Towards the standardization of FDIR in Europe: The new release of the SAVOIR FDIR handbook

Paulo Rosa (Deimos)
Silvana Radu (ESA)
Benedicte Girouart (ESA)

22/11/2024

Content

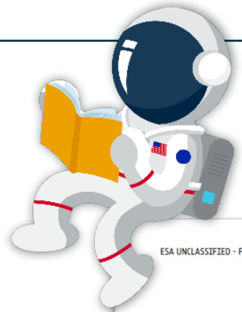
1. What is the SAVOIR FDIR Handbook?
2. Update of the Handbook
3. Composition and support
4. HB update process
5. Major topics tackled
6. What's New?
7. Open topics
8. The New release of the HB
9. Closing remarks
10. What's next?

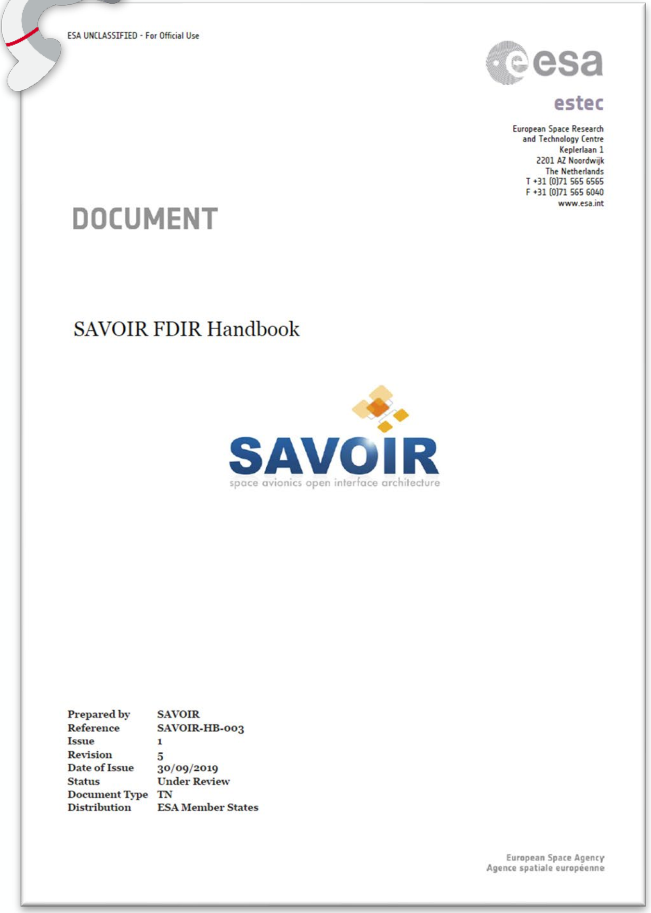
1. What is the SAVOIR FDIR Handbook?

- **Main purpose**: establish a common view on how to realise system health management (or fault management), with a focus on active mitigation, which is commonly referred to as failure detection, isolation and recovery (FDIR)

- Scope:
  - Focused on spacecraft platform avionics, although the general principles will be of use to a potentially wide range of application areas
  - Complements (or proposes changes to) existing working practices
  - It is not normative; it captures knowledge and consolidates best practices and lessons learned

- Current version (2.0) was released by the end of 2019




ESA UNCLASSIFIED - For Official Use

estec

European Space Research
and Technology Centre
Keplerlaan 1
2201 AZ Noordwijk
The Netherlands
T +31 (0)71 565 6565
F +31 (0)71 565 6040
www.esa.int

DOCUMENT

SAVOIR FDIR Handbook

SAVOIR
space avionics open interface architecture

Prepared by	SAVOIR
Reference	SAVOIR-HB-003
Issue	1
Revision	5
Date of Issue	30/09/2019
Status	Under Review
Document Type	TN
Distribution	ESA Member States

European Space Agency
Agence spatiale européenne

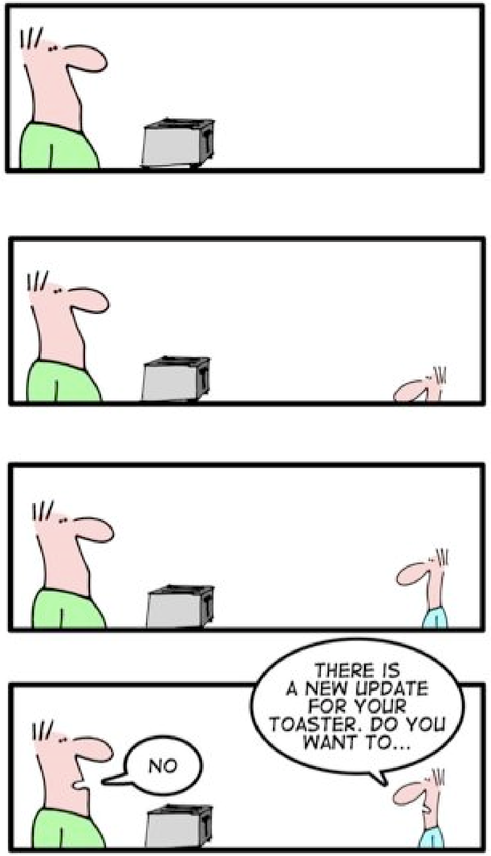
2. Update of the Handbook

Why updating it?

- ✓ Identify missions/technologies for which common FDIR design and processes recommended in the current issue of the handbook are **not applicable or require tailoring**
- ✓ Identify minor aspects within the handbook that are needed for update in order to be aligned with other existing handbooks or technical notes
- ✓ Revise overall handbook and alignment with ECSS
- ✓ Gather lessons learned from satellite manufacturers and mission operators on FDIR and integrate those lessons learned in the handbook

Ensure the handbook can be used for a large range of types of missions, including with regards to new niches such as Close Proximity Operations, high autonomy, use of AI/ML, etc.

- ✓ At the SAVOIR Advisory Group meeting #51, the SAG has decided to continue the FDIR working group for the elaboration of a new issue of the SAVIOIR FDIR



geekandpoke.typepad.com

3. Composition and support

From ESA side:

Name expert	Expertise
Andrei Oganessian	Avionics, SW
Andrew Brown	PA, RAMS
Andrew Wolahan	System, CPO
Benedicte Girouart	GNC, AOCS
Charles Lahorgue	Constellations, RAMS, FDIR
Cristophe Honvault	Software
Christoph Steiger/ Caglayan Guerbuez	Operations
David Pena Hidalgo	Software
Jean-Loup Terraillon	Savoir, MBSE
Laurent Hili	CDHS, AI/ML
Marcel Verhoef	MBSE, SW
Mauro Caleno	Software
Massimo Casasco/ David Sanchez	GNC, AOCS
Roger Walker/ delegated	CubeSats
Silvana Radu	RAMS, CPO, CubeSats, MC
Ferdinando Tonicello	Power

Co-chairs:

- Silvana Radu
- Benedicte Girouart

3. Composition and support

From industry side:

Name expert	Organisation
Alexandre Cortier	ADS
Horst Tjaden	ADS
Nathalie Pons	CNES
Aurelie Strzepek	CNES
Julien Rey	CNES
Jonas Lebram	Beyond Gravity
Olivier Rigaud	TAS
Orion Azzis	TAS
Stefano Di Vito	TAS
Lorenzo Bitetti	TAS
Matthias Hoping	OHB
Machel Gordon	OHB
Michael Brahm	OHB
Maxime Atanian	OneWeb
Paloma Maestro Redondo	RHEA
Paulo Rosa	Deimos

+ many other experts from each organisation with expertise depending on the topic to be discussed or agreed on.

Support to ESA Co-chairs:

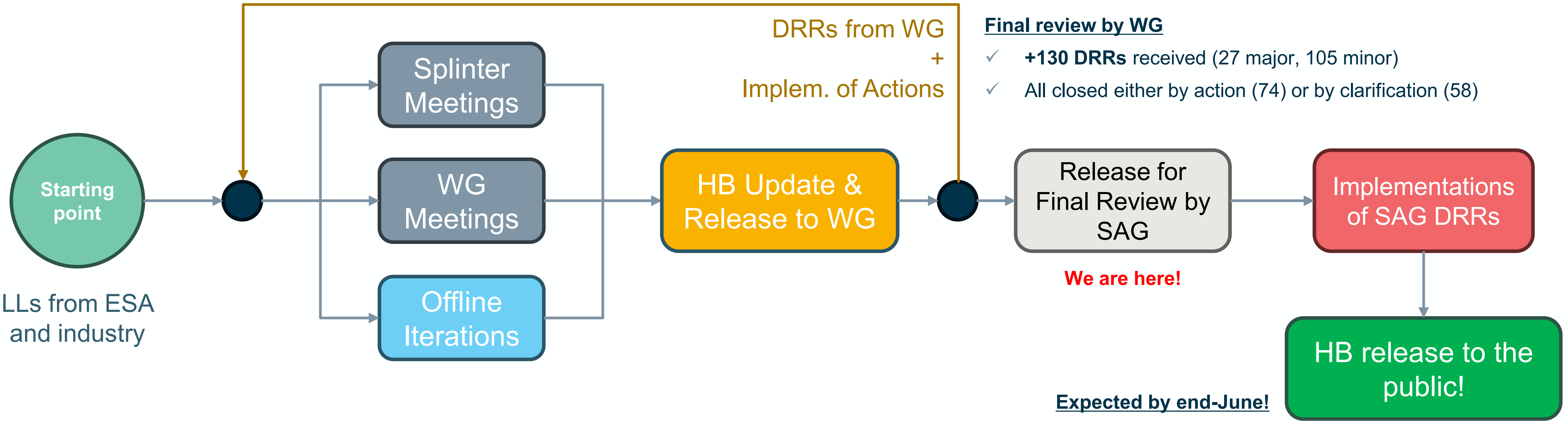
- Paulo Rosa
- Tatiana Fontana

4. HB Update Process

Starting Point: Lessons learned from industry and ESA were provided

- ✓ From missions
- ✓ From small studies
- ✓ From background activities
- ✓ From internal activities
- ✓ From review of handbook against other standards/handbooks/ technical notes

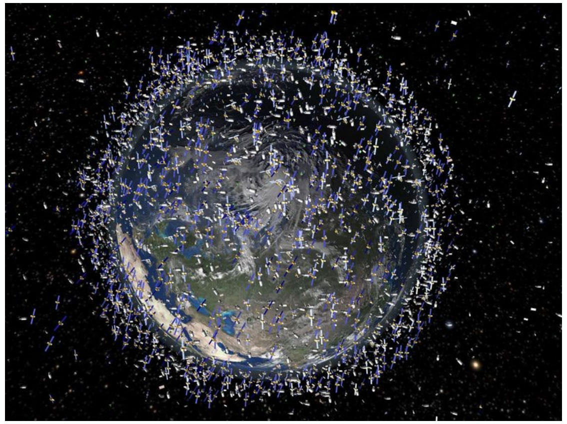
Minor – 50 discussed in splinters or offline
Major – 13 discussed in WG meetings



5. Major topics tackled

1. Alignment with ESA mission classification
2. CubeSats/Small Sats performing complex missions
3. Close Proximity Operations (e.g. in-orbit servicing, ADR, etc.)
4. Use of RAMS analysis for FDIR definition
5. Use of MBSE in FDIR definition
6. Use of AI and ML for FDIR
7. Identify constellations gaps
8. Identify ground segment gaps
9. Establish timeline of FDIR concept definition
10. Disposal
11. FDIR tools recommendation
12. Verification approach for FDIR
13. NewSpace

Postponed for next update due to delay in R&D activities



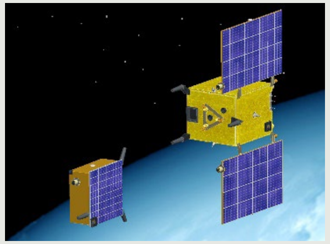
6. What’s New: FDIR Use Cases

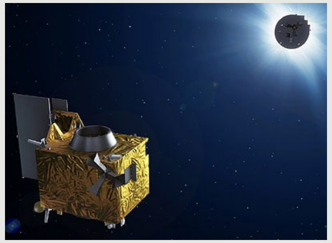
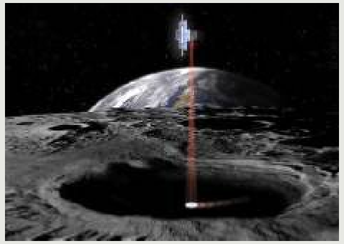
FDIR Use Cases

- ✓ The goal is to provide examples for missions that are more specific (i.e. less conventional), where different or slightly modified designs and processes may be more suitable

APPENDIX F - FDIR USE CASES 149
F.1 CPO Use Case #1: Cooperative Rendezvous Without Capture and Formation Flying 149
F.2 CPO Use Case #2: Cooperative Rendezvous With Capture 151
F.3 CPO Use Case #3: Non-cooperative Rendezvous without capture 155
F.4 CPO Use Case #4: Non-cooperative Rendezvous with capture 157
F.5 CubeSats Use Case 160

- ✓ Each use case includes a description, drivers for FDIR, tailoring needs (e.g., changes to the FDIR process, example missions, and lessons learned


6. What’s New: CPO Use Cases

Close Proximity Operations (CPOs) use cases added

✓Cooperative rendezvous without capture and formation flying

✓Cooperative rendezvous with capture

✓Non-cooperative rendezvous without capture

✓Non-cooperative rendezvous with capture

6. What’s New: CPO w/o Capture & FF

In cooperative rendezvous and formation flying missions, two S/Cs collaborate to achieve a common goal. Typically, one S/C, the chaser, performs thrusting manoeuvres while the other, the target, maintains a favourable attitude. The target S/C may also have active or passive elements to aid relative state measurement.

Drivers for FDIR:

- Need to detect and avoid collisions
- Need to manage small inter-satellite distances
- Need to handle FDIR separately for chaser and target S/C

Tailoring Needs:

- Incorporating specific drivers into requirements analysis, considering interactions between chaser and target S/C
- Ensuring FDIR capabilities without requiring direct communication links.

Example Missions:

- Proba-3, an ESA Formation Flying technology demonstration mission involving two small satellites to test and validate FF mission architectures and techniques

Lessons Learned:

- A master/slave approach for CAM execution allows for one S/C to initiate CAM, with the other acting as a backup if needed. This ensures efficient management of collision risks.

6. What’s New: CPO with Capture

Cooperative rendezvous with capture missions involve reducing the distance between two S/Cs to zero in a controlled manner, commonly seen in In-Orbit Servicing (IOS) missions. Like the previous use case, these missions entail a master/slave relationship where one S/C (the chaser) performs thrusting manoeuvres while the other (the target) maintains a favourable attitude. The target S/C may also have elements to enhance relative state measurement devices.

Drivers for FDIR:

- Need to detect and avoid collisions between the S/C and the potential lack of direct communication between them.
- Requirements for target capture impose the need for the chaser S/C to take over attitude control of the composite.

Tailoring Needs:

- Incorporating specific drivers into the FDIR requirements analysis
- Considering interactions between chaser and target S/C
- Ensuring the FDIR is capable of operating considering changes after capture.

Example Missions:

- Mars Sample Return – Earth Return Orbiter (MSR-ERO), tasked with capturing the Orbiting Sample in Mars orbit, where an uncontrolled collision could jeopardize the mission. IOS missions, such as satellite refuelling or repair, also fall under this category.

Lessons Learned:

- In MSR-ERO, failure detection relies on mechanisms within OBC1, but CAM execution is preferably handled by OBC2 for faster reaction times in certain scenarios, demonstrating the importance of efficient FDIR mechanisms.

6. What's New: CubeSats Use Cases

CubeSats, initially designed for educational and demonstration purposes

- Prioritize **cost and lead time reduction**
- Typically use **COTS components** and **streamlined design processes**

Poses challenges for FDIR due to the low reliability of parts and the need to exploit functional redundancies

Drivers for FDIR

- Limited budgets
- The use of potentially low-reliability COTS components
- The need for increased onboard autonomy due to limited power, mass, and size constraints.

Tailoring Needs

- Optional steps for FDIR requirements and concept definition
- Merging certain steps to streamline the process,
- Reducing documentation requirements
- Update of the DRL

Example Missions

- M-ARGO, a deep-space CubeSat exploring asteroids
- LUMIO, observing meteoroid impacts on the lunar far side
- VMMO, mapping lunar volatile and mineralogy.

Lessons Learne:

- High infant mortality rates
- Failure in communication and power systems
- Careful COTS selection
- Optimization power and communication subsystems
- Attention to flight software development,
- Mitigation of radiation effects
- Model Based Systems Engineering tools can aid in system design, including RAMS considerations.

6. What’s New: Lessons Learnt

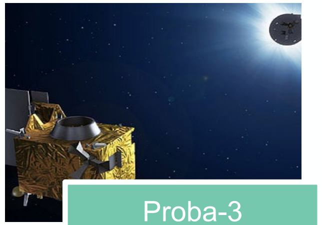
Missions and lessons learned and designs considered when updating:

- Proba-3
- Mars Sample Return – Earth Return Orbiter
- PRISMA
- ClearSpace-1
- Sunrise (ELSA-M)
- RISE (IOS)
- e.inspector
- M-ARGO
- LUMIO
- VMMO

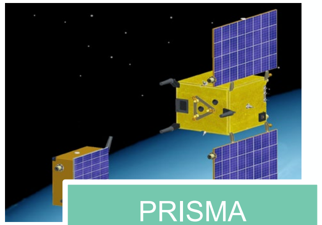
CPOs

CubeSats

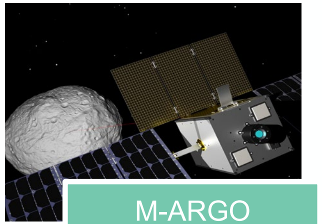
Included in the CPOs and Example Mission section in the FDIR use cases annex (F)


Proba-3


MSR


PRISMA


ClearSpace-1


M-ARGO

LUMIO


VMMO

6. What's New: Lessons Learnt

deimos esa

New structure implemented for LLs

easier consultation.

- Distinction between **guidelines/issues**
- Division of LLs in terms of **field of application**
- Identification of **applicable phases** in mission lifetime for each LL

D.2 FDIR ANALYSES

This subsection centers on lessons learned concerning the analyses related to the FDIR process.

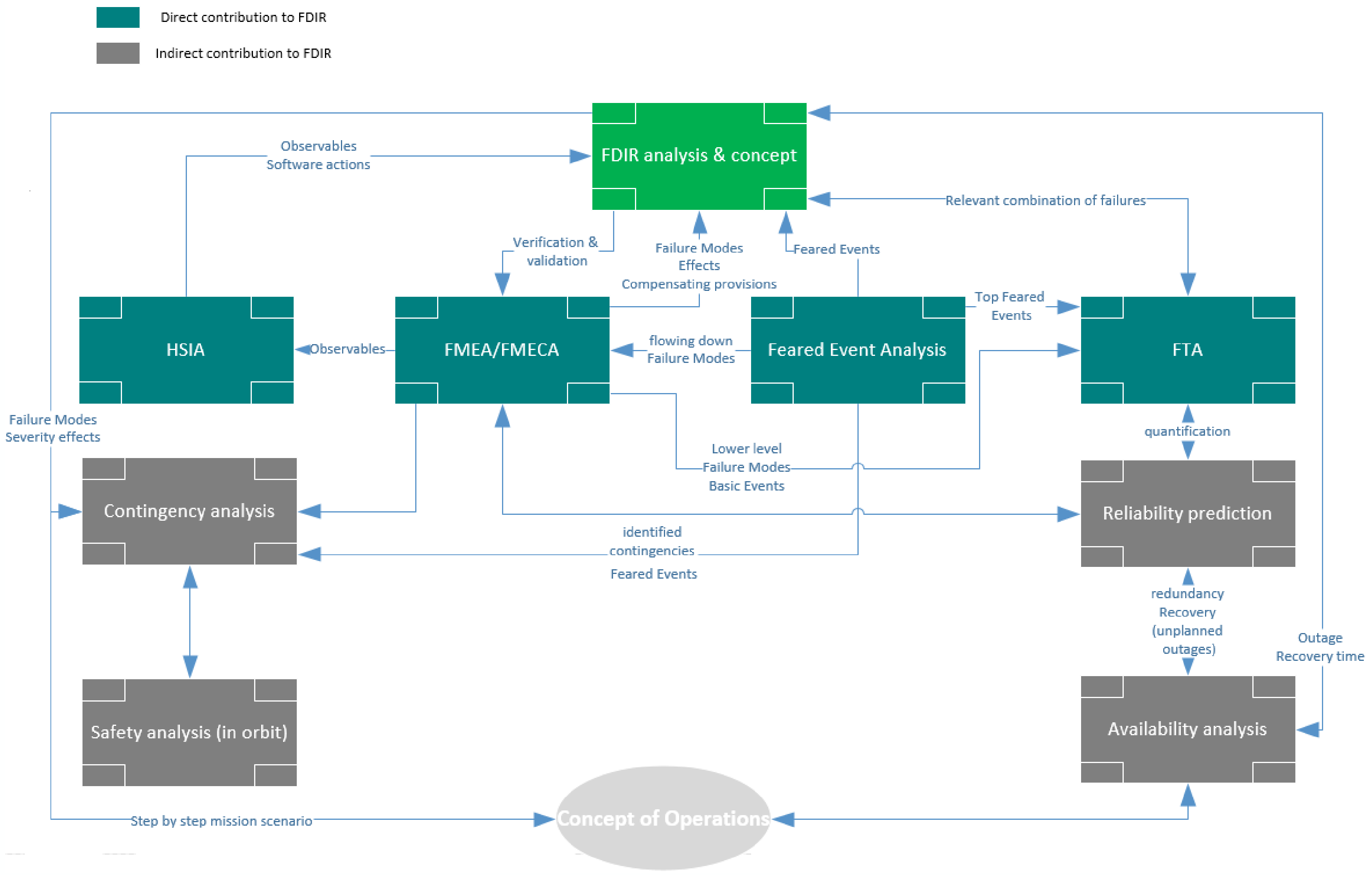
Issues highlighted by LLs:

- Incomplete or immature FDIR for a particular equipment or subsystem (or even system), missing traces of FDIR to FMECA (FMEA events not traced to FDIR or explanation of tracing is missing). — **A** **B** **C** D E
- Failure analysis (based on functional analysis and completed with FMEA) provides FDIR requirements to be inserted in high level specification; usually, FDIR requirements can be considered baselined only at the end of phase B when FTA and FMEA are available; this can be considered a shortcoming. — A **B** C D E

Guidelines in LLs:

- FMEA is not available; list of failures is derived by failure analysis that is based on functional decomposition of system. — **A** B C D E
- Incomplete analysis of system level feared events. — **A** **B** C D E
- FDIR heritage requirements shall be carefully analysed; it is recommended to have centralized, top-down FDIR requirements defined in response to a mission's risk posture and unique objectives (as opposed to inheriting FDIR requirements without re-analysis). — **A** **B** C D E

6. What's New: Relation to RAMS



Purpose:

- To better showcase the interaction between FDIR and RAMS (it is often noticed that this aspect is a constant lack in projects)
- To provide an easier read of the interactions between analysis.

6. What’s New: ESA Mission Classification

The ESA mission classification table, as of the date of preparing this presentation, is depicted here.

Class type	I	II	III	IV	V
Mission Criteria and Marking					
Criticality to Agency strategy (Flagship mission, Internationnal cooperation, Impact on ESA strategic goals, and image)	Extremely high Criticality	High Criticality	Medium Criticality	Low Criticality	Educational purposes
Marking					
Mission Objectives (Directorate priority and purpose, e.g in orbit demonstration, educational)	Extremely high Priority	High Priority	Medium Priority	Low Priority	Educational purposes
Marking					
Cost (Cost at Completion, Including Phase E1)	>700 M€	200 - 700M€	50 - 200M€	1 - 50M€	< 1M€
Marking					
Mission Lifetime (Nominal mission life duration)	> 10 years	5-10 years	2-5 years	1-2 years	1 year
Marking					
Mission Complexity (Design interfaces unique payloads, New technology development)	High	High to Medium	Medium	Medium to Low	Low
Marking					

For mission **Classes I, II, and III**, thorough adherence to the FDIR design and processes is expected and recommended, following all steps outlined in the HB from Step 0 to Step 6, including proposed reviews.

However, for **Classes IV and V**, where missions might be educational or have limited budgets, it's acceptable to skip some steps due to insufficient resources.

For **Class IV**, Steps 0 and 1 are optional, and Steps 3 and 4 can be merged and revised at CDR.

In **Class V**, typically educational missions, it's beneficial to go through all steps, but it's acceptable to skip Steps 0 and 1 and start FDIR concept at Step 2 due to simplicity.

Similarly, merging Steps 3 with 4 and Step 6 are optional for **Class V**.

Also, the recommended applicability of the FDIR steps per mission class can be found here.

Mission class	Step 0	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
I.	A	A	A	A	A	A	A
II.	A	A	A	A	A	A	A
III.	A	A	A	A	A	A	A
IV.	O	O	A	A		A	A
V.	NA	O	A	A		A	O

A – applicable
NA – not applicable
O - Optional

6. What's New: Recommendation of Toolsets

The following toolsets/frameworks are recommended to support the FDIR design, implementation, and verification process:

- GAFE – Generic AOCS/GNC Techniques & Design Framework for FDIR (http://gafe.estec.esa.int/)
- COMPASS – Correctness, Modeling and Performance of Aerospace Systems (https://www.compass-toolset.org/)

✓ More in general, it is recommended that **model-based FDIR** design toolsets are adopted whenever possible, either by adopting the frameworks listed above, or by implementing extensions of MBSE tools, such as Capella, CAMEO, and Enterprise Architect

✓ Several ESA studies have supported the development of the so-called Capella Viewpoints for FDIR and RAMS, including Reliability, Availability, FEA, FMECA, Safety and FTA viewpoints, in addition to proof of concept of FDIR viewpoints.

These toolsets/frameworks help ensure the proper implementation of the FDIR process, while also facilitating the verification and validation of the FDIR, and supporting the production of documentation.

7. Open Topics

- X FDIR based on Artificial Intelligence
- X FDIR based on MBSE
- X FDIR for Newspace
- X FDIR for ground segment

Information gathered from ongoing activities, but still insufficient for inclusion in the HB

Information gathered from ongoing activities, but waiting on the MBSE Hub to finish

Awaiting for mission classes finalisation and to advance with the internal WG activities; no work has been performed

Information gathered and added to the updated version, but limited to use for space segment and not FDIR for GS

All information gathered that is not captured in the updated version of the handbook is part of a dedicated TN that shall be used when a next update is requested

8. The New Release of the HB

The document is divided in **5 Chapters** and 7 Appendices. The content of each is the following (summarized):

Chapters

- ***Chapter 1:*** Introduction, Scope of the HB and reading guide.
- ***Chapter 2:*** Terms and Definitions.
- ***Chapter 3:*** General Overview of FDIR in the context of space mission design.
- ***Chapter 4:*** Detailed overview of the FDIR process in the context of ECSS.
- ***Chapter 5:*** Overview of the FDIR process, as seen from the main ECSS life cycle phase point of view.

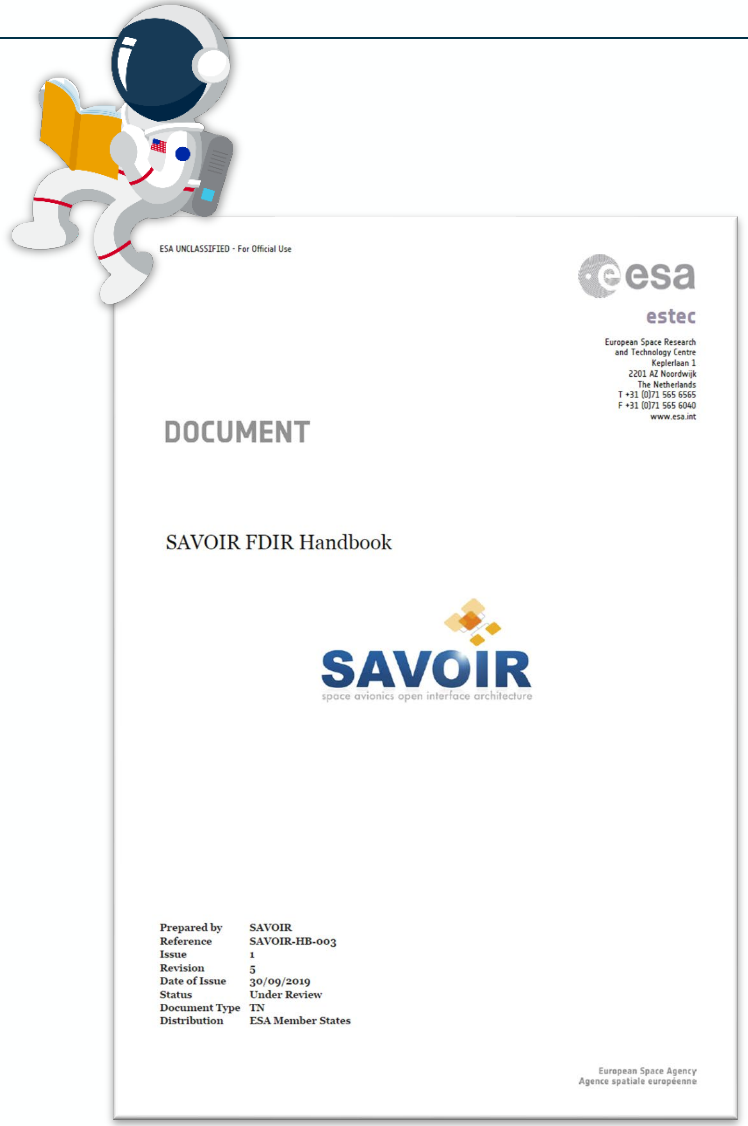
Appendices

- ***Appendix A:*** Backwards traceability of FDIR aspects from domain specific ECSS standards back to the process.
- ***Appendix B:*** Summarised document requirements list for the FDIR process.
- ***Appendix C:*** Document requirements definition for the key artefacts defined as outputs of the FDIR process.
- ***Appendix D:*** Overview of Lessons Learned.
- ***Appendix E:*** Recommendations on toolsets/frameworks to support the FDIR design, implementation, and verification process.
- ***Appendix F:*** Series of FDIR use cases, namely for Close-Proximity Operations (CPO) missions, as well as for CubeSats missions.
- ***Appendix G:*** Overview of the ESA Mission Classification current standard.

9. Closing Remarks

- **The SAVOIR FDIR HB represents a step forward towards the standardization of FDIR in Europe**
  - While not normative, it provides guidelines for cross-disciplinary aspects of the FDIR process, interfacing with other engineering disciplines
  - It is aligned with ECSS and other existing handbooks and technical notes
  - It contributes to a uniform understanding of FDIR drivers, requirements, processes, and interfaces, in Europe

- **New release (issue 3.0) of the SAVOIR FDIR HB coming soon!**
  - Currently under review by the SAVOIR Advisory Group
  - Expected release by Q3 2024


ESA UNCLASSIFIED - For Official Use

estec

European Space Research
and Technology Centre
Keplerlaan 1
2201 AZ Noordwijk
The Netherlands
T +31 (0)71 565 6565
F +31 (0)71 565 6040
www.esa.int

DOCUMENT

SAVOIR FDIR Handbook

SAVOIR
space avionics open interface architecture

Prepared by	SAVOIR
Reference	SAVOIR-HB-003
Issue	1
Revision	5
Date of Issue	30/09/2019
Status	Under Review
Document Type	TN
Distribution	ESA Member States

European Space Agency
Agence spatiale européenne

10. What's Next?

- **The SAVOIR FDIR HB provides a clear indication of the relevance of the standardization of FDIR in Europe**
  - The SAVOIR FDIR HB is the first step towards the elaboration of an ESA FDIR standard
  - This is a need identified by the different stakeholders of the space sector (ESA, the industry, research institutes, academia, etc.)

- **We'll continue promoting the use of the SAVOIR FDIR HB!**
  - ESA will provide dedicated training, upon project requests, already using the updated HB
  - Conference presentations expected during this year (IAC, ADCSS, etc.)
  - ESA will propose the FDIR WG to continue meeting 1-2 per year and keep in touch!

Stay tuned!

Thank you!