AOCS/GNC Autonomy and FDIR
Airbus challenges and way forward

ADCSS 2019, ESA/ESTEC Noordwijk

DEFENCE AND SPACE

P. Bergner, A. Falcoz, C. Hervas-Garcia, K. Lagadec, D. Reggio, P. Régnier, D. Thomas

14.11.2019

AIRBUS

Outline

- Introduction
  - Current and future trends regarding Autonomy and FDIR
  - Trade-offs and potential solutions
- AOCS/GNC FDIR Strategies
- AOCS/GNC FDIR Failure Detection & Isolation Improvements
- AOCS/GNC FDIR Engineering Process, Methods and Tools
- Conclusions and way forward

Current and future trends regarding Autonomy and FDIR

An evolving environment and highly demanding missions

- Architecture / Equipment evolution
  - Large Constellations: reduced redundancy at satellite level, limited to securing deorbit operations
  - Stringent objectives on recurring costs, simpler equipment, COTS with lower performances
  - Complex equipment implementing more functions, highly integrated components, Off-the-shelf equipment (COTS) / “black box”
  - NewSpace components more sensitive to radiation-induced effects (increased SEU rates)
    - Need to tolerate frequent unit outages,
    - fewer (technological) failure observables, poor or even lack of failure modes assessment
- Continuously increasing number of functional requirements
  - Orbital events detection
  - Mechanisms control: Antenna tracking, thrusters pointing, radiators
  - Controlled Re-Entry: new function(s) which may be dedicated to this phase
  - Collision Avoidance: capability to perform Delta-V soon after separation or Safe Mode
  - Electrical Propulsion: long Orbit raising phase to be automated
  - RdV, Separation
- New development processes
  - Autocoding
  - PUS-based FDIR

Current and future trends regarding Autonomy and FDIR

An evolving environment and highly demanding missions

- Stringent AOCS performances requirements
- Critical phases e.g. Orbit Insertion, EDL, RdV
- Critical pointing requirements for payload protection
- Robustness to long unavailability of equipment
  - (e.g. loss of STR during solar flares)
- Fail-Operational strategy even after critical failure
  - (e.g. OBC/RIU/PCDU, AOCS global criteria)
- Long autonomy period without Ground visibility
- Increased Mission availability requirements
  - requiring increased failure detection coverage
  - e.g. incl. performances degradation,
  - requires better failure isolation, more local reconfiguration

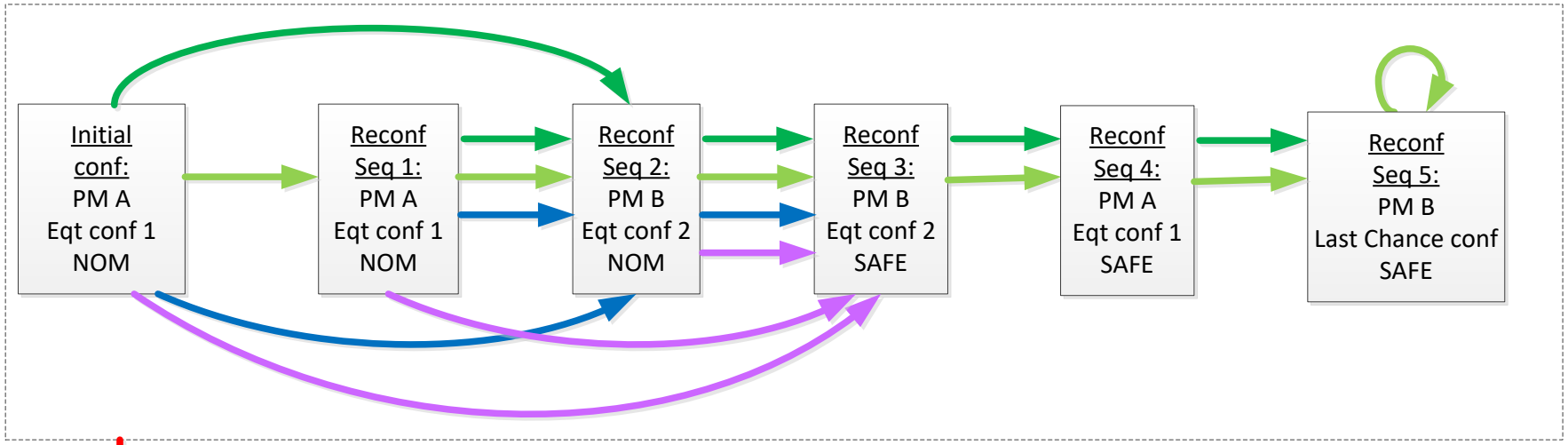
AOCS/GNC FDIR Strategies
Dealing with critical failures

- Critical failures considered:
  - Impacting the Data Handling System and / or the Software
    - e.g. OBC, RIU, PCDU failures
  - Impacting the Attitude / Rates:
    - actuators failure e.g. thruster open failure revealed through global criteria
  - Impacting the Energy: overconsumption, low battery SoC

- Potential solutions:
  - Hot redundancy < 2s
  - Warm restart < 10s
  - Cold restart to Nominal (e.g. after global reconfiguration) < 60s
  - Safe Mode to settle transients, then autonomous restart of critical sequence(s) < 5-60 min

AIRBUS

Example: “Warm” restart to Nominal Mode as first recovery for LEO/GEO



GROUND Commands

Desired Configuration: PM A or B Last Chance conf NOM or SAFE

L3a DHS FDIR	OBSW Failure (e.g. SW traps) => PM Reset (required) + All Platform units switched OFF-ON (=> OPS/SW design simplicity)
L3b DHS FDIR	OBC HW Failure (e.g. Bus controller, SpW I/O failures) => PM Swap (required) + all Platform units Swap (=> design simplicity)
L3b ADCS FDIR	ADCS functional criteria (attitude pointing error, wheel overspeed,…) => ADCS units Swap (required) + PM and all other Platform units Swap (=> design simplicity)
L4 FDIR	Power critical anomaly (deep battery discharge) => SAFE mode trig (all P/L and P/F units switch OFF, restart of a minimal set of P/F units)

=> System Restart mechanism = Watch Dog

AIRBUS

Considering STR use in Safe mode

RATIONALE & MOTIVATION

- In terms of FDIR architecture
  - Recent-generation STRs have an excellent in-orbit reliability record
  - Ever-greater maturity from accumulated flight-hours (wrt. dedicated safe-mode sensors)
  - Most safe mode events do not correspond to HW failures (less incentive for segregation)
  - No credible failure where STRs persistently provide a false attitude without it being flagged
- STRs are used on (almost) all missions
  - major source of genericity for future safe-mode architectures
  - major source of versatility for missions with complex safe-mode requirements
  - cumulative maturity/validation of safe-mode through convergence of architectures
- Operation benefits
  - unmatched observability for situational awareness and diagnostics
  - faster convergence and return to normal mode: large gains in mission availability
  - similar operations for safe modes on different missions

CAVEATS

- Vulnerability (angular rates, radiation, blinding)
- Imperfect reliability (esp. transient glitches, teething issues for new models)
- Might require STR-less backup for ultimate survivability

AIRBUS

ESA/ADS R&D studies on STR-based Safe-Modes

(Airbus DS SAS / Airbus DS Ltd / Jena Optronik)

Tier I (2014-2016) main results: STRs mature enough for use in safe mode

- assessment of STR reliability and failure modes / definition of FDIR approach
- modular safe-mode design approach with generic interfaces
- robustness assessment of the Astro-APS sensor by Jena Optronik
  - unaided acquisition with transverse angular rates up to 7 deg/s
  - tolerance to worst-case solar flares, direct sun illumination, worst-case thermal conditions
- detailed implementation and simulation campaigns for 2 very different reference missions
  - Aeolus (LEO) / Gaia (L2)
  - comparison to conventional safe mode performances

Tier II (2020-2021) main objectives: increase TRL/confidence even further

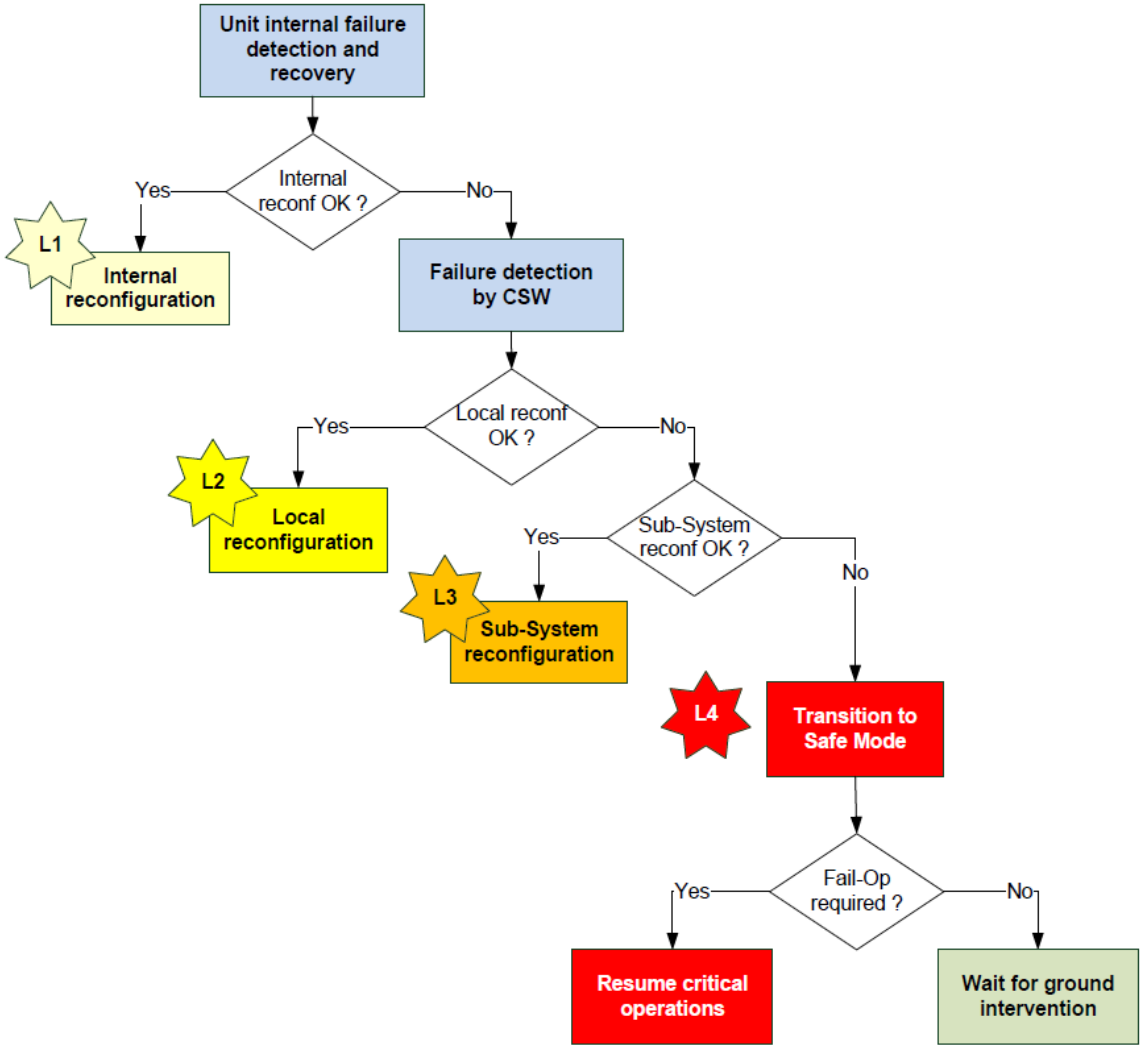
- further focus on science/interplanetary missions (requiring versatile safe mode functionality)
- additional robustness tests
  - combined high-rates/high-radiation situations, artefacts
  - other STR models tested (in addition to JOP's Astro APS)
  - cross-verification by independent testing facilities (AIRBUS DS's µSTOS)
- design of a generic STR-less functionality for initial convergence and backup sun acquisition
  - for ultimate survivability to cover risks of prolonged STR malfunction
- Star-tracker-in-the-loop real-time simulations on new reference missions

AOCS/GNC Autonomy & FDIR

AIRBUS

Resuming critical operations autonomously after transition to Safe Mode

- Transition to Safe Mode for tranquilisation
- Backup MTL used to store and restart the critical sequence of commands.



AIRBUS

Safe / Survival Modes (esp. interplanetary)

- ***Safe Mode***
  - Sun Acquisition phase, Solar Array towards the Sun for a safe power supply
    - e.g. Attitude estimation with SS and GYROs
    - and control with RCTs
  - Safe Hold Mode with 3-axis control, Antenna towards Earth for RF comms
    - e.g. Attitude estimation with STR and GYROs and control with RW
    - incl. autonomous off-loading

- ***Survival Mode***
  - If 3-axis attitude cannot be acquired or maintained
    - (e.g. STR not available, Earth ephemerides not valid or after several failed SAM/SHM loops),
  - the spacecraft automatically enters *Survival Mode* with Earth Strobing i.e. Sun pointing attitude with small rate about the Spacecraft-to-Sun direction. Antenna off-pointed with an angle equal to the Earth-Spacecraft-Sun angle loaded on-board

AIRBUS

Example: Airbus FDIR strategy for critical insertion manoeuvres on interplanetary missions (1/2)

First ESA interplanetary missions with Airbus-built spacecraft :

- **Rosetta :** no time-critical trajectory manoeuvre (classical FDIR concept = ΔV interruption & Safe Mode)
- **Mars Express / Venus Express :** heritage from Rosetta => inhibit FDIR surveillances (accepting higher vulnerability to HW failures)
- **BepiColombo :** no time-critical trajectory manoeuvre, but an independent OBC monitoring S/C attitude with gyros and Sun Sensors to ensure safe Sun-pointing

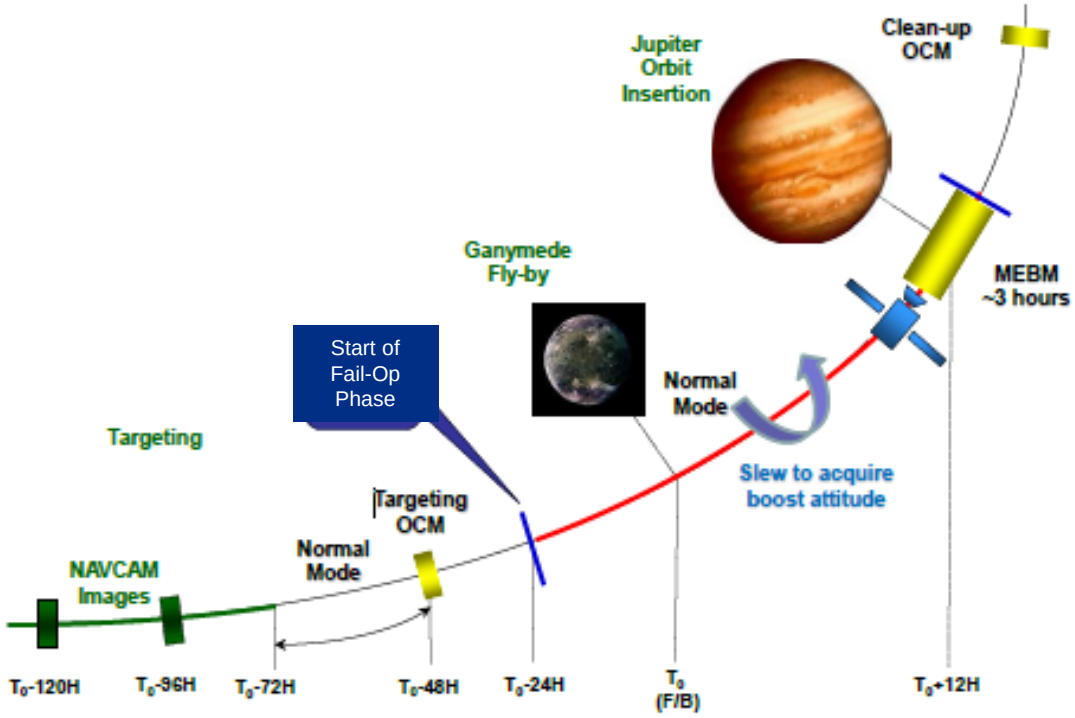
JUICE

- **(and other interplanetary missions with time-critical insersion maneuvers)**
- Cornerstone missions that **must** implement Fail-operational insertion manoeuvres
- **Envisaged solutions :**
  1. Hot reduncancy: CSW running on second OBC in parallel
     - ready to take control in less than ~2s, avoiding Safe Mode
  2. Warm redundancy: 2nd OBC in Stand-By, ready to launch application SW
     - taking control in less than ~5s, after retrieving context data, avoiding Safe Mode
  3. Resume after Safe Mode: only one OBC in cold redundancy,
     - Safe Mode is triggered in case of FDIR alarm, ΔV manoeuvre is resumed autonomously
- **Trade-off criteria to be addressed :**
  - Mission efficiency (ΔV penalties if any, mass and power impacts…)
  - Robustness to failures (HW and operators…) and unanticipated events
  - HW/SW/operations complexity
  - Functional validation complexity (and achievable completeness)
  - Compatibility with specific mission features like main engine restart (soak-back constraint), large deployed solar arrays flexibilities

Example: Airbus FDIR strategy for critical insertion manoeuvres on interplanetary missions (2/2)

JUICE baseline solution = resume after Safe Mode :

- Simplest solution at HW/SW/operations levels
- Best robustness to all types of failures
- Affordable functional validation
- Reasonable impacts at mission level : ΔV resumed after ~10 minutes only, ΔV penalty minimised by slight de-optimization of nominal burn timeline



Resume after Safe Mode solution enablers :

- **Ground-uplinked attitude guidance profile in Safe mode** :
  - Used in flight by ESOC operators on Bepi-Colombo
  - Stored in OBC or SGM EEPROM memory
  - Allows to force the boost attitude in Safe Mode
- **STR-based Safe mode** :
  - Sun search phase is bypassed after Rates Reduction Phase (RRP)
  - Direct transition to STR-based 3-axis attitude acquisition and autonomous slew to ground-commanded attitude
  - STR blindings avoided by proper selection of attitude angle around ΔV inertial direction
- **Insertion manoeuvre command sequence defined in Back-up Mission Timeline activated after Safe Mode convergence** :
  - Stored in OBC or SGM EEPROM memory
  - Commands executed at ground-defined absolute dates or shifted in time, depending on failure occurrence time wrt boost sequence

AIRBUS

Failure Detection & Isolation Improvements

Single parameter monitoring e.g. Limit Check is limited

Functional surveillances vs technological surveillances.

- Functional surveillance can be more generic and independent from the equipment itself. They usually allow covering a large scope of failure modes.
- On the other side, functional surveillance may require more tuning effort while technological surveillances can be fixed for given equipment and can provide faster failure detection time.

Better failure detection & isolation:

- Allowing local reconfiguration minimizing the mission impact
- Allowing optimized (reduced) redundancy at system level
- Avoiding costly investigation on ground

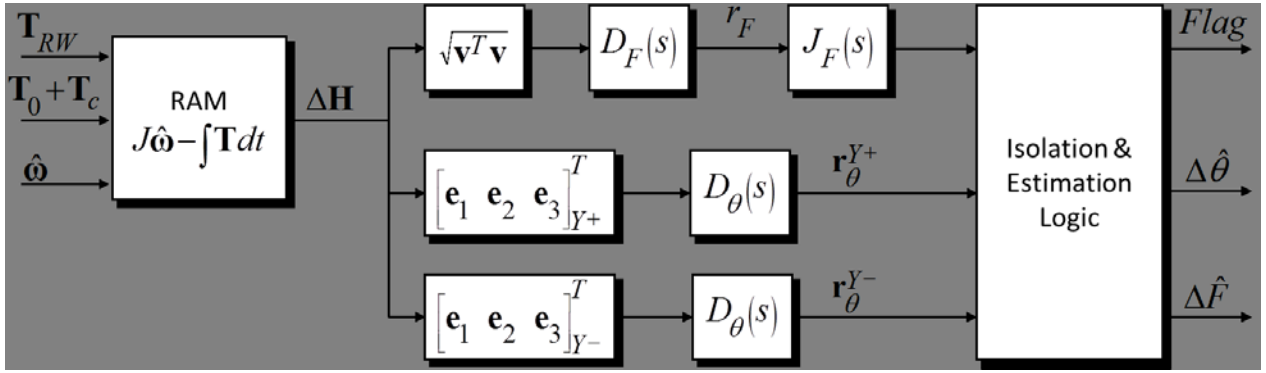
Solution: multi-variables functional failure detection

- Model-Based FDI
- AI / Machine-Learing based FDI

Model-Based FDI

Rationale

- each sensor or actuator failure can be identified via its distinctive dynamic signature
- residual momentum (i.e. modelled vs. measured) as a key indicator
- indicator is filtered to detect failures while avoiding spurious triggering
- isolation capability (unless degeneracy) by designing mutually orthogonal filters



Benefits

- much more sensitive *and* much more specific than catch-all threshold approaches
  - faster detection, fewer false alarms
  - large benefit in dynamic scenarios (e.g. agile slews, station-keeping maneuvers)
- combined failure detection and isolation
  - allows fault-tolerant designs (compensation by remaining units, reconfiguration on-the-fly)

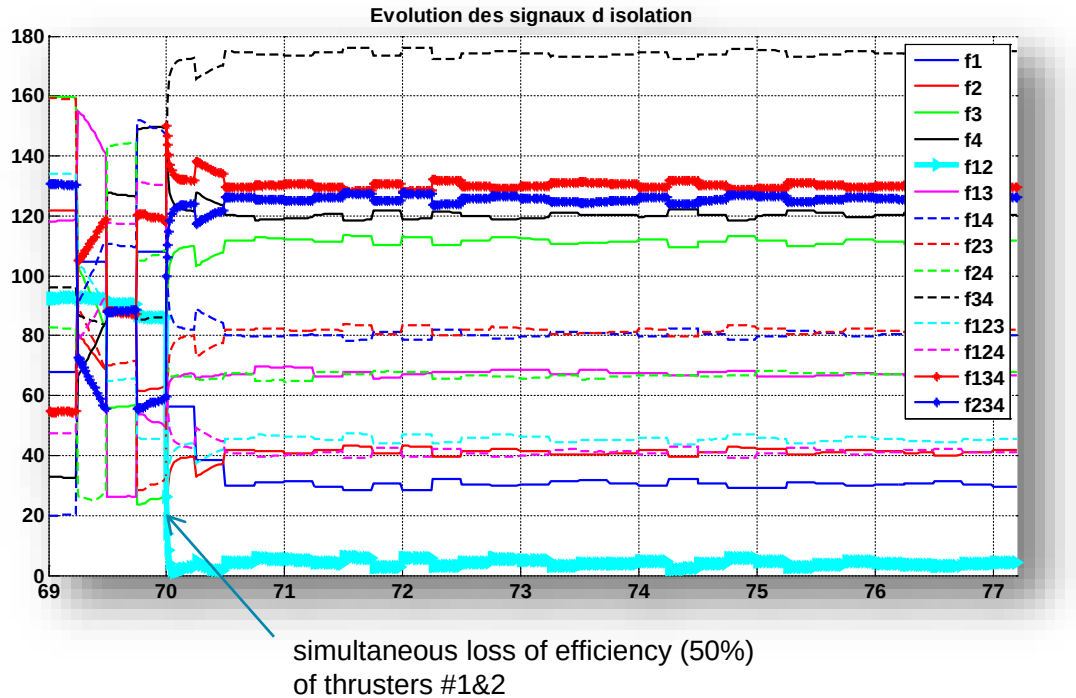
Model-Based FDI: implementation cases and performances

CNES, 2014-2015: application to DTMA failure detection

Failure\Index			C-FDI	A-FDI				
			PD	PD	PI	PW	PM	PF
DTMA YP	Failure	θ1	0,0%	98,7%	98,7%	0,0%	1,3%	0,0%
		θ2	0,0%	97,7%	97,7%	0,0%	2,3%	
		θ3	0,0%	100,0%	100,0%	0,0%	0,0%	
	Bias	θ1	0,0%	100,0%	100,0%	0,0%	0,0%	
		θ2	0,0%	99,2%	99,2%	0,0%	0,8%	
		θ3	0,0%	100,0%	100,0%	0,0%	0,0%	
DTMA YM	Failure	θ1	0,0%	98,2%	98,2%	0,0%	1,8%	
		θ2	0,0%	98,3%	98,3%	0,0%	1,7%	
		θ3	0,0%	99,9%	99,9%	0,0%	0,1%	
	Bias	θ1	0,0%	100,0%	100,0%	0,0%	0,0%	
		θ2	0,0%	98,9%	98,9%	0,0%	1,1%	
		θ3	0,0%	100,0%	100,0%	0,0%	0,0%	
THR	5%-100%	YP	100,0%	100,0%	100,0%	0,0%	0,0%	
		YM	100,0%	100,0%	100,0%	0,0%	0,0%	
MEAN (14000 run)			**14,29%**	**99,35%**	**99,35%**	**0,00%**	**0,65%**	**0,00%**

Method and System For Detecting [...], patent WO2016181079

CNES, 2014: transient and multiple thruster failures



Procede de controle d'attitude d'un engin spatial, patent FR3066029A1

AIRBUS

AI applied to AOCS FDIR: SMART-FDIR internal R&T

Investigating deep-learning techniques as a new approach towards L2/L3 FDIR

Objectives:

- Increasing spacecraft availability and autonomy by capturing more safety critical failures at L2 (reducing the number of failures that propagate into L4)
- Reducing the risks and efforts of designing the FDIR towards a particular set of feared events and failure modes
- Reducing the FDIR design and tuning effort as the algorithms are “learnt” simulated data

Achievements so far:

- In-house *unsupervised* adversarial deep learning technique (MODISAN) offering both detection and isolation (to equipment level) in order to replace L2 algorithms
- Benchmark of SMART-FDIR vs Classical FDIR on GYR-FSS Solar Orbiter use case with promising results
- Characterisation of the OBC/processing power requirements for different MODISAN architectures

Current (C) work and next steps (N)

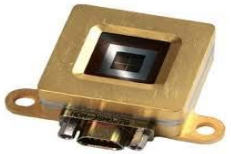
- (C) Assessment of SMART-FDIR impact on the FA chain
- (C) Application to on-ground telemetry processing (as a prior steps to flight)
- (C) Study and demonstrate embed-ability on current and/or future space graded HW
- (N) Early in-orbit demonstration

SMART FDIR

GYR-FSS use case

Gyroscope

Fine Sun Sensor

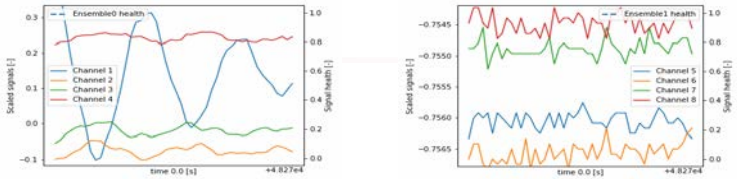


Inputs:

- 4 Gyro Channels
- 4 FSS quadrants currents

Outputs:

- Health Gyro
- Health FSS



2300h
of simulated telemetry

AIRBUS

AI applied to AOCS FDIR: Supervised Learning

Supervised Learning for GYR use case in satellites.

GYRO FROZEN use case: the gyros may freeze and output a constant angle increment leading to estimation error of the rotational speed

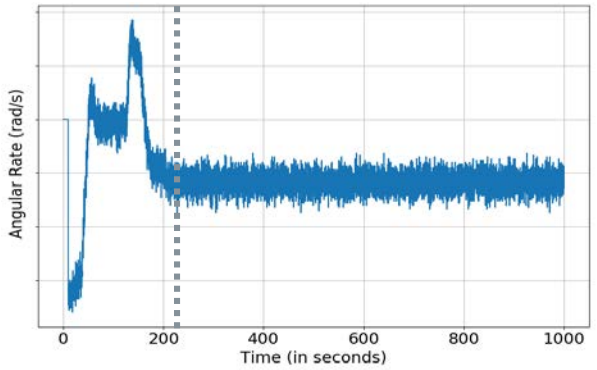
Current methods used to detect these failures are quite complex to implement as they need a lot of manual tuning

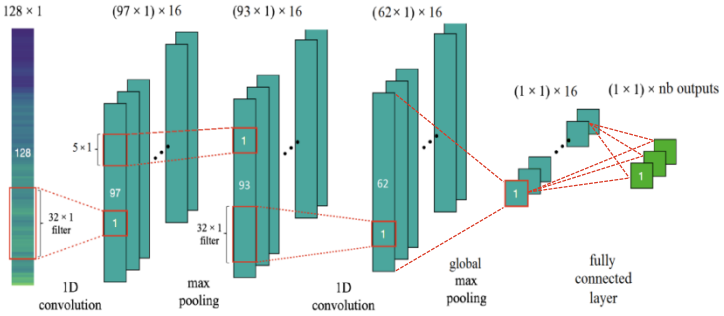
- Supervised deep learning achieved very promising results in this problem since there is clear definition and characterisation of the failure mode and it can be simulated

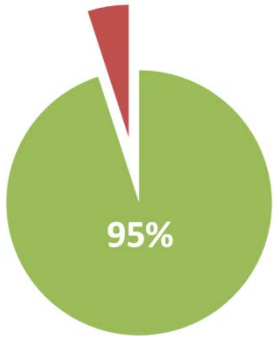
A CNN was used in order to detect 95% of the injected failures in less than 10 seconds with zero false triggering during nominal simulations

Whilst one of the biggest strengths of the unsupervised learning approach (e.g. SMART-FDIR) is that it offers the possibility to detect any failure mode that we may have missed or do not know yet, it is believed that some specific problems (e.g. gyr frozen or thruster stuck open/close) can greatly benefit from the supervised approach.

A combination of “unsupervised” + “supervised” methods is possible







AIRBUS

AOCS/GNC FDIR Engineering Process, Methods and Tools

Improvements in AOCS/GNC FDIR are also achieved through Process, Methods and Tools

- Re-enforced AOCS / FDIR co-engineering process for feared events identification, failure detection and mitigation selection, failure recovery strategy definition ensuring consistency at System level
- FDIR Handbook: Key principles, design rules and guidelines (e.g. tuning) to master the complexity
- AOCS High-Fidelity Functional Simulator which can import System FDIR configuration
- Generic AOCS/GNC FDIR Framework

GAFE – Generic AOCS/GNC FDIR Framework

Overview

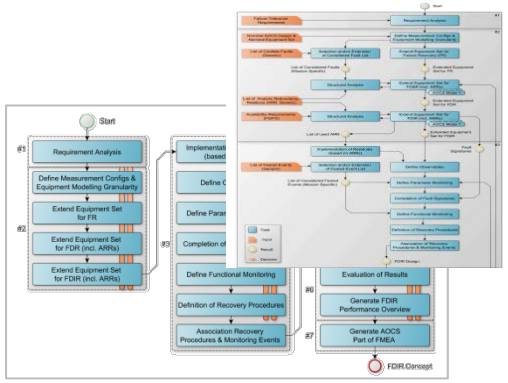
- GAFE was an ESA GSTP study conducted between 2015 and 2018 by Airbus DS Friedrichshafen, Astos Solutions and University of Stuttgart (iFR)

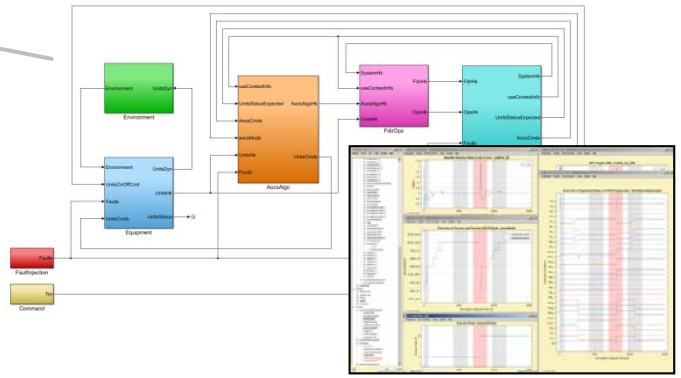
Objective

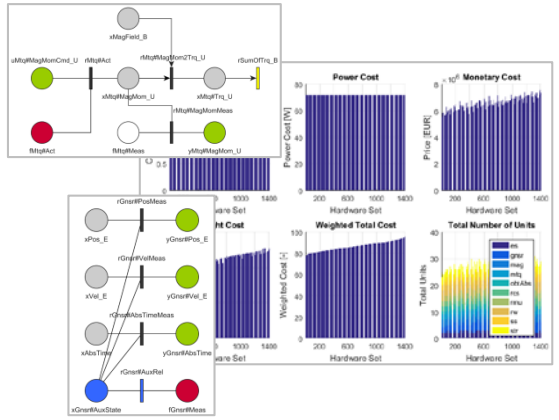
- “Develop an engineering approach & prototype tools to support AOCS/GNC FDIR design and V&V in early project phases”

Results

- **GAFE Framework**, consisting of:
  - GAFE Methodology
  - GAFE Structural Analysis
  - GAFE Simulator







Download

- gafe.estec.esa.int

GAFE – Generic AOCS/GNC FDIR Framework

GAFE Features that support FDIR Design and V&V for Autonomous Missions

- **FDIR Module** providing FDIR related PUS services: parameter monitoring (S12), functional monitoring (S142), fault recovery mechanisms
- **OPS Module** enabling event based operational actions. Example for OPS concept in AOCS safe mode
  - If attitude & rate control errors are below 3° & 0.1°/s for 100s in a row, switch on STRs and GNSR.
  - If STRs and GNSR are in look for 3 min, perform transition to AOCS NOM and switch off Safe Mode equipment → allows automatic mission progression or resume after failure
- **System Configuration Manager** handling “system configurations”, OBC reboot incl. delays, AOCS mode after reboot (e.g. ASM, NOM, same as before), functional chain selection, equipment power cycling, use of context information (SGM), FDIR enable/disable
- **AOCS Mode Management** with conditional main/submode switching and “mode in preparation concept”
- **Equipment Manager** with table driven selection of equipment set to be used, aggregation of equipment set status and support for equipment reconfiguration after failure
- **Generic Equipment Modelling** including operational state machine, standardized status I/F, fault handling (injection, ejection, persistency & performance influence)
- **Libraries**
  - **AOCS/GNC Algorithms Lib** with parametric configurability, generic interfaces, status concept with validity propagation, multi-rate sampling, systematic state collection (for: SGM, set/reset and monitoring)
  - **Equipment Model Lib** with 10 sensor and 3 actuator types, SADM and antenna pointing mechanism

Points of Contact: Domenico.Reggio@airbus.com (Airbus DS), Alvaro.Martinez.Barrio@esa.int (ESA)

AIRBUS

Conclusions

New AOCS/GNC FDIR challenges are coming

- Stringent AOCS performances requirements not only for mission availability but also for its safety
- New control functions
- New equipment, less known, new architectures

We have developed promising solutions

- Earth pointing Safe Mode for LEO/GEO, Star-Tracker based Safe Mode
- Several Fail-Operational strategies to recover critical failures and maintain mission and / or ensure critical sequences execution
- AI-based failure detection and isolation
- Independent safety monitoring

Potential impacts and risks

- Process could be affected e.g. AI providing solutions without the need for FMEA but maybe requiring more testing
- Implementing more FDIR can be counterproductive (increased risk of false positive)
- More autonomy can lead to less determinism, more actions on ground to reconstruct what is done on-board

Way forward

- Strong (cross-discipline) process
- Generic Framework(s)

AIRBUS

Thank you!