SecureIoT

Trustworthiness as Key Enabler for Connected Services in Mobility

Jürgen Neises, Thomas Walloschke

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

Workshop Cyber Secured Autonomous Vehicles
12. February 2021

Measurable Trustworthiness as a key Enabler

Motivation & Objectives

Secure cross-entity (car or component) communication concerns interactions, which can be flexibly automated and are increasingly in demand.

Security requirement: “...to receive that, and only that, which is expected".

Automotive cybersecurity incidents increased by several hundred percent in the last 5 years.

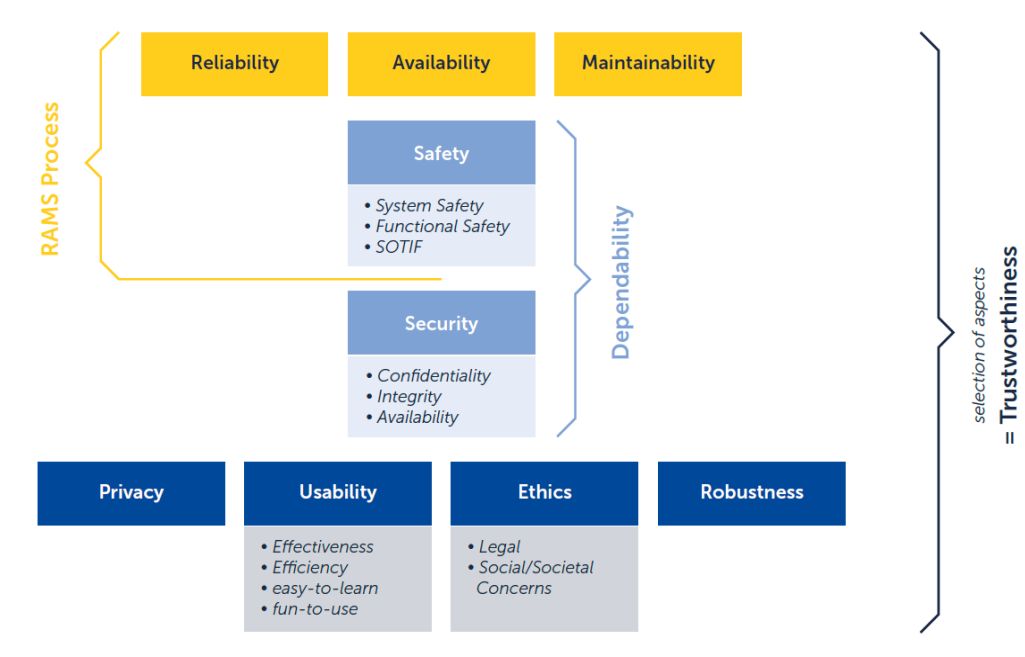
The creation of a system for measurable trustworthiness is to be established.

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

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

Trustworthiness Concepts

Beyond Industrie 4.0



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

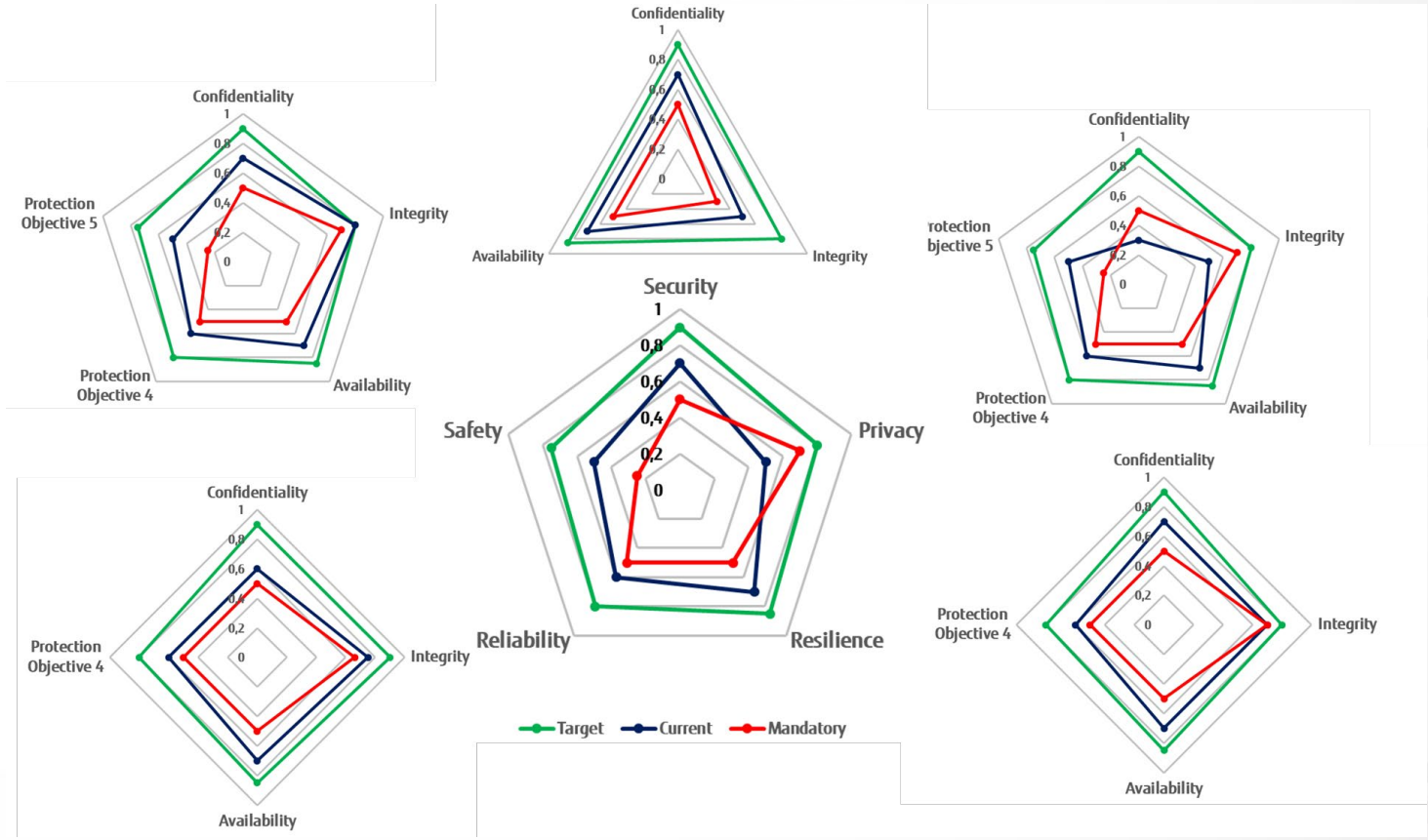
An appropriate Trustworthiness schema depends on the specific expectations and policies, participants' profile and related application in the value chain.

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



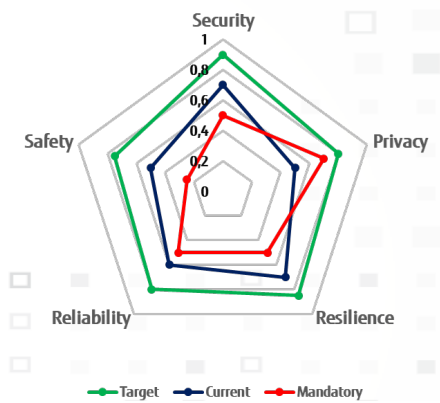
Measuring Trustworthiness

Merging Metrics to Characteristics

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

Domain specific knowledge, standards and regulations define the quantifiable metrics.

Security Characteristic



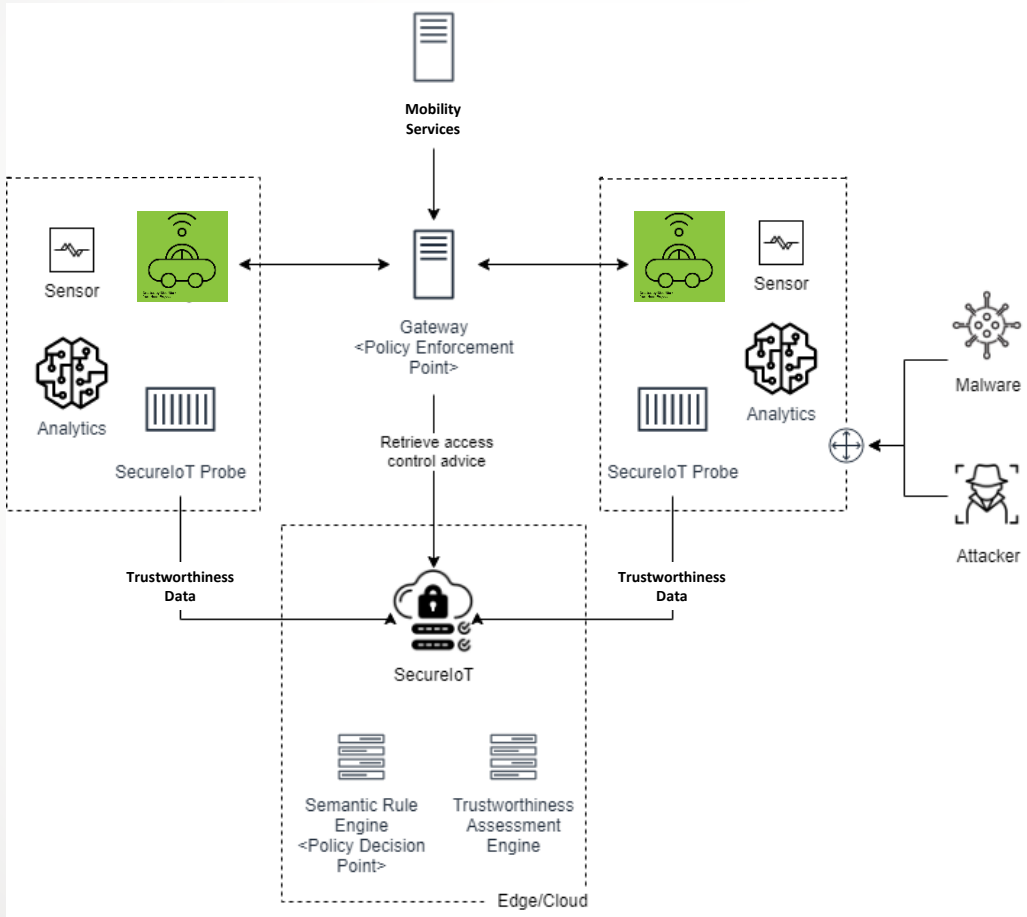
Device Metric
Manufacturer
Firmware Version
Model Number
Exposure Level
Mobility

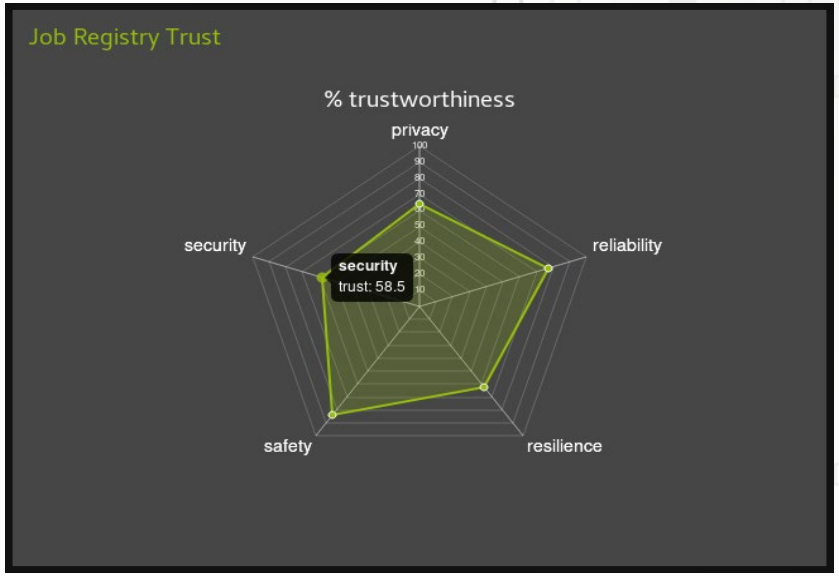
Communication Metric
Protocol (App Layer) Specific
Certificate Issuers

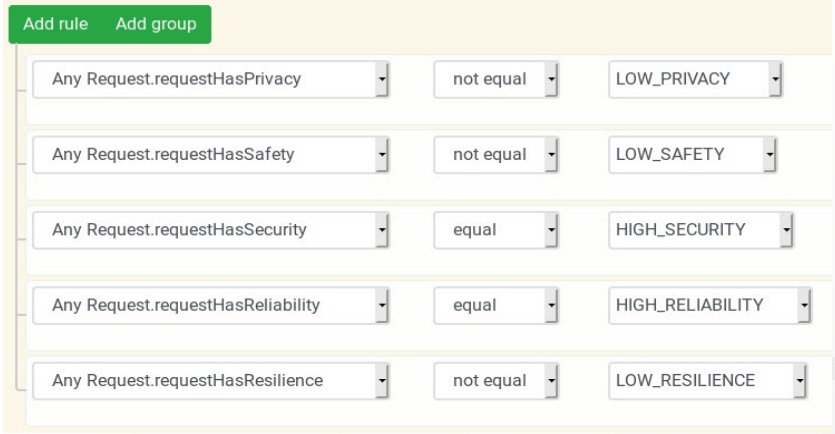
Behaviour Metrics
Network Presence
Activity Duration
Forwarding Delta
Message Destination

SecureIoT: Trustworthiness in Action

Demo Implementation







Self Driving Car icon created by Med Marki from the Noun Project

Future Work

Directions of Development

- **Security Standardisation**
  - Generic sets or catalogues of characteristics for comparison or mitigation of policies and Trustworthiness across geographic areas and legal systems.
  - Entity specific global trust ecosystem.
- **Catalogues of Trustworthiness metrics and schemas**
  - Extend common cyber security management system for automotive systems
  - Facilitate a broad application of Trustworthiness for autonomous systems.
- **Efficient Evaluation**
  - Minimize monitoring and calculation effort for low latency in edge based evaluation
  - Trustworthiness evaluation in a public place and verifiable – interplay of cloud and edge
- **Transparent Product Quality**
  - Continuous evidence-based logging and documentation of the operation parameters.
  - Evaluation of trustworthiness during the production of autonomous systems.
  - Documentation in a distributed ledger as proof of product quality.
  - Consider data sensitivity.

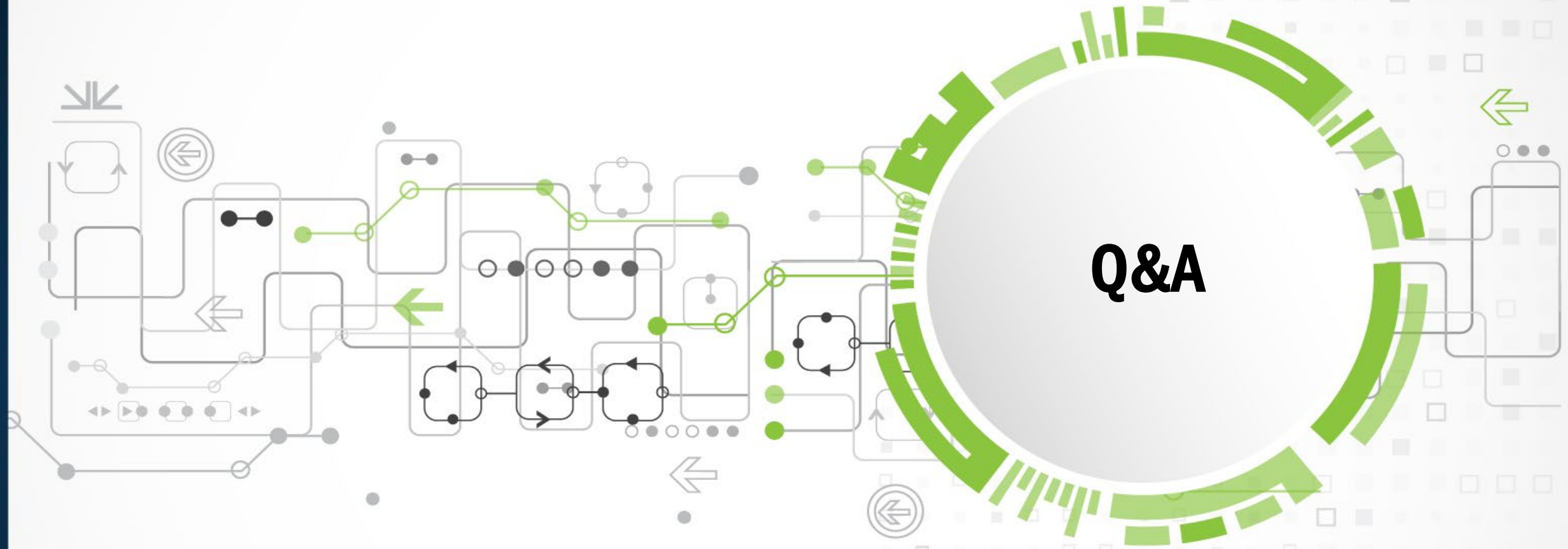
Conclusions

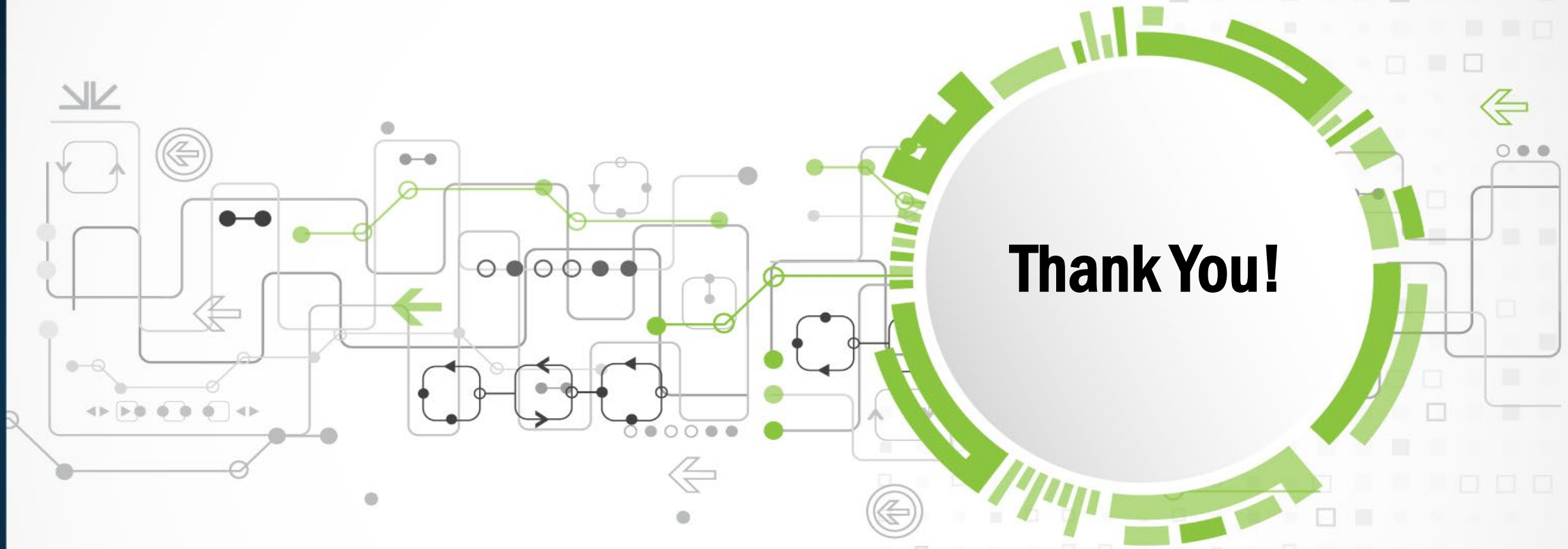
To strengthen resilience in autonomous systems, a better trust model facilitating policy management is imperative.

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 the autonomous systems environment.

In future work, the development of generic metrics, the integration into a cyber Security management system and the application to distributed manufacturing are of particular importance.


Q&A


Thank You!