31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

Axel Berres, German Aerospace Center
Andrius Armonas, Dassault Systemes/No Magic
Tomas Juknevičius, Dassault Systemes/No Magic

Kyle Post, Ford Motor Company
Myron Hecht, The Aerospace Corporation
Dave Banham, BlackBerry QNX

# OMG RAAML standard for model-based Fault Tree Analysis

# Agenda


What is RAAML?

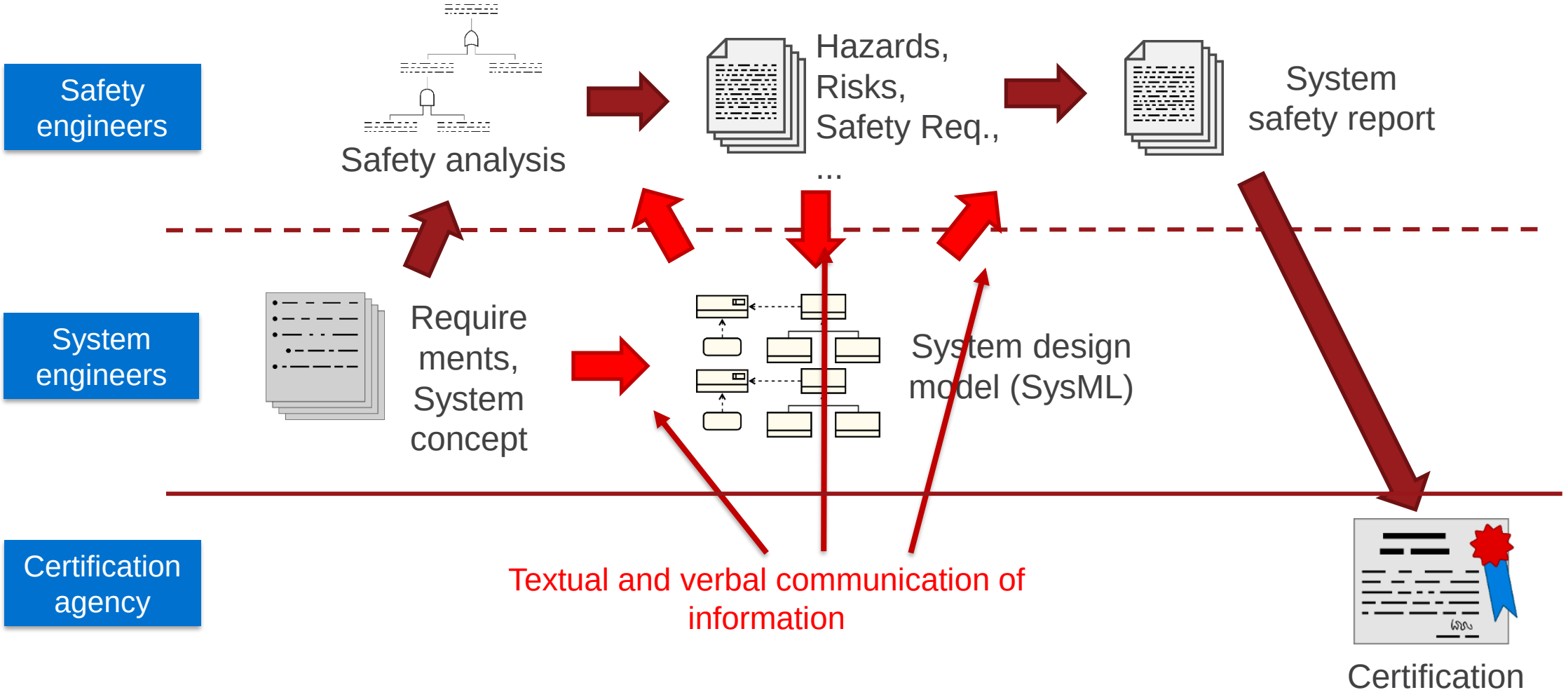
Supported methods

RAAML FTA

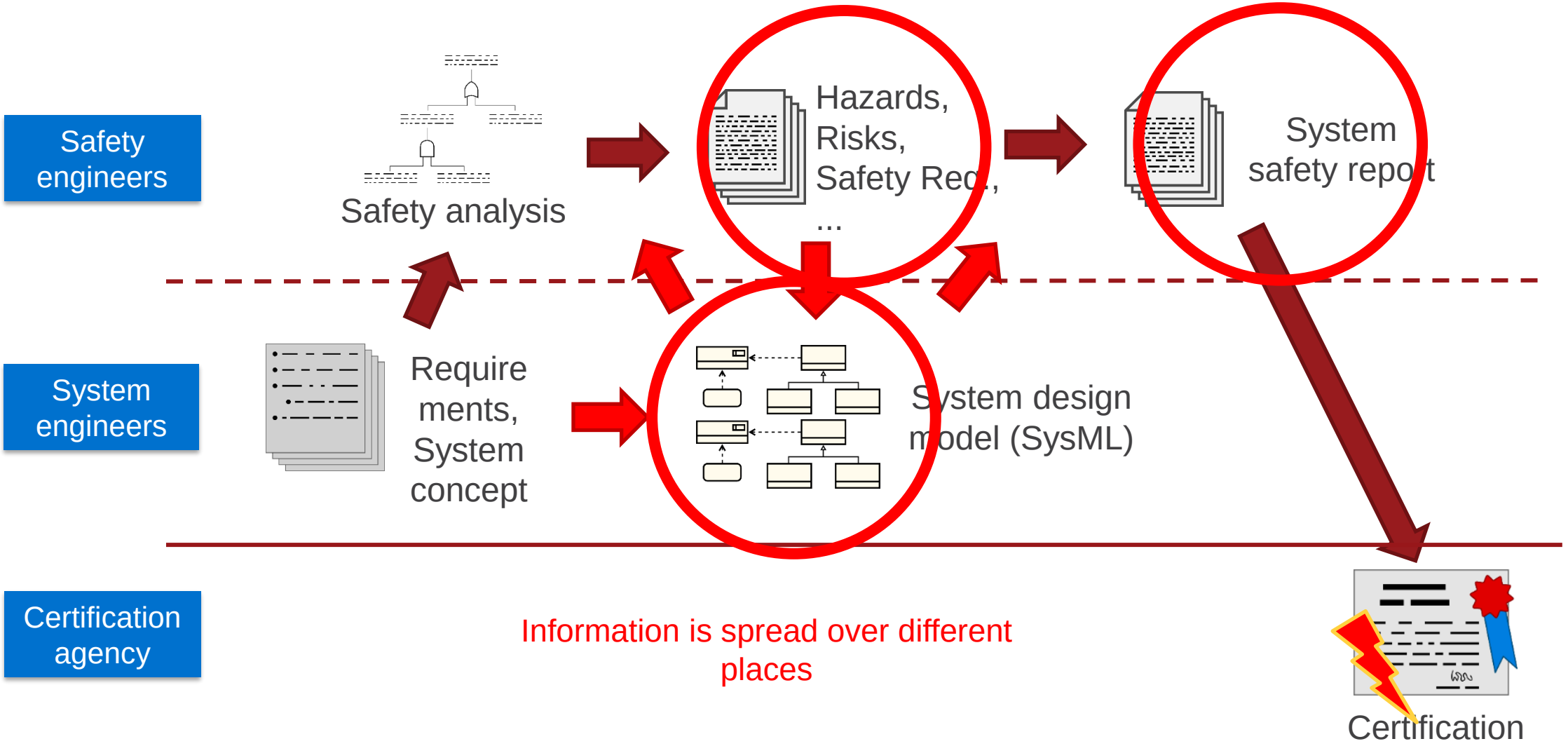
Example

MBSA with RAAML

# System safety the “classic” way



# System safety the “classic” way



# MBSA- Model-based Safety Assessment

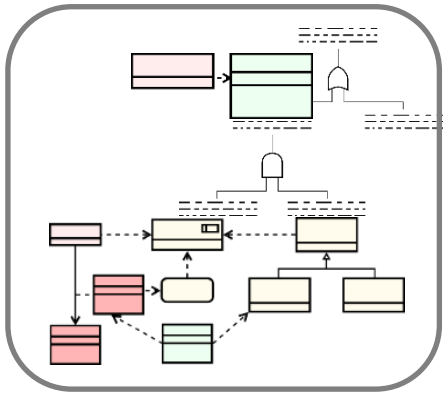
Safety engineers

System engineers

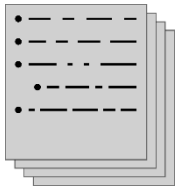
Certification agency

**Trace between safety information and system information within a single model**

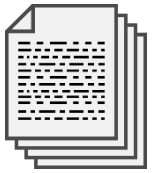
Hazards, Risks, … (RAAML)



System design model (SysML)



Require ments, System concept



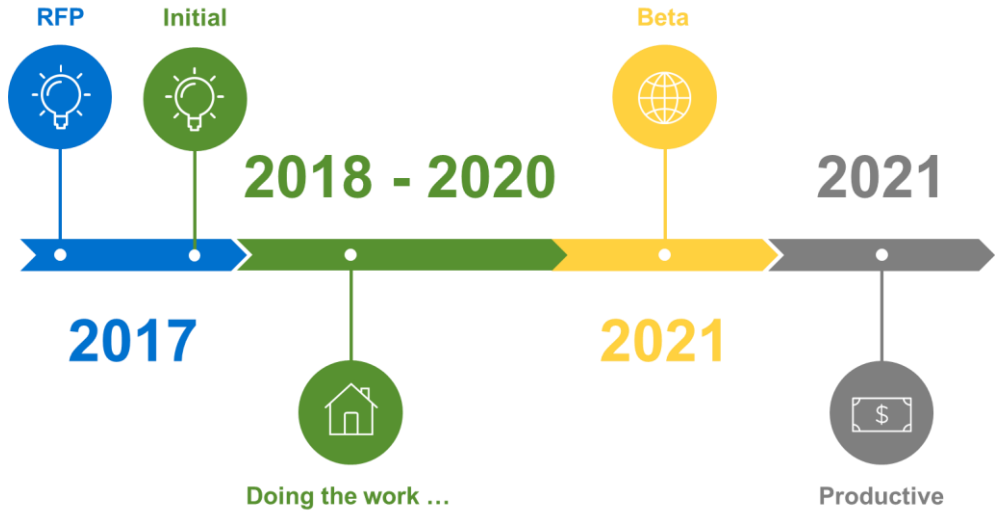
System safety report

**Automatic generation of reports for regulatory authorities**

Certification

**Safety information stored only in one place (eases maintenance)**

# OMG Safety and Reliability working group




Main contributors:

- Ford Motor Company
- Dassault Systemes / CATIA No Magic
- GfSE e.V. (the German chapter for systems engineering
- The Aerospace Corporation
- Japan's National Institute of Advanced Industrial Science and Technology
- NASA Jet Propulsion Laboratory
- France's Alternative Energies and Atomic Energy Commission (CEA)
- Plus comments from many others users

# Agenda


What is RAAML?

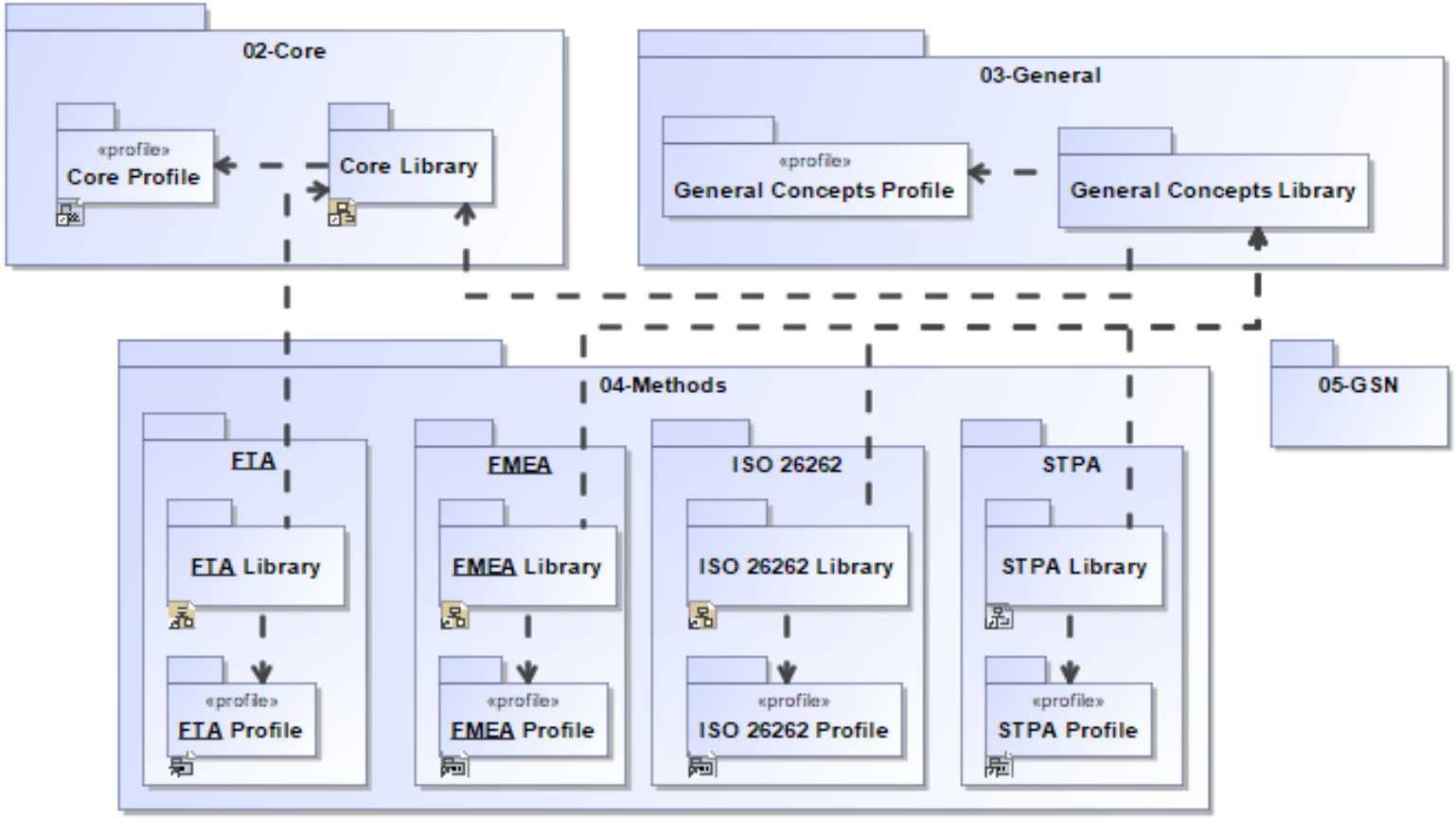
Supported methods

RAAML FTA

Example

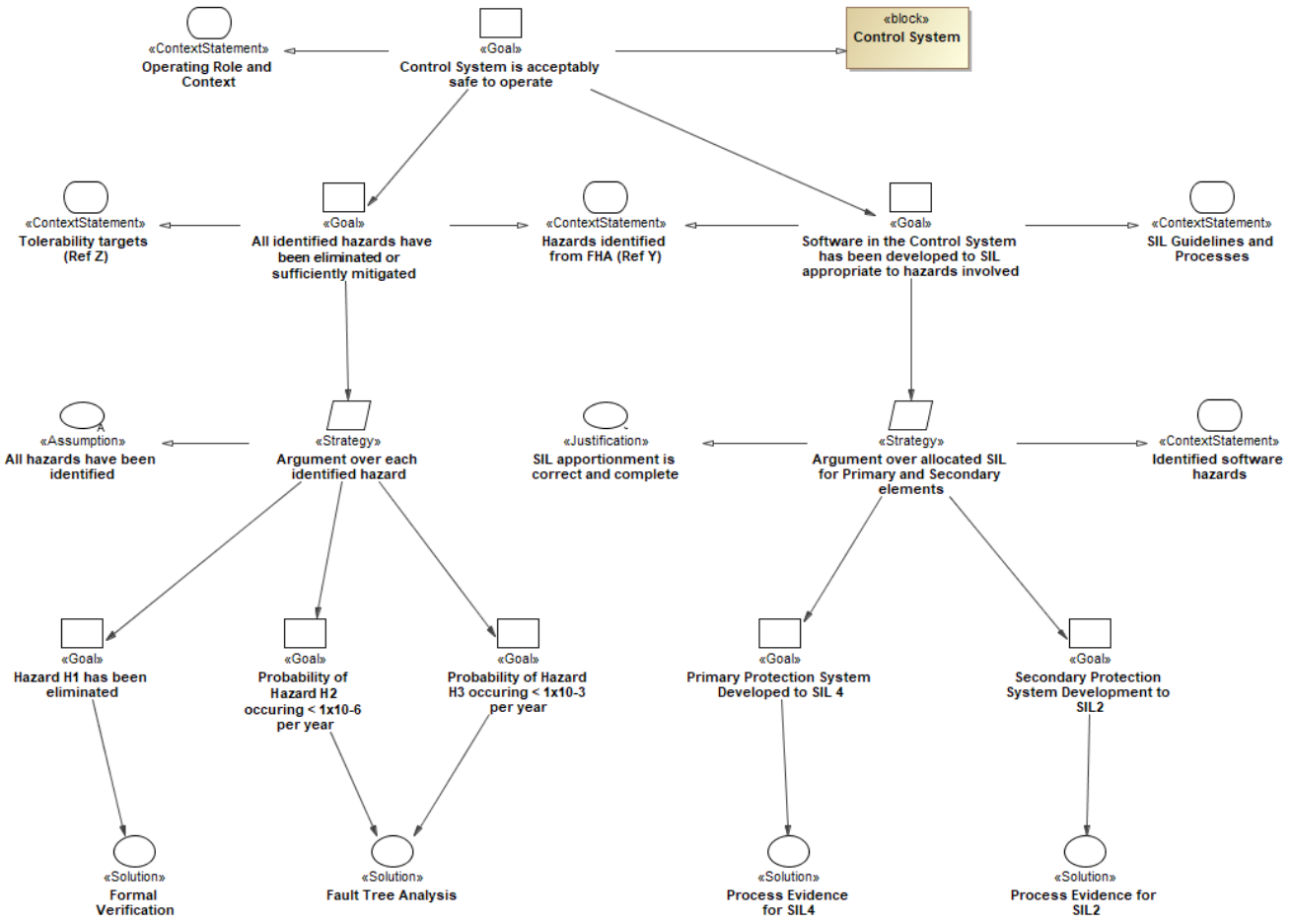
MBSA with RAAML

# RAAML‘s method support



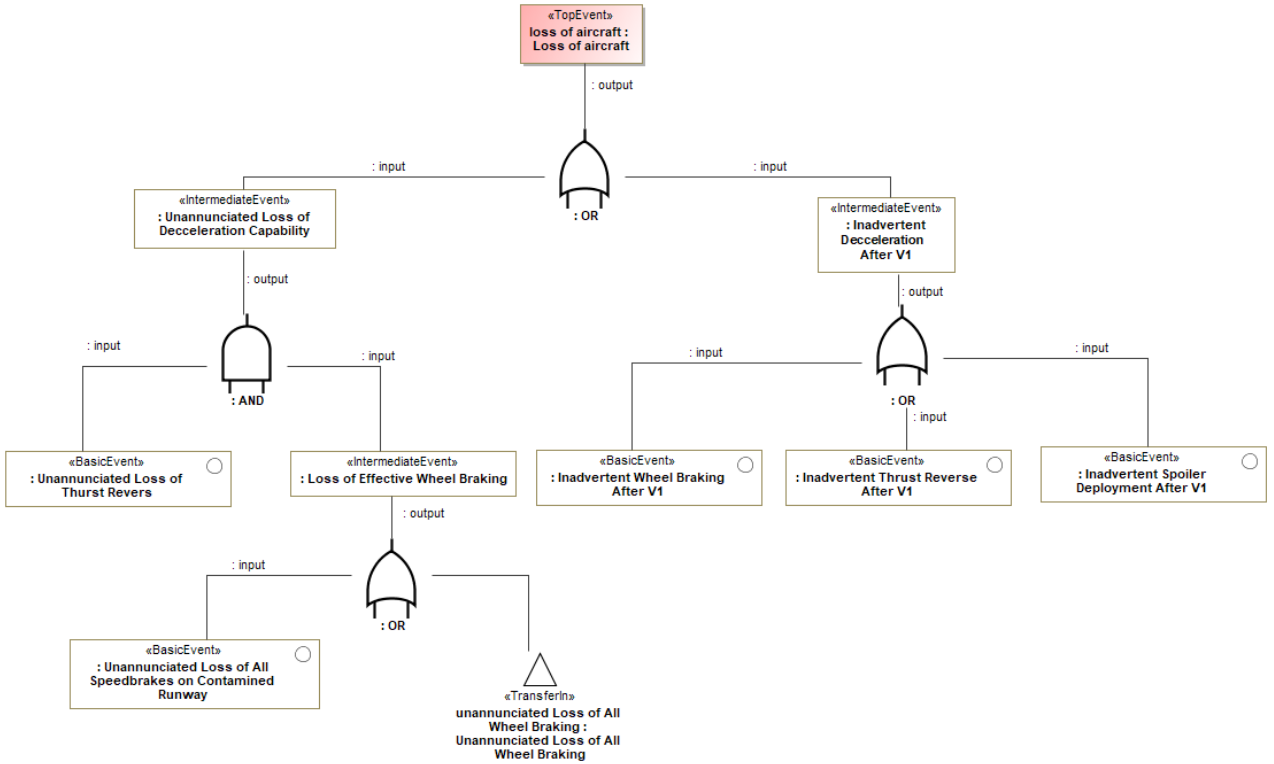
# GSN

- GSN (Goal Structured Notation) is a argumentation notation:
  - used to graphically present the proof that that a goal is fulfilled
  - can be used to argue a system's safety case.



# FTA

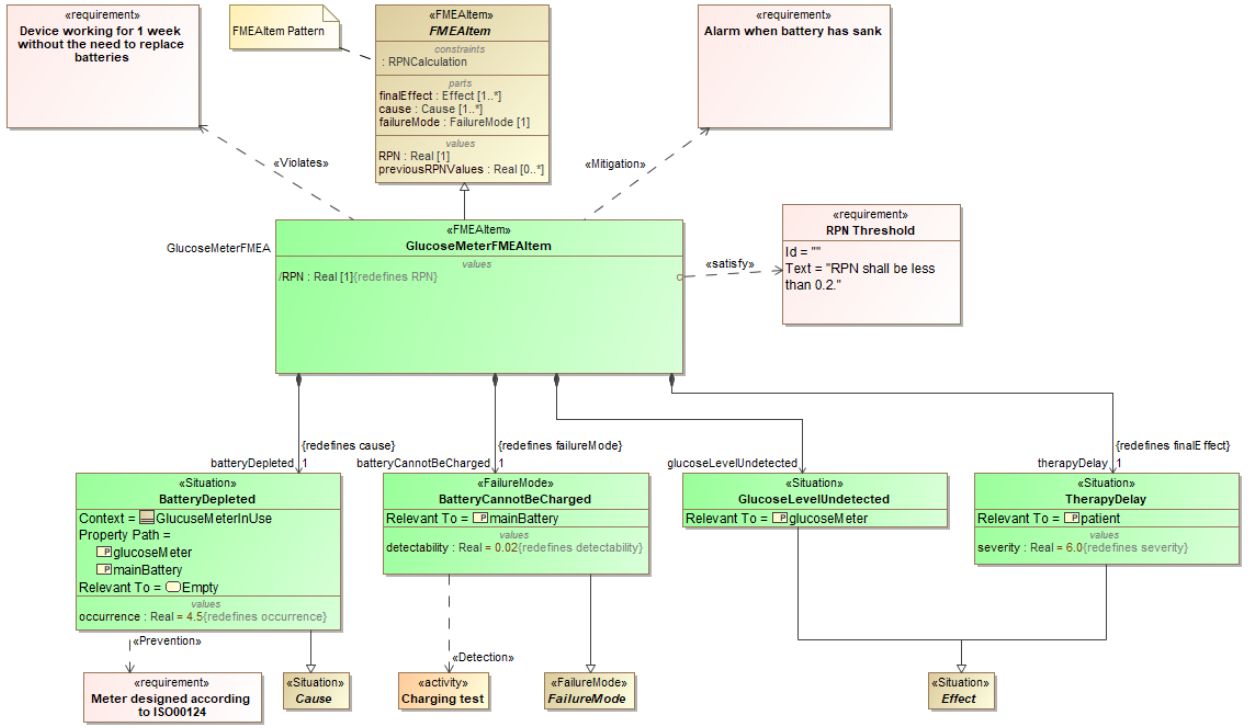
- FTA (Fault Tree Analysis) is a top-down methodology designed:
  - to identify the contributing events to an undesired event across a whole system,
  - to identify how those events combine to enable the undesired event, and
  - to identify combinations of contributing events for design of preventative actions.




IEC 60812

# FMEA

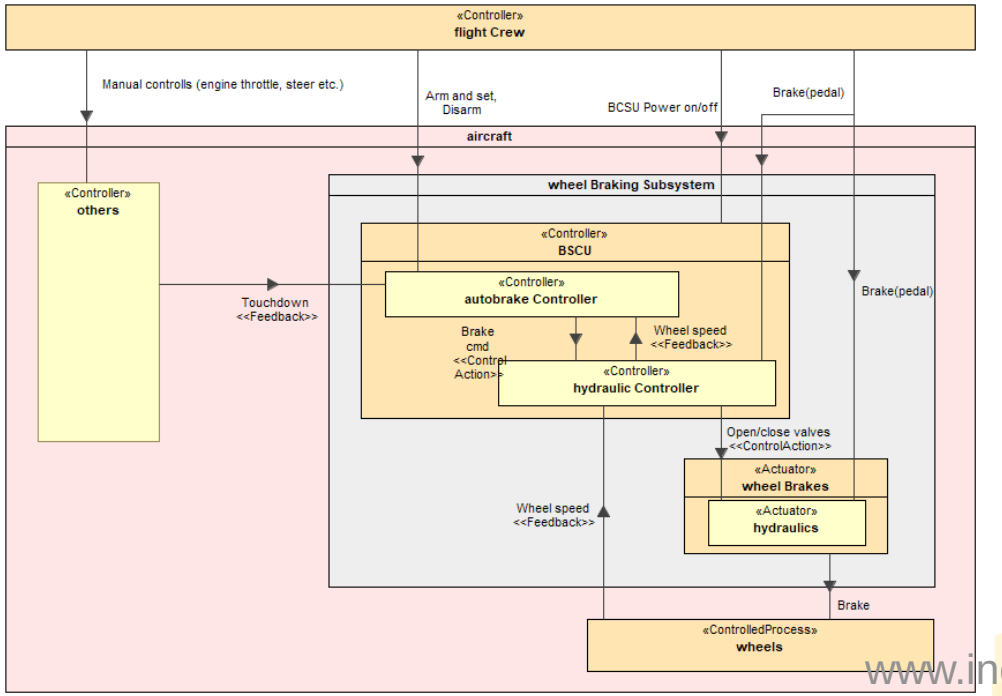
- FMEA (Failure Mode and Effect Analysis) is a bottom-up (or can performed functionally for top-down) methodology designed:
  - to identify potential failure modes for a product, part or process,
  - to assess the risk associated with those failure modes,
  - to rank the issues in terms of importance, and
  - to identify and carry out corrective actions to address the most serious concerns.

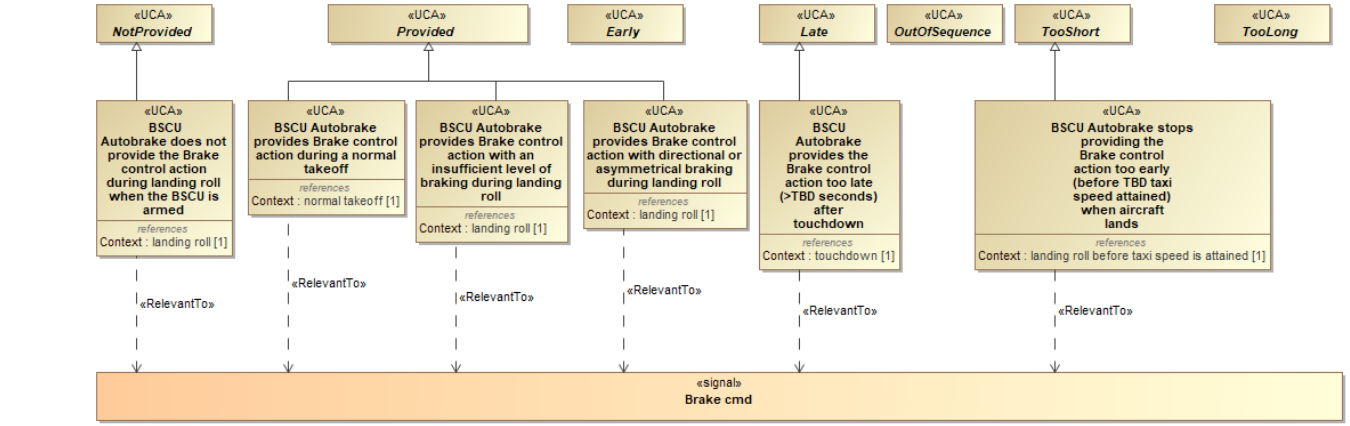



IEC 61025

# STPA

- STPA (Systems-Theoretic Process Analysis) is a systems and controls theory based exploratory methodology designed:
  - to identify system losses to avoid and the contributing hazards
  - to identify control actions which could lead to a hazard and their causes
  - to identify constraints (requirements) on the system to prevent or mitigate hazards
  - can be applied to cyber-physical systems

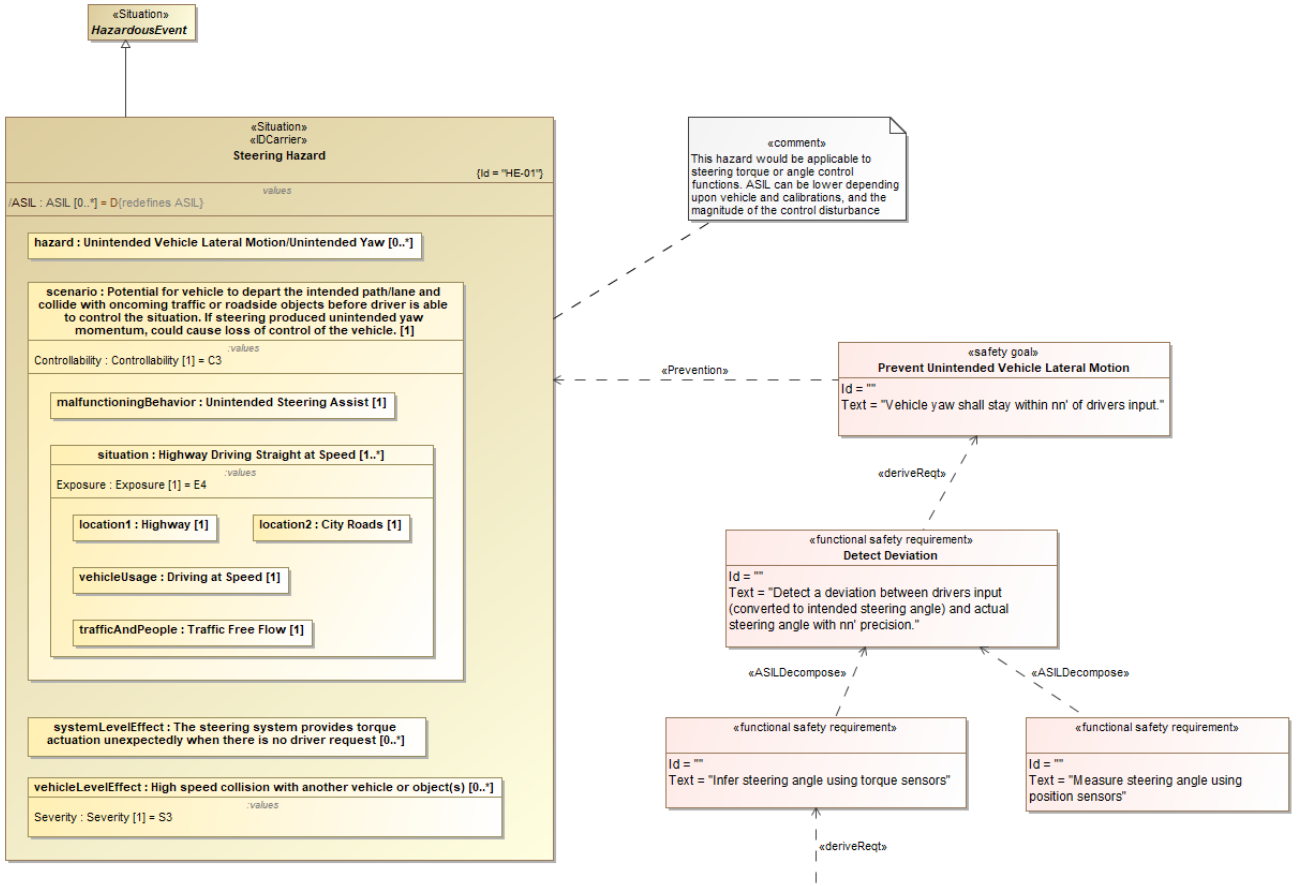



| # | Name | Provided | |
|---|---|---|---|
| 1 | Brake cmd | BSCU Autobrake provides Brake control action with an insufficient level of braking during lar<br>BSCU Autobrake provides Brake control action during a normal takeoff<br>BSCU Autobrake provides Brake control action with directional or asymmetrical braking durir | BSCU Autobrake doe |

# Example domain ISO 26262

- ISO 26262 (Functional Safety) is an automotive process specific functional safety standard:
  - Provides an automotive safety lifecycle
  - Defines a risk-based approach to determine Automotive Safety Integrity Levels



# Agenda


What is RAAML?

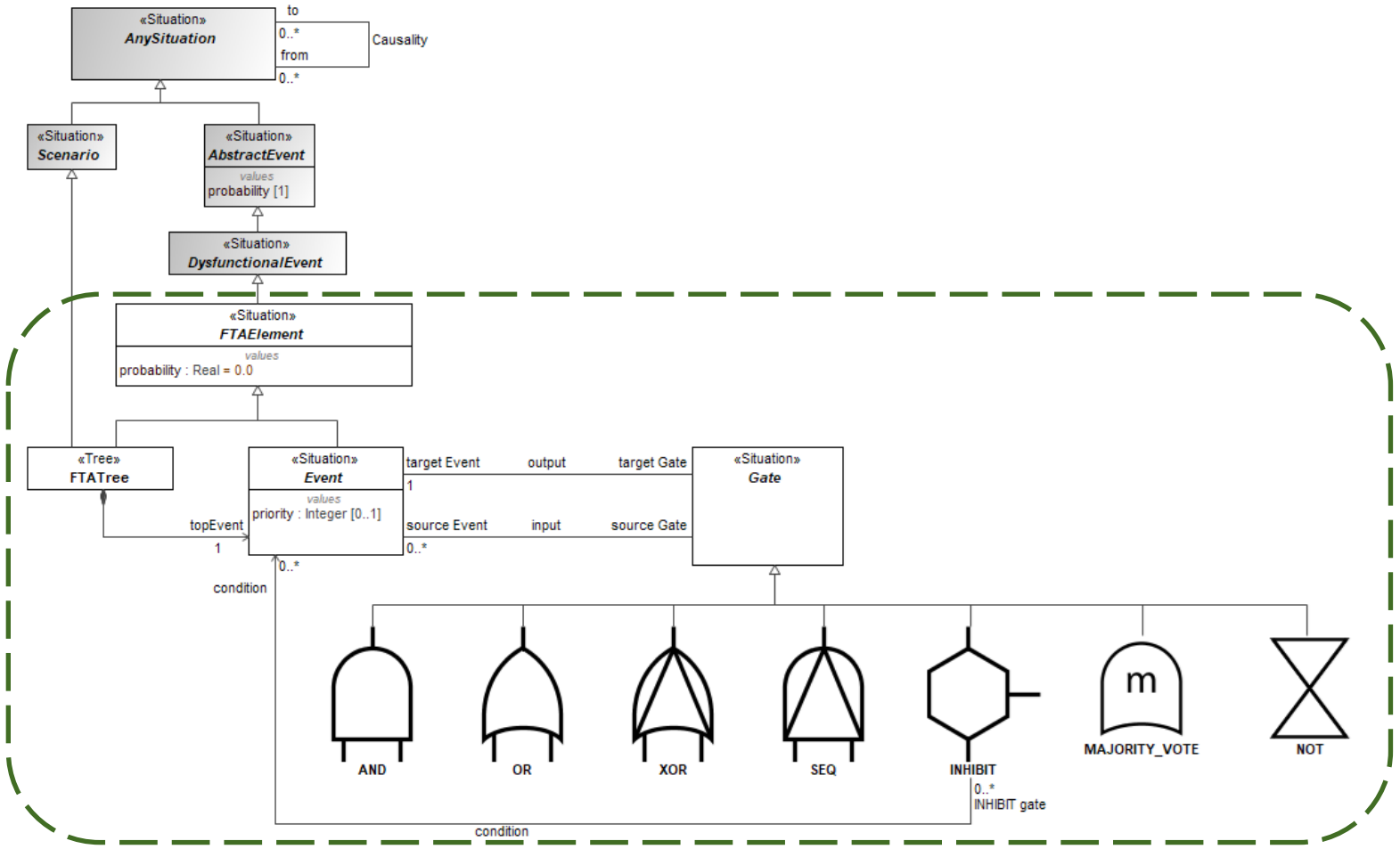
Supported methods

RAAML FTA

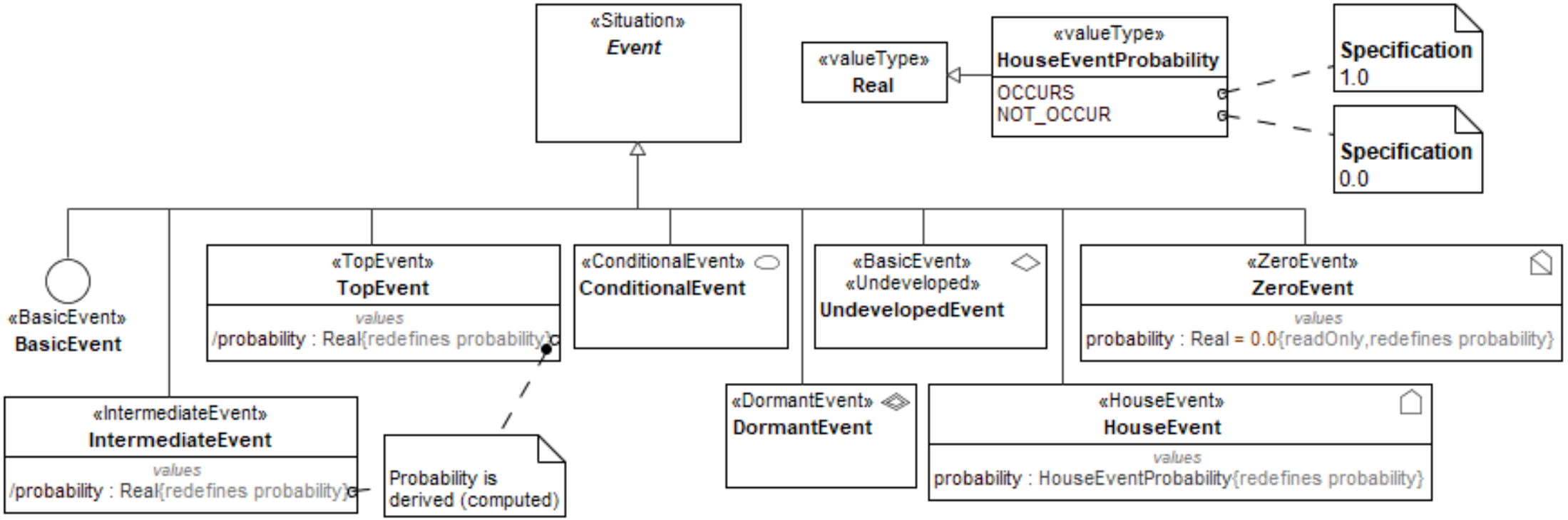
Example

MBSA with RAAML

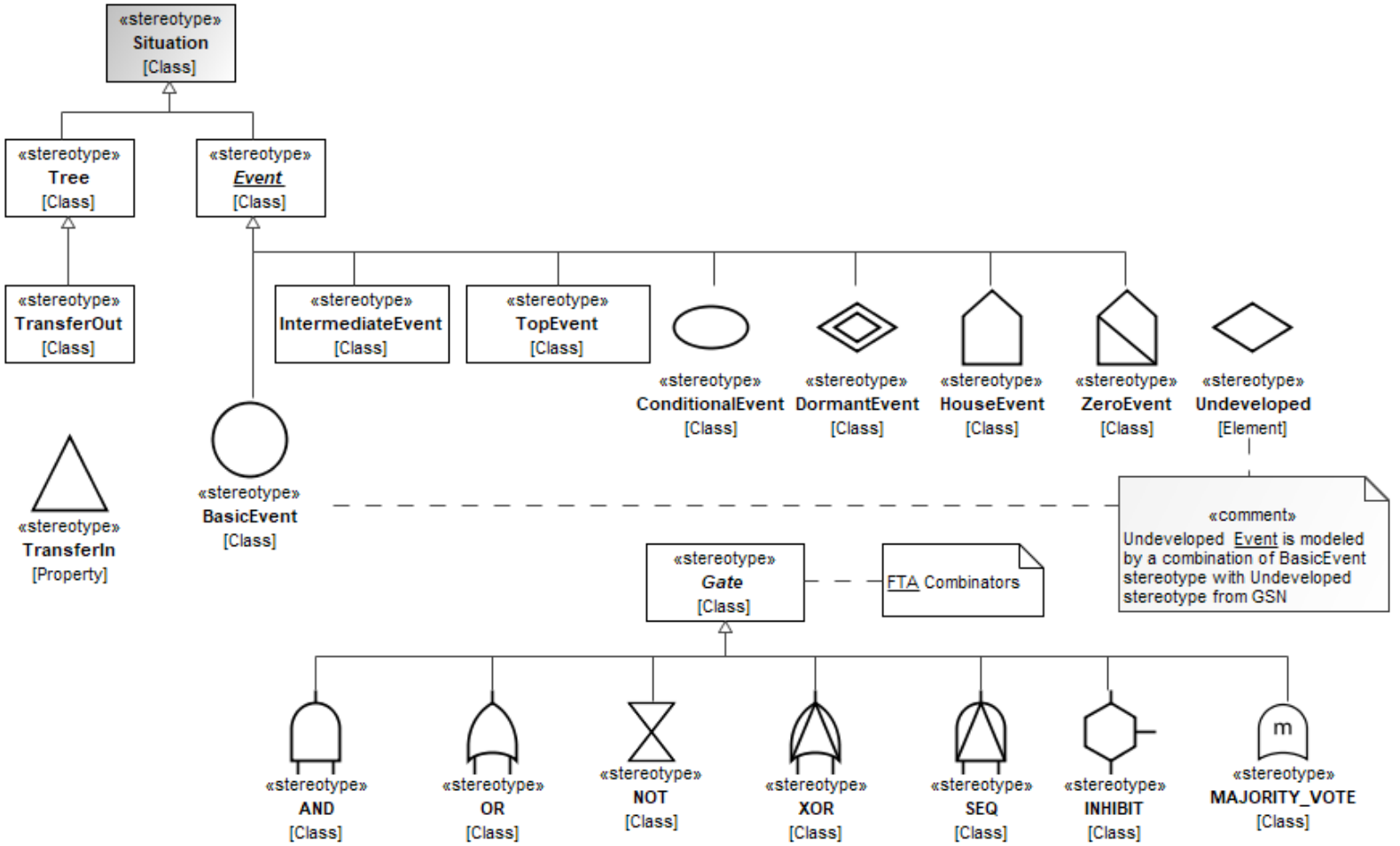
# RAAML FTA - key concepts



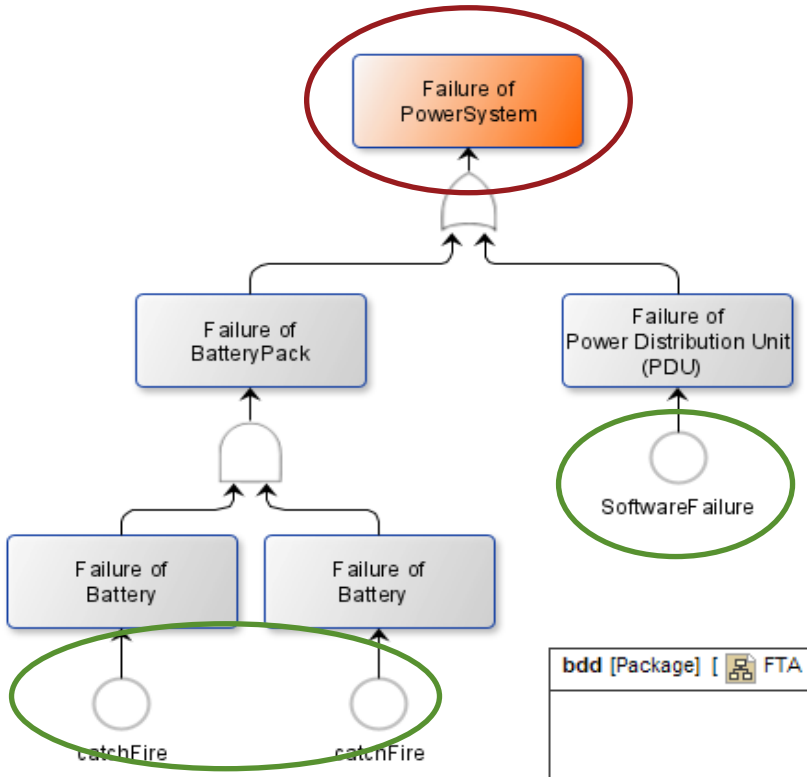
# Library of events

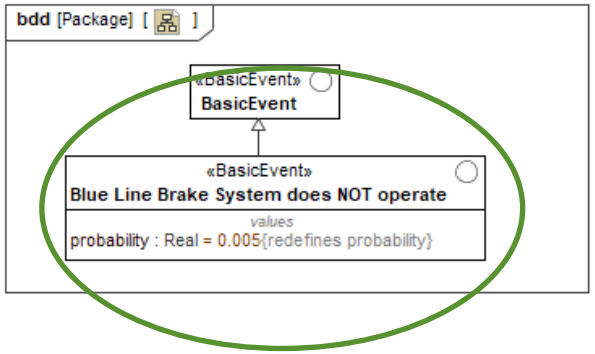


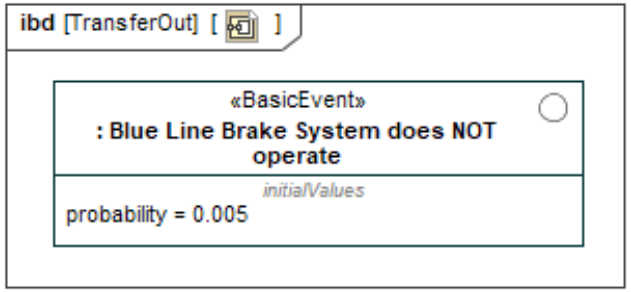
# FTA analysis profile

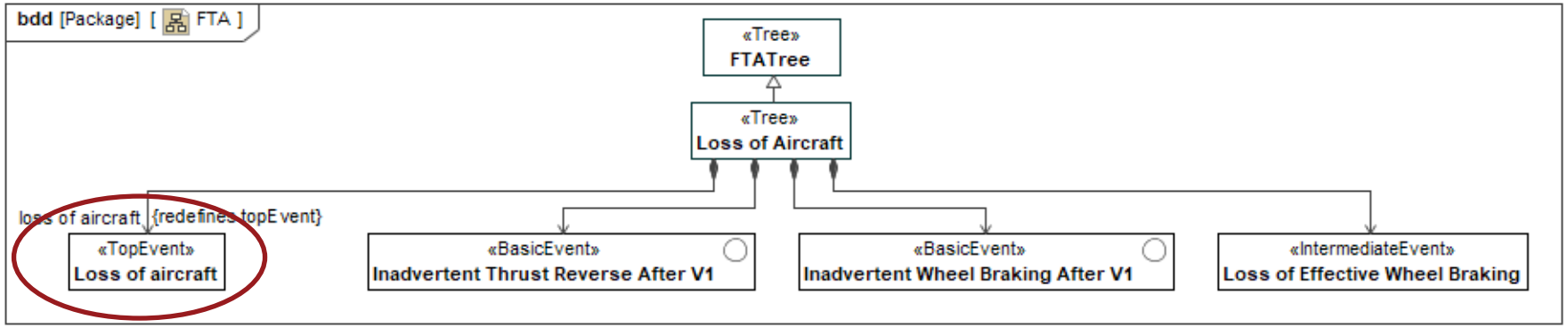


# Modeling an event

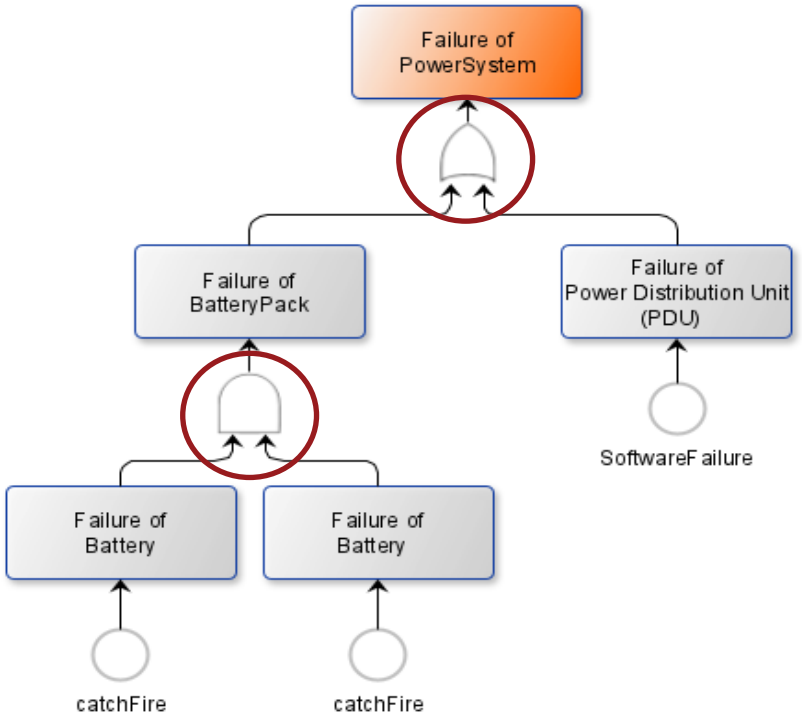


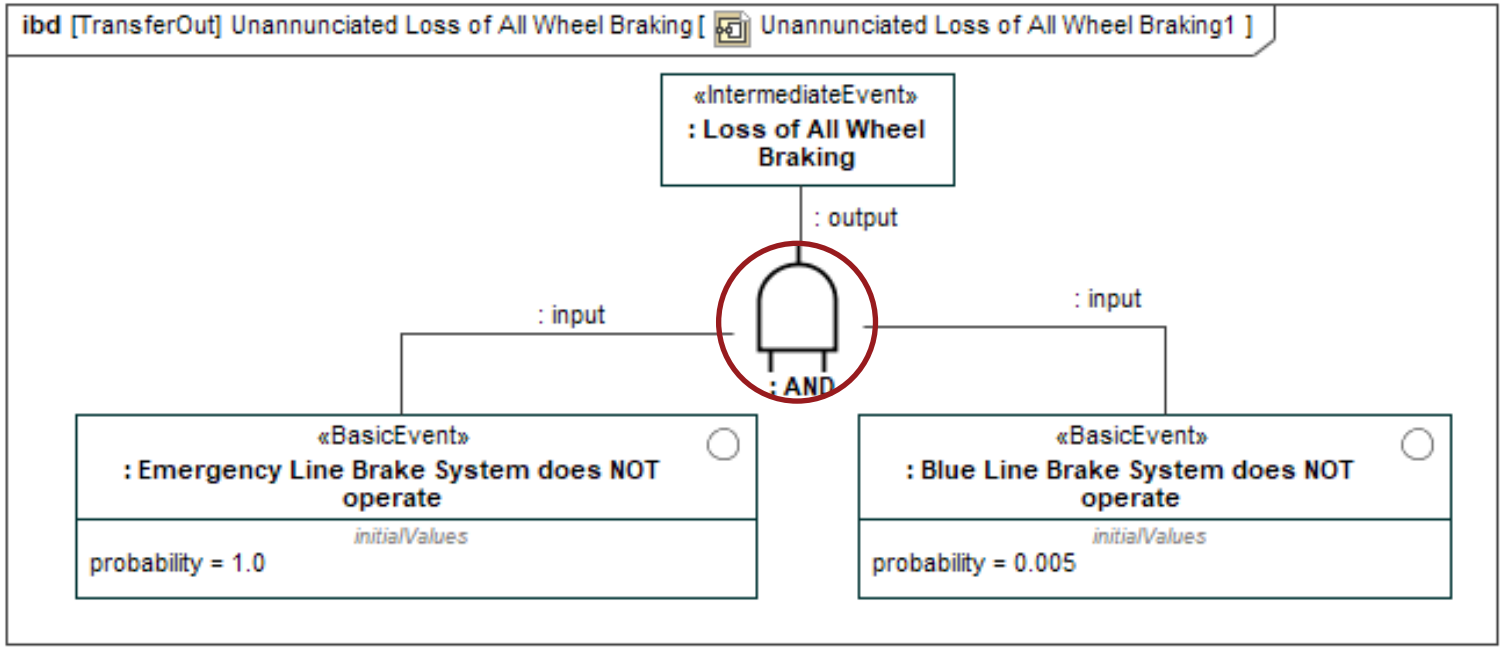



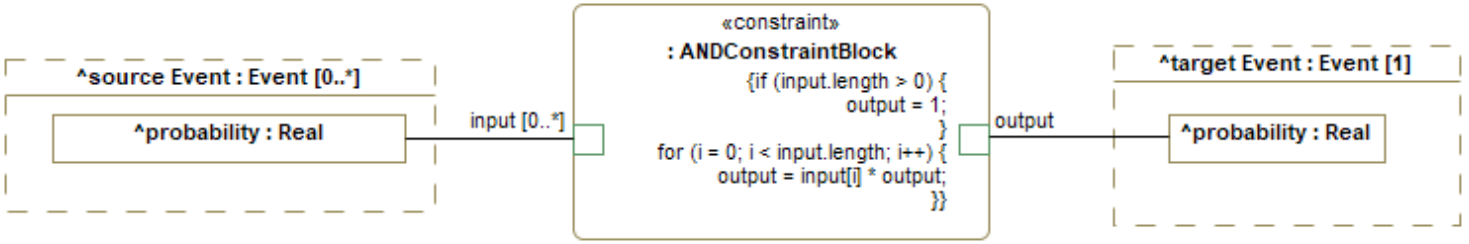



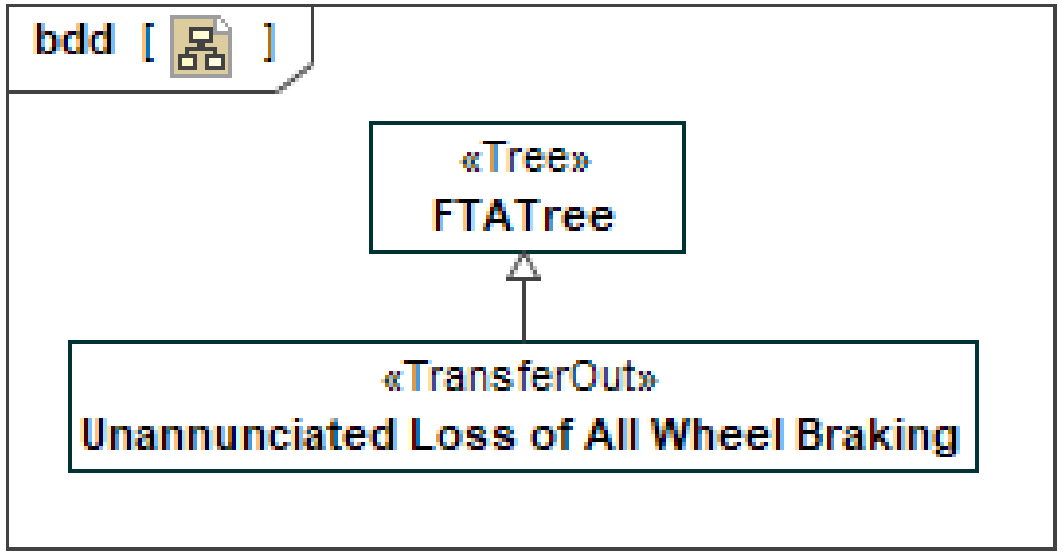
# Modeling a gate

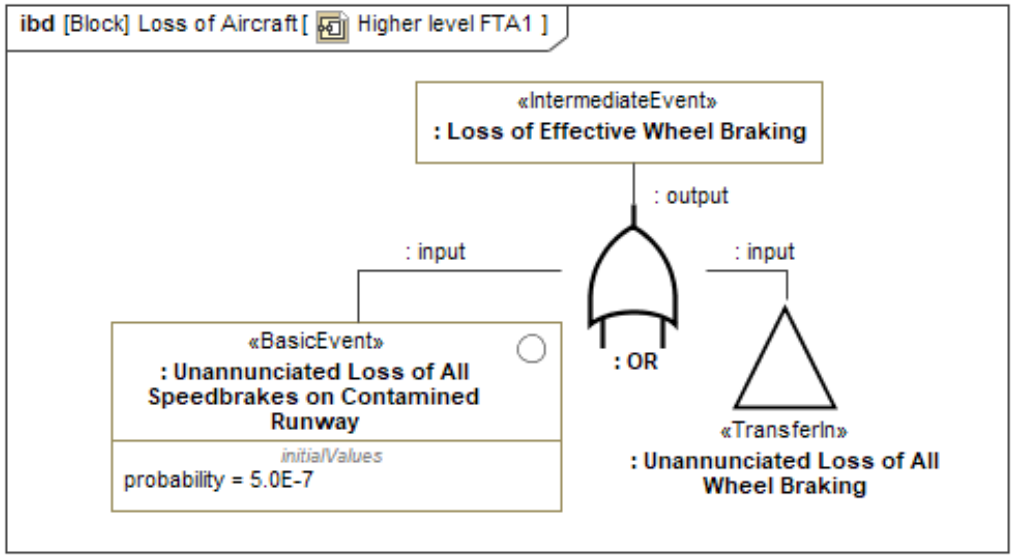


# Decomposing a fault tree



# Agenda


What is RAAML?

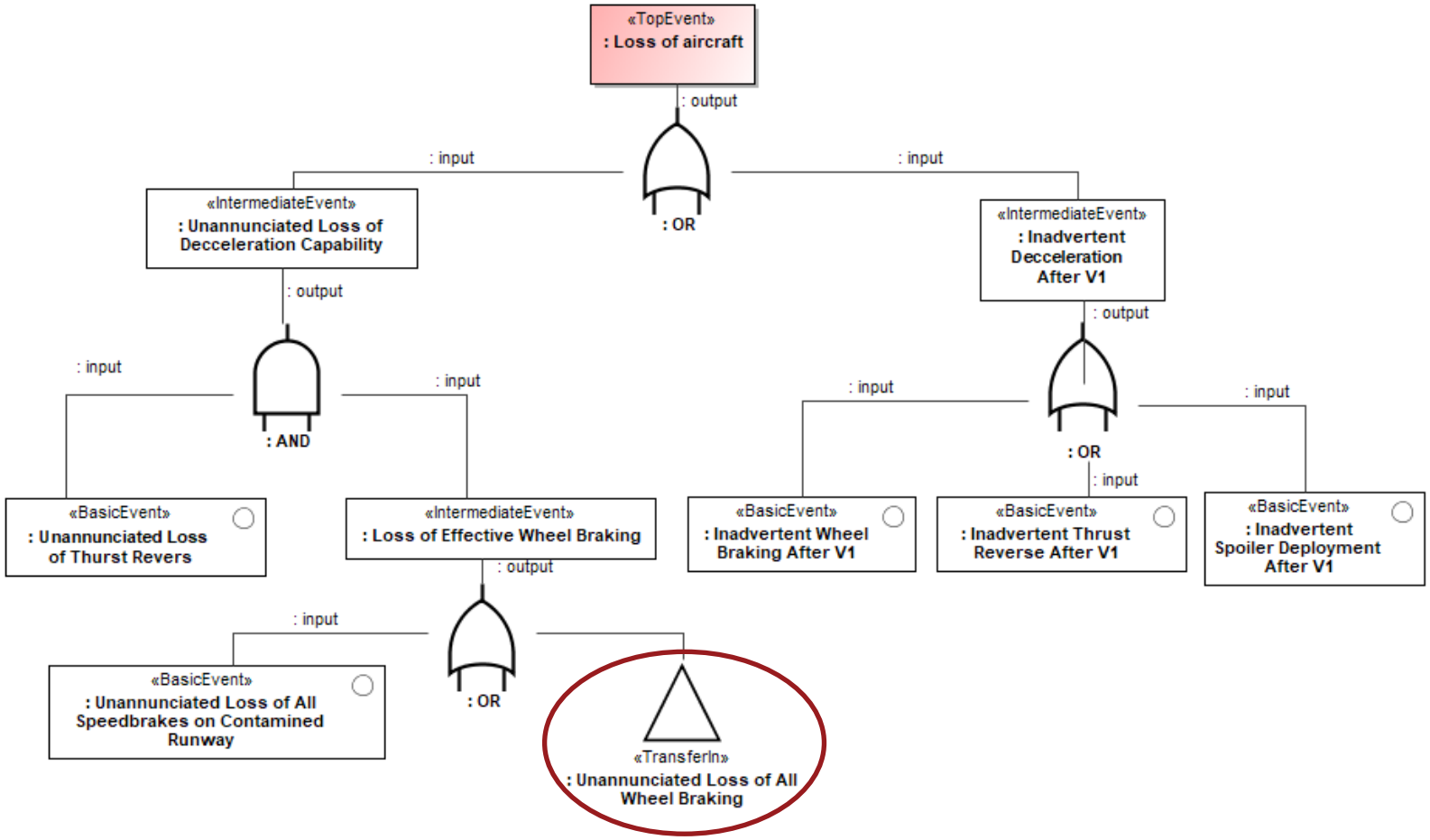
Supported methods

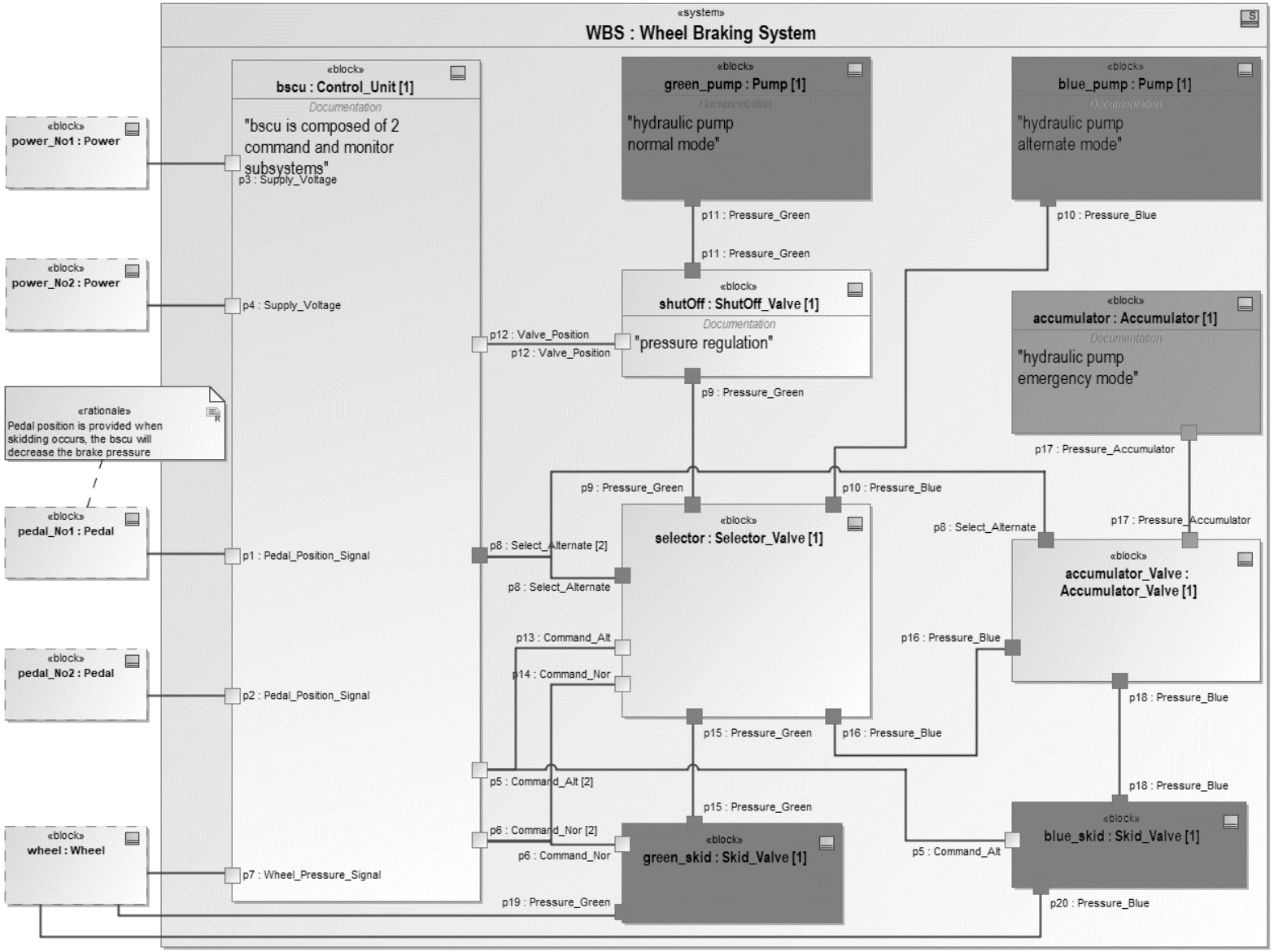
RAAML FTA

Example

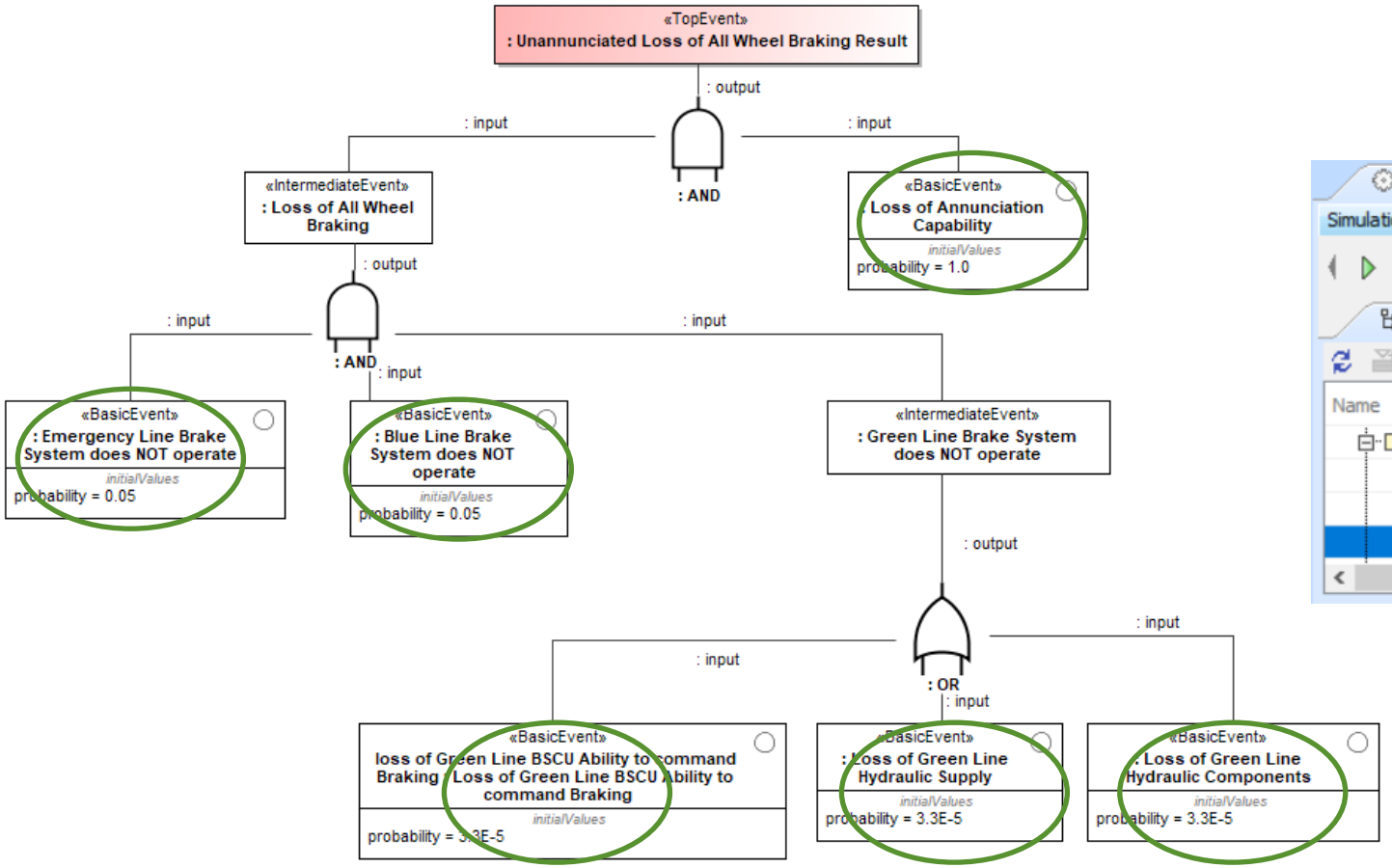
MBSA with RAAML

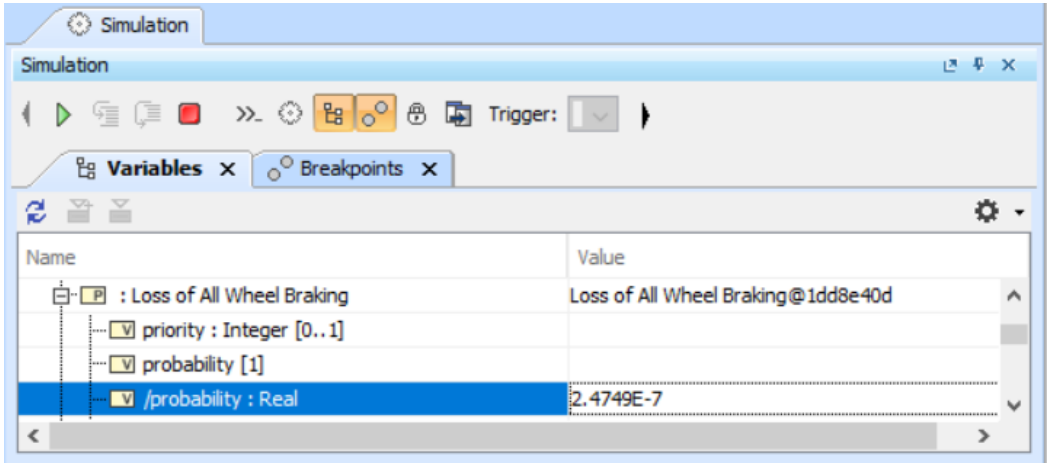
# Example - Top-Level event Loss of aircraft




«system»
WBS : Wheel Braking System
«block»
bscu : Control_Unit [1]
Documentation
"bscu is composed of 2 command and monitor subsystems"
«block»
power_No1 : Power
«block»
power_No2 : Power
«rationale»
Pedal position is provided when skidding occurs, the bscu will decrease the brake pressure
«block»
pedal_No1 : Pedal
«block»
pedal_No2 : Pedal
«block»
wheel : Wheel
«block»
green_pump : Pump [1]
Documentation
"hydraulic pump normal mode"
«block»
blue_pump : Pump [1]
Documentation
"hydraulic pump alternate mode"
«block»
shutOff : ShutOff_Valve [1]
Documentation
"pressure regulation"
«block»
accumulator : Accumulator [1]
Documentation
"hydraulic pump emergency mode"
«block»
selector : Selector_Valve [1]
«block»
accumulator_Valve : Accumulator_Valve [1]
«block»
green_skid : Skid_Valve [1]
«block»
blue_skid : Skid_Valve [1]
p3 : Supply_Voltage
p4 : Supply_Voltage
p1 : Pedal_Position_Signal
p2 : Pedal_Position_Signal
p7 : Wheel_Pressure_Signal
p11 : Pressure_Green
p10 : Pressure_Blue
p12 : Valve_Position
p9 : Pressure_Green
p17 : Pressure_Accumulator
p8 : Select_Alternate [2]
p8 : Select_Alternate
p13 : Command_Alt
p14 : Command_Nor
p16 : Pressure_Blue
p18 : Pressure_Blue
p15 : Pressure_Green
p5 : Command_Alt [2]
p6 : Command_Nor [2]
p6 : Command_Nor
p5 : Command_Alt
p19 : Pressure_Green
p20 : Pressure_Blue

# Fault tree with top-level of WBS



# Agenda


What is RAAML?

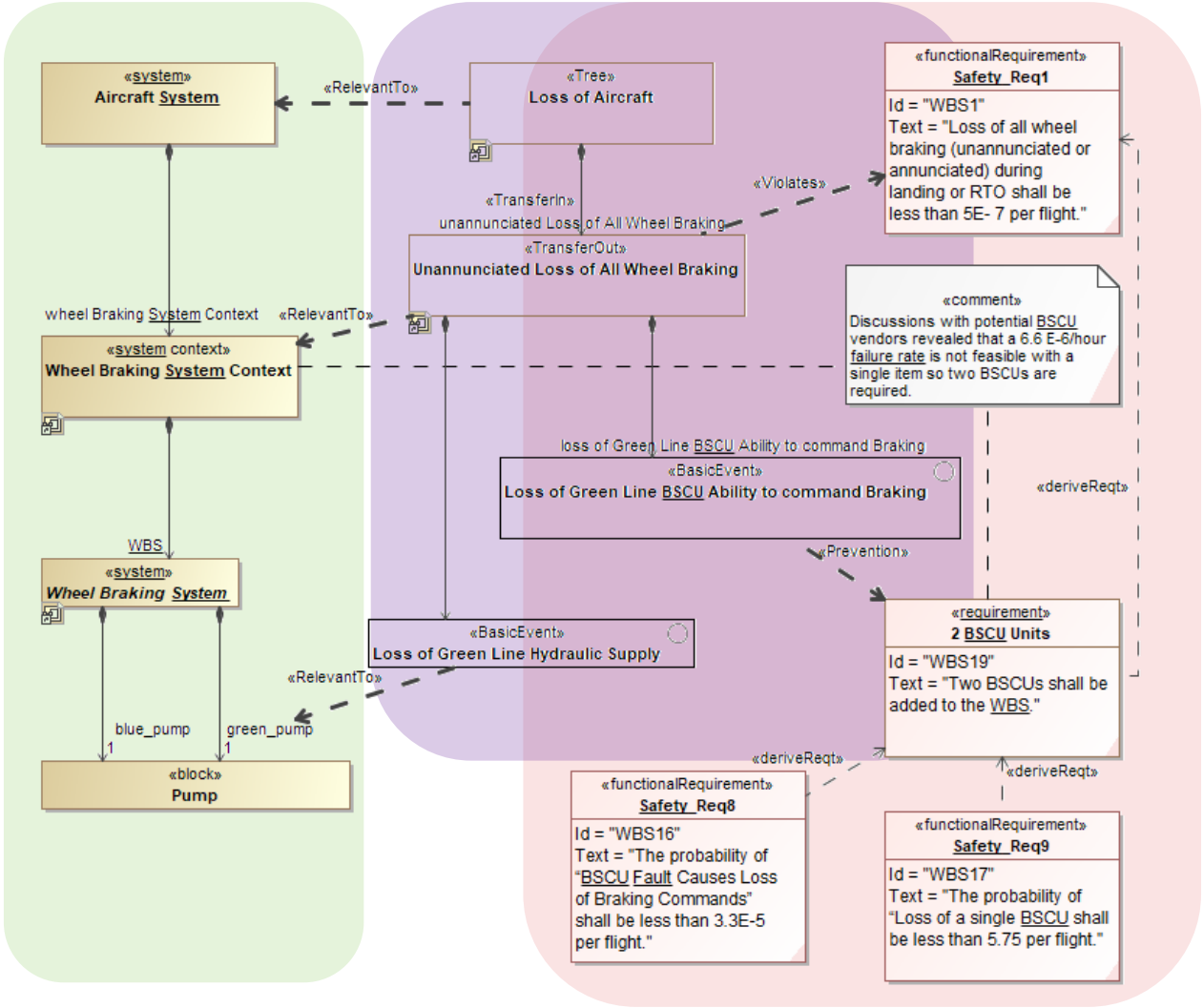
Supported methods

RAAML FTA

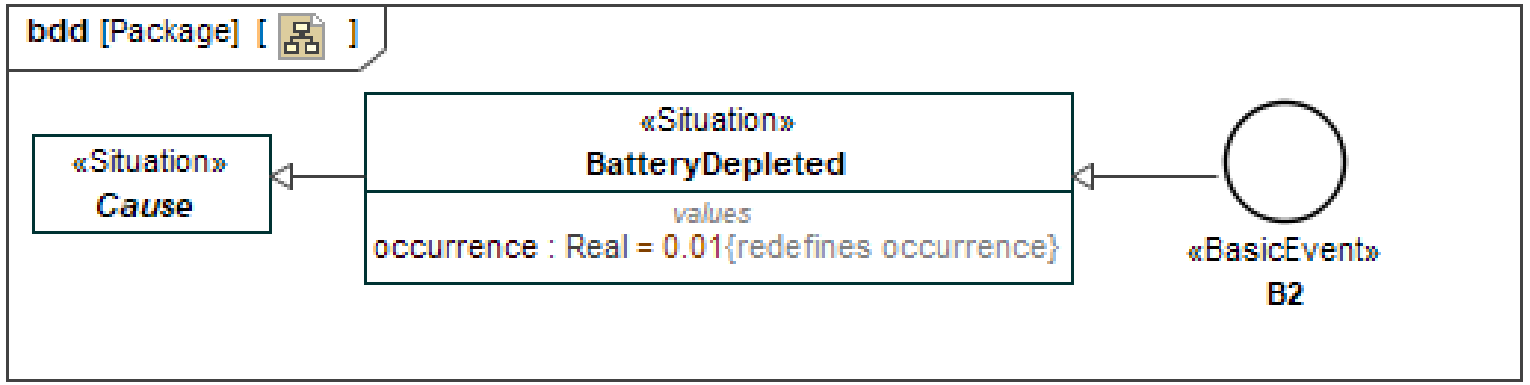
Example

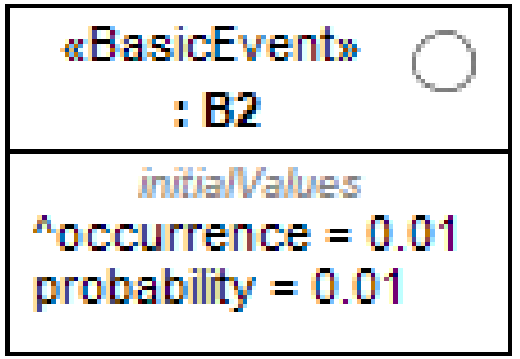
MBSA with RAAML

# MBSA - FTA


«system»
Aircraft System
«RelevantTo»
«Tree»
Loss of Aircraft
«functionalRequirement»
Safety_Req1
Id = "WBS1"
Text = "Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be less than 5E- 7 per flight."
«Violates»
«TransferIn»
unannunciated Loss of All Wheel Braking
«TransferOut»
Unannunciated Loss of All Wheel Braking
wheel Braking System Context
«RelevantTo»
«system context»
Wheel Braking System Context
«comment»
Discussions with potential BSCU vendors revealed that a 6.6 E-6/hour failure rate is not feasible with a single item so two BSCUs are required.
loss of Green Line BSCU Ability to command Braking
«BasicEvent»
Loss of Green Line BSCU Ability to command Braking
«deriveReqt»
WBS
«system»
Wheel Braking System
«Prevention»
«BasicEvent»
Loss of Green Line Hydraulic Supply
«requirement»
2 BSCU Units
Id = "WBS19"
Text = "Two BSCUs shall be added to the WBS."
«RelevantTo»
blue_pump
1
green_pump
1
«block»
Pump
«deriveReqt»
«deriveReqt»
«functionalRequirement»
Safety_Req8
Id = "WBS16"
Text = "The probability of "BSCU Fault Causes Loss of Braking Commands" shall be less than 3.3E-5 per flight."
«functionalRequirement»
Safety_Req9
Id = "WBS17"
Text = "The probability of "Loss of a single BSCU shall be less than 5.75 per flight."

# Combining FMEA and FTA



31st Annual INCOSE
international symposium

virtual event

July 17 - 22, 2021

www.incose.org/symp2021