ValueChain 4.0

EFFRA-ECSO-EC Workshop
Cybersecurity for Manufacturing Environments

17 October 2018

gradiant
Connectivity · Intelligence · Security
for your business

(+34) 986 120 430 | gradiant@gradiant.org | www.gradiant.org

ValueChain 4.0 – Challenges addressed

- **Now: Highly static production processes, oriented towards the manufacturing of concrete series of products with few variations.**
  - Higher flexibility and reconfigurability needed, allowing to adapt production lines simply and fast
- Most manufacturing companies still establish their **services contracts through traditional relationships with their clients and suppliers**.
  - Contracts are mid/long term and lack flexibility
- **The value chain communicates through traditional methods such as phone or fax** or using proprietary technologies or standards like EDI that are point-to-point, not involving all the stakeholders in the process from the beginning.
- **Business process management (BPM) systems are developed as isolated silos**
  - Separate companies do not have the possibility of exploring the creation of shared processes to carry out common goals (e.g. automatically building a supplier/consumer chain).

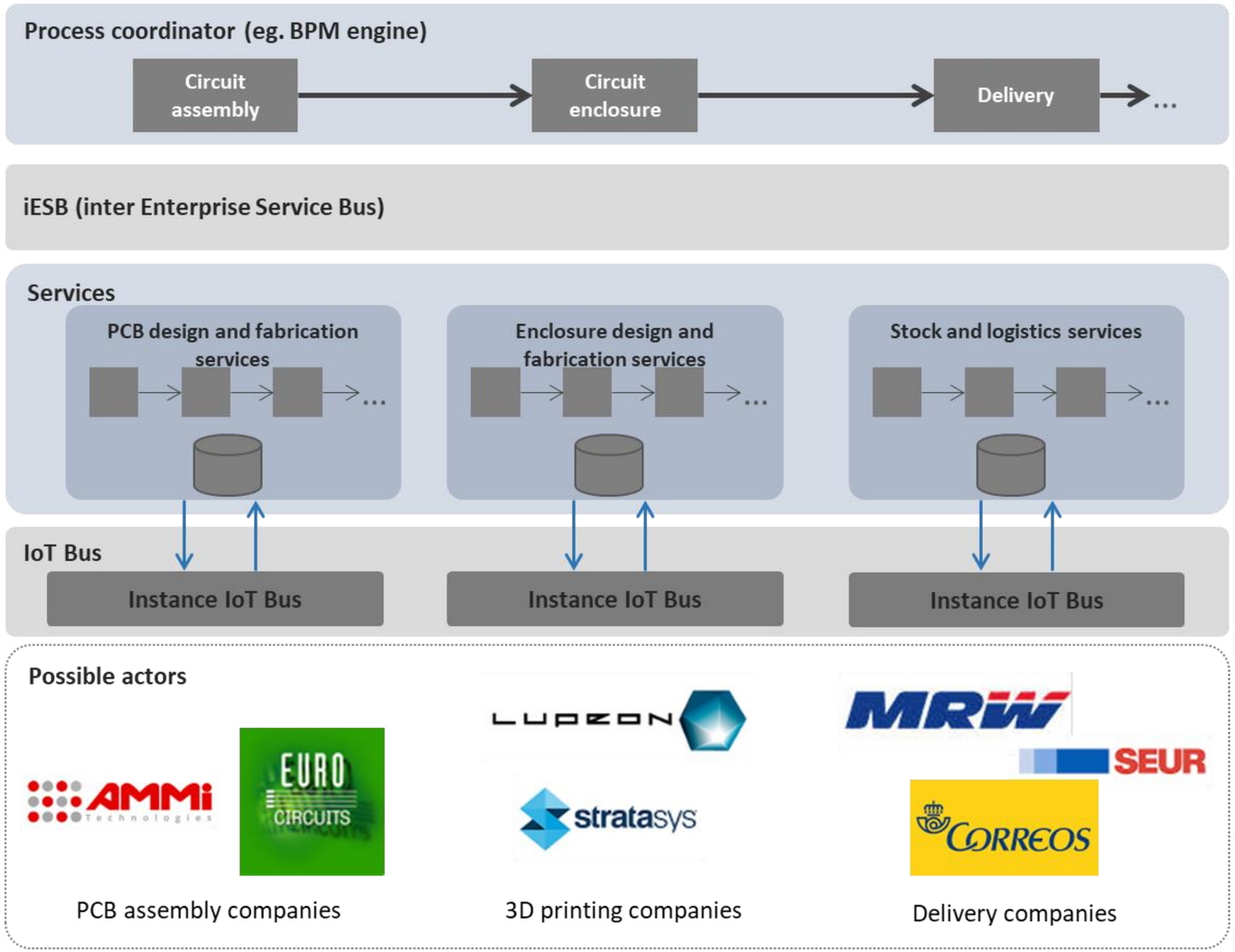
ValueChain 4.0 Overview

Enabling platform to establish business relationships, sharing of business processes and establishment of dynamic contracts between service providers and customers through the servitization of the value chain.

As a first step, the platform will contemplate the following:yy

- Create a framework for the servitization of companies' processes and expose external APIs to access them.
- Implement a **middleware** to communicate companies between themselves but also a company own processes using an event-driven service oriented architecture (EDSOA).
- Establish a mechanism based on **blockchain** and **smart contracts** to create service contracts between suppliers and customers to increase their flexibility and own a distributed ledger with a complete records of the activities carried out in the platform.
- Improve traditional BPM to ease **inter-enterprise collaboration** and the creation of shared processes.
- Include the correct mechanisms to guarantee the **privacy and confidentiality** of data from companies and their interactions with the middleware and other actors.

ValueChain 4.0 example: IoT device manufacturing orchestration



ValueChain 4.0 – Cybersecurity challenges addressed

Prevention of OT threats

- OT network analysis (TRL 3)
- OT software/firmware validation (TRL 3)

Early detection of OT attacks

- Continuous OT network monitoring (TRL 3)
- Remote attestation of Industrial IoT devices (TRL 3)
- Analytics for IT/OT combined environments (TRL 3)

Provision of secure digital identity for industrial IoT & CPS across the value chain

- Permissioned blockchain for integrity and accountability (not started yet)
- Smart contracts for automation of operations supported by blockchain (not started yet)

ValueChain 4.0 – Cybersecurity highlights

Digital Platform Environment Segregation	Operating System Privileged Account Control	**Internal Data Flow Security**	Security Updates	System Hardening	Physical Security	Password Policy
Multi-factor Authentication	User Account Management	Token Management	**Malware Protection**	Software Integrity	Database Integrity	Cyber Incident Response Capability
Security Training and Awareness	Logging and Monitoring	Back Office Data Flow Security	Transmission Data Protection & Encryption	User Session Integrity	**Vulnerability Scanning**	Critical Activity Outsourcing
Transaction Business Controls	Personnel Vetting Process	Physical and Logical Password Storage	**Intrusion Detection**	Penetration Testing	Scenario Risk Assessment	

Key Security developments of our Digital Platform	Willing to Share – Use other experiences of Digital Platforms (Y/N)	Willing to Share – Use other experiences of Security Practitioners (Y/N)
Access management		
Privileged access management (admin)		
Identity management		
Authentication - Authorization	ValueChain 4.0	ValueChain 4.0
White Listing		
Root Access		
Security management principles		
Control measures		
Audit capabilities		
Reporting		
Incident Management		
Event Monitoring – Incident Monitoring - Reporting	ValueChain 4.0	ValueChain 4.0
Encryption		
Key Management		
Privacy Enhancing Technologies		
Denial of Service		
Patch Management		
Over the Air Updates		
Embedded Security	ValueChain 4.0	ValueChain 4.0
Integration		
Firewalling - Proxying		
Cloud Security Mechanisms : please specify		
Isolation		
Virtualization		
End to End Security		
TTP (Trusted Third Party) : please specify		
DRM (Digital Rights Management)		
Other 1 : please specify		
Other 2 : please specify		

Contact

Marcos Álvarez-Díaz

Head of EU Programmes

malvarez@gradiant.org

Backup slides

Valuechain 4.0: Industry 4.0 systems need new security features

New functions needed

- Prevention of OT threats
  - OT network analysis
  - OT software/firmware validation

- Early detection of OT attacks
  - Continuous OT network monitoring
  - Remote attestation of Industrial IoT devices
  - Analytics for IT/OT combined environments.

New trust relations in the Industry 4.0

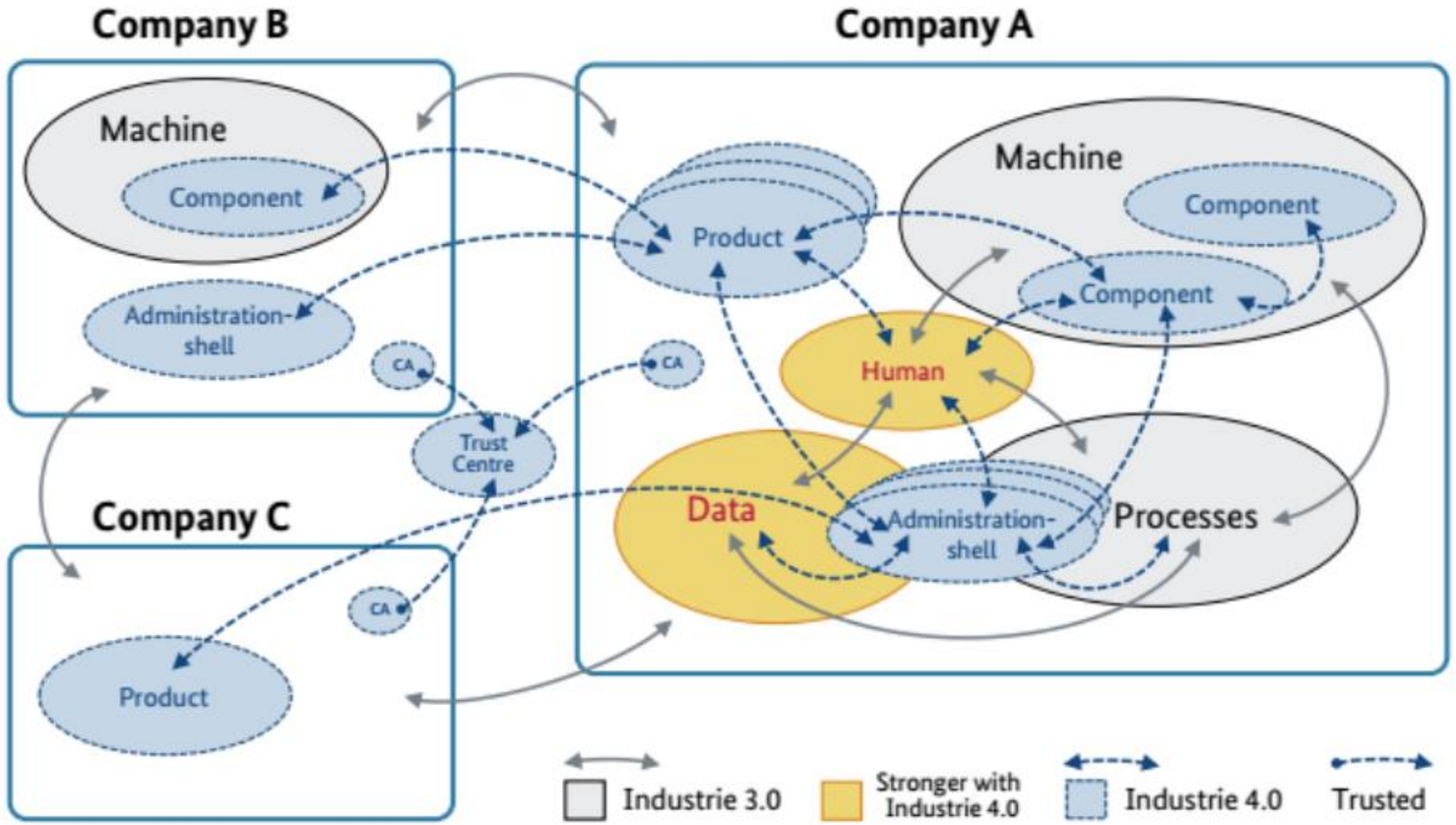


Image source: Platform Industrie4.0