Smart Wireless Solutions – Building Trust in the Internet of Things

Dr. Michael KARNER
VIRTUAL VEHICLE Research Center, Graz/Austria

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

Why Wireless?

Ariane 5

- Telemetry system of 600 to 800 sensors
- Thousands of cables spread all over the 40 meter rocket
- 70% of Ariane5 avionics mass are cables

Airbus A380

Source: faz.net / © AFP

Mercedes Benz E320 CDI T-Modell

Source: autobild.de

DEWI – Dependable Embedded Wireless Infrastructure

- **Coordinator**: VIRTUAL VEHICLE Research Center
- **58 Partners** (13 SMEs, 20 LEs, 25 academic)
- **11 Countries** (AT, BE, ES, FI, FR, IE, LV, NL, PL, PT, SE)
- **21 industry-driven Use Cases (TRL 3-4)**
- **More than 20 demonstrators**
- **4 Industrial Domains**: Automotive, Aeronautics, Building, Rail +Interoperability
- **39.6 M€** Project Budget
- **2014 – 2017**
- **"150 dedicated people working full-time over 3 years"**

www.dewiproject.eu

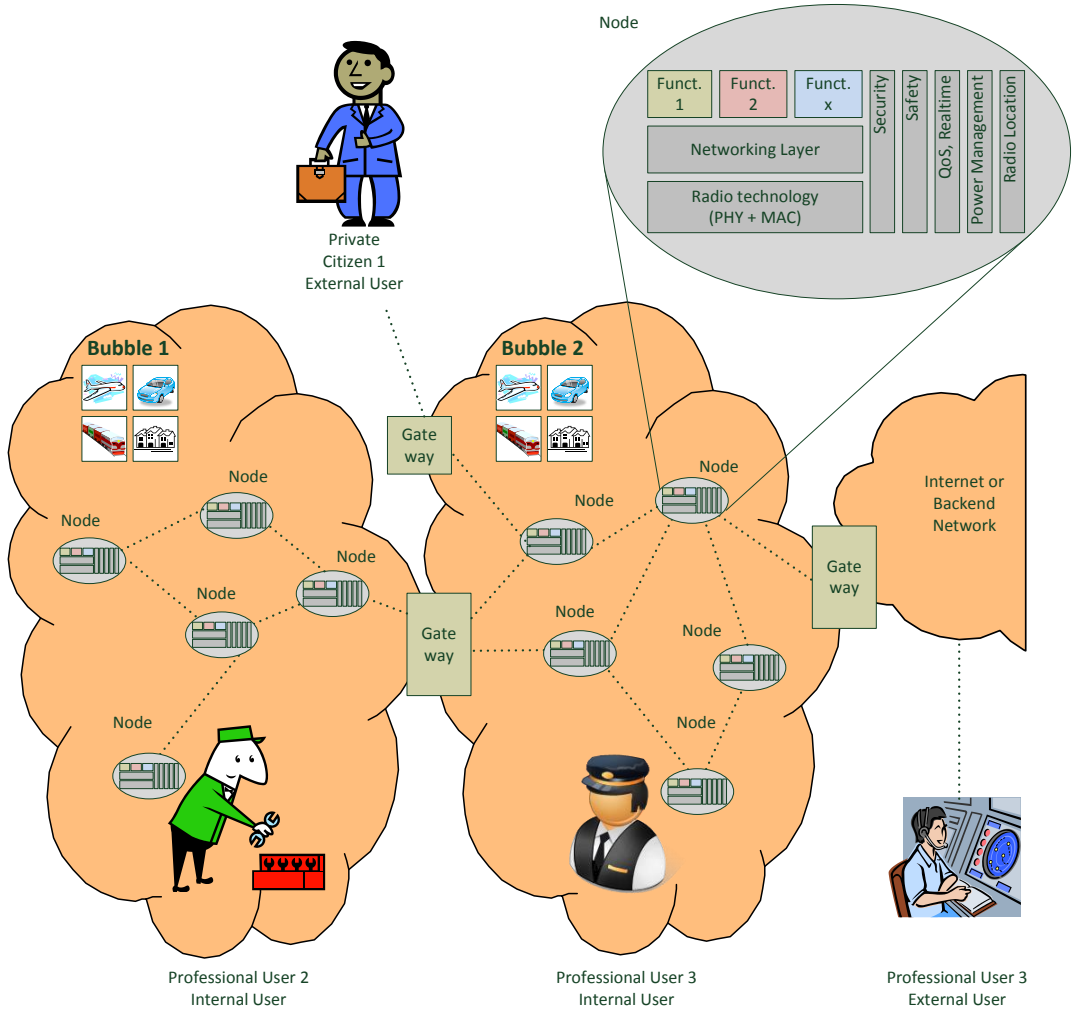
Dependable **E**mbedded **W**ireless **I**nfrastructure

- Wireless connections may reach far beyond mere communication
- In particular in combination with information retrieval from the close environment via WSN
- Key solutions for increased flexibility of citizens (incl. professional users) in their everyday environments (buildings, cars, trains, and airplanes)
  - More local personal control
  - Less stress
  - Less overhead
  - Increase comfort and safety

www.dewi-project.eu

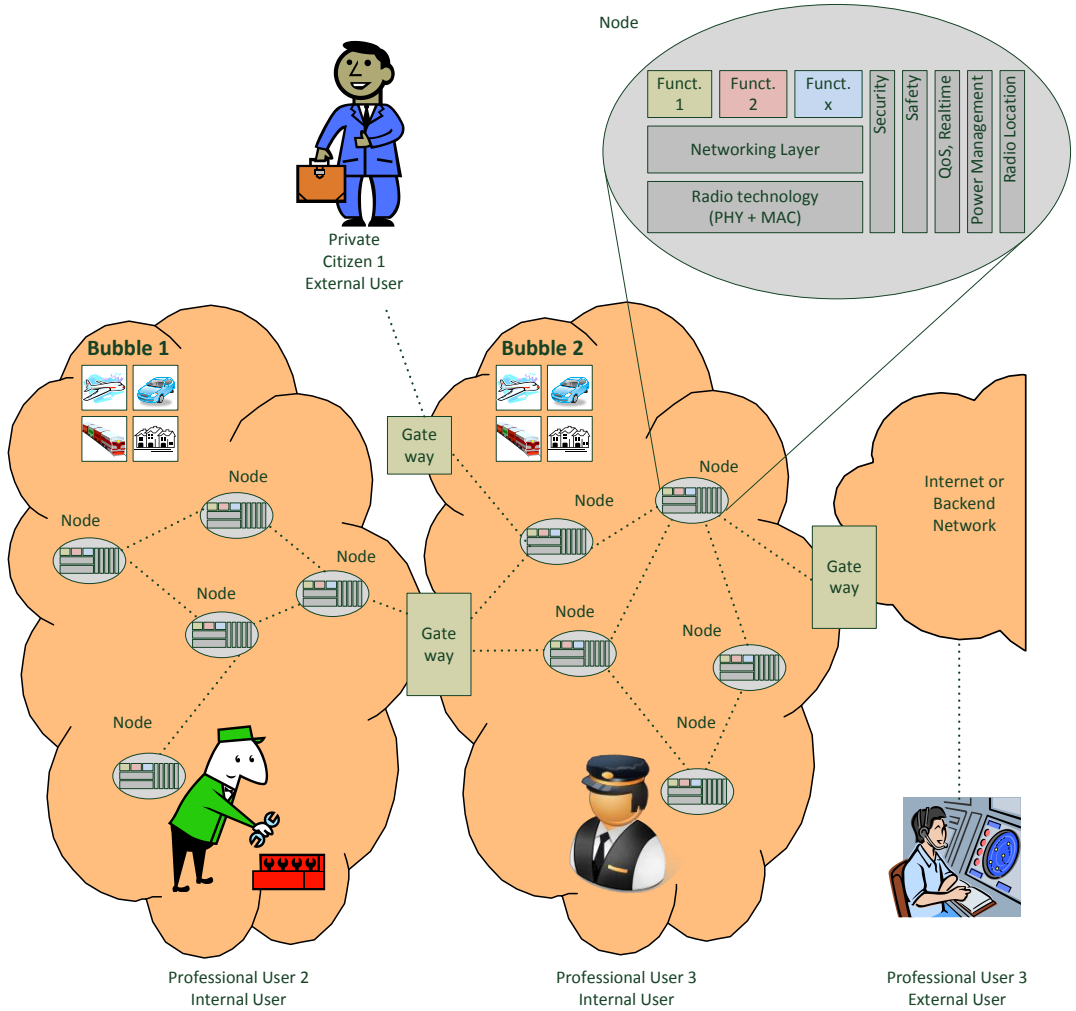
Core Elements of DEWI: Sensor & Communication Bubble

- Bubble elements located in **short range** to each other (local confinement)
- **No handover mechanisms**
- Bubble may be organized in **different topologies**, may be distributed (ad-hoc network) or centralized
- Bubble can interact with other Bubbles / outside world **via DEWI Bubble Gateways only** (no direct access from outside)



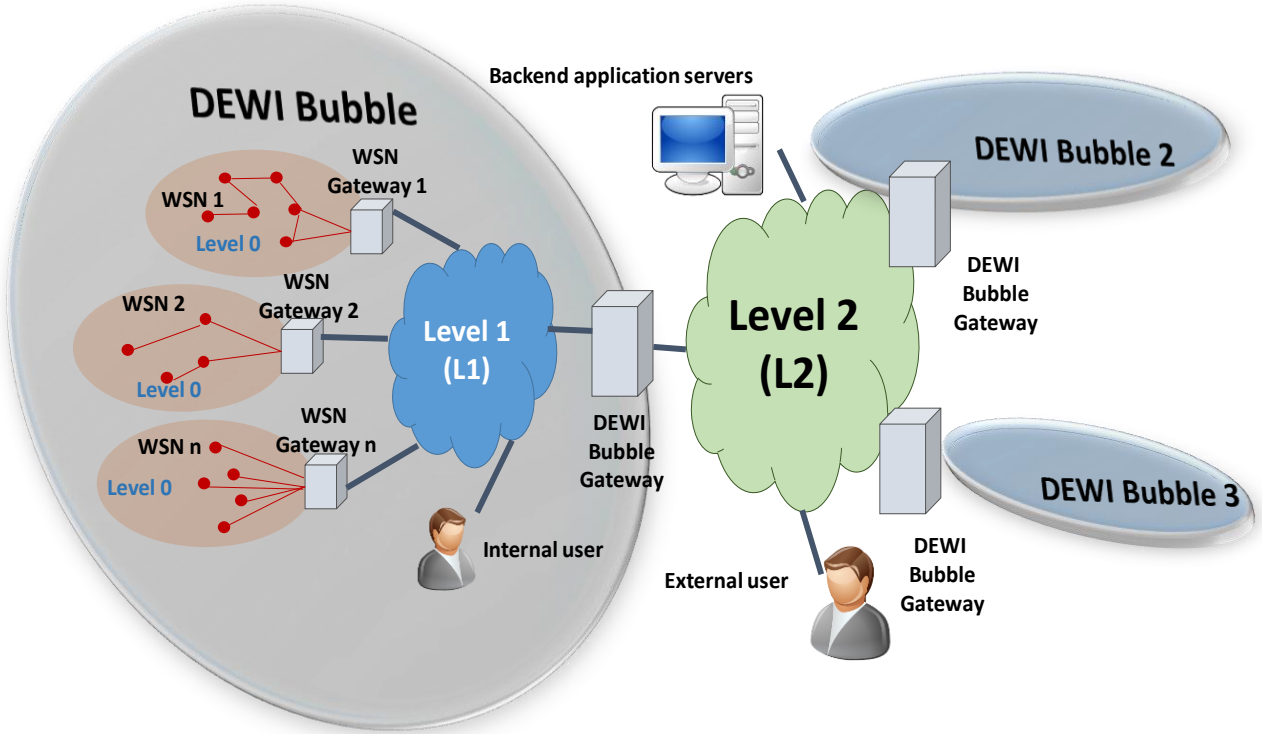
Core Elements of DEWI: Sensor & Communication Bubble

- A **DEWI Bubble Node** is a wireless system that acts as
  - a source of traffic
  - a destination of traffic
  - or a relay node
- A **DEWI Bubble Gateway** is an interface between
  - bubbles or
  - a bubble and the outside world (wireless and wired)
- **Users** (int./ext.) may be
  - professional users
  - private users / citizens



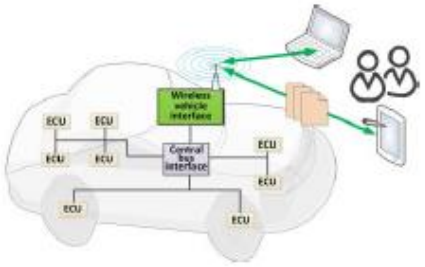
Core Elements of DEWI: High-level Cross-Domain Architecture

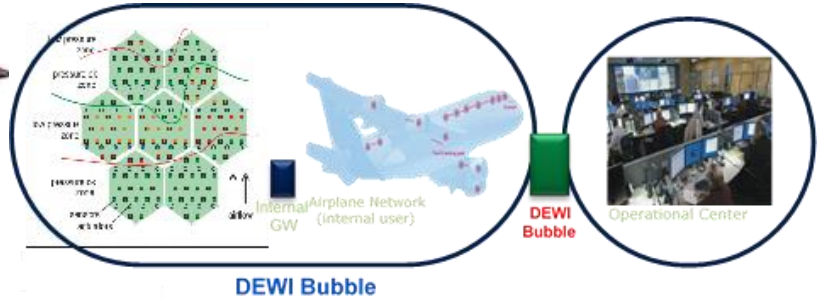
- 3-Level Architecture applicable to all domains
- Fully compliant with international standards (e.g. ISO/IEC 29182) but much more elaborate

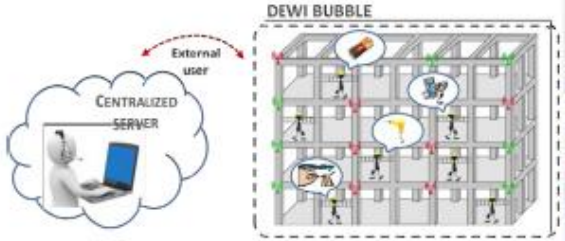


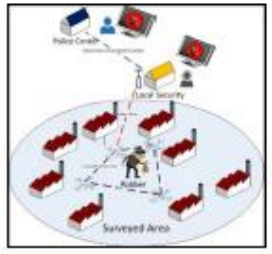
DEWI – 21 Use Cases from European Industry

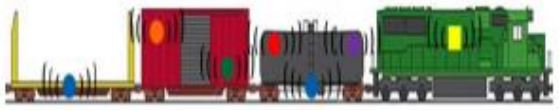
- Aeronautics, Automotive, Rail & Building

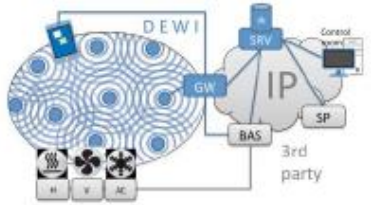






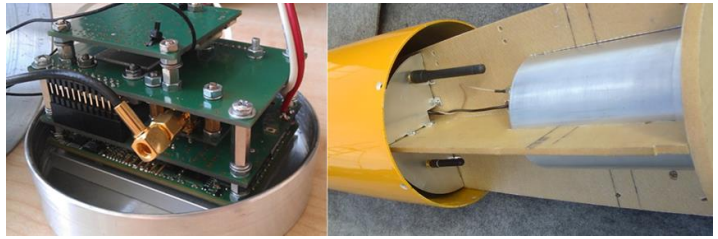




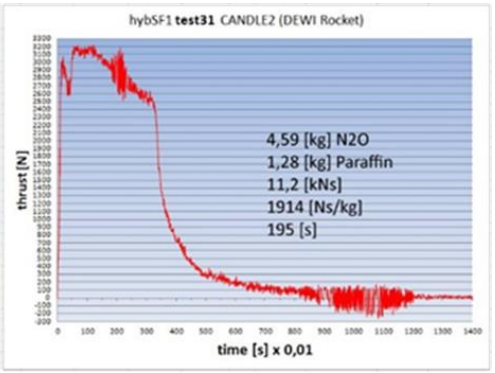


Aeronautics

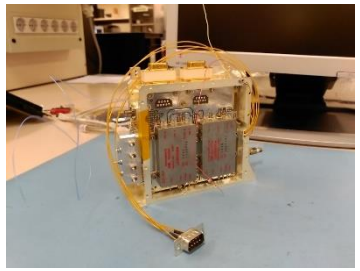
On-board rocket terminal



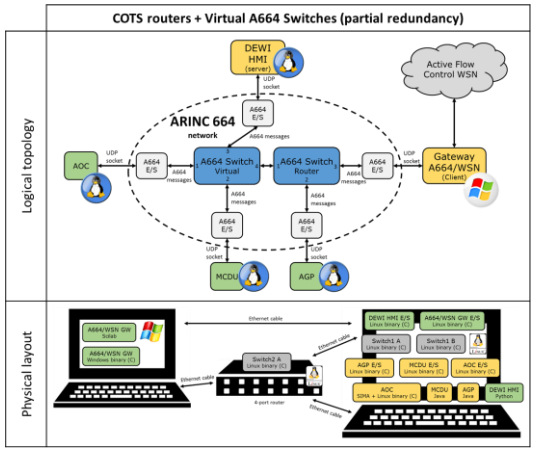
Rocket launch tests and RF trajectory monitoring



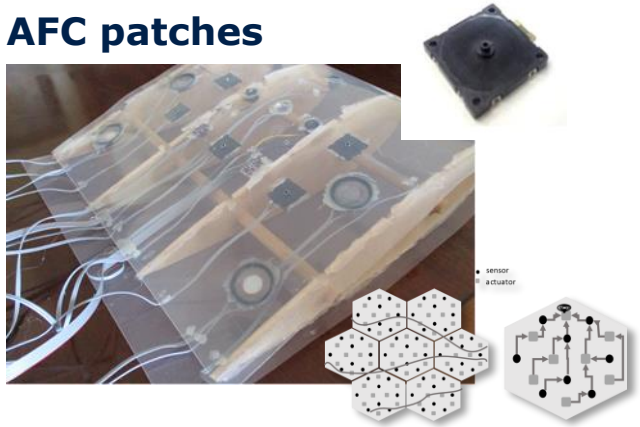
Multi-Telemetry Logger integration tests



Integration with internal aeronautics network

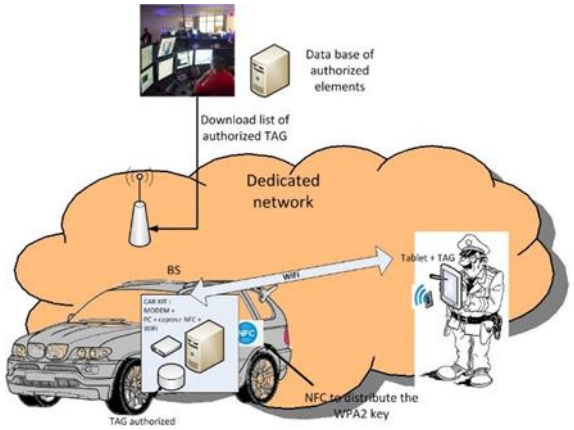


AFC patches

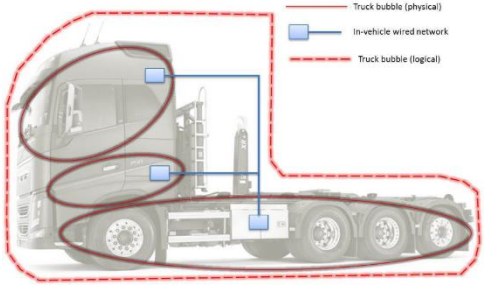


Automotive

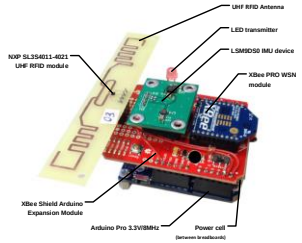
PMR for safety personnel (e.g. police)

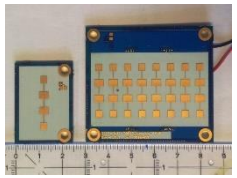


Integration platform / Truck with wireless prototype sensors

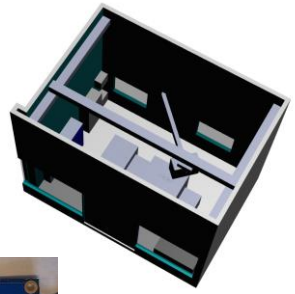


Identification and localization of sensors

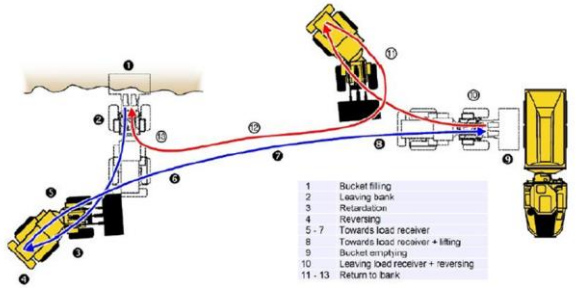




Scalability and coexistence of WSN for testbeds

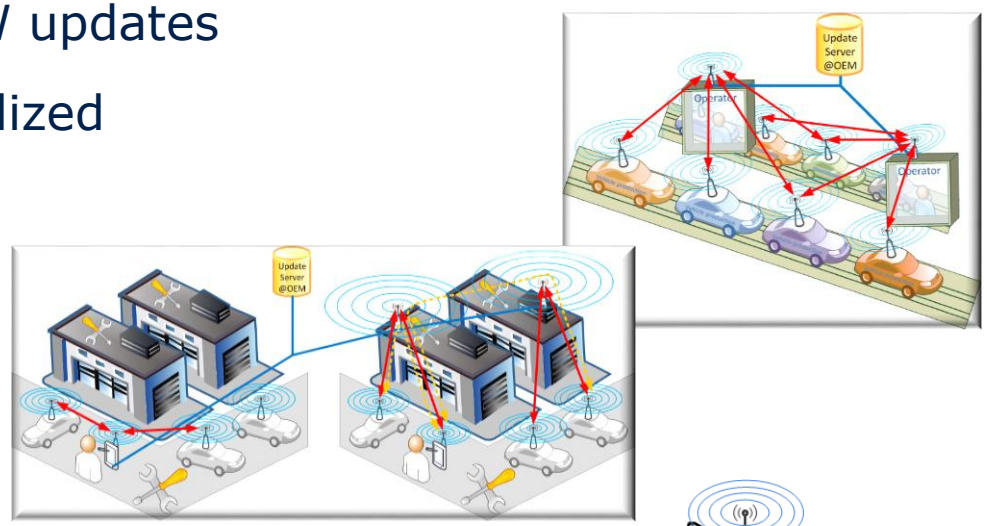


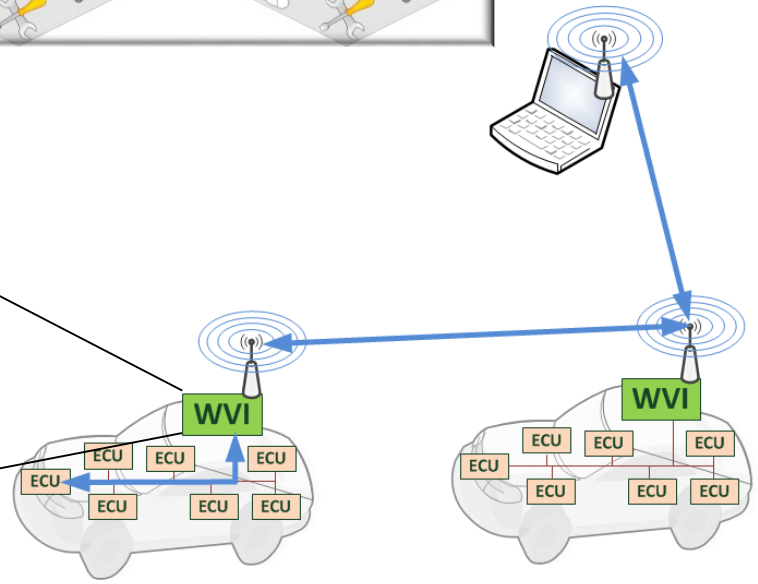
Off-highway vehicle testing for comfort and health assessment of human operators



Automotive: Wireless SW Update

- **OEM-independent** short-range wireless SW updates
- **Backward compatibility** by using standardized protocols and interfaces
- **Parallel vehicle updates**
- **Structured security analysis**





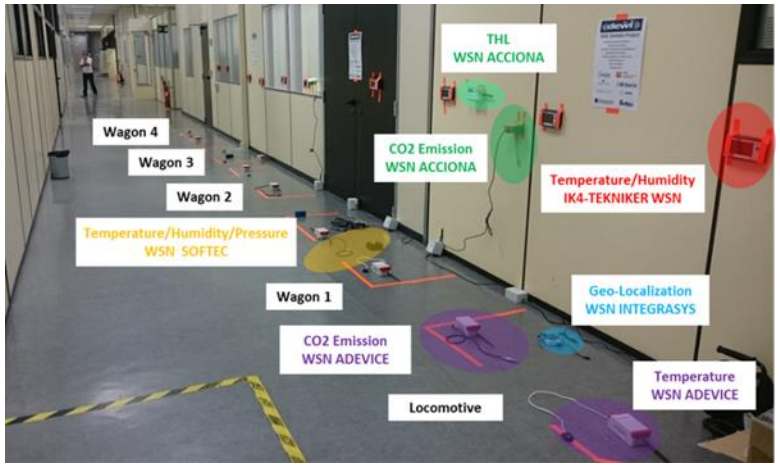
WVI = Wireless Vehicle Interface

WSN and Gateways for:

Train composition and Advanced freight monitoring

Train integrity

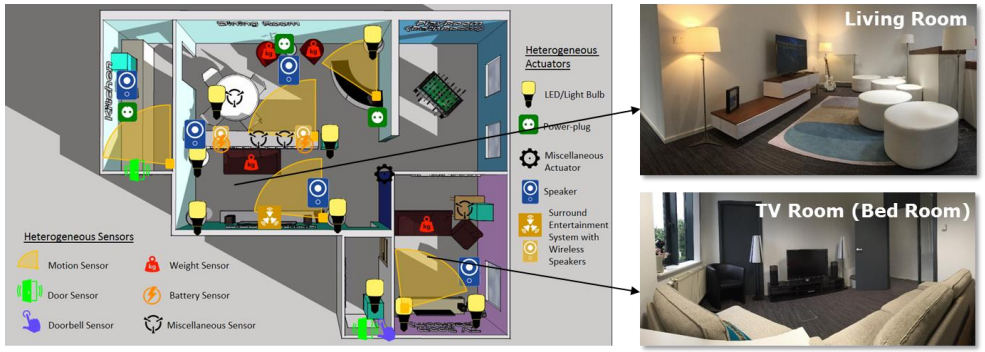
Lab demonstrators (Spain)



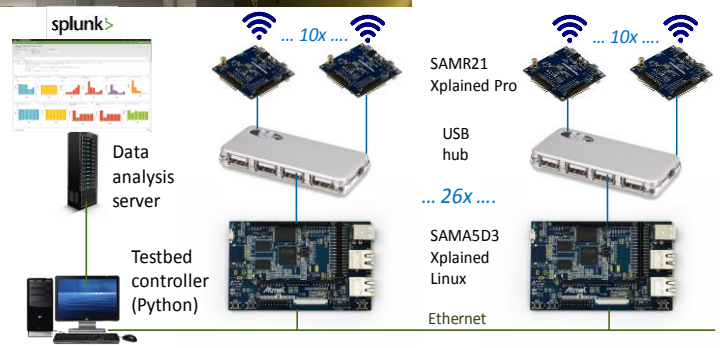
Real-life demonstrator (Latvia)

Building

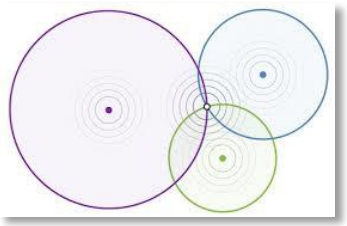
Smart Home Entertainment Demonstrator



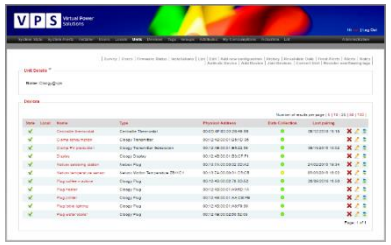
Large scale wireless lighting control



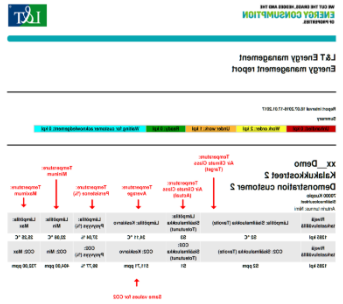
Indoor location system



ZigBee based WSN solution for energy management applications



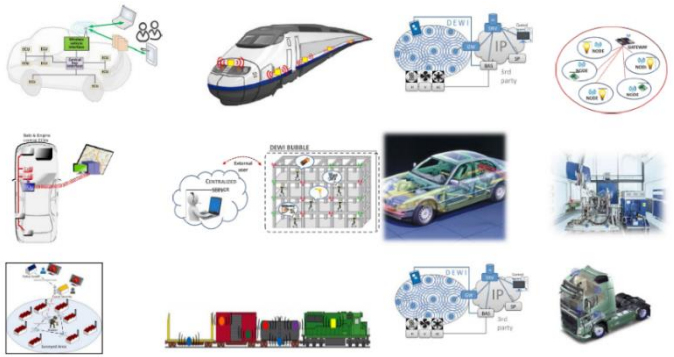
BLE based indoor conditions monitoring



DEWI and beyond …

2014-2017

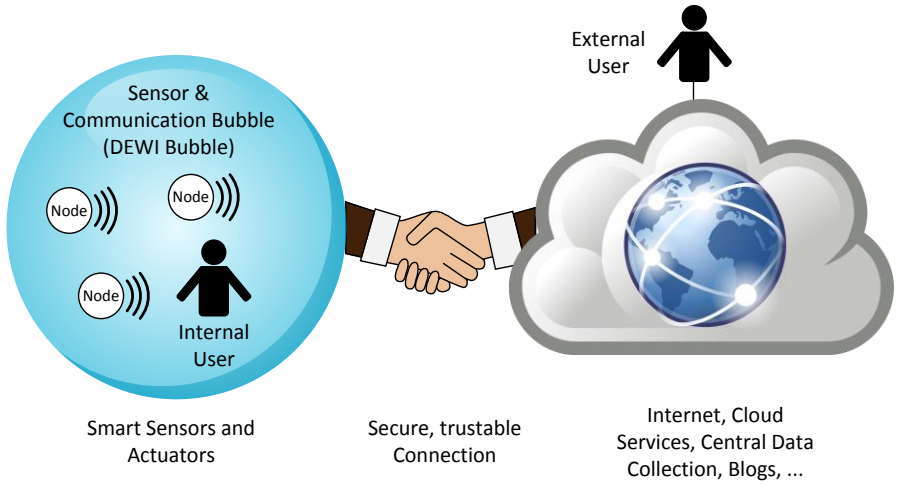
- Applications in aeronautics, automotive, building automation, and rail
- For professional and private users
- Focus on dependability and interoperability
- Multi-domain architecture



TRL 3-4(5)

2017-2020

- Applications in aeronautics, automotive, home/building automation, **healthcare,** and rail **+ cross-domain**
- For professional and private users
- **Focus on (measureable) security, privacy and trustability + Connection to the "Cloud" (5G)**
- Comprehensive use of DEWI results



TRL 6-7

SCOTT – Secure COnnected Trustable Things

- **Coordinator**: VIRTUAL VEHICLE Research Center

www.scottproject.eu

- **57 Partners from 12 Countries**
  (AT, BE, DE, FI, ES, IE, NL, NO, PL, PT, SE, and Brazil)
- **15 industry-driven Use Cases (TRL 6-7)**
- **50 Technology Building Blocks**
- **25 Demonstrators**
- **5 (+1) Domains**: Automotive, Aeronautics, Home/Building, Rail, Healthcare, and Cross-domain
  → truly "cross-disciplinary"
- **~40M€** Project Budget
- **2017 – 2020** (started in May 2017)
- **"more than 120 dedicated people working full-time over 3 years"**

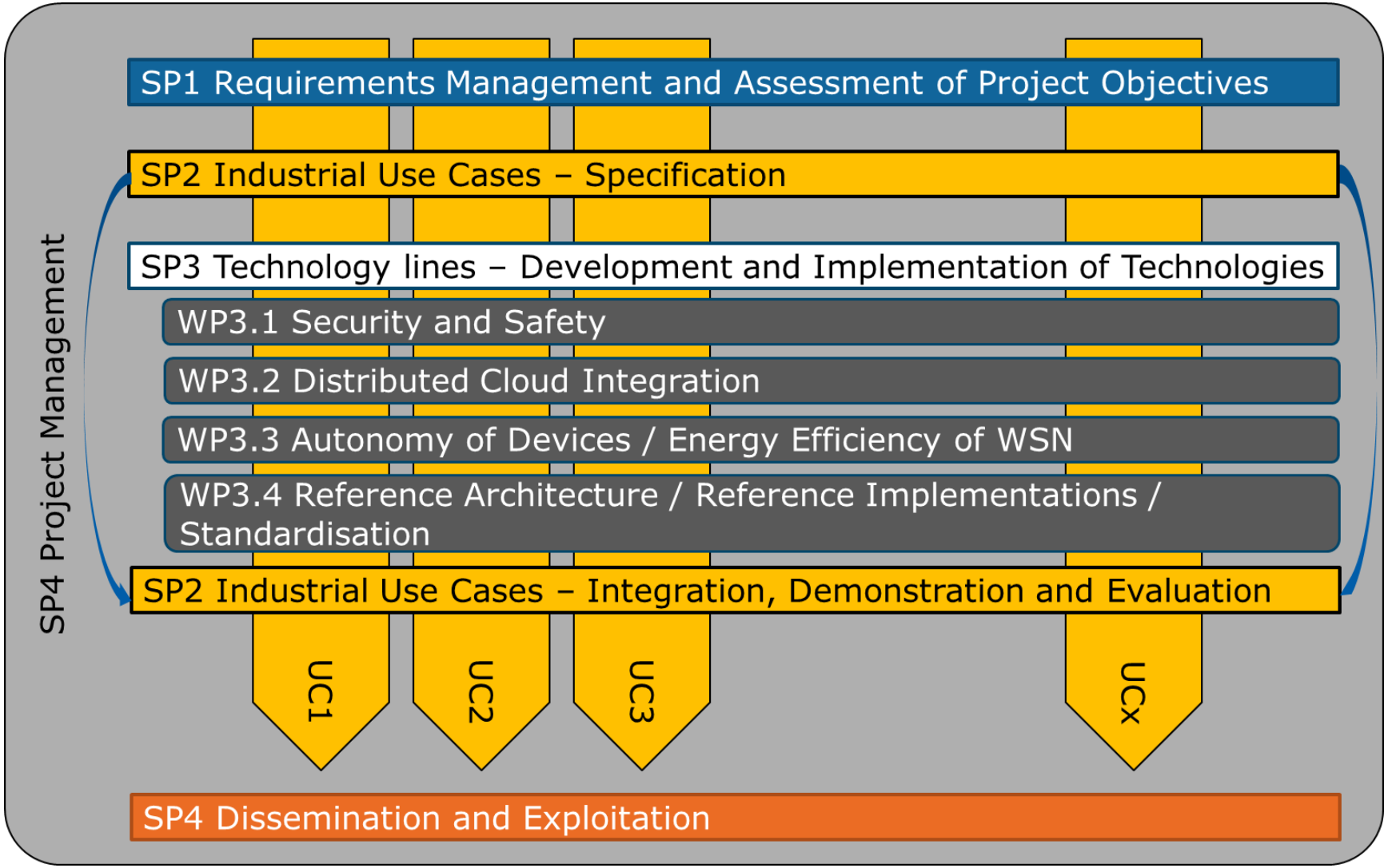
SCOTT: Main Objectives

- Provide comprehensive cost-efficient solutions of wireless, end-to-end secure, trustworthy connectivity and interoperability to **bridge the gap to the market** (key enabler to exploit the full potential of IoT)

- Not deal with just 'things that are connected', but **'trustable things that are connected'**,

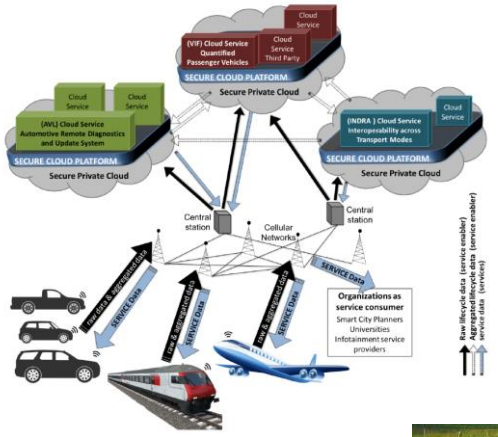
- **Bundle the European key players from several industrial domains**
  - to make full potential of cross-domain synergies and
  - to strengthen Europe's position in the emerging technology field of secure IoT

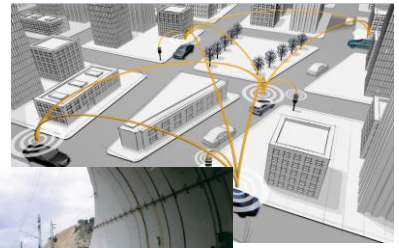
SCOTT: Project Structure



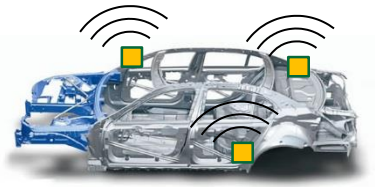
SCOTT – 15 Use Cases from European Industry

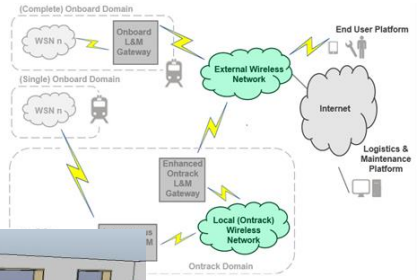
- Aeronautics, automotive, home/building automation, healthcare, rail + cross-domain

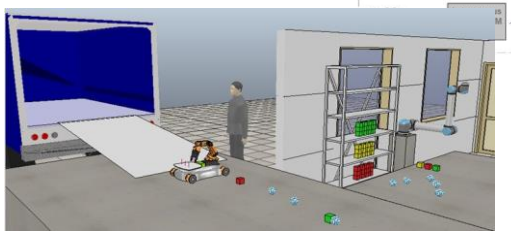




Vehicle-as-a-sensor within smart infrastructure







Trustable wireless in-vehicle communication network

Air quality monitoring for healthy indoor environments

Assisted living and community care

Building Trusted Systems is a Complex Issue of Technical and Non-technical Factors

Framework for Building Trusted Systems

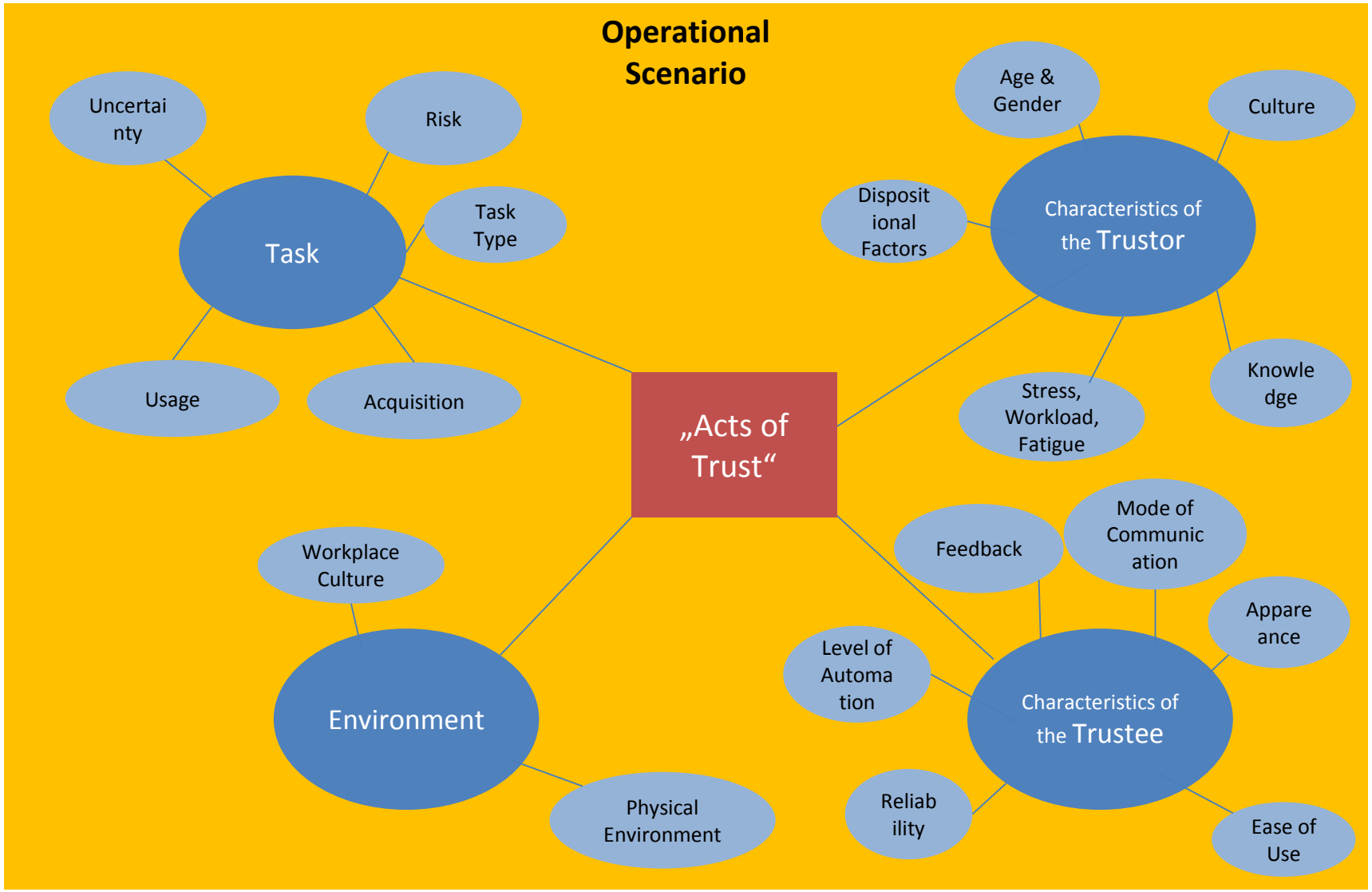
- Trust is different from system acceptance
- Trust **calibration** is essential, not just trust vs. no trust
- There are plenty theories and knowledge about trust
  - How do we translate this into system design?
  - How can we create generalizable lessons learned?
- The central concept in our framework are „trust issues" which are the specific, contextualized concerns that a system does not meet the trustors goals

- *"Trust is the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability."*
  (Lee & See 2004)

If you had the choice, would you cross this bridge?

https://www.scientificcomputing.com/sites/scientificcomputing.com/files/Solving_the_Trust_Equation_Socially_Intelligent_Computers_can_turn_Difficult_Negotiations_into_Win-win_Situations_ml.jpg

Trust Issues



- Trust issues are concerns of users or potential buyers about aspects of the system that relate to the trustor's uncertainty and vulnerability.
  - Can concern reliability, availability, usability, security, functionality, ..
- The extraction of trust issues occurs from the viewpoint of the trustor

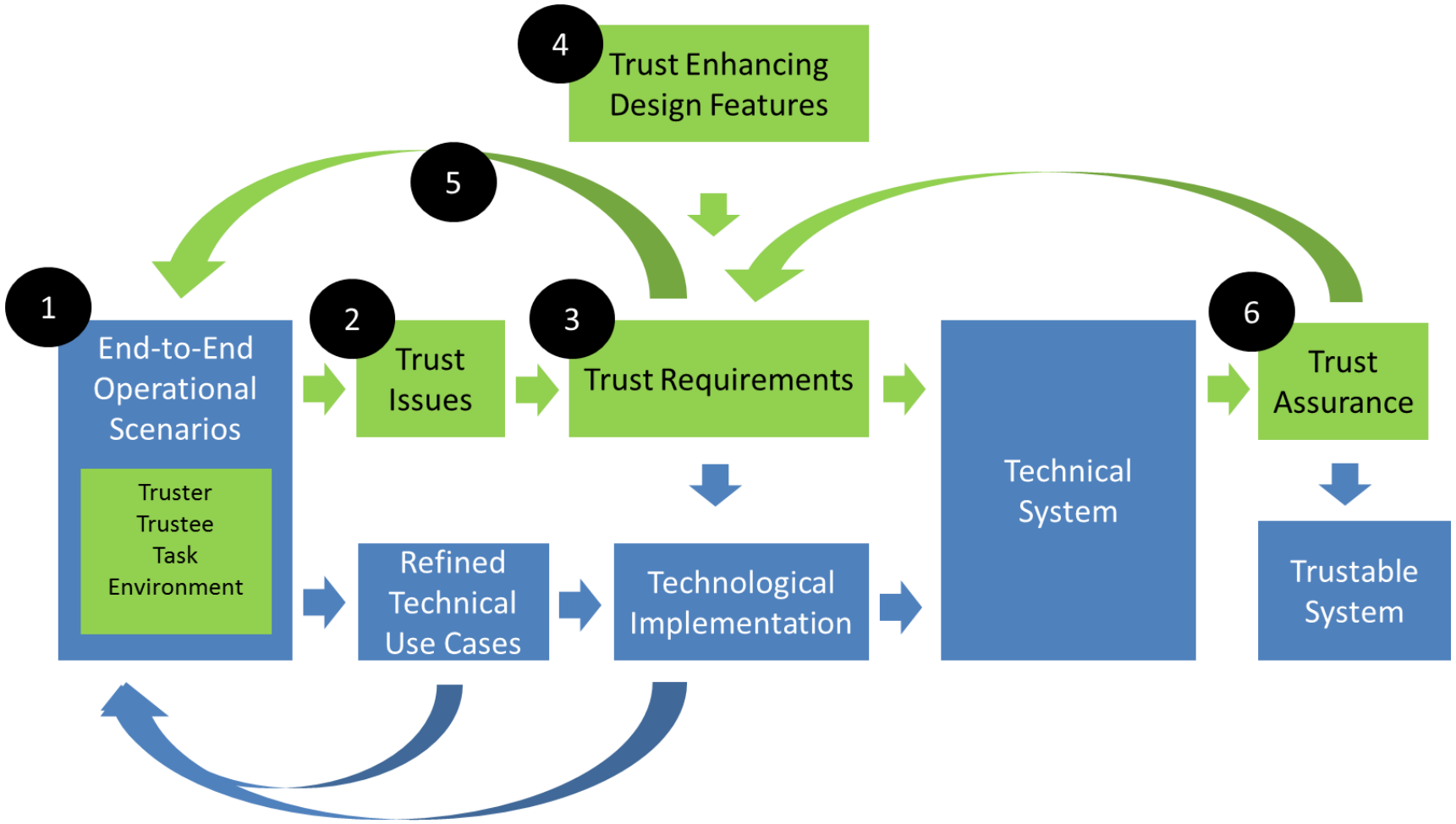
Trust Issues in (Virtual) Healthcare Example (1 of 2)

- Jennifer's elderly father lives alone at his home
  - This is where he prefers to live
- Jennifer is afraid that he may fall and hurt himself
  - Risk of severe complications
- Jennifer looks into emergency alert systems that would allow her father to quickly alert emergency in the case of a fall
  - Such systems generally require a transmitter to be worn
- Knowing her father, Jennifer believes that he would not wear this transmitter ("trust issue")
  - Forgetting
  - Lack of risk awareness
- The system would not provide the intended function
  - How could a system overcome such a trust issue?
  - How about a permanently wearable sensor that automatically detects falls?

Trust Issues in (Virtual) Healthcare Example (2 of 2)

- The fall protection system gives emergency teams directly access to the house
  - E.g. by automatically unlocking doors
- Trust issue: Jennifer's father is afraid that a burglar could exploit the emergency alert system and that emergency crews could be given access to his home
  - Would the main user be amenable to rational explanation of system security?
  - Could additional features be helpful to address the trust issue?
    - How about integrated functionality with a home alert system?

SCOTT Trust Framework



1. Analyse end-to-end operational scenario
   - With sufficient contextual information
2. Extract trust issues
3. Specify trust requirements
   - Internal and external ones
4. Proposed 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

Dr. Michael Karner

- Lead Researcher „Embedded Systems“
- michael.karner@v2c2.at

VIRTUAL VEHICLE Research Center
Inffeldgasse 21A
8010 Graz/AUSTRIA

DEWI

- dewi@v2c2.at
- www.dewiproject.eu

SCOTT

- scott@v2c2.at
- www.scottproject.eu