Abstracts

Tuesday 20 October 2015

Session 1 : SAVOIR Status

Introduction

Speaker: Jean-Loup TERRAILLON (ESA/ESTEC) , Giorgio MAGISTRATI (ESA/ESTEC)

SAVOIR is a joint initiative of the European Space agencies and industry aiming at improving the way Avionics is delivered. It is fully consistent with the recommendations of the high level forum established with Member States and industry at the ESA Council at Ministerial level in 2012.

SAVOIR is based on a procurement scenario: if all agencies or customers specify the systems in the same way, and if all the system integrators procure products with the same specification, then a real product policy will be enabled that will benefit from economies of scale across customers and programmes. By agreeing on reference architectures, interfaces and functional specifications, suppliers can focus on contents.

The presentation will give the scope, context and objectives of the session. There will be a focus on the proposed documentation tree.

****

Results of the Industrial Consultation

Speakers: Jean-Loup TERRAILLON (ESA/ESTEC), Giorgio MAGISTRATI (ESA/ESTEC)

To achieve the above scenario, SAVOIR, represented by the SAVOIR Advisory Group, and supported by studies financed by the Space Agencies, produced various documents that are intended to be part of business agreements.

Before publishing these documents, SAVOIR submitted them to a set of reviews, eventually concluded by this wider industrial consultation. Three documents have been reviewed:

- SAVOIR-TN-001- SAVOIR Functional Reference Architecture
- SAVOIR-GS-001- SAVOIR generic OBC specification
- SAVOIR-GS-002- SAVOIR Flight Computer Initialisation Sequence Generic Specification

The presentation will show the results of the review.

****

Plans for the next Software review

Speaker: Andreas JUNG (ESA/ESTEC)

Based on the experience of the first industrial consultation, the next one will address the software documents that are produced by the CoRDeT and IMA set of studies, and pre-reviewed by SAVOIR-FAIRE. The presentation will give the software documents structure, the way they are produced, and the current schedule.

****

MASAIS working group report (data storage)

Speakers: Christophe HONVAULT (ESA/ESTEC), Giorgio MAGISTRATI (ESA/ESTEC)

The SAVOIR -"MAss Storage Access Interfaces and Services" (MASAIS) working group is addressing the definition of the functional, performance, operational and interface requirements of the on-Board Mass Memory function (now called Data Storage) and its management (SAVOIR Data Storage specification).

The presentation will give the current status of the work.

****

Presentation of the new Avionics Network working group

Speakers: Christophe HONVAULT (ESA/ESTEC), Giorgio MAGISTRATI (ESA/ESTEC)

This new SAVOIR Working Group addresses the definition of the functional, performance, operational and interface requirements of the functional links and their management. The scope is limited to the identification and characterisation of the needs of users in term of communication and does not address the definition of communication standards and protocols.

The presentation will give the current status of the work.

****

Operability and generic OIRD

Speaker: Michael McKAY (ESA/ESOC)

Several activities related to Operability are on-going. Update of the ECSS operability standard (E-70-11), update of the PUS standard, draft of a potential generic OIRD.

The presentation will give the scope, context and objectives of the activities on operability.

****

Session 2 : Related ECSS Standards update

Status of the PUS version C

Speaker: Serge VALERA (ESA/ESTEC)

The PUS standard [ECSS-E-70-41A] is being upgraded in version C. A first draft has been proposed for public review, and the Rids of the public review are about to be dispositioned by the working group.

The presentation will give the status of the standard review.

****

Publication of CAN standard

Speaker: Gian Luca FURANO (ESA/ESTEC)

The presentation will give an update following the publication of the CAN standard (ECSS-E-ST-50-15C "CANbus extension protocol" (1 May 2015)).

****

Keynote

Speakers: Charles Patrick COLLIER (Space VPX)

Charles Patrick Collier, AFRL Space Vehicles Directorate, will present a tutorial on two specifications developed, and one in development under the Next Generation Space Interconnect Standard (NGSIS) effort. The Next Generation Space Interconnect Standard (NGSIS) effort is a Government-Industry collaboration effort to define a set of standards for interconnects between space system components and sub-systems. The two approved and fully ratified specifications are: SpaceVPX (VITA 78) and The RapidIO Space Device Class. The one in development is SpaceVPXLite (VITA 78.1) - this one is specifically focused on SWaP constrained 3U systems.

****

Session 3 : SOIS evaluation by the Primes

Introduction

Speakers: Marek PROCHAZKA (ESA/ESTEC), Jorge LOPEZ (ESA/ESTEC), Sabine KRÜGER (ESA/ESTEC)

Following the publication by CCSDS of the SOIS standards, the Savoir Advisory Group has supported the ESA proposal to fund under GSTP an evaluation of the SOIS technology by the three Large System Integrators Airbus, OHB and TAS. The presentation will introduce these activities.

****

How to use SOIS in current and future flight software

Speakers: Alain ROSSIGNOL (Airbus), Michael BRAHM (OHB), Marco PANUNZIO (Thales)

The presentations will touch in particular the following point:

- Selection of SOIS services (for production FSW)
- Merging into Prime's legacy architecture (production FSW)
- Recommendations to CCSDS
- Practical results of this study for R&D and production

****

Conclusions and recommendations of the Primes and their roadmap

Speakers: Alain ROSSIGNOL (Airbus), Michael BRAHM (OHB), Marco PANUNZIO (Thales)

Based on the results of the studies, the Primes will present their strategy, recommendation and roadmap around SOIS. This session is intended to be interactive.

****

Session 4 : Mission Operation Services

Introduction to MO services

Speakers: Mario MERRI (ESA/ESOC), Mehran SARKARATI (ESA/ESOC)

CCSDS Mission Operations (MO) Services is a standardised regime to provide an extensible set of standard services that support end-to-end information exchange between distributed functions of a space system, focussing primarily on Operations – i.e. monitoring and control and associated added-value functions. The focus of an MO Service is on meaningful information exchange, independent of implementation technology, organised as an information model and a pattern of information exchange.

The presentation will introduce and describe the MO services standardisation initiative.

****

Introduction to MO services, SOIS and SAVOIR harmonisation [MOSS] study

Speakers: Andreas JUNG (ESA/ESTEC), Mehran SARKARATI (ESA/ESOC)

SAVOIR has addressed the flight software architecture in the sub-group SAVOIR-FAIRE, and has defined an On-board Software Reference Architecture (OSRA) in the supporting R&D activities named COrDeT. In the definition of the reference architecture, SAVOIR relies substantially on CCSDS SOIS for the on-board communications: SOIS services are identified in the execution platform of the reference architecture.

The CCSDS MO Services have taken the standpoint of defining operation mechanisms of a global space system including ground mission control system and flight software. In particular, it has defined some architectural elements, layers, design patterns, which should be used both in the ground and in the flight software.

These works, which have been done from two standpoints (avionics and operations), are now reaching each other at the level of the software architecture. The MOSS activity intends in particular to verify that the various concepts are consistent, and if not, to advise on the best solution to achieve architectural consistency.

The presentation will introduce and describe the MOSS study.

****

Results of the MOSS study

Speaker: Peter MENDHAM (Bright Ascension)

The presentation will give the current results of the MOSS study, in particular addressing the User Needs and High level requirements for the MO Services, as well as a way towards a consolidated architecture.

****

Feedback from the audience

Speaker: Jean-Loup TERRAILLON (ESA/ESTEC)

Being given that this initiative is mainly managed through CCSDS as an inter-agencies work, the audience will be given the opportunity to give feedback from the presentations, on the topic of MO Services, their perceived maturity, their applicability range, their impact on current implementation, and more generally any recommendations on how to proceed with this topic.

****

Wednesday 21 October 2015

Session 1 : Avionics Technology Trend

ESA Welcome and Introduction

Speaker: Davide Oddenino (ESA/ESTEC)

The presentation will give the scope, context and objectives of the session.

****

On-Board Computer System Architecture (OBC-SA)

Speaker: Andreas SCHÜTTAUF (AIRBUS DS Bremen)

During the past four decades it could be observed that the software complexity has grown continuously by a factor of two every two years. In the early 70's the amount of software was in the order of a few thousands lines of code while today's mission have to deal with more than 1 million lines of code. It is expected that this trend will continue in the next years. In order to handle this complexity at reasonable costs the productivity in writing software but also for designing the underlaying execution system has to increase significantly.
In other domains like automotive and aeronautics this trend is even stronger and innovation cycles are much shorter. Thus, automotive and aeronautics industry have initiated developments like AUTOSAR or Integrated Modular Architecture (IMA). All these initiatives are based on the definition of standards for computing platforms and the interfaces between these platforms. In the industrial automation domain Open Modular Computing Standards like VPX and compactPCI serial have been used successfully over many years now.
The goals of the Open Modular Avionics Architecture for Space Applications (OMAC4S) initiative started by Airbus, Fraunhofer FOKUS, STI, SYSGO and TTTech are to outline a solution that helps to reduce complexity and costs for space avionics significantly. This initiative is partly funded by the German national space agency (DLR) through the project On-Board Computer System
Architecture (OBC-SA). In this paper we describe how standardization and the usage of already proven technologies from other industrial domains will help to limit the effect of the software development on schedule and costs of satellite projects. The reasons are:

1. the software has to deal with a much smaller spectrum of computing platforms,
2. using standards will allow to combine solutions from different vendors either hardware or software,
3. modular certification will be possible as hardware or software components can be reused without any modification.

The main characteristics of the envisaged open modular system architecture are listed below:

- Network centric approach (High speed Satellite Deterministic Network),
  - Network topology either full mesh or star (depending on availability requirements, data traffic, etc.)
  - Support for different traffic classes over the same physical network (fully deterministic, rate constraint, best effort)
  - time synchronization over network
- Using passive standardized backplane based on an industrial standard adapted for space and supporting the network centric approach
- Full support for time and secure space partitioning
  - to prevent error propagation and to limit the effects of failures in the application
  - to allow applications of different criticality on the same computing platform
- Provision of a software framework that provides all basic services of a typical on-board software
  - housekeeping reporting

- data management and monitoring
- data storage and retrieval
- event handling
- event/action mechanism
- execution of mission timelines and orbit position schedules
- execution of On-Board Control Procedures (OBCP) based on widely used open source interpreter

A technology demonstrator is available. It includes several computing nodes from different vendors with different performance figures interconnected via the network. Each node is executing typical applications like AOCS, TCS, payload data processing etc. on top of a Time and Space Partitioning operating system.

****

Avionics technology trends

Speakers: Brice DELLANDREA (THALES ALENIA SPACE France)

Many conflicting tendencies are currently driving the design of new avionics:

- The need to develop very low cost avionics to be produced in high series, which favours the COTS-based solutions and centralized & integrated solutions,
- The need for improved computing capabilities for new challenging missions (high autonomy, image processing, data processing centralization), which favours the throughput improvement of platform computers or architectures based on fast co-processing elements (DSPs, PowerPCs, etc…),
- The techno-push of new solutions, for instance processors (LEON, ARM), software (TSP concepts) and communication systems (SpaceWire-D, SpaceFibre, TTEthernet, AFDX, and other alternative solutions such as UMEA, FlexRay, Ethernet AVB), providing seducing new features.

There is no single avionics able to answer all the needs of the future market, but several main trends can be extracted from this melting pot of emerging technologies. They will be presented per group of use-cases (telecommunication missions, low-cost constellations, Earth observation missions and science missions). Evolution of the Avionics System Reference Architecture taking into account these new technological opportunities will be presented (merging of mission & platform data links, multi-core processing units or decentralized processing architectures, etc…).

****

Lessons Learned in the Development of Avionics for Modern Microsatellites

Speaker: Jiang LIANXIANG (Shandong aerospace electronics technology institute, China)

With the rapid development of modern micro-satellite technology, it has been widely used in communication, remote sensing, electronic reconnaissance and other fields. It has been widely concerned by the aerospace, military, industrial and scientific research institutions, and has become an important direction of the development of space technology. NASA proposed micro-satellite becomes faster, better, cheaper guidelines, which have been recognized by more and more international peers. In order to obtain high time resolution and spatial resolution, more and more remote sensing satellites fly in formation or constellation, these formation or constellation satellites are similar or identical with each other, the avionics of these small satellite are identical, so they can developed with the same design, furthermore, these utilized avionics could be produced and stored as products off the shelf. For sudden natural disasters or local military reconnaissance and communication application requirements, it requires micro-satellites with rapid development, rapid launch, rapid application, which need to change the development mode of traditional micro-satellite electronic equipment, these micro-satellites could be constructed based on the universal avionics products library. At the same time, it puts forward higher requirements for satellite integrated testing and in orbit testing, which requires the fast system integration and in orbit testing. In order to shorten the processing time of the payload’s data, on-board data processing equipment is employed for small satellite to process payload data in space. In order to improve the autonomy of the modern micro- satellites, micro-satellites require high independent management capabilities, which including health management, task management, etc..

In summary, the characteristics of modern micro-satellite bring new requirement for on-board avionics, whose performance directly determine the ability of small satellites. In order to achieve better, faster and much more economic, we share our learning in the development of on-board avionics for the flying formation remote sensing micro-satellites, whose life is 6 months. Specifically include:(1) the star, double star, bus and the hybrid avionics architecture is compared, the on-board avionics system for the 6-month life satellites adopts open system architecture, the technical and interface specifications of the general products should be developed and published, by which introduce competition mechanism;(2) Standardization, modularization and serialization, the general products of the satellites could be produced in batch mode and stored as off-the-shelf products, the different requirement of satellites is met through the combination of standardized module products. In this way, we can avoid repeated development cost, reduce development costs, improve research efficiency and shorten the development cycle;(3) To explore a new way to selection and quality assurance methods for COTS electronics components, and to reduce the cost of components. At the same time, the the system level fault tolerance design should be strengthened to reduce the quality level of components;(4) equip with the on-board data processing equipment for real-time processing of payload’s data, the tranceivers between satellites should be employed to provide inter satellite network links. Lots of information is exchanged when satellites cooperation to finish the same task.(5) Plug and play makes the OBC recognize the nodes dynamically when smart nodes power on, which would accelerate the system integration;(6)Built-in-test(BIT) methods are employed to shorten the test time during the integration and on-board test.

The principle prototype avionics for the six-month life remote sensing fly formation satellites is developed, the above new technologies and methods are carried out in the development and testing of the prototype, the effectiveness of these measures are demonstrated.

****

Research & Technology activities in on-board data processing domain

Speaker: Olivier NOTEBAERT (AIRBUS DS Toulouse)

The next generation of spacecraft avionics is being prepared in Europe through number of collaborative initiatives between agencies and industry such as SAVOIR or ECSS standards evolutions, aiming at harmonising and standardizing future architectures and technologies. In parallel, Research and Technology efforts are deployed in selecting and maturing new technologies expected to cover future needs for enabling new functionalities, higher performances and a lower cost of Spacecraft avionics.

In this context, Airbus Defence and Space have developed a Research and Technology roadmap which focuses high data processing and communication performance allowing flexibility, modularity and affordability to face both an harsh worldwide competition as well as the necessary limitation of institutional budgets.

Three main axis are explored in priority:

The further consolidation and implementation of avionics interface standardization in on-board avionics architecture and products in coherence with the SAVOIR on-board reference architecture;

The selection and adaptation for future space systems of proven modular architecture solutions for data handling as successfully developed in other industrial and commercial critical applications such as aeronautics or automotive.

Besides a still necessary continuous effort for evolution and improvement of few classical rad-hard and rad-tolerant space processing devices and technologies, alternative solutions enabling a wider use of computing technologies from the very dynamic market of consumer electronics are evaluated for their capability to achieve a breakthrough in term of processing performance per euro spent and per watt dissipated in-orbit.

The most important criteria's for architectural choice and technology selection are the flexibility and the modularity (i.e. the capability to adapt to a large variety of missions profiles without a main redesign and re-qualification effort). This aims at a lower global cost footprint which includes the non-recurring effort for developing a product line and a recurring cost per mission addressing the full avionics industrial production process within a long term business plan.

When deployed on the full avionics system with a truly generic and product oriented approach, this strategy is expected to enable significant performances and costs cutting steps for the spacecraft avionics of the next decades.

****

Simplifying System Design Through Hybrid Dependability Measures

Speakers: Christian M. Fuchs (Technische Universität München)

Future satellite platforms and upcoming mega-constellations such as Outernet, OneWeb and LeoSat will require new approaches to failure tolerance, not only due to efficiency and resource restrictions, but also due to cost reasons. With an increased standardization of platform families and constellations consisting of hundreds of satellites, simplicity, weight and thus per-subsystem costs are of paramount importance, even for the vast budgets available within these projects. Due to the generation-focused aging approach of such constellations, unusually large quantities of more efficient standardized data storage and processing components will be required.

Embedded hardware has evolved considerably over the past decade, among others enabling a rapid evolution of the capabilities of miniaturized satellites. Thus, the space industry will have to adopt the use of such more modern commercial off-the-shelf (COTS) components and technologies. However, most of these solutions cannot yet be used in major high profile space missions. For some technologies, the error pattern encountered can be drastically different with legacy and modern technology. One drastic example of such technology induced differences is modern NAND-flash memory [1], where legacy single-level-cell and current multi-level-cell memory (16+ levels) require drastically different erasure coding and addressing [2], [3], [4]. Thus, (sub)system design as well as error detection and correction (EDAC) must be adjusted to handle these changed requirements.

Hardware-side EDAC is quite efficient when used in components with a coarse structural width, but as structures are shrunk EDAC strength must be increased due to the worse impact and higher likelihood of radiation effects. Due to declining efficiency, additional circuitry, die space and storage capacity are required to handle diminishing returns when compensating with more hardware EDAC, unless specialized rad-hard manufacturing techniques are used. Also pure hardware side measures can inflate complexity drastically, thereby requiring considerable development effort and making testing difficult. In contrast to hardware measures, pure software-side protection does scale well for low structural width components, but offers only weak failure-tolerance guarantees.

Hybrid approaches combining software measures with smart system design and an efficient combination of technologies can enable the use of state-of-the-art COTS hardware. Such solutions can enhance fault detection, isolation and recovery drastically allowing a reduction of per-component redundancy. Thereby, overall complexity and energy consumption can be reduced, increasing system efficiency and testability.

We thus present results of our research towards dependable storage solutions (denoted in blue in Figure 1) [5], [2], [6]). These concepts were originally developed for use aboard miniaturized satellites, as requirements and technological restrictions often force such projects to rely upon widely available COTS hardware. The focus of this talk will be set on the positive effect such concepts can have on space system design, and how they can help enable the use of modern COTS components also for critical and long-term missions. Combined with a smart choice of technologies [7], [8], the outlined concepts can also enable a dependable base for further reliability enhancing concepts, especially regarding compute dependability.

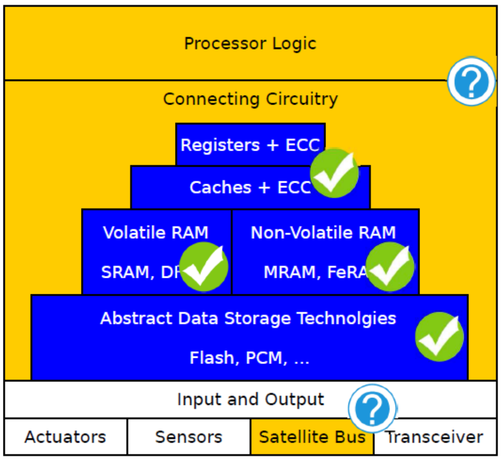

Fig. 1. A high-level logical view on a nanosatellite OBC. Check-marked elements have been researched in detail and were published accordingly. Question marks present denote ongoing research activities regarding compute dependability.

REFERENCES

[1] Y. Cai et al., "Error patterns in MLC NAND flash memory: Measurement, characterization, and analysis," in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012. IEEE, 2012.

[2] C. Fuchs et al., "A fault-tolerant radiation-robust mass storage concept for highly scaled flash memory," DASIA2015, 2015.

[3] S. Gerardin et al., "Radiation effects in flash memories," IEEE Transactions on Nuclear Science, vol. 60, 2013.

[4] F. Irom et al., "SEEs and TID results of highly scaled flash memories," in IEEE Radiation Effects Data Workshop, 2013.

[5] C. Fuchs et al., "FTRFS: A fault-tolerant radiation-robust filesystem for space use," ARCS2015, no. 28, 2015.

[6] "Enabling dependable data storage for miniaturized satellites," 29th AIAA/USU Conference on Small Satellites, 2015.

[7] A. Ferreira et al., "Using PCM in next-generation embedded space applications," in IEEE RTAS 2010. IEEE, 2010.

[8] G. Tsiligiannis et al., "Testing a Commercial MRAM Under Neutron and Alpha Radiation in Dynamic Mode," IEEE Transactions on Nuclear Science, vol. 60, Aug. 2013.

****

Deterministic ETHERNET for Space Applications

Speaker: Jean-François Dufour (TTTech Wien)

Typical spacecraft avionics systems are distributed for achieving the required reliability and availability targets of the mission. However mission requirements differ between launchers, satellites, human space flight and space exploration. Launchers require high reliability with very short mission times whereas satellites or space exploration missions depend on a high availability over very long mission times. Comparing the reaction time requirements of the avionics systems of launchers with those of satellites shows very fast control loops in launchers versus much slower ones in satellite applications. Human space flight missions are the most challenging concerning reliability and availability since human lives are involved and the mission times can be very long (e.g. ISS). Also the reaction times of these vehicles can get challenging during landing or re-entry mission scenarios leading to "deterministic" low latency requirements for the data network.

In these different applications, the last decade has shown a clear trend towards more autonomous functions that are required to fulfill the needs of current and future missions. This autonomy leads to new requirements with respect to increased performance, determinism, reliability and availability. On the other hand, the commercial pressure to reduce the costs of electronic components and equipment in space applications is increasing, which consequently leads to an increased use of "COTS" components, especially for launchers and LEO satellites.

Future spacecraft avionics systems have to be more scalable and modular to be able to deal with these challenges. The most cost effective way to fulfill all requirements is to develop a re-usable platform based on open standards which have a large user base – ideally in several industries (like in the example of the CAN bus). It was demonstrated many times in the past that spinning in validated technologies and standards from massproducing-industries leads to a substantial reduction of the lifecycle costs while often bringing an increase in performance as a bonus, which in turn often result in more capability and thus more engineering and science opportunities.

The onboard communication network is an essential part of such a platform, the selection of a technology that fulfills these above-stated requirements is therefore a key subsystem to address. The use of a single technology and related infrastructure for launcher, satellite, human space flight and space exploration missions could lead to a significant reduction in complexity and would lead to significant savings in weight and power, while in most cases it would increase the performance of the overall system. Current industry trends on state-of-the-art onboard avionics are based on platforms like the NASA core flight software (CFS) developed by GSFC [1] or the Orion distributed IMA platform developed by Honeywell [2]. The use of deterministic

Ethernet within such platforms allows a seamless integration of the onboard avionics with the EGSE platform where Ethernet has already become a standard networking technology.

This presentation focuses on system architectures using the TTEthernet technology to decrease the software complexity and time-to-market [3] for launchers, satellites and human spaceflight, and will further demonstrate the scalability of the technology for these different applications. The presentation also provides an update on the progress made in the ESA's TRP and FLPP-3 projects covering the maturation of the TTEthernet technology in which TTTech Computertechnik works as subcontractor to Airbus DS GmbH. Finally, the presentation indicates areas in which further research and standardization is required to facilitate the adoption by a wider user base in the European space market.

REFERENCES

[1] David McComas, NASA/GSFC's Flight Software Core Flight System, Flight Software Workshop November 7-9, 2012

[2] Mitch Fletcher, "Progression of an Open Architecture: from Orion to Altair and LSS", May 2009

[3] W.Steiner, R.Maier, D.Jameux, A.Ademaj, "Time-Triggered Services For SpaceWire", SpaceWire Conference, Japan 08

****

Round Table Discussion

Panelists:

Panelists will be invited to give their position on various topics.

Session 2: FDIR

ESA Welcome and Introduction

Speaker: Marcel Verhoef (ESA/ESTEC)

The presentation will give the scope, context and objectives of the session.

****

Decoupling FDIR levels by different monitoring frequencies to reduce SW complexity

Speakers: Michael Brahm (OHB)

In general several FDIR levels need to be realised for satellites and other spacecrafts, starting from a single unit failure, to acquisition board failures through to a complete on-board computer failure. One important goal for failure detection and recovery is to avoid false alarms and cascades of alarms when for example a single acquisition board fails which acquires data that is used for the detection several other failures.

Based on a realised satellite project, this presentation introduces a concept which allows the detection of failures on the correct level without a complex software logic behind it.

****

State Aggregation Approximate Dynamic Programming for Model-Based Spacecraft Autonomy

Speakers: Massimo Tipaldi (OHB)

On-board autonomy is becoming a crucial aspect of currently developed and future space projects, especially for deep space exploration missions. Its main goal is to automate on-board sequence execution by interweaving goal-driven commanding with fault detection, diagnosis, and recovery capabilities.

This presentation is focused on a Markovian Decision Process (MDP) based framework, which can offer a way of modeling on-board autonomy mechanism and representing its corresponding data.
Its applicability to the well-known three layered autonomous space systems architecture is mentioned. Special attention is given to its deliberative layer, where Approximate Dynamic Programming (ADP) techniques can be applied to determine the corresponding sub-optimal policies over an MDP large-scale state space, and therefore solve the so-called curse of dimensionality.

In particular, the feature-based state aggregation approach has been chosen. The MDP state space is partitioned based on its reward structure and the optimal cost-to-go or value function is approximated by a constant over each partition or meta-state. An example of such approach is presented, where it is shown how the reward function structure can determine some important properties of the calculated sub-optimal policy, such as the balancing of the spacecraft safety versus the completion of relevant mission objectives.

****

FDIR - State of the art and evolution

Speakers: Antoine Provost-Grellier (TAS)

Autonomy requirements for satellites and scientific missions drive designers to increase the complexity of the FDIR to maintain the mission despite permanent or transient failures with a limited support from ground. However the day-to-day experience on the FDIR shows that FDIR development and validation is always a difficult and cumbersome activity, whatever the autonomy level required.

First, this presentation will focus on the actual practices:

- the state of the art of the FDIR development and validation process in Thales Alenia Space;
- benefit and lessons learnt from several FDIR studies (COMPASS, FAME,..) on TAS projects with specific feedback on the benefit of modeling approach, editor tools to support action sequence customization via the Satellite Data Base.

Then , new challenges for large constellations and use of COTS will be addressed:

- What is the most efficient strategy to support failure detection and recovery ?
- What are the system impacts of fault tolerant design on the mission ? observability required by the operator on transient failures ? -> testability requirements will have to be balanced in order to maintain a simple design.

As a synthesis, recommendations will be proposed for future studies.

****

FDIR process and product experience at Airbus

Speakers: Gunther Lautenschlaeger (AIRBUD DS)

Introduction: The on-board Failure Detection, Isolation and Recovery (FDIR) engineering is part of the core spacecraft elements challenged during all pro-ject life cycle. FDIR is spread over system as well as over various subsystems and equipments. FDIR needs early in the project a consistent design concept, but can only be consolidated later with detailed equipment en-tries. So FDIR is one of the earliest as well as one of the latest system engineering tasks to be performed and by this essential for the success of the project. Feeding late FDIR requirements into SW specification or con-figuration tables may impact the project schedule.

The challenge for the FDIR engineering results in the fact, that the FDIR design spans across nearly all spacecraft disciplines with a highly dynamic and an iterative detailed design feedback. In addition a verification strategies and means for dedicated test functions have to be defined, including test cases, which are not testable on the flight model. All of this shall be per-formed keeping the FDIR solutions simple, cost effi-cient and in time.

Airbus reviews currently the FDIR engineering process applied to different space projects includeing-GAIA, Sentinel-2 and SolarOrbiter. The final goal is to improve the FDIR engineering process during design, development, validation and operational phases.

The following main themes in the FDIR process were identified as possible stakes:

- Quality and phasing of the engineering effort set in place to substantiate and justify design choic-es from system requirements, yielding to an un-even Design & Validation to cost mind-set
- Lack of a shared vision between project actors for FDIR engineering, development and V&V lifecycle, yielding to work in silo attitude as a result, and challenge to phase the overall engi-neering
- Lack of Standardisation & Design policies, from requirement breakdown and traceability into documentation structure to implementation of roles and responsibilities

On the other hand airbus applied and improved best practise in these projects by:

- Improving flexibility in implementation of FDIR solutions

- Introduction of a structured co-engineering be-tween FDIR architect and RAMS engineer re-lated to failure mode effects identification and coverage

Airbus proposed approach to strengthen best practise is to emphasise on:

- Streamlined roles and responsibilities in the RAMS and FDIR development process
- Standardisation of FDIR design and implementation policies
- Identification and control of holistic cost drivers in the development lifecycle
- Use of MBSE techniques to support design definition and justification early in the project
- Phasing of engineering effort in the project lifecycle
- FDIR flexibility in solution implementation

The Key Factors to measure FDIR complexity and cost may be discussed controversially depending on the different Stakeholders within the project and therefore not easy to be identified.

For the same reasons ESA has launched a study "Generic AOCS/GNC Techniques & Design Frame-work for FDIR". The objective of this activity is to propose generic solutions for the AOCS/GNC func-tional chain to recurring issues currently met with Fail-ure Detection Isolation and Recovery (FDIR), both in the technical design versus requirements area and in the early verification area, with the final goal of pro-posing a design framework allowing already in Phase A/B an early prototyping and dynamic verification of FDIR AOCS/GNC mechanisms.

REFERENCES

[1] Airbus: ADS.E.0948 "Operations Architect Process Description", ADS.E.0972 "FDIR Architect Process Description"

[2] ESA: ECSS-E-ST-70-11C "Space engineering; Space segment operability"

[3] NASA: NASA-HDBK-1002 "Fault Management Handbook"

****

Fault Detection, Isolation and Recovery Design for micro-satellite avionics

Speakers: Jiang LIANXIANG (Shandong aerospace electronics technology institute, China)

With the rapid development of modern micro-satellite technology, it has been widely used in communication, remote sensing, electronic reconnaissance and other fields. It has been widely concerned by the aerospace, military, industrial and scientific research institutions, and has become an important direction of the development of space technology. Autonomy is one of the most important characteristics of modern micro-satellites, which requires health management, task management by satellites with more intelligence. Avionics becomes more and more important in satellites, the health management of avionics is very important to upgrade the autonomy of satellites. Fault detection, isolation and recovery(FDIR) is an effective technique to upgrade the ability of health management. FDIR detects fault and accurately isolate it to a failed component or module as soon as possible, which avoids fault transmit and deterioration, and increases system availability.

In the development of avionics for an remote sensing micro-satellite, some FDIR techniques are applied. An FDIR module is designed to monitor and store the CAN bus data. The most important parameters related avionics' health state are selected such as the primary voltage bus is monitored in real-time. If an fault is checked, a serial instructions are send to isolate the fault components. Furthermore, an distributed build-in test(BIT) is adopted for fault detection. The failure mode effect and analysis(FMEA) is developed to select the monitored parameters. And the trend character, statistic character, the redundant relationship between parameters and the time stress information is evaluate for fault detection. The fault Petri-net is employed to describe fault diagnosis knowledge mode, an inverse reasoning mechanism is designed for fault location. Some system-level reconfiguration measures are presented to recovery fault, such as task transition.

****

LCM – The network is not transparent

Speakers: Maurizio Martignano (Spazio IT)

Spazio IT is using LCM (a message passing library - http://lcm-proj.github.io/) to develop the middleware of a ground integration/testing software platform for Airbus Helicopters. Some of the features of this library - and namely: the absence of a centralized server having to relay the message, its many to many type of interaction, transmitting messages only once, without resending them and absolute type safety - are essential for the development of simple and efficient FDIR mechanisms. These mechanisms are mostly based on acknowledging that "the network is not transparent", that "things" may fail and stop working. The presentation will show how these basic FDIR mechanisms work and how they have been implemented based on LCM.

****

Model Based approaches to FDIR

Speakers: Alessandro Cimatti (FBK)

Model based methods are increasingly applied in industry and academia for the safety assessment of systems under faulty conditions, by supporting the production of fault trees, FMEA tables, and reliability measures.

The development of Fault Detection, Isolation and Recovery is poses additional challenges, due to the partial observability of the system state that must be dealt with at run-time, and can only partly be tackled by sensors.

In this talk we will present an overview of the field of Model Based FDIR, analysing the approaches in terms of modelling capabilities, functions and tools available. We will also illustrate current trends in academic research, and the challenges ahead posed by the industrial practice.

We will focus on the techniques and tools developed in a series of ESA-funded project, and a vision statement for FDIR within the COMPASS framework.

****

An Integrated Process for FDIR Design in Aerospace

Speakers: Marco Bozzano (FBK)

The correct operation of complex critical systems increasingly relies on the ability to detect and recover from faults. The design of Fault Detection, Isolation and Recovery (FDIR) sub-systems is highly challenging, due to the complexity of the underlying system, the number of faults to be considered and their dynamics. Existing industrial practices for FDIR are often based on ad-hoc solutions, that are conceived and developed late in the design process, and do not consider the software- and system-level RAMS analyses data (e.g., FTA and FMEA).

In this paper we propose the FAME process: a novel, model-based, integrated process for FDIR design, that addresses the shortcomings of existing practices. This process aims at enabling a consistent and timely FDIR conception, development, verification and validation. The process is supported by the FAME environment, a model-based toolset that encompasses a wide range of formal analyses, and supports the FDIR design by providing functionality to define mission and FDIR requirements, fault propagation modelling, and automated synthesis of FDIR models. The FAME process and environment have been developed within an ESA-funded study, and have been thoroughly evaluated by the industrial partners on a case study derived from the ExoMars project.

****

Round Table Discussion

Panelists:

Panelists will be invited to give their position on various topics.

<u>Thursday 22 October 2015</u>

Operability and Modularity concepts of future RTUs/RIUs

Round Table Discussion

The round table will include the accepted position presentations and an open discussion with the audience.

The aim of the round table is to address the following topics:

- Operability concept of a RTU:
  - A common RTU operability concept for different type of missions (like Science, Earth Observation, Telecom) could bring several benefits in term of cost reduction for Application SW development, implementation of a homogeneous FDIR.
  - SAVOIR will present a draft Operability and Functional specification for a RTU at ADCSS2015. To which level of details a common RTU operability concept should arrive ?
- Modular design of a RTU:
  - which are industry's expectations for what concerns modularity of a RTU ?
  - Modularity shall be seen as a main feature of a product portfolio from a RTU equipment supplier or modularity across RTU suppliers?
- Building Blocks
  - The availability of microcontroller (as standalone ASIC or as IP core in a FPGA) could change the avionics architecture of a S/C allowing the decentralization of tasks very often exclusively performed by the OBC: an intelligent RTU could do much more that simply storing and executing acquisition instructions list.
- Which building blocks are needed for the future RTUs ?
  - At ESA we have in mind several: Point of Loads Converters, Microcontrollers, mixed signal components (ICs and ASIC technologies), Industry's contribution towards a more inclusive determination is paramount.