Component Fault Tree based Safety Analysis

ITEA3 - 17003

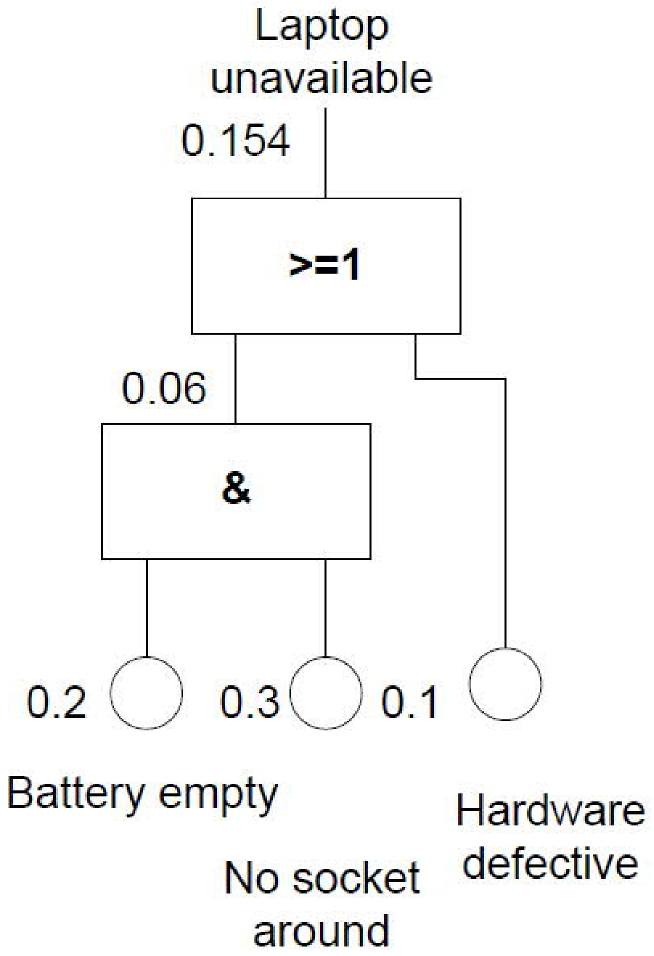
Introduction

- Embedded systems are omnipresent in the daily life
  - Realize **safety-relevant functions**
  - Failure may lead to catastrophic accidents
  - Safety is the most important non-functional property
- Increasing system **complexity**
  - Growing size and importance of software
  - Number of safety-relevant functions grows continuously
- Need and effort for **safety assurance** is increasing drastically
  - Safety analyses are very complex and time-consuming tasks
  - Contrast to the industry's aim to reduce development costs and time-to-market

Background: Fault Tree Analysis (FTA)

- FTA is **systematic top-down** approach for reliability and safety analysis
  - Fault trees trace back influences to a given hazard or failure
  - **Graphically explain** causal chains leading to the hazard
  - Find event combinations that are sufficient to cause hazard (qualitative analysis)
  - Calculate hazard probability from influence probabilities (quantitative analysis)

- Element of a Fault Tree:
  - Root: "Top-Event“
    - Hazard or failed state (or the accident or failure event)
  - Leaves: "Basic Events“
    - Causes that cannot or shall not be refined any further
  - Gates: AND, OR, M-out-of-N, etc.
    - Boolean logic



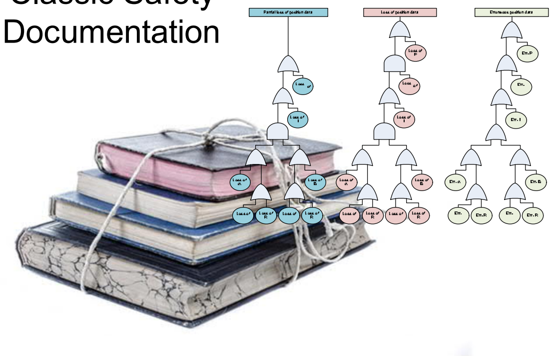
Developing Safety-critical Systems: State-of-practice

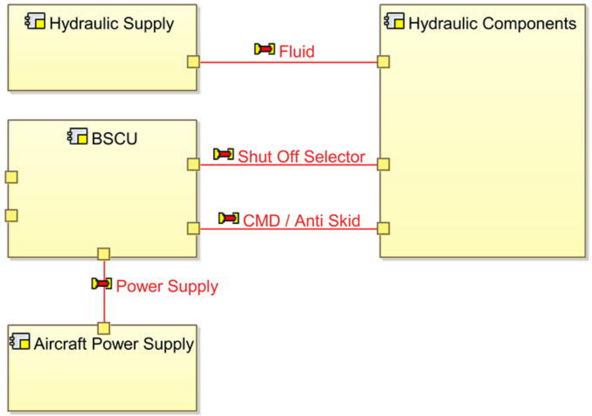
State-of-practice in safety analysis

System engineering

Media Break

Classic Safety Documentation





- **Modifications in safety documents is a very time consuming task**
- **Increased risk of inconsistency due to media breaks**

- **Often model-based (e.g. Capella)**
- **Iterative, incremental or agile**

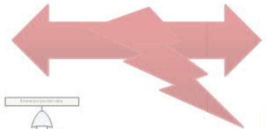
Developing Safety-critical Systems: Model-based safety analysis using Component Fault Trees (CFTs)

State-of-practice in safety analysis

System engineering

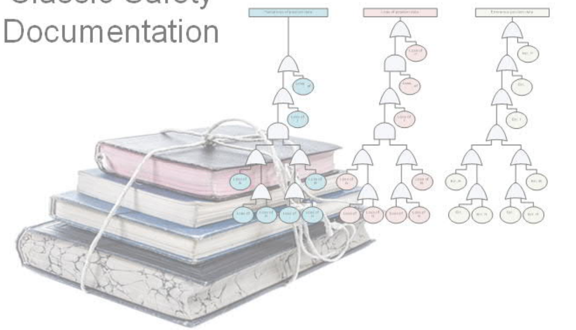
Integrated model-based safety/reliability analysis

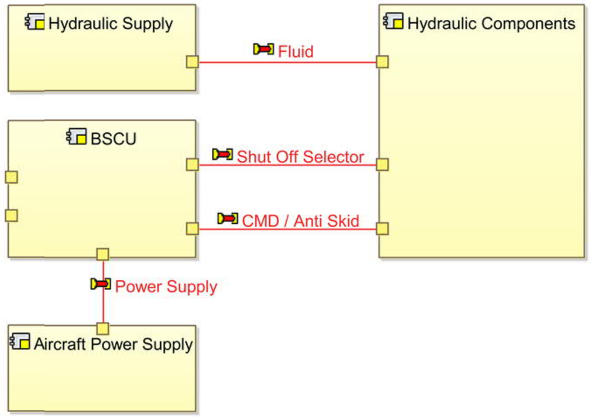
Media Break

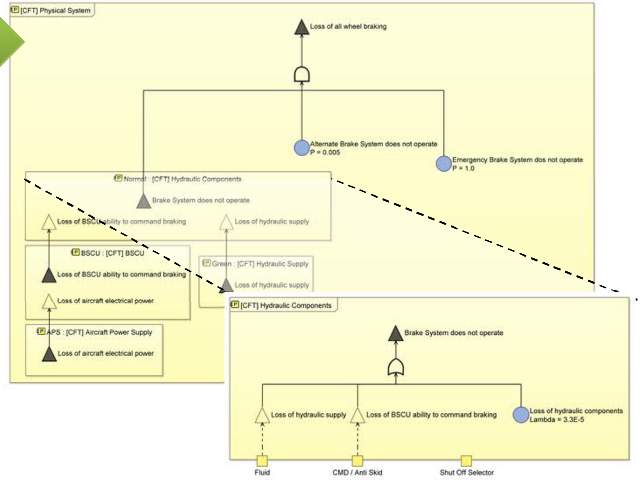


Seamless integration

Classic Safety Documentation







- Modifications in safety documents is a very time consuming task
- Increased risk of inconsistency due to media breaks

- Often model-based (e.g. Capella)
- Iterative, incremental or agile

- Modifications impact only a small part of the safety models
- Automated safety/reliability analysis at early development stages
- Consistency by seamlessly integrated models

Component Fault Trees (CFTs)*

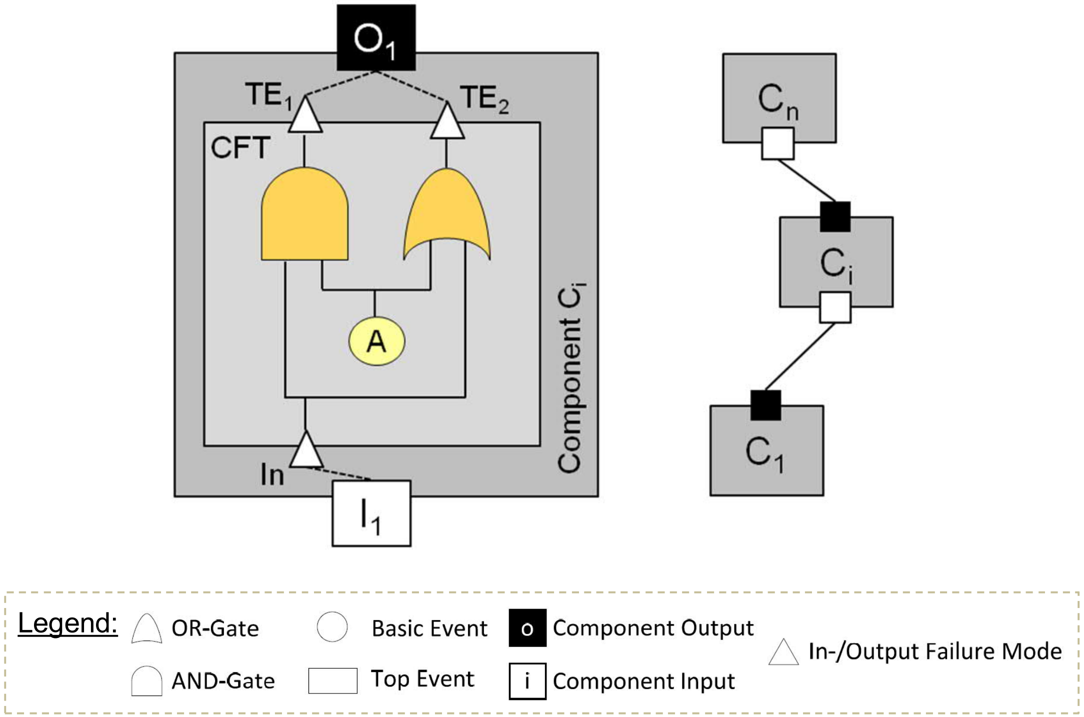
Extend classic fault trees with a component concept

Extension of classic fault trees with a component concept

- Focus on failure modes of an encapsulated system component
- Failures visible at the inport / outport of a component are modeled using Input / Output Failure Modes

Divide-and-conquer strategy for systems

- Modular, hierarchical composition of system fault trees
- Systematic reuse of component CFTs

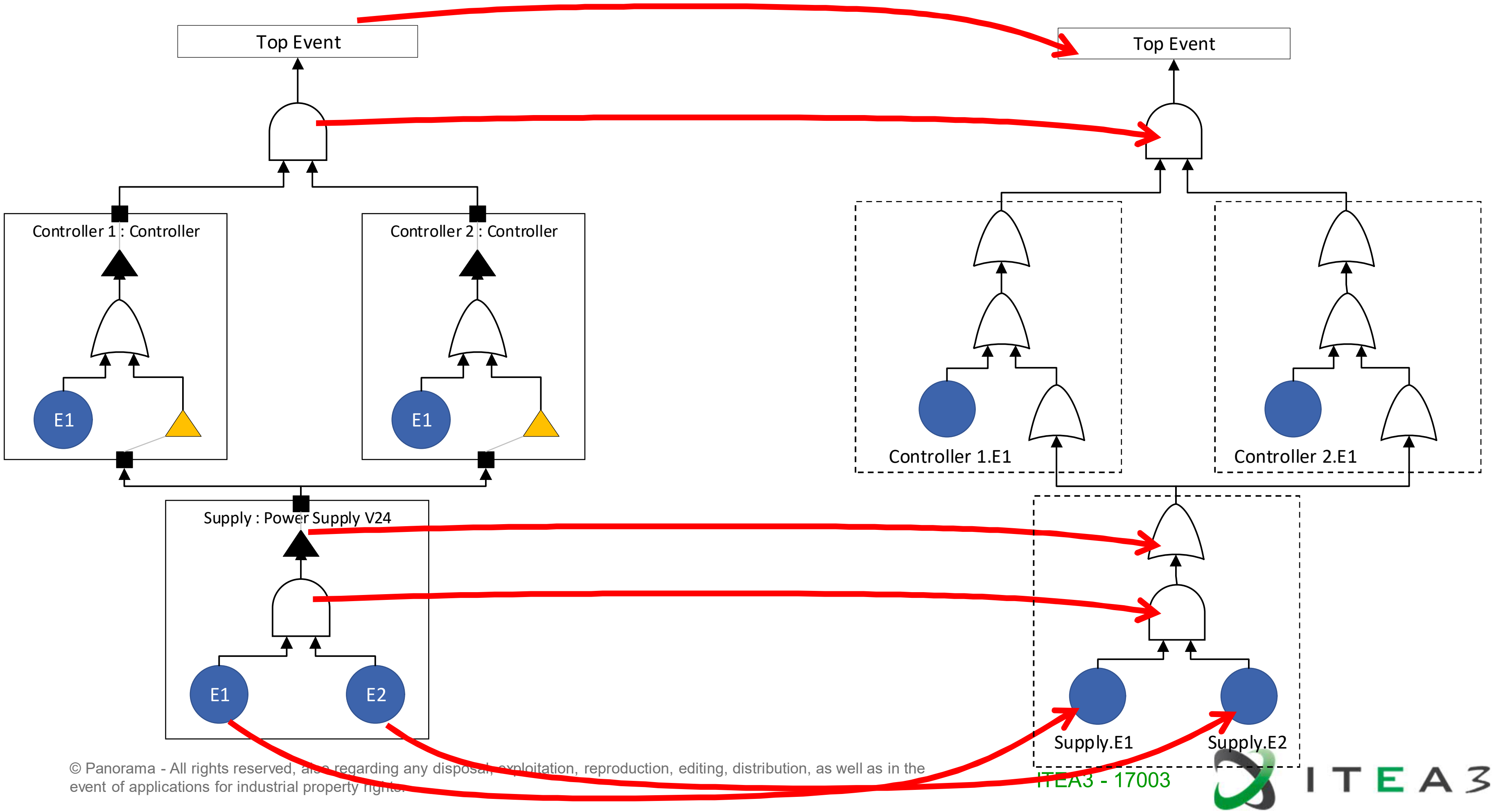


*) Kaiser, B.; Liggesmeyer, P.; Mäckel, O. (2003). “A new component concept for fault trees”, SCS '03: Proceedings of the 8th Australian workshop on Safety critical systems and software

Kaiser, B., Schneider, D., Adler, R., Domis, D., Möhrle, F., Berres, A., Zeller, M., Höfig, K., Rothfelder, M. (2018). „Advances in Component Fault Trees“, Proceedings of the 28th European Safety and Reliability Conference (ESREL)

Component Fault Trees vs. Fault Trees

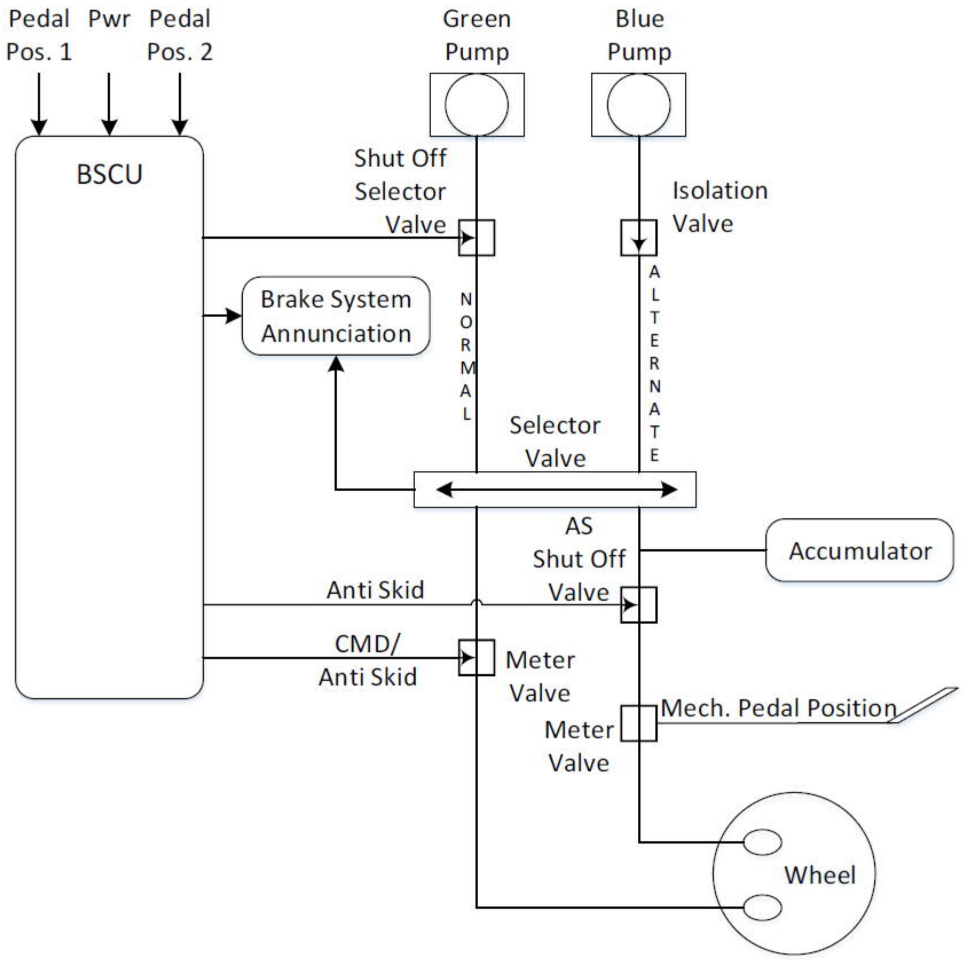
Same Information, Different Model Concept



Aircraft Wheel Brake System Example (from AIR6110)

- Installed on the two main landing gears
- **Braking on the main gear wheels** is used to provide safe retardation
  - During taxing and landing phases
- Also prevents unintended aircraft motion when parked
- May provide differential braking for aircraft directional control
- Secondary function: Stop main gear wheel rotation upon gear retraction

- Braking is commanded either
  - Manually
  - Via brake pedals
  - Automatically (autobrake) without the need for pedal application



Aircraft Wheel Brake System Example

Functional Hazard Analysis (FHA)

– Function: **"Decelerate the wheels on the ground"**
– Average flight length: **5 hours**

– Functional Hazard Analysis (FHA) results:
  - **Loss of all wheel braking during landing or rejected take off (RTO) shall be less than 5E-7 per flight**
  - Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing or RTO shall be less than 5E-7 per flight
  - Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be less than 5E-7 per flight
  - Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight
  - Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be less than 5E-9 per flight

→ Top Events of the Fault Tree Analysis in the System Safety Assessment (SSA) of the Wheel Braking System

V1 = Speed from which the aircraft cannot be safely stopped on remaining runway

Aircraft Wheel Brake System Example

CFT Example

Top Event = Loss of all wheel braking

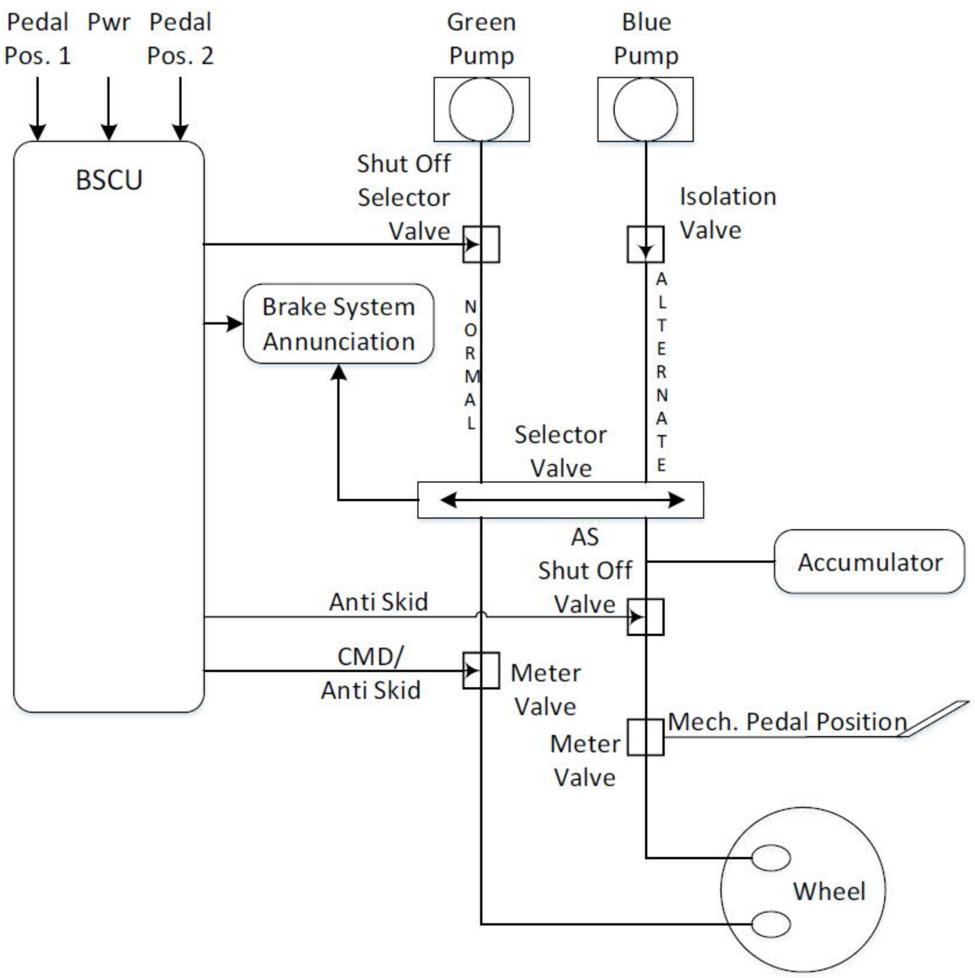
Steps to perform a safety/reliability analysis using CFTs:

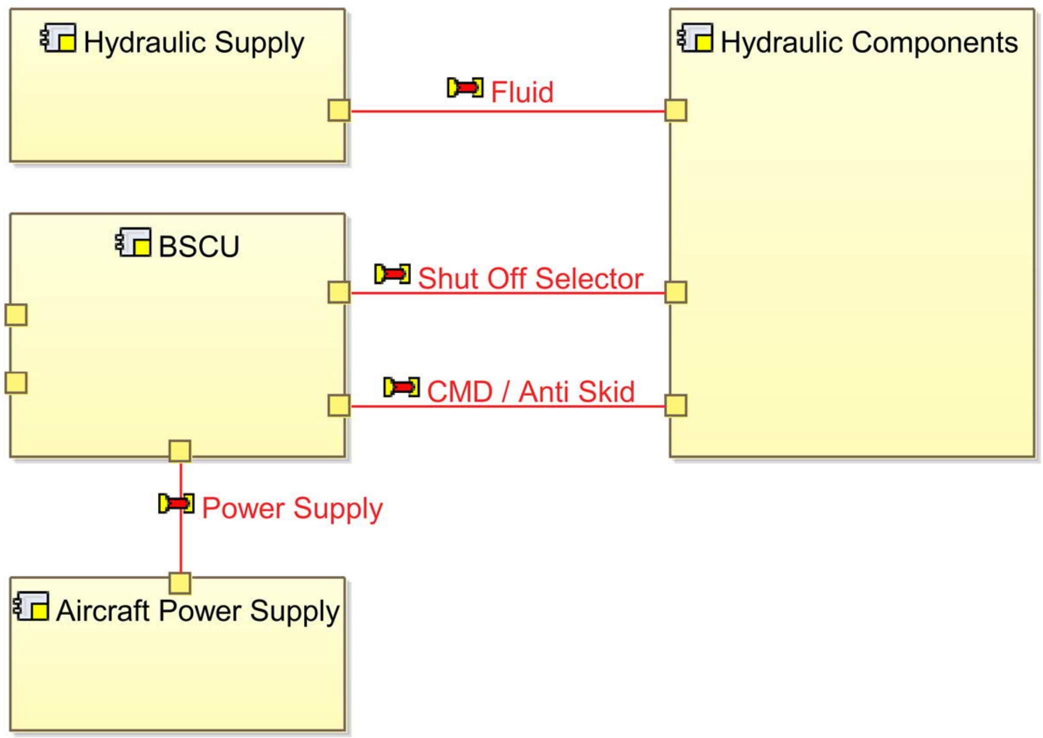
1. Identification of the system components and description of the system architecture (using Capella)
2. Specification of the CFT elements for each system component (using a viewpoint created with Sirius)
3. Semi-automated generation of the system-wide CFT and definition of the CFT's top event
4. Fault Tree Analysis (qualitative or quantitative)

Aircraft Wheel Brake System Example

Definition of the System Architecture (in Capella)

1

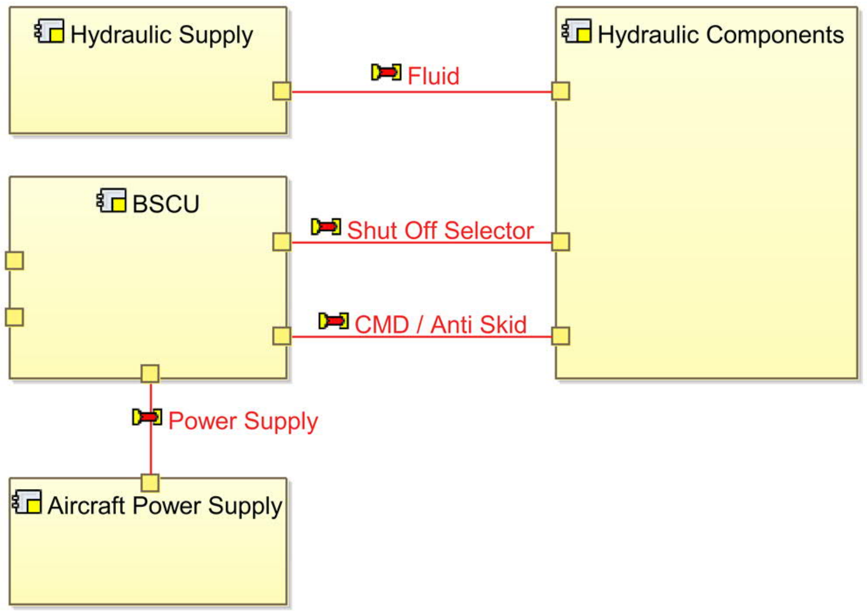


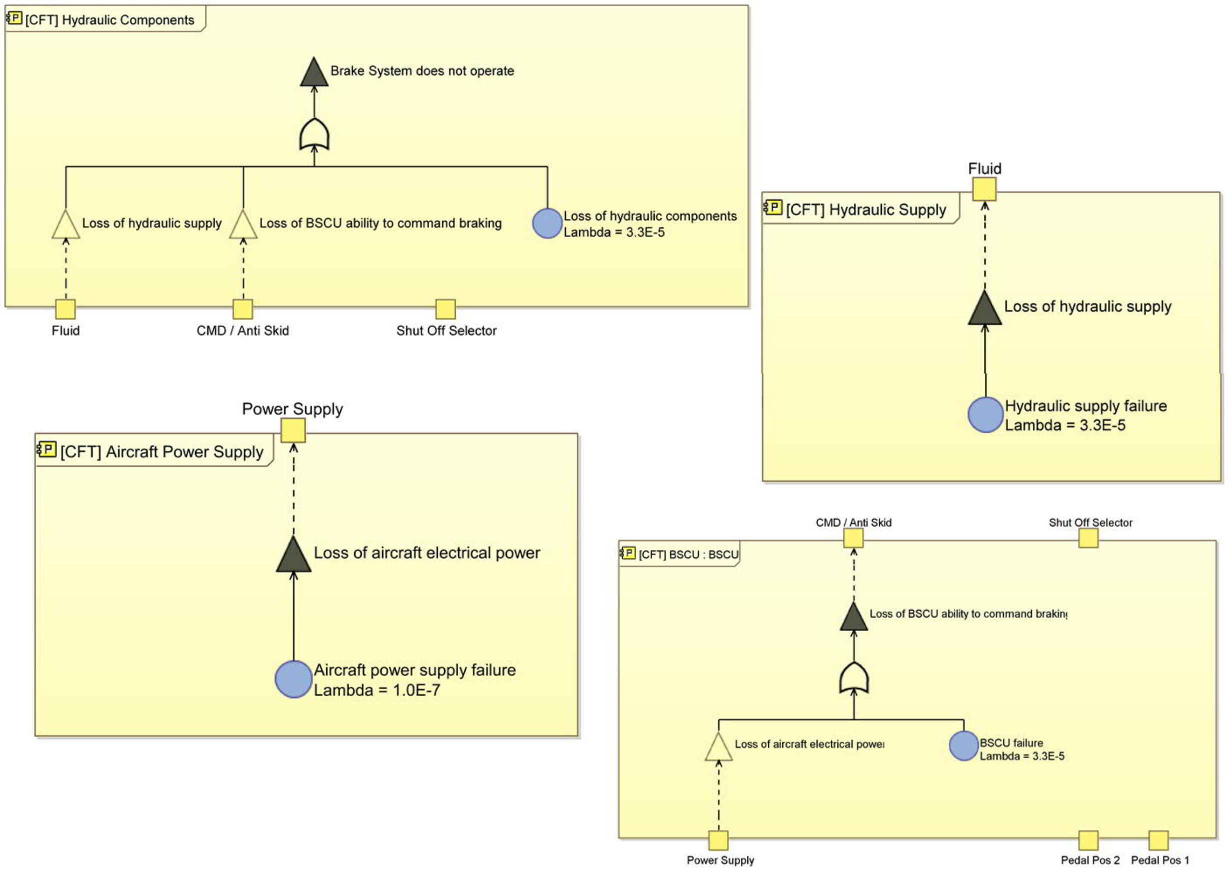


Aircraft Wheel Brake System Example

Specification of the CFT elements (Sirius-based viewpoint)

2

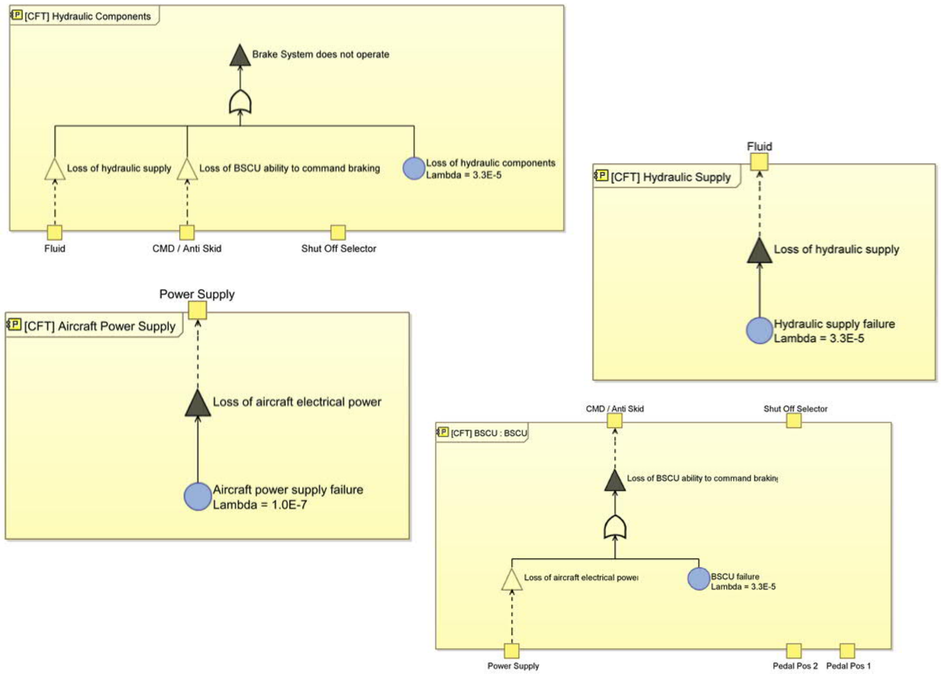


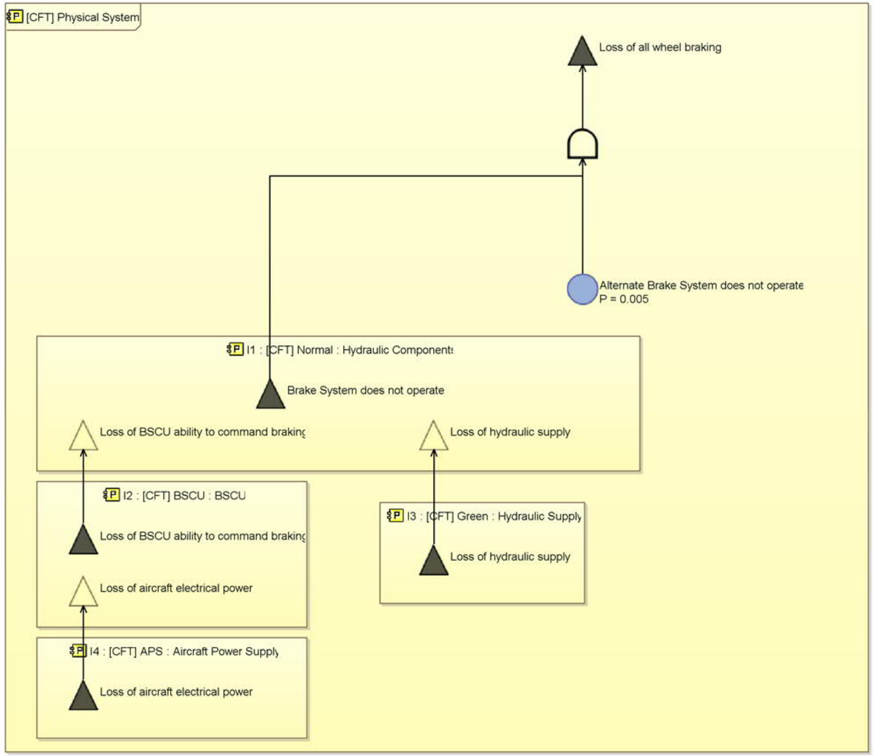


Aircraft Wheel Brake System Example

Semi-Automated generation of system-wide Component Fault Tree

3

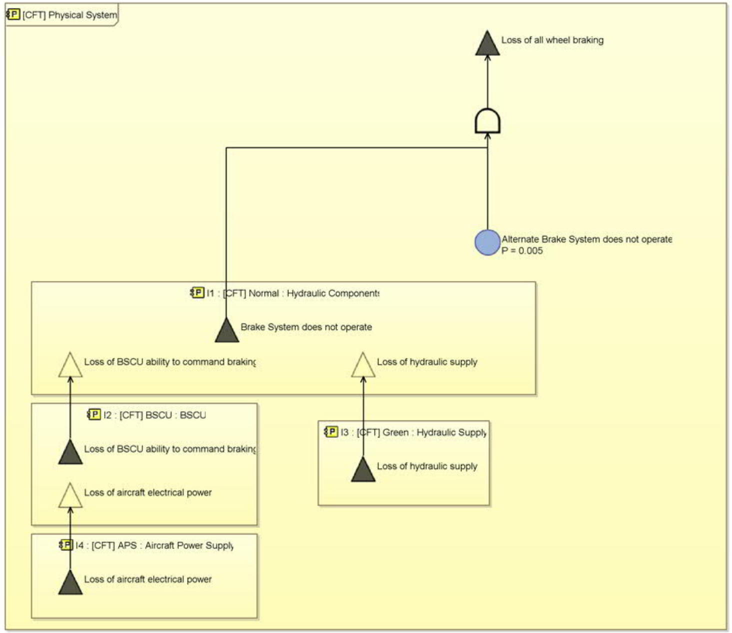


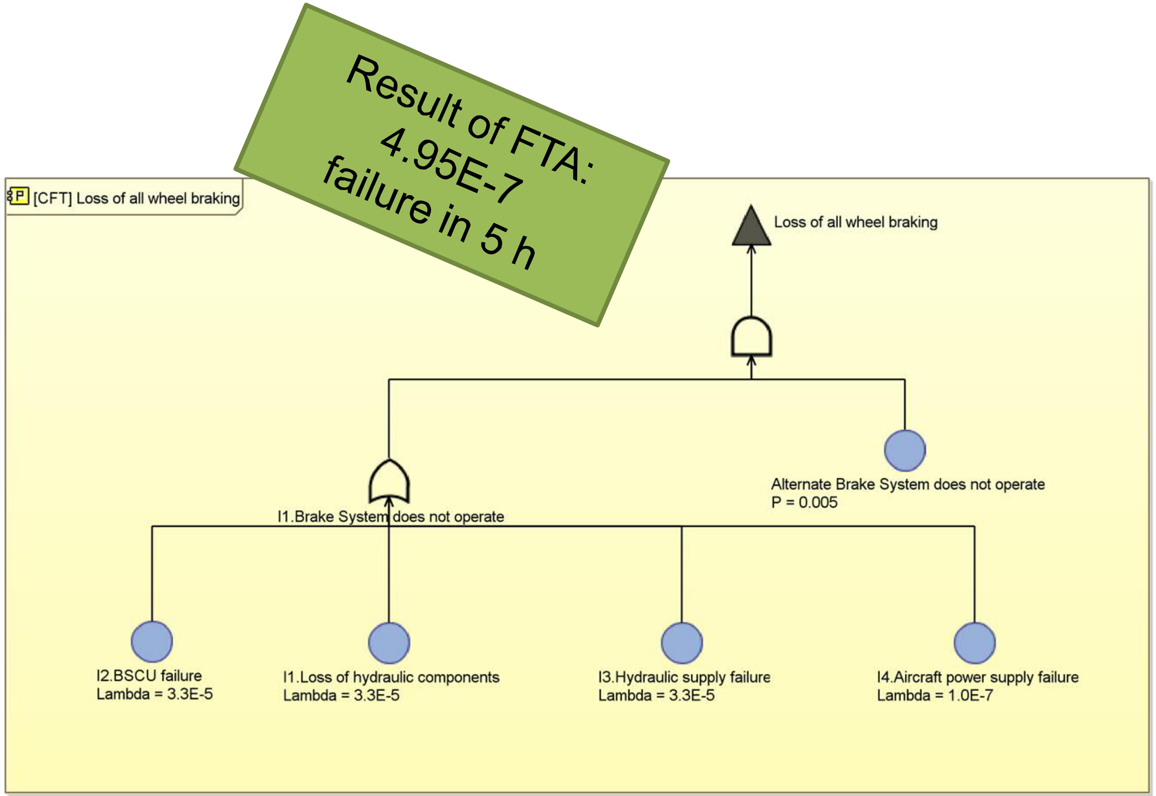


Aircraft Wheel Brake System Example

Fault Tree Analysis

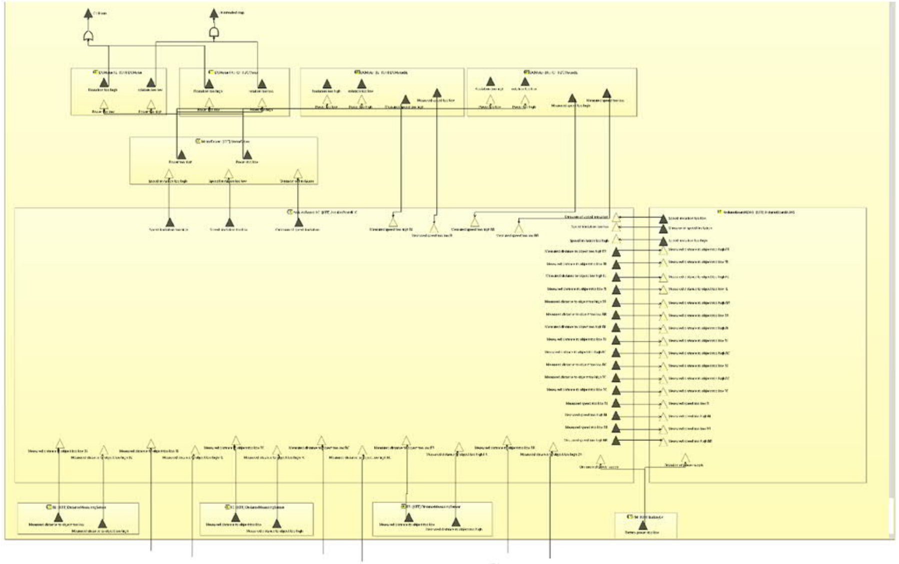
4

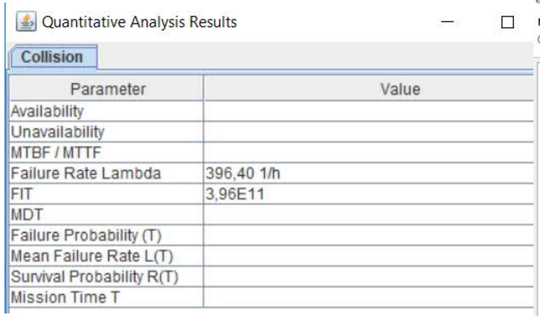




Component Fault Trees analysis for Heterogeneous Embedded Systems

- Component Fault Trees (CFTs)
  - Extension of classic fault trees with a component concept
- One CFT per component contain more than one top event
  - Instead of one Fault Tree for each top event
- Divide-and-conquer strategy for systems
  - Modular, hierarchical composition of CFTs
  - Systematic reuse of component CFTs
- Extension of CFT methodology in PANORAMA w.r.t. heterogenous embedded systems
  - Coupling with the the ALMATHEA metamodel

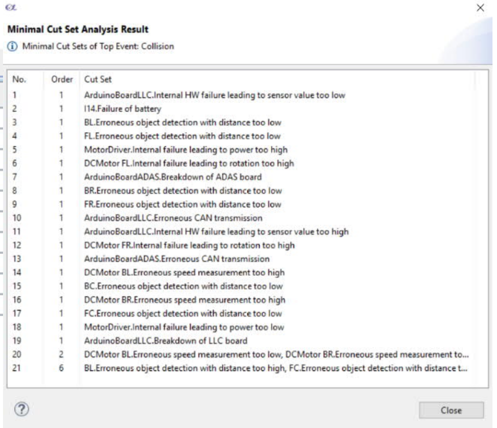




Quantitative Analysis Results

Collision

Parameter	Value
Availability	
Unavailability	
MTBF / MTTF	
Failure Rate Lambda	396,40 1/h
FIT	3,96E11
MDT	
Failure Probability (T)	
Mean Failure Rate L(T)	
Survival Probability R(T)	
Mission Time T	



Minimal Cut Set Analysis Result

Minimal Cut Sets of Top Event: Collision

No.	Order	Cut Set
1	1	ArduinoBoardLLC.Internal HW failure leading to sensor value too low
2	1	I14.Failure of battery
3	1	BL.Erroneous object detection with distance too low
4	1	FL.Erroneous object detection with distance too low
5	1	MotorDriver.Internal failure leading to power too high
6	1	DCMotor FL.Internal failure leading to rotation too high
7	1	ArduinoBoardADAS.Breakdown of ADAS board
8	1	BR.Erroneous object detection with distance too low
9	1	FR.Erroneous object detection with distance too low
10	1	ArduinoBoardLLC.Erroneous CAN transmission
11	1	ArduinoBoardLLC.Internal HW failure leading to sensor value too high
12	1	DCMotor FR.Internal failure leading to rotation too high
13	1	ArduinoBoardADAS.Erroneous CAN transmission
14	1	DCMotor BL.Erroneous speed measurement too high
15	1	BC.Erroneous object detection with distance too low
16	1	DCMotor BR.Erroneous speed measurement too high
17	1	FC.Erroneous object detection with distance too low
18	1	MotorDriver.Internal failure leading to power too low
19	1	ArduinoBoardLLC.Breakdown of LLC board
20	2	DCMotor BL.Erroneous speed measurement too low, DCMotor BR.Erroneous speed measurement to...
21	6	BL.Erroneous object detection with distance too high, FC.Erroneous object detection with distance t...

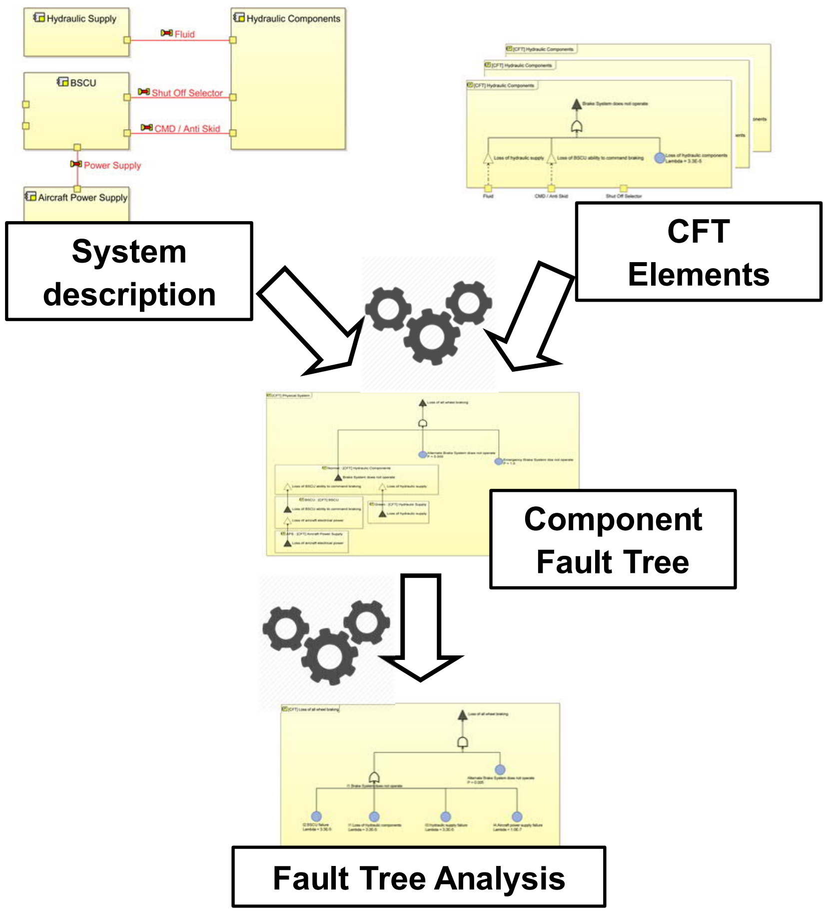
Close

ITEA3 - 17003

Component Fault Trees (CFTs)

Take Away Messages

- Divide-and-conquer strategy for safety/reliability analysis of complex systems
- Systematic reuse of CFT elements along with design artifacts
- (Semi-)Automated composition of pre-existing CFT elements
- Seamless Integration/Synchronization with any MBSE approach (e.g. Capella, SysMLv1/2, etc.)
- Easy integration into any EMF-based modeling approach (e.g. ALMATHEA)



Dr. Marc Zeller
Siemens AG, Technology

Otto-Hahn-Ring 6
81379 München
Germany

Mobile +49 (172) 103 60 65
E-mail marc.zeller@siemens.com