Towards generating ECSS-compliant fault tree analysis results via ConcertoFLA

Barbara Gallina, Zulqarnain Haider, Anna Carlsson
{barbara.gallina, zulqarnain.haider}@mdh.se
anna.carlsson@ohb-Sweden.se

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

Certifiable Evidences & Justification Engineering (Research Group)
Context and motivation

Space Systems

Compliance

Dependability, Safety and Security Requirements...

Tool Supported analysis and generation of fault tree analysis results

Complexity Reduction

Compliance to ECSS

ECSS Standards
Talk outline

• Background
  – European Cooperation For Space Standardization (ECSS)
  – Tool Supported CHESS Methodology
    • ConcertoFLA

• Generation of ECSS-compliant Fault Tree analysis results approach

• Attitude Control System (ACS) Example
  – Modeling of ACS and Dependability
  – Failure Logic Analysis (FLA)
  – FLA Results and Fault Tree (FT) Generation

• Summary
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.

**NOTE** The main purpose of all dependability analyses is to improve the design by providing timely feedback to the designer, to reduce risks within the processes used to realize the products and to verify conformance to the specified dependability requirement.

6.4.2.5 Fault tree analysis (FTA)

a. A Fault Tree Analysis shall be performed to ensure that the design conforms to the failure tolerance requirements for combinations of failures.

**NOTE 1** ECSS-Q-ST-40-12 is a guideline for FTA.

---

| SEVERITY       | LEVEL | DEPENDABILITY (ECSS-Q-ST-30) | SAFETY (ECSS-Q-ST-40) Extract from ECSS-Q-ST-40C |
|----------------|-------|------------------------------|-----------------------------------------------|
| **Catastrophic** | 1     | Failures propagation (refer to point 5.3.2.c) | “Loss of life, life-threatening or permanently disabling injury or occupational illness.” |
|                |       |                              | Loss of an interfacing manned flight system |
|                |       |                              | Severe detrimental environmental effects. |
|                |       |                              | Loss of launch site facilities. |
|                |       |                              | Loss of system |
| **Critical**   | 2     | Loss of mission              | Temporarily disabling but not life-threatening injury, or temporary occupational illness. |
|                |       |                              | Major detrimental environmental effects. |
|                |       |                              | Major damage to public or private properties. |
|                |       |                              | Major damage to interfacing flight systems, |
|                |       |                              | Major damage to ground facilities.” |
| **Major**      | 3     | Major mission degradation   | |
| **Minor or Negligible** | 4 | Minor mission degradation or any other effect. | |
7.5.2 Hazard analysis

a. Hazard analysis shall be performed in a systematic manner, beginning in the concept phase and continuing through the operational phase, including end-of-life and disposal.

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.

b. A fault tree analysis, or its equivalent, shall be performed to verify the failure tolerance requirements.

NOTE Refer to ECSS-Q-STD-40-12 “Fault tree analysis - Adoption notice ECSS/IEC 61025” for further instructions on fault tree analyses.

| Severity  | Level | Dependability (refer to ECSS-Q-STD-30) | Safety (ECSS-Q-STD-40) |
|-----------|-------|----------------------------------------|------------------------|
| Catastrophic | 1     | Failures propagation                    | Loss of life, life-threatening injury or permanently disabling injury or occupational illness; Loss of system; Loss of an interfacing manned flight system; Loss of launch site facilities; Severe detrimental environmental effects. |
| Critical   | 2     | Loss of mission                         | Temporarily disabling but not life-threatening injury, or temporary occupational illness; Major damage to interfacing flight system; Major damage to ground facilities; Major damage to public or private property; Major detrimental environmental effects. |
| Major      | 3     | Major mission degradation               | ---                     |
| Minor or Negligible | 4 | Minor mission degradation or any other effect | --- |
5.4.4 **Criticality classification**

The supplier shall provide the lower level suppliers with the relevant results of the safety and dependability analyses performed at higher and his level (ref. clauses 6.2.2.1 and 6.2.2.2), including:

1. the criticality classification of the software products to be developed;
2. information about the failures that can be caused at higher level by the software products to be developed.

**EXPECTED OUTPUT:** Safety and dependability analyses results for lower level suppliers [RB, ;-; SRR].

### 6.2.2.2

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.

**EXPECTED OUTPUT:** Software dependability and safety analysis report [PAF, ;-; PDR].

| Category | Definition |
|----------|------------|
| A        | Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: |
|          | → Catastrophic consequences |
| B        | Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: |
|          | → Critical consequences |
| C        | Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: |
|          | → Major consequences |
| D        | Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: |
|          | → Minor or Negligible consequences |
IEC 61025

- A fault tree is an organized representation of the conditions or other factors causing or contributing to the occurrence of a defined outcome, referred to as the “top event”

- Fault tree analysis is a deductive (top down) method of analysis aimed at pinpointing the causes or combination of causes that can lead to the defined top event
CHESS is an open-source methodology and toolset available from Eclipse/Polarsys
- Model Driven Methodology
- Component Based Approach
- Separation of Concerns
- Dependability Profile

https://www.polarsys.org/projects/polarsys.chess
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} \rightarrow \text{FPTC Expressions} \rightarrow \text{output ports} {failures}

Inputport\_failuretype \rightarrow Outputport\_failuretype

- Failure types
  - Value [Coarse, Subtle]
  - Timing [Early, Late]
  - Provision [Omission, Commission]

- Component behavior
  - Sink
  - Source
  - Transform
  - Propagate
Generation of ECSS-compliant Fault Tree analysis results approach

Architectural elements modelling

Is restructuring needed?

Yes

No

Failure logic modelling
Component level

Causality paths exploitation for FT generation

Results Interpretation

Analysis invocation

Failure logic modelling
System level
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.
Components behave as propagator in the preliminary design, before introducing dependability means.
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
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::ACComposite::angVelocity" name="angVelocity" connectedPorts="/testport
  <failures type="failure" id="valueSubtle"/>
  <failures type="failure" id="valueCoarse"/>
</inputPorts>
<inputPorts id="model::modelComponentView::ACComposite::gyroDistTorques" name="gyroDistTorques" connectedPor
  <failures type="failure" id="valueSubtle"/>
  <failures type="failure" id="valueCoarse"/>
</inputPorts>
<inputPorts id="model::modelComponentView::ACComposite::sunEstVec" name="sunEstVec" connectedPorts="/compo
  <failures type="failure" id="valueSubtle"/>
  <failures type="failure" id="valueCoarse"/>
</inputPorts>
<outputPorts id="model::modelComponentView::ACComposite::ctrlTorque" name="ctrlTorque" connectedPorts="/testport
  <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>
Generation of Fault Tree

ACS provides inaccurate torques

valueSubtle failure at TorqueSelector’s ctrlTorque output port

valueCoarse failure at TorqueSelector’s ctrlTorque output port

valueCoarse failure at ACS sunEstVec input port

valueCoarse failure at FeedforwardController component’s feedforwardTorque output port

valueCoarse failure at ACS gyroDistTorques input port

valueCoarse failure at ACS sunEstVec input port

valueCoarse failure at ACS sunEstVec input port

valueCoarse failure at ACS sunEstVec input port

valueCoarse failure at ACS sunEstVec input port

valueCoarse failure at PDController component’s propTorque output port

May 21-22 2018, 6th Scandinavian Conference on System & Software Safety
Summary and Future Work

• CHESS toolset is used to
  – Model the ACS
  – Model dependability information
  – Perform failure logic analysis

• Generation of FTA-results in the context of ECSS and IEC 61025

• Provision of tool-support.
Thank you for your attention!

Discussion time…

Call For Fast Abstracts – Deadline: 02 July 2018 – Notification: 09 July 2018

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