SpaceOps 2010 Conference<br> <b><i>Delivering on the Dream</b></i><br> <i>Hosted by NASA Mars
25 - 30 April 2010, Huntsville, Alabama

AIAA 2010-2231

A New Model-Based Approach for Specification Analysis and Refinement of Space Operations

Marcelo Henrique Essado de Morais[1] and Ana Maria Ambrosio[2]
National Institute for Space Research (INPE),
General Space Engineering and Technology (ETE),
Space Engineering and Technologies Course (CSE).
Av. Dos Astronautas, 1758 - São José dos Campos, SP,12227-010, Brazil.

ABSTRACT

In this paper we present a new approach to refine software requirements which may be applied to precisely define satellite operation requirements. The analysis and refinement is based on a test methodology that consists of a systematic way to model a system through Mealy Finite State Machines. The proposed approach has being applied in early phase of the ITASAT-1 Mission, a Brazilian university small-technological satellite as case study. It is presented the effectiveness of the approach and some results from previous works found in literature.

I. Introduction

This paper presents the use of a model-based approach for Verification and Validation (V&V) of satellite/software operation requirements for space applications. This work takes place in the context of ITASAT Program established by the Brazilian Space Agency (Agência Espacial Brasileira – AEB) and developed in cooperation by the National Institute for Space Research (Instituto Nacional de Pesquisas Espaciais – INPE), the Technological Institute of Aeronautics (Instituto Tecnológico de Aeronáutica – ITA) and other universities. The goals of the ITASAT Program are: (a) the generation of technological innovations for the aerospace sector; (b) the strengthening of the national industry; (c) the dissemination of knowledge; and (d) the training of human resources. This task is performed through conceptualization, design and development of small satellites and applied research related to national interests. The model-based approach for V&V of software requirement is based in a testing methodology. The idea of applying the testing methodology for satellite/software operation definition came from the good results obtained with CoFI (Conformance and Fault Injection) methodology on previous work[2,24]. As part of the ISVV (Independent Software Verification and Validation) process, the results with the application of the COFI methodology has surprised the mission management as many errors were found[3]. However, the errors were found only in latter phases. Thus a variation of COFI (Conformance and Fault Injection), named COFI-ref will be applied in early phases of the ITASAT Mission, as part of the mission requirement refinement. With this opportunity we intend to demonstrate the effectiveness of focus the designer's attention to incomplete, ambiguous and incorrect requirements that occur during the software development process and operations definition.

It is known that the software development process is conceptually an abstract form of model transformation. It starts from a stakeholder model requirements analysis and go through the system design model[4]. The success or failure of such transformation depends mainly of the initial model that captures the user needs. The same process occurs to acquire the user concerns for a space mission operation. Advanced satellite systems require new approaches not only in the area of the satellite itself but also in the field of operations[18].

In order to determine the feasibility and desirability of a suggested new major system and establish an initial baseline compatibility with ITASAT Program the proposed approach has been developed based on the operation modes of the spacecraft at system-level requirements.

[1] System Analyst/Master Degree Student, General Space Engineering and Technology (ETE): Space Systems Course (CSE), messado@dem.inpe.br.

[2] Satellite Simulations Group Coordinator, General Space Engineering and Technology (ETE): Ground System Development Division (DSS), ana@dss.inpe.br.

The positive points of this approach are:

a) To provide feedback for the development team through a new version of the DRD (Document Requirements Definition); and
b) To discover , since the early phases, the specification errors; and
c) To promote partial milestones before the formal requirements review, established in a space mission.

This paper is organized as follows:

- Section 2, describes the ITASAT Mission and its context for the Case Study;
- Section 3, describes the Problem Statement;
- Section 4, describes the COFI-Ref approach;
- Section 5, describes Related Works found in literature; and
- Section 6, describes a conclusion and future works besides the lessons learned whit the case study.

II. The ITASAT Mission

The increasing importance of small satellites for Earth Observation and other applications motivates the Brazilian Space Agency (AEB) to propose a technological development program to meet the demand for future generations of micro and nanosatellites in the Pluri-Annual Action, named “Development and launching small technological satellites” (4934 Action). This action consists of a series of space missions with capability to test experiments in orbit, develop and test innovations in the satellite and payload technologies, and improve the Brazilian space industry capabilities in this segment.

The ITASAT Program is supported by the AEB, aiming to improve Brazilian autonomy in the area of small satellites. It is also a principle to integrate industry and universities using international standards. In this context, the ITASAT-1 mission is the first mission of this program. The project shall be conducted in a way to enable to meet the objectives expressed, using for this purpose, consolidated practices in the project management, in the system engineering and knowledge management. Another goal is to improve management practices, as well as to create teaching and training mechanisms for the dissemination of those management practices for the National System for Space Activities Development.

The ITASAT-1 Mission comprehends the development, the launch and the operation of a small university technological satellite for use in a low Earth orbit, capable of providing data collection services as offered by the Brazilian Environmental Data Collection System, besides offering mean to test in orbit experimental payloads.

The Brazilian Environmental Data Collection System space segment operates with the SCD-1, SCD-2 and CBERS-2B satellites, and its basic idea is to automate the environmental data acquisition by means of a Data Collection Platform (DCP) that acquires, processes, and transmits messages in burst mode to the satellites in a repetition period of 40 to 220 seconds. When the satellite passes over the mutual visibility of the DCP and the Receiving Ground Station, a message transmitted by the DCP could be received at the Receiving Ground Station. As soon as the pass is over, all the received messages are sent by this station to the Data Collection Mission Center for further processing, data base management and data dissemination to the users.

The ITASAT-1 satellite shall carry on board the Digital DCS Transponder compatible with the existing in the SCD-1, SCD-2 and CBERS-2B satellites, as the main experimental payload.

Nowadays more than 700 data collection platforms were installed in Brazil, such as for hydrology, meteorology, water quality, oceanography studies. Potential applications such as fishing vessel monitoring and animal tracking are very important not only in term of commercial revenues but strategic in terms of environmental monitoring and wild life studies. More than 100 users’ organizations are registered to receive the data collected from the platform networks installed. Figure 1 depicts the ITASAT System related to the Data Collection System composed by the ITASAT-1 satellite (space segment) and the Data Collection ground segment.

The general architecture of the ITASAT System includes:

a) The ITASAT-1 spacecraft with the Digital DCS and other experimental payloads (space segment);
b) The TT&C Ground Segment with Cuiabá and Alcântara tracking stations; and
c) The Data Collection Ground Segment including DCP networks.

The spacecraft will provide the following bus functions: tracking, telemetry, command communications and data handling, passive attitude stabilization; attitude determination and control; sunlight power and battery storage; structural integrity; and passive thermal control.

The next section presents the problem statement.

III. Problem Statement

The ITASAT-1 System Engineering Team is responsible to produce the Documents for system-level and, though a formal review delivery the respective document to the V&V Team as starting point of Refinement process. As part of the COFI-ref (COnformance and Fault Injection for Requirements Refinement) approach showed on Figure 3 the Document Requirements Definition (DRD) is the input for the refinement process. This section will describe part of the DRD that contextualize the problem itself.

The mission cycle comprehends the following phases:

a) Assembly, Integration and Test Phase (AITP);
b) Launch Readiness Phase (LRP);
c) Pre-launch Phase (PLP);
d) Launch and Early orbit Phase (LEOP)
e) Commissioning Phase (CP);
f) Operational Phase (OP); and
g) Decommissioning Phase.

AITP - During the AITP the spacecraft is being integrated and tested. Also the ground segment is being prepared for the mission.

LRP - The LRP contains the finishing of all acceptance tests, the transportation to the launch site and the demonstration of the ground segment scope of operation. In this phase the staff for operation shall be instructed and trained.

PLP - The PLP contains the transportation at the launch site as well as the launch campaign which includes the servicing and the check-out of the spacecraft and its integration to the launcher, including latest checking.

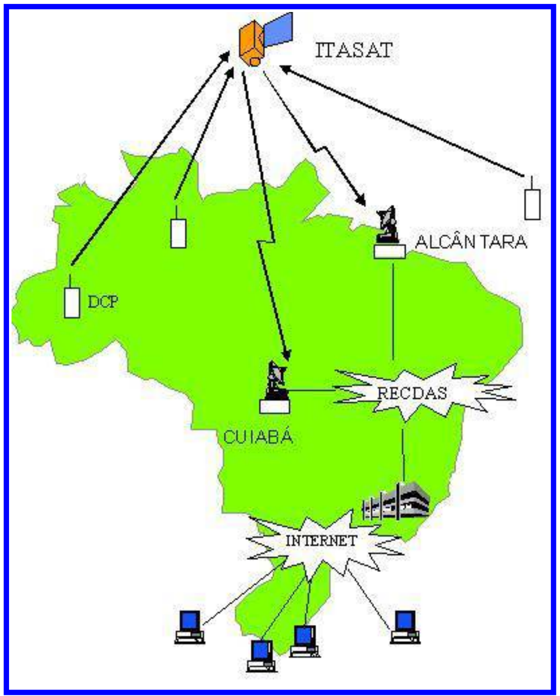

Figure 1. ITASAT System related to data collection, where the ITASAT-1 satellite plays a very important role to the continuity of the Brazilian Environmental Data Collection System.

LEOP - The LEOP contains the launch itself, the satellite separation from the launcher, the first initialization of the spacecraft as well the first acquisition of the spacecraft.

CP - At this phase the spacecraft has its first contact to the ground segment including the first transmission of telemetry data and the receiving of the first commands. Within this phase all subsystems and devices are tested and the attitude control subsystem starts to de-tumble the spacecraft for attitude stabilization. Alto the payloads are tested. The ground segment proves the operability and the customer confirms the functionality of the space segment as will be passed to the customer and changes to the Operational Phase.

OP - At this phase the operational use of the payload and the testing of the experimental payloads.

DP - If the operational lifetime is over and if the customer decides that the spacecraft shall be decommissioned his phase starts and if necessary a de-orbiting maneuver will be executed and the whole spacecraft will be decommissioned.

As part of the Mission Description Document the ITASAT-1 has 8 operational modes:

a) Launch Mode;
b) Survival Mode;
c) Testing Mode;
d) Alignment Mode;
e) Payload Mode;
f) Experimental Mode;
g) Operational Mode; and
h) Propulsion Mode.

Figure 2 shows the operational modes and the relationship between them. It is important to realize that this figure is drawn exactly as it is in the DRD.

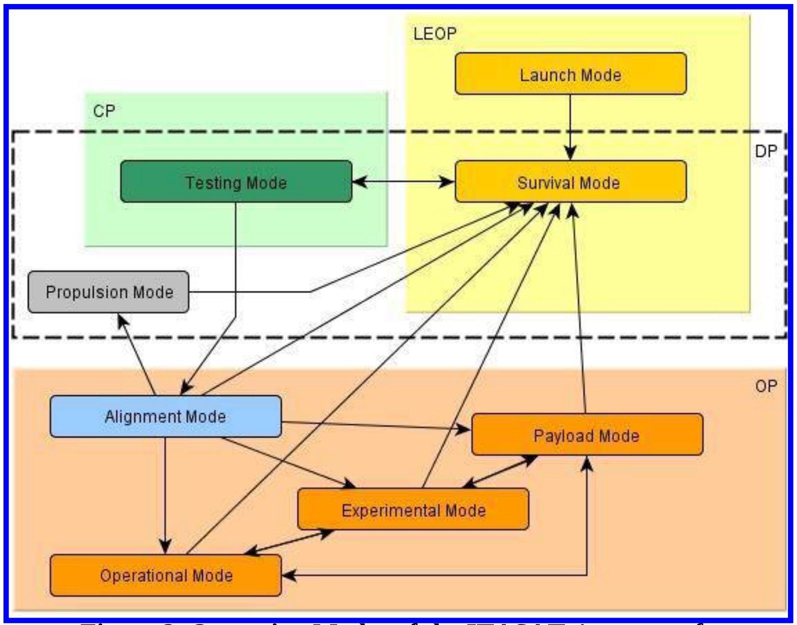

Figure 2. Operation Modes of the ITASAT-1 spacecraft.

From Figure 2 we realize that the Operation Modes merges between them. The Launch and Survival Modes belongs to the Launch and Early Orbit Phase as well as Testing Mode that belongs to the Commissioning Phase. However the Testing Mode, Survival Mode and Propulsion Mode belong to the Decommissioning Phase. Finally the Alignment, Operational, Experimental and Payload Modes belong to the Operational Phase.

A description of the operational modes is given below:

Launch Mode - During the launch the s/c (spacecraft) stays in the launch mode. It fulfills the launch provider requirements. There is no electric power supply for all subsystems and all mechanisms are securely locked.

Survival mode - After ejection the s/c changes into the survival mode. In this mode, the attitude of the s/c and its spin rate is undefined. In this mode all payloads (operational and experimental) are turned off. The same is ACS. In this mode the task of the s/c is to keep a positive energy budget over one orbit and to ensure it ability to communicate well. In the case of failure or malfunction that affects the whole s/c it switches into the survival mode automatically, independent of the current mode.

Testing mode - From the survival mode the s/c switches into the testing mode. This mode is a possibility to test all the subsystems and payloads before passing the s/c to the costumer. The testing mode provides all the functions of the survival mode and in this mode the first telecommand data will be received. After this mode the s/c can change to the alignment mode or the payload mode. Starting from this mode it also can be decommissioned.

Alignment mode - The alignment mode is for de-tumbling the s/c and to align it to specified orientations in the flight coordinate system. It is an intermediate mode from the Testing mode to the Payload mode, the Experimental mode, the Operational mode or the Propulsion mode.

Operational mode - In this mode the experimental payload is turned off and just the operational payload is working, besides the subsystems.

Propulsion mode - The Propulsion Subsystem is used for de-orbiting and therefore belongs to the Disposal Phase.

Payload mode - In this mode, achieved from Alignment mode by ground command, all satellite subsystems including the payload, but excluding the possible propulsion system, is in their final operating configuration. The mission technological data is being collected and transmitted to Earth during visible passes.

Experimental mode - In this mode besides the subsystems just the experimental payloads are working. This mode provides time to do experiments and to test for example the new onboard computer

To complement the description of the Operational Modes, Table 1 presents the relationship between the subsystems and its modes of operation.

Table 1. Operation Modes versus Subsystems.

Modes / subsystems	TCS	EPS	TT&C	ACDH/OBDH	ACS	Exp. Payload	Operational Payload	Propulsion System
launch mode	off	off	off	off	off	off	off	off
survival mode	on	on	on	on	off	off	off	off
testing mode	on	on	on	on	on	test	test	off
alignment mode	on	on	on	on	on	off	off	off
payload mode	on	on	on	on	on	on	on	off
experimental mode	on	on	on	on	on	on	off	off
operational mode	on	on	on	on	on	off	on	off
propulsion mode	on	on	on	on	on	off	off	on

Next section will present a description of the COFI-ref methodology.

III. COFI-ref Methodology Description

The COFI testing methodology consists of a systematic way to create test cases for reactive systems. The system to be tested is modeled in Mealy machines. In COFI the system behavior is partially represented in state models where transitions represent inputs and outputs of the interfaces. The COFI-ref is based on the COFI.

The COFI-ref methodology comprehends 4 main steps, as illustrated in figure 3:

a) DRD Acquisition
b) Identification;
c) Model-Based Modeling; and
d) Requirement Refinement.

The DRD (Document Requirements Definition) is the input of the COFI-ref. In the first step, the team in charge of the system specification, before a project review, provides the DRD for the COFI-ref team. This is what we call "DRD Acquisition". The second and third steps were extracted from the standard COFI methodology. The tasks involved in second step, the Identification, are:

a) Identify the services that a user recognizes;
b) Identify hardware faults that can occurs (and that system shall resist);
c) Identify the events (inputs) and reactions (outputs) of the system.

For the case study the services that a user recognize is related to the Operation Modes itself. Table 2 presents the hardware faults that can occurs to the system. In the first column is presented the subsystem while second one its acronym. On third column a short description of the fault is showed.

For step 3 we have to create partial models based on Finite State Machines. The tasks involved are to define, for each Service previously created:

a) Normal Operation Mode;
b) Specified Exception;
c) Sneak Paths; and
d) Fault Tolerant.

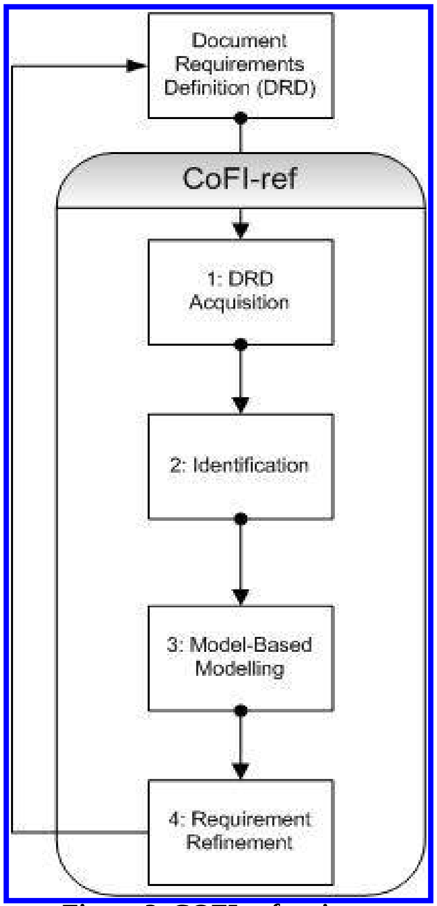

Figure 3. COFI-ref main steps.

Table 2. Physical Failures that may occur.

Item	Acronym	Description
Experimental Payload	f.opp	an anomaly on satellite operational payload
Operational Payload	f.exp	an anomaly on satellite experimental payload
Payload	f.pay	an anomaly on satellite payloads
Propulsion	f.prp	an anomaly on propulsion subsystem
Satellite bus	f.bus	an anomaly in satellite bus: thermal control, attitude and orbit control, power, on-board computer, tt&c
Structure	f.str	structure with an anomaly

In order to present the case study, Figure 4 shows the Normal Operation Mode behavior through a Finite State Machine (FSM). The initial state is Launch Mode whereas the final one is Survival Mode. The transitions between the states are signed with a letter. Table 3 identifies these transitions and shows the result of the step 2, "Identification: the events (inputs) and reactions (outputs) of the system to be operated."

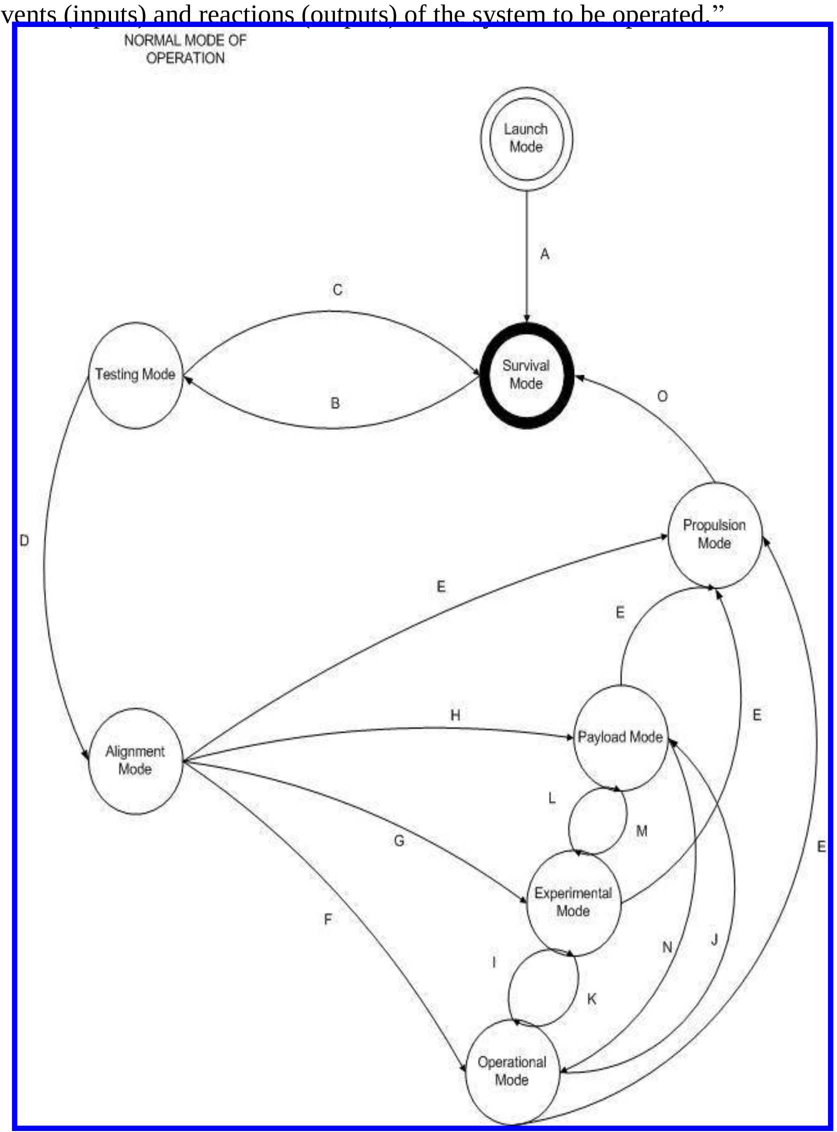

Figure 4. Finite State Machine representing the Normal Operation Mode.

Table 3. List of Events (inputs) and reactions (outputs) of the system to be operated.

Acronym	Events (Input)	Description	Actions (Output)	Description
A	FIRST_TC	send first s/c telecomand	FIRST_TM	receive s/c first telemetry
B	PAYLOAD_TEST	init s/c payload test	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_OFF; EXP_TEST; OPP_TEST; PRP_OFF	evaluate s/c payload test
C	PAYLOAD_TEST_NOK	s/c payload test ok	SC_MALFUNCTION	s/c payload test evaluated
D	PAYLOAD_TEST_OK	experimental and operational payload tests ok	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_OFF; PRP_OFF	alignment operation mode
E	SC_DECOM	de-orbiting maneuver is executed	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_OFF; PRP_ON	
F	OPERATIONAL_INIT	de-tumbling operation	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_ON; PRP_OFF	operational payload is turned on
G	EXPERIMENTAL_INIT	turn on the experimental payloads	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_ON; OPP_OFF; PRP_OFF	experimental payload is initiated
H	PAYLOAD_INIT	turn on the payloads	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_ON; OPP_ON; PRP_OFF	all satellite subsystems including the payload are turned on
I	OPP_2_EXP	to init the operation of experimental payload	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_ON; OPP_OFF; PRP_OFF	experimental payload is initiated
J	OPP_2_PAY	to init the operation of payloads	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_ON; OPP_ON; PRP_OFF	all satellite subsystems including the payload are turned on
K	EXP_2_OPP	de-tumbling operation success	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_ON; PRP_OFF	operational payload is turned on

L	EXP_2_PAY	operational payload is off and payload must start	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_ON; OPP_ON; PRP_OFF	operational payload is turned on
M	PAY_2_EXP	operational payload is on and ground station has visibility of the s/c	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_ON; OPP_OFF; PRP_OFF	operational payload is turned off and data transmistion starts
N	PAY_2_OPP		TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_ON; PRP_OFF	
O	PROPULTION_INIT	initiate propulsion and s/c starts to de-orbiting	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_OFF; PRP_ON	disable payloads and starts the disposal
P	PAYLOAD_NOK	malfunction of payload	SC_MALFUNCTION	s/c switches into survival mode
Q	EXPERIMENTAL_NOK	malfunction of experimental payloads	SC_MALFUNCTION	s/c switches into survival mode
R	OPERATIONAL_NOK	malfunction of operational payload	SC_MALFUNCTION	s/c switches into survival mode
S	SC_TEST_DECOM	from this mode it also can be decommissioned	TCS_ON; EPS_ON; TT&C_ON; ACDH_ON; ACS_ON; EXP_OFF; OPP_OFF; PRP_ON	to be decommissioned the s/c shall go to propulsion mode
T	ALIGNMENT_NOK	if a malfunction of the s/c occurs on alignment mode	SC_MALFUNCTION	s/c switches into survival mode

The last step, the Requirement Refinement represents the refinement itself. This step requires the inclusion of some other steps as shown in Figure 4. It represents the innovation on COFI standard methodology.

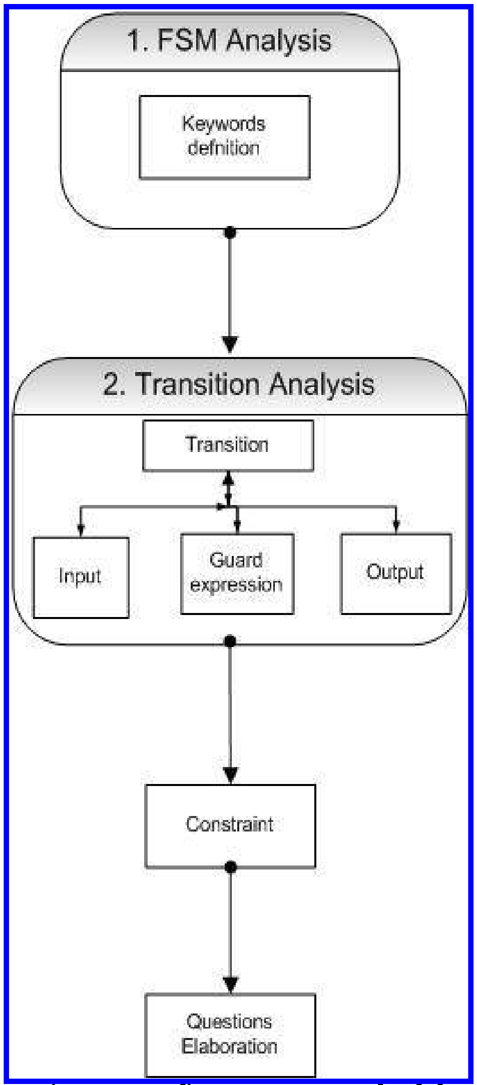

Figure 5. Steps of the Requirement Refinement approach of the COFI-ref methodology.

The steps included in the Requirement refinement are:

a) To identify the keywords on Partial Models;
b) To analyze the transition. Its inputs, guards and actions;
c) To identify the constraint of the System to be operate; and
d) To formulate simple questions based on the previous steps.

With the ITASAT-1 DRD the V&V Team starts to apply the methodology. To start the refinement we must keep in mind that we will work with three major areas:

a) The semiotics;
b) The grammar of the language; and
c) The properties and attributes of the requirements.

The next section describes the refinement approach based on Figure 4.

A. The Refinement Requirements Approach

In this section we describe the refinement approach applying it on the case study proposed.
Based on the FSM showed in Figure 4 we defined the following keywords:

a) First;
b) Payload;

c) Spacecraft;
d) Operational; and
e) Experimental.

Through Transition Analysis, presented in Figure 5, we raise questions whose answers are not necessarily found, for instance:

a) How the System knows what will be its state right after the alignment?
    i. It will be a telecommand from Ground Station or an on-board command?
b) Is it possible to change the satellite state from Operational, Experimental and Payload Modes to Propulsion Mode if the spacecraft shall be decommissioned?
c) It makes sense if the spacecraft starts a de-orbiting maneuver from any states other than Survival, like in Testing Mode?

For the Constraints of the system to be operate the FSM modeled on previous step can show exactly what is needed. The Figure 6 presents the Fault Tolerant model, in order to illustrate these constraints whereas The new transitions are based on the physical failures defined previously, on Table 2..

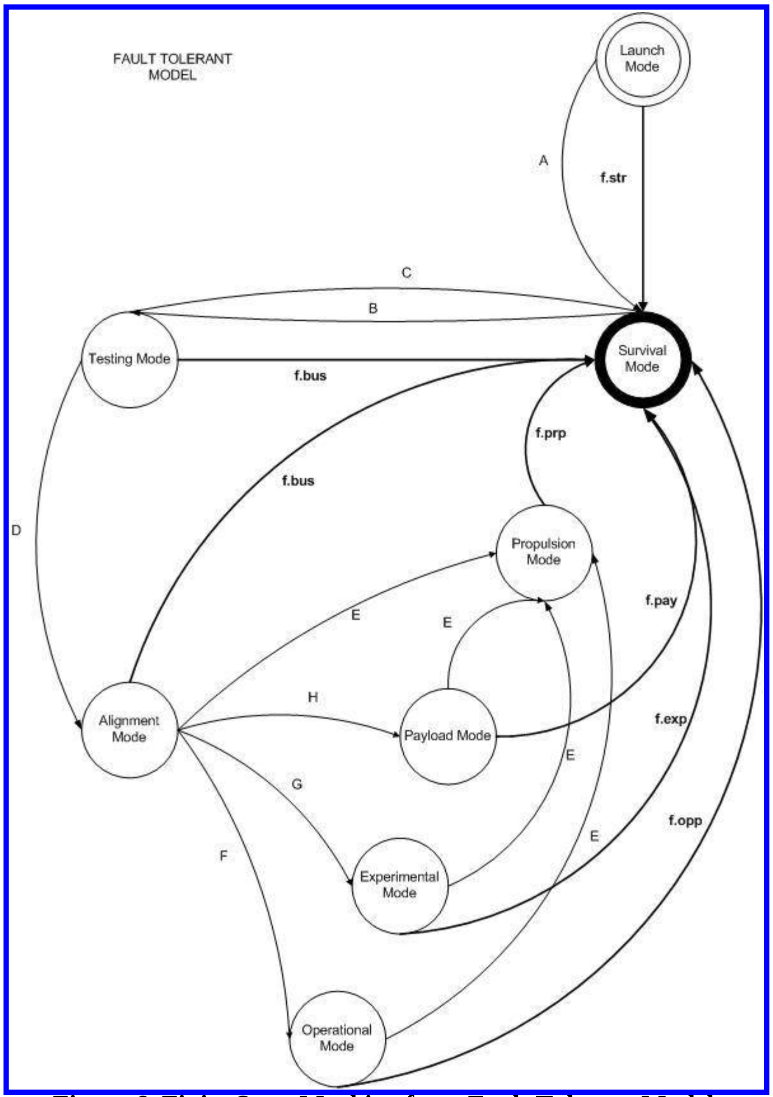

Figure 6. Finite State Machine from Fault Tolerant Model.

Now, the last task of Refinement comprises of elaborating questions based on the previous results. This process is based on a inductive process extract from empiric observations[22,23,27].

a) Could the spacecraft, during the Testing Mode, be decommissioned without pass through the Survival Mode?
b) When and what the circumstances, besides a failure, the spacecraft will be decommissioned on Testing Mode?
c) Is it correct that the spacecraft never goes to Alignment Mode if any of the payloads fails? That is, the spacecraft never will be monitored if a payload fail occurs?
d) Is it correct that the satellite shall go to the Alignment Model if just one of the payloads work well?

B. Contribution to the DRD

In order to turn the contributions a simple process this part of the COFI-ref includes textual elements of the language which is write follow the good practices for writing requirements.

1. The spacecraft shall know which is the next state after the Alignment Mode through:
   a) Telecommand from Ground Station; or
   b) On-board command.

2. The satellite shall be decommissioned from the following Operation Modes:
   a) Testing Mode;
   b) Alignment Mode;
   c) Payload Mode;
   d) Experimental Mode; and
   e) Operational Mode.

Notes:

i. This kind of solution implies that the implementation of each one of these states (operation mode) should carry an equal function call. On the one hand it could be better to decentralize the code, on the other hand, it’s bad because to implement it will need more code lines. See transition E on Normal Operation Mode.

ii. Is really necessary to start a decommission of the spacecraft on Testing Mode? Initially it will happen only if a failure or malfunction occurs what, in fact, the spacecraft will go to Survival Mode. The transition S on Specified Exception and Sneak Path 2 cover this decommissioning event.

3. The satellite, during the Testing Mode shall go to Survival Mode if a failure occurs on Experimental Payload Test.

3.1. The satellite, during the Testing Mode shall go to Survival Mode if a failure occurs on Operational Payload Test.

Note: If a failure occurs like the spacecraft never goes to Alignment Model. Is it right?

Based on this refinement process some proposals can be made in order to optimize the system:
a) Describe textually the details about the operational modes, like proposed above;
b) Insert two diagrams to show the model behavior. One representing the Normal Operation Mode and another one the Specified Exception Model.

This two recommended solutions will causes that the three different levels of requirement customers: (a) the stakeholders, (b) the system architect and (c) the system developer speaks the same language and can understand themselves.
The next section presents some related works and shows its results.

IV. Related Works

Nowadays has been much research in areas like Requirement Engineering[17, 25, 26]. The requirement specification is a complex task, due to its degree of abstraction, time-consuming, expensive and error-prone. According to Cybulski (2002) more than 56% of all software defects are due to error introduced in requirements specifications, taking up to 82% of development time to fix.

Related researches to Requirement Engineering shows problems related to the bad requirements specification. In Duren (2006) study for Validation of Mission Space, the author presents the problems associated with the activities of the life cycle requirements. His research is related with cost and schedule of the mission from the requirements, until the final stages of operation and maintenance. Table 4 presents the results of his work. The first column shows the mission and their respective year. The second describes the problem found and the third shows the validation activities that contributed to the mission failure.

Table 4. Excerpts from NASA Mishap reports. Adapted from Duren (2006).

Mission/year	Mishap	Validation-related Contributing Factors
Genesis /2004	G-switch installed backward → parachute not deployed → hard landing	"no system-level test" (of G-switch)\
Columbia /2003	debris damaged thermal tiles → loss of crew and vehicle	"Current tools, including the Crater model are inadequate…." "flight configuration was validated using extrapolated test data(…) rather than direct testing"
Comet Nucleus Tour(CONTOUR) /2002	overheating of s/c by solid rocket motor plume → vehicle lost	"Project reliance on analysis by similarity"
Wide-field infrared Explorer (WIRE) /1999	electronics startup transient → early cover jettison → cryogen boil-off → science mission lost	"failure to correctly identify the source of the signal which caused the Electro Explosive Device (EED) Simulator to "latch" upon Pyro Box power-up during spacecraft integration testing".
Mars Polar Lander (MPL) /1998	software flaw → descent engine shutoff too soon → vehicle lost	"employed analysis as a substitute for test in the verification and validation of total system performance…tests employed to develop or validate the constituent models were not of an adequate fidelity"

This relation shows the importance that this kind of studies, that dealing with the improvement of V&V activities focused on space applications.

Our work aims to contribute to a systematic V&V during the initial phase of the project activities what involves the Requirement Engineering. It is known that the requirements specification is the result of an interactive process between stakeholders and systems architect, both of which will gradually improving its knowledge of the system to be operate or under development. Table 5 summarizes works identified in literature with similar proposals. The first column shows the authors. The second identifies the problem, while the third presents the proposed solution. In the fourth and fifth columns are exposed the limitations of the techniques and advantages discussed by the author.

Table 5. Comparison between works related to the requirement engineering and modeling.

Author/year	Problem description	Proposal solution	Limitation	Advantage
Garcia-Duque et al (2009)	How to identify and storage the knowledge on each project review ?	Formulation of two methodologies to conduct the activities on analysis and requirement reviews on a automatic way.	It is not evaluated inconsistency and conflicts between the requirements.	Integrate of two formal method techniques.
Halligan (2003)	**1.** identify metrics that can be used to the requirements or to the process (requirement engineering) or both. **2.** How metrics can meet the design	**1.** Metrics definition; **2.** Parser element definition.	It is unknown the cost of implementing these metrics. However it is expected to account 2% of the total amount of requirement engineering efforts.	**1.** The metrics follow the ISO and MIL standards. **2.** Seems to be feasible for complex systems.

	criteria?			
Liu (2002)	**1.** How formal methods can help the user to seek, identify and explain the largest possible number of requirements themselves wants? **2.** Non-determinism of functional requirements (more than a transition to a single event).	Refinement of requirements on formal (formal specification techniques), informal (natural language representation) and semi-formal (graphical language).	Non functional to operation on large scale. In this case the refinement operation can be realized by a software program.	Use formal techniques for refinement as a means to capture certain requirements and correct them.

V. Conclusion and Future Works

This work presented a refinement approach based on formal methods. It has been applied on a study case of the ITASAT Project, a Brazilian small-technological satellite.

It was showed that it is possible to refine a Document Requirements Definitions using formal language following the mathematical rigor, once we use the Finite State Machines and its own properties.

The refinement is based on the grammar of the language that it is applied. Many authors describes the refinement through some mathematical formalism, however the use of formal methods show us that this formalism is used and one of the COFI-ref methodology concern is to hidden the mathematical formalism in a way that these properties still be followed.

The Lessons Learned showed us that how more the individuals are trained more effectiveness it will be the results. In other words, the analysts must have at least an intermediate knowledge about the methodology and the correlates techniques like: formal methods, automata theory, analysis and systems development, programming, parsing, etc.

The Future Works relies on the development of the COFI-ref process in a manner of make some comparisons between similar techniques, like presented on Table 5 and to develop some metrics to the refinement itself.

ACKNOWLEDGMENT

We are gratefully to the Brazilian Space Agency (AEB) for fund the project and the financial support of the following entities: FAPESP, CNPq, CAPES and FINEP. We would like to thanks Dr. Davi Fernandes at ITA and Dr. Wilson Yamaguti at INPE the Project Managers and other colleagues of the ITASAT Program.

References

[1] Ambrosio, A. M., Eliane Martins, N.L.Vijaykumar, S.V. de Carvalho. “Systematic Generation of Test and Fault Cases for Space Application Validation.” *Proceedings of the 9th ESA Data System in Aerospace (DASIA), 30 Mai – 2 Jun. 2005,* Edinburgh, Scotland. Noordwijk: ESA Publications, 2005. Papers on Disc [CD-ROM].

[2] Ambrosio, A. M.; Martins, E.; Vijaykumar, N.L.; de Carvalho, S.V. “A Conformance Testing Process for Space Applications Software Services.” *JACIC - Aerospace Computing, Information, and Communication, Vol.3, N.4, pp.146-158*. Publisher American Institute of Aeronautics and Astronautics - AIAA, April 2006, USA.

[3] Ambrosio, A. M.; MAattiello-Francisco, M. F.; Martins E. "An Independent Software Verification and Validation Process for Space Applications." *In: CONFERENCE ON SPACE OPERATIONS 9. (SPACEOPS 2008), 2008*, Hidelberg. Proceedings... 2008. p. 9. CD-ROM. (INPE-15303-PRE/10112).

[4] Aydal, L, E. G., PAIGE, R. F., Utting, M. & Woodcock, J. (In Press). “Putting formal specifications under the magnifying glass: Model-based for Validation.” *In Proceedings of 2nd International Conference on Software Testing, Verification, and Validation*, Denver, Colorado, USA, April 1-4, 2009.

[5] Best Practices Working Group of the Space Operations and Support Technical Committee (SOSTC) of the American Institute of Aeronautics and Astronautics. “Satellite Mission Operations Best Practices.” *AIAA Space Operations and Support Technical Committee (SOSTC). April, 2003*

[6] Cybulski, J. L. “Automatic Refinement of User Requirements: A Case Study in Software Tool Evaluation.” *Proceedings of the Thirteenth Australasian Conference on Information Systems*, pp. 757-771, Victoria University, Melbourne, Australia, 2002.

[7] Darimont, Robert and van Lamsweerde, Axel. “Formal refinement patterns for goal-driven requirements elaboration.” *SIGSOFT Software Engineering Notes*, 1996, vol. 21, pages 179-190.

[8] De Jong E., Jaco van de Pol, Jozef Hooman. “Refinement in Requirements Specification and Analysis: a Case Study.” *In 7th IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS)*, 2000, pages 290-298.

[9] Duren, R. M. “Validation (not just Verification) of Deep Space Missions.” *IEEE Transactions*, March 2006, 13pp.

[10] ECSS-E-10 Part 1B, Space Engineering - System Engineering - Part1: Requirements and process. 18 November 2004.

[11] ECSS-E-40 Part 2B, Space Engineering - Software - Part 2: Document requirements definitions (DRDs). 31 March 2005.

[12] ECSS-E-70 Part2A, Space Engineering - Ground systems and operations - Part2: Document requirements definitions (DRDs), 2 April 2001.

[13] ECSS-E-ST-70-11C, Space Engineering - Space segment operability. 31 July 2008.

[14] ECSS-M-ST-10C, Space Project Management - Project Planning and implementation. Revision 1, 6 March 2009.

[15] Garcia-Duque Jorge ; Pazos-Arias José J. ; Lopez-Nores Martín ; Blanco-Fernandes Yolanda ; Fernandez-Vilas Ana ; Diaz-Redondo Rebeca P. ; Ramos-Cabrer Manuel ; Gil-Solla, Alberto. “Methodologies to evolve formal specifications through refinement and retrenchment in an analysis and revision cycle.” *Requirements Engineering Journal*, vol. 14, 2009, pages 129-153.

[16] Halligan, R. “Requirements Metrics: The Basis of Informed Requirements Engineering Management.” *In: COMPLEX SYSTEMS ENGINEERING AND ASSESSMENT TECHNOLOGY WORKSHOP*, 1993, Naval Surface Warfare Center, Dahlgren, Virginia. Proceedings.

[17] IBM Corporation. “Get It Right the First Time: Writing Better Requirements.” 2008.

[18] IEEE Std. 830-1998. “IEEE Recommended Practice for software Requirements Specifications*.” IEEE Computer Society*, 1990.

[19]Landua, B.; Kesenheimer, H., "Efficient Approaches to Satellite Operations, " Space Mission Operations and Ground Data Systems - SpaceOps '96, *Proceedings of the Fourth International Symposium* held 16-20 September 1996 in Munich, Germany. Edited by T.-D. Guyenne. ESA SP-394. Paris: European Space Agency, 1996., p.1306

[20] Letier, Emmanuel and Van Lamsweerde, Axel. “Reasoning about partial goal satisfaction for requirements and design engineering.” *SIGSOFT '04/FSE-12: Proceedings of the 12th ACM SIGSOFT.* Twelfth international symposium on Foundations of software engineering, 2004, pages 53-62.

[21] Liu, S. “Capturing Complete and Accurate Requirements by Refinement.” *IEEE International Conference on Engineering of Complex Computer Systems*, 2002.

[22]Peirce, C. S., "How To Make Our Ideas Clear", Popular Science Monthly 12. Indiana University Press, 286-302 o., 1878.

[23] Polya, G. "How To Solve It: A New Aspect of Mathematical Method", 2nd ed., Princeton University Press, New Jersey, 1957.

[24] Pontes, R. P.; Morais, M. H. E.; Veras, P. C.; Ambrosio, A. M.; Villani E. “Model-based Refinement of requirement specification: A Comparison of two V&V Approaches.” *COBEM, International Congress of Mechanical Engineering*, November 15-20, 2009, Gramado, RS, Brazil.

[25] Pressman, R. S. “Software Engineering. A Practioner´s Approach.” Mcgraw-Hill, 2005.

[26] Sommerville, I. “Software Engineering.” Addison-Wesley, 8th ed., 2007.

[27] Tall, D., "The Psychology of Advanced Mathematical Thinking", in Tall D. O. (ed.) Advanced Mathematical Thinking, Kluwer: Holland, 3– 21.