Software quality assurance of cryocooler drive electronics software used in spacecraft

Savitha A[1],*, Sudeesh B[1] and PrakashaRao P J V K S[1]

[1] Mission Software Quality Assurance Division ISRO Satellite Center, Bangalore, 560002, India.;
   savitha@isac.gov.in(S.A); sudeesh@isac.gov.in(S.B); pjvks@isac.gov.in(P.S)
* Correspondence: savitha@isac.gov.in

Abstract: Software plays an important role in the ISRO space mission. Reliability of this software is vital to achieve zero defects in space systems and services. There are varieties of software used in realization of spacecraft. Mainly it is categorized into onboard, mission and ground software. Evaluation of this software is the major activity for a software quality assurance person. Software quality engineer has to certify the software based on system level requirements, mission requirements and functional requirements. All the hardware and software interactions also have to be verified. Risk management is the key factor for effective software management. Software life cycle activities are carried out based on ISRO software process document. Following these standards and guidelines helps to find the defects in the earlier phase of software development life cycle. This paper mainly describes the software quality assurance activities carried out for control drive electronics unit used in GSAT spacecraft. SQA activities complied against the IEEE12207 standards (ISPD-2) at ISRO level. Pulse Tube Cryocoolers are active cryogenic devices used to generate cryogenic temperatures in the 50K-80K range in a single stage. Cryocooler drive electronics unit generates identical drive to both the compressors of pulse tube cryocooler.

Keywords: Attitude and orbit control system(AOCE), pulse tube cryo-coolers(PTC), cryo drive electronics unit(CDEU), teleCommand processor(TCP), bus controller(BC), remote terminal(RT), telemetry(TM), telecommand(TC), watch dog timer(WDT), software requirements specification(SRS), software requirements document(SRD), software design document(SDD), quality assurance(QA), software quality assurance(SQA), software requirements review(SRR), ISRO software control board(ISCB), ISRO software process document(ISPD), software development life cycle(SDLC), software quality assurance(SQA), software development life cycle(SDLC).

1. Introduction

T he responsibility of the SQA engineer is to

- Assess the software development process.
- Evaluate the conformance of software processes and software product
- Evaluate the effectiveness of the software processes.

This paper brings out all these above activities carried out for CDEU software.

ISPD describes the software life cycle processes and identifies the essential documents as the outcome of various life cycle processes like System requirement specification document, software design document, software project management plan, configuration management plan etc. An appropriate development life cycle model can be chosen based on software category using the guideline for selection of software development life cycle. The processes, activities and tasks applicable for the software category are mapped to the chosen life cycle model.

With the above explained framework we are able to establish complete traceability. The SDLC model adopted helped in finding missing functionality and to accommodate new requirements which came at last stage of the project. This framework helped to find the anomaly in the early stages of the project.

The PTC has two compressors C1 and C2. It is mounted back to back to reach a cooling effect of 80K by removing 0.7W heat load. The CDEU delivers sinusoidal drive to both the compressors. The drive can be programmed for various parameters based on the heater load. There is various logic for CDEU operation. Safety logics are also built-in like, over voltage and over current protection etc. The software requirements and interface specifications for the cryo cooler is organized into following sections:

- Mission Requirements
- System Requirements
- Functional Requirements
- Memory organization and Hardware interface registers
- Software Requirement Specifications

Since CDEU being the new system, all the requirements were discussed and complete testing was carried out. If it is a repeat project then only changes will be discussed in the SRR. Testing will be carried out for the changes and regression testing will be carried out to see the effect of change on other modules.

2. Cryocooler drive electronics unit system overview

CDEU delivers sinusoidal drive to both compressor C1 and C2. It can be programmed for parameters like voltage, phase, offset and frequency. CDEU monitors voltage, current and frequency, temperature of the cold tip and pressure of the gas for both the compressors. This CDEU package is stack of three cards Power card, Instrumentation card and Controller card hosted on the mother board. It is interfaced with TCP for data commands and pulse commands through 1553 interface. TCP is the bus controller and CDEU is one of the remote terminals for it. It also has 1553 interface with telemetry package to monitor the health of cryo cooler and other parameters like temperature etc. Figure 1 shows the various modes of operation of CDEU.
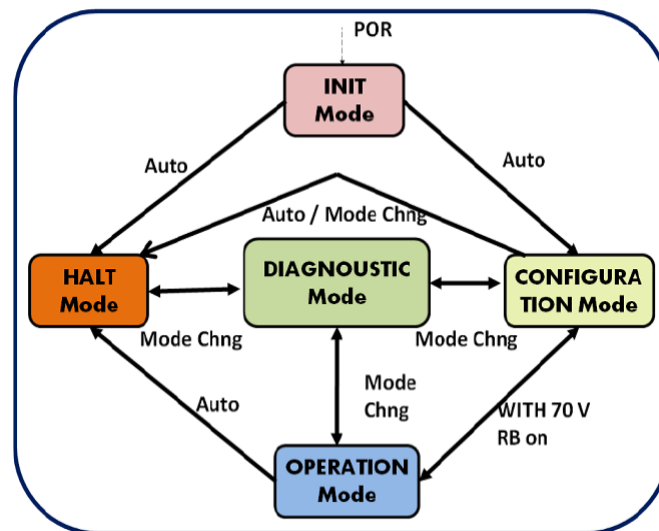

Figure 1. Different modes of CDEU

The functionalities are broadly classified as:

- Different modes of operation bases on requirement
- Command reception through 1553 interface , command decoding and execution
- Control of linear motor drive parameters, Configuration of system parameters
- Acquisition of parameters from hardware and transmit to TM subsystem
- Fault detection and recovery logic

3. ISRO software control board adaption of IEEE 12207

ISRO has created a framework for developing software and ensuring its quality through the implementation of a software standard IEEE-12207 as defined in the ISRO Software Process Document. ISCB is responsible for the effective implementation of ISPD encompassing all classes of software pertaining to various centres and units of ISRO.

4. Software quality assurance for CDEU

4.1. Software requirement specifications

All the requirements were discussed in the SRS committee. Since this being a new system there is no heritage for it, hence all the requirements were reviewed. If it is a repeat project then only changes will be reviewed. The SRS committee recommendations for any change in requirements or to include any new module for the correctness of the system are taken for implementation. Minutes for the SRS and closeout will be released soon after the review. It is most important for the completion of process and also to establish traceability. After the review approved SRS document will be released.

4.2. Design phase

Approved SRS document after the SRR is the input to software design. The software design review is carried out with members from different groups like mission, controls, subsystem and SQA. The design review was carried out in steps. Initially with the designer peer review was carried out. Any change in the design, correctness of requirement implementation is verified by the quality engineer. After all the modules peer review is completed the minutes will be presented to the SDR committee. The CDEU design was verified against the approved SRS. Any changes or action on QA engineer or on designer will be included in the minutes. The action should be closed before the code is released to SQA engineer. Figure 2 shows the SDLC followed for onboard software.
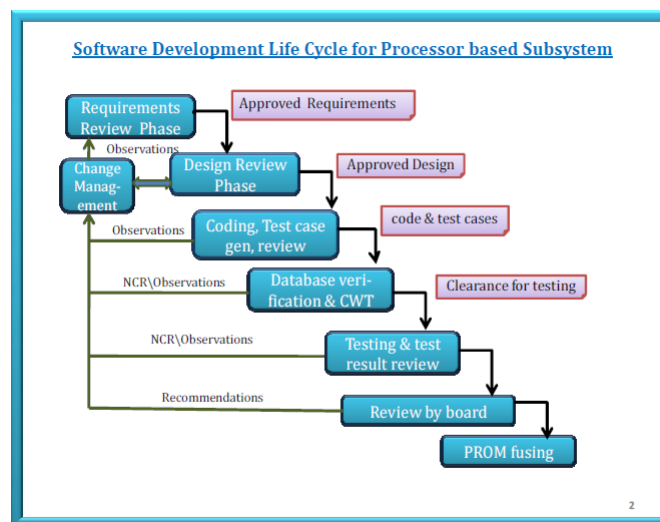

Figure 2. Development, Verification and validation within IEEE 12207 framework

Some of the recommendations like WDT flow chart has to be modified, Message ID can be displayed appropriately all these were taken care in the next version of SDD. This will be the approved design document.

4.3. Coding Phase

With the approved design document the coding will begin. The code is written in assembly language 8086. CPU86 IP core is qualified for on-board and to be used with the safe subset instructions. Once the code is available for software quality assurance engineer, codewalk through has to be carried out. The automated tool helps in verifying the safe subset. Figure 3 shows the utility which will generate the report file saying whether the instruction is in safe subset or not. Any observations during codewalk through will be presented to committee.

4.4. Testing Phase

Test cases were generated based on the system level requirements, negative cases were also generated to test the same. Test cases for all the modes of CDEU were tested. Also mode transition from one mode to other
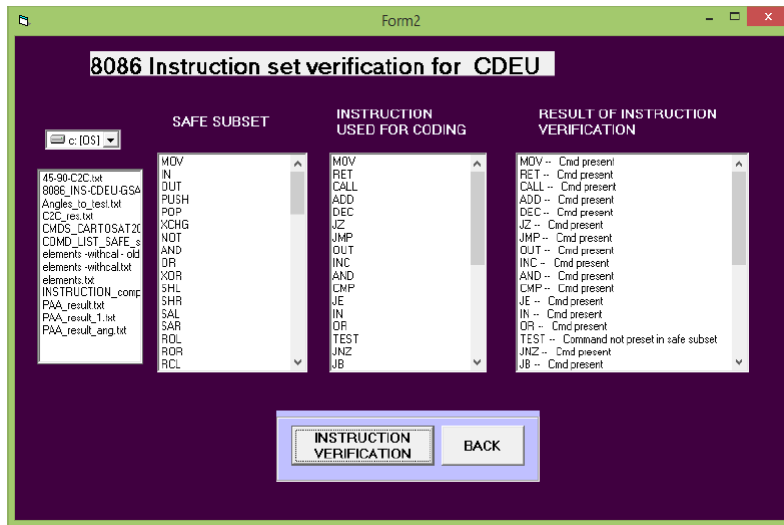
Figure 3. Validating the CDEU instructions against the safe subset

mode was also carried out. It will be going to halt mode automatically being in configuration mode or in the operation mode. Figure 4 shows the mode transition testing carried out as part of initial bench level testing [1]. Negative logic tests were tested in-depth. Even the mission scenario tests were carried out. All boundary conditions were thoroughly verified. All the telecommands and telemetry were verified. This is the major test to know that CDEU is functioning as per requirements [2].

To From	Init Mode	Configuration Mode	Operational Mode	Diagnostic Mode	Halt Mode
Init Mode	NA	Auto (With Check of Raw Bus and Cal Voltage)	NA	NA	Auto
Configuration Mode	Cmd rejected	√	√ (With 70V RB ON)	√	√
Operational Mode	Cmd rejected	√	√	√	√
Diagnostic Mode	Cmd rejected	√	√	√	√
Halt Mode	Cmd rejected	√	Cmd rejected	√	√

Figure 4. CDEU mode transitions as tested

One of the tests carried out for soft start and soft stop for CDEU by PWM enable and disable command is shown in Figure 5. The soft start voltage and the step size for soft start are commandable. Once PWM enable command is given till it reaches the commanded voltage it increases in steps [3]. Once PWM disable is given it decreases in steps and reaches zero volts.

5. Reviews and recommendations

All the observations and non-conformances found during codewalk through and testing will be presented to sub system review board. Based on committee recommendations change was carried out in the operation module to take care of safety logic. Regression testing was carried out for the same. Configuration management was also carried out. Initial version of the code was released once the designer level tests were

Figure 5. Soft start and soft stop with PWM Enable and disable

carried out. Later after testing and with committee recommended change new version of code is released. Delta code walk through was also carried out. As part of database verification all the limits, register values were verified.

6. Conclusion

The software is developed based on ISRO Software Process Document and documents were generated as per IEEE template. Software development process is clearly stated along with linkage of activities with inputs, process, outputs, responsibility and linkage to ISPD processes in this document. Our existing practices are much more strengthened in terms of documentation, process followed with the application of ISPD. Many non conformances were detected at the early stages and implemented. Hence it has saved much time during testing. It has shown our ability to refrain our existing processes with international standards. SQA provides the pre-certificate to project which has the list of SQA activities complied for the project.

Author Contributions: All authors contributed equally to the writing of this paper. All authors read and approved the final manuscript.

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Singh, R. (1996). International Standard ISO/IEC 12207 software life cycle processes. *Software Process: Improvement and Practice, 2*(1), 35-50.

[2] Sommerville, I. (2011). *Software engineering 9th Edition. ISBN-10137035152.*

[3] Pressman, R. S. (2005). *Software engineering: a practitioner's approach*. Palgrave Macmillan.