

Smart Factory / Connected Machines

Definition of a "Smart Factory"

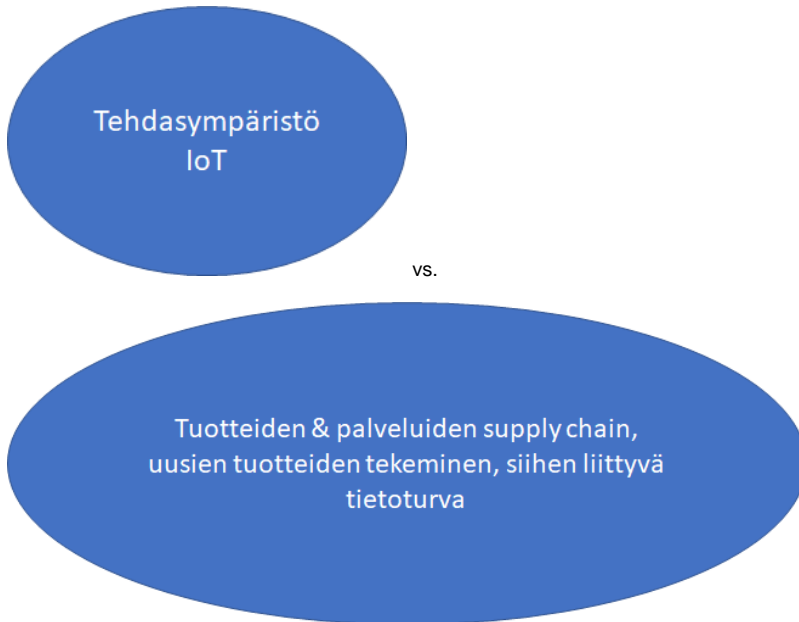
...

Definition of "Connected Machines"

....

Description

- IoT cyber strategy
- Integrity of software updates
- Integrity of online connection to cloud
- Monitoring connected machines for cyber attacks
- Operator and service personnel secure logging
- Firewalls between intelligent machine connections.
- Completeness of data modelling
- Product liability
- Wireless connectivity (denial of service)
- DOS attacks in WSNs (wireless sensor networks)



What is more interesting? Small vs. big?

Ideas

- Provide knowledge, increase awareness especially for SME sector
- Point is to increase knowledge about the appropriateness of CyberSec to companies
- Security by design
- Identity and its management
- Focus area: Detection of attacks
- Risk management cost efficiency
- Trust in the Manufacturing Supply Chain (i.e parts from different manufacturers, assembly, warehousing, logistics, distribution and deployment)
 - Identification of potential cybersecurity threats and mitigation techniques
 - Verification of the integrity, and trustworthiness, of the overall supply chain, manufactured components as well as data flows
 - Devising methods to develop resilient systems out of potentially insecure parts of the supply chain, based both on trust as well as evidence
- Operational Security in connected factories, IT Systems and machines
 - Performing local and remote attestation of autonomously operating/executing machine components
 - Conducting the secure deployment, orchestration and trustworthy execution of components, lightweight containers and VMs, particularly for edge computing

- Enabling stakeholders to perform real-time and near real-time monitoring and anomaly detection, based on traffic observation and attested (as well as encrypted) data in a privacy-preserving manner
- Designing dynamic data visualisations of the real-time security state in smart factory and connected machines as well as user interfaces supporting context-specific comprehension and security management
- Deploying PKI and AAA infrastructure enabling certificate-based access control and revocation policies
- Information Sharing for Collaborative Security Management
 - Usage of modern encryption schemes such as Attribute-based encryption, which facilitates efficient data sharing, collaboration and even revocation, among multiple stakeholders based on a common attributes for fine-grained role-based access control, without the need for traditional username/password-based schemes
 - Delivery of cybersecurity events and incident data among stakeholders, using standardized incident exchange formats such as IODEF, STIX and VERIS used by Cybersecurity Incident Response Teams (CSIRTs) for collaborative incident handling and automated responses to prevent propagation of vulnerabilities.

Questions

- CyberSec in industrial companies
- CyberSec assessment
- Digital identity
- ability to control increasing intelligence
- IoT ecosystem solutions
- Cyber security of a whole value network
- Business cases?
- Risk vs business?
- How to ensure accessibility of data also from remote sites and from machines of subcontractors and suppliers?
- International dimension!
- Monitored and controlled mobile equipments with wireless communication (automated and remote controlled)

Research questions

Industrial partners

Organization	Contact person	Role & contribution
(AIKO cluster)		
(Glaston)		
Annitech		
(Pyroll)		
(Insta Defsec)		
Missing Link		
(Satron Instruments)		
(Ponsse / EPEC)		
Kalmar		
Gofore		

Research partners

Organization	Contact person	Role & contribution
TAMK		
Tampere University/ITC/Computing Sciences	Bill Silverajan, Antonis Michalas	<ul style="list-style-type: none"> • Lightweight Authentication, Encryption and Key Exchange • Software and Software/Hardware Hybrid Attestation • Secure Onboarding, Provisioning and Firmware Updating • Secure Management of Virtualisation Technologies (VMs and Containers) • ML-based Anomaly Detection in Remote/Edge Networks • Advanced UIs for Security Data Visualisation

