

Approaching Runtime Trust Assurance in Open Adaptive Systems

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

© Fraunhofer ESE

Fraunhofer Institute for Experimental Software Engineering

Innovation Through Dependable Software

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

■ 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**

www.iese.fraunhofer.de

© Fraunhofer ESE

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 !!!**

© Fraunhofer ESE

Example: Ambient Assisted Living

© Fraunhofer ESE

Certification & Safety Engineering Artefacts

Openness	Safety Engineering Lifecycle			
	Safety Analysis	Safety Concept	Safety Case	Certificate
Standalone System	FTA, FMEA, ...	Text Documents ABD	Text Documents GSN	Text Documents
Component Based System	FLM (FTA, FMEA, ...)	ABD, SCT, (Text Documents)	Modular GSN, SCT	Text Documents, SEooc
Open Systems	FLM (FTA, FMEA, ...)	ABD, SCT, (Text Documents)	Modular GSN, SCT	ConSerts

Which models can be shifted to runtime?

© Fraunhofer ESE

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 ESE

ConSerts: Mappings

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

7

Fraunhofer ESE

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.

8

Fraunhofer ESE

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

9

Fraunhofer ESE

Thank you for your interest

Contact:

Dr. Martin Becker
 Disposition Head
 ES Development

Fraunhofer-Platz 4
 67663 Kaiserslautern
 Telefon +49(0)31 6900-2240
 Fax +49(0)31 6900-92246
 martin.becker@ese.fraunhofer.de
 www.ese.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, security!
- 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!

11

Fraunhofer ESE