FDIR variability and impacts on avionics :

Return of Experience and recommendations for the future

Jacques Busseuil
Antoine Provost-Grellier

Presentation summary

- **Survey of FDIR main features and in-flight experience if any for various space domains and missions**
  - Earth Observation (Meteosat Second Generation - PROTEUS)
  - Science missions (Herschel/Planck)
  - Telecommunication (Spacebus – constellations)

- **FDIR main features for short term ESA programs and trends (if any!)**
  - Exploration missions (Exomars)
  - Meteosat Third Generation (MTG)
  - The Sentinels
  - Met-OP Second Generation

- **Conclusion and possible recommendations**
  - From in-flight experience and trends

MSG (1) – FDIR Specification

The MeteoSat 2nd Generation has a robust concept :

- Spin stabilised in GEO : no risk of loss of attitude control
- 360° solar array : solar power available in most satellite attitudes
- on-board autonomy requirements :
  - GEO - normal operations : 24 hours autonomous survival after one single failure occurrence.
  - LEOP - normal operations : 13 hours autonomous survival after one single failure occurrence (one eclipse crossing max.)
  - GEO & LEOP - critical operations : ground reaction within 2 minutes

FDIR implementation to cover autonomy requirement

- Time criticality (in GEO normal ops)
  - criticality < 5 sec ➔ handled at unit H/W level
  - criticality > 5sec & < 24hours ➔ handled at S/W level
  - criticality > 24hours ➔ handled by the ground segment
- On-board autonomous actions classification
  - level A: handled internally to CDMU / DHSW: transparent wrt mission impacts. (e.g. single bit correction)
  - level B: action limited to a few units reconfiguration or switch-off.
  - level C: Payload switch off by DNEL
  - level D: Reconfiguration to the satellite safe mode

MSG (2) – Anomalies in flight

- Since 2002, anomalies recorded in flight leading :
  - To Safe mode :
    - Ground operation error e.g. mismatch between selected unit and FDIR
  - Various SETs on electronic components, generating false alarms handled at different FDIR levels:
    - equipment switch-over (i.e. RTU)
    - false DNEL triggering (PL off)
    - PM switch-over (safe mode)

Proteus missions (1)

The LEO Proteus PF :

- Five Missions have been based on (from JASON1 launched in 2001 to SMOS launched in 2009)
- The FDIR strategy is based on half satellite configuration, with the following drivers :
  - set the S/C in a safe state in case of problem
  - be robust to spurious events in order to preserve mission availability
- FDIR strategy implemented is :
  - Detection and Isolation on board – recovery on ground.
  - Two levels of isolation :
    - Safe mode
    - Unit isolation (switch off) for few units/modules : PL, MM, 1553, GPS

Proteus (2) – Anomalies in flight

- The following anomalies recorded in flight have triggered a safe mode :
  - On JASON 1 : 6 safe modes triggered, due to
    - Unit failures : Reaction Wheel and Tx
    - SET in RW
    - Ground operation error e.g. MM bank suspected in failure wrongly selected
    - Double EDAC in PM
    - NB: contractual life time 3 years, almost 10 years in flight
  - On Calipso : 1 safe mode, due to
    - SET in RW
  - On others mission, no safe mode triggered
  - Numerous anomalies recorded due to GPS constellation problem (maintenance ?!), no impact on the missions
  - Nota : PL anomalies not recorded as separately treated by Mission teams.

H/P (1) – FDIR Specification

Herschel and Planck : 2 missions on L2 based on the similar avionics :

- on-board autonomy requirements :
  - Satellite mission shall be maintained without ground contact for any 48 hours period during the operational life, assuming no major failure condition.
  - The spacecraft shall survive without ground contact for any 1 week period during the operational life

FDIR implementation to cover autonomy requirement

- 5 levels hierarchical FDIR strategy
- Autonomous Fail-Operational : mission continuity privileged for level 0 to 2 failure cases.
- Implementation of Safe mode (level 3) and Survival mode (Level 4) :
  - Safe mode : Earth Acquisition Mode and high data rate maintained
  - Survival mode : Sun Acquisition Mode and low data rate.

H/P (2) – Anomalies in flight

- The following type of anomalies have been recorded in flight :
  - On Herschel (launched in may 2009):
    - PL anomalies :
      - Erroneous monitoring – impact : equipment Off – Safe mode (level 3)
    - SET on Gyro : unit switch over
    - RAM overflow on STR : unit off or unit switch over
  - On Planck (launched in may 2009):
    - RAM overflow on STR : unit off or unit switch over
    - Transitory anomaly on I/O acquisition : reset I/O acquisition
  - No survival mode triggered
  - No anomaly induced by Ground

Typical Telecom customer FDIR requirements :

"For all mission phases, the satellite shall provide all necessary FDIR mechanisms to detect, isolate and recover autonomously from any failure with the objective to ensure satellite survival and to minimize mission outage and fuel consumption."

"In any case of failure detection and recovery, the satellite integrity shall be preserved even with no ground support."

"The satellite design shall be able to provide a safe mode in which the satellite shall be maintained into safe conditions in response to predicted critical failure such that further deterioration of the dynamic state of the spacecraft is prevented and in which is minimized the satellite on-board power demand including thermal regulation."

Which leads to the Principles and Architecture with the "classical" layered 5 levels of FDIR.

This is currently implemented on all Thales Alenia Space spacecrafts, both for GO applications (SpaceBus 4000, AlphaBus platforms) and low orbit constellations.

Telecom FDIR mechanism

FDIR overview :

- On-board FDIR system surveys a set of observables and, when an anomaly is confirmed as detected, triggers the predefined recovery action depending on the current FDIR state .
- The FDIR State allows the implementation of "escalation" of recovery actions, e.g. if the first recovery action was not successful on the next detection of the same fault, a harder recovery will be executed.
- On board FDIR shall be complemented by ground activities:
  - control and configure on board FDIR (enable/disable surveillances).
  - control directly equipments not critical for satellite safety (like TM function); or not monitored by on board FDIR (like TC redundancy).
  - perform anomaly investigation.
  - recover satellite from the SAFE to Nominal mode.

Spacebus – Anomalies in flight

- There are some lessons learned from in-flight anomalies:
  - All transitions to safe mode are due to operator errors (except one on SB3000)
    - Operators errors increase with the system complexity
  - Units most subject to reconfiguration:
    - RWL's due to SET (now the FDIR switch ON again the wheel autonomously)
    - STR for various reasons (straylight, SW bugs) for the first SB4000, no mission impact (hot redundancy)
  - SET are still a problem for the RWL's, much less on up-to-date electronics
- From these lessons learned, a major subject for customers is:
  - Fastest possible recovery from safe mode to normal mode
    - Transition using one TC only to be worked out
- They like the SB4000 FDIR as designed today
    - Good compromise between autonomy and complexity

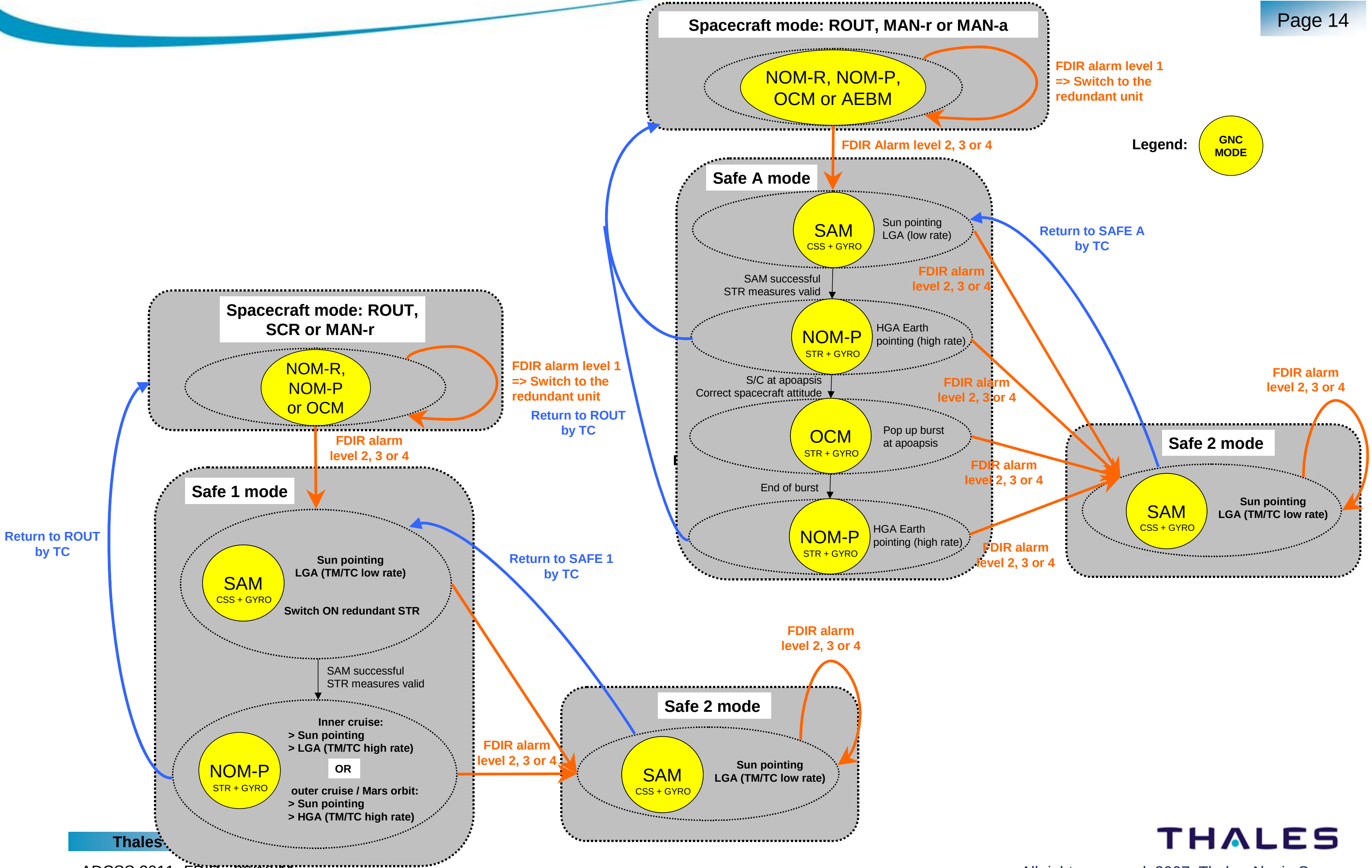
Constellations – Anomalies in flight

- There is not enough life time of Globalstar2 constellation to draw conclusions but for one point:
  - There has been a lot of problems to qualify the 1N thrusters for the required throughput (large amount of fuel for the required delta-V's and lifetime) and required ON/OFF cycles
  - This qualification seems not very reliable
    - Not always similar results for different thrusters at end of test
  - This does not question the FDIR which detects well the underperformance of thrusters
    - Either due to thrusters themselves or bubbles in the propulsion system
  - But there should be some work done to increase reliability of thrusters qualification
    - Especially for low thrust thrusters
    - Re-qualification for each program should be avoided

EXOMARS (1)

- EXM has a classical 5 levels (0 to 4) hierarchical FDIR strategy with the following exceptions linked to exploration mission:
  - « Fail-op « strategy during critical manœuvres (e.g insertion)
    - Redundant computer in warm redundancy as control shall be recovered in less than 10 secs
    - No transition to safe mode allowed, level 4 inhibited
    - Note that same strategy was designed for Mars Express and inhibited in flight
  - 3 safe modes are implemented
    - Safe 1 mode including classical SAM submode and NOM-P submode (STR, GYR and propulsion, HGA Earth pointed)
    - Safe 2 mode (SAM only) used when safe 1 or safe A mode FDIR triggered
    - Safe A mode used during Aerobraking phase
      - Risk of satellite damage or destruction
      - Includes transition to SAM, NOM-P, OCM (pop-up burst at apoapsis) and NOM-P

EXOMARS (2)


Spacecraft mode: ROUT, MAN-r or MAN-a
NOM-R, NOM-P, OCM or AEBM
FDIR alarm level 1 => Switch to the redundant unit
Legend:
GNC MODE
FDIR Alarm level 2, 3 or 4
Safe A mode
SAM
CSS + GYRO
Sun pointing LGA (low rate)
Return to SAFE A by TC
FDIR alarm level 2, 3 or 4
SAM successful STR measures valid
NOM-P
STR + GYRO
HGA Earth pointing (high rate)
S/C at apoapsis Correct spacecraft attitude
FDIR alarm level 2, 3 or 4
OCM
STR + GYRO
Pop up burst at apoapsis
FDIR alarm level 2, 3 or 4
End of burst
NOM-P
STR + GYRO
HGA Earth pointing (high rate)
FDIR alarm level 2, 3 or 4
Safe 2 mode
SAM
CSS + GYRO
Sun pointing LGA (TM/TC low rate)
FDIR alarm level 2, 3 or 4
Spacecraft mode: ROUT, SCR or MAN-r
NOM-R, NOM-P or OCM
FDIR alarm level 1 => Switch to the redundant unit
Return to ROUT by TC
FDIR alarm level 2, 3 or 4
Return to ROUT by TC
Safe 1 mode
SAM
CSS + GYRO
Sun pointing LGA (TM/TC low rate)
Switch ON redundant STR
SAM successful STR measures valid
NOM-P
STR + GYRO
Inner cruise:
> Sun pointing
> LGA (TM/TC high rate)
OR
outer cruise / Mars orbit:
> Sun pointing
> HGA (TM/TC high rate)
Return to SAFE 1 by TC
FDIR alarm level 2, 3 or 4
FDIR alarm level 2, 3 or 4
Safe 2 mode
SAM
CSS + GYRO
Sun pointing LGA (TM/TC low rate)

Meteo Third Generation - MTG

FDIR strategy will be driven by the following requirements :

- The primary objective of the FDIR shall be to detect any spacecraft condition (e.g. attitude, rates, orbit changes, etc.) that present a potential threat to the safety of the satellite and to correct any such condition and isolate the cause by means of transition to safe mode.
- The secondary objective of the FDIR shall be to maintain the operational condition of the satellite by the correct, timely and unambiguous detection of equipment and software failures, errors and anomalies, and the recovery of such failures, errors and anomalies by automatic software action and/or hardware reconfiguration.
- The on-board autonomy management functions shall be capable of performing all operations to safeguard the space segment for an autonomy duration of 48 hours in the presence of a single failure, reduced to 24 hours during LEOP
- To meet the required unplanned outage yearly percentage (I.e. reduced number of safe mode) shall be < 1%calculated on an annual basis for the duration of the satellite nominal operational life, with the assumption that the safe mode recovery duration is 48 hours

A classical approach with 5 level hierarchised strategy can be suitable

- but it is required to keep attitude mode continuity for up to level 3 for the PF anomalies.

Sentinels

FDIR strategy is driven by the following requirements :

- No single failure shall lead to Safe Mode
- The Satellite shall be able to maintain nominal operations even in presence of single failure cases affecting a subsystem, and without any need for telecommands from the ground control stations, for a period of at least 14 days.
- The attitude sensors and actuators involved in the ESAM shall be different from the sensors and actuators involved in the nominal Earth pointing mode
  - Two different approaches have been done between S1 and S3 :
    - On S1, an Ultimate safe mode has been introduced, with dedicated HW module to interface additional set of thrusters, CSS and CRS.

A classical approach with 5 level hierarchised strategy has been adopted for Sentinel 3

- With continuity of mission within level 1 failure recovery.
- Safe mode using few PF units : CSS, MAG, MTB, SMU, 2 RWs. Safe mode is re-entered in case of failure, with redundant pair of RW.

Met-OP SG

- FDIR requirements are still under discussion in the on-going phase A but there are 2 drivers:
  - Ensure mission survival whatever happens:
    - This has been put at an extreme level initially with requirements such as « no time limited survival with solar array deployment failed »
      - This has enormous system and cost impacts
    - Or such that the satellite shall be « robust » against **double failure**, combining double on-board failures or double operational errors or one of each (!!)
    - The Emergency and Safe Mode (ESM) shall use different (redunded) sensors and actuators than the ones used in other modes and a « separate » SW, and shall have its own FDIR
    - The ESM shall maintain a safe attitude with no use of consumable but also be able to do de-orbiting manœuvres and satellite passivation at the end of life time
      - ➔ ESM is at the end a complex safe mode, so less reliable…
  - Ensure operational mission at the maximum extent
    - More classical approach for operational missions but it is required (TBC) to identify and recover some instruments failures autonomously

Conclusions and recommendations

Conclusions

- Feed back from commercial market (where system availability is a must):
  - FDIR as designed today is a good compromise between system availability/autonomy and complexity
    - Additional complexity increase the risk of misunderstanding of the system behaviour by the operators and the risk of lack of full verification of the system (FDIR validation being a critical path for all programs)

- Overall in-flight REX:
  - Sensitive PF equipments are wheels and thrusters, which are often subject to anomalies or failures
    - STR sensitivity to environment has improved a lot
  - Payload equipments are also source of mission interruption (at minimum ..)
    - Design, Failure detection and FD validation to be improved
  - Electronics are subject to SEU/SET but simple redundancy scheme (FDIR level 1) is adapted for recovery
  - No problem in safe mode, although safe mode units and SW not segregated
    - Deep testing of safe mode is a general rule

Recommendations

- To shorten recovery time from safe mode for operational missions
- The new law on required EOL de-orbiting and satellite passivation has to be taken into account in the design and will impact the FDIR and safe mode for all Earth orbiting missions:
  - More robust delta-V capability EOL: which impacts? Specific mode and/or equipments?
- To harmonize FDIR system level requirements for all Earth observation satellites (at least ESA!) taking benefit of industrial return of experience on similar « operational services oriented » missions
  - And avoid unnecessary segregation of safe mode (which may be less reliable because less tested and more complex with FDIR required in this mode)
- To think about required P/L FDIR especially for operational services missions
  - Some Telecom customers start discussion on this matter
- To put some effort on actuators reliability improvement
- To pursue investments in model based robust FDIR systems for highly variable and uncertain systems
  - Especially for exploration where full autonomy is required