International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Framework for Safety Critical System Software

Savitha. A, Sudeesh B

Reliability and Quality Assurance Software Group, ISRO Satellite Center, Bangalore, Karnataka, India

ABSTRACT

U R Rao Satellite Centre (URSC) is the lead centre of the Indian Space Research Organisation in the development and operationalisation of satellites for communication, navigation and remote sensing applications. It also has launched many interplanetary missions. Now execution of "GAGANYAAN" is planned in phase manner. In the initial phase, test vehicles will be used to demonstrate the abort capability during different phases of mission i.e. development & qualification testing of Crew Escape System (CES) and recovery. Subsequently, two unmanned flights are planned prior to human spaceflight to demonstrate the manned mission capabilities. As humans are involved software safety plays a critical role. Presently ISRO is having ISRO Software Process Document (ISPD) based on IEEE 12207:2015 framework for software life cycle activities. For Gaganyaan project considering safety in to picture additional software safety standard is brought out based on DO178C. To develop and certify safety critical software ISRO software control board has brought out the ISRO software safety standard for a transition from mission critical software to safety critical software development. This paper discusses how to incorporate safety and security standard in addition to the existing ISPD standard.

KEYWORDS: *ISRO Software Safety Standard (ISSS), Preliminary Hazard Analysis (PHA), SubSystem Hazard Analysis (SSHA), ISRO Software Process Document (ISPD), Software Fault Tree Analyses (SFTA) , Software Failure Modes and Effects Analyses (SFMEA), Software Certification Process (SCP), Software Hazard List (SHL), Software Certification Process (SCP), Independent Verification and Validation (IV&V)*

How to cite this paper: Savitha. A | Sudeesh B "Framework for Safety Critical System Software" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.1541-1544, URL: www.ijtsrd.com/papers/ijtsrd43652.pdf

IJTSRD43652

I. INTRODUCTION

To have a uniform engineering standard across all centres of ISRO, ISRO brought out its Software Engineering Standard called ISES 92 (ISRO Software Engineering Standard) in 1992 [1]. All centres of ISRO followed this standard for software development and implementation. Later ISES-92 was revisited as the complexity of software was increased and many fault tolerant features were considered for the design and also many autonomy features were incorporated. Subsequently ISRO Software Control Board (ISCB) came into existence which brought out "ISRO Software Process Document" (ISPD). It acts as an implementation guide in line with IEEE-12207 for all centres of ISRO. ISPD provides an excellent framework for development, verification and validation of mission critical software.

There are different classes of software used in different centres of ISRO. The ISPD Issue-1 was released to use the common standard in all centres for implementing IEEE 12207:1996. The focus of ISPD was mainly on the software life cycle activities followed for different category of software. Some of the software categories like onboard software, Checkout & Simulation software, Launch Operations Support & Test Facilities software, Image /data processing software, Mission design software and many more. The main focus was on software requirements, design, implementation and software verification and validation, maintenance and configuration management.

ISPD Issue-2 is a revised version of ISPD-Issue-1. This version is introduced to achieve a fully integrated suite of system and software life cycle processes. It included new category of software like spacecraft operations software, FPGA design, system software. It addressed some more process like risk management, knowledge management, system analysis, decision management etc.,

As for as safety and security is concerned for Gaganyaan mission ISPD Issue-2 has been augmented with many more features addressing safety, security and certification process. ISRO Software Control Board has made a comprehensive study of all applicable international standards, it has generated the first issue of ISRO Software Safety Standard (ISSS). It will be used by all software teams across all centres of ISRO to realise safety critical software and to achieve zero defect in space systems.

The purpose of this standard is to enable the project team, software development and implementation team, independent verification and validation team, QA teams, review teams and certification team to carry out the software life cycle activities necessary to ensure that acquired or developed software has the required safety and security features, and to certify the software for its end use. This standard is applicable to all the software categories described in ISPD-Issue2 and any software used for safety critical mission, which are classified as Catastrophic, Major and Minor based on the Preliminary Hazard analysis at system level and software subsystem level. Figure 1 explains the software life cycle process for safety critical software.

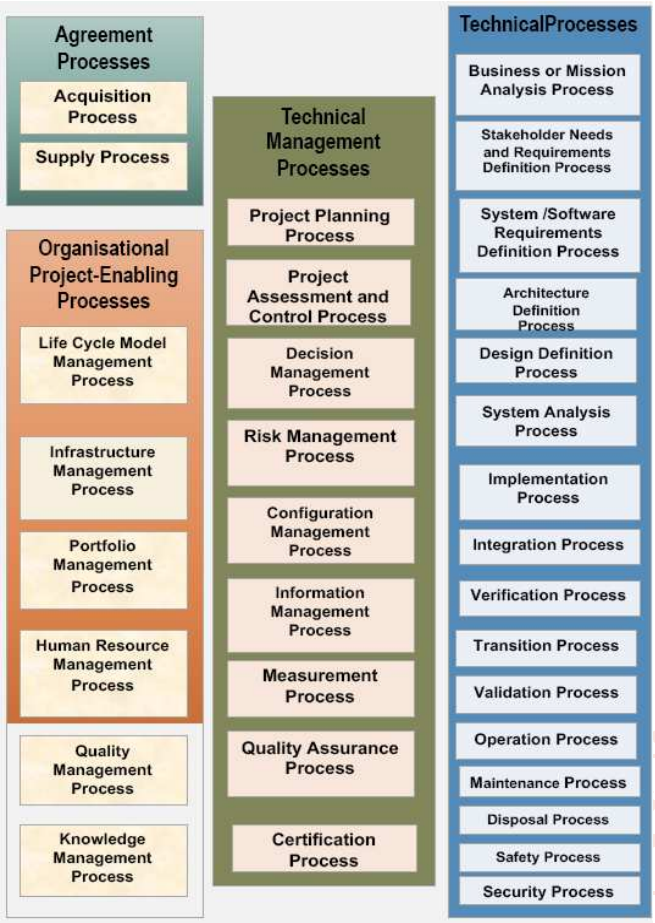

Figure1: Software life cycle process for safety critical Software

II. PROCESSES FOR SAFETY CRITICAL SOFTWARE

The Software life cycle process are categorized into Agreement process, Organisational Project-Enabling Processes, Technical Management Processes and Technical processes.

A. Agreement Processes
B. Organisational Project-Enabling Processes
C. Technical Management Processes
D. Techni*cal processes.*

A. Agreement Processes

The Agreement processes specify the requirements for the establishment of agreements between suppliers and acquirers. These processes are executed through the purchase procedure between acquisition and supply processes for the establishment of expectations and responsibilities related software assurance, including legal requirements and licensing requirements and many more. In the acquisition process project requirements are met and in supply process these requirements are serviced.

B. Organisational Project-Enabling Processes

The Organizational Project-Enabling processes are concerned with meeting the project requirements by providing the resources required. It has processes like life cycle management process, Infrastructure management process, portfolio management process, human resource management process, quality management process and knowledge management process. Each has separate activities which all holds good for safety critical system.

C. Technical Management Processes

These processes are used to establish and perform technical plans for the project. The activities are carried as per the plan depending on the risk and complexity of the project. The technical management processes are project planning processes, Project Assessment and Control Process, Decision Management Process, risk management process, Configuration Management Process, Information Management Process, Measurement Process, Quality Assurance Process and Certification process. As per safety critical software the last process that is certification process got included. In this process certification has to be issued based on the project plans whether all activities are carried out or not in each phase of SDLC. There is a separate board for certification which will audit and issue the certificate at each stage of project development life cycle.

D. Technical processes.

The Technical processes outline the activities that change the services to possess the timeliness and convenience, the price effectiveness, and also the practicality, maintainability, usability and other quality metric needed. the process are business or mission analysis process, stakeholder needs and requirements definition process, system /software requirements definition process, architecture definition process, design definition process, system analysis process, and so on. as for safety critical software is concerned 2 new process safety process, security process got added.

III. SOFTWARE SAFETY ASSURANCE PROCESS

Software safety assurance process is to identify the safety functions in system requirements for hardware, software and firmware. Based on the identification the safety functions are mapped to the requirements, design, implementation and test cases. The safety assurance process ensures the requirements are classified as safety critical and non-safety critical and ensures the safety requirements are correctly implemented with all the failure conditions accommodated. This process also ensures the functionality is met at specified time or sequence with predefined conditions correctly with fault detection, isolation, tolerance, and recovery

The level of safety is defined through the preliminary hazard analysis and software sub system hazard analysis. PHA defines the overall hazards of the system. Later it is categorized as software critical and hardware critical. The software critical hazards are categorized early in the software development life cycle. Those hazard causes residing in the software component become the subject of the software subsystem hazard analysis. The hazards can be in the design or in the operational concept. Those hazard causes residing in the software component become the subject of the software subsystem hazard analysis.

The PHA and the SSHA categorizes the safety critical software into 3 categories.

1. Catastrophic

System/Software whose failure will result in loss of life, loss of mission or serious injury to the crew

2. Major

System/Software whose failure will result in partial disabilities, injuries, large reduction in the mission functionalities

3. Minor

System/Software whose failure will result in mission degradation or discomfort leading to physical distress to crew possibly causing minor injury

Once the software is categorized as safety critical. The Software Fault Tree Analyses and Software Failure Modes

and Effects Analyses will help to determine the critical failure conditions.

IV. SOFTWARE SECURITY ASSURANCE PROCESS

Software Security Assurance is the process to ensure that the software is designed with security requirements, coding is done with secure guidelines. Security testing is carried out in a safe secure environment and vulnerability assessment is done. Periodic review of secure threats and secure release is more important for the secure software. The process should take care of misuse of data, resources, inaccuracy and any potential harm to the system. This process removes any vulnerabilities during implementation of the design, testing, deployment and during operation and maintenance processes. The most important is any new changes to the existing requirement will not create any vulnerabilities.

V. SAFETY CRITICAL SOFTWARE PROCESS FLOW

The safety critical software process flow activities are carried out in each phase of software development lifecycle. The software requirements definition process, design process, implementation process, integration, verification and validation process, operation process, maintenance process all are discussed in detail. Each of process is discussed with inputs, activities/tasks, safety specific activities with the output in each phase. The safety critical software specific activities process flow in software requirements is depicted in Figure 2, along with inputs, activities and outputs.

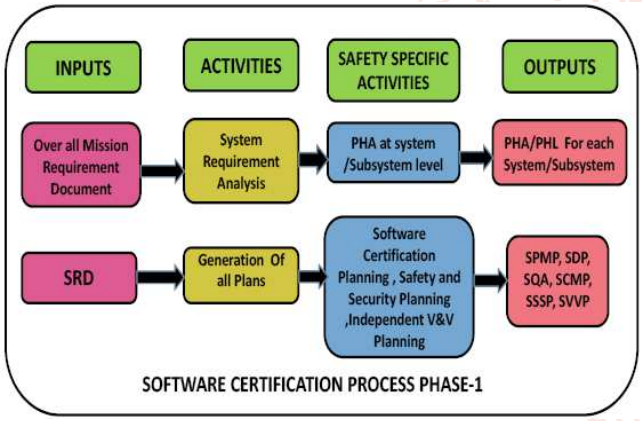

Figure 2: Software Certification Process Phase-1

Bi-Directional Traceability ensures that at each phase of software development life cycle all functions are implemented as expected and right products are produced at the output of each phase along with results and reports. It ensures the link from one phase of SDLC to another phase, it traces both in forward and backward direction.

The Figure 3 shows the Forward and Backward Traceability during life cycle process.

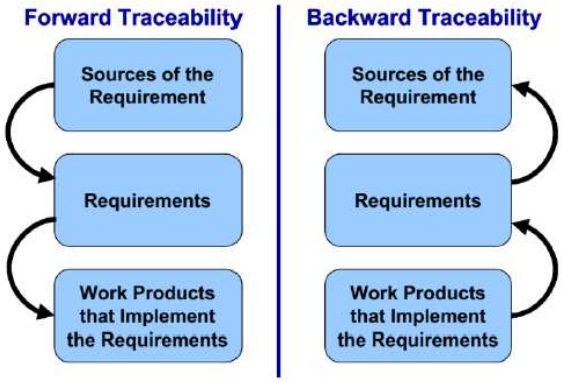

Figure 3: Forward and Reverse traceability

The forward traceability will trace each unique requirement to the design, design to code and the code to the test results and the verification and validation mechanism. The backward traceability ensures that work product is implemented as per requirements and requirements are traced back to the sources of the requirement.

VI. SOFTWARE CERTIFICATION PROCESS

Software certification has four audit phases. It will ensure that safety and security is taken care and implemented in all phases of software development life cycle. It will issue the certificate at the end of process. The certification team will ensure the following activities are carried out.

A. Pre-audit Meeting and prepare the checklist for certification process
B. Certification Audit team shall audit the activities carried out in each phase of SDLC
C. Certification Phase Audit Report will be generated for the audit findings
D. Non-Conformance Management
E. For new and modified requirements, the re-certification activities will be carried out

Figure 4 shows four certification process in each phase of the software development life cycle.

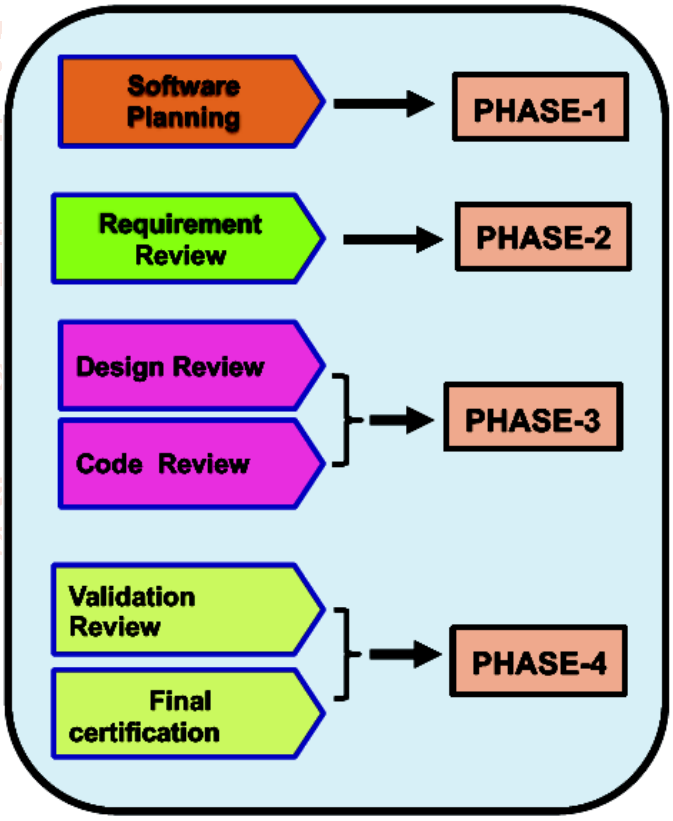

Figure 4: Four Phases of Certification process

A. Software Certification Process Phase 1

This phase is the first phase of certification process which comes at the project planning phase. The main goals are to ensure all plans, standards, guidelines, policies are established. Plans like software certification plan software development plan, software configuration management plan, verification and validation plan safety plan etc., are generated. Hazard analysis reports, certification phase readiness report is available. The audit team will audit the and ensure all reviews are carried out and minutes are available. If the certification team is satisfied it will issue the certificate else if any non-conformances are there it has to be resolved.

B. Software Certification Process Phase 2

This phase is during the requirements phase of the software development life cycle. The main goal is to ensure software requirements comply with requirement standards. Compliance of life cycle plans, reviews. Traceability is Established between system and software requirements. Audit team will verify all the review record, plans and traceability carried out.

C. Software Certification Process Phase 3

This phase is during the design review and code review phase. The main objective is software design will comply to design standard. Code is developed as per the coding guidelines. Traceability is established between requirements and design and to code. All the design reviews and code inspection shall be carried out. The audit team will verify design is as per design guidelines and code is as per coding guidelines else non-conformances will be raised. Audit team will ensure all design reviews are carried out and minutes of the meeting is available.

D. Software Certification Process Phase 4

Phase four of certification is in validation and final certification phase. The certification team will ensure all the verification and validation activities are completed. Completion of all the activities of SDLC. Bidirectional traceability is established. Independent verification and validation are carried out. Robust and functionality testing is carried out as per the plan. Results are available and test results review is carried out. The final product meets all its requirements taking care of safety and security. The certification team will ensure no open issues are available to issue the final certificate.

VII. CONCLUSION

This paper discusses the two well established industry software development standards: IEEE/EIA 12207 and RTCA D0178C for computer-based software systems. Our existing process will be much more rigorous by practicing this standard. This standard is applicable for all safety critical software used for space applications. It is not only applicable for onboard software but for all the software like mission operation software ground software used for testing the spacecraft, legacy software and commercially off the shelf software and the qualification of tools used in safety critical system.

ACKNOWLEDGMENT

We wish to convey our gratefulness to all our colleagues in Reliability and Quality Assurance Software Group and all the members of ISRO software control board and other colleagues from other centers of ISRO for their support.

REFERENCES

[1] Space product assurance - FMEA/FMECA analysis - ECSS-Q-ST-30-02C

[2] ISRO-DOS Committee for software Engineering standards, ISRO Software Engineering Standard (ISES-92), ISRO, May1992

[3] IEEE/EIA 12207.0-1996(ISO/IEC 12207) Standard for Information Technology – Software life cycle Processes

[4] MIL-STD 1629 "Procedures for performing a failure mode and effect analysis"

[5] NASA Software Safety Guidebook - NASA-GB-8719.13

[6] ISRO software control board, ISRO Software Process Document, ISRO-SES-PD-100 ISSUE-1.

[7] IEEE/EIA 12207.1-1996(ISO/IEC 12207) Standard for Information Technology – Software life cycle Processes Life cycle data

[8] RTCA DO-178C,Software Considerations in Airborne Systems and Equipment Certification