A survey on Fault Detection, Isolation and Recovery (FDIR) Module in Satellite Onboard Software

Fatemeh SalarKaleji
Satellite Research Institute
Tehran, Iran
f.salar@sri.ac.ir
fatemeh.salar@gmail.com

Aboulfazl Dayyani
Satellite Research Institute
Tehran, Iran
Dayyani@ymail.com

Abstract— **The complexity of the avionic systems in satellites is rising as space missions become increasingly more sophisticated. This complexity emphasizes the need for more dependable systems with minimal anomalies. As satellite manufactures seek to convert many hardware implemented functionalities into software, the On-Board Software (OBSW) is becoming a major component in every satellite. Noticeably, more tasks for Fault Detection, Isolation and Recovery (FDIR) are being implemented in software, where the need comes for a well-defined software architecture that supports a cost-effective implementation of the FDIR functions. FDIR was already explained as key functionality of the OBSW. Obviously not all failures are subject to onboard identification and not all failures are subject to onboard recovery. The FDIR concept to be worked out for the spacecraft during the engineering phase follows some basic requirements and principles, implements a certain failure hierarchy- specifying furthermore on which level the failure is to be fixed- and finally it implements a consistent approach for the functionality transferring the spacecraft to Safe Mode and how to recover from there.**

Since a FDIR concept usually follows a hierarchical approach, in this paper we will indicate a FDIR and safeguarding hierarchy example in the paper. In this structure we will indicate the levels of failures which handled by unit internal, subsystem software, satellite system software, onboard computer hardware reconfiguration unit and ground. Also we will explain the FDIR hierarchy in safe mode implementation in a bit more detail.

In this paper we will consider FDIR technologies in the On-board software in a satellite. Today, there are several proposed methodologies and frameworks which try to solve this problem. We will analyze the functionalities in FDIR Module implemented in an OBSW Framework. Also we have a survey on the FDIR hierarchies and their relationship to the Packet Utilization Standard (PUS) Services.

Keywords— Fault Detection, Isolation and Recovery (FDIR), Software FDIR, On-Board software (OBSW), Satellites, Frameworks, Packet Utilization Standard (PUS), On-Board architectures.

I. INTRODUCTION

"Failure Detection, Isolation and Recovery", (FDIR), was already explained as key functionality of the On-Board Software (OBSW). Obviously not all failures are subject to onboard identification and not all failures are subject to onboard recovery. The FDIR concept to be worked out for the spacecraft during the engineering phase follows some basic requirements and principles, implements a certain failure hierarchy – specifying furthermore on which level the failure is to be fixed – and finally it implements a consistent approach for the functionality transferring the spacecraft to Safe Mode and how to recover from there. A properly defined Safe Mode with full satellite observability is essential for FDIR operations. The Safe Mode must also assure a proper balance of the satellite produced and consumed resources (mainly power) since the diagnosis of failures plus recovery in most cases will not be possible within one ground contact (in particular not for polar orbiting Earth observation satellites). In this paper we have a survey on FDIR in the following sections:

II. FDIR REQUIREMENTS

Typical requirements for FDIR design at the beginning the satellite system engineering phase request that:

- A clear hierarchy is to be defined which type of failure is to be identified and managed on which level FDIR level.
- The satellite must be able to reach its Safe Mode autonomously.
- The Safe Mode, if triggered, shall not limit ground in any way with spacecraft observability and commandability.
- Ground may also be allowed to submit commands which are blocked for the OBSW or are not allowed in that sequence for the OBSW.
- Ground must be able to perform a detailed status analysis and failure event history analysis for unique failure identification.
- Ground may alter operational limits to avoid future Safe Modes – e.g. in cases of failures triggered by equipment degradation.

978-1-4673-6396-9/13/$31.00 ©2013 IEEE

- Obviously – but not trivial to realize – the transition to Safe Mode itself shall not endanger the satellite, i.e. for example shall not require potentially hazardous commands or command sequences.
- Also in Safe Mode the On-Board Computer (OBC) shall be running and shall allow for OBSW patch and dumps and memory patch and dump functions.
- For all failures imagined during satellite engineering it must be assured that they clearly can be distinguished due to their symptom sets.

III. FDIR Approach

The FDIR approach is based on sequences of failure detection onboard TM or corresponding variables in the OBSW-DP and as a result on onboard and ground TC actions for isolation and recovery. These may not necessarily be unique due to the Engineered redundancies and unit internal and external cross Couplings. For each potential failure these chains of failure detection and resulting failure handling – at least failure isolation, preferably also including recovery – must be elaborated. Such a design is typically achieved by following the design guidelines cited below:

- Failure detection must be based both on parameter monitoring on unit and on system level and as a complement on functional monitoring level. This implies that onboard monitoring permanently must check whether parameters are within appropriate ranges and whether all relevant processes are running; mode transitions are properly performed etc.
- Usually the FDIR concept provides both basic approaches:
  - Fail Operational – where a redundant equipment directly can be called into operation without endangering failure escalation (e.g. in case of a heater failure, a thermistor failure, an X-band modulator or amplifier failure).
  - Fail to Safe Mode – which transfers the satellite to Safe Mode.
- For the Fail Operational case the failure isolation will be performed by removing the failed equipment from the operational functional chain by reconfiguration to the redundant one. The failed unit then is listed in the Satellite Configuration Vector (SCV) as non-healthy unless reset by ground intervention.
- Onboard reconfigurations are based on OBSW functions or dedicated On-Board Control Procedure (OBCPs) according to the changed settings in the SCV and the recovery function / OBCP being triggered.

The Safe Mode must be properly defined. Safe Mode is usually the mode operating the S/C with equipment that has the maximum redundancy and consumes the minimum amount of resources. Besides the Safe Mode there may exist other safeguarding S/C configurations which are subject to the individual S/C design.

- By which means Safe Mode can be triggered OBSW functions, HW alarms etc. has to be carefully engineered. OBSW triggered Safe Mode must be armed against accidental function triggering.
- The transition to Safe Mode usually clears all HW interfaces and SW functions. In most cases this is achieved by switching over the entire S/C HW to its redundant side – which then automatically makes use of the redundant set of physical units, interconnections and cabling. And in addition by OBC reconfiguration and resulting reboot things like loaded timelines, running OBCPs or functions etc. are all cleared. This prevents the OBSW to resume interrupted functions or timelines during or after FDIR process.
- Each OBC processor board keeps its own OBSW image in RAM. One OBC processor running one image keeps the S/C stable in Safe Mode. PUS Service 6 is applied for OBSW patching and Function Service 8 is used for triggering reconfiguration functions or OBCPs respectively which reconfigure to the other processor with the patched OBSW image or which reboot the same OBC processor with the patched image.

IV. Satellite FDIR From OBSW Perspective

Already it was indicated that an FDIR concept usually follows a hierarchical approach. Fig.1 below depicts such an approach- again for a fictional satellite.

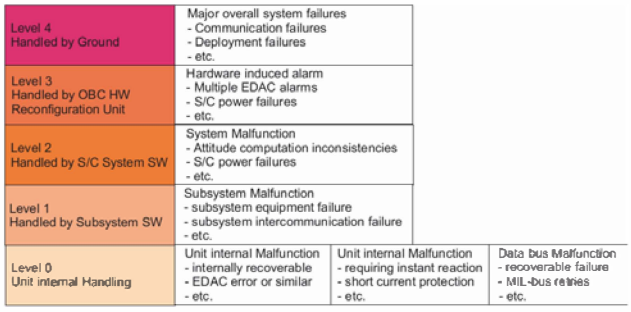

Fig. 1. FDIR and safeguarding hierarchy example.

- The lowest level comprises the handling of failures entirely on unit level, either because it is feasible – such as Error Detection and Correction (EDAC) error handling – or because the equipment by default provides this feature, or because a certain FDIR function on lowest level is extremely time critical – such as reaction to short currents or overvoltage. This level also comprises data bus failures invoked by electromagnetic effects and the like.
- The next higher levels 1 and 2 cover failures being handled on OBSW level, either on subsystem control

level or requiring upper system level. Examples are also indicated in the figure. On this level of above equipment there are monitors available for limit check of unit parameters but also subsystem level abstract verifications such as for example a plausibility check of Global Positioning System (GPS) provided position against internal solution from orbit propagator functions.

- Level 3 then comprises failures which need hardware reconfigurations via the OBC's reconfiguration unit. These include the monitoring and reaction to Hardware alarms and the like.
- And finally level 4 comprises the failures that cannot be handled on board the satellite itself without ground intervention at all.

Each Level of FDIR handling function can escalate the failure to the next higher layer in case the problem cannot be isolated or recovered on its level. E.g. many system level failures may lead to hardware alarms triggering reconfigurations on Level 3, such as power failures or OBC watchdog failures. Vice versa failure recovery is always performed from higher to next lower level.

Again it must be remembered, that a simple equipment reconfiguration to its redundant occurrence triggered on whatever FDIR level – and keeping the rest of the satellite on nominal side can only be applied with restrictions. Depending on root cause – this approach might lead to killing the redundant unit too. Therefore this method is avoided in all severe FDIR cases and the entire satellite is reconfigured to Safe Mode which – as was cited – usually reconfigure the entire S/C including buses and power lines to the redundant side.

V. SAFE MODE IMPLEMENTATION

Having explained the FDIR hierarchy the Safe Mode shall be described again in a bit more detail. Since transition of the satellite to Safe Mode breaks all onboard functions and thus all mission product generation by means of the above cited hierarchical FDIR approach the cases for Safe Mode triggering shall be limited as far as possible.

The need for automated Safe Mode triggering is also driven by how fast ground is able to identify failure symptoms and ground is able to trigger isolation and recovery activities. The possibilities in this area for a permanently visible geostationary satellite differ significantly from those for a polar orbiting LEO satellite.

The guidelines for a Safe Mode configuration are as follows:

- OBC will preferably operate on the redundant side, including OBC HK mass memory unit and safeguard memory for SCV and including CCSDS processing unit.
- OBSW is operational in Safe Mode controlling satellite in a way to assure attitude stability and sufficient power generation by solar array pointing. OBSW in particular will also perform satellite limit monitoring with dedicated Safe Mode Settings.
- The main data bus on board will be operating on the redundant side.
- The Power Control and Distribution Unit, (PCDU), will at least be operated on its redundant controller side. PCDU bank redundancy switching is usually only applied in case of failures in the PCDU itself. Power bus voltage monitoring is performed by PCDU applying dedicated Safe Mode limits.
- Attitude Orbit Control System (AOCS) will operate on the redundant side – including reaction control system.
- Unnecessary equipment such as payload instruments and other equipment from the payload data handling chain is not used due to interrupted mission product generation and will be shut off or down to a low resource consuming state.
- The "Payload Data Handling and Transmission", (PDHT), subsystem and the payload instrument(s) will be switched off or down to safe configurations.
- S-band receivers will – if not affected themselves by the failure – remain hot redundant.
- S-band Transmitter will – if not affected itself by the failure – remain on the nominal side.

In transition to satellite Safe mode: Safe Mode can be induced from ground via the following mechanisms:

- By execution of a dedicated High Priority Command for Safe Mode
- By execution of a dedicated Safe Mode TC function or OBCP – representing a critical command and requiring an Arm-And-Fire mechanism – which triggers a dedicated alarm to the OBC reconfiguration module

Safe Mode can be induced on board at least by the following mechanisms:

- Failures detected by the AOCS
- Failures detected by essential system monitors
- System undervoltage detection (via PCDU logic)
- Failures during repeated OBC reconfiguration sequences of the satellite

In Recovery from Safe Mode: A key principle of Safe Mode is that Safe Mode recovery requires ground interaction. No auto-recovery from Safe Mode is foreseen in contrast to other potential safeguarding modes of a specific mission. For recovery command from Safe Mode the following steps are required as minimum in most cases:

- Configuration of the spacecraft SCV for nominal operations after completion of failure diagnosis
- In case OBSW patches – were applied – selection of the OBSW boot image
- Reboot of the desired OBC redundancy with the selected / patched OBSW image and loading of the SCV
- Wait until OBSW has applied SCV and has switched all redundancies to desired settings

- Perform all S/C system mode transitions to a nominal mode including AOCS subsystem to a nominal AOCS mode
- Preparation of nominal S/C operations by resource reconditioning, loading of new mission timeline

VI. FDIR Related Packet Utilization Service (PUS)

This section is the most intriguing part of the state of the art concerning the FDIR technology. The PUS services relation with FDIR has never been addressed in the literature and in the context that is going to be seen in the thesis onwards. During the wide survey one to build a profound state of the art, the connection between the FDIR constituents and the PUS services was found an interesting field to unveil. PUS allows implementing FDIR functions in a common way across project borders, so that satellite operators are faced with a standardized framework for various missions. The PUS therefore allows standardizing the operational and fault management architecture between ESA missions.

The PUS services closely related to FDIR are discussed onwards emphasizing how they provide the means to complete the FDIR context. Some information and descriptions are borrowed from the ECSS-E-70-41a.

This ECSS-E-70-41Astandard is solely concerned about telecommand and telemetry Packet Utilization hence referred to as PUS or the Packet Utilization Standard. In this standard an application level interface is defined between the space and ground segments. This enables the ground segment to monitor and control the spacecraft sub-systems and payloads as well permit the satellite continuous reporting.

The PUS services related to FDIR can be divided into two main categories, services that are considered as a Fault Detection (FD) mechanism as a whole i.e. On-board Monitoring PUS Service 12 and Test PUS Service 17 and other services, which help shape, an FDIR implementation in the most standardized manner possible. The only PUS service used for monitoring and surveillance purposes is the On-board Monitoring PUS service 12. This service is considered as whole fault detection and monitoring mechanism where when coupled with the Event-Reporting PUS service 5 the Isolation part is incorporated. The Event-Reporting service allows specifying the severity levels in the form of error anomaly reports. The Recovery comes after by the incorporation of the Event-Action Service that is responsible to relate specific event with a series of on-board operations namely On-board Control Procedures (OBCPs). Fig.2 clarifies the idea of PUS services mechanism.

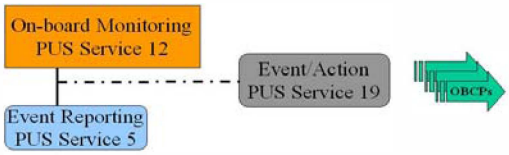

Fig. 2. PUS Services forming a monitoring and surveillance mechanism.

VII. Conclusion

In this paper we have a survey on FDIR module in satellite onboard software. We considered FDIR concept, FDIR requirements and FDIR methods. Then we present FDIR from OBSW view and the FDIR implementation items in Safe mode. Also relation between FDIR and PUS protocol was considered.

References

[1] As'ad Michael Salkham, "Fault Detection, Isolation and Recovery inOnBoard Software",International Master's Program in Dependable Computer Systems, CHALMERS UNIVERSITY OF TECHNOLOGY Department of Computer Science and Engineering, Göteborg 2005.

[2] Jens eickhoff, "Onboard Computers, Onboard Software and Satellite Operations", Springer,2012.

[3] R. Gessner1, B. Kösters, A. Hefler, R. Eilenberger, J. Hartmann, M.Schmidt, "Hierarchical FDIR Concepts in S/C Systems", SpaceOps2004 Conference, Montreal, Canada, May 17-21, 2004.

[4] ECSS-e-70-41A, "Telemetry and telecommand packet utilization" http://www.ecss.nl.