SecureIoT

Trustworthiness as facilitator of Policy and Access Management in Supply Chains

Jürgen Neises, George Moldovan, Thomas Walloschke, Cosmin Grigorias, Bianca Popovici

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779899

Conference on Shaping a globally secure Industrie 4.0 Ecosystem
29. January 2021

Measurable Trustworthiness as a Security Characteristic

Motivation & Objectives

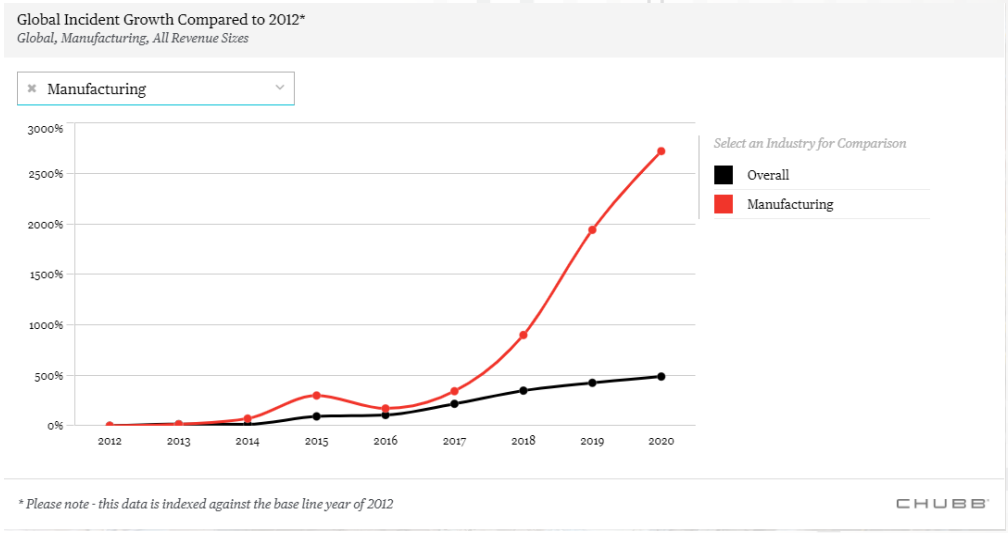
Secure cross-company communication in Industrie 4.0 also concerns transactions in supply chains, which can be flexibly automated and are increasingly in demand.

Security requirement: "...to receive that, and only that, which was ordered".

The evolution of Global Incident Growth by several orders of magnitude in the manufacturing sector is dramatic.

The creation of a system for measurable trustworthiness is to be established.

The goal is primarily to keep possible security-related disruptions as low as possible.



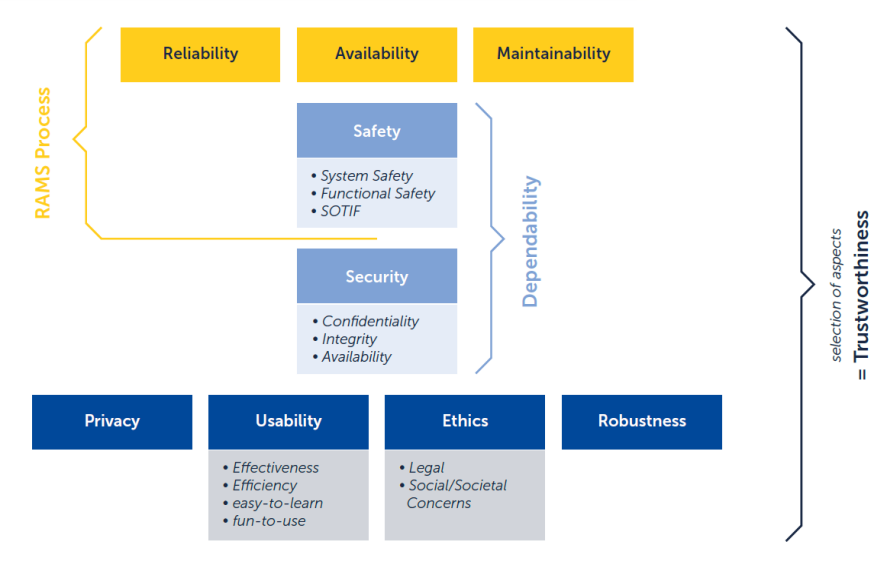
Global Incident Growth Compared to 2012 based on industries (Source: CHUBB)

Attacks on the manufacturing and technology sectors have reached 2nd and 3rd place in the ranking of attacks in 2020.

- Create transparency in the area of trustworthiness.
- Derive concrete steps to create trust models.
- Create automatically verifiable processes down to machine level, especially in communication.

Trustworthiness Concepts

Industrie 4.0 and beyond



Source: Putzer, H. J.; Wozniak, E.: "**Trustworthy Autonomous/Cognitive Systems – A Structured Approach**", fortiss Whitepaper (2020), https://www.fortiss.org/fileadmin/user_upload/Veroeffentlichungen/Informationsmaterialien/fortiss_whitepaper_trustworthy_ACS_web.pdf

IIC: Trustworthiness in Industrial IoT (IIoT) means that

*"A satisfactory level of **confidence can be established** and the **partner system** (be that a sensor, a machine or a factory) **is what it claims to be, fulfils its tasks and not endangers the business partners** by introducing malicious components into the network."*

Platform Industry 4.0 Trustworthiness as quality KPI:

*"The term 'trustworthiness' is used to describe the **quality of existing and future relationships between companies, people, systems, and components**. A trustworthy system ensures that all of its components **behave in an expected manner**."*

Platform Industry 4.0 and RRI join in:

*""For **supply/value chain security and risk management**, the term 'Trustworthiness' corresponds to the supplier's ability to **meet the expectations** of the potential contract partner **in a verifiable way**".*

Measuring Trustworthiness: Characteristics, Attributes, Properties

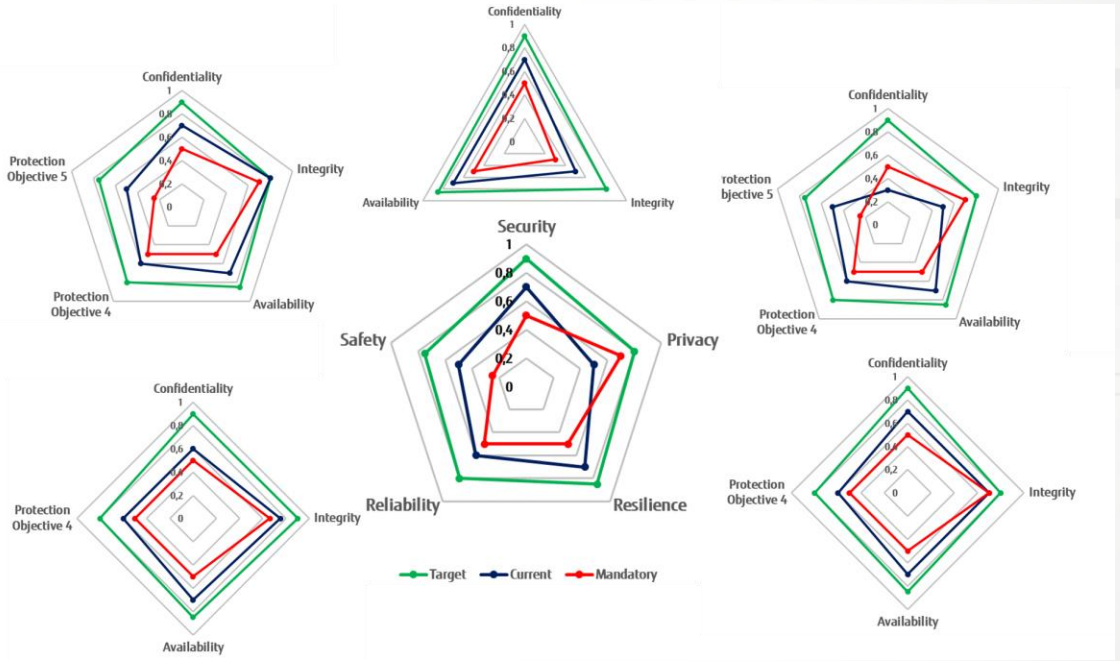
An appropriate Trustworthiness schema depends on the specific expectations and policies, participants' profile and related application in the value chain.

A weighted combination according to system characteristics and the attributed Protection Objectives define the Trustworthiness schema.

Up to now the development of pragmatic schemas is subject of individual analysis and specifications.

Future objective: Common catalogues of easily applicable Trustworthiness schemas describe most relevant use cases.

A universal model



Measuring Trustworthiness

Metrics as Semantic External Events

Trustworthiness relies mostly on external observations in order to avoid a reporter's bias and misinformation.

In the context of trustworthiness, metrics represent numerical values associated to devices and events.

Two main dimensions proposed and used within the work:

- Dynamic/Activity type
- Source type, based on the observed entity and their processes

Contextual Metrics	
Messages Forwarding	Correct priority and flags used for critical system packages.
Messages Priority	Prioritizing of message processing based on expected priorities and time constraints.

Connection Metrics	
Communication Protocol	Nature of the communication protocols and their specific reliability
Certificate Issuers	Current external review of the certificate provider and his processes.

Behaviour Metrics	
Messages Forwarding	Denoting whether the devices forwards events and message to the expected destination.
Packet Loss	Number of packages the devices fails to receive or transmit.

Device Metrics	
Manufacturer	Reputation of the Manufacturer
Firmware Version	Known issues of the currently deployed version.

Measuring Trustworthiness

Merging Metrics to Characteristics

Standard monitored attributes and the semantic observations groups to be aggregated into quantifiable Characteristics

A manufacturers priorities, knowledge sources and requirements define the specific composition and quantifiable metrics.

Security Characteristic

Metric
Manufacturer
Firmware Version
Model Number
Exposure Level
Mobility

Metric
Protocol (App Layer) Specific
Certificate Issuers

Metrics
Network Presence
Activity Duration
Forwarding Delta
Message Destination

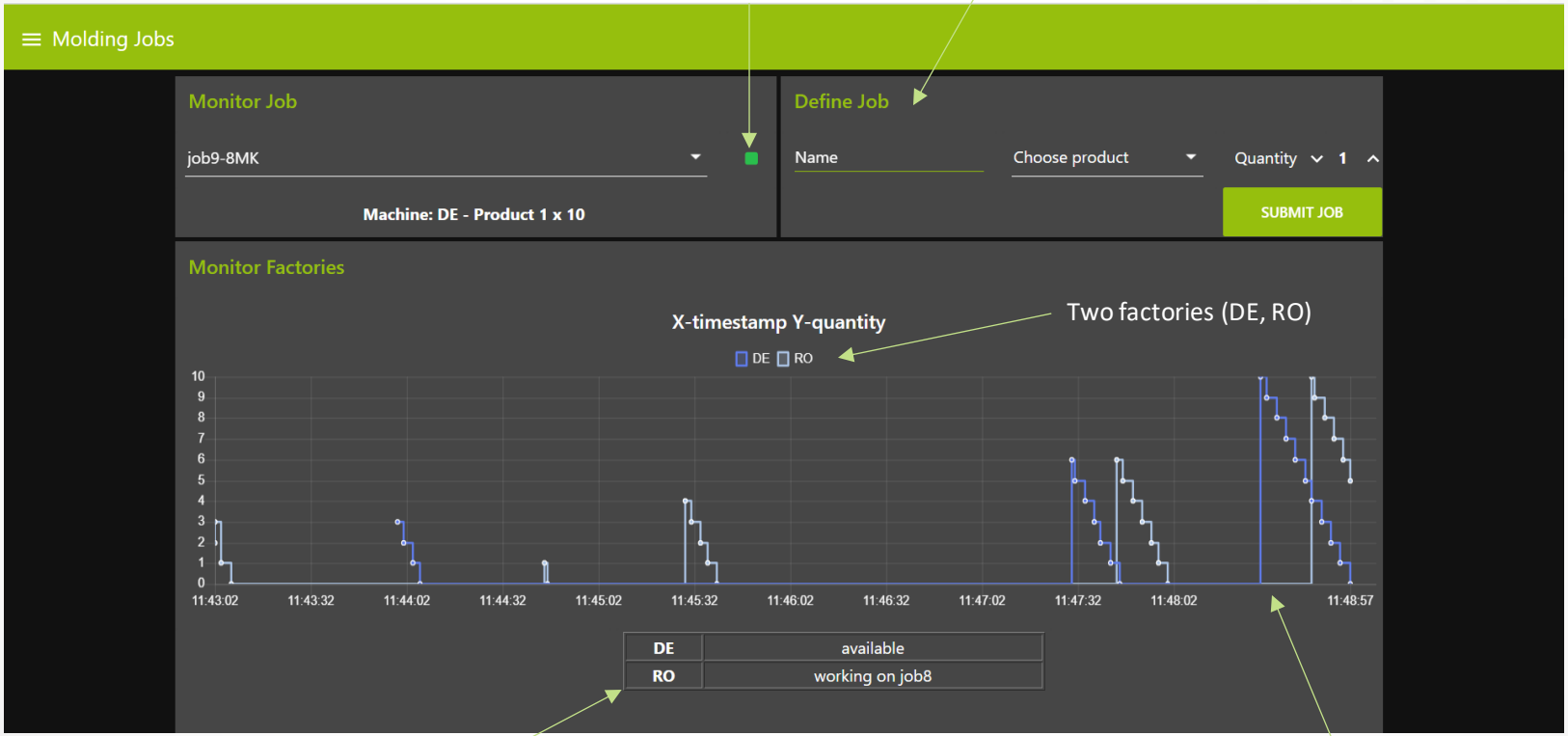
SecureIoT: Trustworthiness in Action

Application Scenario

1. Submit a new job
(System trustworthiness evaluated beforehand)

2. Monitor Job (status, job allocation per machine)

Red – Submitted
Orange – In Progress
Green - Done

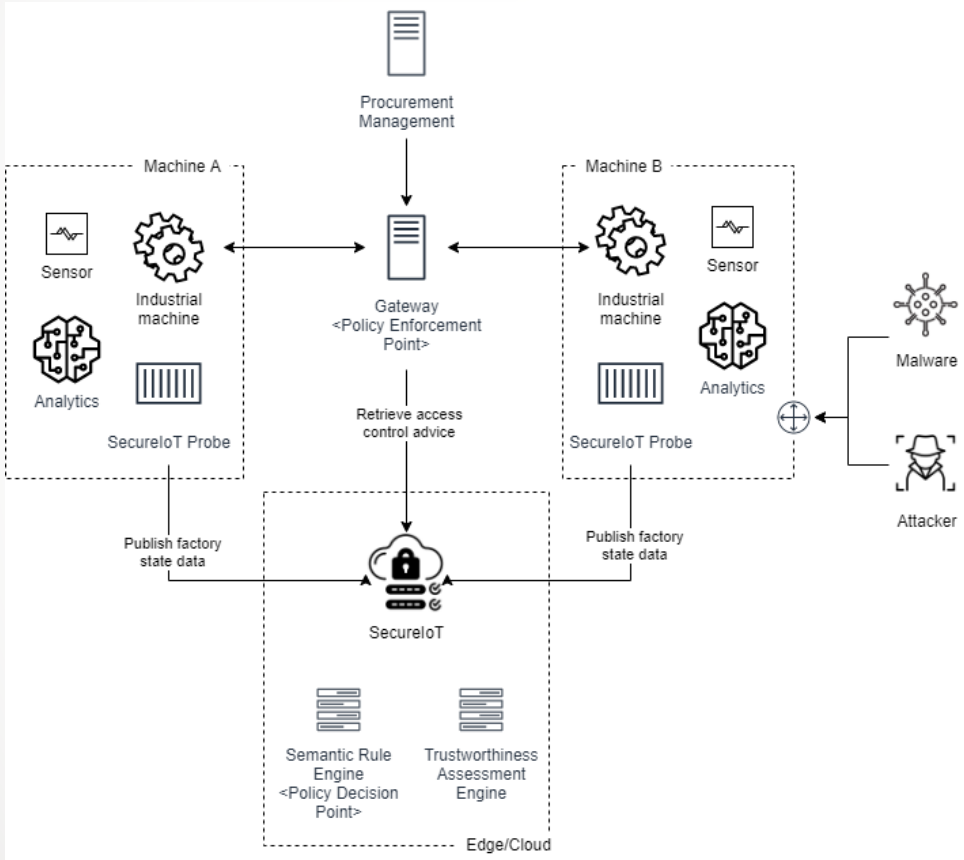


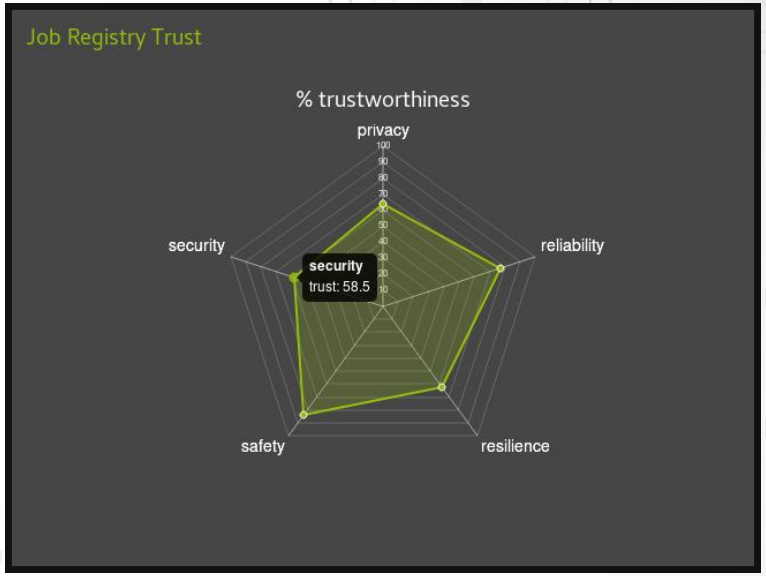
3. Monitor each factory status
(Available/Working)

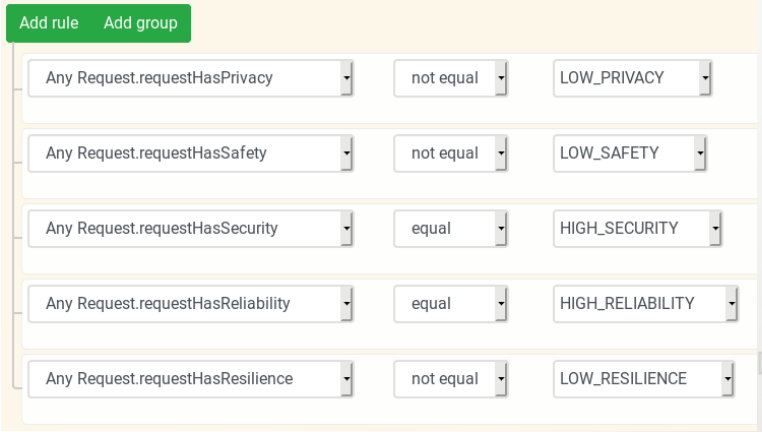
3. Monitor progress of jobs per machine
(completed part counter)

SecureIoT: Trustworthiness in Action

Demo Implementation







Future Work

Directions of Development

- **Security Standardisation**
  - Generic sets or catalogues of characteristics for comparison or mitigation of policies and Trustworthiness across different domains.
  - Entity specific global trust ecosystem.
- **Catalogues of Trustworthiness metrics and schemas**
  - Extend common Information-Security Management-Systems
  - Facilitate a broad application of Trustworthiness in Industrie 4.0 and beyond.
- **Efficient Evaluation**
  - Minimize monitoring and calculation effort (edge based evaluation)
  - Trustworthiness evaluation in a public place and verifiable – interplay of cloud and edge
- **Transparent Product Quality**
  - Continuous evidence-based documentation of the production parameters.
  - Evaluation of trustworthiness during the production of a batch or even a single good.
  - Documentation in a distributed ledger as proof of product quality.
  - Consider data sensitivity.

Conclusions

To strengthen resilience in dynamic supply chains, a better trust model facilitating policy management is imperative.

A pragmatic model for automatic and measurable Trustworthiness is presented and the modelling as well as exemplary metrics and attributes for its evaluation are explained.

Based on an application in the Horizon 2020 project SecureIoT, it is presented how this model and the described metrics can be used to manage trustworthy access to resources in an industrial environment.

In future work, the development of generic metrics, the integration into an industrial ISMS and the application to distributed manufacturing are of particular importance.


Thank you