SIEMENS
Ingenuity for life

Model-based Safety Analysis on Capella using Component Fault Trees (CFTs)

Dr. Marc Zeller | Capella Day 2019

Developing Safety-critical Systems: State-of-practice

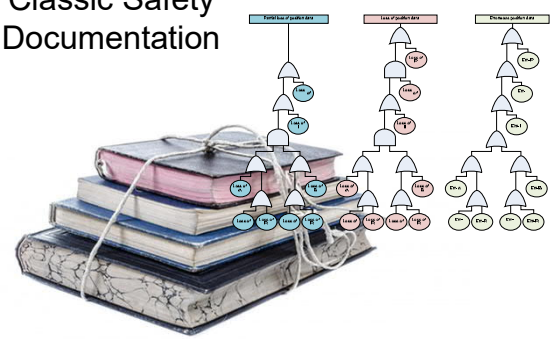
SIEMENS
Ingenuity for life

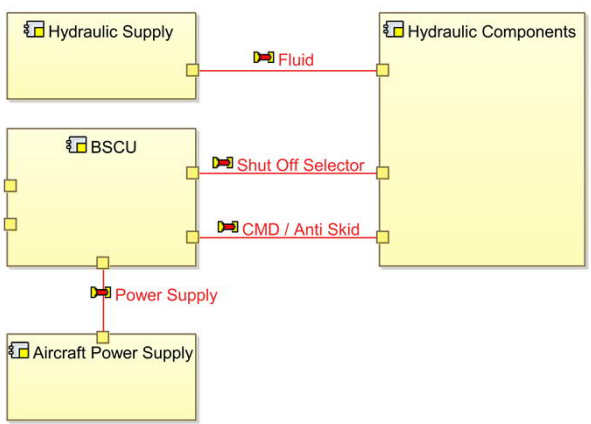
State-of-practice in safety analysis

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
- Iterative, incremental or agile

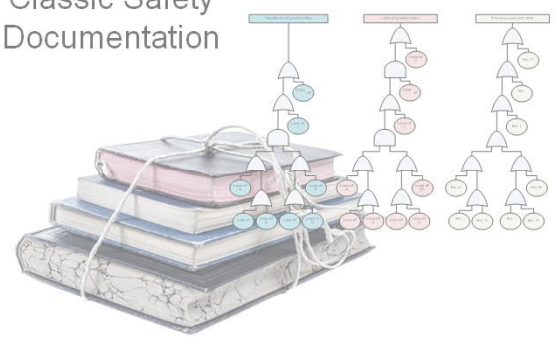
Developing Safety-critical Systems:
Model-based safety analysis using Component Fault Trees (CFTs)

SIEMENS
Ingenuity for life

State-of-practice in safety analysis

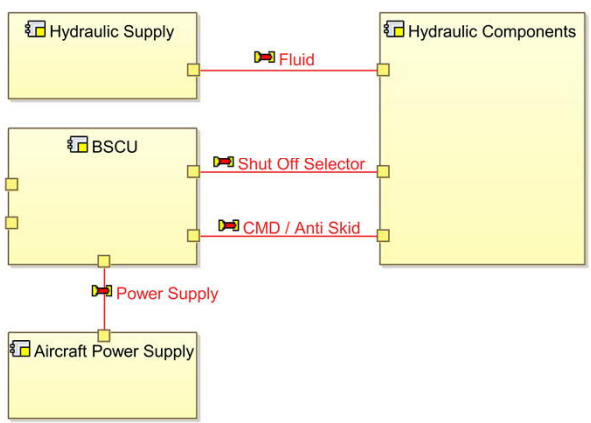
Media Break

Classic Safety Documentation



- Modifications in safety documents is a very time consuming task
- Mostly done at the end of projects, high risk to fail certification
- Inconsistency due to media breaks

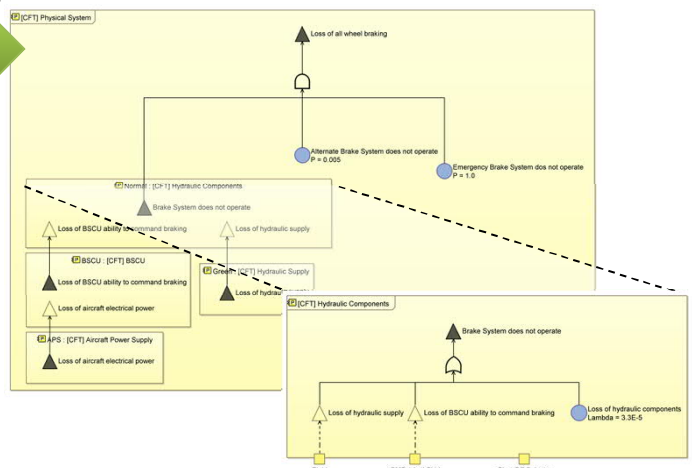
System engineering



- Often model-based
- Iterative, incremental or agile

Integrated model-based safety/reliability analysis

Seamless integration



- 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

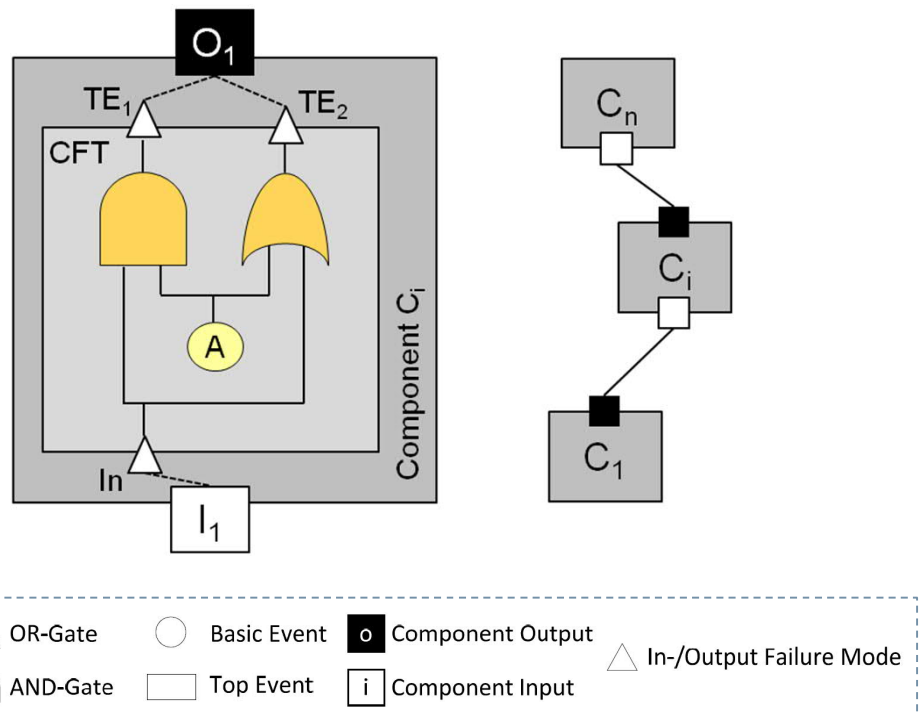
SIEMENS
Ingenuity for life

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



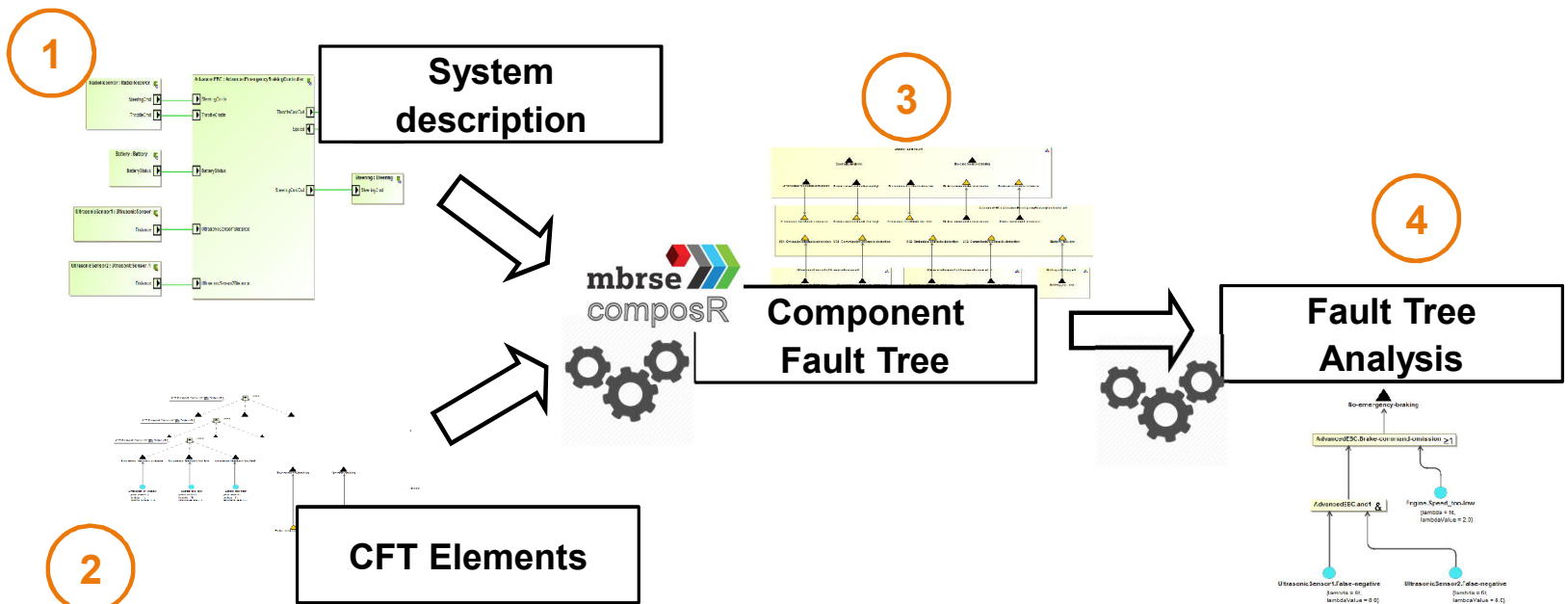
*) Höfig, K., Joanni, A., Zeller, M., Montrone, F., Rothfelder, M., Amarnath, R., Munk, P., Nordmann, A. (2018). Model-based Reliability and Safety: Reducing the complexity of safety analyses using component fault trees, Proceedings of the 2018 Annual Reliability and Maintainability Symposium (RAMS)

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 Tree based Safety/Reliability Analysis
Modeling & Analysis Workflow

SIEMENS
Ingenuity for life

CFTs @ work



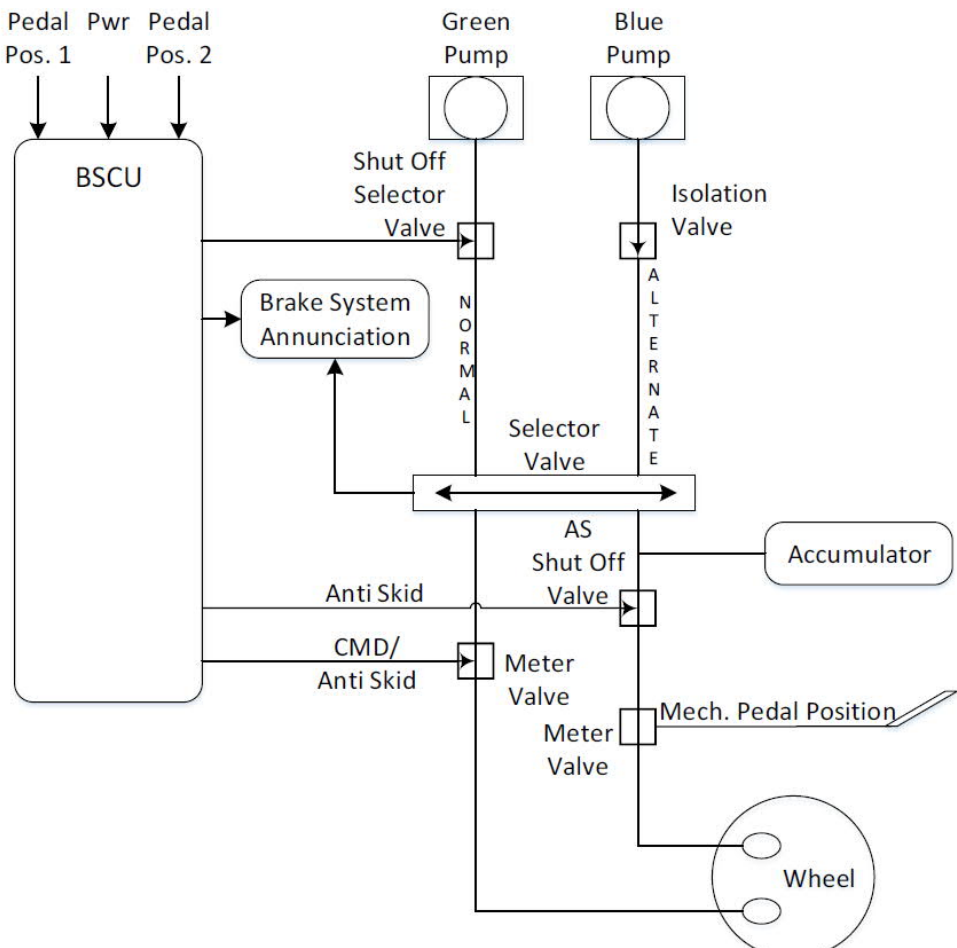
Aircraft Wheel Brake System Example Overview

SIEMENS
Ingenuity for life

Example from AIR6110

- Installed on the two main landing gears
- Braking on the main gear wheels is used to provide safe retardation
  - During taxiing 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
Hazard Analysis

SIEMENS
Ingenuity for life

- Function: “Decelerate the wheels on the ground”
- Average flight length: 5 hours

- 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 in the PSSA 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

SIEMENS
Ingenuity for life

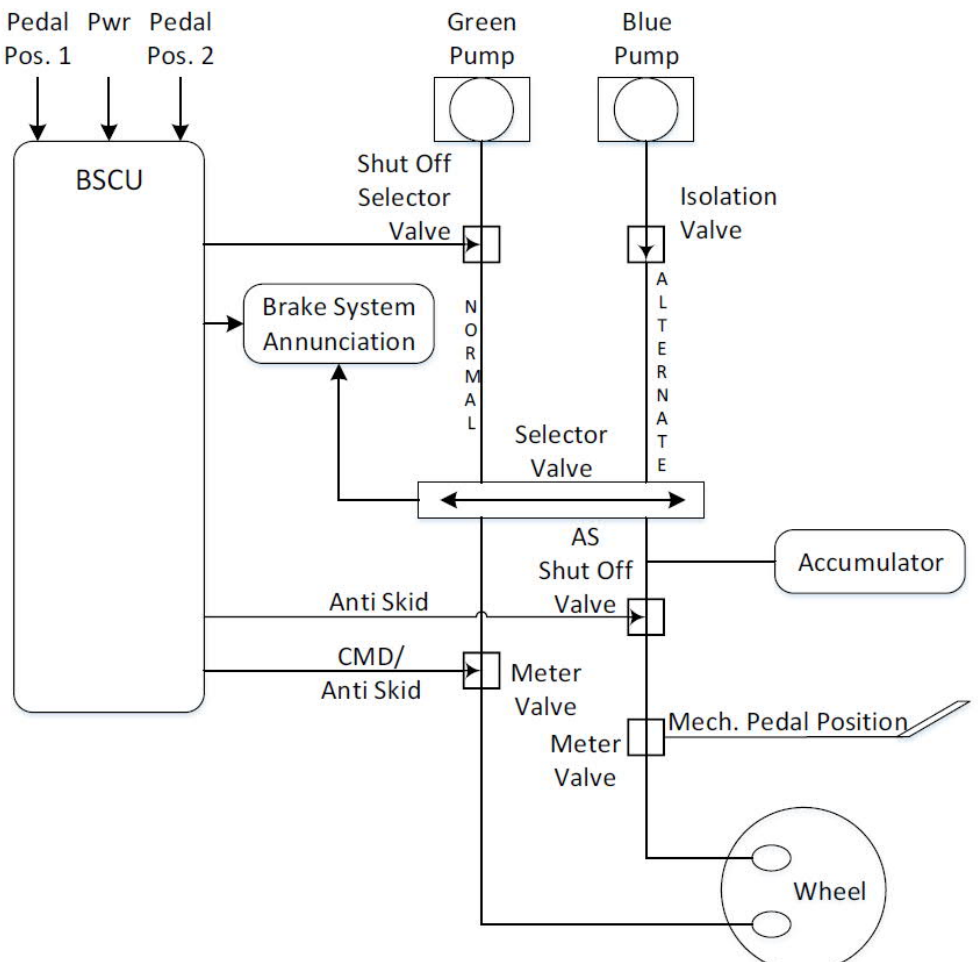
Top Event = Loss of all wheel braking

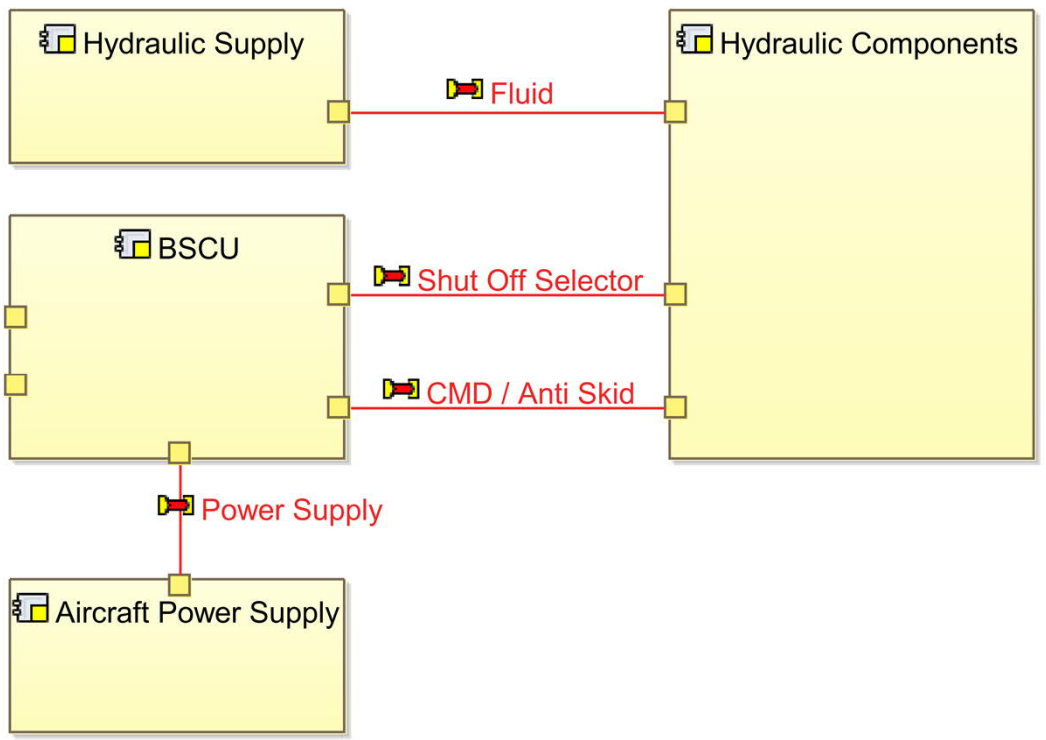
Steps to perform a safety/reliability analysis using CFTs:

1. Identification of the system components and description of the system architecture 1
2. Specification of the CFT elements for each system component 2
3. Creation of the system-wide CFT and definition and of the CFT's top event 3
4. Fault Tree Analysis (qualitative or quantitative) 4

Aircraft Wheel Brake System Example
Definition of the System Architecture (in Capella/SMW)

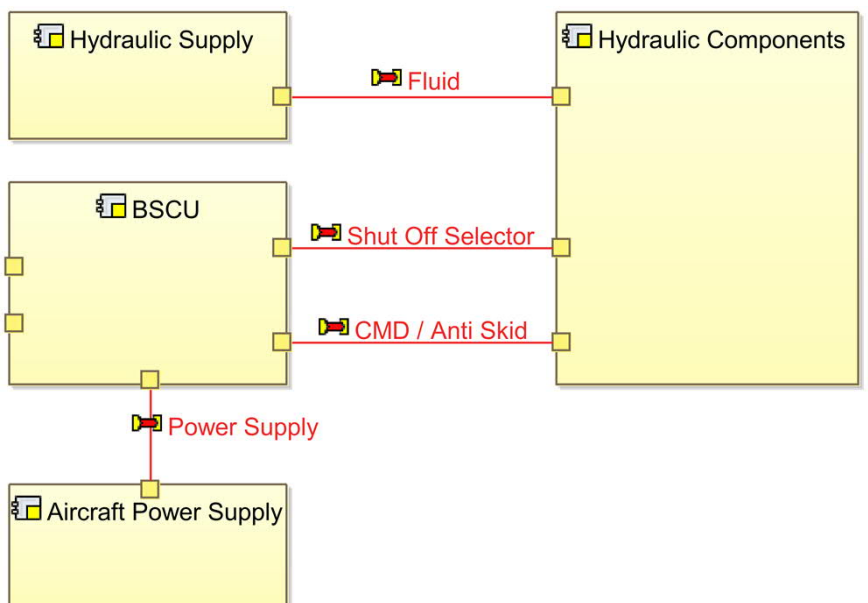
SIEMENS
Ingenuity for life

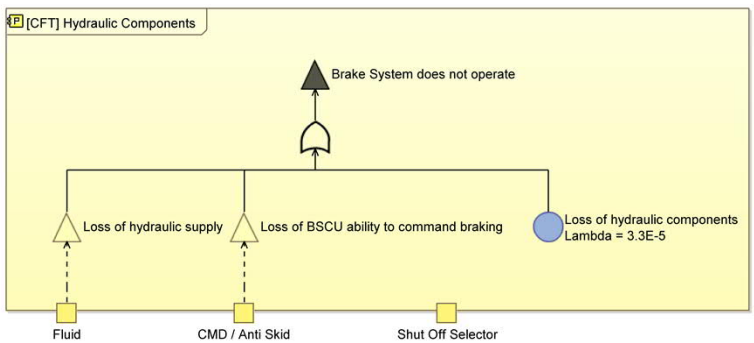


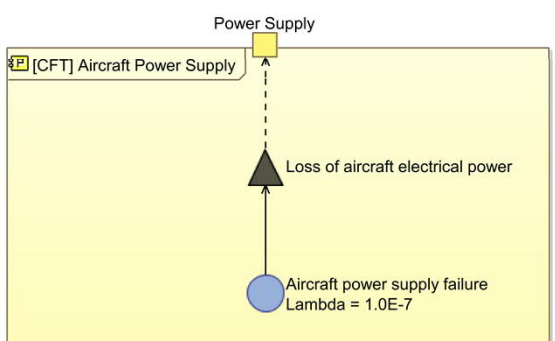


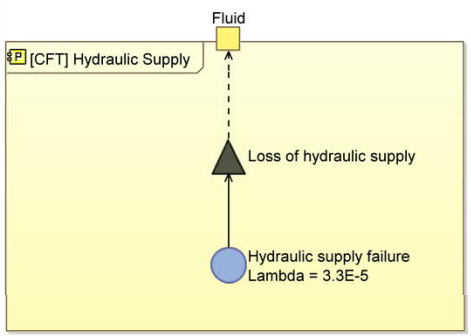
Aircraft Wheel Brake System Example
Specification of the CFT elements

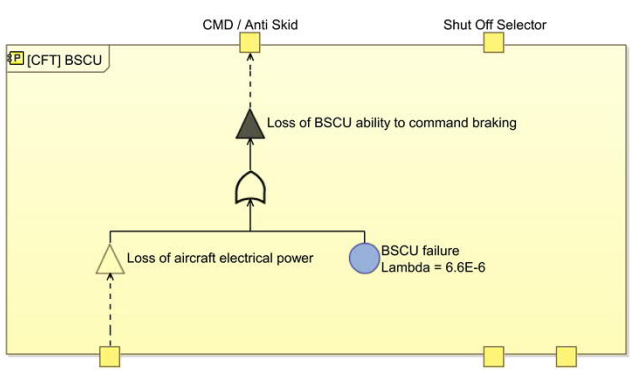
SIEMENS
Ingenuity for life





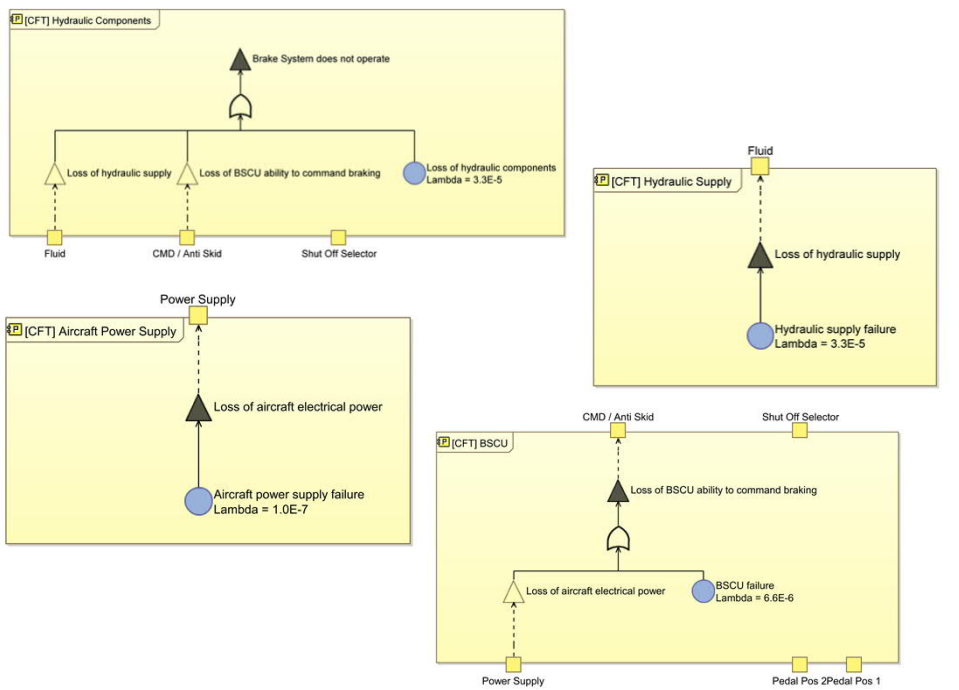


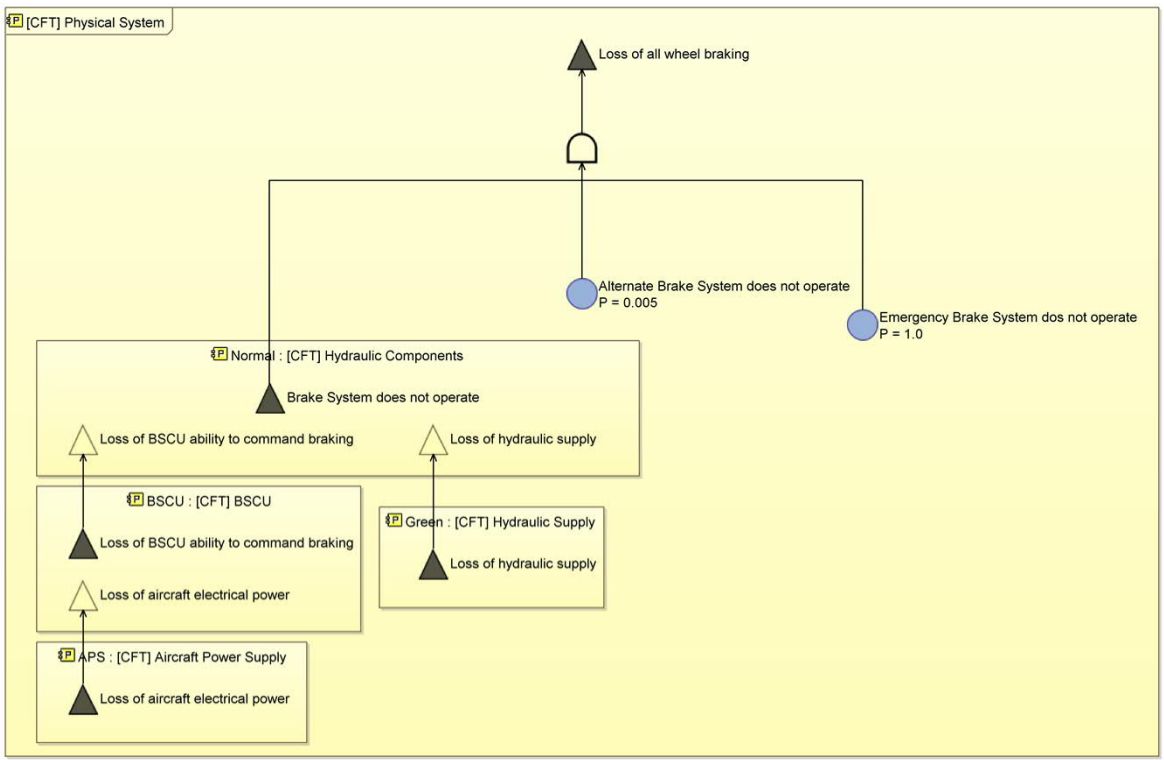




Aircraft Wheel Brake System Example
Creation of the system-wide Component Fault Tree

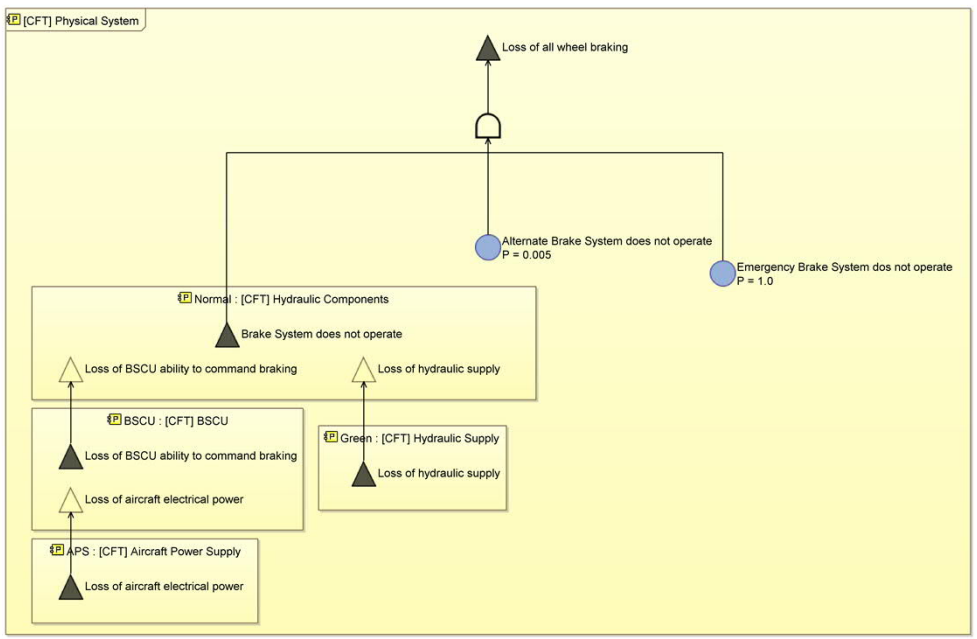
SIEMENS
Ingenuity for life



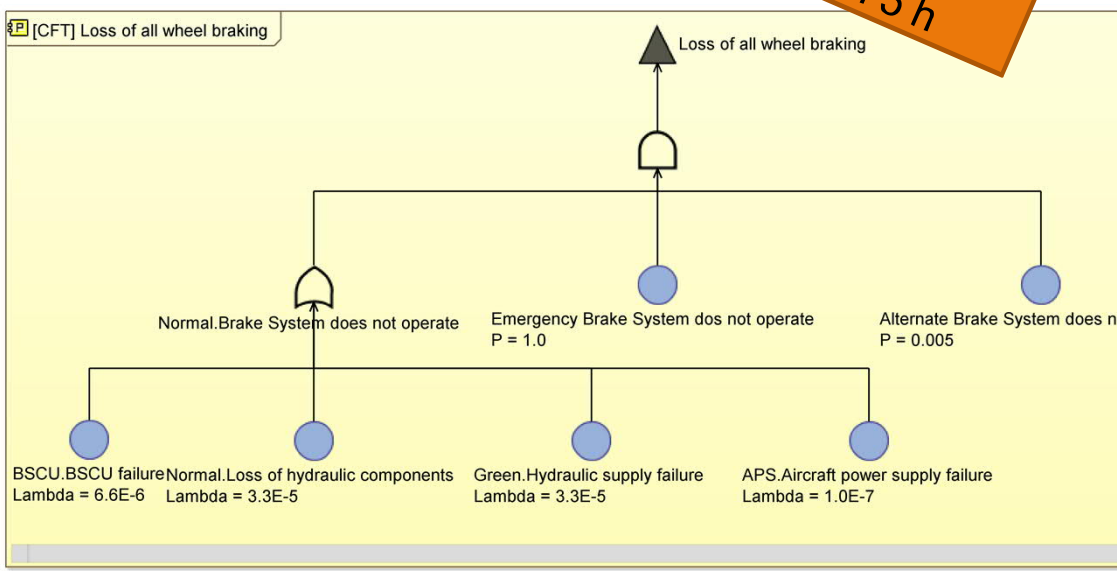


Aircraft Wheel Brake System Example
Fault Tree Analysis

SIEMENS
Ingenuity for life



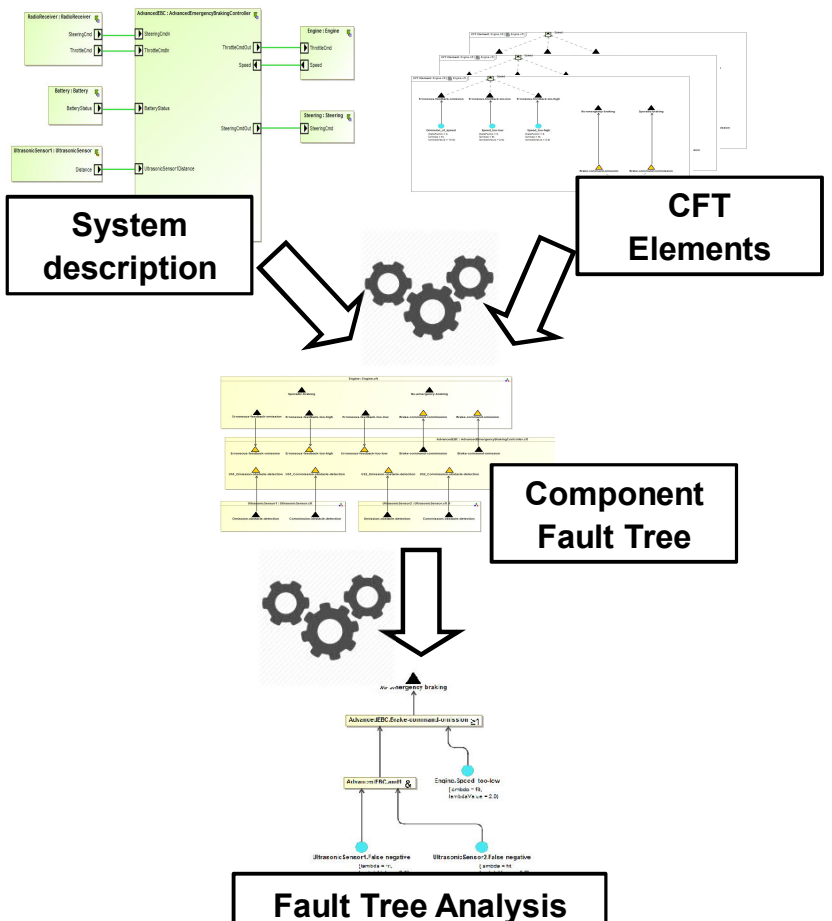
Result of FTA:
1.65E-7
failure in 5 h



Component Fault Trees (CFTs)
Take Away Messages

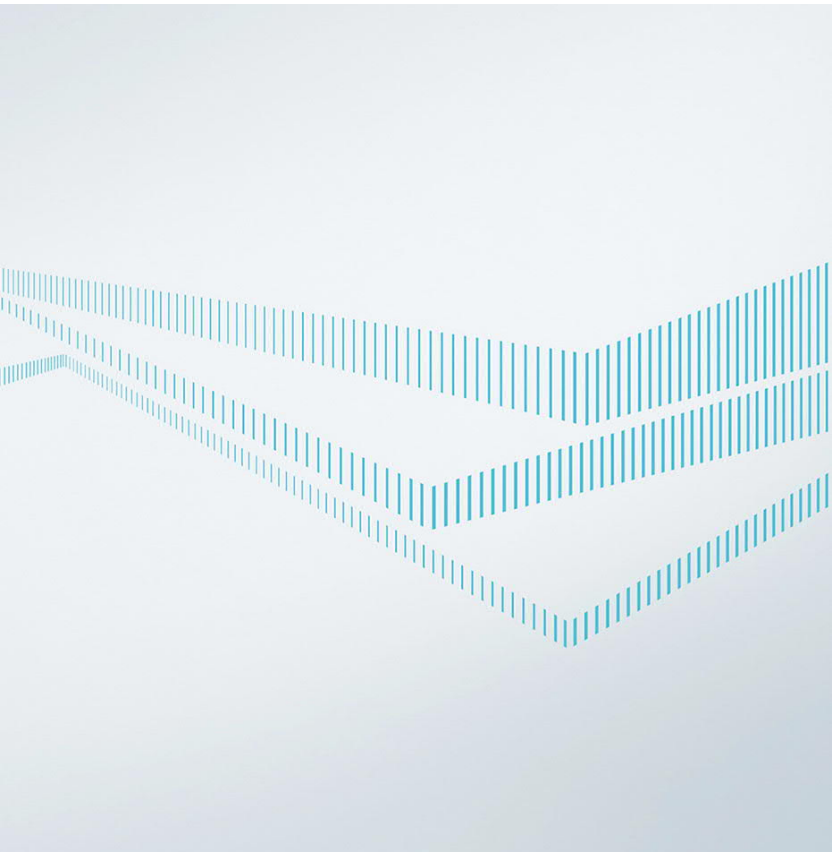
SIEMENS
Ingenuity for life

- Divide-and-conquer strategy for complex systems
- Systematic reuse of safety artifacts along with design artifacts
- Automated composition of pre-existing safety artifacts
- Support top-down / bottom-up / middle-out approaches
- Quantitative & qualitative FTA using proven-in-use methods & tools
- Integration/Synchronization with any system modeling approach (e.g. SysML)



Thank you for your attention !
Questions ?

SIEMENS
Ingenuity for life



Dr. Marc Zeller
Research Scientist
Model-based Reliability & Safety Engineering

mbrse

marc.zeller@siemens.com

Phone: +49 89 636-633980