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

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

FOCUS ON THE SYSTEM

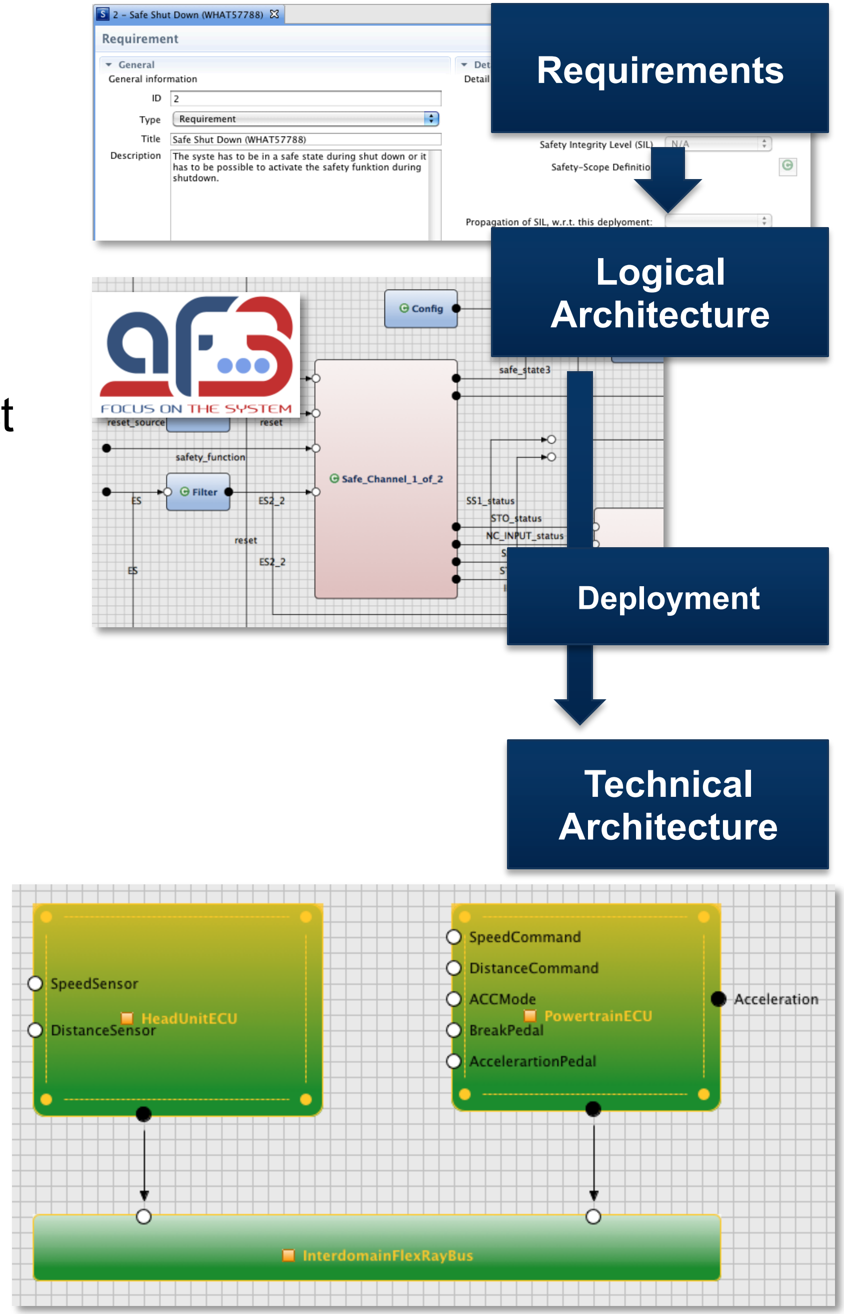
AutoFOCUS3 Basics

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)



2 - Safe Shut Down (WHAT57788)

Requirement

General

General information

ID: 2

Type: Requirement

Title: Safe Shut Down (WHAT57788)

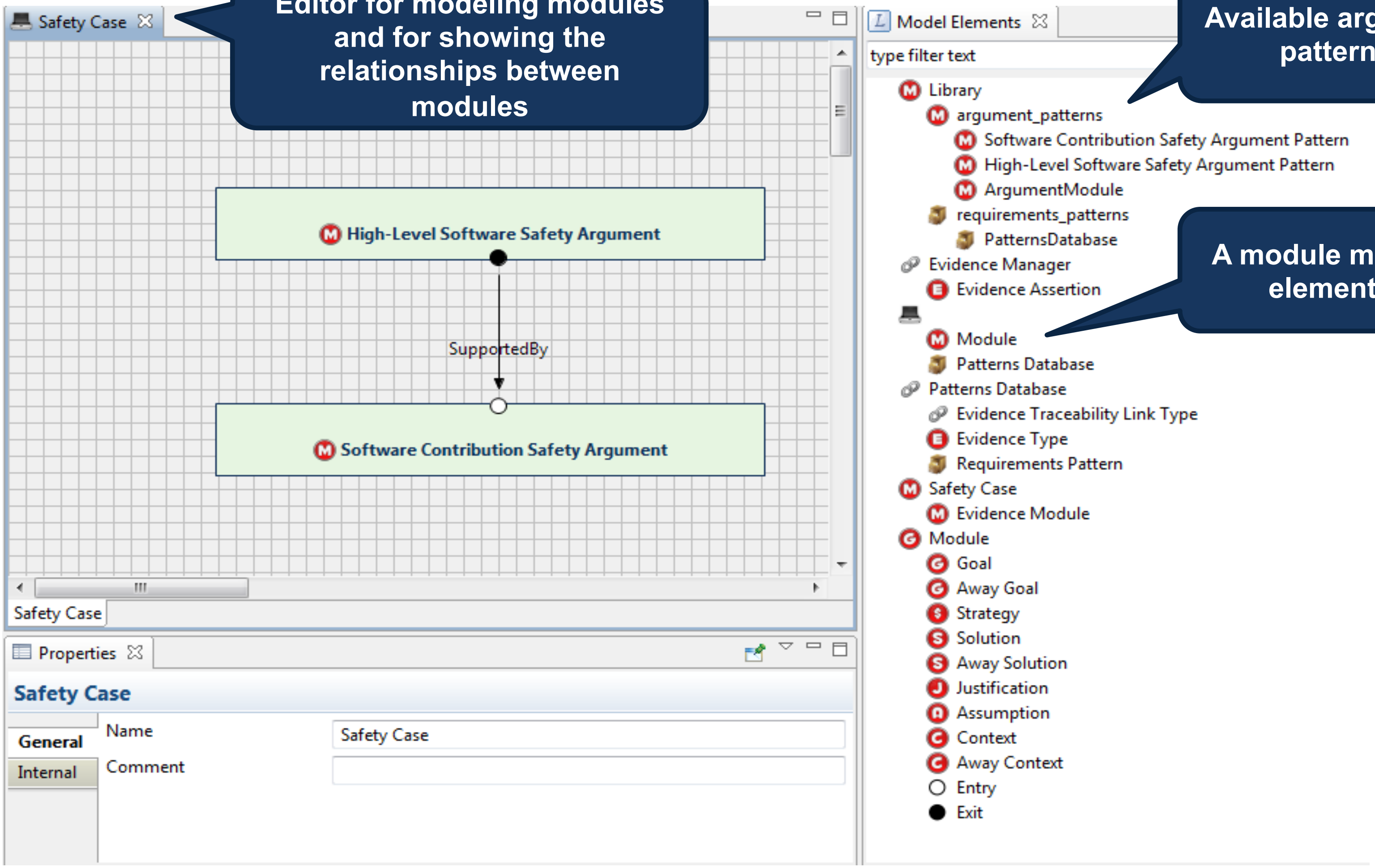
Description: The syste has to be in a safe state during shut down or it has to be possible to activate the safety funktion during shutdown.

Safety Integrity Level (SIL): N/A

Propagation of SIL, w.r.t. this deplyoment:

Safety Cases in AutoFOCUS3

The module view



Editor for modeling modules and for showing the relationships between modules

Available argument patterns

A module model element

- Library
  - argument_patterns
    - Software Contribution Safety Argument Pattern
    - High-Level Software Safety Argument Pattern
    - ArgumentModule
  - requirements_patterns
    - PatternsDatabase
- Evidence Manager
  - Evidence Assertion
-
  - Module
  - Patterns Database
- Patterns Database
  - Evidence Traceability Link Type
  - Evidence Type
  - Requirements Pattern
- Safety Case
  - Evidence Module
- Module
  - Goal
  - Away Goal
  - Strategy
  - Solution
  - Away Solution
  - Justification
  - Assumption
  - Context
  - Away Context
  - ○ Entry
  - ● Exit

Safety Case

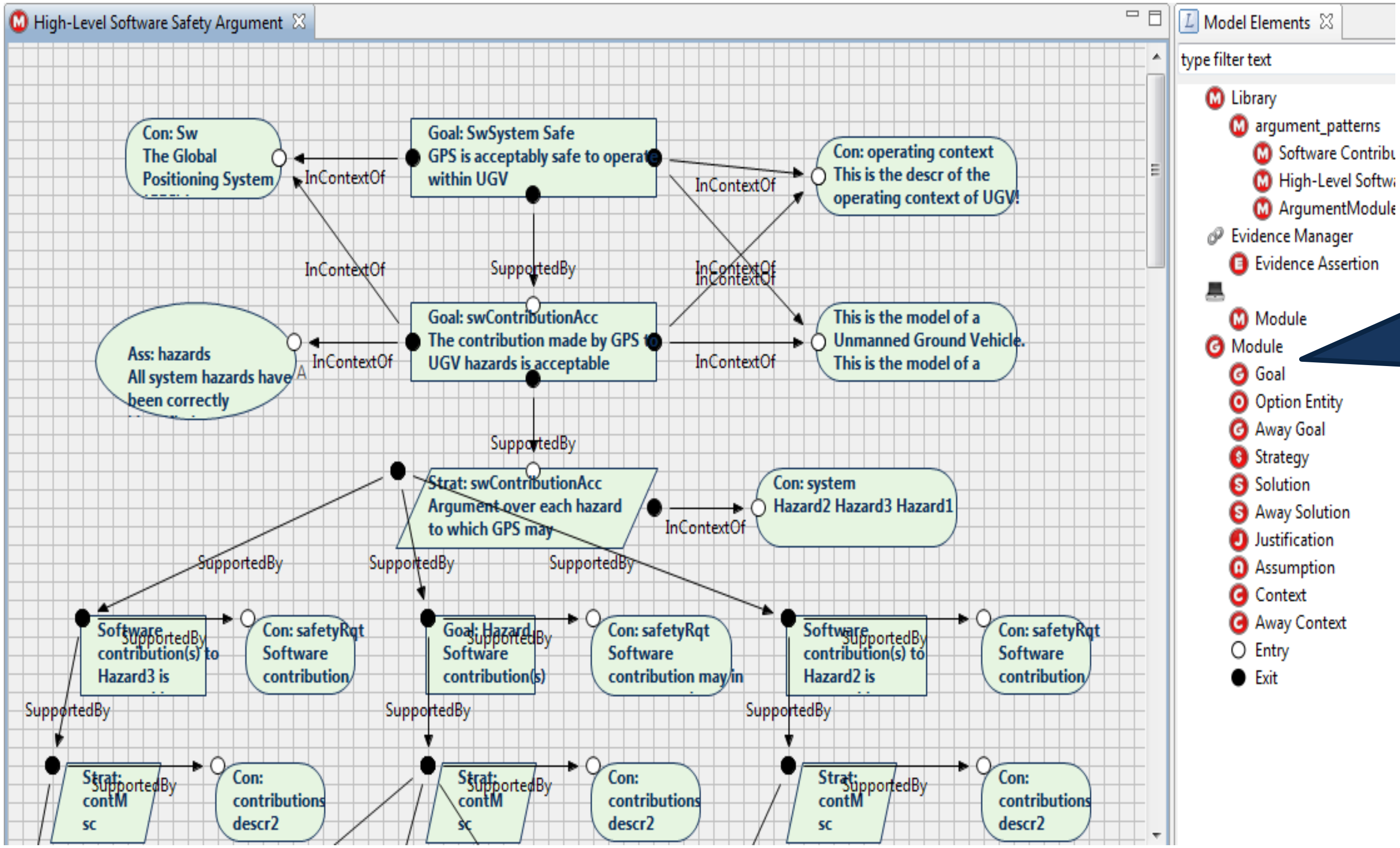
General | Internal

Name: Safety Case

Comment:

Safety Cases in AutoFOCUS3

The argument structure view



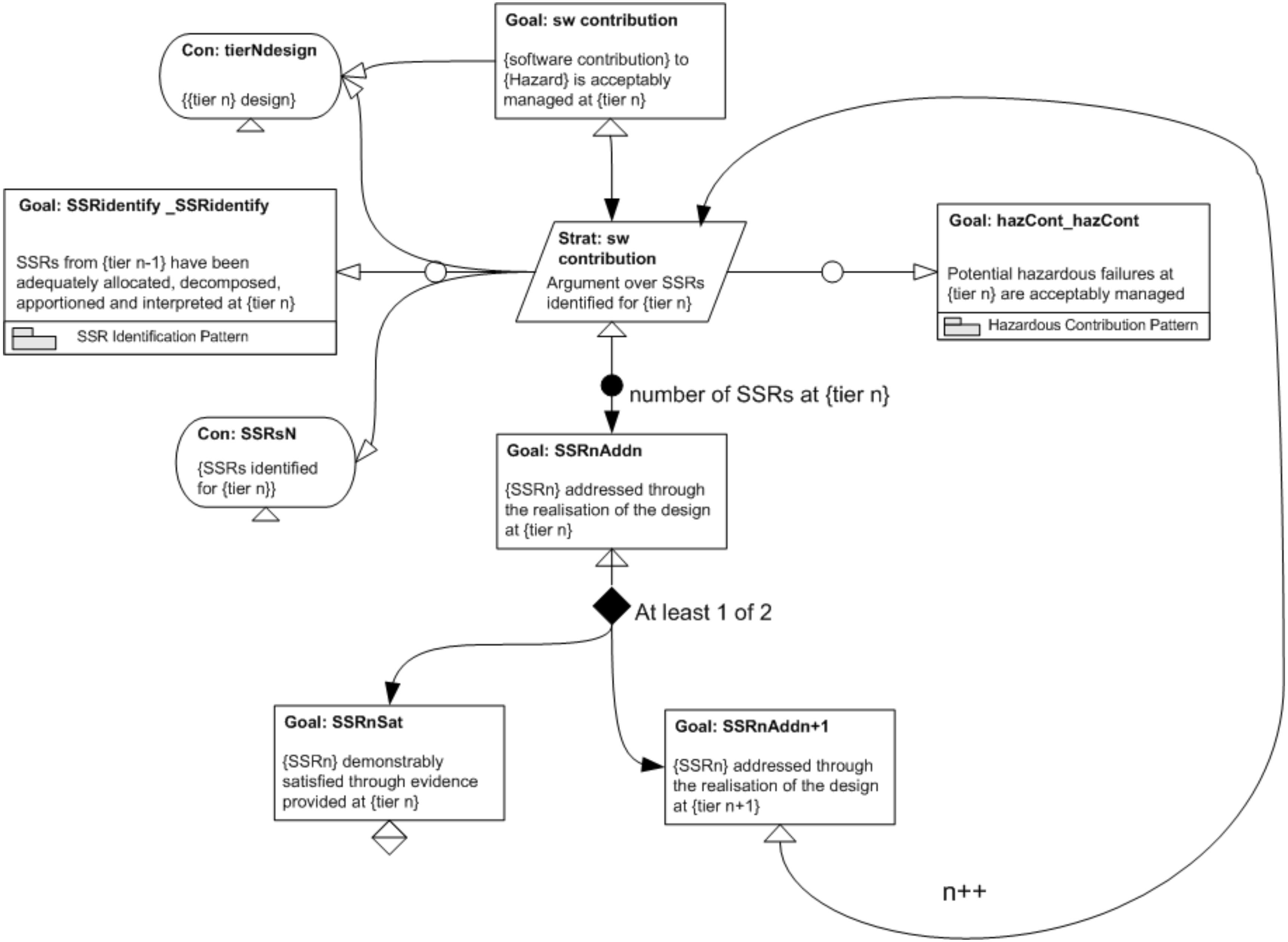
GSN model elements

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

Software Safety Case Pattern



Goal: sw contribution

{software contribution} to {Hazard} is acceptably managed at {tier n}

Con: tierNdesign

{{tier n} design}

Goal: SSRidentify _SSRidentify

SSRs from {tier n-1} have been adequately allocated, decomposed, apportioned and interpreted at {tier n}

SSR Identification Pattern

Strat: sw contribution

Argument over SSRs identified for {tier n}

Goal: hazCont_hazCont

Potential hazardous failures at {tier n} are acceptably managed

Hazardous Contribution Pattern

Con: SSRsN

{SSRs identified for {tier n}}

number of SSRs at {tier n}

Goal: SSRnAddn

{SSRn} addressed through the realisation of the design at {tier n}

At least 1 of 2

Goal: SSRnSat

{SSRn} demonstrably satisfied through evidence provided at {tier n}

Goal: SSRnAddn+1

{SSRn} addressed through the realisation of the design at {tier n+1}

n++

Evidence Manger in AF3

A prototypic implementation

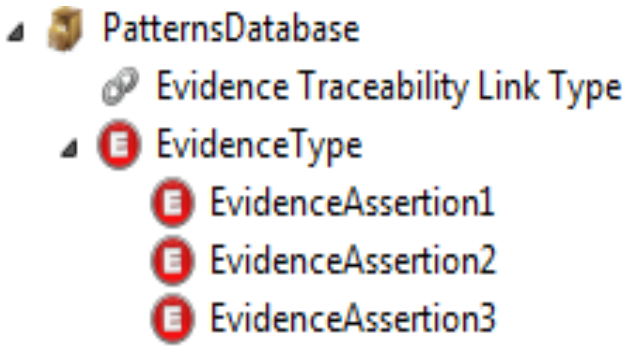
The AF3 Evidence Manager contains **EvidenceItems**, **Assertions** made about the contained EvidenceItems and the **relationships between EvidenceItems**.

The user can:

✓ Define EvidenceItem types

✓ Define Evidence Assertion patterns for a certain EvidenceItem type

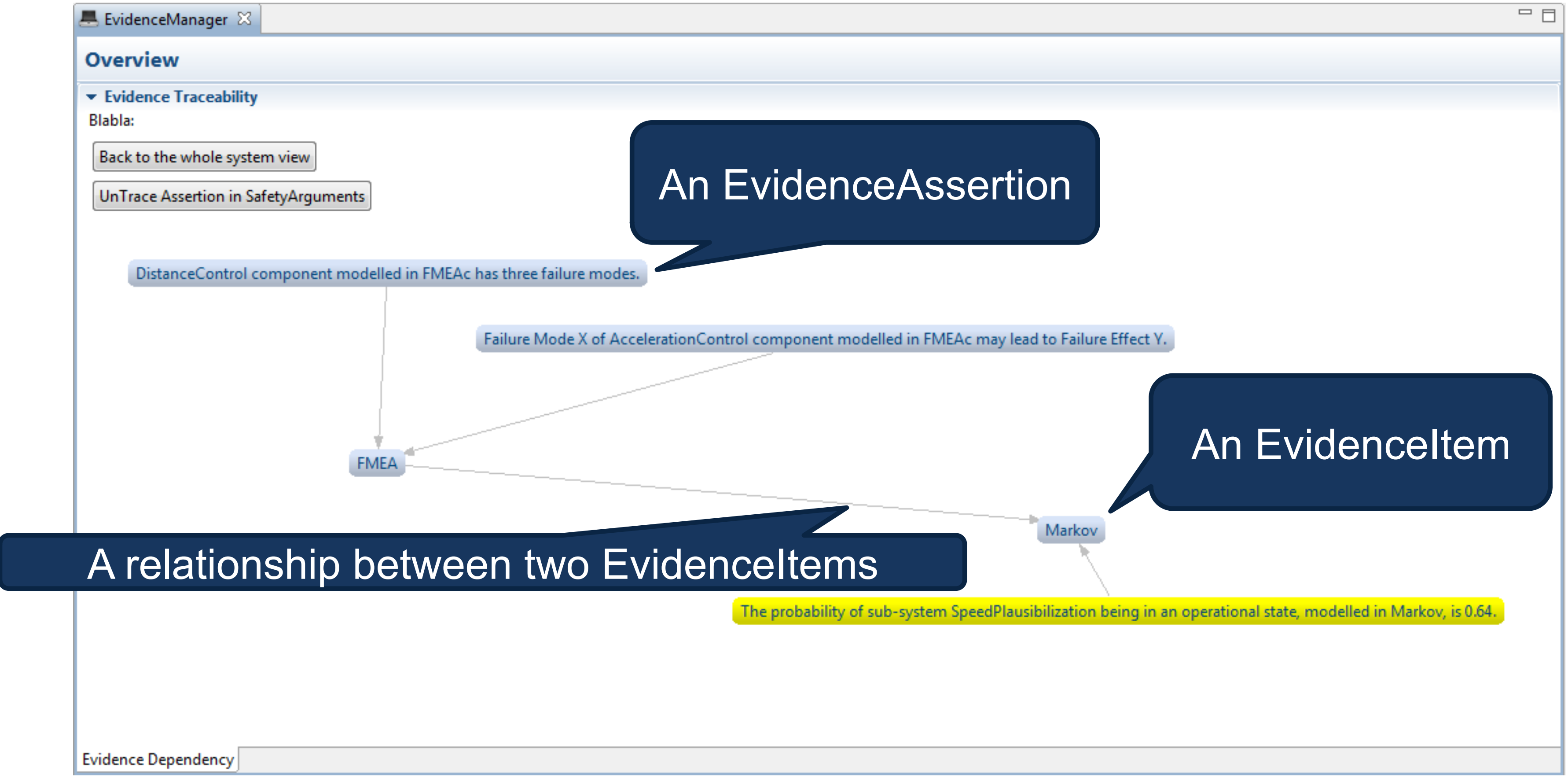
✓ Define types of links that can exist between two EvidenceItems



- PatternsDatabase
  - Evidence Traceability Link Type
  - EvidenceType
    - EvidenceAssertion1
    - EvidenceAssertion2
    - EvidenceAssertion3

Evidence Manger in AF3

A prototypic implementation



DistanceControl component modelled in FMEAc has three failure modes.

Failure Mode X of AccelerationControl component modelled in FMEAc may lead to Failure Effect Y.

The probability of sub-system SpeedPlausibilization being in an operational state, modelled in Markov, is 0.64.

An EvidenceAssertion

An EvidenceItem

A relationship between two EvidenceItems

Thank you

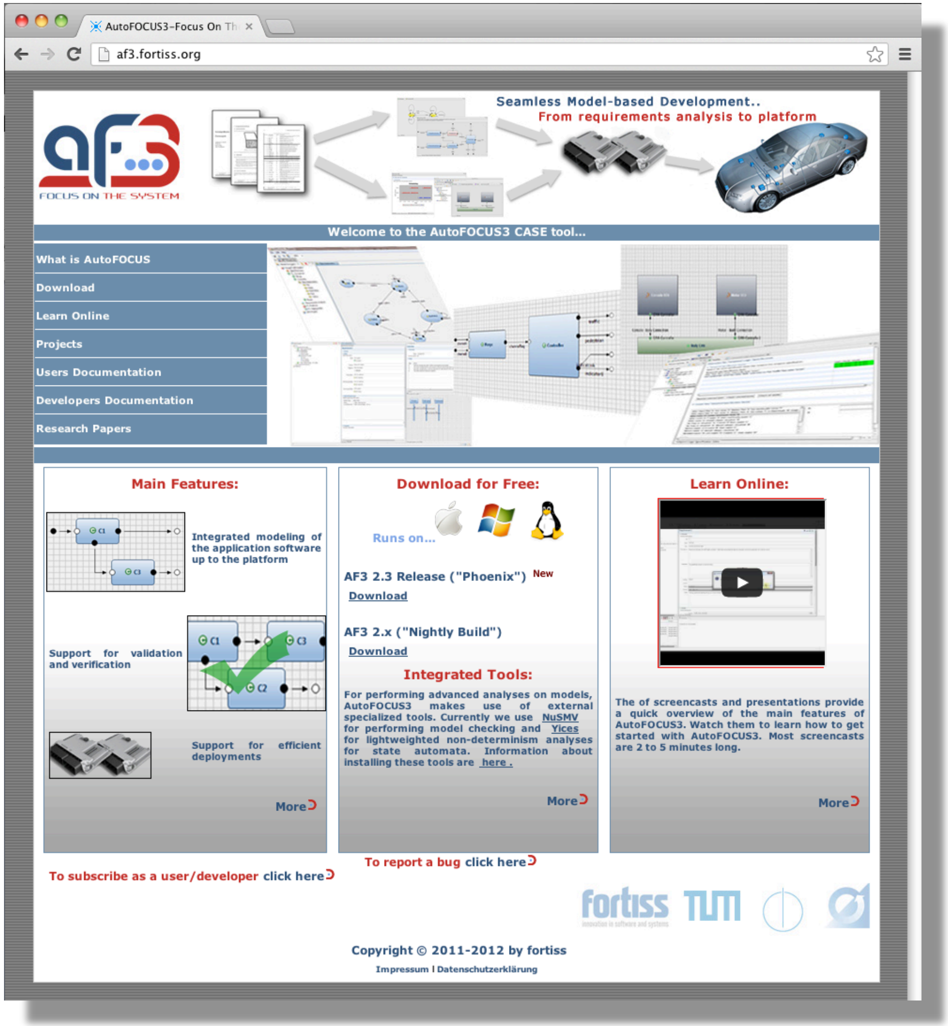
Carmen Carlan (carlan@fortiss.org)
Sebastian Voss (voss@fortiss.org)

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:



AutoFOCUS3-Focus On Th
af3.fortiss.org
FOCUS ON THE SYSTEM
Seamless Model-based Development..
From requirements analysis to platform

Welcome to the AutoFOCUS3 CASE tool...

Main Features:

Integrated modeling of the application software up to the platform

Support for validation and verification

Support for efficient deployments

More

Download for Free:

Runs on...

AF3 2.3 Release ("Phoenix") New

Download

AF3 2.x ("Nightly Build")

Download

Integrated Tools:

For performing advanced analyses on models, AutoFOCUS3 makes use of external specialized tools. Currently we use NuSMV for performing model checking and Yices for lightweighted non-determinism analyses for state automata. Information about installing these tools are here .

More

Learn Online:

The of screencasts and presentations provide a quick overview of the main features of AutoFOCUS3. Watch them to learn how to get started with AutoFOCUS3. Most screencasts are 2 to 5 minutes long.

More

To subscribe as a user/developer click here

To report a bug click here

Copyright © 2011-2012 by fortiss

Impressum I Datenschutzerklärung

FOCUS ON THE SYSTEM

http://af3.fortiss.org

Open Source

Requirements Engineering

Modeling of Systems

Verification and Testing

Scheduling Synthesis

Code Generation and Deployment