InSecTT

Intelligent Secure Trustable Things

Bringing Internet of Things and Artificial Intelligence together: But is it Trustworthy?

Michael Karner, VIRTUAL VEHICLE Research GmbH

2022-06-23

IoTWeek 2022: Identity, trust and privacy in an intelligent, smart IoT World. Challenges and outcomes

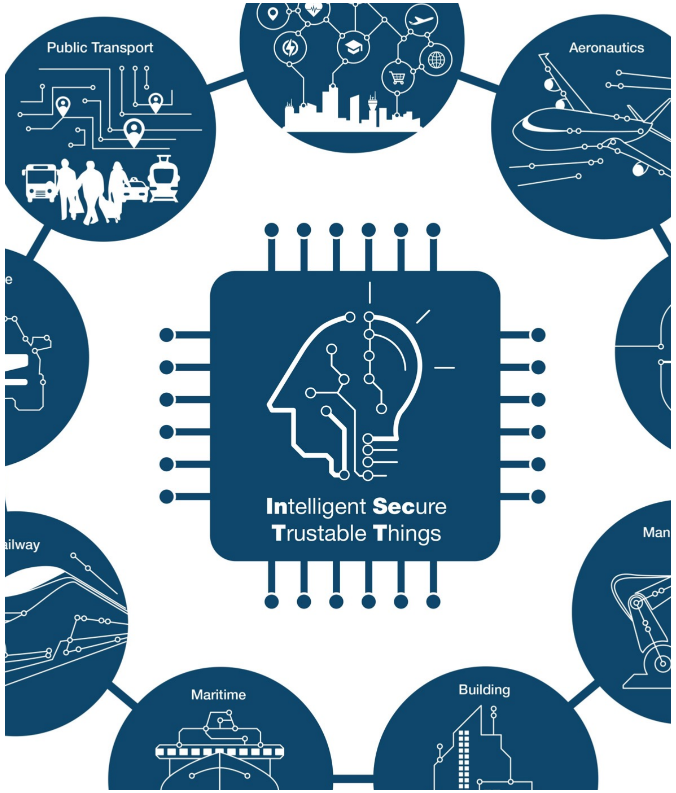
InSecTT has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey

Disclaimer excluding JU responsibility
The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

Artificial Intelligence of Things (1)

- **Artificial Intelligence of Things** (AIoT):
  natural evolution for both AI and IoT (mutually beneficial)
  - **AI increases the value of the IoT**
    - through machine learning -> transforming the data into useful information knowledge
    - Enabling sophisticated security analysis & protection
  - **IoT increases the value of AI**
    - through connectivity and data exchange

- **Moving AI to the edge**
  - **Processing data locally** on a hardware device
  - **Real-time applications** for self-driving cars, robots and many other areas in industry can be enabled

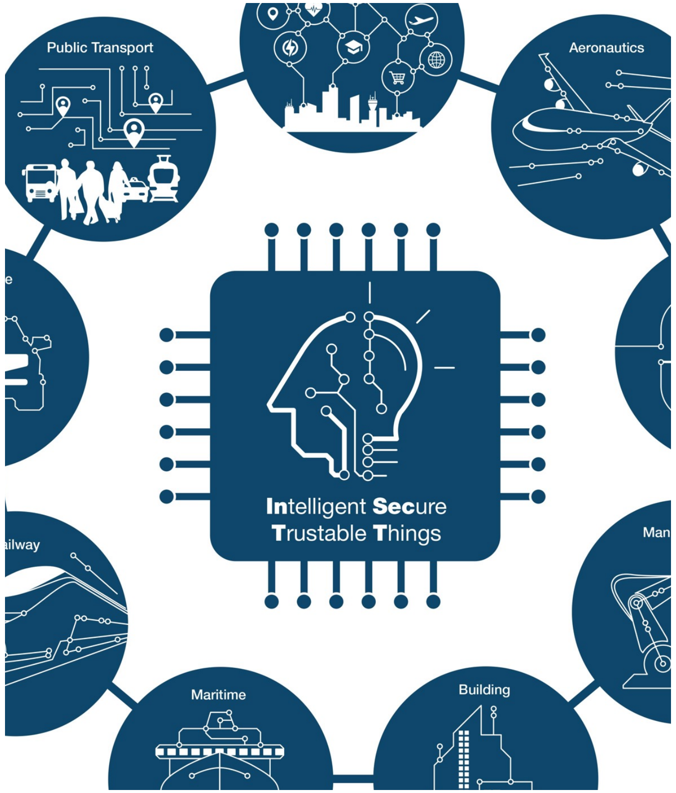


Artificial Intelligence of Things (2)

- **Users are challenged to understand and trust** their increasingly complex and smart devices
  - Resulting in **mistrust, usage hesitation and even rejection**
  - → **Ethics and public trust** in deployed AI systems are now receiving **significant international interest**

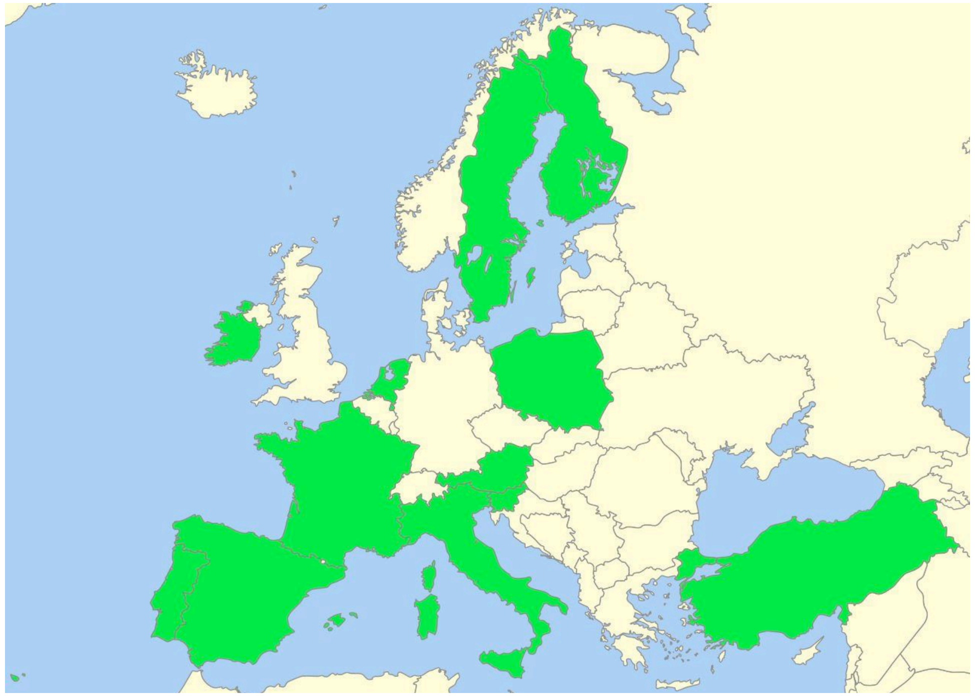
- **AIoT in InSecTT:**
  - Focus on **robustness and ethics**
  - Ensuring the developed systems are **resilient, secure and reliable**
  - Prioritizing the principles of **explainability and privacy**

- InSecTT is utilizing AI for **two core tasks** in the IoT context:
  - **AI-supported Embedded Processing** for industrial tasks like typical **speech and image recognition tasks** that AI is used for today, but **also specific smaller control and monitoring tasks** needed in **industry**
  - **AI enhanced wireless transmission**
    - Improving **reliability** as well as **security** in heterogeneous and even hostile environments



Project Data InSecTT

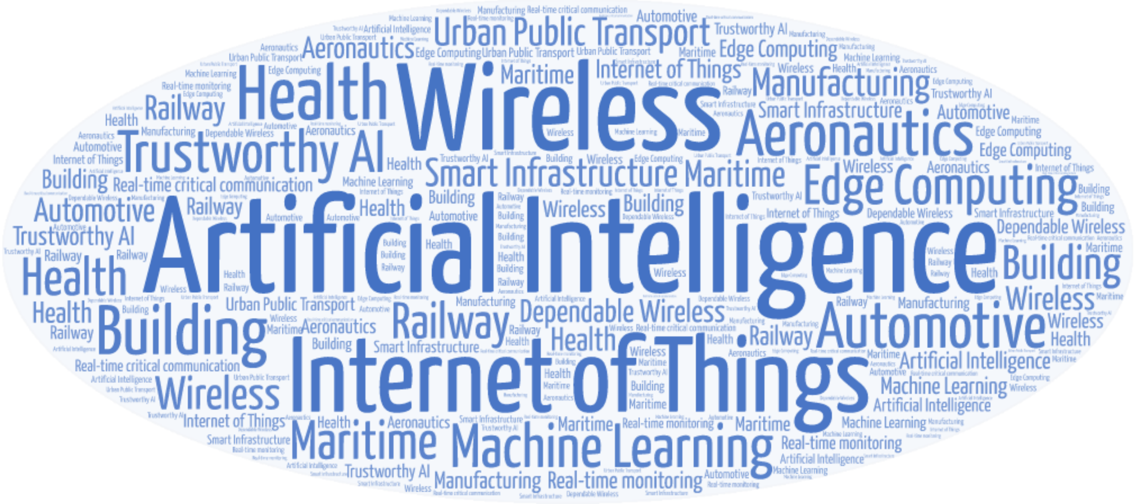
- **Funding**: ECSEL Call 2019 – Innovation Action
- **Coordinator**: VIRTUAL VEHICLE Research GmbH
- **Duration**: 36 months (June 2020 – May 2023)
- **Partners**: 52 from 12 countries (EU+Turkey)
- **Use Cases**: 16 from 9 industrial domains
- **Building Blocks**: 5 (reliable AI for IoT)
  5 (secure, safe and
  reliable wireless systems)
- **Effort**: 5600 person months
  (~155 full-time equivalents over 3 years)
- **Project size**:
  - Total: 48 Mio EUR / 25 Mio EUR Funding



Partners, e.g. VIF, ABB, AVL, Altran, CISC, CEA-LIST, Indra, JKU, Leonardo, Liebherr, KTH, NXP, RISE, Silicon Austria Labs, ST Microelectronics…

Project Goals & Objectives

- **In**telligent
  - Intelligent processing of **data applications** and communication characteristics locally at the edge
- **Sec**ure
  - Industrial-grade **secure, safe and reliable solutions** that can cope with cyberattacks and difficult network conditions
- **T**rustable
  - **Increase trust for user acceptance**, make AI explainable and give the user control over AI functionality
- **T**hings
  - With energy- and processing constraints, in heterogeneous and **hostile/harsh environments**
- applied in **industrial** solutions for European industry

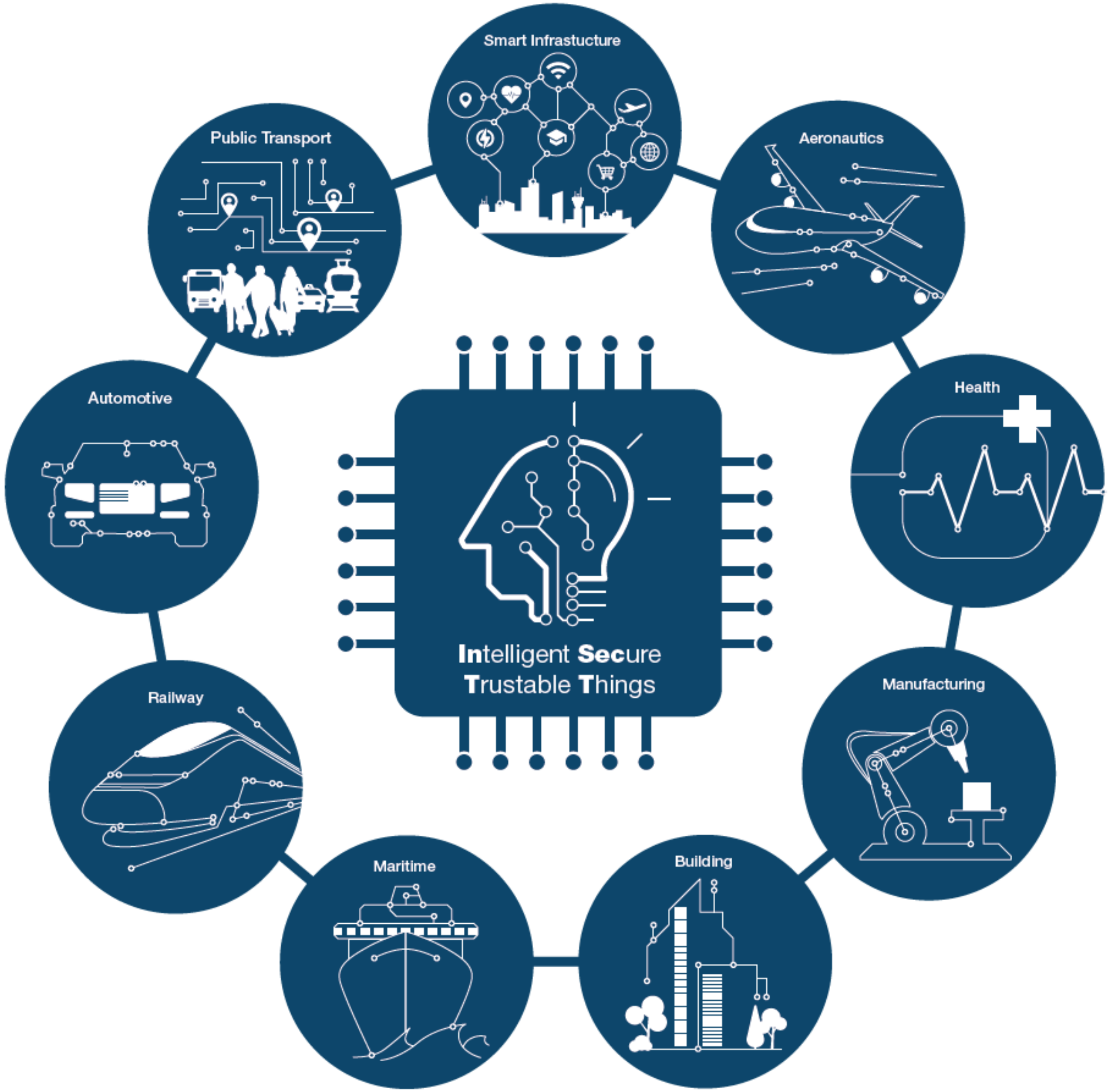


Bringing Internet of Things and Artificial Intelligence together
→ **AI + IoT = AIoT** (Artificial Intelligence of Things)

InSecTT Video: https://www.youtube.com/watch?v=CF8aVYzv_zo

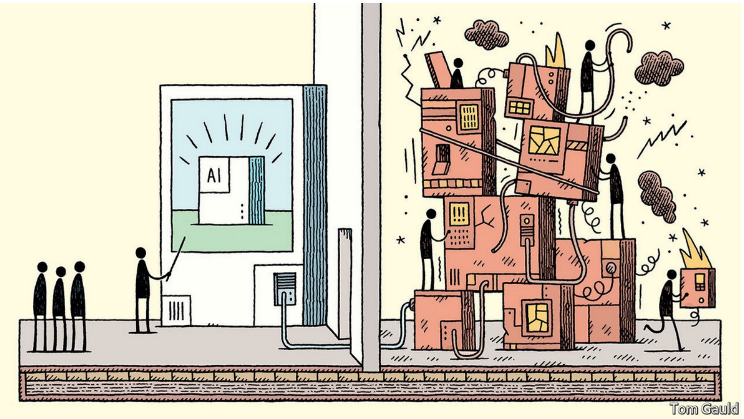
Edge… bring computation and data storage closer to the location where it is needed

Use Cases / Domains driving the Project

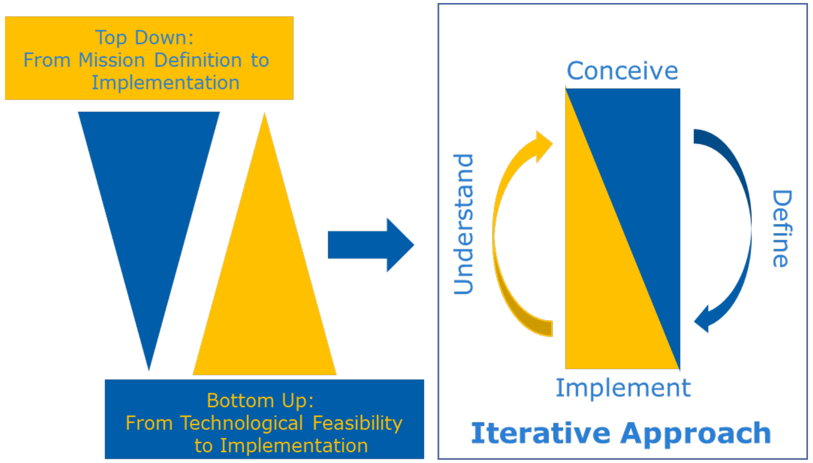


Building Trust in AI

- InSecTT: investigate and demonstrate how AI can be made trustworthy
  - Explainable, understandable, “interactable” AI
  - Future of AI is increasingly less seen in autonomy and more in collaboration between humans and AI



© Economist.com

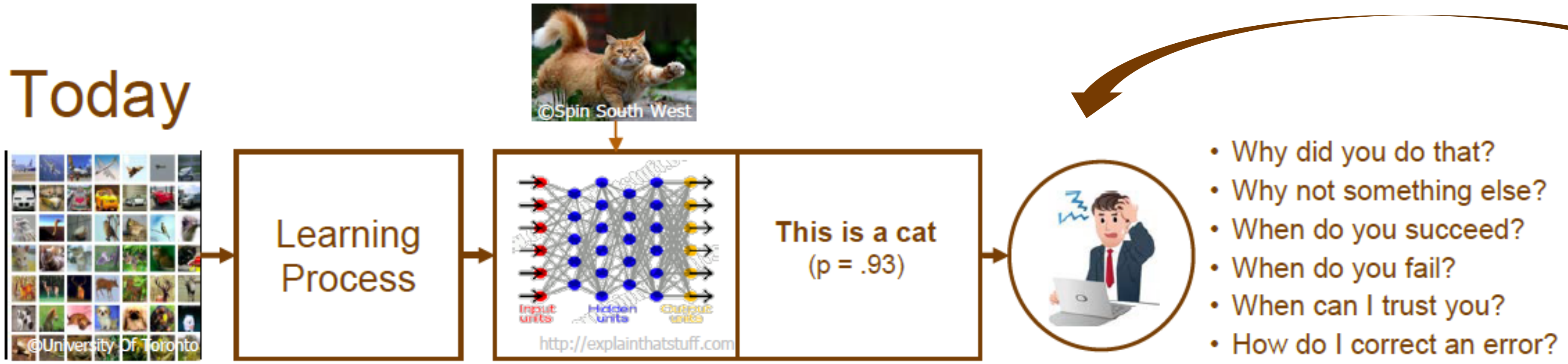


Top Down:
From Mission Definition to Implementation
Bottom Up:
From Technological Feasibility to Implementation
Conceive
Understand
Define
Implement
Iterative Approach

© Economist.com

Example Explainable (and understandable) AI

Today

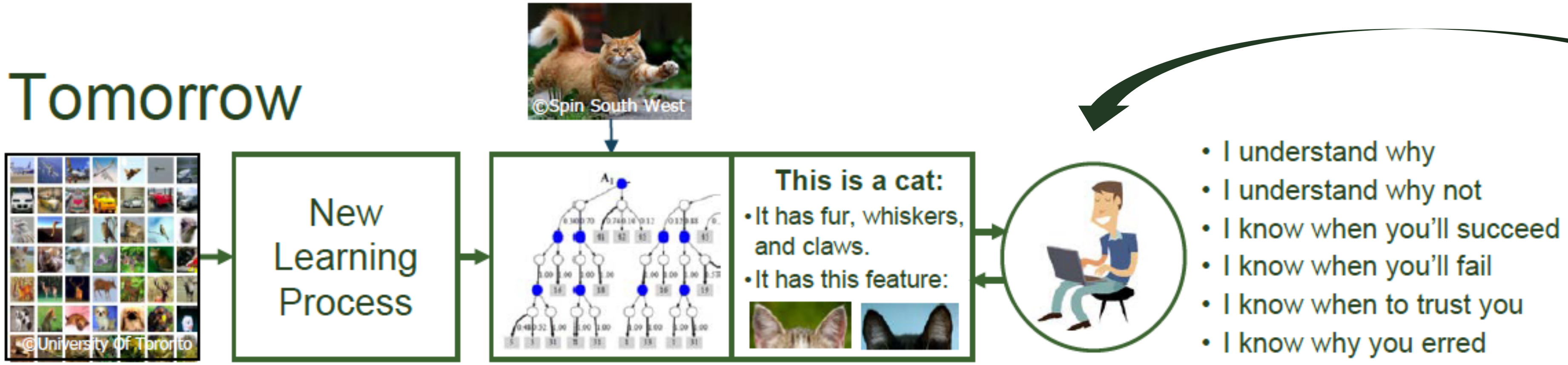


Training Data → Learning Process → Learned Function → Output → User with a Task

- Why did you do that?
- Why not something else?
- When do you succeed?
- When do you fail?
- When can I trust you?
- How do I correct an error?

No detailed knowledge about user and usage enter the technological development process !

Tomorrow



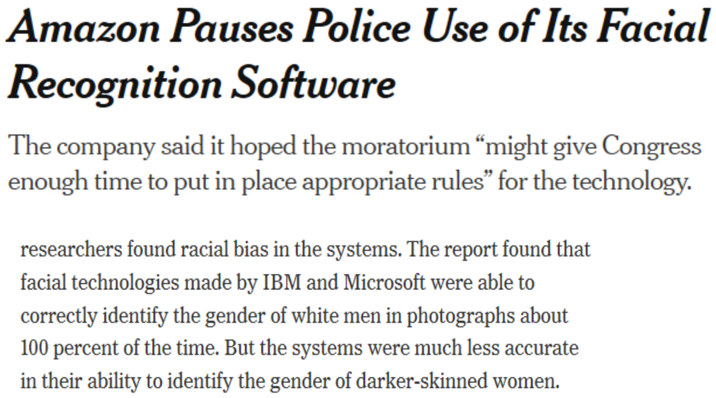
Training Data → New Learning Process → Explainable Model → Explanation Interface → User with a Task

- I understand why
- I understand why not
- I know when you'll succeed
- I know when you'll fail
- I know when to trust you
- I know why you erred

Detailed Knowledge about user and usage for technological development process !

https://www.darpa.mil/attachments/XAIProgramUpdate.pdf

Considering the user perspective may help avoid unintended consequences of AI?



Amazon Pauses Police Use of Its Facial Recognition Software

The company said it hoped the moratorium "might give Congress enough time to put in place appropriate rules" for the technology.

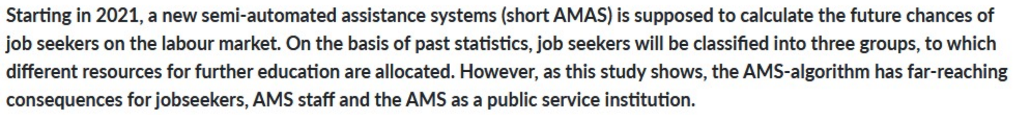
researchers found racial bias in the systems. The report found that facial technologies made by IBM and Microsoft were able to correctly identify the gender of white men in photographs about 100 percent of the time. But the systems were much less accurate in their ability to identify the gender of darker-skinned women.

The New York Times

June 10, 2020

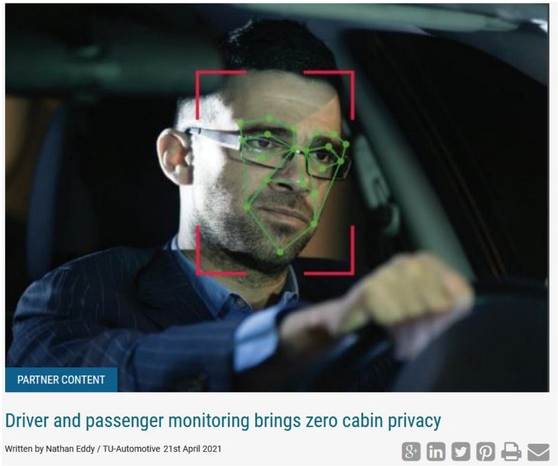
AI at work: Staff 'hired and fired by algorithm':
https://www.bbc.com/news/technology-56515827

T-800



Starting in 2021, a new semi-automated assistance systems (short AMAS) is supposed to calculate the future chances of job seekers on the labour market. On the basis of past statistics, job seekers will be classified into three groups, to which different resources for further education are allocated. However, as this study shows, the AMS-algorithm has far-reaching consequences for jobseekers, AMS staff and the AMS as a public service institution.

https://www.oeaw.ac.at/en/ita/projects/ams-algorithm



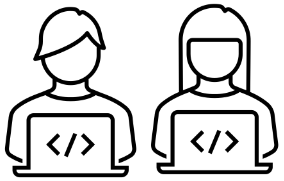
Driver and passenger monitoring brings zero cabin privacy

Written by Nathan Eddy / TU-Automotive 21st April 2021

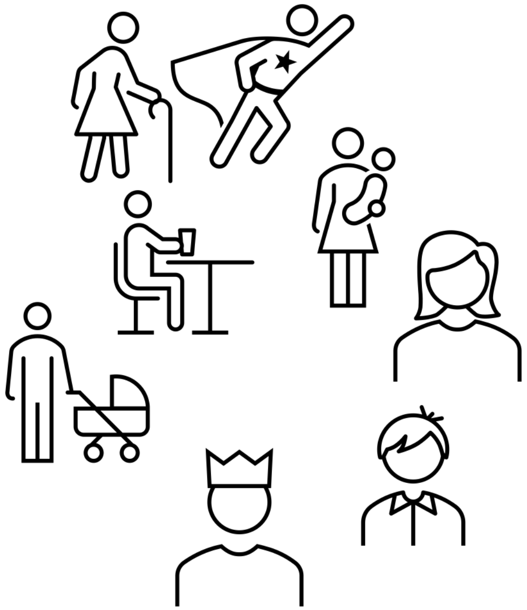
Two Different Perspectives toward Trustworthiness

Can we trust this algorithm works as we intend it?
How does it respond to a previously unknown stimulus?
…

Developer's Perspective



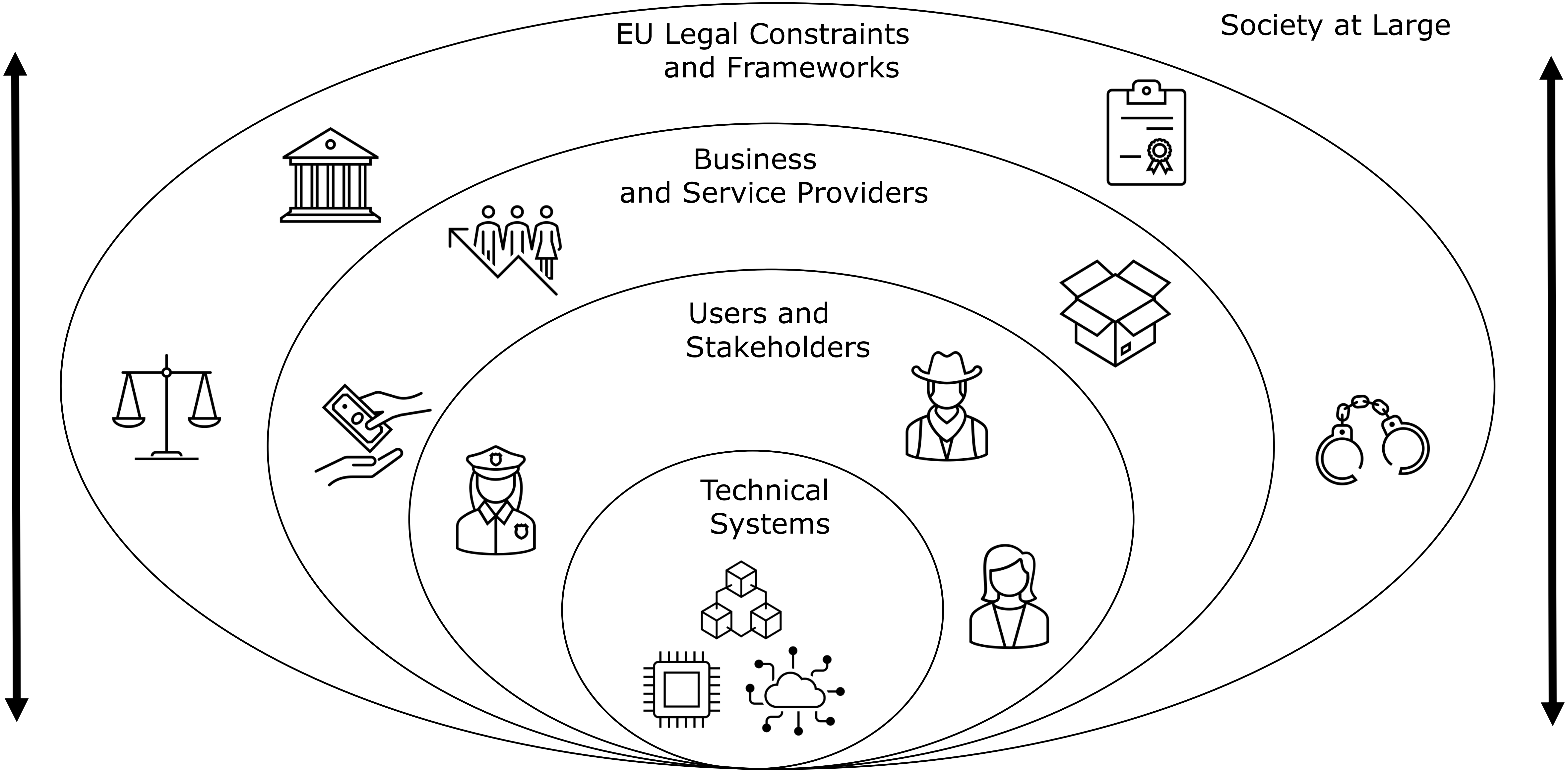
User's Perspectives



Can we trust this product does something useful, reliable, and does not cause us hidden problems or disadvantages later, that we do not understand now…

Very different aspects of trustworthiness!

Principles cut across various layers


Society at Large
EU Legal Constraints and Frameworks
Business and Service Providers
Users and Stakeholders
Technical Systems

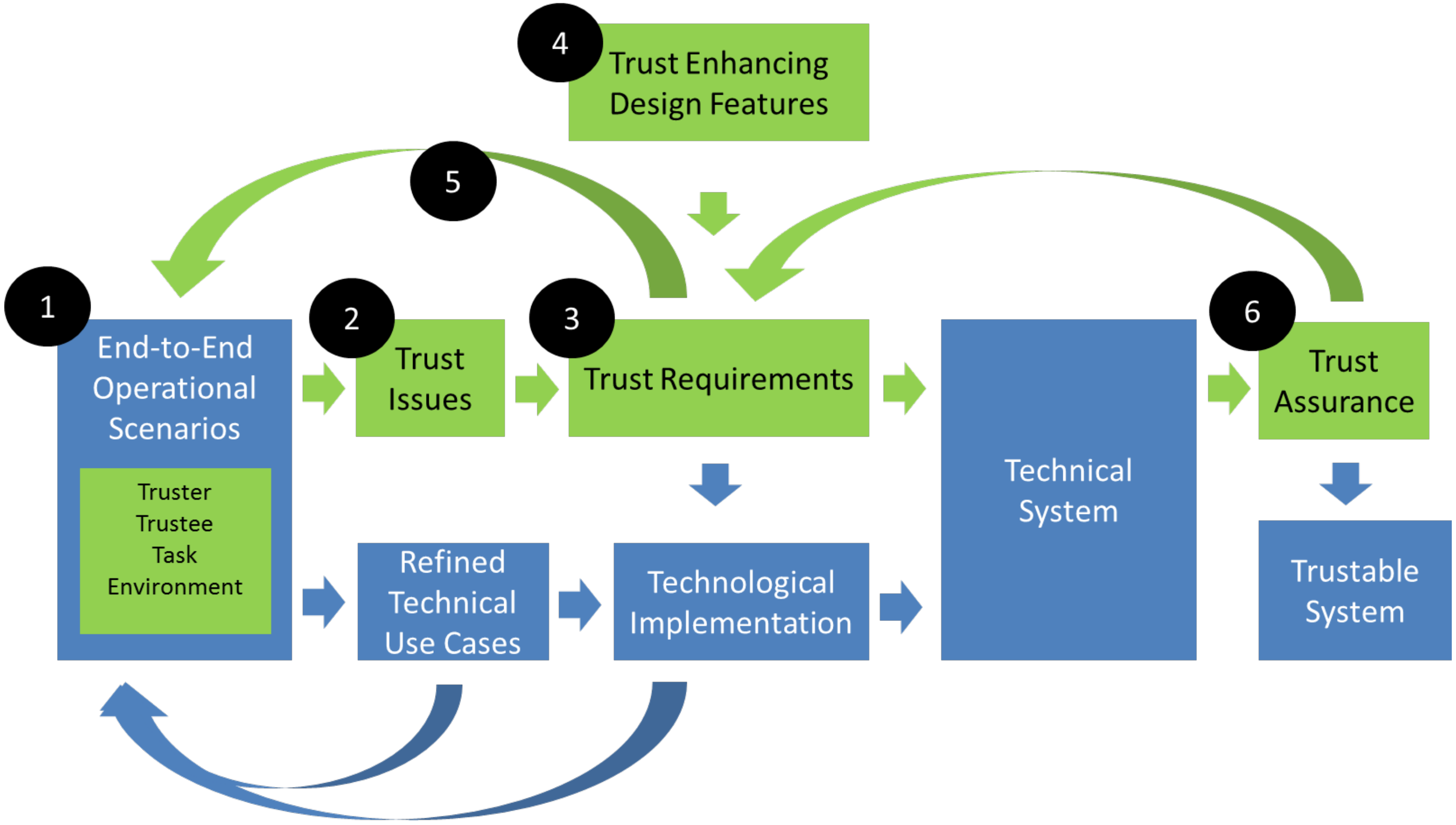
Trust Framework

.. is about ..

- stepping back
- to see the system more holistically
- to understand the people who have to build trust
- to understand the environment of usage
- to identify trust vulnerabilities
- to identify trust requirements

.. early on in the design process.

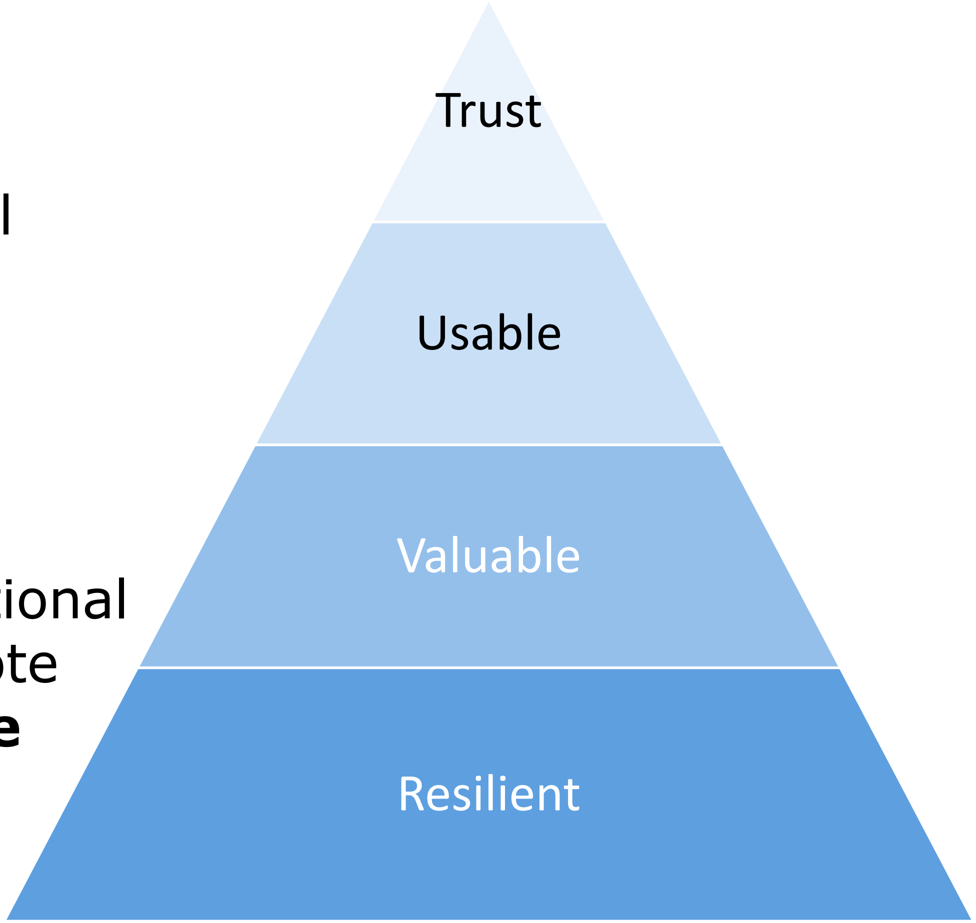
Trust Framework


4
Trust Enhancing Design Features
5
1
End-to-End Operational Scenarios
Truster
Trustee
Task
Environment
2
Trust Issues
3
Trust Requirements
Technical System
6
Trust Assurance
Refined Technical Use Cases
Technological Implementation
Trustable System

1. Analyse end-to-end operational scenario
   - With sufficient contextual information
2. Extract trust issues
3. Specify trust requirements
   - Internal and external ones
4. Propose trust enhancing design features
5. Iterations
6. Conduct trust assurance

Main Trust Enhancing Design Guidelines

- **Keep the human-in-the-loop**: build collaborative structures rather than hierarchical structures
  - Repeated touch-points
- Consider **increasing** the **transparency** of high-level automation **to promote greater trust**
- **Simplify** the **algorithms** and **operations** of the automation **to make it more comprehensible**
- Provide **users** with accurate, ongoing **feedback concerning the reliability** of system and the situational factors that can affect its reliability in order to promote **appropriate trust** and **improve task performance**



Reference Architecture: Objectives

- **Definition**: “A set of guidelines for infrastructure organization of IoT use cases supporting the objectives of the projects (AI at the edge)”
- The framework for a **high-level analysis** of all building blocks of use cases in different industrial domains
- **Interface** and **vulnerability** analysis per layer and entity.
- Framework for **reusability** and **cross-domain** interpretation
- High level perspective of use case **requirements, road-map, and forecast analysis**
- Compilation of **expertise** accumulated across different **use cases** in different **industrial domains**
- Framework for **standardization** needs in detail

Security / Privacy

Energy constrained

Edge/Cloud AI-IoT

Trust and Architecture

Trusted AI in the edge

new cooperations

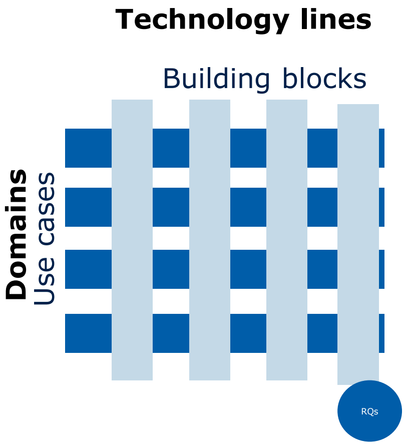
worldwide uptake of “European Technology” and infrastructure

EU as a center of leading, trusted, user (citizen) friendly, secure, and reliable AI-IoT ecosystems

Creating trust in AI-IoT solutions and increasing their social acceptance

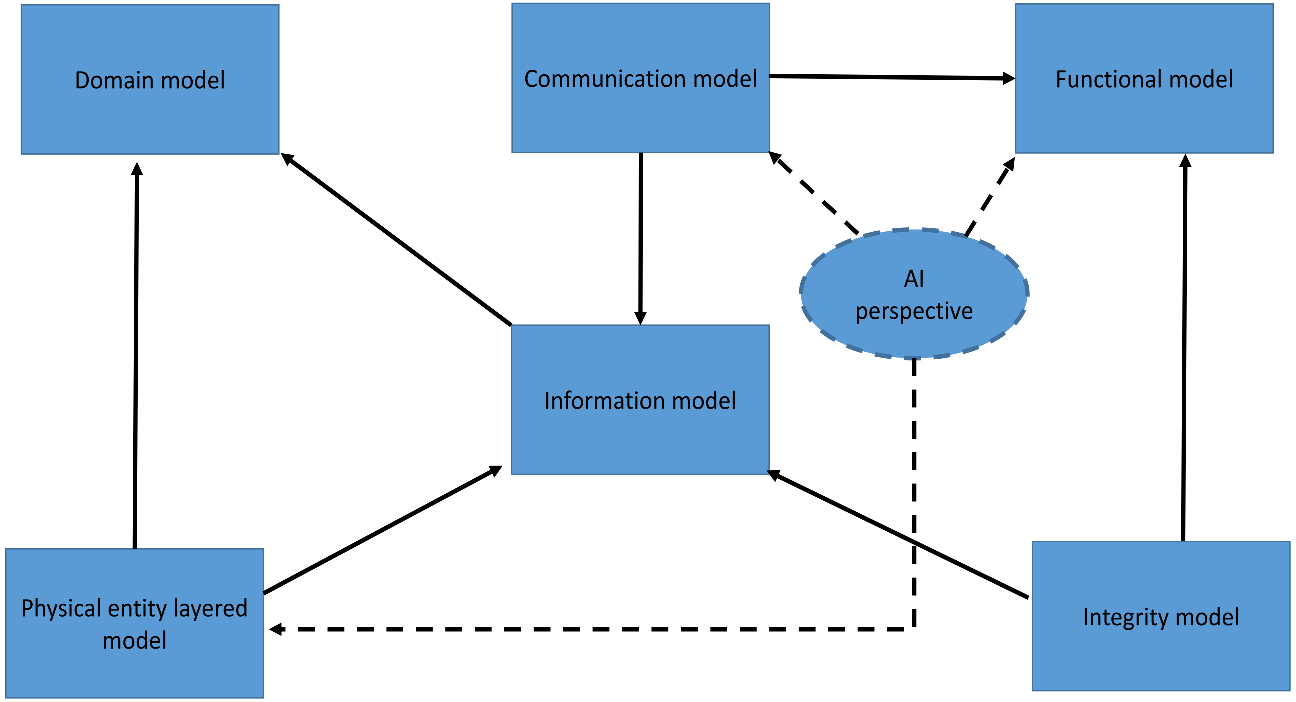
full potential of the AI-Internet of Things for the **benefit of Europe’s Industry, SMEs and Start-ups**

Additional private investments by the for-profit companies



Reference Architecture

- The proposed InSecTT Reference Architecture (RA) consists of **multiple views or perspectives of a generic AIoT system**
- The multiple views approach is **useful for modern AIoT use cases with multiple stakeholders**
- The InSecTT RA consists of
  - Entity model
  - Functionality Model
  - Information Model
  - Domain Model
  - Communication model
  - Ontology model



Summary

- Bringing Internet of Things and Artificial Intelligence together

  → **AI + IoT = AIoT** (Artificial Intelligence of Things)

  - Focus on **robustness and ethics**
  - Ensuring the developed systems are **resilient, secure and reliable**
  - Prioritizing the principles of **explainability and privacy**

- Building Trust in the IoT & AI
  - User acceptance!

- Showcased in a broad variety of industrial domains

InSecTT

Intelligent Secure Trustable Things

Thank you!

www.insectt.eu **michael.karner@v2c2.at**

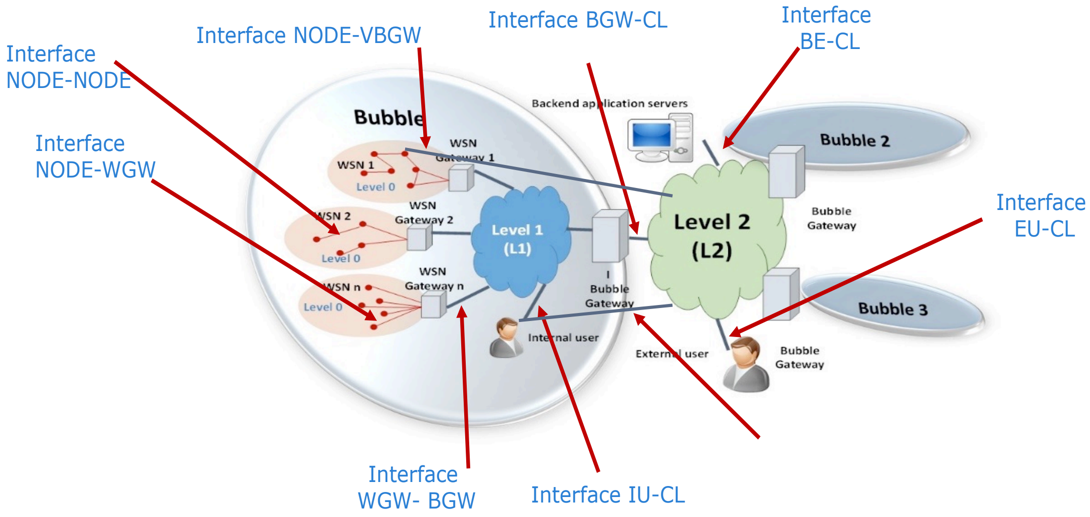
@InsecttProject (Twitter) **LinkedIn** **YouTube**

InSecTT has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey

Disclaimer excluding JU responsibility
The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

RA: Bubble Concept

- **Bubble**
  - Set of **objects in a confined space** communicating via **wireless** and supporting **wireless infrastructure** in an industrial domain
  - Managed by a **unique physical and/or virtual gateway**
  - Support **improved AIoT solutions** using the **Bubble gateway as Edge processor**
- **Attributes**
  - Interoperability (single protocol or semantics model for interoperability)
  - Integration of new and legacy critical industrial sensors to a modern AIoT infrastructure
  - Improved interfaces to support trustable AIoT solutions
- **Three-level organization** ideal for critical industrial use cases
  - L0 Wireless
    - Nodes and WSN Gateway
  - L1 wireline- existing critical infrastructure
    - For example: aeronautical internal bus, CAN bus
  - L2 interoperability
    - Cloud, Edge servers. The Bubble Gateway can also act as fog or Edge server.



Evolution of the Bubble Concept

Based on ISO/SNRA
Interoperability ETSI M2M, IoT-ARM
L0/L1/L2 layering for Wireless/wireline Model

Dependability inside the bubble
Integration Wireless/wireline industrial WSN and IoT
Cross-domain reusability
Interoperability
Integrated sensors into IoT

Full IoT architecture (around the bubble)
Hybrid ISO SNRA ITU, ISO, AIOTI, IEEE IoT architectures
L0/L1/L2 layering for Wireless/wireline
Security sublayers and processes

Dependability inside the bubble
Integration Wireless/wireline industrial WSN and IoT
Cross-domain reusability
Interoperability
Integrated sensors into IoT
Trustworthiness and security metrics
Bubble gateway as Edge processor
Inter-bubble communications based on trust indicator
Blockchain compatibility

Full IoT architecture (around the bubble)
Hybrid ISO SNRA ITU, ISO, AIOTI, IEEE IoT architectures
L0/L1/L2 layering for Wireless/wireline
Security sublayers and processes
Specific AI models and impact analysis

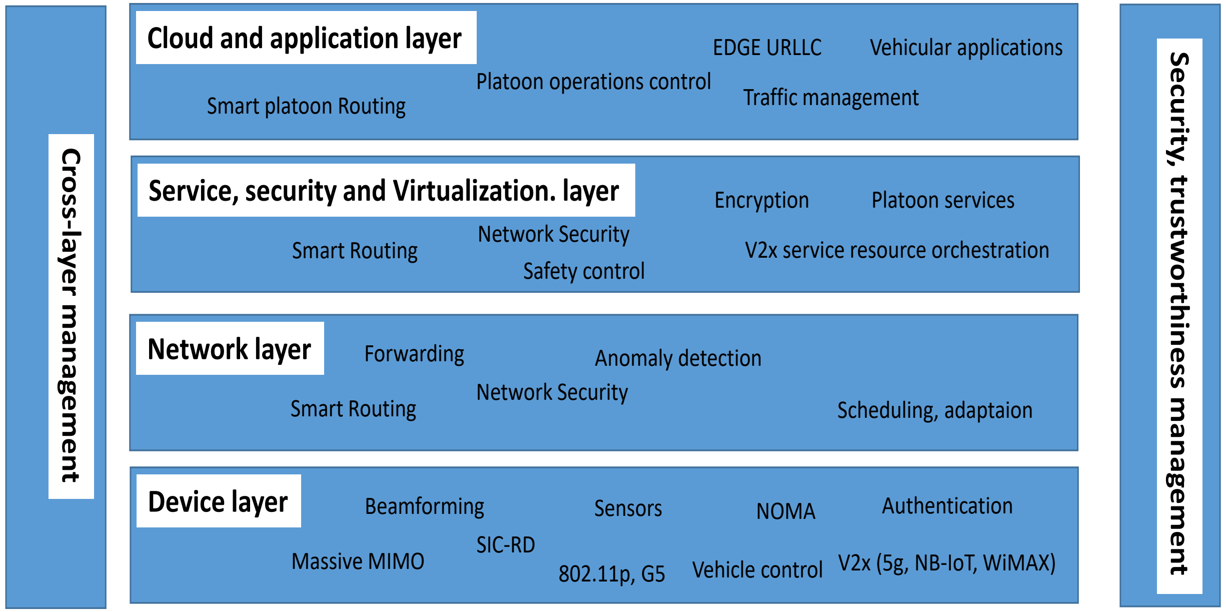
Virtualized Bubble
Multiple connections inside the Bubble
Long and short-range communications
Direct cloud connections inside the bubble and for internal users

What do you get by following the Bubble specs?

- **Guidelines** to achieve **dependability, security, safety, privacy and trustworthiness** inside the bubble
- Specific measures for interaction between **Wireless and wireline infrastructure with real time constraints**
- **Cross-domain interoperability**
- **International IoT standards compatibility**
- **Privacy and trustworthiness by design** approach
- Collected experience of real **industrial use cases**
- Integrated **trust methodology** to include end user and stakeholder perspective

Example Use Case: Platooning

- Concept of the bubble applied to **autonomous vehicles and smart transportation systems with cellular infrastructure**
- Interface definition and trade-off analysis in different platooning scenarios
- Hardware and software interface analysis



Cross-layer management

Cloud and application layer

EDGE URLLC

Vehicular applications

Platoon operations control

Smart platoon Routing

Traffic management

Service, security and Virtualization. layer

Encryption

Platoon services

Network Security

Smart Routing

V2x service resource orchestration

Safety control

Network layer

Forwarding

Anomaly detection

Network Security

Smart Routing

Scheduling, adaptaion

Device layer

Beamforming

Sensors

NOMA

Authentication

SIC-RD

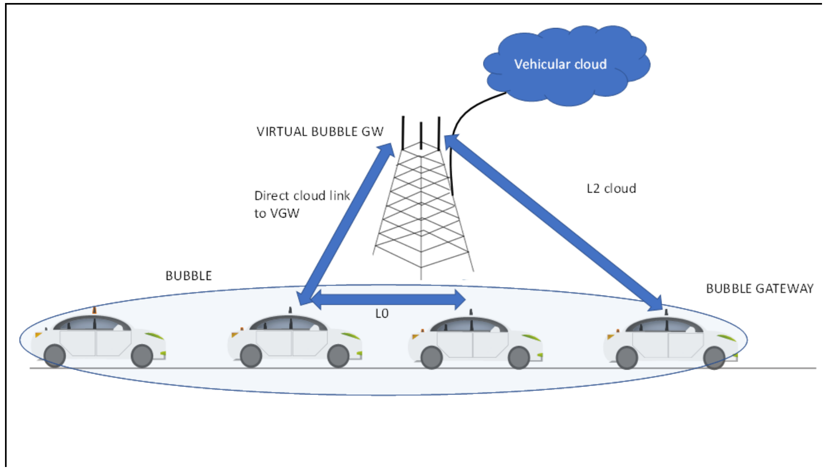
Massive MIMO

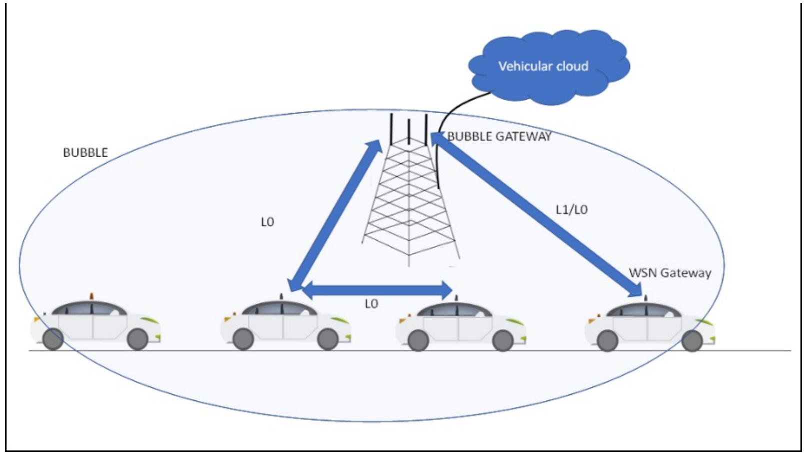
802.11p, G5

Vehicle control

V2x (5g, NB-IoT, WiMAX)

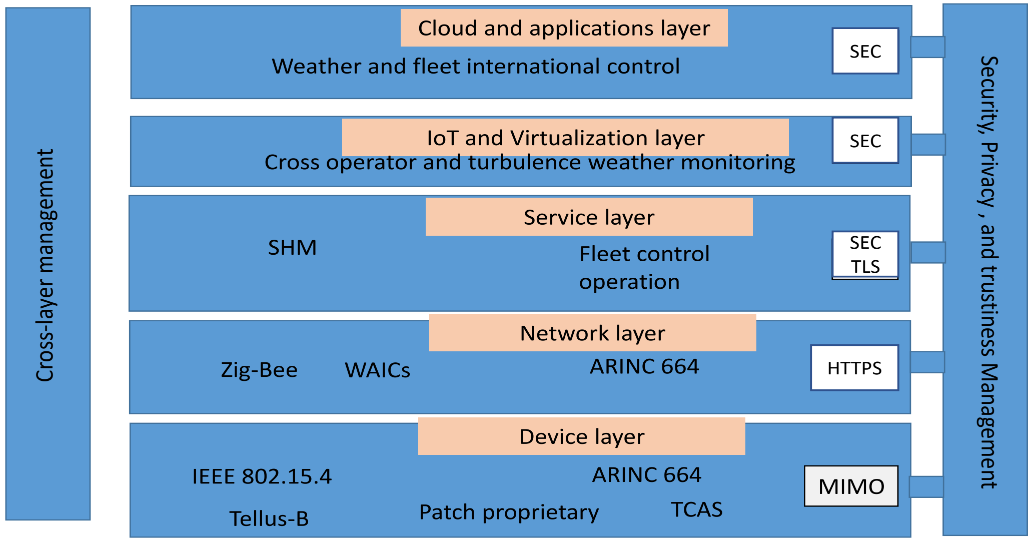
Security, trustworthiness management





Example Use Case:
Wireless Avionics Intra-Communications

- Adaptation of the reference architecture for **intra-communication systems on board aircraft.**
- Bubble concept to provide immunity against interference
- Functionality model adapted to provide critical real time performance compatible with ARINC 664
- Closely correlation of cybersecurity and safety in the aeronautics industry
- Trustworthiness analysis of wireless solutions for aeronautics



Cross-layer management

Cloud and applications layer
Weather and fleet international control
SEC

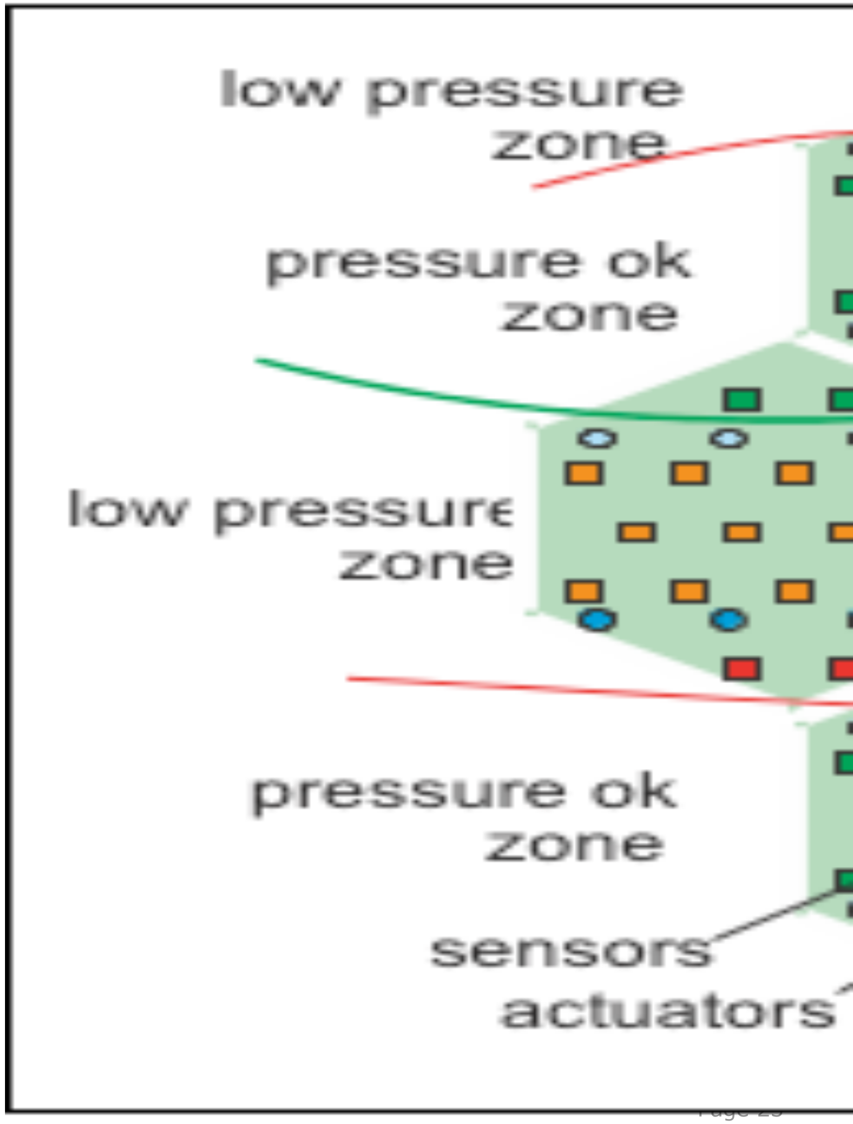
IoT and Virtualization layer
Cross operator and turbulence weather monitoring
SEC

Service layer
SHM
Fleet control operation
SEC
TLS

Network layer
Zig-Bee
WAICs
ARINC 664
HTTPS

Device layer
IEEE 802.15.4
Tellus-B
ARINC 664
Patch proprietary
TCAS
MIMO

Security, Privacy , and trustiness Management



low pressure zone
pressure ok zone
low pressure zone
pressure ok zone
sensors
actuators