Towards an FDIR process: the SAVOIR FDIR handbook

Marcel Verhoef (ESA), Alvaro Martinez Barrio (ESA), Murray Kerr (DEIMOS)

16/10/2018

How the SAVOIR FDIR Handbook became to be..

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

SAVOIR working group – FDIR handbook

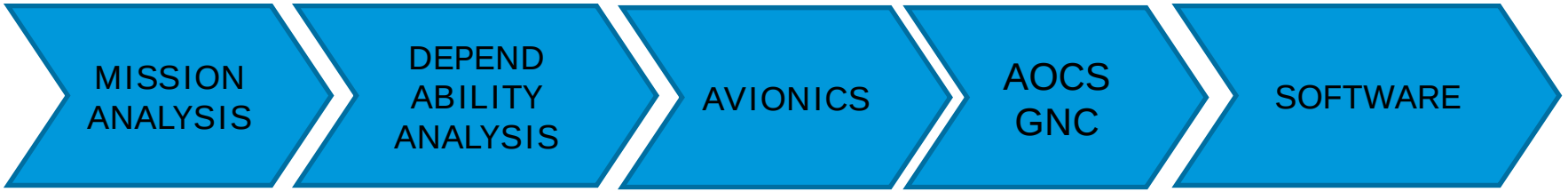
- Working group established with industry early in 2017
- Very active (40+ participants) and productive
- Aim is to produce an FDIR handbook in 2018
- Internal draft available (work in progress)
- Inspired by NASA-HDBK-1002 (Draft, 2012)
- Consolidation of ESA TRP and GSTP R&D results

Focus of the SAVOIR FDIR handbook:

- Unification of terminology used (multi-discipline)
- Identification of FDIR in all engineering processes
- Definition of an FDIR process in context of ECSS E-10
- Alignment of working methods – supplier
- Alignment of expectations – consumer
- Identification and promotion of best practices

Generic view on S/C FDIR – a real systems issue

- Identify the main mission phases (launch, separation, orbit raising, operations)
- For each mission phase, determine the feared event(s) leading to mission loss
- For each feared event, determine the means necessary to mitigate that risk
- Design a spacecraft concept that is able to deliver all these mitigations
    - dependability concept (FO or FS) and redundancy architecture
    - FDIR strategy (active management of known failure modes)
- Consolidate FDIR implementation (unit → subsystem → system → ground)
- Demonstrate fitness for use (through verification and validation)
- Caveat (1) : significant parts of the FDIR is implemented in flight software
- Caveat (2) : cross-cutting concern touching almost all disciplines and design artifacts



SAVOIR FDIR Handbook – process steps (1)

- Step 0 : FDIR Requirements
- Step 1 : FDIR Concept definition
- Step 2 : FDIR Architecture
- Step 3 : FDIR Detailed design
- Step 4 : FDIR Implementation
- Step 5 : FDIR Validation
- Step 6 : FDIR Operations

For each process step, we identify:

(1) The objective of the process step

(2) Identifiable programmatic dependencies

(3) Required inputs (per discipline)

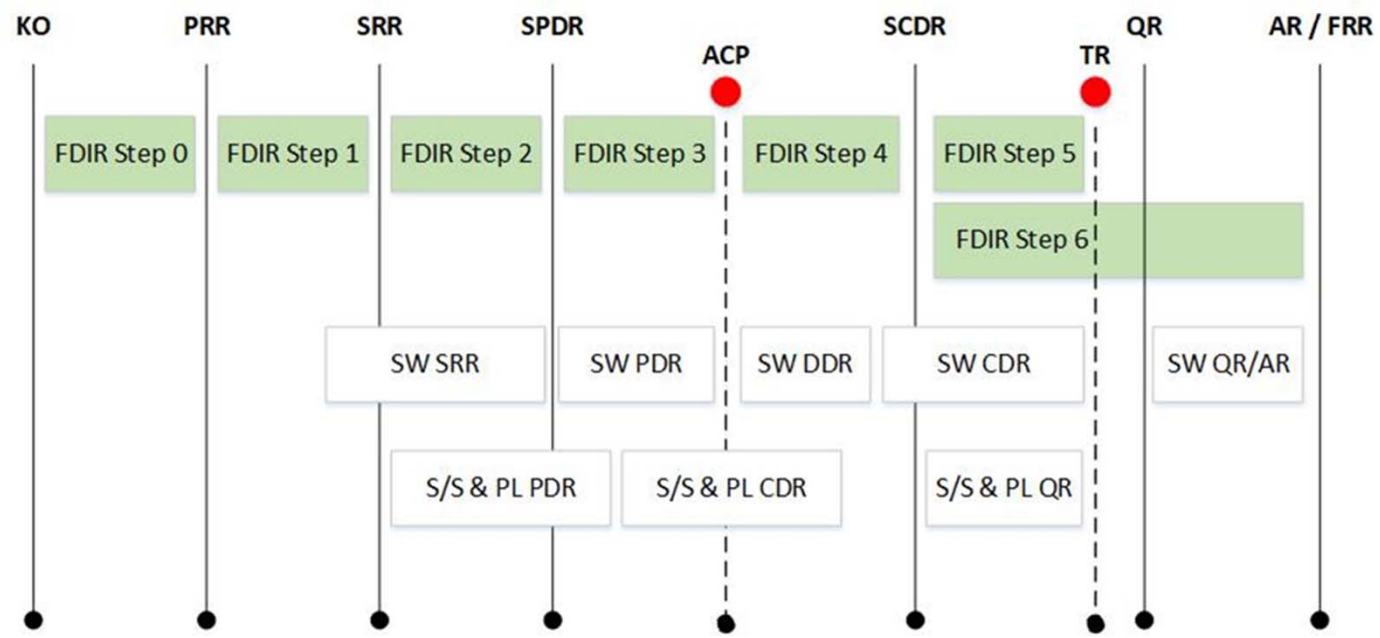
(4) Expected outputs

(5) Description of the activities to perform

(6) Guidelines and lessons learned

(7) Resources to be used in this step
- methods
- tools

SAVOIR FDIR Handbook – process steps (2)



FDIR process steps in relation to ECSS E-10 and domain specific activities (draft)

SAVOIR FDIR Handbook – architectural checkpoint

- Purpose of architectural checkpoint (executed as an iterative process step)
  - consolidate FMEA and FDIR from all sub-system and unit level
  - ensure unique and consistent identification of all failure modes
  - determine appropriate level of fault detection (who is responsible)
  - ensure appropriate observability definitions and V&V requirements
  - determine appropriate level of fault mitigation (who is responsible)
  - define V&V requirements for all active mitigations
  - demonstrate compliance to system-level requirements (i.e. w.r.t. timing, availability)
- This process ensures high readiness levels before S-CDR and SW-SRR (w.r.t. FDIR)
- Prepares for consistent RAMS / FDIR requirement traceability at system level (for QAR)
  - all observables are covered
  - all autonomous recovery actions and flight operations procedures are covered
  - all failure modes are covered

SAVOIR FDIR Handbook – tuning review

- Consolidation of all change made during implementation and AIT, w.r.t.
  - changes in monitoring definitions
  - changes in recovery actions
- These changes are typically captured in the SRDB, and are part of the *configuration* of flight software (which is not necessarily considered as a SW change)
- Ensure that all V&V steps necessary are taken for each FDIR change
- Complements the NCR/NRB process flow (typically followed for each individual change)
- Ensure consistency of the FDIR in its entirety / avoid conflicts or interdependencies
- Ensures readiness for S-QAR

SAVOIR FDIR handbook status and outlook

- First complete draft handbook (r14) is due in Oct 2018
- Internal review (working group) is planned for Q4 2018
- Approval of FDIR handbook by SAVOIR SAG expected end of Q1 2019

- Caveat: SAVOIR documents are restricted to ESA member states

- Potential future directions:
  - extend handbook to include design best practices (new technologies)
  - consolidate FDIR process with international partners (e.g. NASA / JAXA)
  - transfer SAVOIR HB into ECCS artefact (TM, HB or full standard)

Many thanks to working group members!

Marcel Verhoef (co-convener)
Alvaro Martinez Barrio (co-convener)
Ana Rugina
Andrea Accomazzo
Andrei Oganessian
Antonio Harrison Sanchez
Benedicte Girouart
David Jameux
Giorgio Magistrati
Guillermo Ortega
Jean-Loup Terraillon
Luca Bolognino
Manrico Fedi Casas
Yuri Yushtein
Jesus Gil Fernandez
Fulvio Capogna

ADS: Gunther Lauthenschlaeger, Dave Thomas (lead), Ilario Cantiello, Jean-Paul Blanquart, Patrick Bergner

DEIMOS: Paulo Rosa, Murray Kerr (lead), Mariano Sánchez Nogales, Miguel Hagenfelt,

OHB: Massimo Tipaldi (lead), Hong-Joon Chun, Gordon Machel, Matthias Hoping

CNES: Christian Pouliquen

DLR: Catherin Hobbie, Sascha Mueller

RUAG: Torbjorn Hult

TAS: Regis de Ferluc, Brice Dellandrea, Antoine Provost-Grellier (lead), Gianluca Aranci, Luigi Galvagni, Philippe Fourtier