ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

# A Framework for the Software Aspects of the Safety Certification for Indigenously Developed Aircraft Systems

Manju Nanda , J Jayanthi, Shamsundar Dhage,

Scientist, National Aerospace Laboratories, Bangalore, India[1,2]

STO, National Aerospace Laboratories, Bangalore, India[3]

**Abstract:** Safety critical systems need certification from the authorized agency before deploying the system in field. Certification is the final clearance to the system for complying with the project requirements pertaining to functionality, performance and safety. The entire lifecycle process for the application follows a well defined approach to certify the system. This certification approach varies from one industry standard to other. Certification is an activity which is based on evidences to validate the system functionality, performance and safety.

In this paper we discuss a certification approach which can be developed into a framework for safety critical aerospace applications. The approach has been proposed based on the groups experience in certifying three safety critical systems i.e. Stall warning/Aircraft interface computer system, Automatic flight control system and Engine indication and crew altering systems. The framework can be used as a reference for the clearance of the safety critical software for civil aircraft systems in the country.

**Keywords:** Safety critical systems, certification, engineering process, certification framework

## I. INTRODUCTION

Every safety critical system need to be cleared by the certification agency before it gets inducted into the product. The certification approach for every system in the program is planned during the plan phase of the engineering process. Different industry standards provide guidelines to certify the safety critical systems. The certification standard for the various industries [11], [12], [13], [14] and [15] is shown in the Figure 1.

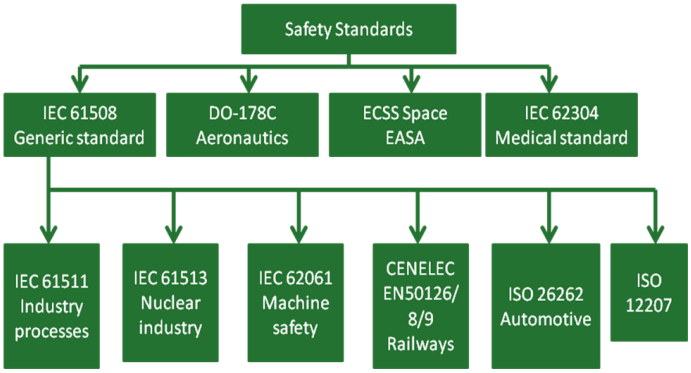


Figure 1: Certification approach for different industry standards

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

These standards guide the certification authorities to certify the system for the application. The certification authorities are required to audit the development, verification and the various support activities. The audits performed by the certification agency are known as Stage of Involvement (SOI) audits. Each audit is positioned at strategic points in the lifecycle to reduce the risk of failing the final certification audit. An early indication of a potential certification failure is vital to ensure that the software process is not heading in the wrong direction. An audit failure will normally require that an artifact must be reworked before the audit can be repeated. These audits at critical SOI build up the confidence of the certification agency before the final certification clearance.

In order to increase the confidence of the evidence for certifying the critical software three principles are considered. They are:

1. Necessity of the evidence: the evidence to support the scope of safety scenarios. Too much evidence will disturb the evaluator, and too little is not sufficient to support safety features of the software
2. Adequacy of the evidence: evidence must be clear, definite and objective.
3. Suitability of the evidence: types of evidence such as the result of analysis and testing, historical data must be suited to support safety scenario

These issues are considered in developing the certification framework [3]. This paper proposes a certification framework for safety critical systems in the Indian scenario. The certification framework proposed is based on the experience of certifying three safety critical systems for the civil aerospace domain. The proposed certification framework provides the approach for clearing the software as per the Indian civil aerospace agency DGCA (Director General for Civil Aviation) as per the RTCA DO-178B/C standard [17], [19].

The paper is divided into various sections. Section II briefs on the prior work carried out in the field of certification for safety critical systems. Section III explains the certification approach for systems developed in-house as case studies. Section IV emphasizes on the need for certification framework and section V focuses on the proposed certification framework for future applications as per RTCA DO-178B/C.

## II. PRIOR WORK IN CERTIFICATION FOR SAFETY CRITICAL SYSTEMS

Certification being the integral part of development of any safety critical systems, several studies have been conducted in the past & recent times in making the certification process more easier, adaptable and focused on the goal. These studies are spread across various domains and wide areas of interest in the field of software system certification.

The handbook on "Certification and Accreditation Process Handbook for Certifiers" [5] establishes standard approach for performing Certification & Accreditation (C&A) on systems regardless of the acquisition strategy or life-cycle status. It is for the use of all personnel involved in the C&A of systems regardless of the classification or sensitivity of the system

The paper on "Certification issues in automotive software", [6] discusses issues in the certification of automotive safety critical systems, role of standards in certification and their relationships with certification body, process, product, people and system.

"Suggestion of Criteria and Certification Process to Secure the Safety of Railway Software" [7] discusses the characteristic of railway software and analyses safety related standards are analyzed. The authors also suggest development methodology and certification procedure for the developer and assessor to easily make safety critical railway software while following the safety criteria.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

"A context aware framework for product based software certification" [8] provides a dynamic environment for the certification process by integrating development and certification domains with the help of ontology. Its main objective is to allow the certification process to be able to adjust to ever changing certification demands and extend more easily into different domains.

The paper "A Safety Application Certification Framework" [9] mainly discusses the need for certification & proven certification methodologies in most of the safety critical software like automobile, aerospace (WAAS) and public systems (CPWS).

"A SysML-Based Approach to Traceability Management and Design Slicing in Support of Safety Certification" [10] discusses a framework to enable systematic and efficient software design inspections during safety certification. This work mainly focuses on traceability & few limited aspects of design for certification.

All the above studies highlight on the different approaches for certification for different industrial domains. Each of these domains discuss on specific aspects of certification as per the industry standard but they collectively contribute in designing one or the other part of the proposed framework.

The above studies also show that so far no major work has been done in proposing or designing a generic certification framework for safety critical airborne systems. The designers of system often face problem in selecting understanding and implementing the appropriate approach for the certification of their systems. Each of the certification process has a learning curve as there is no reference for implementing. This has been an inspiration for a thought to design a certification framework as this will provide a knowledge repository of tools, techniques, methods and metric for certifying a airborne system software. .

## III. CASE STUDIES

As part of case studies we discuss three safety critical aircraft systems which are indigenously developed and are being certified by the DGCA. These systems are integral part of the SARAS aircraft developed by CSIR-NAL [16]. These systems are:

- SWS/AIC system : Stall Warning System and Aircraft Interface Computer system
- EICAS system : Engine Indication and Crew Alerting System
- AFCS system : Automation Flight Control System

The software's for SWS/AIC, EICAS and AFCS is indigenously developed as per RTCA DO-178B Level A criticality. Level A is the highest criticality of the software.
The criticality of the software is determined from the safety assessment process and hazard analysis by examining the effects of a failure condition in the system [18].

SWS/AIC system provide the pilot with the information regarding the critical warnings like the landing, takeoff, overspeed and pitch trim. The system also informs the pilot of the impeding stall condition. SWS/AIC system software is the first software in the country to be cleared by DGCA for 25 hours of flight. EICAS system takes inputs from various avionics systems and generates critical graphical data in appropriate format for the pilots during the flight. AFCS for the SARAS aircraft is a limited authority autopilot system with built-in features like the smooth engagement and the disengagement, flight director guidance, annunciations on the EFIS and CWP with a fail-safe architecture.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

All these system software's are developed by adopting "V'' model in an iterative manner. Every stage of the engineering process has a dependency on its previous stage. In every iteration a delta development has traversed through all the stages before the next iteration begins. The safety assessment is carried out at the beginning of the project to address the impact of safety aspects of the software on the aircraft and a detailed plan for ensuring the safety at all stages of development and verification. Even though this assessment is done once at the beginning of the project, it is revisited for every change in the requirement and/or design and/or development to ensure that the already assessed safety status is not affected.

The approach discussed here involves the evidences for certification being identified at each of the software lifecycle stages and at every stage the certification artifacts are generated. Thus the preparedness for certification begins right from the requirements phase. This not only eliminates the demand on generation of artifacts but also ensures that the processes follow the safety aspects from certification point of view. This increases the understanding of the development & verification team about the certification process and thus bridges the gap between the software & certification. Artifacts are generated as part of certification process in each of the phases i.e. the requirements phase, design phase, development phase, verification phase and the configuration phase.

Planning phase plans the project from design, quality, verification-validation, quality, configuration and certification point of view. Five planning documents, Plan for Software Aspects of Certification, Software Development Plan, Software Verification Plan, Software Configuration Management Plan and Software Quality Assurance Plan are generated. The checklist for the review and assurance of these documents is generated. Using the checklist checks the correctness and completeness of the documents are assured.

Requirements phase captures the project requirements in the Requirements Data document. The requirements are reviewed for correctness, completeness, traceability and safety point of view. Review checklists and Problem report are generated

Design phase conceptualizes the software. The software design description documents capture all this. Design Review Checklists (both system & software), Traceability Matrix between Requirements & Design are generated for correctness, completeness, traceability and safety. This refers to safety requirements in design.

Development phase implements the software as per the design. Reviews are done for the source code, executable object code, code compliance and traceability between the source code and design.

Configuration, quality and verification phase are the integral phases. These activities are done in parallel with the requirement, design and implementation phases. Configuration phase generates the SLCECI (Software Life Cycle Environment Configuration Index), Software Configuration Index and Software configuration management records. Quality phase generates the phase wise audit reports, document audit reports, configuration audit reports, verification audit report and the consolidate quality record.

Verification phase is one of the most critical phases of the engineering process and it verifies and validates the software for its functionality, performance and safety. This is done at every phase by means of reviews, analysis and testing. Checklist and test cases and procedures are generated. A consolidated software verification report is also generated. Bird's overview for the case studies is provided in TABLE I.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

TABLE I: Case studies

| Case Study | SWS/AIC System | EICAS (Engine Indication and Crew Alerting System) | AFCS(Automatic Flight Control System) |
|---|---|---|---|
| **Functionality** | To inform the pilot of the impeding stall condition, provide critical system warnings like the landing, takeoff, overspeed, hydraulic low pressure and baromismatch. The system also provides trim control and monitoring. | EICAS system interfaces with parameters from various aircraft critical sub systems and interfaces to the pilot in the graphical mode. The status of the sub-systems is display for informing the pilot. | Automatic flight control system is integrated into the aircraft to reduce the pilot workload. The primary flight control system of the aircraft has ailerons for roll control mounted on the wing, elevators on the horizontal stabilizer for pitch control, and a rudder mounted on the vertical fin for directional control. |
| **Metrics** | 18 Builds released, 14,000 SLOC, 4000 test cases developed | 5 Builds released, 68,000 SLOC and 10,000 test cases developed. | 9 Builds released, 25,000 SLOC and 3200 test cases developed. |
| **Challenges** | First time setting up the software engineering life cycle process for RTCA DO-178B Level A standard | Tailored IV&V process for first of its kind "Display" application<br>Different development approach….**rapid prototyping**. | First time for modular architecture<br>Limited experience with object code verification & registry verification |
| **Achievements** | Pioneered in establishing the complete SDLC process as per RTCA DO-178B Level A.<br>DGCA clearance for the SWS/AIC software for the safety of flight. | Tailored the established IV&V process activities based on the program requirements for a level A safety critical software.<br>Taking up new challenges and executing it successfully as per the organizational needs. | New idea generation for some of the IV&V activities.<br>IV&V process establishment. |

The certification objective for each of the system is achieved but the approaches for achieving the objectives were different as there existed no prior reference and the certification process was dependent on the certification authtorities. Since each of the system was unique in itself, certification process took time which also included the learning time. Though each of the avionic system is safety critical and the software is developed to Level A criticality, the approaches towards the certification were different. The SWS/AIC system is a federated system with the kernel providing the real time scheduling; the kernel used is a customized kernel in an object form. EICAS system is a federated display system, having a

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

real time kernel available in the source format. AFCS is a modular system with a real time operating system. The RTOS is available in the object format.

The development of the application software is different for the different hardware architectures and also since it is tailored to design approach, the verification-validation approach is different. Since each of the projects was unique, there were different challenges to meet the same DO-178B objectives. Based on the criticality of the software, the DO-178B mandates generation of a set of documents as part of evidences for the certification. [2]. However, to increase the confidence among the certification team, our approach generated several additional data, documents and reports. For example, for Level A software the DO-178 mandates to satisfy 66 objectives whereas the development of SWS/AIC system has generated one & half times the number of documentary evidences for compliance to the standards. Similarly the EICAS software process has generated twice the number of mandatory artifacts and in the SARAS-AFCS the number is again one and half times.

## IV. NEED FOR A CERTIFICATION FRAMEWORK

As more and more avionics systems are being designed, developed and certified in the country, the certification of these systems is the biggest challenge. So far systems were designed and developed and then certified. In current Indian scenario the approach to design the systems for certification should be adopted. For this approach, a certification framework which provides the designers the knowledge repository for certification is needed.

Technologies are becoming complex and to design and certify these technologies, new techniques are adopted. Model-based design, development, object-oriented programming, formal methods are some of the techniques adopted by the industry in design, development and verification of the state of art systems. The certification also needs to cater to these techniques. RTCA DO-178C released in June 2012 addresses these techniques to certify the safety critical aerospace systems. In order to minimize the time, budget from the conception to installation of the system without compromising on the safety and functionality the certification process needs to be formalized by means of the certification framework. The certification framework will provide the means of approach for the certification of a given safety critical system. The means of approach will provide a set of tools, techniques that can be used to certify the system.

Certification framework is a field of research where principles of science and engineering are used to ensure that the objectives of the standard are met. The evidence generated as part of the process should be determined systematically to ensure that they satisfy the defined and the measurable criteria. This will develop the confidence in the system being designed and developed. In the current certification there are gaps as each process from design to certification is dependent on the certification agency. In India for civil aerospace certification it is DGCA (Director general of civil aviation) and in defense aerospace Centre for military and airworthiness and certification.[18]

The need for certification framework is required to help designers design the systems for certification. As of now certification is treated as an external entity and systems are not designed for certification. The certification framework will provide guidance to the designer to design the system for certification [1]. For a successful certification of the system, the developer must know what the certifier expects as a quality submission, and the certifier must know what the developer could submit. These problems are not easily remedied simply by document specification, as certification experts' work on a wide variety of devices. Thus, a solution to these problems would necessarily be applicable both across and within domains [2].

To overcome this gap between the designers and the certification agency, the certification framework is required. One of the key requirements for certification framework is metrics. Some of the metrics the certification framework will

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

guide the engineers to develop are the metrics related to problem reports, test coverage, quality and safety. These metrics will provide the proof for the certification agency for the safety and functionality of the system against the requirements.

## V. PROPOSED CERTIFICATION FRAMEWORK

The certification framework being proposed is built upon proven techniques and practices that have been adopted to increase safety in the airborne software systems. The goal of certification framework is to systematically determine, based on the principles of science, engineering and measurement theory, whether an artifact satisfies accepted, well defined and measurable criteria. The challenge is to develop a certification process that achieves this goal as we must evaluate pieces of evidence about the artifact, which systematically increase our confidence that it is satisfactory, until the point where we make the determination that the artifact is acceptable, and assign a certification [4]

The proposed certification framework will provide techniques and metrics for the designers to design the system for the certification. This certification framework will be targeted for RTCA DO-178C standard [4]. RTCA DO-178C encompasses the object-oriented approach, model-based approach and the formal methods approach to be implemented for a safety critical airborne system. The proposed certification framework for DO-178C will be the first in the country which will provide reference to the designers for designing a system for certification with confidence.

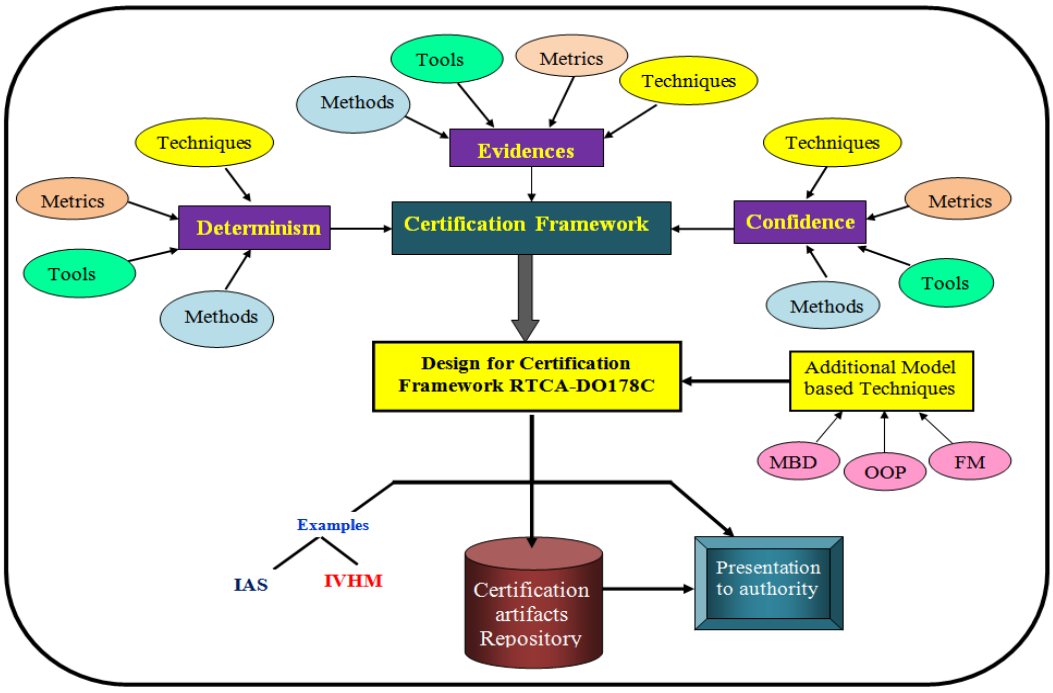


Figure 2: Proposed Certification Framework

The figure 2 shows the proposed certification framework. The framework provides a repository for designing critical and highly complex systems for certification. These complex systems could be the Integrated Avionics System (IAS) [19] or the Integrated vehicle health monitoring system (IVHM) [20]. For this purpose the designers needs to design

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

the systems which develops confidence in the certification authority with determinism. To achieve this, we need various tools, techniques, methods and metrics. These tools, techniques and methodologies form input for the generation of evidence & confidence with determinism. They help in deriving many metrics that provide important information about the development and verification processes and their assessment from certification point of view. The artifacts generated as part of the evidence thus provides the confidence in building the basis for the generic Certification Framework.

This generic framework is being developed for the RTCA DO-178C standard. This standard is the most versatile and stringent standard and if we develop the framework for this standard we can configure it for any other standards as described earlier.

## VI. CONCLUSION

This work focuses on the need for the certification framework in today's world where certification of the software is very critical in safety applications. The certification framework provides an approach for the designers to design and develop their software and generate the relevant proof to develop the confidence apart from the evidence required for the certification. The generic framework proposed captures all the process, methods and techniques that can be used to provide evidence, confidence and determinism of the software for the highly safety critical and complex systems. This framework also bridges the gap between the design and certification.

## ACKNOWLEDGMENT

The authors would like to thank the Director, CSIR-NAL for providing with the opportunity to work in these areas.

## REFERENCES

Panayiotis Steele "Certification-Based Development of Critical Systems", Department of Computer Science, University of Virginia, 85 Engineer's Way, P.O. Box 400740,Charlottesville, VA 22903, USA.

[1] Ian Dodd [a], IbrahimHabli [b], "Safety certification of airborne software : An empirical study", a. Airservices Australia, Building 101 Da Vinci Business Park, Locked Bag 747 Eagle Farm, QLD 4009, Australia, b. Department of Computer Science, University of York, York YO10 5GH, United Kingdom

[2] Fuping Zeng, Minyan Lu, Deming Zhong, **Software Safety Certification Framework Based on Safety Case,** School of Reliability and System Engineering, Beihang University, Beijing, China.

[3] http://en.wikipedia.org/wiki/DO-178C

[4] **NCSC-TG-031,** Version 1 ISWG-9608-28 , "Certification and Accreditation Process Handbook for Certifiers:"

[5] Mario Fusani, "Certification issues in Automotive systems", Systems and Software Evaluation Centre, **ISTI – CNR, Pisa, Italy,** Automotive SPIN - Milano, ISTI-CNR 11 October 2007

[6] Eui Jin Joung , *Advanced EMU Research Team, Korea Railroad Research Institute, Uiwang 360-1, Korea,* "Suggestion of Criteria and Certification Process to Secure the Safety of Railway Software"

[7] A thesis by Volodymyr Babiy, H.B.Sc., McMaster University "A context aware framework for product based software certification"

[8] J. R. Richardson, Principal Systems Engineer, Raytheon HTMS, Fullerton, CA, "A Safety Application Certification Framework"

[9] Shiva Nejati, Mehrdad Sabetzadeh, Davide Falessi, Lionel Briand Thierry Coq, Simula Research Laboratory , Oslo, Norway,. "A SysML-Based Approach to Traceability Management and Design Slicing in Support of Safety Certification"

[10] http://www.iec.ch/functionalsafety/ *dated 16/09/2013*

[11] IEC , ISO "International Standard IEC 62304 ; Medical Device Software – Software Life Cycle process" , 1st edition 2006-05.

[12] http://en50126.blogspot.in/2009/01/safety-approval-process.html *dated Jan 2009.*

[13] http://www.iso.org/iso/catalogue_detail?csnumber=43464 *dated 14/11/2011*

[14] http://dgca.nic.in/ *dated 16/09/2013*

[15] http://www.nal.res.in/pdf/saras-2011.pdf *dated 16/09/2013*

[16] http://en.wikipedia.org/wiki/DO-178B *dated 16/09/2013*

[17] http://www.rac.gov.in/nri_labs/cemilac.html *dated 16/09/2013*

[18] Integrated Avionics System (IAS), Integrating 3-D Technology On A Spacecraft Panel, D.J.Hunter, IEEE Aerospace conference proceedings, 2002, Pages: 2185-2191, Volume 5, Doi: 10.1109/AERO.2002.1035385

[19] Impact Of Integrated Vehicle Health Management (IVHM) Technologies On Ground Operations For Reusable Launch Vehicles (RLVs) And Spacecraft, IEEE Aerospace Conference Proceedings, 2000 , Pages :179-186,Volume 2, Doi: 10.1109/AERO.2000.878223