Approaching Runtime Trust Assurance in Open Adaptive Systems

Daniel Schneider, **Dr. Martin Becker,** Dr. Mario Trapp
martin.becker@iese.fraunhofer.de

Fraunhofer IESE

Fraunhofer Institute for Experimental Software Engineering

Innovation Through Dependable Software

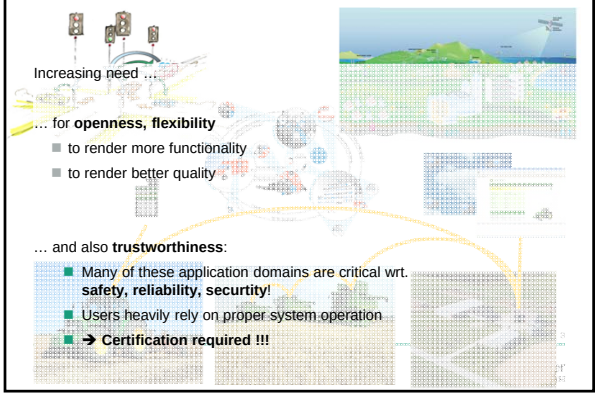
- Located in Kaiserslautern, Germany
- Leading Institute for Software Engineering
- Founded 1996
- 200 Employees

www.iese.fraunhofer.de

- Mission:
  - Provision of **new Engineering Methods** and Technology to be applied in Industry
  - **Technology Transfer** (Selection, Adaptation, Piloting, Coaching)
  - Independent **Assessment** and **Improvement** of **Software-intensive** Systems

Fraunhofer IESE

World of Systems Changes



Increasing need …

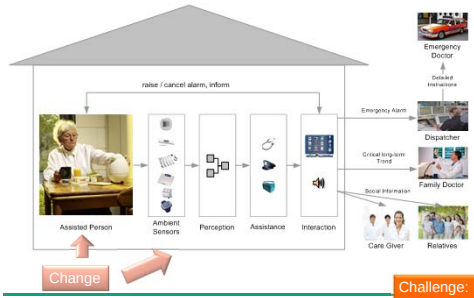
… for **openness, flexibility**

- to render more functionality
- to render better quality

… and also **trustworthiness**:

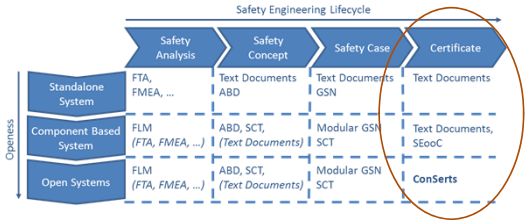
- Many of these application domains are critical wrt. **safety, reliability, security**!
- Users heavily rely on proper system operation
- ➔ **Certification required !!!**

Example: Ambient Assisted Living



Challenge:
- multiple overship
- recertification

Certification & Safety Engineering Artefacts



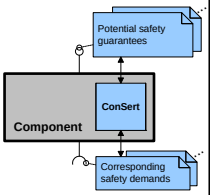
Which models can be **shifted to runtime**?

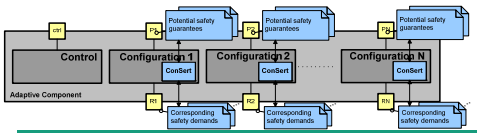
Fraunhofer IESE

Conditional Safety Certificates

Major differences to "traditional" certificates:

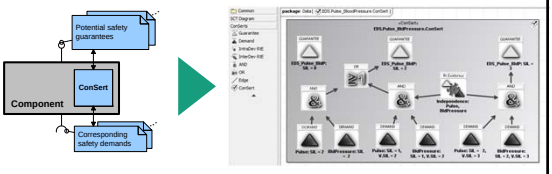
- not static but **conditional**,
- covers a **number of variants**, and,
- is available in an **semi-formal** form at runtime.
- Needs to be **defined per configuration/variant**





Fraunhofer IESE

ConSerts: Mappings



- **Boolean functions**
- a **separate ConSert Tree** (CST) for each safety guarantee
- each CST is representing a Boolean function f: $B^n \rightarrow B$

Fraunhofer IESE

Approaching Trust

Augment ConSerts with Trust related guarantees and demands

- **Dependability**: availability, reliability, safety, integrity, maintainability
- **Security**: integrity, confidentiality, availability

Implies corresponding conditional certification of these properties at development time

Challenge:
- respective quality models and service levels
- scalability of the ConSerts

Trust: A service S can be trusted when it is acceptably dependable and acceptably secure. This implies that all (lower level) services, involved in rendering the service S, comply with corresponding requirements with respect to their dependability and security as well, and that the dependence between these services (and respective systems) can be accepted.

Fraunhofer IESE

Next Steps

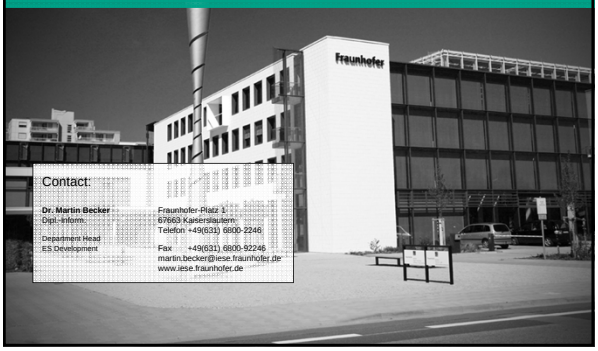
- **Investigate your** presented **approaches**
- Define **trust quality model**
- **Extend ConSerts** accordingly
- Conduct a bigger **case study**
- Involve **certification bodies**

- Short term: **Discuss** this important topic **with you!**

Thank you for your **interest** & **input**

Fraunhofer IESE

Thank you for your interest



Contact:

Dr. Martin Becker
Dipl.-Inform.

Department Head
ES Development

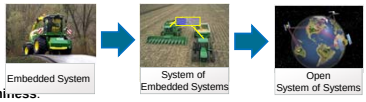
Fraunhofer-Platz 1
67663 Kaiserslautern
Telefon +49(631) 6800-2246

Fax +49(631) 6800-92246
martin.becker@iese.fraunhofer.de
www.iese.fraunhofer.de

Plug&Trust

Upcoming application domains (Car2Car, AAL, Operation Room of the Future, …) show the **need for openness, flexibility**….

- Different devices, machines, or vehicles are combined at runtime to fulfill higher-level functionalities in cooperation
- Dynamic changes due to changes in requirements, device availability, resources..



… and also **trustworthiness**.

- Many of these application domains are critical wrt. Important properties such as **safety, reliability, securtity**!
- Users heavily rely on proper system operation, certification required

However, there has not been much research done on QA and certification of such open systems!

Fraunhofer IESE