Multi-Concern Dependability-centered Assurance for Space Systems via ConcertoFLA

Barbara Gallina, Zulqarnain Haider, Anna Carlsson, Silvia Mazzini, Stefano Puri

{barbara.gallina, zulqarnain.haider}@mdh.se
anna.carlsson@ohb-Sweden.se
{stefano.puri, silvia.mazzini}@intecs.it

This work is supported by the EU and VINNOVA via the ECSEL project **AMASS**
https://www.amass-ecsel.eu/

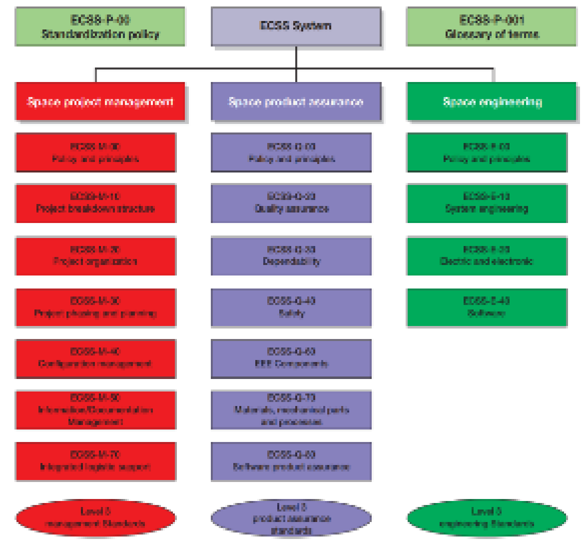
Context and motivation

Space Systems

Compliance

Dependability, Safety
and Security Requirements…

ECSS Standards



Tool Supported Dependability-centered
Multi-Concern Assurance

- Co-analysis
- Management of trade-offs
- Complexity Reduction
- Compliance to ECSS

Talk outline

- Background
  - European Cooperation For Space Standardization (ECSS) Standards
  - Tool Supported CHESS Methodology
    - ConcertoFLA
- Multi-Concern Dependability-centered Assurance Approach
- Attitude Control System Example
  - Modeling of ACS and dependability
  - Failure Logic Analysis (FLA)
  - FLA results and interpretation for dependability attributes
- Conclusion

ECSS Standards

Dependability ECSS-Q-ST-30C

6.4.1 General

a. Dependability analyses shall be conducted on all levels of the space system and be performed in respect of the level that is being assessed i.e. System, Subsystem and Equipment levels.

Safety ECSS-Q-ST-40C

7.5.2 Hazard analysis

7.5.4.5 Fault tree analysis

a. The fault tree analysis shall be used to establish the systematic link between the system-level hazard and the contributing hazardous events and subsystem, equipment or piece part failure.

Software Product Assurance ECSS-Q-ST-80C

6.2.2.2

a. The supplier shall perform a software dependability and safety analysis of the software products, in accordance with the requirements of ECSS-Q-ST-30 and ECSS-Q-ST-40 and using the results of system-level safety and dependability analyses, in order to determine the criticality of the individual software components.

Secure Software Engineering Standard ESSB-ST-E-008

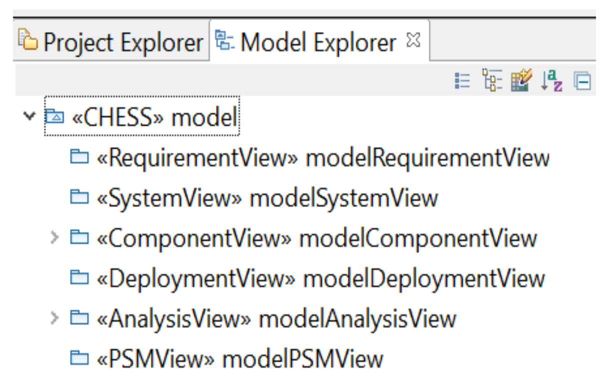
7.2.2.2

b. **The supplier shall perform a cyber-security risk assessment of the software products in order to determine the security sensitivity of the individual software components.**

Tool Supported CHESS Methodology

- CHESS is an open-source methodology and toolset available from Eclipse/Polarsys
  - Model Driven Methodology
  - Component Based Approach
  - Seperation of Concerns
  - Dependability Profile

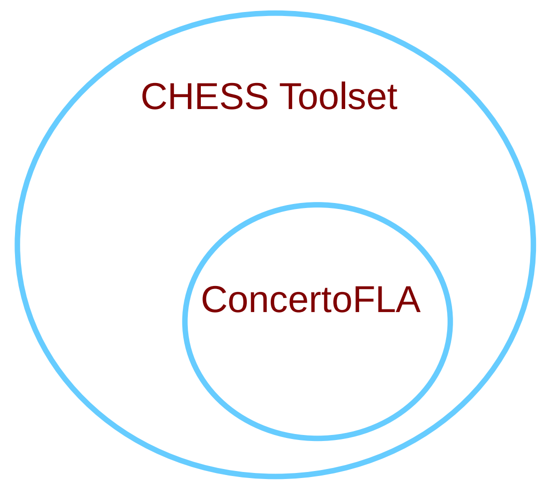
CHESS



https://www.polarsys.org/projects/polarsys.chess

ConcertoFLA

- ConcertoFLA is a failure logic analysis tool to qualitatively evaluate failure behavior of a component based system, given the failure behavior of individual components



Overview of ConcertoFLA approach

- Failure Propagation Transform Calculus (FPTC)

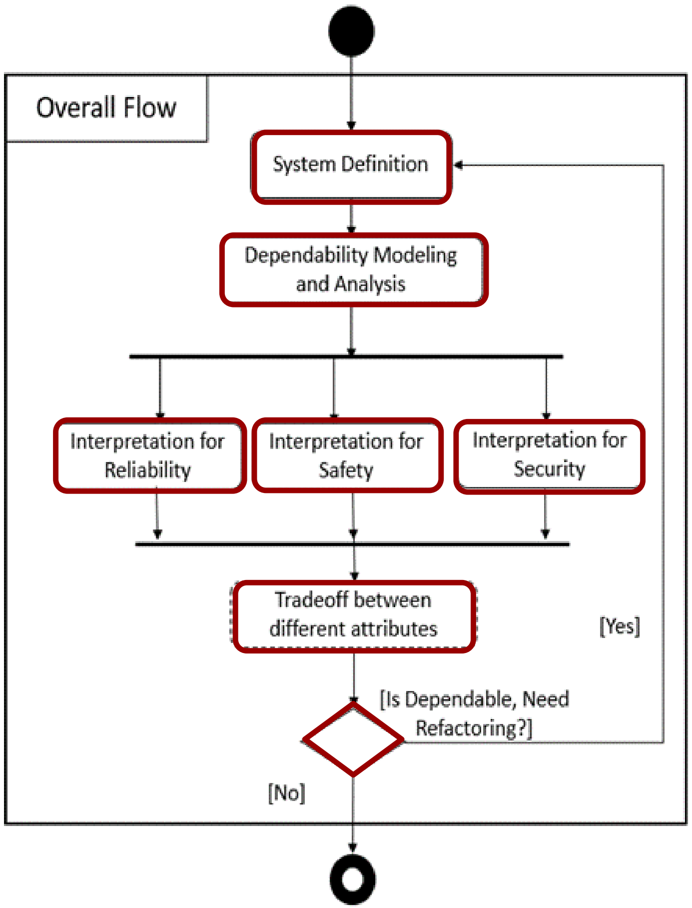
Input ports {failures} → FPTC Expressions → output ports {failures}

Inputport.failuretype -> Outputport.failuretype

- Failure types
  - Value [Coarse, Subtle]
  - Timing [Early, Late]
  - Provision [Omission, Commission]
- Component behavior
  - Sink
  - Source
  - Transform
  - Propagate

Multi-Concern dependability centered assurance

- Qualitative evaluation of system dependability
  - Is the system acceptably safe, secure, reliable? etc.
- Design decisions
  - Introduce safety, security and reliability measures accordingly
  - System designer evaluates the tradeoff and re-design



Attitude Control System (ACS)

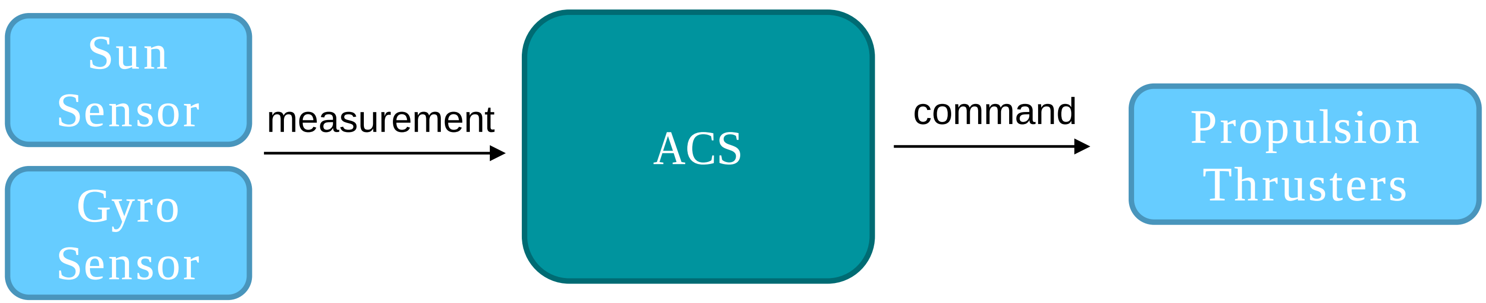
- ACS controls the orientation of the satellite relative to a reference object.

- Attitude Control Functions
  - Process units data
  - Estimate the state
  - Compute the control torque to be applied on satellite for maintaining desired attitude

ACS Operational modes

- Different operational modes
  - Depending upon missions
  - Involves different units – sensors and actuators

- Sun Acquisition and Survival mode (SASM)



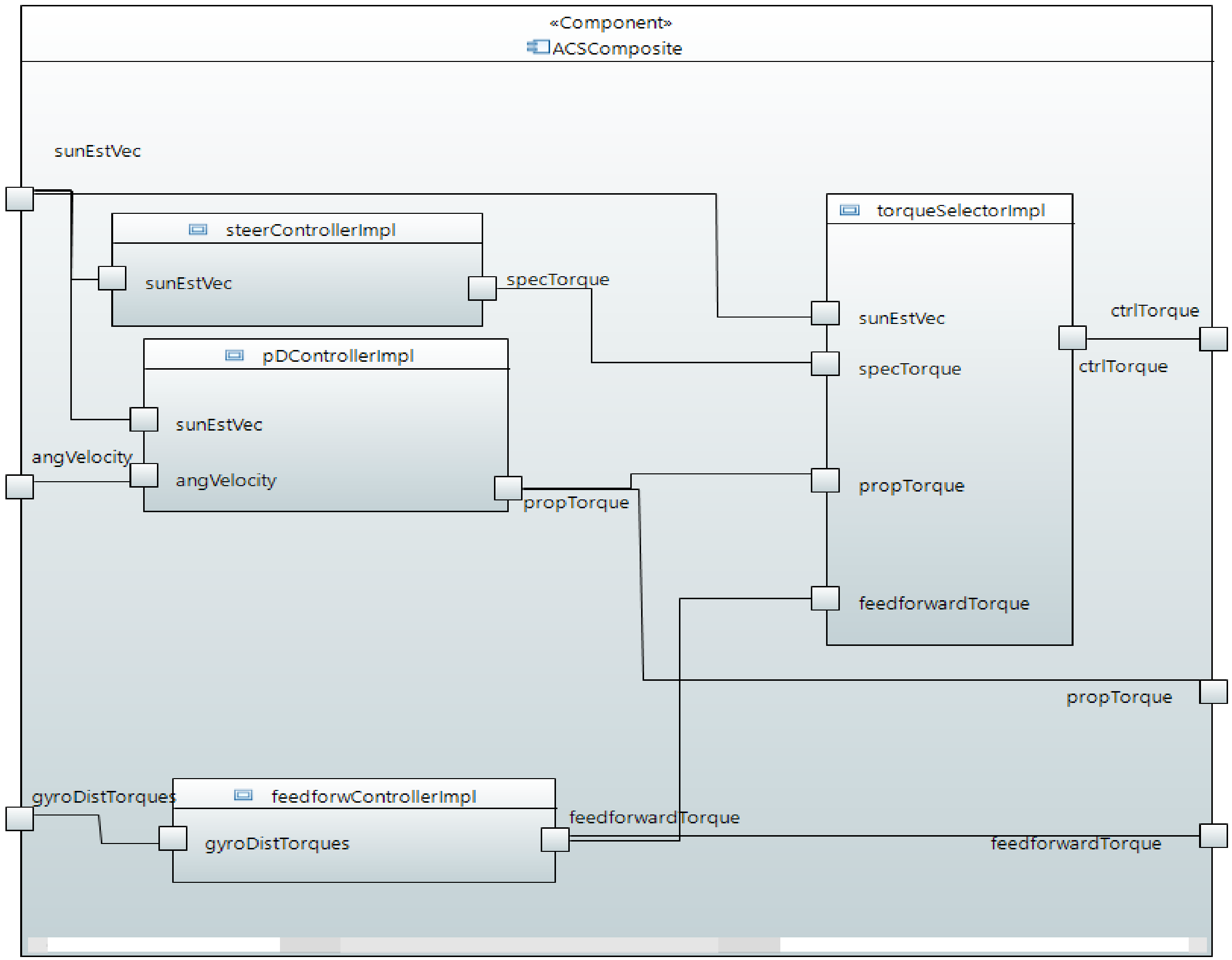
SASM Mode Functional Requirements

- Functional Requirements for computing the torque in SASM mode

The RCT sun acquisition control function shall compute and output a control torque based on:
- PD-controller
- Gyroscopic torque compensation
- Deadband filter.

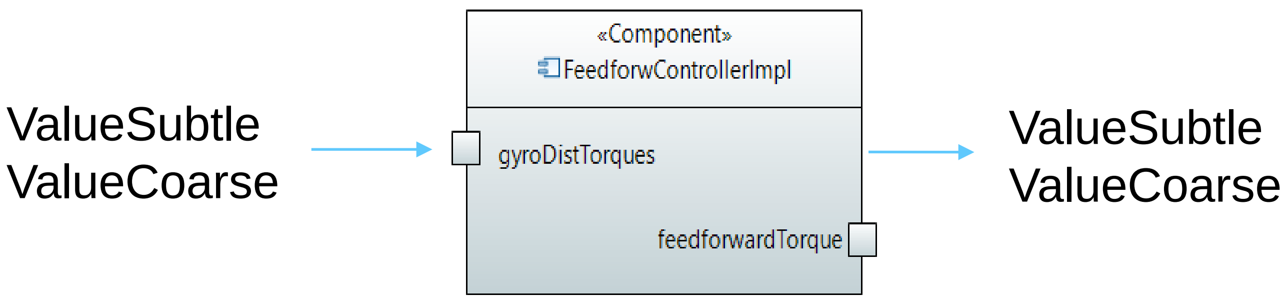
in order to point the S/C (it's reference direction) at the sun.

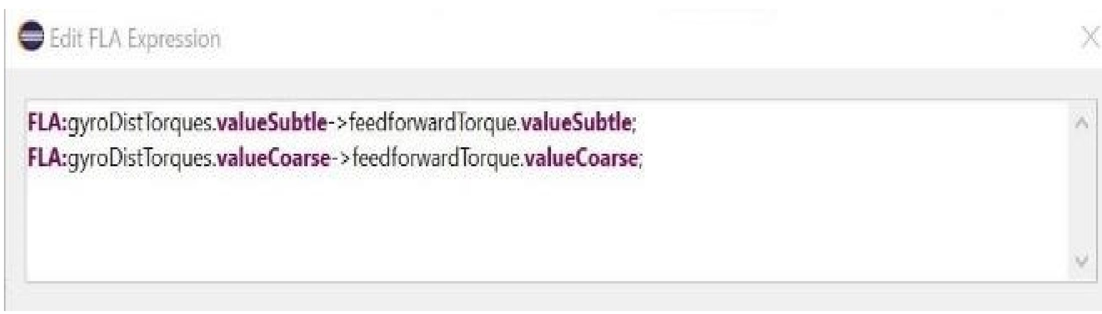
ACS Architecture in CHESS



Failure Behaviour of Components

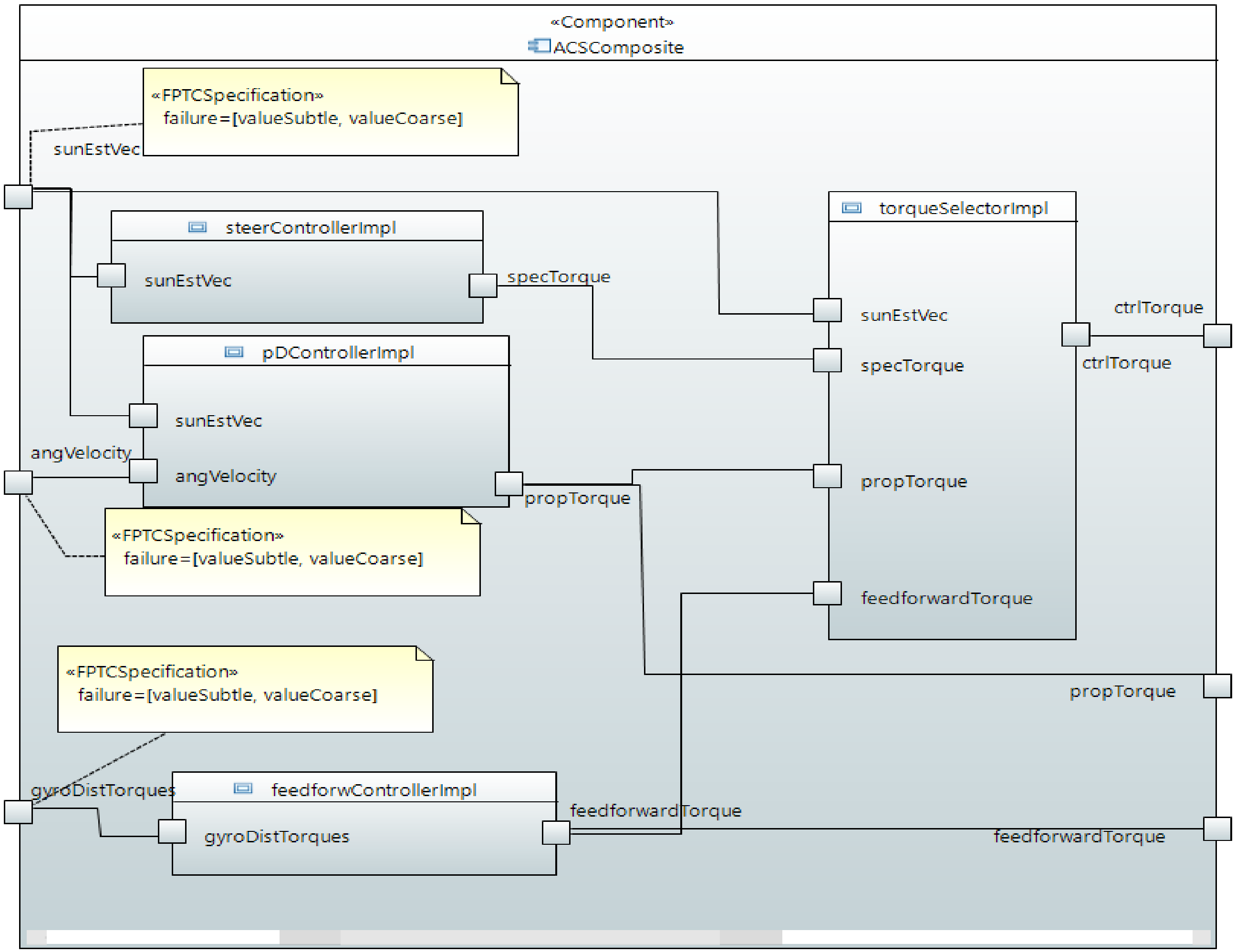
- Components behave as propagator in the prelimnary design, before introducing dependability means



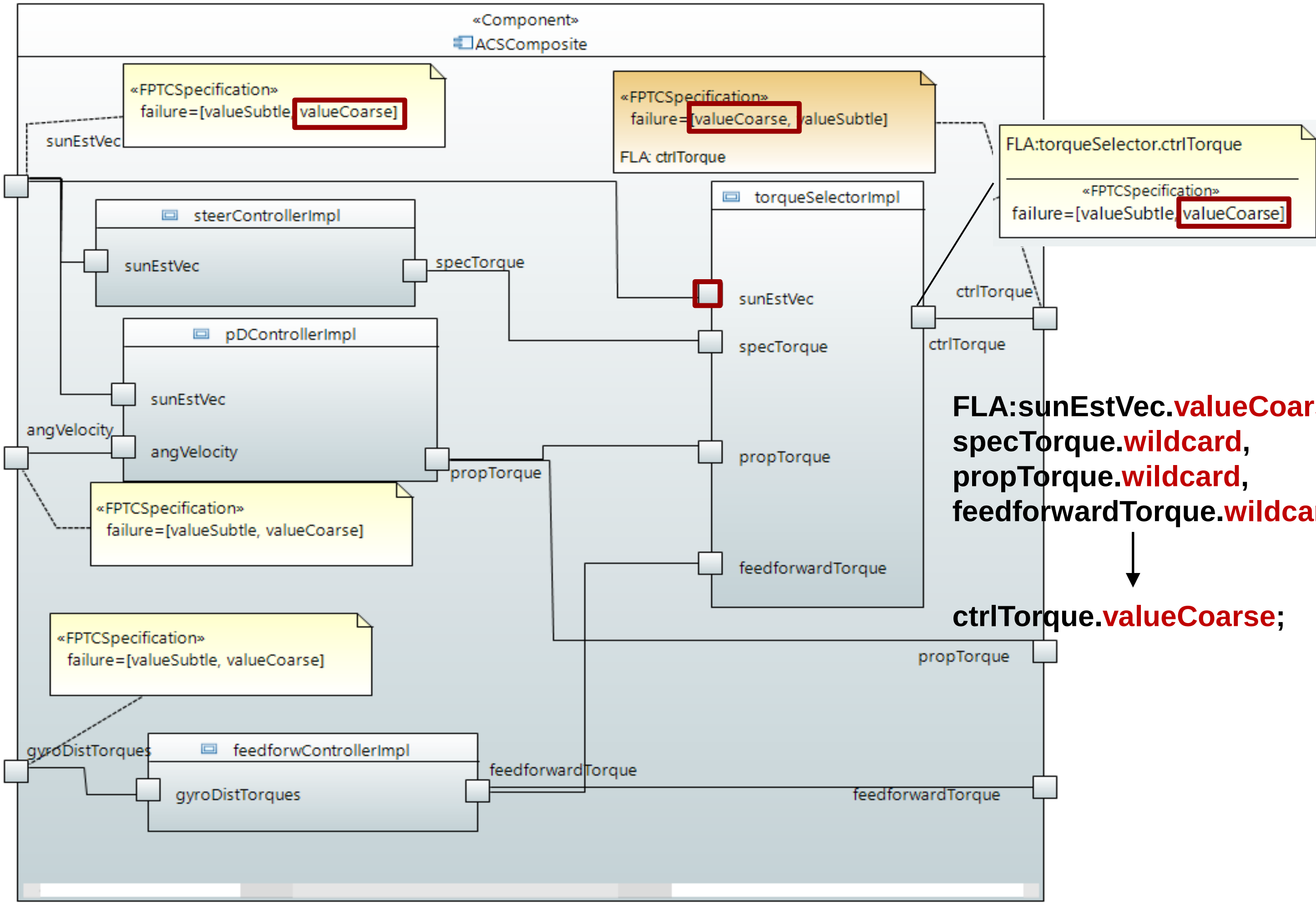


Fault Injection

- The value of the state estimates is invalid



Backpropagation of Results



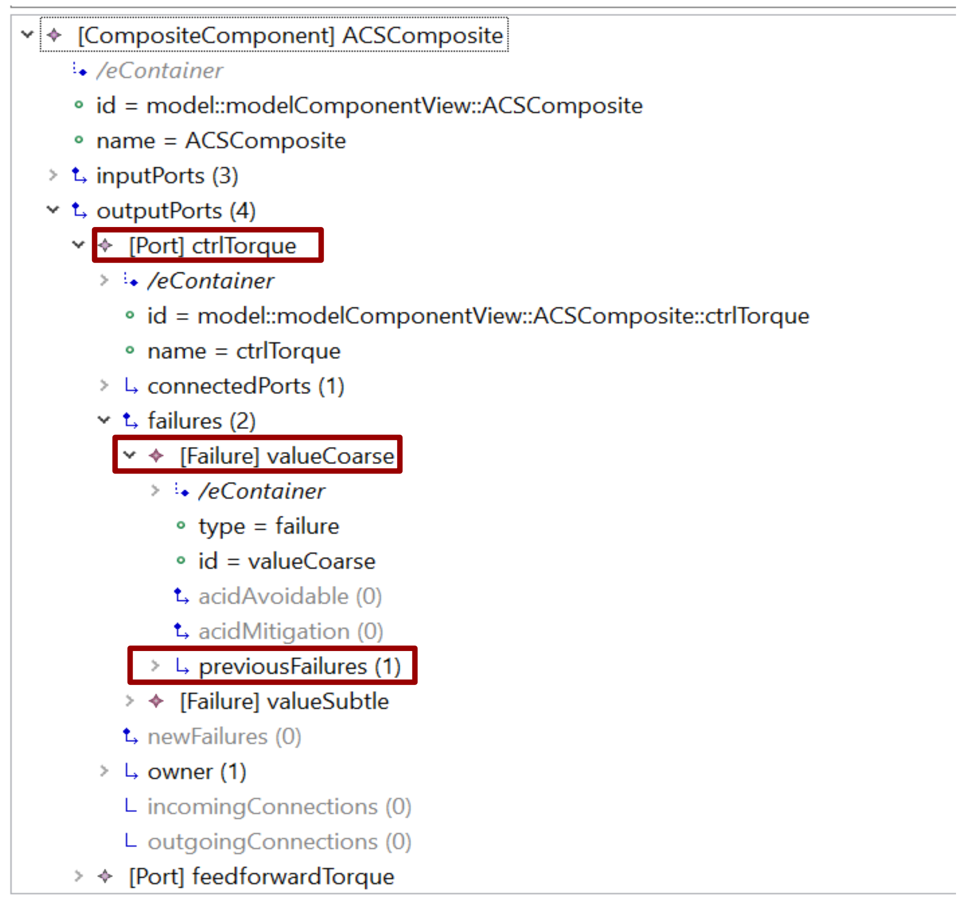
FLA:sunEstVec.valueCoarse, specTorque.wildcard, propTorque.wildcard, feedforwardTorque.wildcard

↓

ctrlTorque.valueCoarse;

Failure Propagation Paths

- Failure Propagation Path Browser
  - Output Ports
  - Failure Type
  - Previous Failures

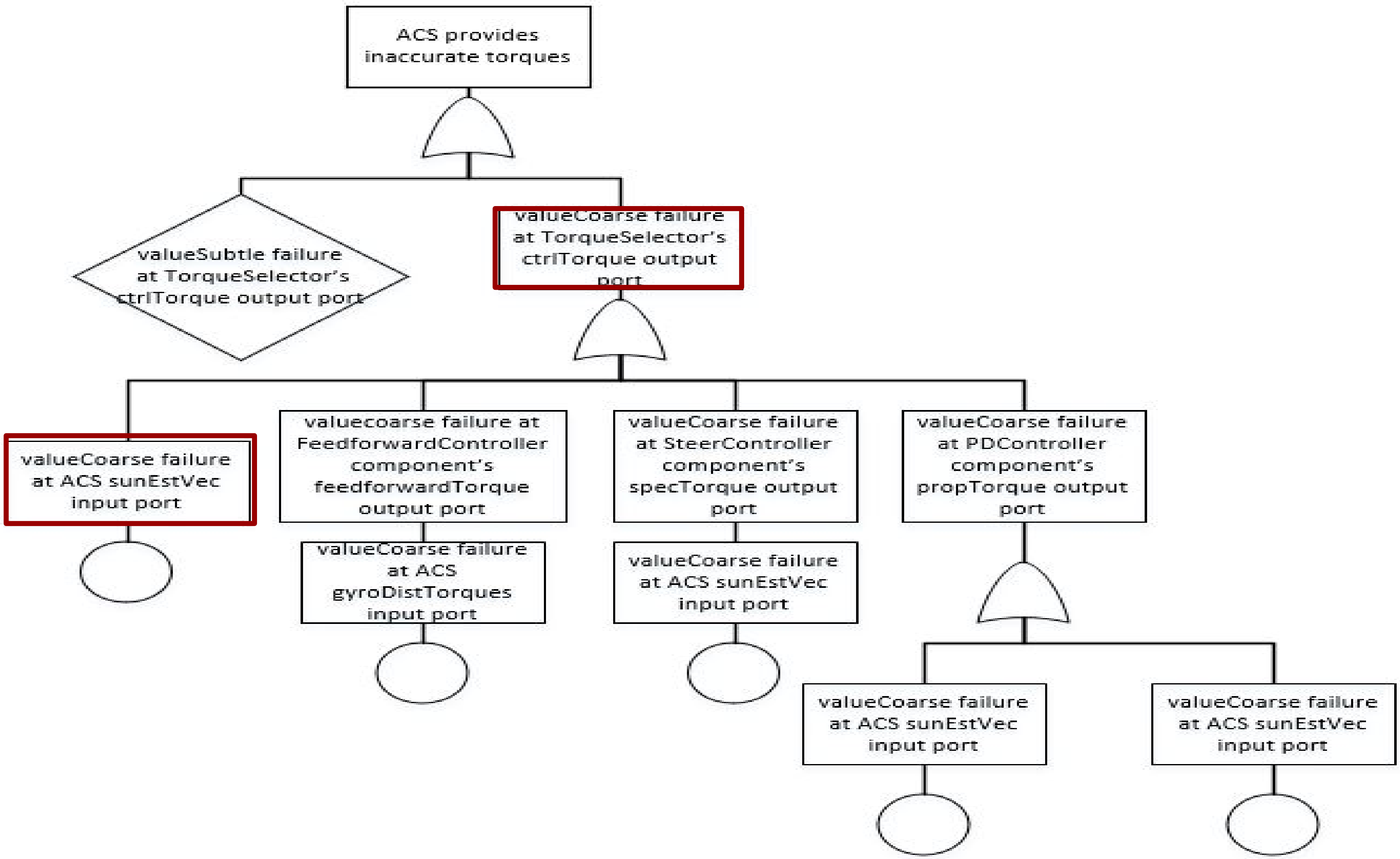


MÄLARDALEN UNIVERSITY SWEDEN · OHB SWEDEN · intecs the Brainware Company · AMASS

Failure Propagation Paths

```
<?xml version="1.0" encoding="ASCII"?>
<flamm:CompositeComponent xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:flamm="http://www.polarsy
  <inputPorts id="model::modelComponentView::ACSComposite::angVelocity" name="angVelocity" connectedPorts="//@c
    <failures type="failure" id="valueSubtle"/>
    <failures type="failure" id="valueCoarse"/>
  </inputPorts>
  <inputPorts id="model::modelComponentView::ACSComposite::gyroDistTorques" name="gyroDistTorques" connectedPor
    <failures type="failure" id="valueSubtle"/>
    <failures type="failure" id="valueCoarse"/>
  </inputPorts>
  <inputPorts id="model::modelComponentView::ACSComposite::sunEstVec" name="sunEstVec" connectedPorts="//@compo
    <failures type="failure" id="valueSubtle"/>
    <failures type="failure" id="valueCoarse"/>
  </inputPorts>
  <outputPorts id="model::modelComponentView::ACSComposite::ctrlTorque" name="ctrlTorque" connectedPorts="//@co
    <failures type="failure" id="valueCoarse" previousFailures="//@components.2/@outputPorts.0/@failures.0"/>
    <failures type="failure" id="valueSubtle" previousFailures="//@components.2/@outputPorts.0/@failures.1"/>
  </outputPorts>
```

Interpretation for Reliability



Interpretation for Safety

- Safety Hazard
  - Inacurate control torques in Sun acquisition and survival mode

Interpretation for Security

- Security Breach
  - ACS provides corrupted services and loses integrity

Dependability Measures Updated

The RCT sun acquisition control function shall flag the control invalid and output a control torque of zero if any of: - estimated sun vector - estimated rate are invalid.
The RCT sun acquisition control function shall flag the control invalid and output a control torque of zero if the angular momentum estimation function indicate that there is no valid S/C body rate.

MÄLARDALEN UNIVERSITY SWEDEN
OHB SWEDEN
AMASS

Conclusion and Future Work

- CHESS toolset is used to
  - Model the ACS and dependability information
  - Perform failure logic analysis
  - Manually interpret the results for multi-concern

- Provision of tool-support.

MÄLARDALEN UNIVERSITY SWEDEN

OHB SWEDEN

intecs the Brainware Company

AMASS

Thank you for your attention!

Discussion time…

Call For Fast Abstracts….. Deadline July 2, 2018

http://www.es.mdh.se/safecomp2018/fast-abstracts-call.php