FDIR DD&V
From Behind the Scene to Front Stage

Armin Schwab [1)], David Pecover [2)], Yves Mulet [3)], Jean-Francois Gajewski [3)], Enrico Noack [4)]

[1)] Astrium GmbH, Earth Observation, Navigation and Science, Friedrichshafen, Germany

[2)] Astrium Limited, Earth Observation, Navigation and Science, Stevenage, United Kingdom

[3)] Astrium SAS, Earth Observation, Navigation and Science, Toulouse, France

[4)] Astrium GmbH, Space Transportation, Bremen, Germany

All the space you need

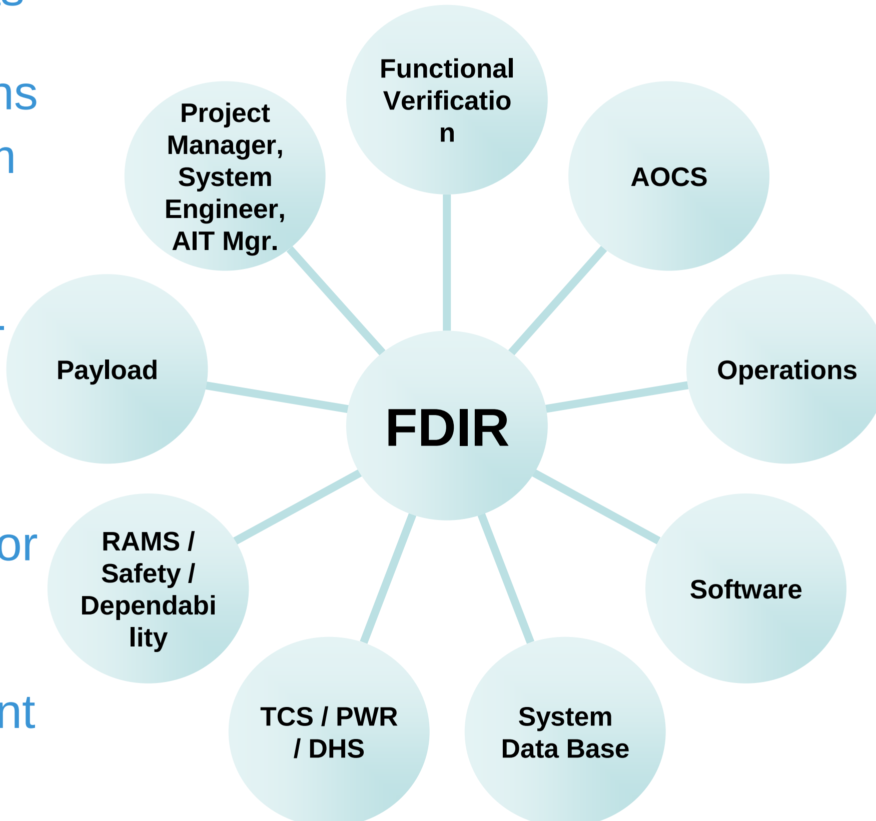
ASTRIUM
AN EADS COMPANY

Topics

- Key Challenges of FDIR
- Key Factors for Mastering FDIR
- Key Aspects of cost efficient S/C Operations and FDIR
- Improve Efficiency of RAMS/FDIR process
- Key Factors in measuring FDIR complexity and cost
- FDIR in Low Cost Missions – Myriade
- FDIR DD&V for cost efficient Columbus Operations

Key Challenges of FDIR DD&V

- Identify functional design requirements from high level primary mission requirements as well as from secondary system design objectives, targets and boundary conditions
- Develop in early project stages the system functional capabilities and assignments despite lack of final system design details
- Manage and integrate the emerging multi-discipline, highly dynamic and iterative detailed design feedback into the FDIR design and development
- Define verification strategies and means for functions, which often are not testable on the flight model
- Keep the solutions simple and cost efficient
- Monitor and master these aims over the complete product life cycle.



FDIR is an elementary System Engineering Discipline

Key Factors for Mastering of FDIR

- Improve awareness regarding RAMS / FDIR activities of management and technical teams :
  - Know what they have to do and why
- Get the involvement of each in accordance with the overall and common RAMS / FDIR Policy
  - Know their role and responsibility
- ➢ Establish FDIR as explicit functional operational system engineering discipline ⬄ Astrium MPC Operation and FDIR
- Improve efficiency of the RAMS / FDIR Process:
  - Communicate on the available methodologies and tools
  - Explain to relevant contributors, the objectives and application of methods and tools
  - Investigate and assess model based development approaches
  - Consider system-of-systems engineering approaches
  - Measure FDIR complexity and cost over the complete product lifecycle

Key Aspects of cost efficient S/C Operation and FDIR

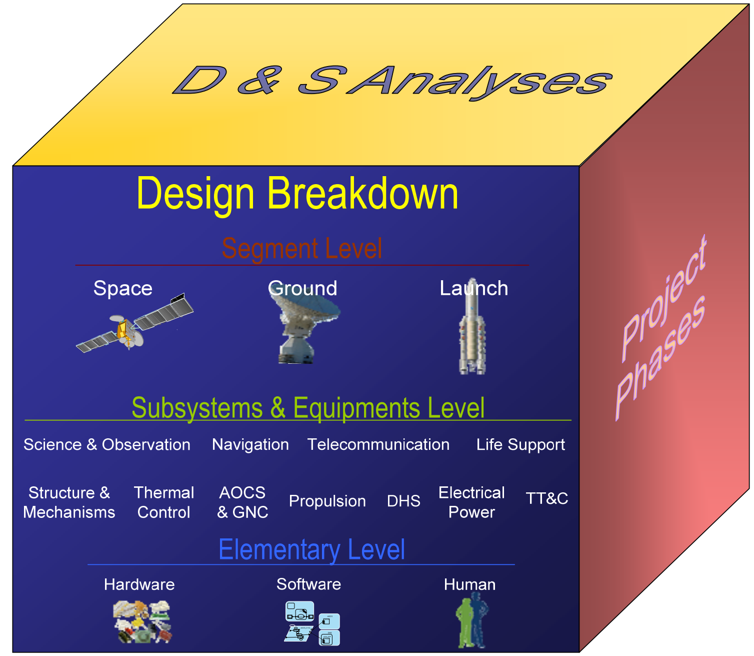
- Flexibility of the satellite design to provide capabilities
  - For the S/C operator to allocate which of the redundant units are included in the nominal chain and which in the redundant chain.
  - For at least one alternative configuration that can achieve the same function using different on-board units.
  - To access well-defined inputs and outputs from the ground for workaround solutions in case of contingency operations.
  - To provide resizable on-board data reporting, forwarding, storage and retrieval functions to cater for non-nominal mission events.
  - To support scalable on-board FDIR and autonomy by integrated S/C configuration management for nominal and failure cases and application of a service based hierarchical controlled implementation

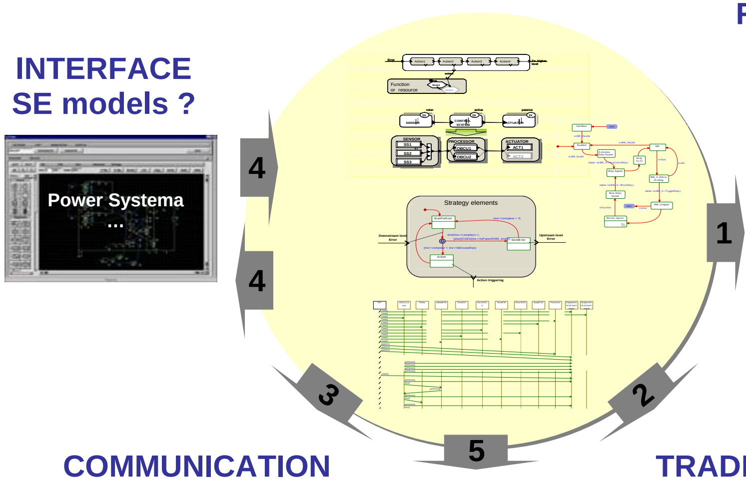
The FDIR concept directly impacts availability

- On-board Autonomy vs. Ground Controlled Operation
  - On-board autonomy is required to bridge non-coverage periods
  - Assess operation cost versus increased implementation cost

Improve efficiency of the RAMS / FDIR Process

- Tools and Methods Awareness
  - Failure Modes and Feared Events Catalogue allowing to combine RAMS, FMECA and functional operational design solutions
  - Principle and Guidelines Training
- Model based FDIR Engineering





Re USE

RAMS & FDIR PROCESS

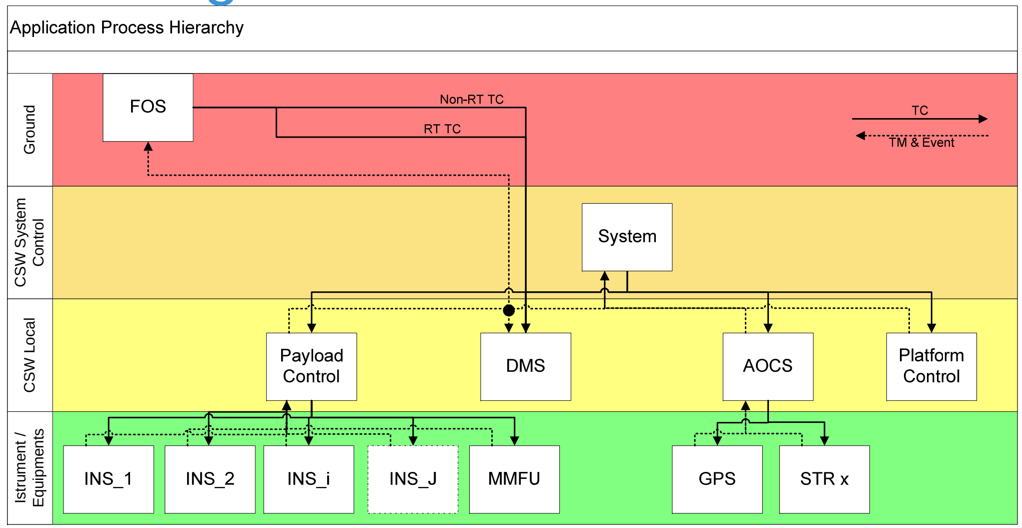
- System description
- RAMS & FDIR analysis
  - Support for analysis
  - Verification of Properties
  - Traceability of Rqts
- Automatic generation
  - R/A Prediction
  - PRA
  - FMECA/HSIA
  - FTA
  - Reports …

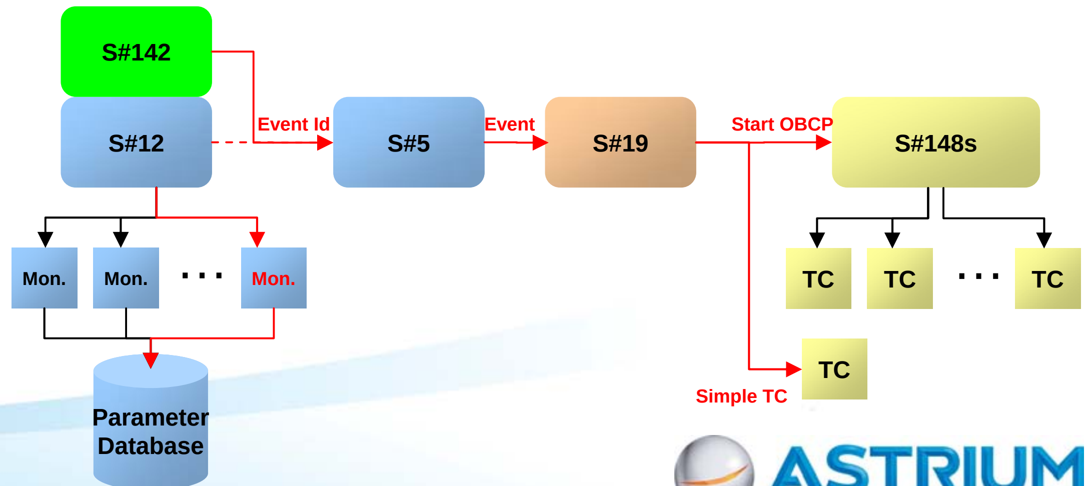
Modelling Languages

AADL: Architecture Analysis and Design Language
SysML: System Modelling Language
SimFIA: tool based on AltaRica language (APSYS)
UPPAAL Universities of **Upp**sala and of **Aal**borg,

Improve efficiency of the RAMS / FDIR Process

- Modular and distributed functional operational reference architecture with proper apportioning of SW functions and configurable FDIR services
- Configurable S/C Configuration Management
- Generic equipment management based on S/C configuration information and status
- Extended nominal commandability
- FDIR reactions composed of TC function sequences
- State and Time partitioned FDIR hierarchy



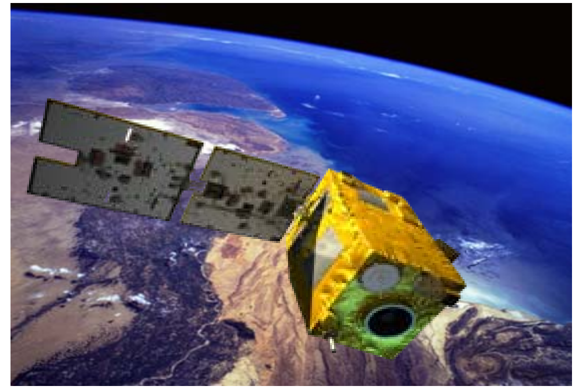


Key Factors in measuring FDIR complexity and cost

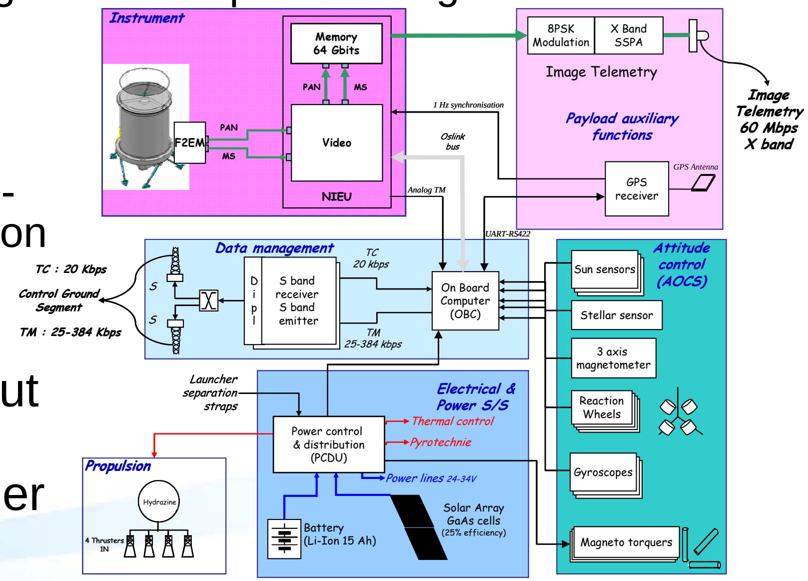
- Programmatic
  - Programmatic versus industrial system breakdown
- Mission and System Requirements
  - Detailed Availability and Reliability
  - Autonomy
  - Number of customer mission / system requirements
  - Variability / Constance w.r.t. predecessor mission
- System Design Definition / Verification
  - Number of mode and redundancy combinations
  - Number of monitors and recoveries
- FDIR key parameters
  - FDIR Approach on System, Platform and Payload level
  - Number of specific FDIR SW requirements
  - Concurrency of FDIR definition

FDIR in Low Cost Missions - Myriade

- Mission Characteristic
  - Myriade line was developed by CNES in the early 2000's in partnership with Astrium and TAS.
  - Specification on best effort basis for "high performance" mission demonstrators without precise availability; lifetime goal >= 1 year.
  - Design Characteristics:
    - Basically single string with few redundancies embedded e.g. RM, Memory, TX
    - Equipments inherited from ground technos (e.g. T805 computer from ground telecom market, not radiation hard)

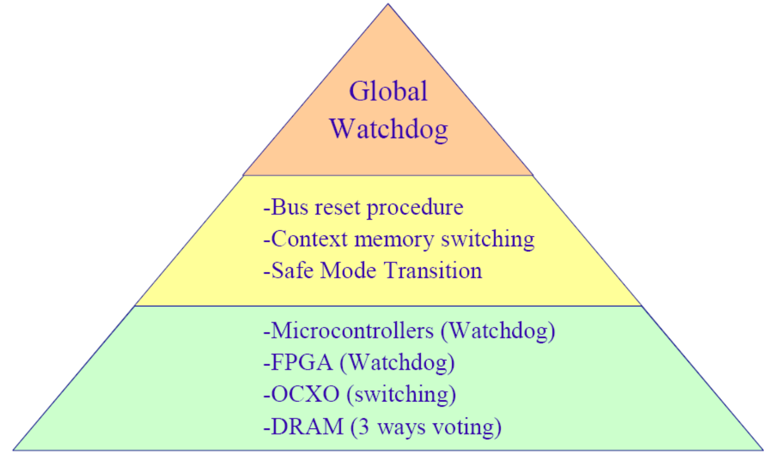


- In-orbit Feedback:
  - 10 launched spacecrafts
    - 7 survived their life duration and were successfully de-orbited after 2 years of extended mission
    - 3 still in operation, None lost.
    - 5 S/C ready for launch with Pleiades in 2011
  - Numerous "transient failures" experienced, but no critical effect caused by SEU
  - Several safe mode transitions recovered under ground control.
  - Globally all missions rated successful.



FDIR in Low Cost Missions - Myriade

- FDIR strategy:
  - Three level hierarchy based on:
    I. Equipments power cycling
    II. Mode changes
    III. computer reset with limited No. of context based restart in hot (attempting Fail-Op) with final restart in cold (Safe mode)
  - FDIR concept focused on SEU imposed failure management, RW failure management and Safe Mode definition in view of minimum redundancies
  - FDIR mechanisms implemented in SW
  - Computer reset is most often used recovery strategy triggering an endless 5 stage reconfiguration process
  - Context recovery supports recovery of operating mode and timeline, but may cause subsequent reboots as not protected against inconsistencies and corruption
- Intensive FDIR verification with
  - A lot of test scenarios
  - Intensive failure case stimulation with intrusive and special electronic



	SEU effects on software	Recovery Strategy
Communication Failures	Temporary exchange loss	- critical actions are executed twicce - Exchange re-execution - Exchange abort
	Loss of communication and control of a component	- Traditional functional monitoring - Component reset
	Loss of an interface	- Bus reset - Software restart
Software Failures	Software Corruption	- Integrity and Coherence test - software restart due to hardware interruptions - Traditional functional monitoring
	On-Board Software dynamic behaviour alteration	- Software restart

FDIR DD&V for cost efficient Columbus Operations

Mission characteristics

- Low Earth Orbit
  - Near real time data
  - Frequent and long contact times
- Long term mission (2008 to 2020)
  - Cost of operation driver for life-cycle cost
- Failure Management
  - 24 hours autonomy requirement
  - Onboard Failure Management for
    - Health Monitoring
    - Safe Mode switching and
    - Recovery of time critical failures

In-Orbit Feedback

- Conventional on-board FDIR service capabilities are fully adequate for robust health monitoring and surveillance but limited for performance monitoring
- Leakage, trend and performance monitoring, false alarm protection cause high operational effort of the Flight Control Team
- Initial studies indicate high potential of modern data mining and data analysis methods but these require significant computing resources

FDIR DD&V for cost efficient Columbus Operations

- Cost reduction potential:
  - Increase of autonomy by automation of the ground system
  - Rationals:
    - Use of commercial S/W
    - No resource limitations
    - Simple access and maintenance
- Columbus Utilisation
  - Test-bed for cost-efficient operational concepts