MINISTÉRIO DA CIÊNCIA E TECNOLOGIA
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

INPE-14074-PRE/9243

SAFETY IN A WEB-BASED SATELLITE FLIGHT PLAN SUPORTING SYSTEM

Maria de Fátima Matiello-Francisco
Benedito M. Sakugawa
Edgar Toshiro Yano

Paper presented at the Data Systems in Aerospace – DASA 2005, May 30th to June 2nd 2005 – Edinburgh, Scotland.

INPE
São José dos Campos
2006

Safety in a Web-based Satellite Flight Plan Supporting System

M.F. Mattiello-Francisco[1]
National Institute for Space Research – INPE, São José dos Campos, Brazil

B.M. Sakugawa[2]
Civil Aviation Certification (CAvC/IFI/CTA), São José dos Campos, Brazil

and

E.T. Yano[3]
Aeronautical Institute of Technology - ITA, São José dos Campos, Brazil

This paper is an experience report in applying safety concepts from IEC 61508 – Safety Life Cycle approach to the Web application software developing for scientific satellite mission operation. The system, named Flight Plan Supporting, is part of the Ground Segment facilities and aims to aid the scientific investigator in controlling the on-board satellite payload remotely by using Internet. The safety concepts were useful to reduce risks identified in the system conception. The hazard and risk analysis contributed to provide the design of the software system with mechanisms to minimize faults. **Keywords: Web application, safety system, IEC-61508, satellite operation, risk analysis.**

I. Introduction

IN order to reduce cost in scientific satellite missions, the scientific payload is moving towards operational independence from the satellite platform. More and more the scientific community is involved in the satellite operation routine. SACI (Brazilian Scientific Application Satellite) project took on this challenge providing the principal investigators with facilities to remotely control their on-board instruments via Internet [1].

A software system based on open source technology was required to support SACI Flight Plan preparation. The system allows the user to edit, organize and schedule remotely, via WEB pages, the telecommands (TCs) to be sent to the satellite and executed on-board later. Figure 1 shows a view of SACI Ground Segment where the scope of Flight Plan Supporting system – FPS is in evidence. It consists of a distributed system with Data Base SERVER in Linux platform and uses a client/server model of communication. The scientific community users, meaning the principal investigators responsible for operating the instruments on-board of a satellite, are connected to the Internet through a WWW Browser.

Since the satellite payload operation would be distributed, an important concern was to apply the system safety approach in the project development. System safety attempts to identify potential hazards before the system is designed to define and incorporate safety design criteria, and to build safety into the design before the system becomes operational [2].

Therefore, the development lifecycle followed the IEC 61508 model [3]. The design and development of safety-critical systems, according to IEC 61508, considers the development processes throughout its various stages following an overall safety lifecycle. It covers all aspects of a system's life, from conception to decommissioning, and also considers the diverse aspects of its realization. Safety lifecycle is very similar to overall system lifecycle, with the additional hazard and risk analysis phase, as part of the system requirements phase.

[1] Technologist, DSS, Av. dos Astronautas, 1758 São José dos Campos – 12227-010 Brazil, fatima@dss.inpe.br.
[2] Technologist, IFI, Pça Marechal Eduardo Gomes, 50 São José dos Campos – 12228-901 Brazil, benedito.sakugawa@ifi.com.br.
[3] Technologist, ITA, Praça Marechal Eduardo Gomes, 50 São José dos Campos – 12228-901 Brazil, yano@comp.ita.br.

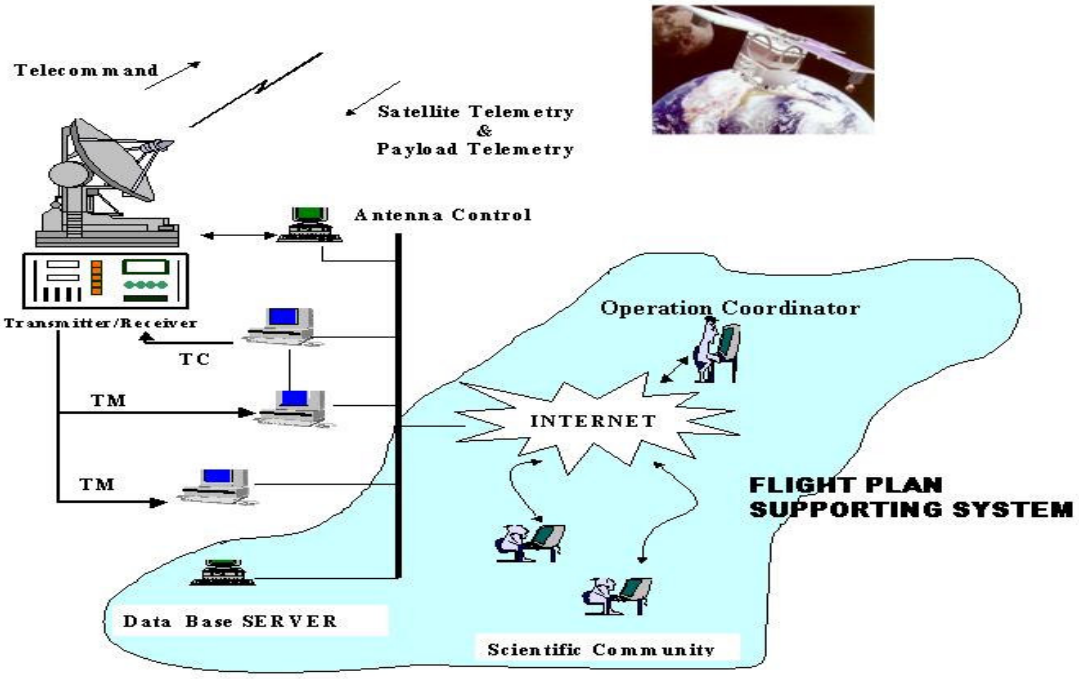

Figure 1. Scope of Flight Plan Supporting System in the Satellite Ground Segment

The IEC 61508 standard demands that safety requirements are associated with four values of Safety Integrity Levels (SIL). SIL is a target for the probability of a dangerous failure. The integrity level is a classification of risk associated with a safety requirement. The IEC 61508 Safety Lifecycle is a risk-driven development approach. A SIL value assigned to a software element will determine the development methods used and the level of testing performed.

II. Vision of the Solution

In general, the scientific satellite missions approach is a set of technological and/or scientific instruments for space data acquisition in order to validate a theory or an engineering solution. Although the instruments are related to the satellite mission purpose, charactering the mission payload, a degree of independence among them is supposed. This aspect allows each principal investigator to control his/her experiment, increasing the operation efficiency and reducing costs. Differently from the satellite conventional way of operation, centralized in Operation Controlling, an automatic Flight Plan facility explores the Principal Investigators (PI) ability in controlling their experiment potentiality in collaboration with the Operation Coordinator (OC).

The identification of stakeholders' profiles was essential to base the vision of the solution and to define the user's role and system interface with other systems presented in Ground Segment, such as the Orbit Determination System and TC Transmission System. The diagram in Figure 2 presents the relationship between FPS system and users (PIs, OC and Database Administrator – AD) as well the data communication with the external subsystem mentioned above.

From this context and system needs, the FPS system conception was based on the advantages and risk of implementing the new solution taking into account the hazards associated to the solution. Early in the system requirement definition, system objectives and success criteria were analyzed in order to identify aspects of the software system related to risks such as WEB transaction vulnerability for intrusions, lacks of integrity into Data Base SERVER for providing PIs with reliable TCs, and high dependence on TC code automatic generation. For instance, a *system objective* is **SO** – Explore the scientific potential of the instrument with more efficiency, mainly in degraded operation. A *success criterion* can be SC – Less rejected TC rate received on board due to inconsistency reported in housekeeping telemetry.

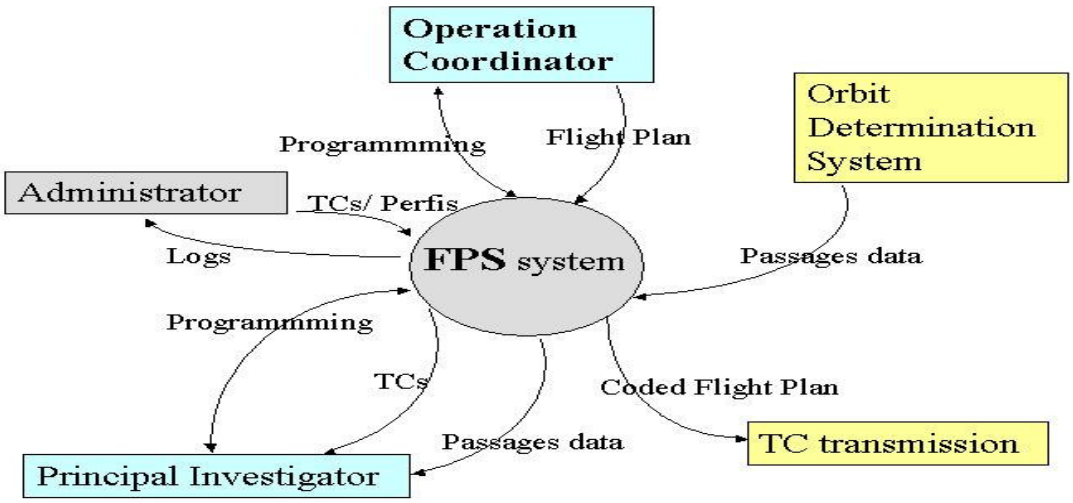

Figure 2: Flight Plan Supporting System Interfaces

III. Functional Requirements

After the scope definition of the FPS system presented in section 2, the system functionality specification got started, taking into account some assumptions in terms of operational scenario. Just as an example: from the particular TC list available for every instrument, the PI programs the TCs sequence to be sent on each satellite passage over the Ground Station (passage window). The OC integrates it with other instruments TCs sequences and delivers the flight plan to the PIs in order to be approved. Use case scenarios approach was used to specify all FPS system requirements as result of interaction analysis between the actors (PI, OC and AD) and the system activities. Summarizing, the WEB Flight Plan Supporting system provides functionalities such as: PI authentication, passage updating, passage choosing, TCs sequence programming and visualization, flight plan generation and visualization, flight plan codification. As examples, eight functional requirements are described: **REQ-1**: Display the FPS system main WEB page requiring Login and Password to operate remotely the chosen satellite mission, **REQ-2**: Validate the user access associating permission for operation (User Profile) and displaying the particular next page contents: list of the next passages (provided by the Orbit Determination Subsystem), list of the TCs associated to the User Profile, and facilities for TCs sequence programming, **REQ-3**: Provide user facilities to select from the passages list only one passage to which a TCs sequence is programmed. **REQ-4**: Provide user facilities to program TCs sequence selecting TCs from the instrument particular TCs list. TC execution on board can be temporized, therefore the programming shall allow the user to specify how many seconds from the reception, the TC execution must be waited. **REQ-5**: Provide user facilities to program more then one TCs sequence per passage, whether necessary, creating a Flight Plan Program (FPP), **REQ-6**: Provide facility to store a FPP into Data Base SERVER and modify it, whether the time is not expired. **REQ-7**: Option to visualize ready FPP shall be provided from a selected passage, **REQ-8**: In case of OC Profile is recognized, the system displays all programmed FPPs for a particular passage and provide facilities to reprogram them as well as to generate final Flight Plan (FP).

IV. Hazard and Risk Analysis

Following IEC 61508 safety lifecycle, the article concentrates in applying the activities corresponding to the 4 first phases of the standard, more precisely, oriented to the safety requirement allocation in the FPS System. The hazard and risk analysis process (phase 3) were carried out within phase 4 (Overall system requirements) to determine the appropriated integrity level for the system. For this project the concept of safety was a little different, since the satellite did not have any physical danger in terms of human life. Safety Integrity Level (SIL) was associated to the function if its failure could directly lead to the following consequences: Total loss of mission- SIL 4; Partial loss of mission- SIL 3; Unrecoverable loss of scientific or satellite data- SIL 2; One or more satellite passage windows over Ground Station missed- SIL 1.

For example, one hazard identified was: "The Ground transmitted misused TC to satellite". For this hazard the consequences identified were: **Total loss of mission**: satellite non-operating (no power supply, no communication); **Partial loss of mission**: satellite operating in degraded mode, total loss of one or more scientific experiments; **Loss of satellite data** collected since the last passage window due to a satellite reset; **Loss of scientific data**: a natural space event of scientific interest is missed; **One or more satellite passage missed**: windows for transmitting TC were missed leading to a partial loss of information due to satellite storage limitation. The worst consequence is "Total loss of mission", whose "probability" of occurrence could be qualified (according to IEC 61508) as "occasional", once the satellite operator can eventually send misused TCs that lead to a satellite loss. Therefore, the related risk is intolerable, demanding a safety-related system with SIL 4. However, due to software architecture choice, the functions performed by the safety-related system were combined in a way that none of them could solely lead to the worst consequence identified. The Fault-Tree Analysis (FTA), in figure 3, applied to the hazard illustrates the case.

The leaves of the FTA represent the potential causes (**CA**) for the hazard. Each cause can be seen as a safety function failure. There was not any safety function whose failure could solely lead to a "total loss of mission". Therefore, no safety function had SIL 4 assigned to it. Safety functions classified as SIL 3 do not mean that single failure would lead to a "partial loss of mission", but a combining (AND gate) would lead to a "total loss of mission". The same mechanism was applied to SIL 2 safety functions, which can be seen as sub-functions of a SIL 3 function.

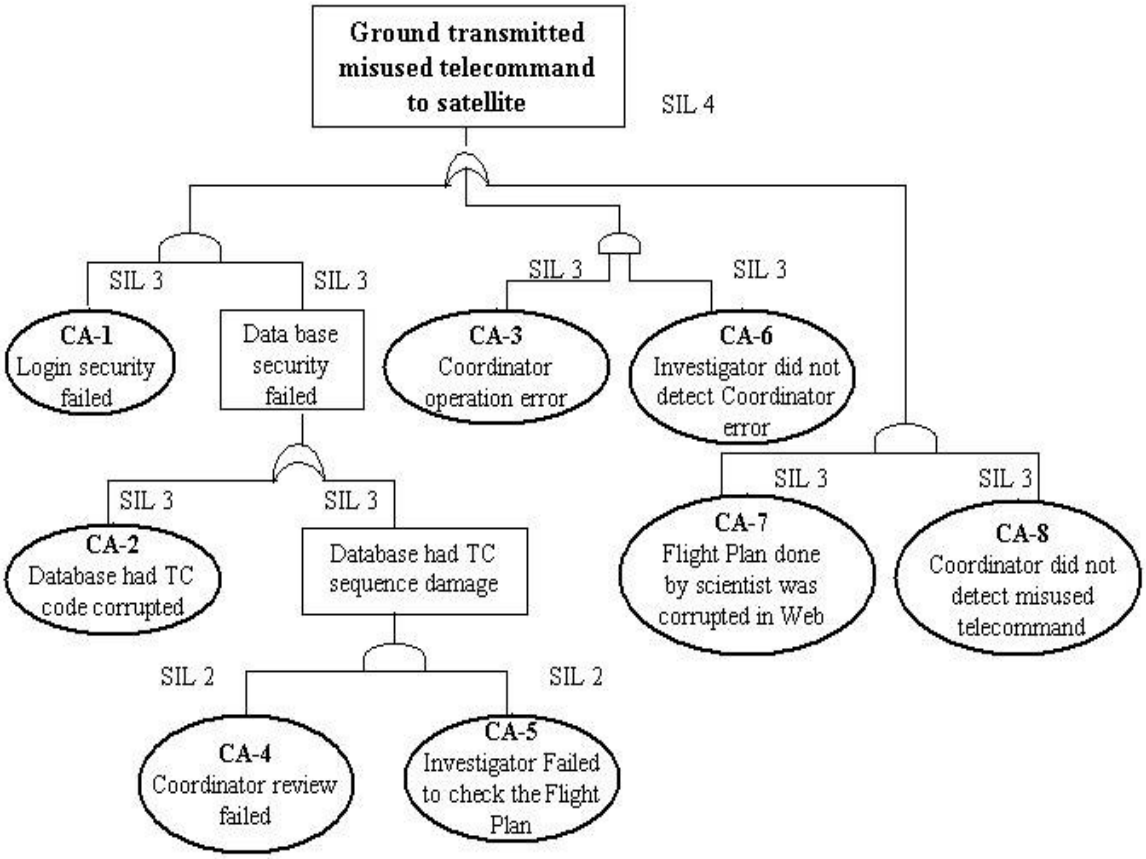

Figure 3: Fault Tree Analysis (FTA) for Flight Plan Supporting System

The next step was to identify and allocate safety requirements to those causes, which means specifying the safety requirements for the safety functions. A total of 15 safety requirements were identified, and some are listed below:

SR-5*: The system shall keep three copies of the database to store TCs codes, and the database reading shall be done through voting.*

SR-10*: The system shall classify the TCs according to their criticality level, and shall notify the operator (coordinator or investigator) whenever he or she tries to use TCs with potential damage to the satellite.*

SR-11*: The minimum unit handled by the coordinator shall be the* sequence of TCs*, in order to guarantee a TC atomic execution. Only the investigator shall create it.*

SR-12: *Every flight plan, for web transmitting, shall be encrypted.*

SR-14*: The flight plans shall comprise only labels that identify TC codes. The link between the labels and TC codes shall be done in the last step when no more web transaction is required.*

Additionally, nine operational requirements were specified. Some are listed below:

OR-7: In case the investigator (or satellite operator) rejects the flight plan, the coordinator shall contact him or her through means others than the system (e.g. telephone, email) in order to take the right action.

OR-8: If the coordinator intends to change some TCs he or she shall request the related investigator or satellite operator for authorization by email.

The relationship among causes, safety requirements, and operational requirements is provided in the traceability matrix described in the next section.

V. Prototyping and Designing for Safety

The user interface was prototyping as showed in figure 4. The main window requests the username, password and satellite mission.

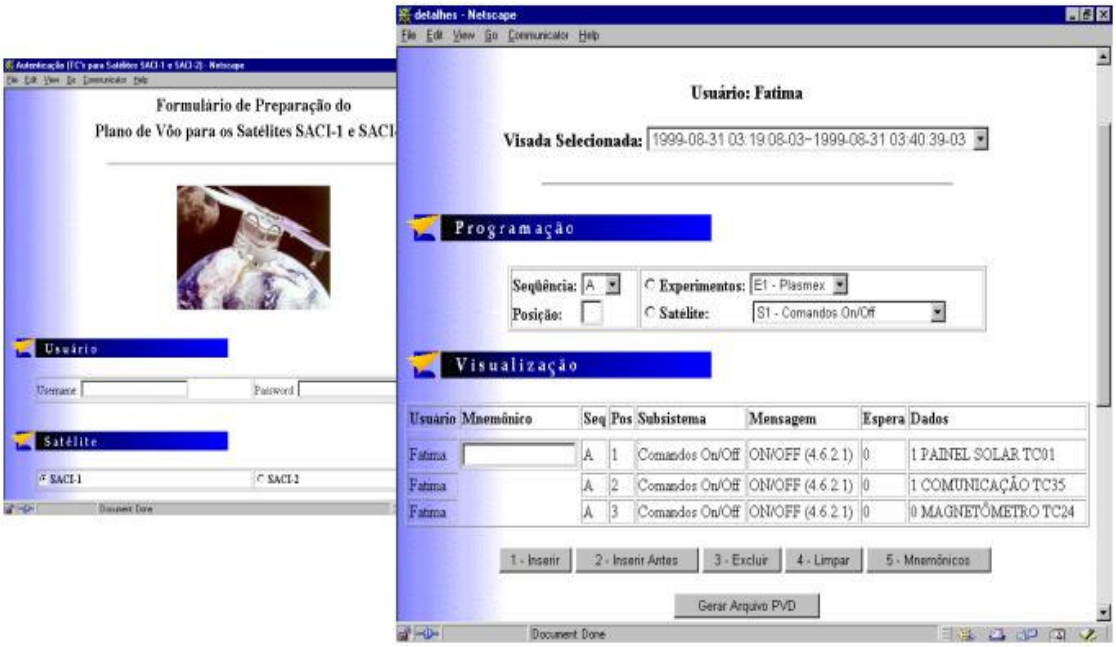

Figure 4: User interface prototyping

Whether the user is recognized by FPS, a second window is displayed with facilities for the user to select an available passage and work on the flight plan programming.

As recommended by IEC 61508 in the software safety requirements specification table, appropriate techniques/measures shall be selected according to the safety integrity level. Particularly for functionality related to SIL3 and SIL4 semi-formal methods of designing are highly required. Also logic/ function block diagrams and sequence diagrams are highly required. Therefore, UML* artifacts: activities diagram, class diagram and sequence diagram were produced as evolutions of the use case analysis presented in section 3 and to complete the object-oriented FPS system design. The Activities Diagram presents in Figure 5 gives an overview of the main actor's tasks (PI, OC and DataBase Admnistrator).

* UML – Unified Model Language

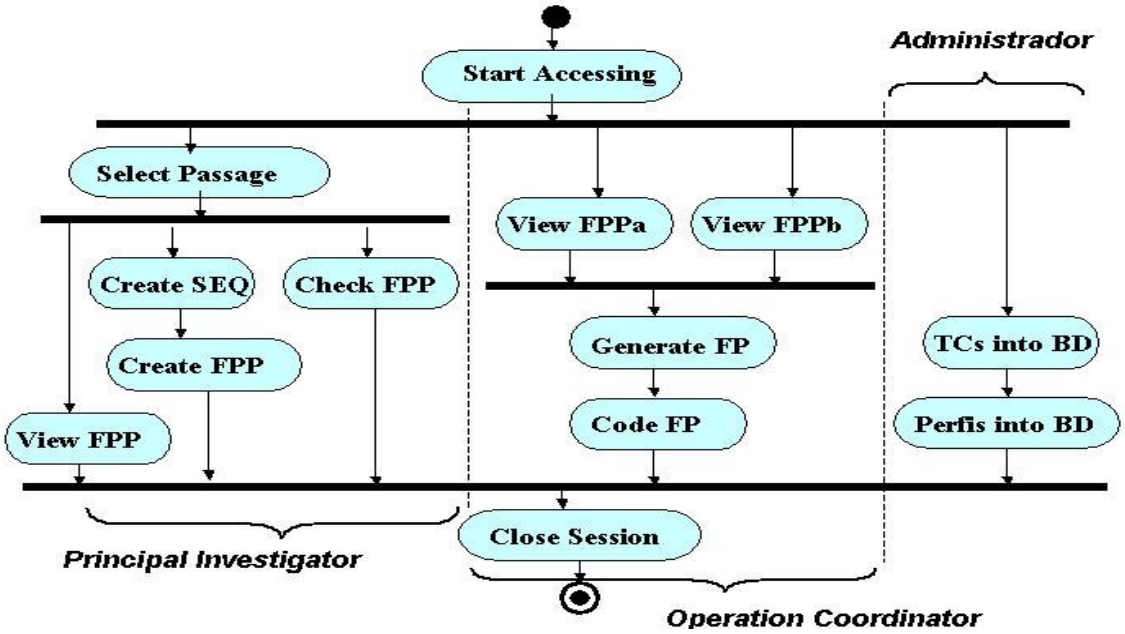

Figure 5: Activities Diagram

The system classes were coded and tested. The integration testing was divided in four phases; the first one focused on user profiles validation. The second phase validated the FPS interfaces with the real external systems such as Orbit Determination System in a local network environment. In the third phase of testing intrusions and anomalies simulated WEB vulnerability in order to check the safety techniques. The sequence diagram, in figure 6, represents the test case TC-43, where some kind of WEB corruption in a FP is simulated. FP was accepted by the PI but not rightly received back by OC, representing the causes CA-7 and CA-8 analyzed in FTA. So the safety requirement SR12 was tested. The last phase test cases were executed in real WEB environment. In total, 127 test cases were applied.

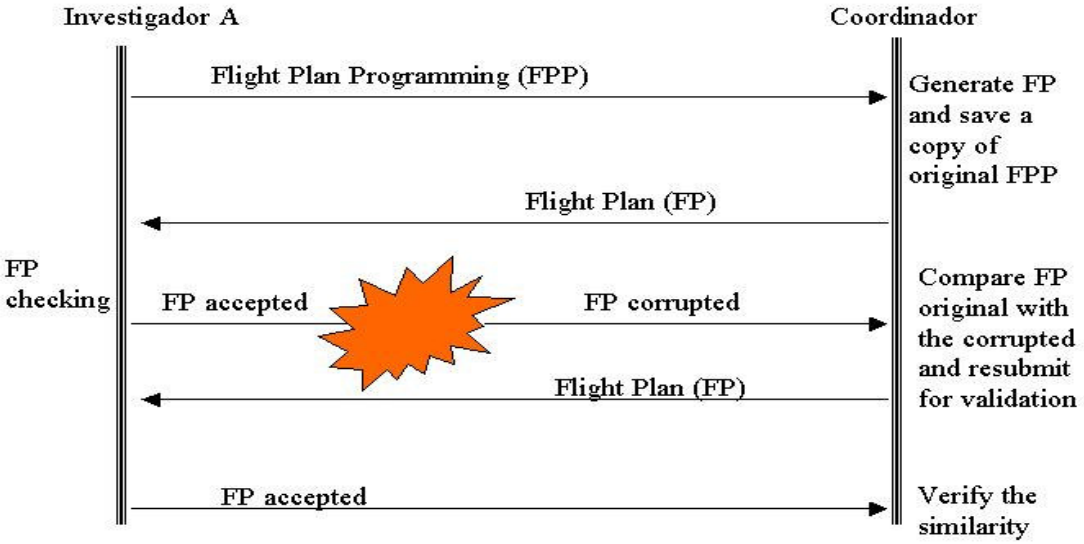

Figure 6: Sequence Diagram for a Test Case

Figure 7 shows the relationship among the safety requirements, potential cause for the hazards/ SIL, the component class that implements the functionality, the associated operational requirement, the architectural mechanisms whether adopted, and the test cases.

Safety Requirem.	Hazard Causes / Required SIL	Object -Oriented implementation	Operational Requirement	Architectural Mechanisms	Test Cases
SR-1	CA-1/ SIL 3	TCs Class	OR-2, OR-3		TC-28.3,
SR-2	CA-1/ SIL 3	TCs Class	OR-4, OR-3		TC-28.9, TC-39
SR-3	CA-1/ SIL 3	TCs Class	OR-5, OR-3		TC-1.5, TC-1.6, TC-1.7
SR-4	CA-1/ SIL 3	TCs Class	OR-6		TC-28.4 a TC-28.8, TC-34 a TC-37
SR-5	CA-2/ SIL 3	TCs Class; Progr Class		* Redundância	TC-40
SR-6	CA-2/ SIL 3	TCs Class; Progr Class		* Redundância	TC-40
SR-7	CA-2/ SIL 3	TCs Class; Progr Class		* Redundância	TC-41
SR-8	CA-3/ SIL 3, CA-4, CA-5 / SIL 2	TCs Class ; Progr Class FP Class	OR-9		TC-32
SR-9	CA-3/ SIL 3, CA-4, CA-5 / SIL 2	FP class; Progr Class FpCodification class	OR-7		TC-42
SR-10	CA-6/ SIL 3	TCs Class; Progr Class	OR-8		TC-25.1 a TC-25.3
SR-11	CA-6/ SIL 3	SeqTCs Class	OR-8		TC-26.5 a TC-26.10
SR-12	CA-7, CA-8/ SIL 3	FP Class	OR-9		TC-43
SR-13	CA-7, CA-8/ SIL 3	TCs Class		**	TC-47
SR-14	CA-7, CA-8/ SIL 3	TCs Class; FP class; FpCodification class			TC-27.1, TC-27.2
SR-15	CA-7, CA-8/ SIL 3	TCs Class; FP Class	OR-9		TC-44

Figure 7: Traceability Matrix

VI. Conclusion

This paper has presented a critical software system designed to support satellite flight plan programming via WEB, aiming to reduce operation costs by means of principal investigator collaboration on his/her instrument controlling. The vulnerability of the WEB required a system safety development approach in the project. The goal of the article was to highlight both the safety requirements identification obtained from determining the overall characteristics of the system and looking at its hazards, and the use of IEC 61508 to manage hazards through risk analysis, safety-oriented design and testing. Although emphasis on the first four phases of safety lifecycle has been given in order to demonstrate the IEC 61508 standard contribution on structuring FPS software for safety, other phases of the lifecycle have also been followed, such as Safety Validation Planning and Execution phases, briefly mentioned in session 5.

Acknowledgments

M.F. Mattiello-Francisco author thanks Finaciadora de Estudos e Projetos (FINEP) for financial support to the QSEE project, Qualidade do Software Embarcado e aplicações espaciais, 2006 http://www.cea.inpe.br/~qsee

References

[1] Mattiello-Francisco, M.F, Neri, J.A.C. "A compact and autonomous Ground System for SACI-1 Mission Controlling" 2th International Symposium on Spacecraft Ground Control and Data Systems, 08 – 12 Fevereiro 1999, Foz do Iguaçú, Brasil .

[2] Nancy Leveson, White Paper on Approaches to Safety Engineering –- Abril 23, 2003.

[3] Neil Storey, Safety-critical Computer Systems – First Edition, 1996.