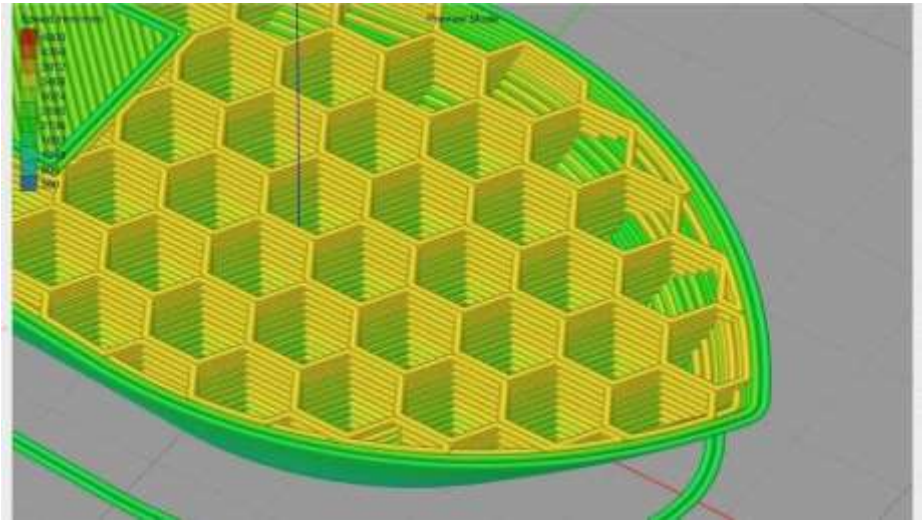
Nexova ENGIE Laborelec SABCA

Processing of Data (slice)

Company B receives the file and inspects it, after the file will be sliced according to the specification

Slicing is the process of transforming a 3D model (e.g., STL file) into a GCODE file that can be handled by an additive manufacturing process (e.g., 3D-printing)

- Ensure that the properties of the printed object are as specified, for instance infill rate
- Slicing is configured correctly for materials (filament dimensions, temperature ..), machines (extruder width, printing speed ..) etc.
- Any modification to the Gcode would lead to altered performance



Nexova ENGIE Laborelec SABCA

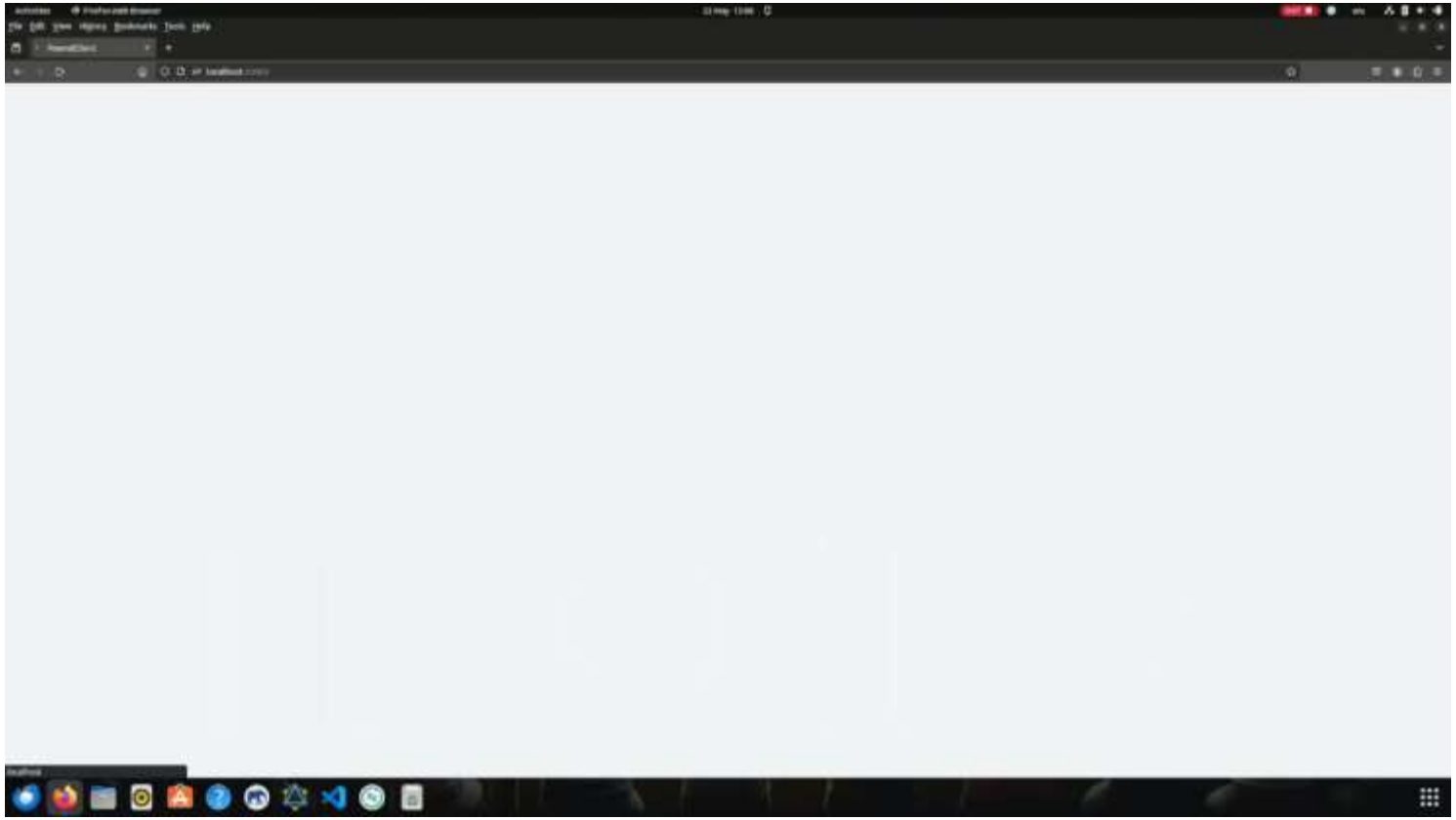
Demonstration

DC1

Demonstration

DC5

Same MAIT case as DC1, but attack is on printer protocol



Nexova

ENGIE Laborelec

SABCA

Conclusions

Scenarios needs to be tailored for the real-world cases as implemented in the industry

The simulation is applicable to other domains as well, primarily within wider manufacturing but as soon as we see processes, complex supply-chains and cyber issues there is a potential to use the PAEMD demonstrator.

Demonstrator seems most useable in training and awareness campaigns, this due to the technical nature of the demos.

The use of containers means that asset management is a lot easier than traditional virtualization.

Limitations:

Networking is simplistic and various non-TCP/IP (canbus, i2c …) connectivity is not natively supported, we need edge-computer providing these interfaces

Exploitation of vulnerabilities are limited, due to use of containers

Nexova

ENGIE Laborelec

SABCA

Key Take-aways

The security is becoming more challenging due to digitalization, more heterogenous architecture and an increasingly complex supply-chain in the manufacturing sector

Manufacturing is in the focal point of adversaries; we see many directed attacks against ICT and OT we don’t think this will change without good awareness and directed resources.

Spacecraft manufacturing is essential to safekeep European market and strategic position, why security needs to be on agendas and strategies.

Standard, controls and security practices are available for most cases, we need to ensure that the awareness and understanding of risk within the industry to ensure that sufficient investments are made into security

Nexova ENGIE Laborelec SABCA

QA

Thank you!

Nexova

ENGIE Laborelec

SABCA