Adopting a model-based approach for satellite operations' diagnosis

Nikolena Christofi, Claude Baron, X Pucel, Marc Pantel, M Machin, C Ducamp

13^{th} *International Conference on Modeling, Optimization and Simuation* - MOSIM*'20 - November 12-14, 2020*
Agadir - Morocco "New advances and challenges for sustainable and smart industries"

Adopting a model-based approach for satellite operations' diagnosis

N. CHRISTOFI

LAAS-CNRS, IRT Saint Exupéry
INSA Toulouse, Université de Toulouse
nikolena.christofi@irt-saintexupery.com

C. BARON

LAAS-CNRS, ISAE-Supaéro, Quartz-Supméca
CNRS, INSA Toulouse, Université de Toulouse
claude.baron@laas.fr

X. PUCEL

Information Processing & Systems
ONERA, Toulouse, France
xavier.pucel@onera.fr

M. PANTEL

IRIT, Toulouse INP
Université de Toulouse, France
marc.pantel@toulouse-inp.fr

M. MACHIN

IRT Saint Exupéry
APSYS-AIRBUS, Toulouse, France
mathilde.machin@irt-saintexupery.com

C. DUCAMP

Airbus Defence & Space
Toulouse, France
christophe.ducamp@airbus.com

ABSTRACT: *The diagnosis procedure in satellite operations is constrained by strict time limits. If a failure occurs, operators must be efficient and proactive, as diagnosis must be completed within the smallest number of visibility windows (pass duration over the ground station which are usually very short and separated by long periods where the ground cannot communicate with the satellite). Improving the diagnosis procedure and tools, time and precision-wise, is therefore essential. The proposal presented in this position paper is to provide the operators with operation-dedicated models to help them in reacting quickly and in finding a suitable repair solution as fast as possible. These models will gather system architecture, functional and dysfunctional data taken from system engineering and safety analysis models. The paper presents the framework of the proposed solution and discusses different implementation options.*

KEYWORDS: *MBSE, MBSA, operations, system engineering, safety, space systems, satellites, model-based engineering, operational diagnosis.*

1 INTRODUCTION

Carrying out mission-assigned activities in satellite operations imposes strict time limits, as the satellites' availability depends on their position with respect to the ground station, which also defines their visibility window, i.e the duration (also called time "window") during which the satellite can send and receive messages to and from the ground station. In the case of alarms occurrence which cannot be handled onboard, on-ground operators need to quickly react during the satellite passage since they need to identify whether it is indeed an error, and if so, to find the root cause and correct it, within the limited time-frame of the current and following visibility window(s). Waiting for the next window(s) increases the mission costs and risks, since the satellite issue can worsen. Current practices provide a good level of safety performance in operations but a lack of availability, i.e. the worsening is limited but the cost can rise significantly to recover the operation. Thus, availability, which is described as the capability "to keep [the system in] a functioning state in the given environment" [Cloutier, 2019], [INCOSE, 2012], is a very important system feature, especially for the clients -the recipients of the service provided by the satellite.

The communication between the satellite and the operation centres is bounded by strict time constraints. For example for Earth-observation satellites placed in Sun-Synchronous Orbits (SSO), with an altitude typically between 600 and 1000 km over the Earth

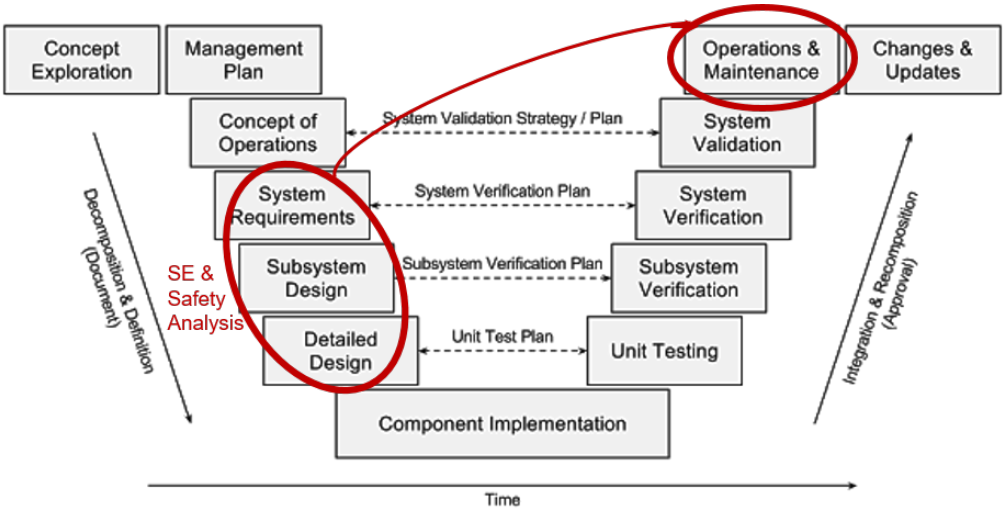

Figure 1 – Positioning the operational phase in the system engineering life-cycle [Esfahbod, 2013].

surface, the visibility window lasts between 8 and 15 minutes. This is because they only pass over the same point on the ground at the same time in a fixed period [Takashi, 2000]. Improving the diagnosis procedure and the associated tools for operators is therefore an essential and challenging task, especially in regards to system availability.

The operators' mission tasks require multidisciplinary knowledge and background in -among other disciplines- systems engineering, dependability and diagnosis. They need to be able to characterise failures arising from alarms and associated data, which are raised at system, subsystem or equipment level, and to find the root causes that initiated the fault chain. In addition, operators need to propose a repair sequence to fix the issue or reduce its impact. Even though they undergo a thorough training aiming to prepare them for their tasks, fully mastering all disciplines involved in a space system is hard to achieve, so they often need to communicate with other experts during diagnosis and repair solutions.

In some cases, a major issue was identified: operators mostly relied on their experience concerning the system structure and behavior and the possible failure causes. In an effort to support efficient diagnosis, we propose to provide them with *models*, to help them in quickly and precisely identify the causes of the alarms reported by the system, and, in the case of failures, to design appropriate repair procedures. This paper therefore advocates the use of model-based approaches where the system models, together with the safety-related dysfunctional model, would contribute in building an operation model to support the operators in performing diagnosis.

This paper is a position paper, and is organised as follows. First the context and problem are introduced and the interests of using model-based approaches is being discussed. We then present a first draft of our model-based approach in order to improve operational diagnosis. We conclude and present several research perspectives aiming at deepening the proposal or considering alternative solutions.

2 CONTEXT AND MOTIVATIONS

The common practice today in operational diagnosis is that the operators are given a semi-formal description of a system (e.g. structured documents written in natural language), together with an observation of the system's behaviour which conflicts with the way the system is meant to behave. Diagnosis is part of the operational phase, which is one of the last phases in a satellite life-cycle, as can been seen on figure 1. The traditional system life-cycle sequentially first consists in the system development: its decomposition into subsystems, the development of each subsystem, and the integration of the subsystems that allows delivering and deploying the system. Then, the (usually) combined operation and maintenance phase begins.

2.1 Diagnosis in space operations

Space systems are composed of on-board parts (platform and payload), and on-ground parts, both of which contain instrumentation and tests that are useful for fault diagnosis. Each payload and platform (power and thermal management, attitude and orbit control subsystem (AOCS), communication, on-board processing & storage i.e. on-board computer (OBC), structural and, telemetry & telecommand (TM/TC)) subsystem has specific diagnosis modules either crafted manually, or according to existing model-based or data-based approaches. Each diagnosis module can identify abnormal situations and emit

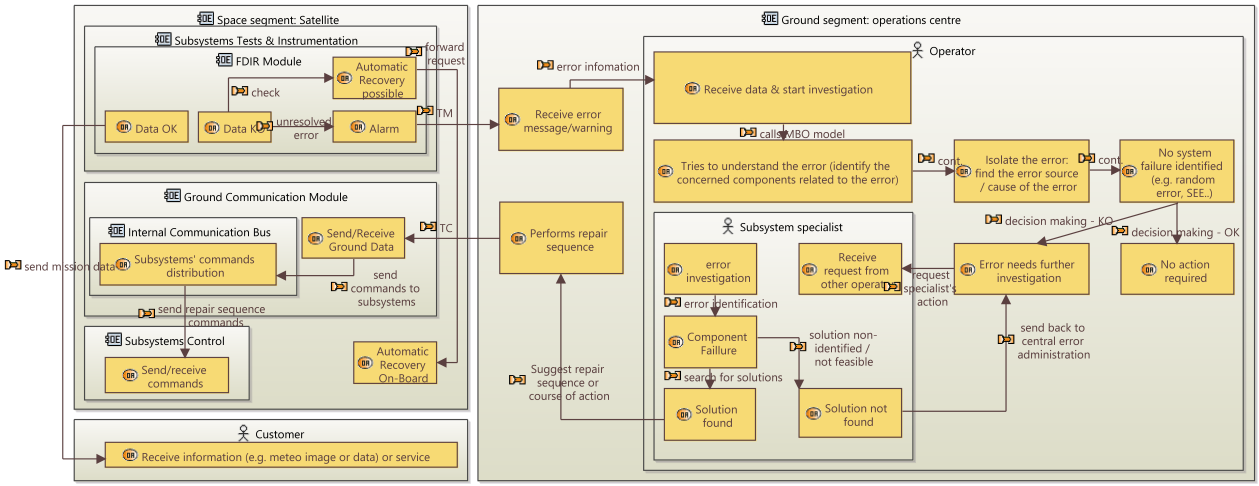

Figure 2 – Model example of the operational diagnosis procedure.

alarms. Figure 2 shows how these alarms are processed.

The satellite control centres receive the relevant data transmitted at each passage (TM) over the ground stations, and if these include any alarms (i.e. a potentially abnormal situation was observed), the operators start investigating the alarms raised, which may or may not correspond to failures. If not, the data can be processed to be sent to the customer -for our case, Earth-observation units. When looking for the cause of the alarms, the operators first exclude any subsystems and their components not related to the alarms and limit the search field of the possible alarm sources. The sources can be multiple as alarms can gather data coming from different parts of the satellite. When analysing the alarms in detail, the goal of the operators is to identify the real components in failure and restore the nominal configuration as close as possible (using nominal components rather than redundant ones). However the operators might sometimes find that the alarms have been raised simply as a warning, or that their cause was errors that have no impact on the system and that require immediate intervention, or that they simply resulted from a Single Event Effect (SEE, effect of a cosmic ray or particle), etc. In the latter case, the operators usually take no action (apart from logging the alarms).

After confirming the identification of the error, the operators and/or specialists need to suggest possible repair sequences and courses of action to be followed on board the satellite, through the control centres and the communication modules on earth and in space during the current or the next visibility windows. If these ones are not able to resolve the error, they send it back to the error handling centres to be assigned to other teams, with higher level of expertise, or related to other subsystems, as shown in figure 2.

The problem here is that, in worst-case scenarios, the above described procedure needs to be performed in very little time. In our case, the duration of the visibility window is a few minutes. More than often, the operators do not manage to analyse the alarms and identify the corresponding errors during this short visibility window, while the experts cannot propose associated repair actions, so they have to wait for the next satellite passage, and sometimes several windows are needed. *Losing several hours of satellite availability can cost a high amount of money.*

2.2 Operational Diagnosis constraints

The limited storage on board the satellite induces more restrictions for diagnosis. The satellite can only save some of the sensors' measurements every cycle, so the operators need to "tell" the satellite which data to record and transmit each time, that may be useful in analysing the alarms. Thus the limited resources and access make diagnosis a more critical process for space systems than for other kind of systems, resulting in high failure costs.

The system-related information which the operators process to assist them in diagnosis, comes from the system development activities performed earlier in the satellite design phases, especially system architecture and safety models production (encircled in figure 1). The result of this work are focused on models, which are produced by the system architects, functional leaders and safety analysts. These specialists have a thorough and deep understanding of the system architecture and all of its functions -in a design point of view, i.e., with a limited knowledge of the constraints the operators face in a day-to-day basis. Thus, these models usually fail to meet all of the operators' needs, since they could lack diagnosis-useful data or may contain too much unrelated information

that can lead to confusion and hold back the diagnosis performance.

The analysis of the current practise highlights the need for better diagnosis practices, and especially better assistance provided by data from development phases. We identified several pathways for improvement, that focus either in the system development phase or in the operation and maintenance phase: these two phases being interconnected. The pathway that is considered in this paper consists in improving the diagnosis process by introducing Model-Based Operations (MBO) models, in alignment with Model-Based Systems Engineering (MBSE) and Model-Based Safety Analysis (MBSA) models of the system. These models will facilitate the data management interoperability.

3 MODEL-BASED APPROACHES

As the complexity of systems rapidly increased, the use of model-based approaches has become widely spread in the industry, including the space domain. Among several, they offer two main interests: facilitating the system development and analyses (system design & dysfunctional analysis), as well as supporting the communication and collaboration between the engineering teams from different disciplines and various stakeholders. In particular, models are used in systems engineering to represent requirements, functions, architecture, and in dependability assessment, to analyse whether the system design exhibits weak points. This paper introduces how the satellite operational diagnosis will be improved thanks to the utilisation of this model-based approach linked to SE, Safety and in-service support processes.

3.1 Model-Based Systems Engineering

INCOSE[1] defines Model-Based Systems Engineering (MBSE[2]) as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life-cycle phases". MBSE is especially expected to replace the document-centric approach that has been practiced by systems engineers in the past decades and to influence the future practice of systems engineering by being fully integrated into the definition of systems engineering processes [INCOSE, 2020], while enhancing productivity and quality, reducing risk, and providing improved communications among the system development team. These models are formal accounts of the information provided previously in the documents as graphics or natural languages. Their formal nature enables their automatic processing by software tools to conduct automated validation/verification and model/code generation activities both offline and online (models at runtime that we target in our proposal).

3.2 Model-Based Safety Assessment

Model-Based Safety Assessment (MBSA) is a technique which models the system's structure and dysfunctional behavior in order to provide Safety analysis results, but also for Reliability, Availability and Maintainability (RAMS). In space missions, after the satellite has reached its final operational orbit, the focus is on Availability, i.e. the system's capability to be kept in a functioning state in the given environment, and Maintainability, i.e. the system's capability to be timely and easily maintained, including servicing, inspection and check, repair and/or modification.

In order to perform such dysfunctional analysis at system level, it is required to have a fundamental knowledge of (a) the nominal system behavior, limited to the scope and the level of abstraction useful for the dysfunctional analysis, in particular the reconfiguration and protection systems defined in the SE model, and (b) the various ways the failures can occur and propagate inside the system [Machin, 2019]. Consequently, MBSA uses a formal model describing both the nominal system behavior and the possible faulty behaviors, to analyse combinations of faults and their consequences in terms of availability and safety since, when a critical error occurs, the system is not available until the error is resolved.

3.3 Model-Based Diagnosis

Model-based Diagnosis is part of a larger task described in [Schwabacher, 2007] as Integrated System Health Management (ISHM), that includes both fault diagnosis and prognosis. The range of techniques used for system health management is represented in figure 3.

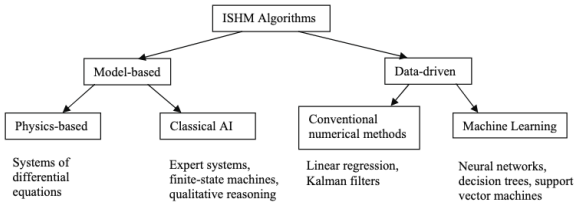

Figure 3 – Taxonomy of ISHM algorithms [Schwabacher].

Diagnosis can also be decomposed in several stages [Travé, 2006]: (a) **fault detection**, which aims at

[1] www.incose.org/
[2] www.omgwiki.org/MBSE/doku.php

discriminating normal system states from abnormal ones, i.e. states which result from the presence of a fault; (b) **fault isolation**, also called **fault localisation**, whose goal is to point at the faulty components in the system; (c) **fault identification**, whose output is the kind of fault and possibly the models of the system related to this fault. These tasks are usually identified by the **FDI** acronym, standing for **Fault Detection** and **Isolation**, and are often extended with a fault **Recovery** task, under the **FDIR** acronym. The more precise diagnosis stages require more precise models or data, which can be difficult to produce and validate.

4 A MODEL-BASED APPROACH TO IMPROVE OPERATIONAL DIAGNOSIS

The paper's proposal aims to support each considered life-cycle step (architecture design, availability analysis and diagnosis in operations) by models, to ensure precision, quickness and traceability in diagnosis. Our goal is to assist the operators in the troubleshooting phase, by providing easy access to the information relevant for diagnosis and repair design. This information will be organised into a Model Based Operation (MBO) model, depicted in figure 4, where the procedure the operator follows to isolate the source cause in using the MBO model is illustrated. Furthermore, we aim at partially automating the diagnosis procedure by providing appropriate computational tools. In order to implement this proposal, we plan to conduct a thorough domain analysis of the operation phase of the system life-cycle: how this phase is currently conducted by operators; what are the Process, Methods and Tools they rely on; and to model these elements. This will lead to a proposal of an ontology/metamodel for the operational phase and its relation with MBSE and MBSA.

In order to build the behavioural models in the design phase, we rely on standard languages, methods and tools, such as the SysML based Cameo Systems Modeller[3]. Regarding the availability analysis and diagnosis models, our purpose is to ensure efficient modeling so as to achieve their respective objectives. The process in which these models are created, updated and distributed amongst the engineering teams, also raises an important issue, related to the productivity of the availability analysis and diagnosis cycles.

4.1 Relationship between different kinds of models

If the same engineer was responsible for performing all steps of the process: system architecture, dysfunctional analysis, and production of the MBO model, all the consistency issues among the different types of models would be considered as solved. In reality however, this is not the case, since different specialists work concurrently on every step of the process. Availability analysts need to work with a "baseline" version of the SE model, i.e., a frozen version, that is not up to date to the latest changes done by the System architect. This de-synchronized work is required because analysis is time consuming, and the System architecture may evolve in the meantime.

At the end of each exchange cycle between the MBSE and MBSA teams, the consistency issues need to be tackled, for instance, performing version merging to re-synchronise availability analysis and MBSE. As a consequence, integrating MBSE and MBSA models into one model is not as efficient as expected, consistency-wise. Moreover, industrial tools able to achieve both objectives are currently not available. We thus prefer to consider two different models for MBSE and MBSA models and make explicit dependency relations between both models. As MBO models will gather data from both MBSE and MBSA models, we plan to rely on these explicit dependency relations in order to build the models.

4.2 The MBO model

Since MBSA requires the inclusion of information related to system failures, components faults and their propagation, the MBSA models are, unavoidably, manually produced (partially at least). On the contrary, the MBO model, as illustrated in figure 4, intends to gather information both from functional (MBSE models) and dysfunctional (MBSA models) in order to present to the operator data in a way that enables managing the strict timing constraints imposed by the space context. We therefore suggest generating the MBO model from both MBSE and MBSA models, and eventual generation configuration data if human expertise is needed in order to select the most appropriate data.

At the same time, as illustrated in figure 4, the MBO model will contain additional information, that are not available neither from the MBSE nor the MBSA generated models, i.e. the "operational knowledge". The goal is to integrate data from previous experience (faults occurred in the past, their identified source fault, their consequence in the system and their resolution), as well as the operators' expertise acquired through long experience in performing operational diagnosis activities, which only exists so far only in the form of human expertise, and not in the form of a model.

At the moment, verbalising the operators' and experts' diagnosis experience is studied only through experimental projects and in low maturity levels. We firmly believe that our proposal will bring a signifi-

[3] www.nomagic.com/products/cameo-systems-modeler

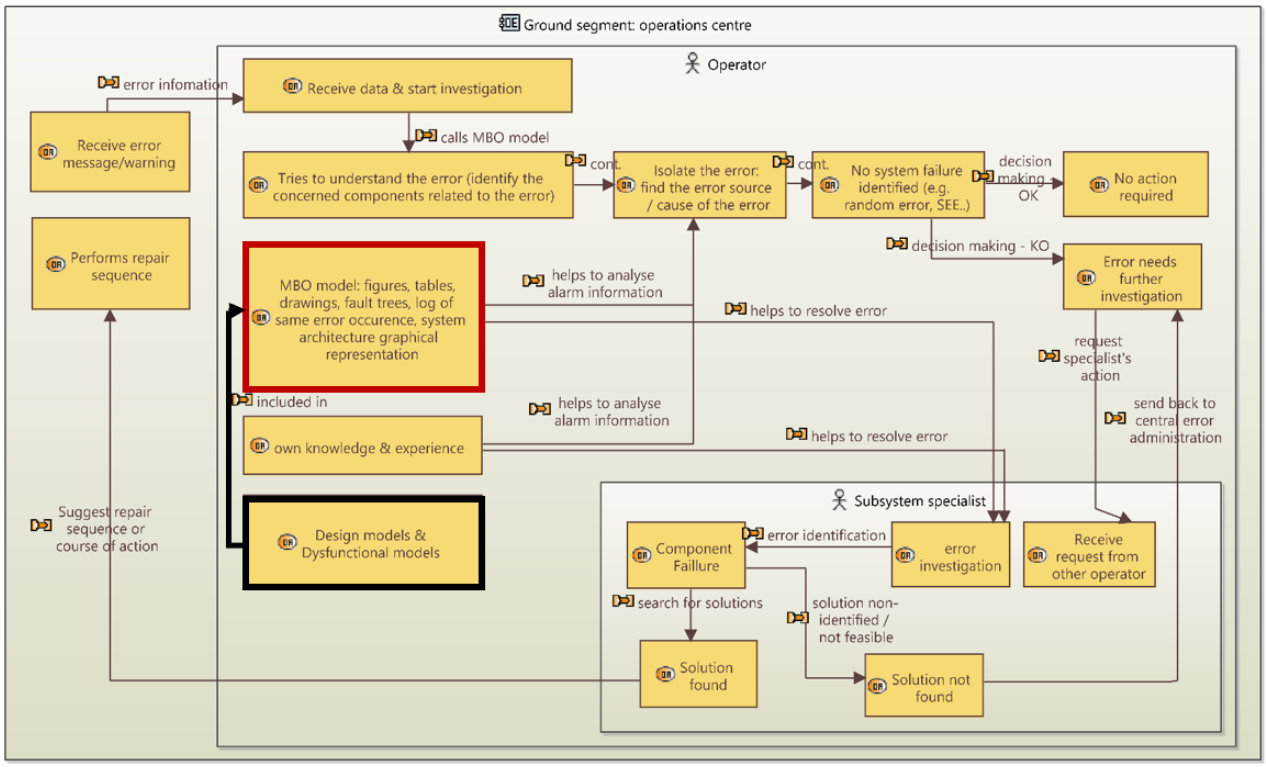

Figure 4 – Example of MBO model including the operational diagnosis procedure.

cant improvement in the operational diagnosis community. The elements presented in this paper are the results of an early coarse domain analysis of the space system operation activities. This work is currently being refined and extended to strengthen these results.

In our context and considering our goal, model-based diagnosis techniques will let us specify a way to enrich the MBO (diagnosis) model used in current practice in order to account for more information from the MBSA model. In return, given a precise definition of a MBO model, a range of techniques, based on constraint satisfaction and model-checking, can be used to ensure that different faults produce different symptoms in the MBO model. The precise nature of the algorithms to use depend on the content of the MBO model, and on the reasoning applied to transform observations (symptoms) into explanations (diagnoses).

4.3 Diagnosis approach

Each system component diagnosis can be performed with a technique appropriate to its physical nature (e.g. differential equations for AOCS, linear regression for power supply), to generate *health indicators* such as alarms and other signals. In contrast, the operator receives these health indicators and reasons at the global system level, where the techniques most appropriate are those that integrate well with MBSE and MBSA models.

Symbolic Artificial Intelligence approaches (in opposition to Machine Learning approaches), and in particular consistency-based diagnosis is particularly suitable for integrating knowledge from different sources, and can also be implemented over computation tools such as constraint solvers and SAT solvers.

Let us illustrate our approach with an application example. Suppose an alarm is triggered by the ground segment because some sensor data failed a quality test (e.g. blurry or under-exposed pictures, etc.), and the failure (bad picture quality) is confirmed by the operator. Consistency-based diagnosis can let us immediately rule out many components in the explanation of this alarm. Moreover, consistency-based reasoning lets us confront the initial symptoms and diagnosis test results with models of nominal and abnormal behaviour in order to detect, isolate, identify the fault, to assess that a new type of fault occurred, or to suggest that some parts of the models are wrong or outdated.

MBSE and MBSA models often account for the order of events under the form of state machines. Diagnosis also exists for discrete-event models [Zaytoon, 2013], as well as state estimation [Pralet, 2016]. Data-based (i.e. Machine Learning) approaches have been widely applied for monitoring industrial processes [Qin], and are a natural complement of model-based approaches.

Such approaches can be used as a way to generate new symptoms whose consistency with MBSE and MBSA models is used for diagnosis.

The aforementioned MBO model will gather the meaningful data from the separate development models and make explicit the relations and interactions between the various engineering domains involved in the development of the system. These relations can then be used in order to ease the different models' synchronisation as well as the integration of the various diagnosis conducted by the domain experts in a distributed diagnosis approach.

A list of possible explanations for the symptoms can be automatically generated with various techniques, including consistency-based diagnosis, or a data-based module. However, in the end, the final diagnosis is selected and validated by the operator(s).

5 CONCLUSION

In this paper, the authors defend that the use of model-based approaches in the design and dysfunctional analysis phases of a space system development cycle, in combination with the adoption of a MBO model during the operations and maintenance phase, following the satellite's deployment, can improve the current operational diagnosis practices. The goal is to integrate into one single model all the information useful to the operator to perform diagnosis efficiently. We believe that the proposed methodology and tools are particularly appropriate for application in the space systems domain, where MBSE and MBSA models already exist, so it is a good opportunity to use them for diagnosis.

Beyond recognised common interests, such as alignment in a collaborative way of working, the proposal of adopting a model-based approach that relies on a domain analysis of the operation phase within the life-cycle, will allow making the data (and their interconnection) related to the diagnosis and repair design processes, more explicit. In addition, it will also help making the actual processes and associated methodologies explicit, which one can improve by building tools to automate them.

ACKNOWLEDGMENTS

The authors thank all individuals, companies and research institutes involved in the S2C project of IRT Saint Exupéry and IRT SystemX and in particular, Airbus Defence and Space for proposing and supporting this research topic. This work is supported by the French Research Agency (ANR).

REFERENCES

Barreyre C., Laurent B., Loubes J.-M., Boussouf L., Cabon B., 2019. Multiple Testing for Outlier Detection in Space Telemetries. *IEEE Transactions on Big Data*, Vol. 6 Iss. 3.

Cloutier, R.J., 2019. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*. SEBoK Editorial Board, v. 2.1.

Esfahbod, B., 2013. Vee model for systems engineering process. *Wikimedia Commons*.

INCOSE, 2012. Systems Engineering Handbook (SEBoK): *A Guide for System Life Cycle Processes and Activities*, version 3.2.2. San Diego, CA, USA: International Council on Systems Engineering (INCOSE), INCOSE-TP-2003-002-03.2.2.

INCOSE SE Vision 2020. *INCOSE Technical proceedings*. INCOSE-TP-2004-004-02.

Kleer J., Kurien, J., 2003. Fundamentals of model-based diagnosis. *IFAC Proceedings Volumes*, 36.

Machin M., Saez E., Virelizier P., De Bossoreille, X., 2019. Modeling Functional Allocation in AltaRica to Support MBSE/MBSA Consistency. *Model-Based Safety and Assessment*, 3–17.

Pralet, C., Pucel, X., and Roussel, S., 2016. Diagnosis of intermittent faults with conditional preferences. *Proceedings of the 27th International Workshop on Principles of Diagnosis (DX'16)*.

Qin, S. Joe., Survey on data-driven industrial process monitoring and diagnosis, 2012. *Annual reviews in control* 36.2 (2012): 220-234.

Reiter, R., 1987. A theory of diagnosis from first principles. *Artificial Intelligence*, 32(1):57-95.

Schwabacher, M., and Goebel, K., 2007. A survey of artificial intelligence for prognostics. *AAAI Fall Symposium: Artificial Intelligence for Prognostics*, p. 108-115.

Takashi, I., 2000. *SATELLITE COMMUNICATIONS: System and its Design Technology*. Tokyo: OHMSHA/IOS Press.

Travé-Massuyès, L., Escobet, T., and Olive, X., 2006. Diagnosability Analysis Based on Component-Supported Analytical Redundancy Relations. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 36:1146-1160.

Zaytoon, J., and Lafortune, S., 2013. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control* 37.2: 308-320.