A Software Brazilian Industry Experience in Using ECSS for Space Application Software Development

Fatima Mattiello-Francisco[a,1], Valdivino Santiago[b], Ana Maria Ambrósio[b], Leise Jogaib[c] and Ricardo Costa[c]

[a]Senior Software Engineer for Space Tecnologies Area at INPE
[b]National Institute for Space Research – INPE, São José dos Campos, SP, BR.
[c]DBA Engenharia de Sistemas LTDA, Rio de Janeiro, RJ, BR.

Abstract. This paper presents the tailoring of ECSS software product assurance requirements aiming at the development of scientific satellite payload embedded software by a Brazilian industry software supplier. The software item, named SWPDC, developed on DBA´s Software Factory context, by DBA Engenharia de Sistemas LTDA, is part of an ongoing research project, named Quality of Space Application Embedded Software - QSEE, developed by National Institute for Space Research – INPE, with FINEP financial support. Among other aspects, QSEE project allowed to evaluate the adherence of a Software Factory processes with INPE requirements for embedded software development process. Although no familiar with space domain, the high maturity level of such supplier, CMMI-3 formally evaluated, facilitates the Software Factory compliance to the requirements imposed by the custumer. Following the software verification and validation processes recommended by ECSS standards, an Independent Verification and Validation - IVV approach was used by INPE in order to delegate the software acceptance activities to a third part team. Contributions of the ECSS standard tailored form along the project execution and benefits for the supplier in terms of process improvements also are presented.

Keywords. Software quality, software development processes, space mission lifecycle,

1 Software for Space Systems

In space systems, a software product is part of a network of systems. Space systems include manned and unmanned spacecraft, launchers, payloads, experiments and their associated ground equipment and facilities. Software includes the software component of firmware. Space projects are generally expensive and take long time to be completed.

[1] Senior Software Engineer, Space Software Applications, Space Tecnologies Enginerring, National Institute for Space Research - INPE, Av. dos Astronautas, 1758, Sao Jose dos Campos, SP, Brazil; Tel: +55 (12) 3945 7124; Fax: +55 (12) 3945 7100; Email: fatima@dss.inpe.br; http://www.inpe.br/atifs/fatima/

The insertion of the industry into the space programs environment, as subsystem suppliers, has demanded improvements into the space agency's project management processes in order to successfully accomplish the projects. In different areas of application, one can see initiatives of industry and government toward the standardization and best practices for project management. European Cooperation for Space Standardization – ECSS is a great result of cooperative efforts of the European Space Agency - ESA, National Space Agencies and European space industry association.

Typical space mission lifecycle is the basis of the model used by ECSS to manager the development of the different space mission subsystems, which includes space application software. Nowadays, space agencies have dedicated special attention to the software project management. Such concerning is reflected in the management, quality assurance and software engineering volumes of ECSS.

This article addresses the Software Product Assurance volumes [ECSS-Q-80A and B] only. The fundamental principle of this standard is to facilitate the customer-supplier relationship, assumed for all software developments, at all level. They contribute to these objectives by defining a set of requirements to be met throughout the system lifetime which involves the development and maintenance of space application software. The requirements deal with quality management and framework, lifecycle activities and process definition, and quality characteristics of the software product [3].

Since the objective of software product assurance is to provide adequate confidence to the customer, the standard is usually tailored for a particular contract by defining specific subset requirements.

In order to evaluate Software Factory model as a satellite payload embedded software item supplier, the standard was tailored for the project *Quality of Space Application Embedded Software - QSEE*, under developed by National Institute for Space Research – INPE. In this context INPE´s team played the customer role [1].

This paper is organized as follows: section 2 introduces ECSS-Q-80 structure and on tailoring guidelines; section 3 presents DBA's Software Factory model and the software development processes followed by the supplier; section 4 discusses the standard tailored form for the particular software development item, the satellite payload embedded software – SWPDC, a case study of QSEE project. Finally, section 5 concludes with contributions of the standard tailored form for project execution and benefits for the supplier in terms of processes improvements.

2 ECSS-Q-80 Structure andTailoring

According to the structure of this ECSS Software Product Assurance standard the requirements are grouped in the following three categories: (i) requirements on management and framework of software product assurance; (ii) requirements on software lifecycle activities and processes; (iii) requirements on the quality of software products, including both executable code and related products such as documentation and test data. Each requirement has a corresponding *Required Output* identified that, among others, intents to assist the customer in the selection of the requirements during the tailoring process.

Tailoring for software development constraints takes into account the special characteristics of the software being developed, like the software type (database, real-time) and the system target (embedded processor, web, host system), and the development environment as well. Those issues are subject of Space System Software Engineering Process as defined in ECSS-E-40. Together the two standards specify all processes for space software development [2].

In order to carry out the tailoring of the software product assurance process on the scope of QSEE project without addressing ECSS-E-40, two relevant aspects must be pointed out. First, the software product is satellite payload embedded software, therefore a critical item. Second, although the supplier is not familiar with the technology and software development environment imposed by the customer, the Software Factory maturity CMMI-3 provides confidence to the customer in terms of its solid software development structure based on well established processes. Thus, the tailoring took into account the software development processes and the software lifecycle adopted by the supplier.

3 DBA´s Software Factory Model

The Software Factory concept uses the fundamentals of industrial manufacturing, such as standardized components, specializes skill sets, parallel processes and a predictable and scalable consistency of quality. It can achieve a superior level of application assembly even when assembling new or horizontal solutions. Software Factories have gained recent popularity as a cost-efficient way to reduce the time it takes to develop software. Conceptually, Software Factories represent a methodology that seeks to incorporate pre-built, standard functionalities into software which is typically disaggregated by domain.

The macro-flow diagram on the left of Figure 1 reflects the software development lifecycle typically performed by DBA. The related sub-processes represented by the each of the four columns on the right side of Figure 1 show the adherence to the SW-CMMI 3 key process areas: Process Control, Change Management, Configuration Management and Quality Assurance.

In order to be produced by DBA´s Software Factory (FSW), a Software PROJECT shall be characterized and a particular project team is allocated to carry out the requirements gathering and software development project management activities. Figure 2 presents the relationship among the PROJECT and FSW teams.

Prior to implementing such project management structure, the following steps and documentation should be forthcoming:

1. Customer provides an initial view of schedule, and scope of the proposed job.
2. DBA gives an initial assessment of the effort required to meet those requirements (including an estimation of the number of Function Points required), and whether it can provide such services.
3. Customer will then further specify the elements of an application development service order, along with the following items: (a) All available documentation of the project, architecture, patterns, interfaces, etc.; (b) Hardware and software configurations for the development and production environment; (c) Restrictions that should be observed during the software development.

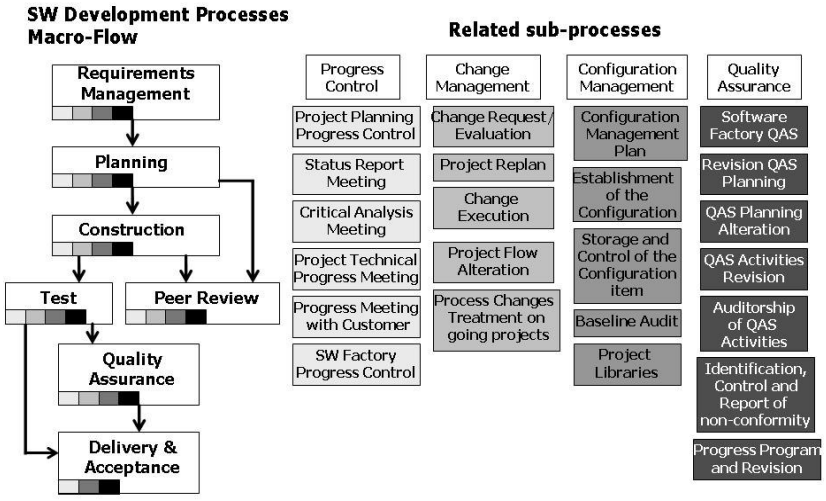

Figure 1. DBA Software Development Processes and related Sub-processes

4. Service Level parameters: DBA and Customer jointly establish the artefacts that are deployed at Analysis and Design and that describe the technical specifications necessary for FSW programmers to implement and test the code. Possible artefacts are: Use Case Specification; Information flow for System X - Template to describe the whole system information flow (to detail the flow of information for each Use Case).

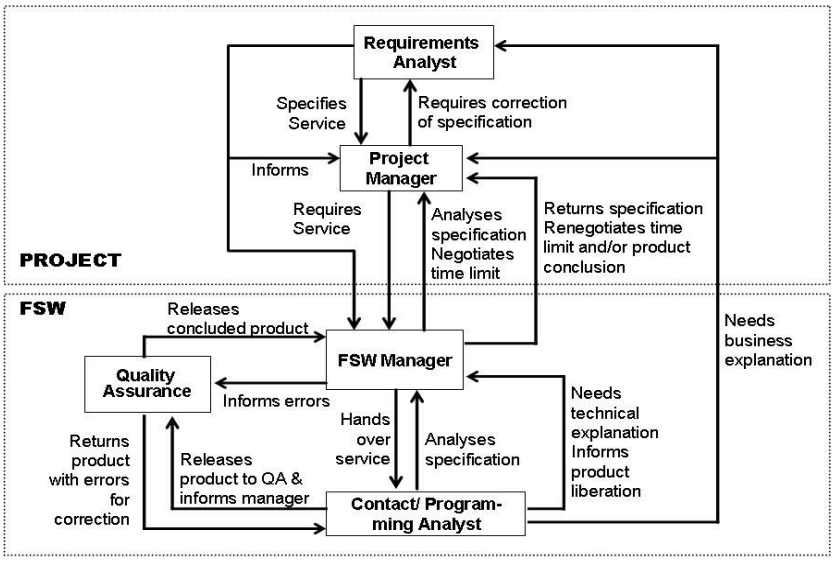

Figure 2. PROJECT and FSW relationship

5. The Project Designer will then issue a production order (OP) along with a set of artefacts shall be provided (Use Case, Classes and Sequence diagrams).
6. The Project Test Plan, with testing guidelines that should be followed for acceptance of the product developed by the FSW.
7. Testing Design - describes test cases for each technical specification.

Since the SWPDC software supplying by the FSW is subject of space domain application technology transfer to the Brazilian Software industry, the PROJECT team was composed by one senior DBA Project Manager and two Software Analysts. The last have been on job trained in similar embedded at INPE laboratory during six months before the SWPDC effectively got started.

4 Tailored Requirements

Software product assurance plays a mandatory role within the overall software engineering process. The complexity of software development and maintenance requires discipline to build quality into the product from the very beginning.

According to ECSS-Q-80B, the software product assurance requirements are grouped in three set of activities: (i) the assurance programme implementation, (ii) the assurance of the development and maintenance process and (iii) the assurance of the quality of the software product.

Table 1. Requirements related to software product assurence programme implementation

Requiremen	Description	Tailored Form	Tool	Document
Contractual Aspects	Supplier and Customer define a contract	Established when project QSEE was approved by governmental financial support (FINEP)	-	Agreements on Project Proposal
Software Product Assurance Planning and Control	Supplier provides a plan complying requirements and being approved by customer	SPA items included in DBA Software Development Plan document, reviewed and approved in SSR	Compliance matrix	SDPlan
Software Product Assurance Reporting	Supplier provides mechanisms for assessment of the current quality of the product	Reviews data package and tool allowing the customer to follow each Production Order (OP) into the FSW	Reports from a proprietary tool (SAF)	SDPlan
Non-conformances	Software Reviewer Board and baseline established by supplier/ customer	Formal Reviews point out the discrepancies (RIDs) and project control meetings	-	RB
Software Problem	Supplier defines and implements procedures for logging, analysis and corrections of software problems	Software Problems identified in the FSW have well established internal procedure. RNCs are problems identified on acceptance testing.	DBA FSW work-flow involves QA team	SDPlan

The tailoring process was carried out following these three groups in a complementary way by means of careful analysis of their requirements. Table 1, Table 2 and Table 3 summarize, as examples, some of the applicable requirements analysed and their tailored form for SWPDC product assurance. The first two columns of each table contain the ECSS-Q-80 requirement and its description, respectively. The column entitled *Tailored Form* describes the way the recommend requirement has been tailored in this project. Whenever a facility is provided to support the requirement, the column *Tool* introduces it. The *Document* column lists the customized documents in which such requirement is complied. Table 1 lists some requirements corresponding to the group (i).

Requirements Baseline (RB) is the main document provided by customer. It imposes six formal reviews: Software Specification Review (SSR), Preliminary Design Review (PDR), Detailed Design Review (DDR), Critical Design Review (CDR), Qualification Review (QR), and Acceptance Review (AR). Also it defines the documents to be provided by the supplier: Software Development Plan (SDPlan), Software Test Plan (STPlan), Software Technical Specification (STSpec), Software Design Document (SDD), Software Test Specification (TestSpec) and Test Report (TRep). From the independent team, the following documents are required: Independent Verification and Validation Plan (IVVPlan), Independent Verification and Validation Test Specification (IVVTSpec), Independent Verification and Validation Report (IVVRep). The Formal Reviews are documented in Technical Review Report (TRRep) which includes identified discrepancies (RIDs). During the acceptance phase, Non-conformances report (RNC) is delivered by IVV team to the supplier copied to the customer.

Concerning the ECSS requirements presented in Table 1, a brief analysis about their correspondence with DBA Software Development processes and related sub-processes (Figure 1) show those requirements met the Progress Control and Quality Assurance Sub-processes.

Table 2 lists some requirements corresponding to the group (ii). Since ECSS-Q-80B subdivides the software assurance process requirements in three categories, that organization was also adopted in that table.

The ECSS requirements related to software lifecycle are met by two DBA Software Development processes: Requirement Manager and Planning. And by related sub-processes: Progress Control and Change Management. The process assurance requirements applicable to all software engineering processes are met by Peer Review, Quality Assurance and Delivery & Acceptance processes. And by related sub-processes: Configuration Management and Quality Assurance. Whereas the process assurance requirements related to individual software engineering activities are met by Construction and Test processes. And by related sub-processes: Change Management.

Table 3 lists some requirements corresponding to the group (iii). The correspondence between the requirements on Table 3 and DBA processes presented in the Figure 1 macro-workflow is consequence of the software development lifecycle phases. Thus, the first requirement row meets the Requirements Management and Planning processes. Second requirement meets the Construction process. And the last two rows meet the Test, Peer Review and Delivery & Acceptance processes.

Table 2. Requirements related to the software process assurence

Requirement	Description	Tailored Form	Tool	Document
Software Development Lifecycle				
Life cycle definition and review	Software devel. life cycle shall be defined by supplier and reviewed by customer	Software development lifecycle followed by DBA Software Factory has been approved by the customer on SSR	DBA Work-flow	SDPlan
Milestones	A series of technical meetings or reviews shall be defined	Reviews have been established on the RB by customer according to space mission life cycle.	-	RB and SDPlan
Applicable to all Software Engineering processes				
Documentation of Processes	Software project plans shall cover all activities of software development	Development Plan and Test Plan provided by supplier and by Independent Verification and Validation team	-	SDPlan, STPlan, IVVPlan
Handling of Critical Software	Apply measures to assure software confidence	Independent team designs FSM model-based testing using automatic test case generation tool.	CoFI and Conda do	IVV Plan IVVTSpec IVVRep
Software Configuration Management	Supplier shall use a configuration management system	The system used by the Software Factory process has been approved by customer	VSS	SDPlan
Verification	The verification plan shall identify facilities, training ad skills to carry out the verification activities	FSW comply the reviews imposed in RB adding internal verification techniques such as pair review. IVV Plan provided by the independent team.	-	RB, SDPlan, IVVPlan
Related to Individual Software Engineering activities				
Software Requirement Analysis	Requirements specification shall be provided by customer as input.	Technical Specification document was elaborated by supplier taking RB as input customer provided	-	RB and Protocol Spec TSpec
Architectural Design	Use of a design methodology and design standards appropriated to the type of the software.	Software Design using UML artefacts, usually adopted in the FSW, was required by the customer, which provided the document template.	Interprise Architecture	SDD
Software Delivery and Acceptance	Customer judges whether or not the product is acceptable according to previously agreed criteria.	The acceptance process defined in RB focus on testing at instrument level, subsystem and system by customer. Model-based testing is used in the acceptance process.	CoFI methodology MME Conda do	IVV Plan IVVTSpec IVVRep

Table 3. Requiments related to the software product quality assurence

Requirement	Description	Tailored Form	Tool	Doc.
Technical Specification	Software requirements shall be documented in a Software Technical Specification.	A complete, detailed and unambiguous set of requirements shall be provided by supplier taking RB as input.	Traceability matrix	RB and STSpec
Design and Related Documentation	Software design shall meet the software quality requirements (minimum hierarchy dependency and interfaces for the software component	Software Design Document shall be produced by FSW as a proposed solution to the requirements detailed in the Technical Specification. Use Case approach from UML was recommended.	-	SDD
Test and Validation Documentation	Detailed test planning (test cases, procedures, results) shall be consistent with test strategy.	A set of document was defined by customer in order to cover the two testing level strategy (internal to FSW and IVV)	-	STPlan, TestSpec IVVPlan, IVVTSpec
Reports and Analysis	Reports of all assurance, verification and validation activities	Two report documents were required by customer in order to cover the two testing level strategy (internal to FSW and IVV) Also a RIDs and RNCs..	-	TRep IVVRep. TRRep

5 Tailored Form Contributions

The tailored form contributed to simplify the technology transfer process of the embedded software from INPE to DBA. Specific requirements concerning with independent verification and validation carried out by a third team were defined because the full validation of the software product on the target computer was not feasible on the FSW context. This team participation on the reviews allowed early understanding of the software operational behavior which contributed in using model-based testing techniques as part of the acceptance process.

Although no familiar with space domain, the supplier maturity level, CMMI-3 formally evaluated, facilitates the FSW compliance to the requirements imposed by customer. The project oriented approach adopted by DBA to deal with the well stabilized processes of its FSW minimized the difficulties inherent to aggregating new project knowledge domain to the FSW environment.

6 References

[1] Quality of Space Application Embedded Software (QSEE). Available at: <http://www.cea.inpe.br/~qsee>. Accessed on: Feb. 23th 2007.
[2] Space Engineering - Software, ECSS-E-40 standard, May 2005.
[3] Space Product Assurance – Software, ECSS-Q-80A and B standard, October 2003.