fortiss

München, 08. May 2013

Towards model-based Safety Cases in AutoFOCUS3

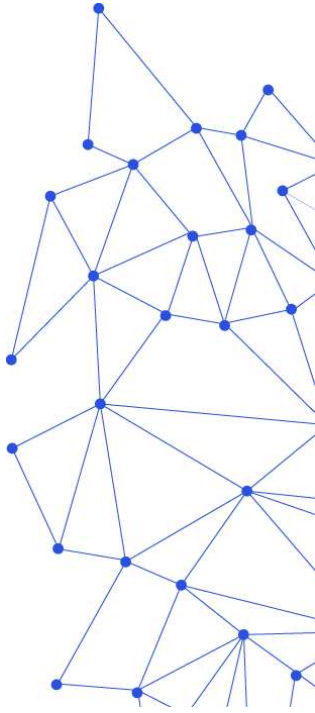
(http://af3.fortiss.org)

Seamless model-based systems engineering

Carmen Carlan and Sebastian Voss

fortiss GmbH
An-Institut Technische Universität München

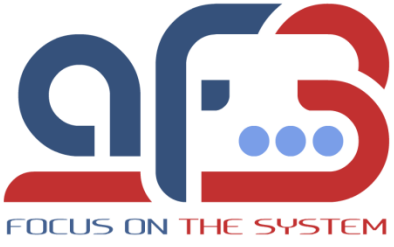
Research supported by the EU under the Distributed MILS contract Nr. 318722



Background

- Increasing complexity in **domains**, **technologies**, **functionality** and **development** in the embedded systems domain

- Provision of methods and technologies for **seamless development of high quality embedded systems** through AutoFOCUS3 tool – chain



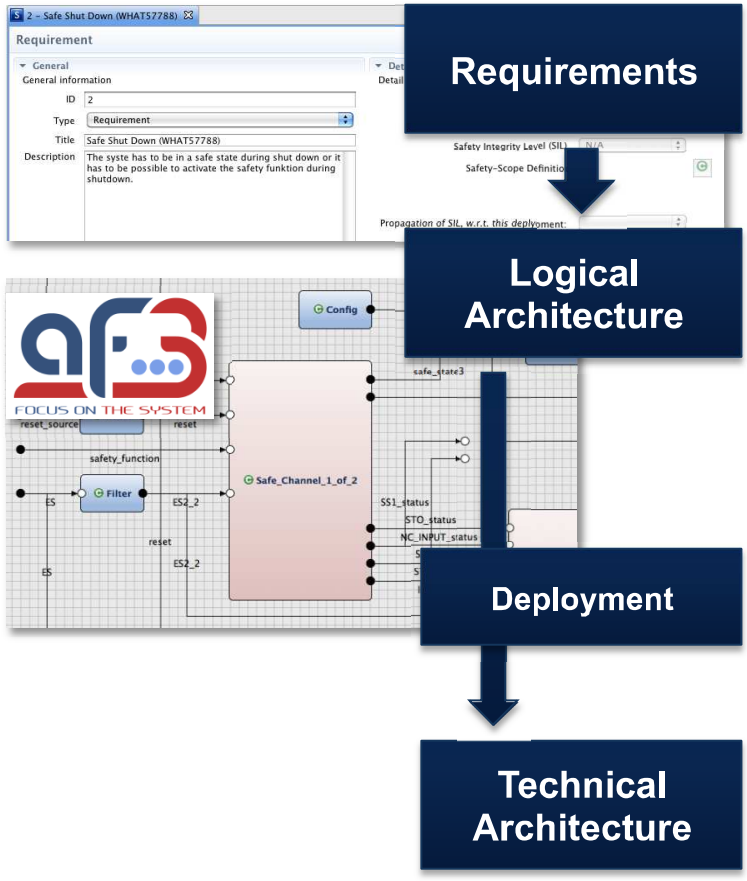
AutoFOCUS3 Basics

AF3 - Highlights

- **AF3 framework:**
  - Provides **modular construction** of the system
  - a **seamless model-based** System Development
  - (Standard-relevant) **Levels of abstraction** (e.g. logical, technical)
  - explicates **Allocations** and **Refinements** between different abstractions
  - Deeply integrated **Formal Verification** Techniques
  - **Open source** (http://af3.fortiss.org) and free of charge
  - **One-Click Code Generation**
  - Support of Standards (e.g. FIBEX, ReqIF)
  - Mechanisms to validate/verify **Functional Correctness**
  - Efficient **Test Case Generation**
  - **…**
- **AF3** supports **Modular Model-based Development** of Embedded Systems for various kinds of platforms

AF3 Product - Development

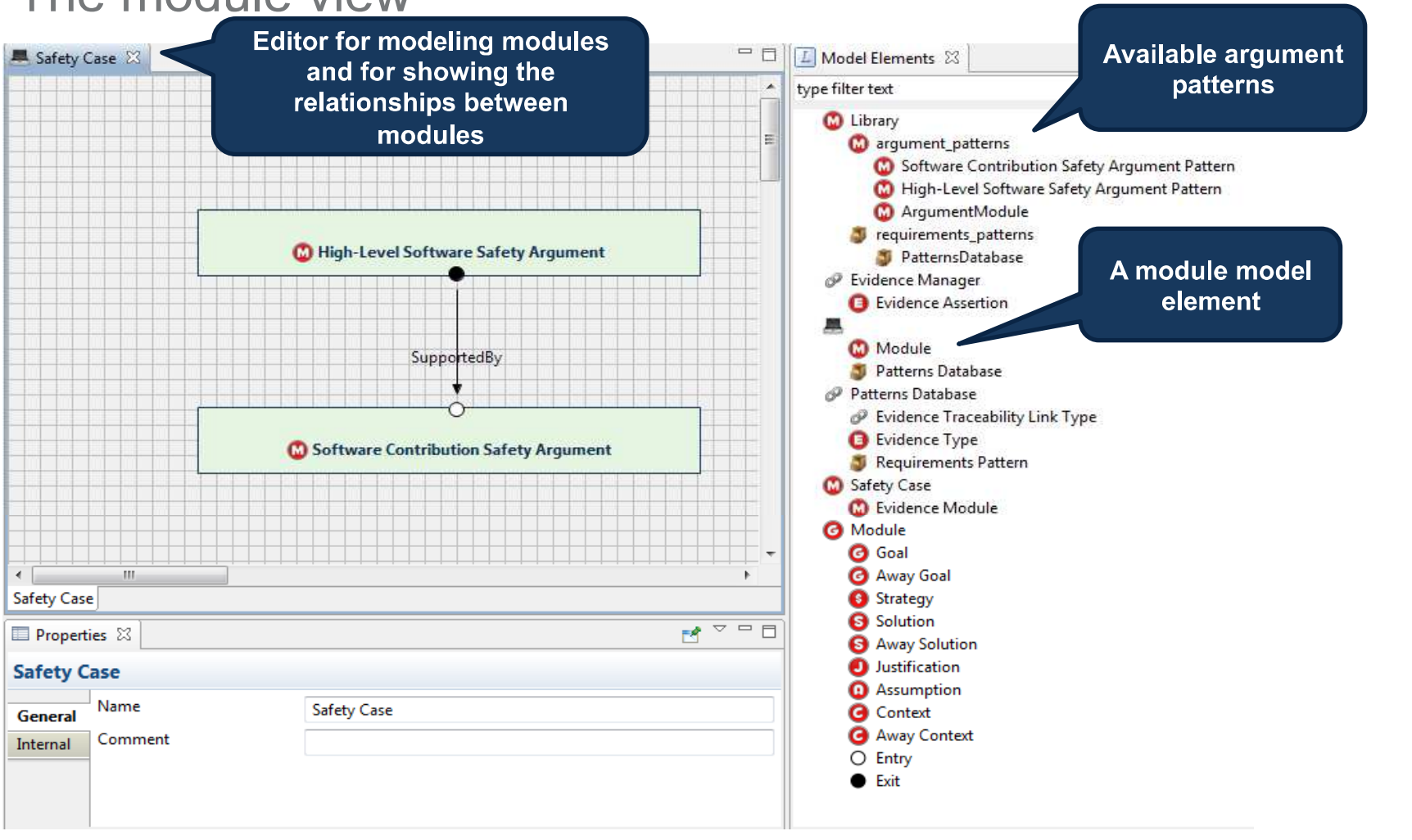
- AF3 **framework:**
  - supports Concept Phase and Product Development at **System**, **Hardware** and **Software** Level
  - explicates **Allocations** and **Refinements** between different abstractions
  - provides modular, hierarchic concept for **Networks of Components**
  - can be **simulated, verified, synthezied**
  - Supports **Automated Verification** (e.g., contracts)
  - Supports **Automated Generation** (e.g., test cases, code, schedules)



fortiss

Safety Cases in AutoFOCUS3

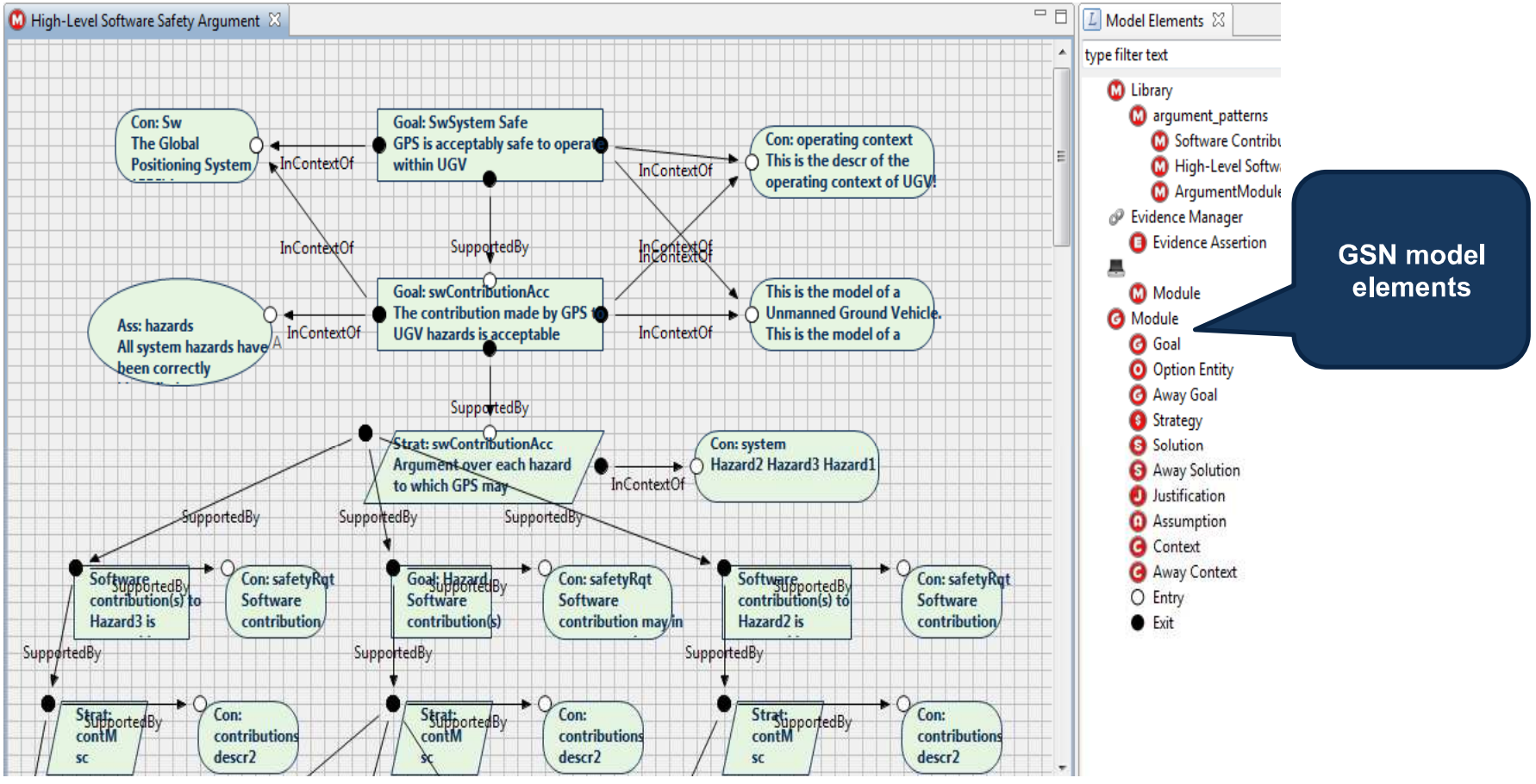
The module view



fortiss

Safety Cases in AutoFOCUS3

The argument structure view



fortiss

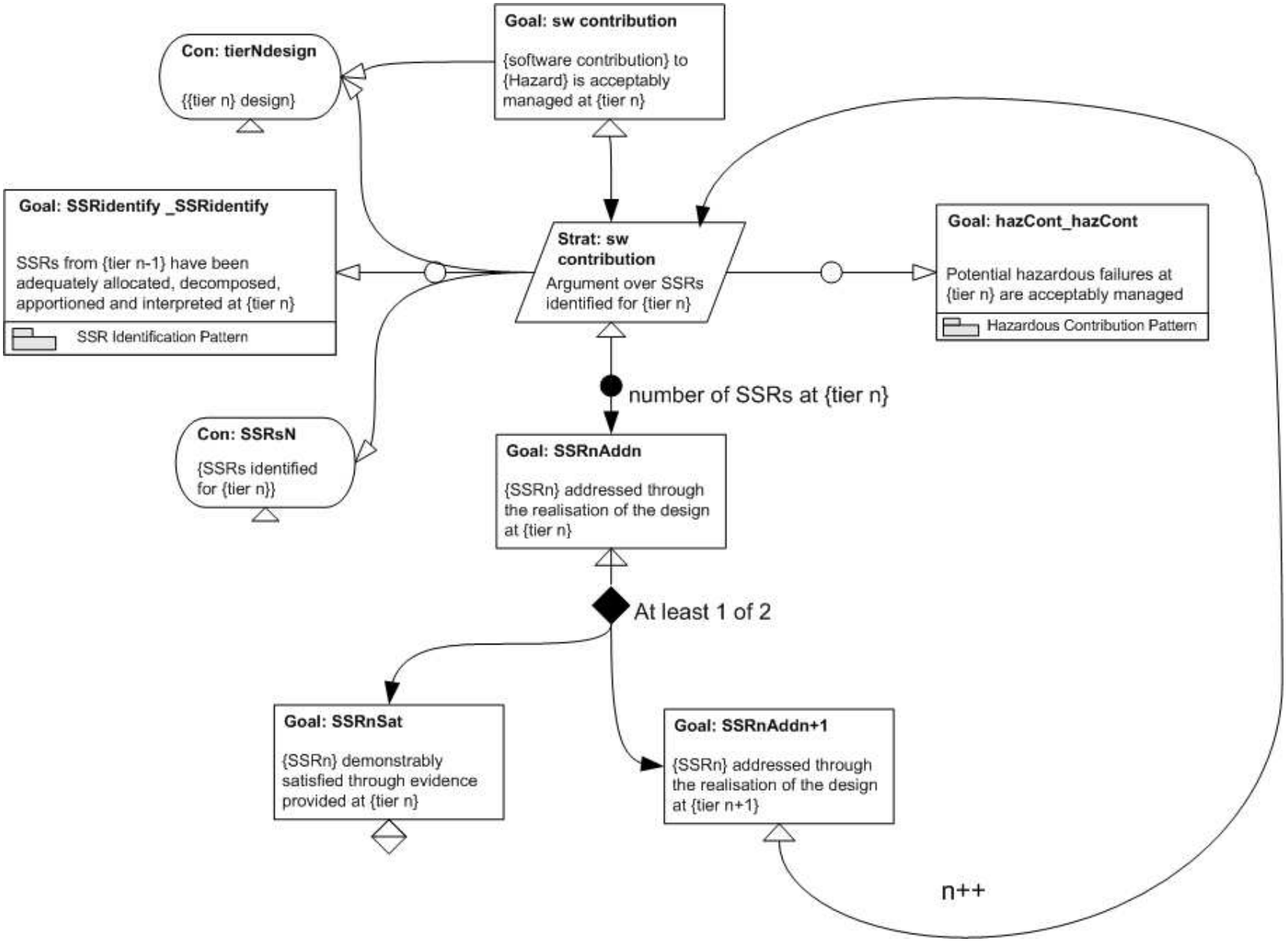
Safety Cases in AutoFOCUS3

Linking GSN elements with AF3 elements

- ✓ Goals <-> Safety Requirements
- ✓ Solutions <-> AF3 elements
- ✓ Parts of a claim <-> Safety Requirements
- ✓ Parts of a claim <-> Hazards
- ✓ Parts of a claim <-> Logical Components
- ✓ Parts of a claim <-> Platform Components

fortiss

Software Safety Case Pattern



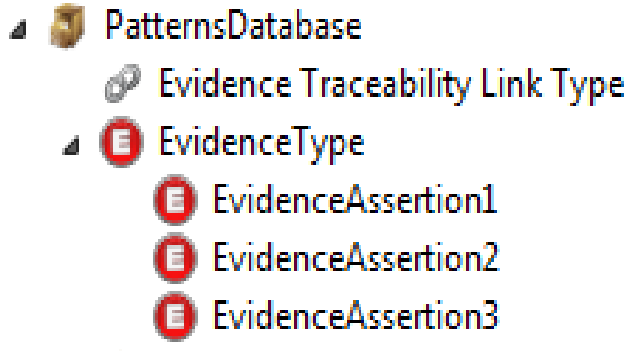
Evidence Manger in AF3

A prototypic implementation

The AF3 Evidence Manager contains **EvidenceItems**, **Assertions** made about the contained EvidenceItems and the **relationships between EvidenceItems**.

The user can:

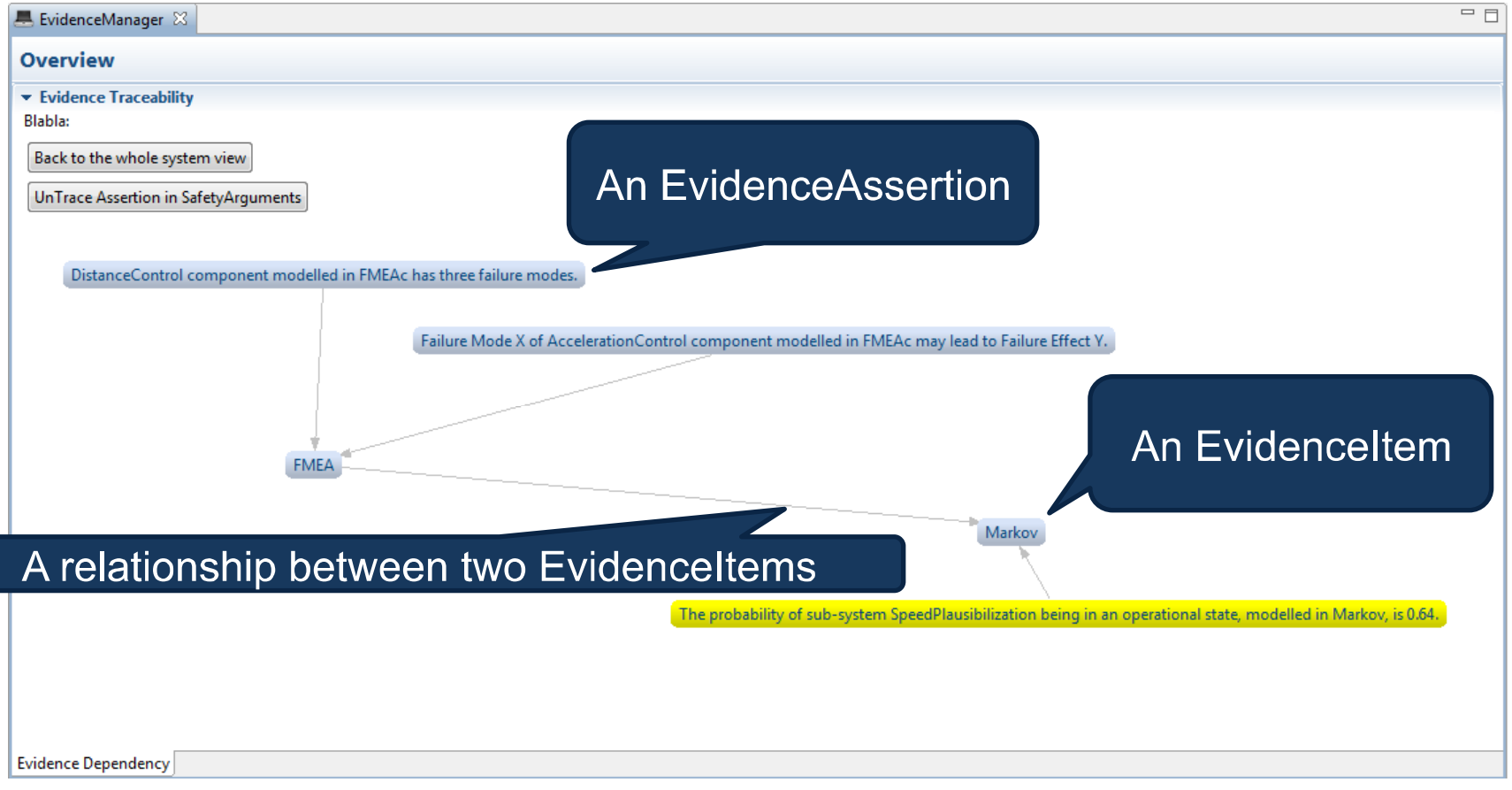
- ✓ Define EvidenceItem types
- ✓ Define Evidence Assertion patterns for a certain EvidenceItem type
- ✓ Define types of links that can exist between two EvidenceItems



fortiss

Evidence Manger in AF3

A prototypic implementation



fortiss

Thank you

Carmen Carlan (carlan@fortiss.org)
Sebastian Voss (voss@fortiss.org)

fortiss GmbH
An-Institut Technische Universität München
Guerickestraße 25 · 80805 München · Germany

tel +49 89 3603522 33 **fax** +49 89 3603522 50

www.fortiss.org

Please try yourself:

FOCUS ON THE SYSTEM

http://af3.fortiss.org

Open Source

Requirements Engineering

Modeling of Systems

Verification and Testing

Scheduling Synthesis

Code Generation and Deployment