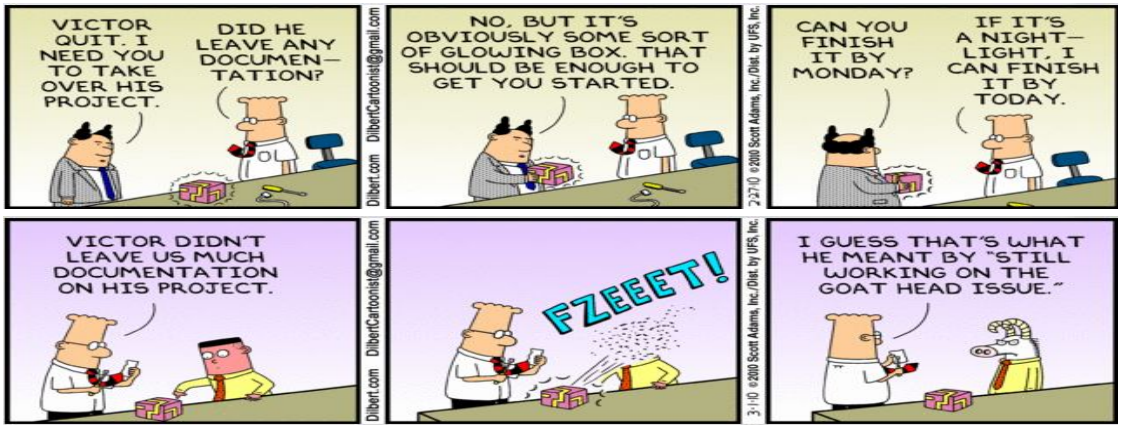
Improving Consistency Checks between Safety Concepts and View-based Architecture Design

PSAM12 – Probabilistic Safety Assessment and Management

22-27 June 2014, Honolulu, Hawaii

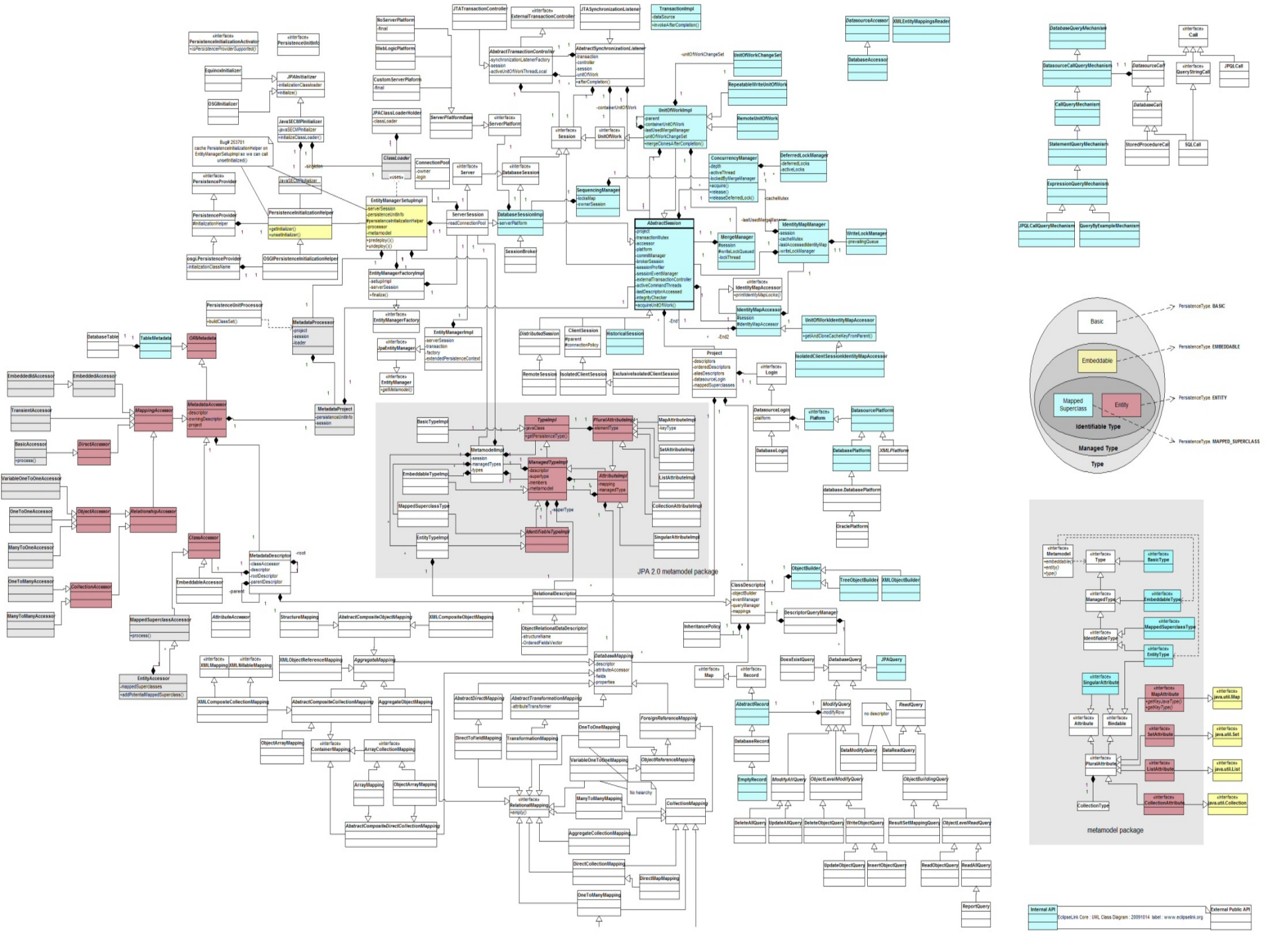
Pablo Oliveira Antonino (Pablo.Antonino@iese.fraunhofer.de)

Mario Trapp (Mario.Trapp@iese.fraunhofer.de)

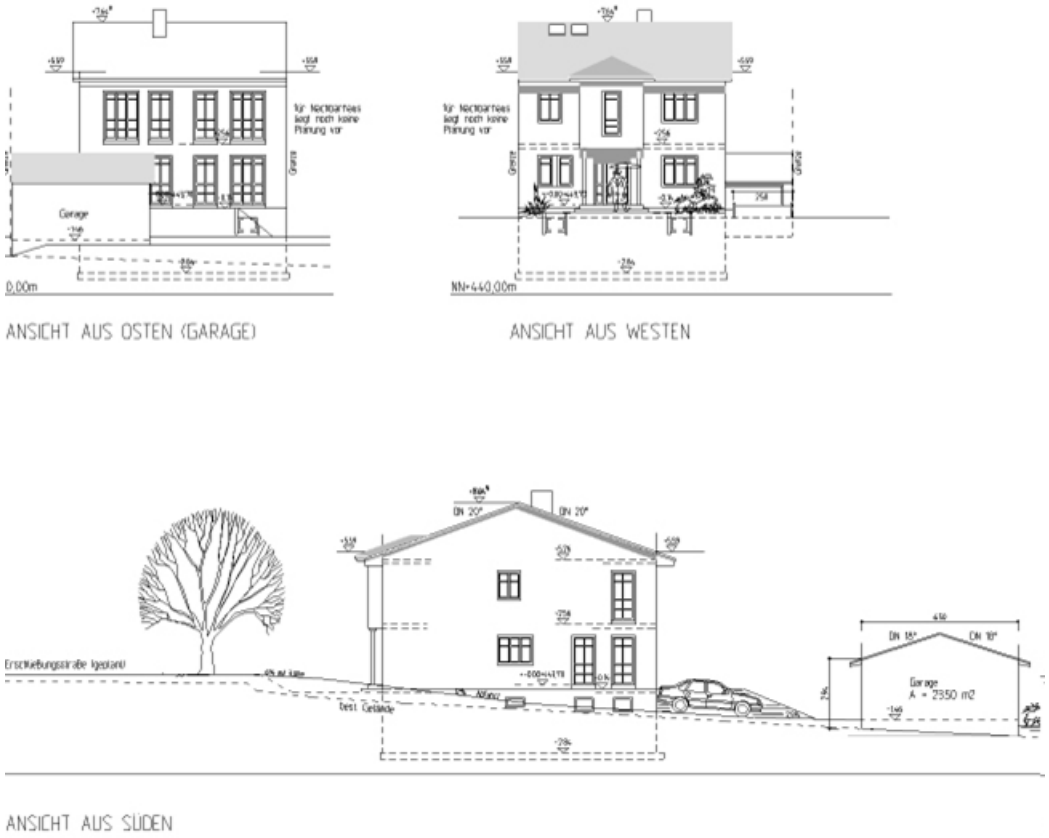


Fraunhofer IESE

View-based Architecture Design


JPA 2.0 metamodel package
metamodel package
Basic
Embeddable
Mapped Superclass
Entity
Identifiable Type
Managed Type
Type
PersistenceType.BASIC
PersistenceType.EMBEDDABLE
PersistenceType.ENTITY
PersistenceType.MAPPED_SUPERCLASS
Internal API
External Public API
EclipseLink Core : UML Class Diagram : 20091014 label : www.eclipselink.org

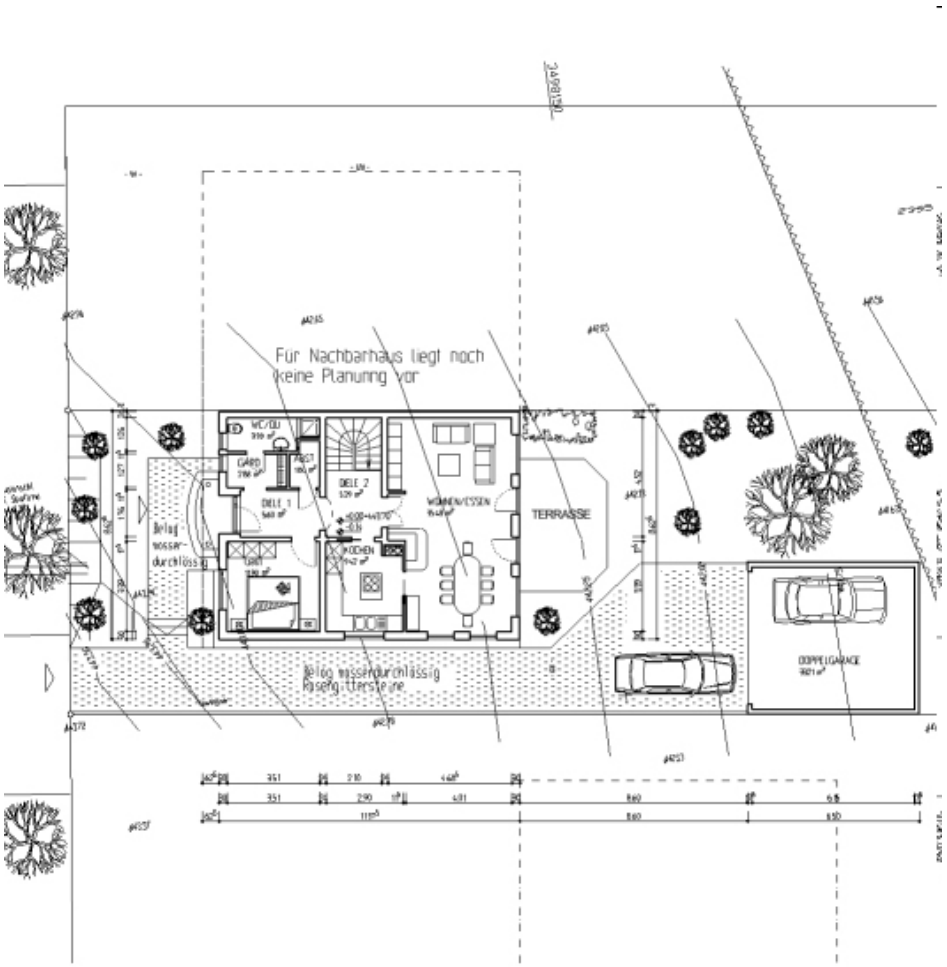
Analogy – Views on a Building



http://www.planungswerkstatt-bau.de

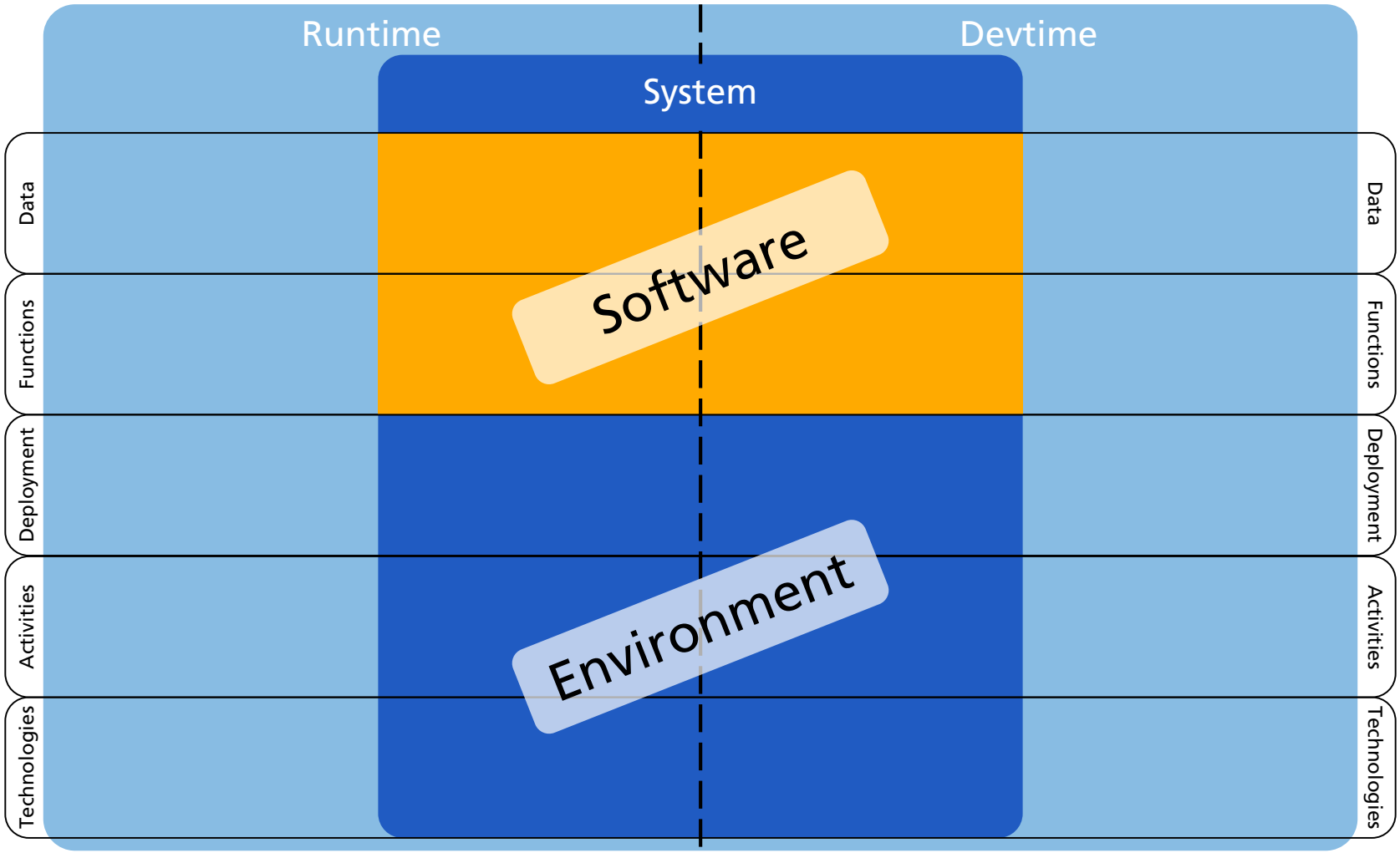
Fraunhofer IESE

Analogy – Views on a Building



http://www.planungswerkstatt-bau.de

View-based Architecture design



Fraunhofer IESE

Safety Concepts

Safety Concepts

- Safety concepts are requirements with a strong emphasis on the architectural elements that compose the measures to be used to prevent safety-critical failures.

ISO 26262 – Road vehicles -- Functional safety

GET THE FACTS

- "For the 34 (safety) incidents analyzed, 44% had inadequate specification as their primary cause."

  Health and Safety Executive (HSE), *Out of Control: Why Control Systems Go Wrong and How to Prevent Failure, 2005*.

- "Almost all accidents related to software components in the past 20 years can be traced to flaws in the requirements specifications, such as unhandled cases."

  Safeware Engineering, 2005.

Multitude of artifacts

REQUIREMENTS

ARCHITECTURE

SAFETY MODELS

TEST SPECIFICATION

SOURCE CODE

- **ISO 26262 –** Road vehicles -- Functional safety

  Safety requirements shall be traceable to (i) each source of a safety requirement at the upper hierarchical level, (ii) each derived safety requirement at a lower hierarchical level, i.e. realization in the design, and (iii) the specification of verification.

- **DO-254, DO-178C, ARP 4754, ARP 4761** – Aerospace

  “software developers must be able to demonstrate traceability of design against requirements.”

- **ANSI/AAMI/IEC 62304:2006 –** Medical Devices

  "Traceability between requirements, software system test, and risk control measures implemented in the software."

- **FDA –** Medical Devices

  "Traceability analysis must be used to verify that the software design of a medical device implements the specified software requirements, that all aspects of the design are traceable to software requirements, and that all code is linked to established specifications and test procedures."

GET THE FACTS

- Traceability among hazards, safety requirements, and architecture of equipments submitted to FDA are usually incomplete, incorrect, and conflicting.

  US Food and Drug Administration – FDA, 2013.

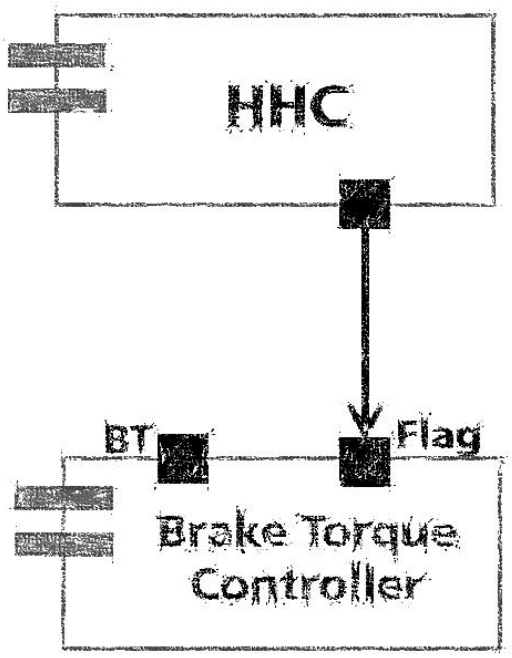
- Creating and documenting traceability immediately prior to certification is a common proceeding.

  Mäder et al., 2014.

- "None of the existing traceability approaches described in the literature are appropriate to meet this demand of the safety-critical domain ."

  CoEST - Center of Excellence for Software Traceability, 2012.

Hill Holder Controller



Hazard

Self-Braking

Safety Goal

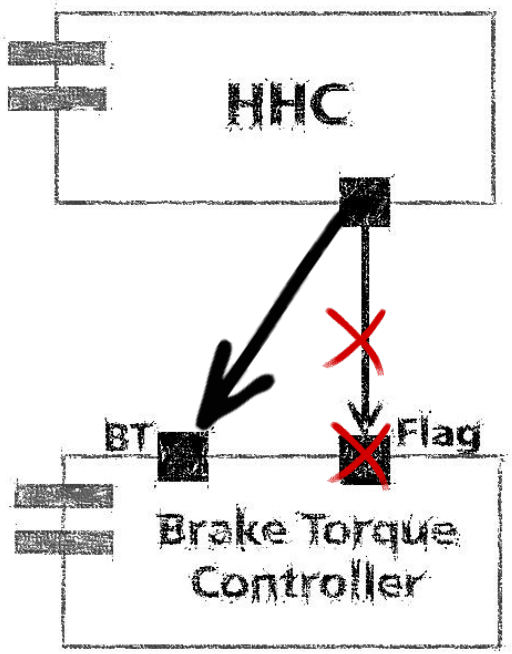
No unintended self-braking

Assumption

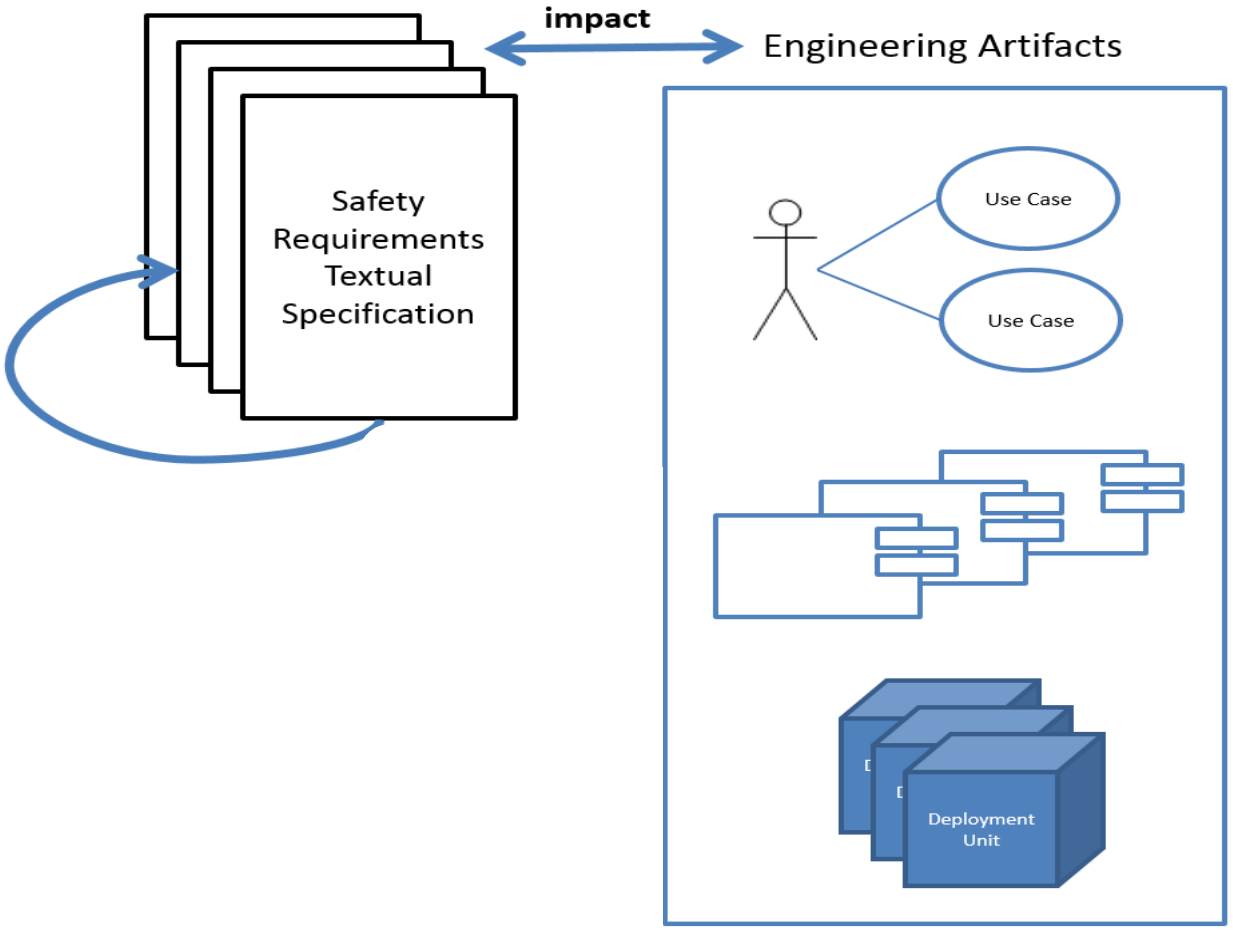
HHC only passively holds brake pressure that has been created by the driver.

Strategy

Brake Torque Controller should provide an interface that ensures that only pressure created by the driver is held.



Fraunhofer IESE



- **Causes**
  - Multitude of textual documents to specify safety requirements;
  - Different understanding of underlying concepts and terminologies.

- **Consequences**
  - Ambiguous, incomplete, and inconsistent safety requirements;
  - Decrease the efficiency of safety assurance.

Our Approach

CORE

Improving completeness and consistency of safety requirements with respect to architecture design and failure propagation models

Identifying inconsistent and incomplete safety requirements specifications

Consistency and Completeness Checks

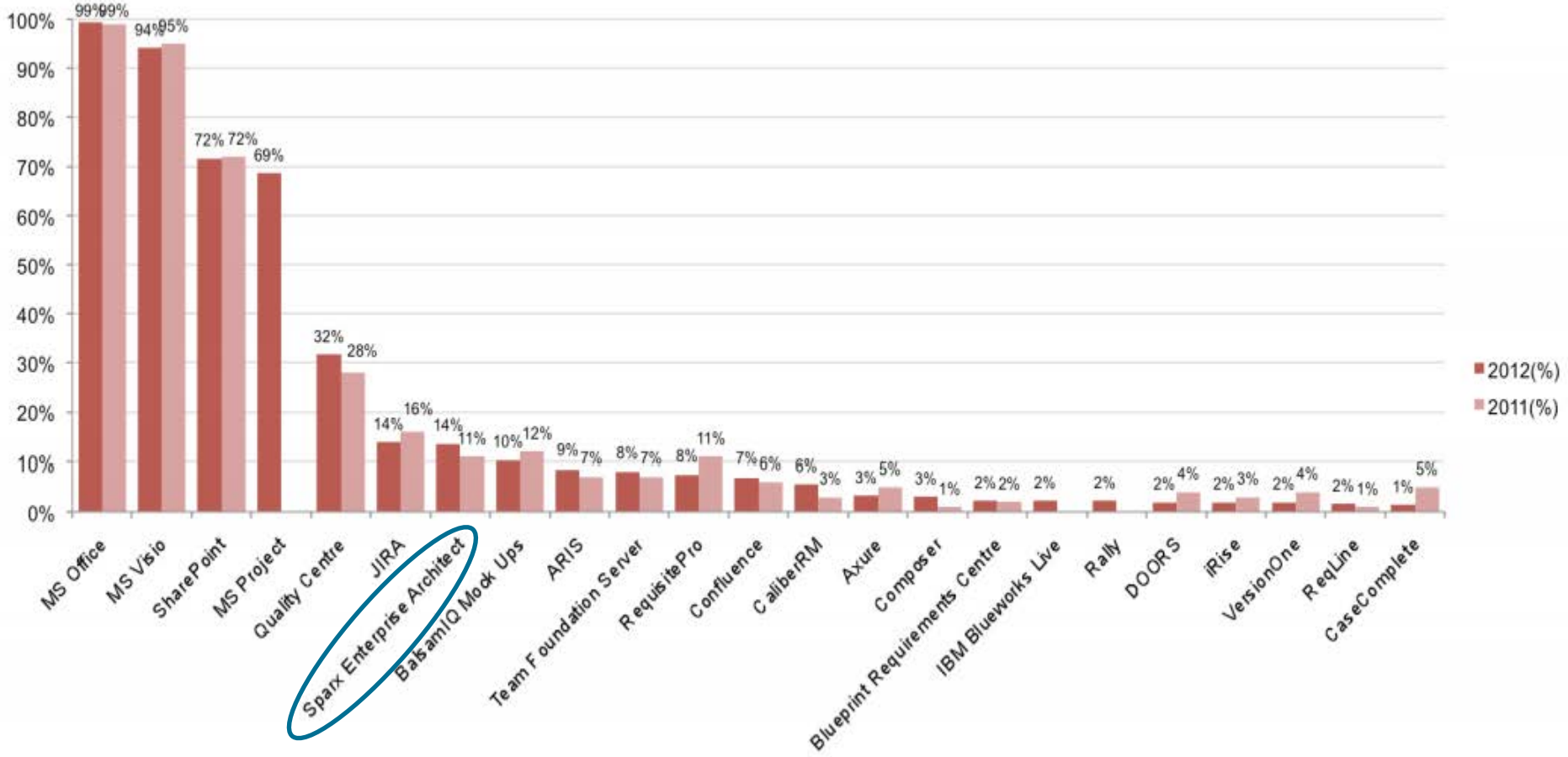
Specifying complete and consistent safety requirements with respect to architecture design and failure propagation models

Safety Requirements Decomposition Pattern

Parameterized Safety Requirements templates

Tool support

Why Enterprise Architect?



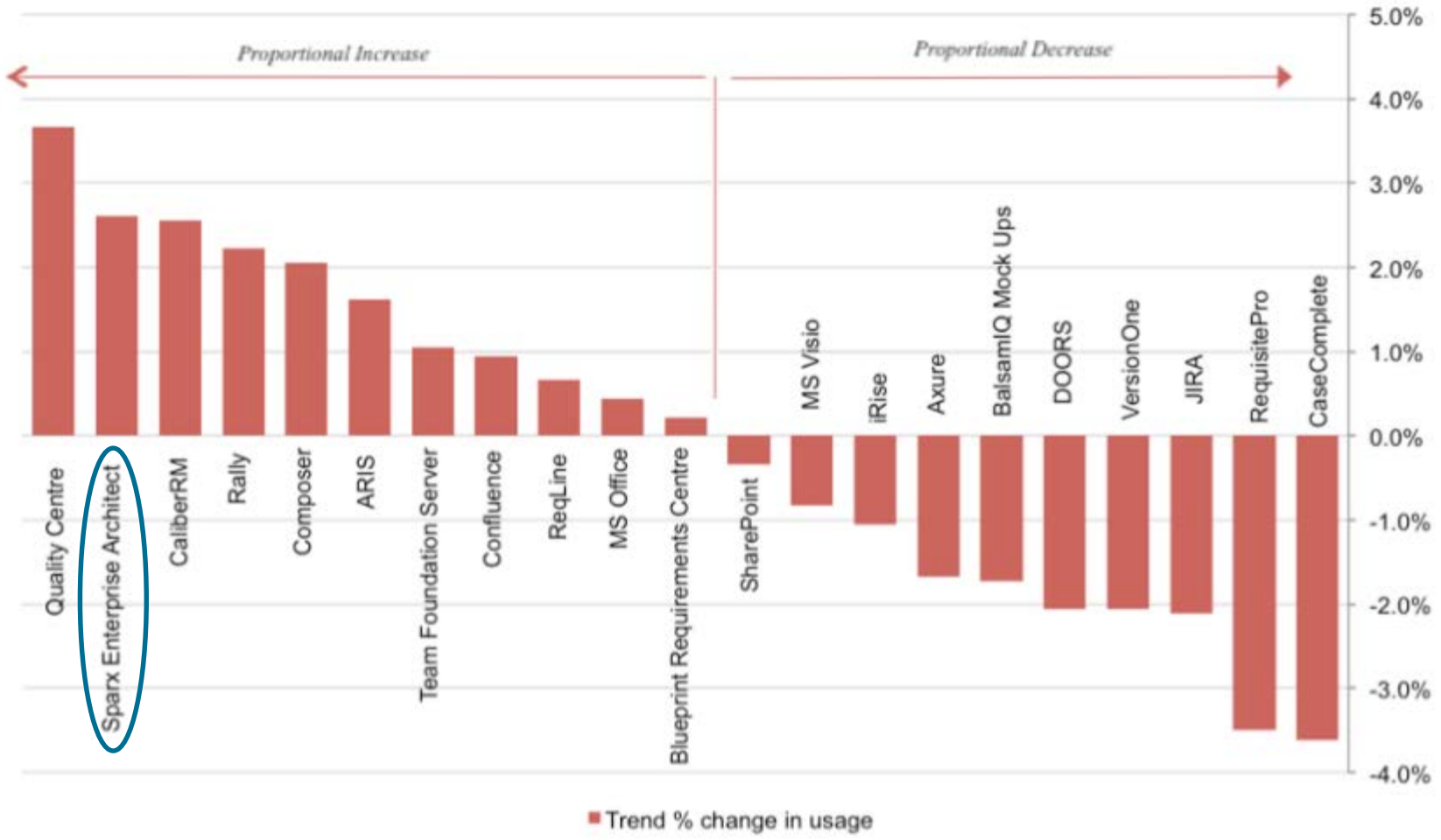
Source: IIBA UK Business Analysis Survey 2012 (http://uk.theiiba.org/images/reports/basurvey2012_final_v1_0s.pdf)

JOHN DEERE

ACES

Fraunhofer IESE

Why Enterprise Architect?



Source: IIBA UK Business Analysis Survey 2012 (http://uk.theiiba.org/images/reports/basurvey2012_final_v1_0s.pdf)

JOHN DEERE ACES Fraunhofer IESE

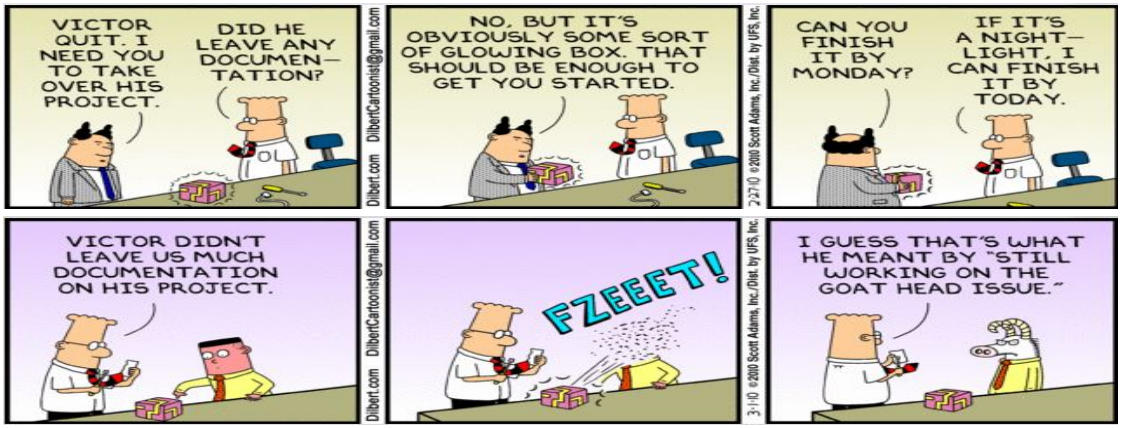
Improving Consistency Checks between Safety Concepts and View Based Architecture Design

PSAM12 – Probabilistic Safety Assessment and Management

22-27 June 2014, Honolulu, Hawaii

Pablo Oliveira Antonino (Pablo.Antonino@iese.fraunhofer.de)

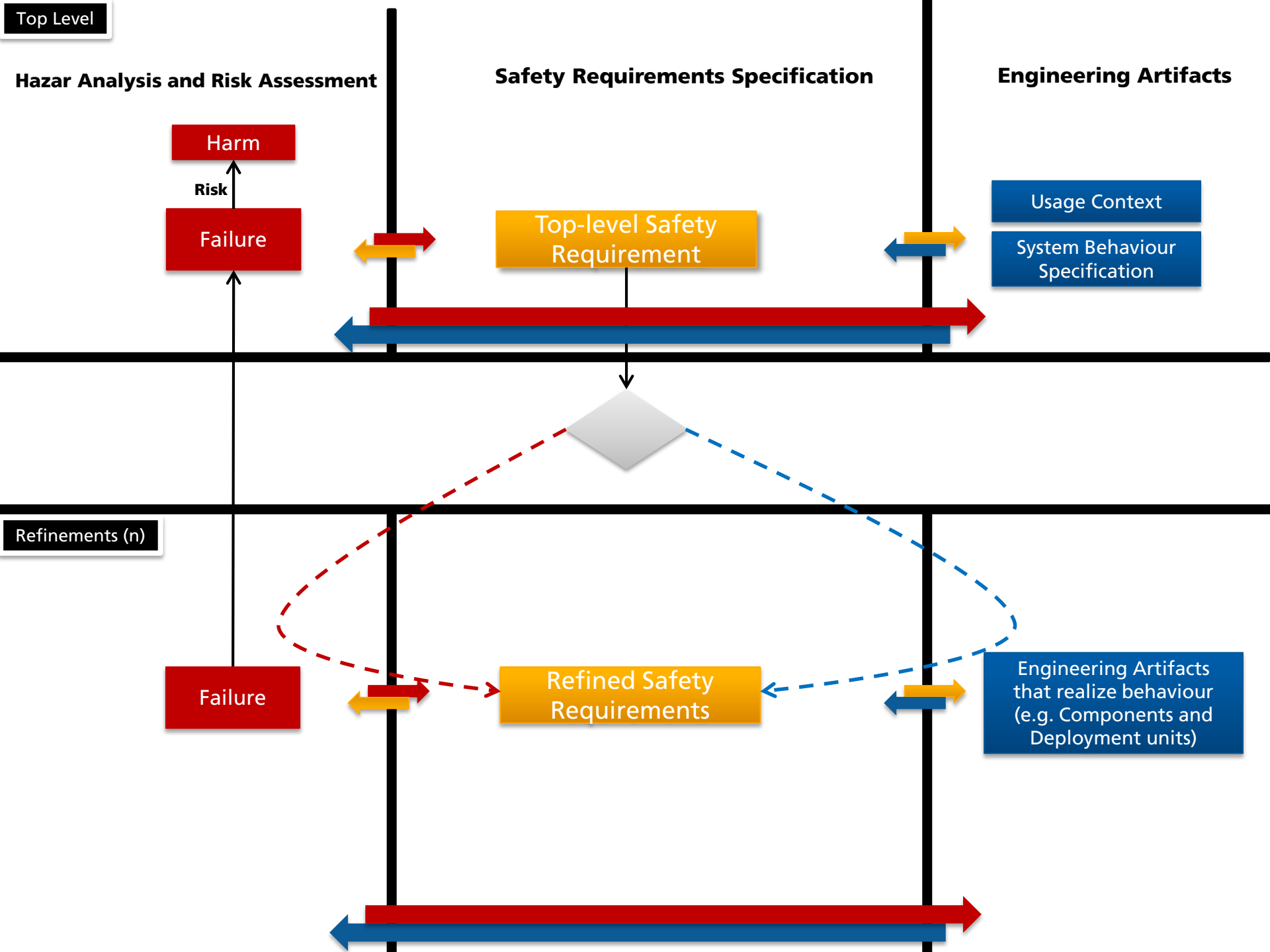
Mario Trapp (Mario.Trapp@iese.fraunhofer.de)



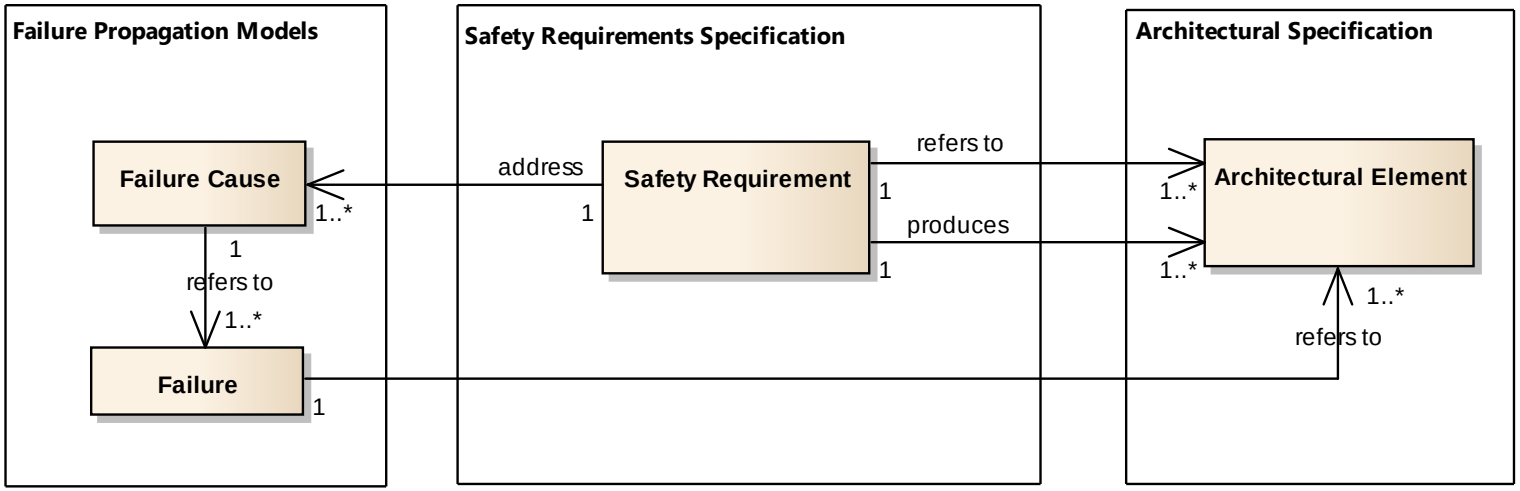
Fraunhofer IESE

Linked Slides

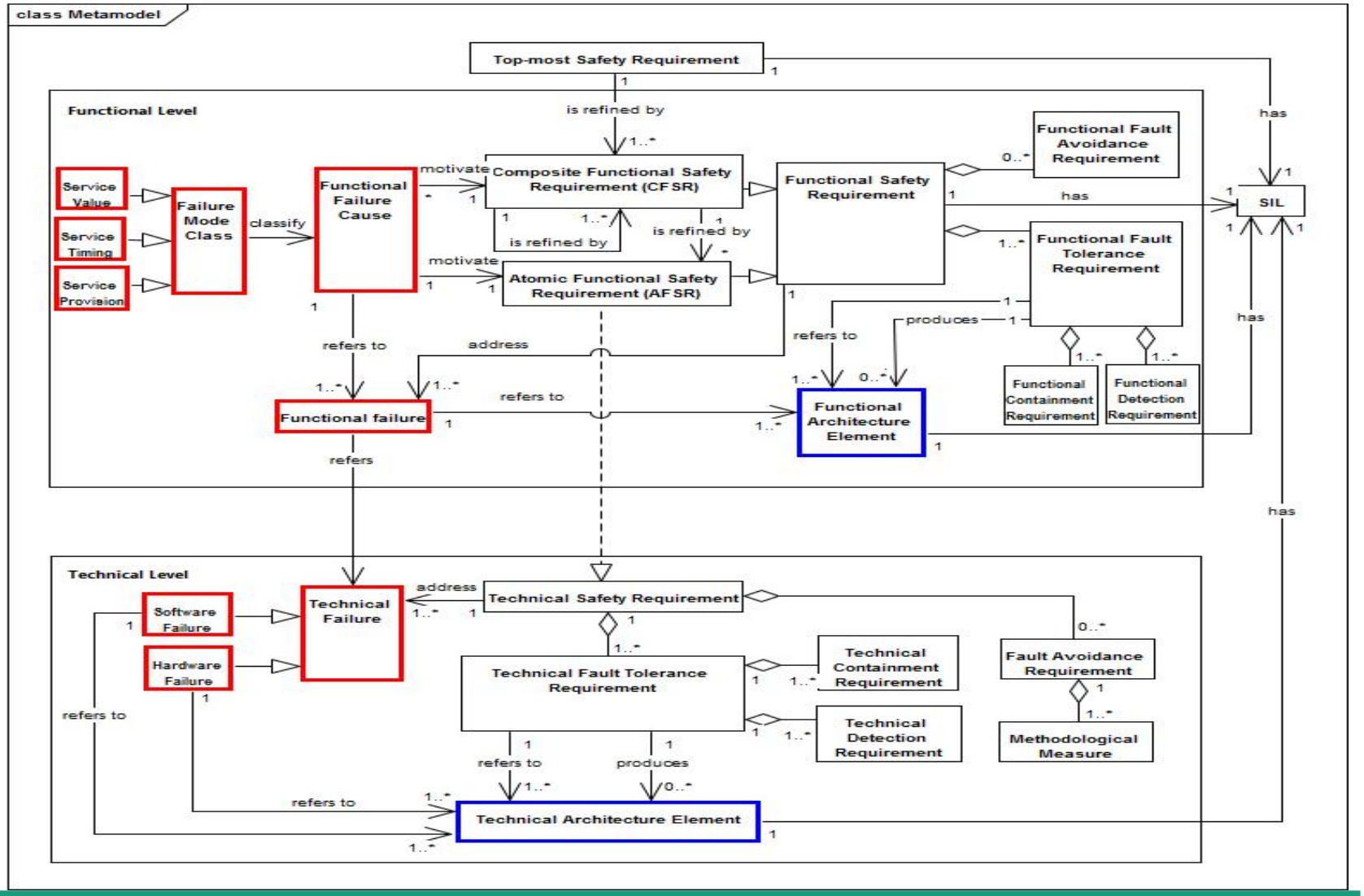
Safety Requirements Decomposition Pattern


Top Level
Hazar Analysis and Risk Assessment
Safety Requirements Specification
Engineering Artifacts
Harm
Risk
Failure
Top-level Safety Requirement
Usage Context
System Behaviour Specification
Refinements (n)
Failure
Refined Safety Requirements
Engineering Artifacts that realize behaviour (e.g. Components and Deployment units)

Safety Requirements Decomposition Pattern



Safety Requirements Decomposition Pattern



Fraunhofer IESE

Linked Slides

Parameterized Safety Requirements Templates

Safety Concepts Decomposition Pattern (2/2)

Safety Goal

[System|Component Group|Component|Computing Node] shall [avoid|not cause|not permit |not be | not | no] [harm]

Technical Safety Requirement

Service Value

[Component Group|Component] shall [perform action] [artifact affected by action] [Values threshold of measurement: within|exactly with|not exceed|not less than][Data constraint]

Service Timing

[Component Group|Component] shall [perform action] [artifact affected by action] [timing threshold of measurement: within|before|after|exactly|no later than] [timing constraint]

Service Provision

Under Development

Fault Tolerance Requirement

Detect and Handle **[type of violation]** violation

Detection Requirement

It should be detected if **[artifact affected by action]** is not **[action perfomed - past tense] [threshold of measurement] [Value Constraint]|[Timing Constraint]**

Containment Requirement

[artifact affected by action] shall be handled

Safety Patterns

Various templates

Fault Avoidance/Removal Requirement