FDIR - state of the art and evolutions

TAS-F point of view

JM. Pasquet – R. de Ferluc – A. Provost-Grellier – B. Dellandrea

ADCSS– 21 OCTOBER 2015

Agenda

- Benefit and Lessons learnt from ESA studies on FDIR
- State of the art of FDIR process – development and validation
- New challenges
- Recommendations

THALES ALENIA SPACE France

FDIR ESA studies – overview

TAS-F have been involved in many ESA studies:

T
R
L

- **FAME (Failure and Anomaly Management Engineering)**
  - Definition of the FDIR development methodology and associated V&V process
  - Development of the Failure and Anomaly Management Engineering (FAME) Environment as an extension to COMPASS toolset.
- **FDI AOCS**
  - Improvement of AOCS, FDIR & Avionics for compliance with LEO de-orbitation new requirements
- **COMPASS**
  - develop a toolset for evaluation of system-level correctness, safety, dependability, and performance (performability) of the on-board computer-based systems.
- **COMPASS GRAPH**
  - Develop a graphical editor for SLIM models.
- **AUTOGEF (Automated Model Generation for FDIR)**
  - Development of the Automated Model Generation Toolset for FDIR (AUTOGEF) as an add-on to the COMPASS Toolset, and definition of the associated methodology. (Synthesize FDIR diagnosis and controllers in SLIM model for an given system).

Low TRL

FDIR ESA studies - TAS-F Benefits and Lessons learnt

Improvement of the FDIR process

- **All studies outputs taken into account to improve the TAS FDIR development process and associated tools for the new programs**
  - Harmonization/standardization of the FDIR Activities
  - Harmonization of documentation
  - Terminology

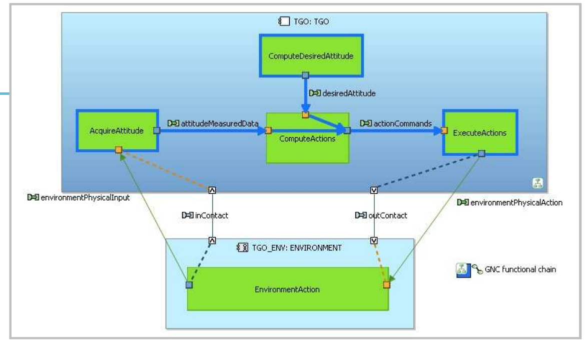
Evaluation of tools for FDIR Modeling , model checking and simulation

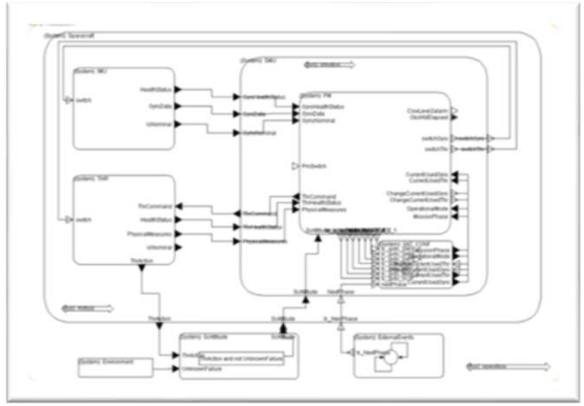
- **Not deployed in programs:**
  - Need to define properly what we want to prove with model checking (spec justification, design consistency , timing validation)
  - Toolset for automated FDIR synthesis is not mature

TAS-F Feedback

Way forward

- **Modeling and simulation shall be reinforced for new programs** :
  - Early consolidation of the system design (redundancy scheme, …)
  - Early validation of the FDIR design (FDIR strategy, …)
- **FDIR development process shall be supported by a dedicated toolset (editors, simulation, analysis tools)**





Opportunities

- **Develop of connection between COMPASS and Melody Advance (Capella)** will allow to optimize the FDIR Detailed Design
  - Melody Advance used in TAS programs to model system/avionics/equipment
  - Transition from MA to SLIM (architecture only) was prototyped (CNES study)
  - Nominal behavior and error models added at SLIM level, FDIR added at SLIM level
- **SLIM language to be improved to support efficient behavior modeling** (synchronization, timing aspects, …)
- **Couple FDIR analysis to Capella to avoid an additional cost for modeling activities**
- **Introduce FDIR in the AOCS simulator to validate early FDIR concepts and design**

Agenda

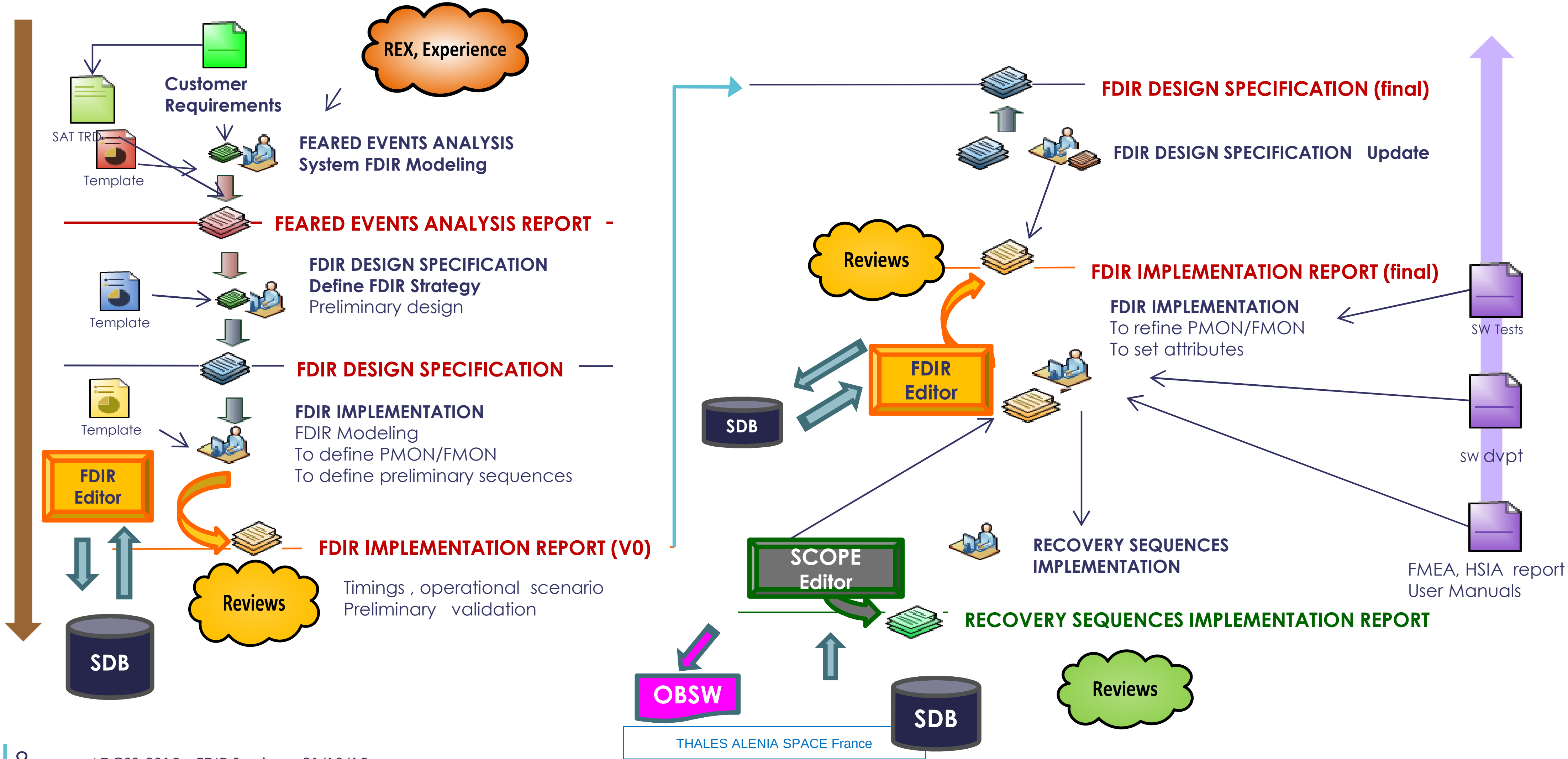
- Benefit and Lessons learnt from ESA studies on FDIR
- State of the art of FDIR process – development and validation
- New challenges
- Recommendations

The state of the art of the FDIR development and validation process

Applied Process

- **FDIR development Process is stabilized and tools are mature**
- **Process applied early in the preliminary design phase**
- **Continuous process along development to support detailed implementation**
- **Implication of system team, avionics team, SW team, RAMS team**
  - FDIR is a system activity
  - FDIR implemented in avionics

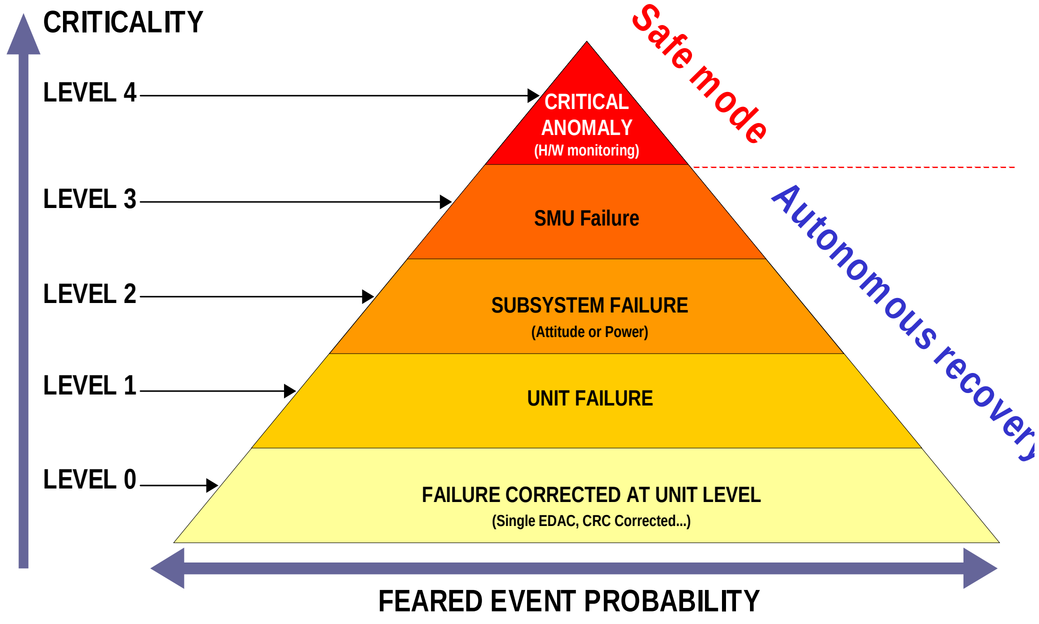
The FDIR development and validation process



FDIR process harmonization / standardization

FDIR process harmonization needs to converge on operational concepts

- **Operation Modes, satellite operational phases**
- **FDIR level & criticality :**
- associated to failure level (from the feared analysis)
  example : Level 1 : detected failure at unit level
- associated to recovery actions (from the FDIR strategy)
  example : Level 1 : recovery has no impact on the mission



- **SAFE mode concepts**
- Design rules , strong heritage
- New integrated avionics lead us to reconsider some design rules

Need to harmonize FDIR concept

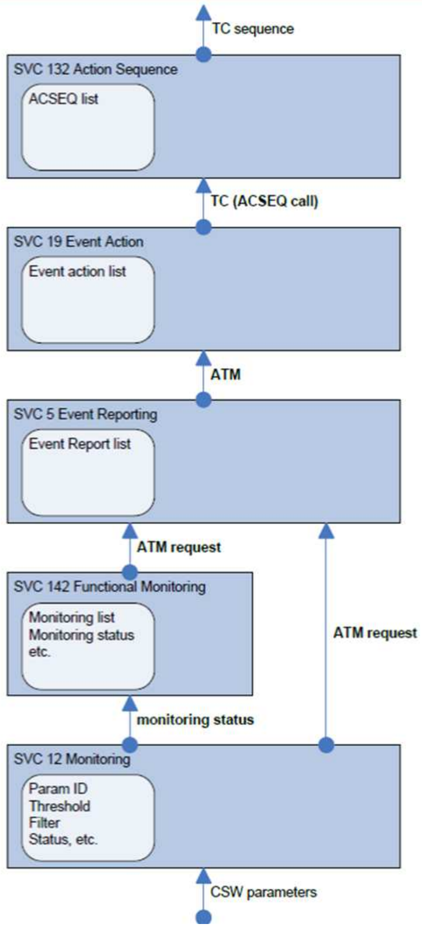
FDIR process harmonization / standardization

FDIR implementation : use of standard solutions is possible

- **Monitoring** : often based on OBSW . Parameter periodic checks associated to a filtering delay to confirm failure occurrence
- **Recovery :** implemented by a set of commands to be executed either by HW (Reconfiguration Module) and/or the OBSW

- **Standardization can be supported by the PUS :**
  - SVC 12 for Monitoring, including Functional Monitoring notion
  - SVC 19 for triggering Actions following failure detection (Event report emitted)
  - SVC 21 for Action sequences

Adopt standard solutions for a FDIR reference architecture



PUS services to support FDIR

FDIR implementation process must be supported by standard FDIR tools

Definition of the parameter set and associated threshold

- Bottom-up approach based on FMEA information ➔ must be supported by a standard toolset

FMEA sheets : a template shall allow automatic data collection

- Failure observability shall be identified in consistency with EDS (real telemetry)
- Thresholds shall be included in FMEA (degraded signal /level for instance)
- FMEA Format must be standardized to simplify extraction and traceability toward FMON definition
- Could be inserted in EDS

Tuning of delays and threshold to guaranty temporal separation between levels

- Verification of proper implementation of FDIR strategy must be supported by modeling and simulation tools
  - This stage is often performed by paper analysis and iterative validation
  - Can be supported by simulation (RHAPSODY, COMPASS ..) ➔ validation process to be optimized

To standardise FMEA sheets & harmonize/optmize verification process thanks to adequate tools

Agenda

- Benefit and Lessons learnt from ESA studies on FDIR
- State of the art of FDIR process – development and validation
- New challenges
- Recommendations

THALES ALENIA SPACE France

New Challenges

FDIR for deep space missions

- EXOMARS Reentry phase need AFO design to guarantee success of the mission in case of failure

FDIR for Geo Telecom Satellites

- Electrical Orbit Raising (3-6 months) with short visibility period require satellite autonomy
- Payload management autonomy and automatic reconfiguration are requested for some missions

FDIR for Large Constellations and COTS

- Large constellations require satellite autonomy for operation
- Introduction of COTS has to be compensated by fault tolerant architectures to support SEU/SET
- SOC approach will simplify redundancy schemes

Multicore computers

- Fault contention , fault detection, fault recovery

New Challenges

Reduce FDIR development costs

- Rely on standard mechanisms to support Failure monitoring and Failure recovery mechanism (PUS monitoring services, action sequences, OBCP)
- Use of FDIR editor to generate consistent action sequences
- Validation on simulators (SVF) and reduce the number of test on the real HW
- Simplify the FDIR strategy / automatons

- Introduce Fault Tolerant mechanism at low level to handle SEU/SET events

Agenda

- Benefit and Lessons learnt from ESA studies on FDIR
- State of the art of FDIR process – development and validation
- New challenges
- Recommendations

Recommendations

- Need for FDIR stabilized and matured process to support new challenges
- FDIR concepts harmonization shall be continued
- Introduce standardization of FMEA format and automated link with EDS
- Reinforced modeling in early phase , develop coupling between Capella and Compass to anticipate verification and optimize FDIR validation