FDIR engineering supported by ECSS

A.Oganessian
Noordwijk
26/10/2011

Space System Fault Management

Space System Fault Management consists of cooperative design of **Space System**, **Ground** and **Operator Action** (HW, SW and Operational Procedure) which allow Space System to continue operation or reach a safe state when system faults/failures occur.

Extent of Fault Management in Space System

including level of foreseen **autonomy**, **dependability** and **safety** in the expected operational profile

depends on requirements derived from **Mission Type**, **Goals** and **Objective**,

Extent of Fault Management in Space System – reflected in ECSS

1. ECSS-Q-ST-30C Dependability
2. ECSS-Q-ST-40C Safety
3. ECSS-E-ST-70-11C Space Segment Operability

System Analysis

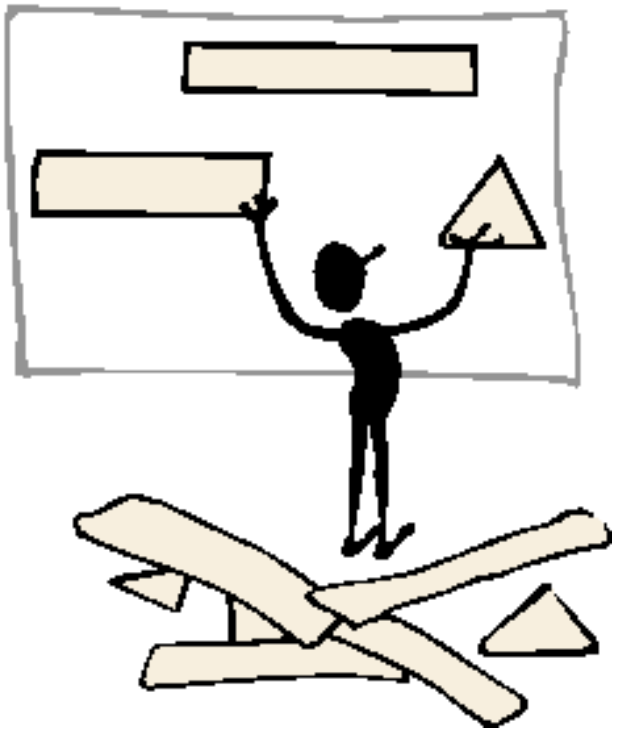
Faults are identified through analysis process which covers Space System and Operating Environment, including:

- **Fault Tree Analysis**
- **FMEA/FMECA Analysis**
- **Hazard Analysis**
- **HW/SW Interaction Analysis**

System Analysis – reflected in ECSS

1. ECSS-Q-ST-30-02C FMEA/FMECA
2. ECSS-Q-ST-40-09C Availability
3. ECSS-Q-ST-40-09C Hazard Analysis
4. ECSS-Q-ST-40-12C FTA
5. ECSS-Q-ST-30C Dependability (FMECA/FMEA/FTA)
6. ECSS-Q-ST-80C SW Product Assurance (SW Criticality)

FDIR Requirements



Amount of built in redundancy and cross-strapping

AOCS related FDIR requirements

Hierarchy, locality, levels etc.

FDIR Requirements – reflected in ECSS

1. ECSS-E-ST-60-30C – Attitude and Orbit Control Systems (in preparation)
2. ECSS-E-ST-70-11C Space Segment Operability

Example of AOCS FDIR requirement

The draft standard "Satellite AOCS requirements" (ECSS-E-ST-60-30C Draft1, under public review) does not impose upfront architectural design:

5.1.2.2 Hardware and software redundancy scheme

a. The AOCS shall justify the hardware redundancy implemented against failure tolerance requirements and reliability requirements.

b. The AOCS shall justify that the design of the safe mode minimizes the risk of common design error and avoids common failure with the modes used for the nominal mission.

NOTE This AOCS safe mode justification can involve for instance one or several of the following features:

- The use of redundant hardware branches in the safe mode
- The use of different sensors and actuators in the two classes of modes
- The use of separate software for the two classes of modes
- The potential in flight validation status of the safe mode, which can provide confidence in the design.

To be compared with a commonly used design requirement:

R-AOCS-0180 The Emergency and Safe Mode [ESM] shall use Actuators and Sensors different from those used in nominal Operational Mode .

Verification and Validation

FDIR Testing is based on threats scenarios, but is not systematic.

Robustness and Stress Tests are used, but they are loosely coupled to FDIR System.

Verification and Validation – reflected in ECSS

1. No specific ECSS ?

Do we have methods to support the complete FDIR engineering tasks ?

FTA & FME(C)A

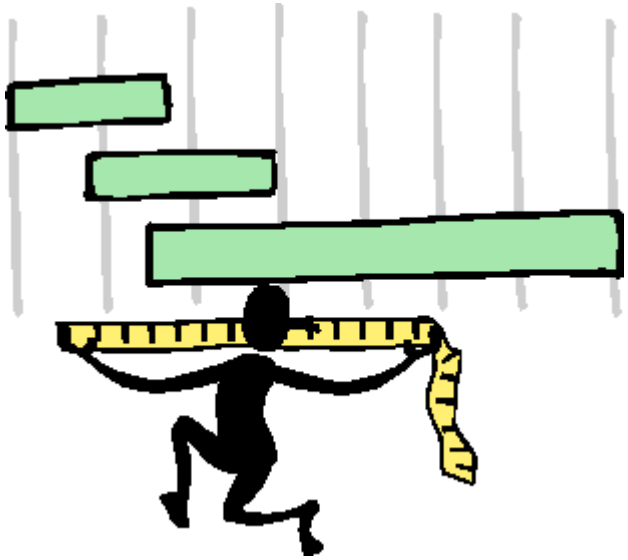
FMEA (bottom-up approach) - considering effect of component failures on the system. FMEA can not be completed until System design has sufficient levels of details.

FTA (top-down approach) - for each potential failure finding out the root cause. FTA does not guarantee that every Possible component failure mode which contribute to system failure has been considered.

There is no guarantee that FMEA & FTA cover **all possible failure modes**, **combination of failure modes** and **their effects**, and they are limited to realistic from analyst point of view set.

FTA / FMEA – two contributors to FDIR requirement and design, yet no single methodology exists to support System Engineer in crafting FDIR.

System FDIR Engineer lifecycle



FDIR engineering milestones and its relation to project milestones ?

How do we measure maturity of System Fault Management ?

System FDIR engineering lifecycle and its relation to project lifecycle is not clear and needs elaboration (what is reviewed FDIR wise at project milestones ?, what are measurable criteria for FDIR maturity etc.)

Definitions

Fault (two definitions as “state” and as “event”), **Failure, Error**

Fault Tolerance, **Failure** Tolerance

ECSS-P-001B – 2004.06.14 – Glossary

Error **propagation,** Fault **propagation,** Failure **propagation**

ECSS-E-ST-70-01C – Sp
Co

Next higher operational control instance (FDIR **level**)
ECSS-E-ST-70-11C – Space Segment Operabilit

Definitions need to be revised for completeness and consistency

Failure Detection, Isolation, Recovery (FDIR)
most of ECSS
Fault Detection, Isolation, Recovery (FDIR)
ECSS-Q-ST-30C - ISVV Guide
Fault Detection, **Identification**, Recovery (F
ECSS-E-ST-40C - Software

r a failure or group
ission, or **phase** dependent
ECSS-E-ST-10C – System Engineering

Recovery **strategy**
ECSS-E-ST-40C - Software

FDIR **strategy**
ECSS-E-ST-70-01C – Spacecraft Onboard Control Procedures

Thank You !