Towards a FDIR handbook

M. Verhoef (TEC-SWE)

ADCSS SAVOIR session – 18-10-2016

ESA UNCLASSIFIED - For Official Use

Agenda

- Background
- Internal ESA working group
- Inputs and scope of the handbook
- Preliminary table of contents
- SAVOIR involvement – FDIR working group
- Status and conclusion

Background

ADCSS 2015 – special session on FDIR, main conclusions:

- Processes must be further improved and consolidated
- Clear need for common terminology used across industry
- The main challenge remains to be FDIR verification and validation
- Tools are considered essential but not yet sufficiently robust or lacking integration with other engineering tools

- Need to establish a community
- Need to establish a common goal

- First step: FDIR handbook

Internal working group

Working group was formed at ESTEC:

- TEC-SWE (Marcel Verhoef) – convenor
- TEC-S (Jean-Loup Terraillon)
- TEC-SWS (Ana Rugina)
- TEC-SWE / HRE-PEE (Yuri Yushtein)
- SCI-PSA (Andrei Oganessian)
- TEC-ECN (Alvaro Martinez Barrio, Guillermo Ortega Hernando)
- TEC-ECC (Benedicte Girouart)
- TEC-QQD (Antonio Harrison Sanchez)
- TEC-QQS (Manrico Fedi Casas)
- TEC-EDD (Giorgio Magistrati)
- TEC-EPD (David Jameux)

ESA WG kick-off in March and April 2016, four meetings to date.

Inputs for the handbook

Results from several completed TRP and GSTP studies:

- COMPASS, VERIFIM, AUTOGEF, FOREVER, HASDEL, FAME, FDI-AOCS

Alignment with currently on-going studies:

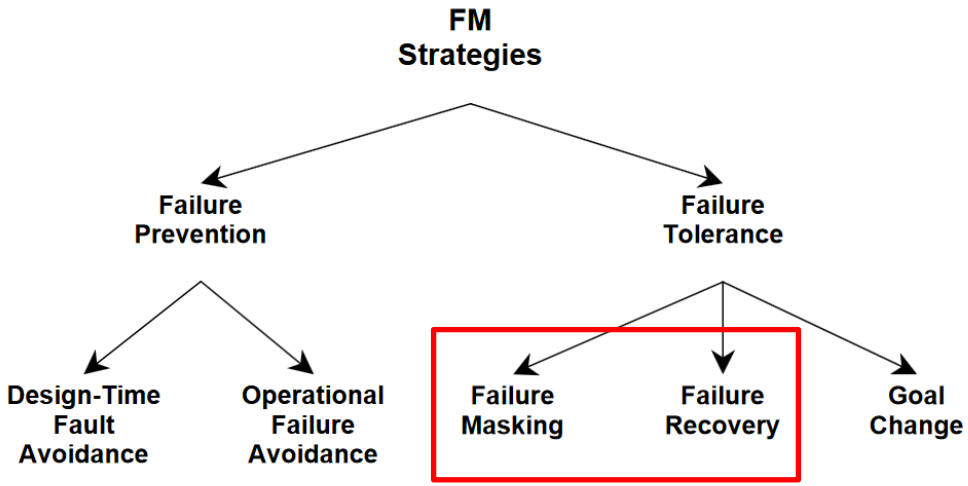
- GAFE, CSSP, CATSY

Experiences from ESA missions (specifications, best practices, lessons learned)

Other resources: NASA (draft HDBK-1002), CNES

Current scope of the handbook

- Primary focus on design, engineering, verification and validation of on-board failure masking and failure recovery mechanisms of a given dependability architecture
- Autonomy and operations aspects not deeply covered



Preliminary table of contents (1)

- Annotated Terms and Definitions
- FDIR in ECSS standards
  - Identify where FDIR is referenced in the current standard
  - Is terminology consistently used?
  - Are process steps consistent from multi-discipline perspectives?
  - Are inputs and output identified for each process and review step?

  - ➢ Guidelines on how to use / interpret the current set of standards
  - ➢ Clarify and align terminology used
  - ➢ Clarify expectations on input and output artifacts for each process steps
  - ➢ Identify potential improvements to the ECSS standards

Preliminary table of contents (2)

- FDIR process (in context of existing ECSS processes)
    - Feared Event modelling, FTA, FMEA: flow-down and traceability
    - The role of Software FMEA
- FDIR strategy and scope
    - Mission phases and modes
- FDIR architectural principles
    - Hierarchy : system, sub-system, units / equipment
    - (agreement on definition of) FDIR levels
    - Configurability
- FDIR design principles and generic requirements
- FDIR implementation considerations and best practices
- FDIR end-to-end verification and validation aspects
- Tool support

SAVOIR involvement

- Progress has been reported to SAVOIR AG since initiation of internal WG
- SAVOIR AG has agreed to the establishment of an SAVOIR FDIR WG
- SAVOIR FDIR WG to review and complement draft FDIR handbook
- Confirmed participation from:
    - Thales Alenia Space (F, I)
    - Airbus (UK, D, F)
    - OHB
    - CNES
    - DLR
- Airbus and TAS have already agreed to share results from completed TRP studies for re-use and adoption in the handbook
- Kick-off foreseen before EOY

Status and conclusions

- Internal ESA working group formed
- Scope and contents are identified
- Draft handbook is (slow but steady) work in progress
- First draft by EOY for internal review in ESA working group
- SAVOIR FDIR working group kick-off expected by EOY