DEPENDABLE
COMPUTING

CLASS SYSTEM CERTIFICATION

John Knight and Jonathan Rowanhill
Dependable Computing LLC

Uma Ferrell
Ferrell And Associates Consulting

Dependable Computing Technical Report TR-2014-4

12/1/2014

Dependable Computing LLC
2120 North Pantops Drive, Charlottesville, VA 22911-8648
www.dependablecomputing.com

CLASS System Certification

Abstract

CLASS addresses certification as a fundamental part of the entire lifecycle from system concept formation to system decommissioning, and bases certification on the system safety case. The safety case combines and structures many items that would normally be identified and elicited separately as part of existing certification mechanisms. By definition, the safety case documents the rationale for belief in the adequacy of the safety of the subject system, and maintenance of the safety case across the complete lifecycle facilitates the requisite certification activities. CLASS includes an Analysis Framework that allows indirect evidence about the subject system to be eliminated, and so the doubts in the properties of a system that are engendered by indirect evidence are avoided. CLASS also includes a monitoring mechanism which provides a high level of confidence that the expected properties established by the Analysis Framework will be true. In order to conform to the requirements of regulating agencies, CLASS certification includes two audit phases that are expected to be accomplished by experts from the regulating agency. For the FAA, these experts would be licensed Designated Engineering Representatives (DERs).

1 Introduction

Support for system certification based on the notion of certification that is in current use by regulating agencies is a crucial element of CLASS. Development of a system that was not amenable to certification would be pointless.

Certification has a variety of different meanings in different contexts. CLASS certification is motivated by and informed by the process that is required by the US Federal Aviation Administration (FAA). Certification in this context is:

> “the legal recognition by a certification authority that a product, service, organization or a person complies with the requirements. Such certification comprises the activity of technically checking the product, service, organization, or person and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval, or other documents as required by national laws and procedures. In particular, certification of a product involves: (a) the process of assessing the design of the product so as to demonstrate an acceptable level of safety; (b) the process of assessing an individual product to ensure that it conforms with the certified type design; (c) the issuance of a certificate required by national laws to declare the compliance or conformity has been found with standards in accordance with items (a) or (b) above”[1].

The existence of the safety case for the system of interest and the synchrony between the two elements of the SSCP enable the safety case to be the focus of certification. CLASS certification answers the fundamental question - whether a system is adequately safe to operate in its intended environment - by analysis of the safety case.

A system created using CLASS will proceed to certification as the second phase of the overall lifecycle. However, the certification phase is neither the beginning nor the end of the certification process. The property of being certified must be maintained throughout the remainder of the lifecycle, up to and including the decommissioning (final) phase. This requirement for maintaining the property of being certified indicates that certification itself must contribute to the infrastructure necessary for maintaining the property during operation, maintenance and decommissioning.

As well as certification supporting the post-certification lifecycle phases, the *creation* lifecycle phase must contribute to certification throughout the remainder of the lifecycle. The activities involved in creation must enable the certification process throughout the lifecycle. These concerns and the goals of certification help define the requirements for certification in CLASS.

[1] This is the definition that was provided by the Final Report of RTCA Task Force 4 - Certification, February 26, 1999.

In the remainder of this paper, an overview of CLASS certification is presented in Section 2. Section 3 presents a summary of the Filter Model, the theory upon which CLASS certification is based [1]. The structure of the audit mechanisms used by CLASS certification is based on the concept of certification in the context of a safety case introduced by Graydon, Knight and Green [2]. This model is summarized in Section 4. In Section 5, the means by which CLASS deals with large safety cases are reviewed. Stakeholder considerations are discussed in Section 6. In Section 7 the basic issues that arise in the certification of aircraft systems within the current FAA framework are reviewed. This review provides the basic contraints that a complete certification mechanism within CLASS has to address. The review also provides a basis for judgment of the suitability of theoretical concepts that are being pursued within the development of CLASS.

2 Overview

Certification as practiced currently by most regulating agencies is composed of three parts:

- Auditing conformance with mandated standards. In the case of the FAA, for example, these standards include RTCA DO–178B/C for software.
- Auditing of the process undertaken during development. In the case of the FAA, for example, auditing of the process is undertaken by FAA licensed Designated Engineering Representatives (DERs).
- Auditing of the product and the associated development artifacts over and above the requirements imposed by the mandated standards. This audit phases enables analysis tailored to the specific requirements of the subject system. In the case of the FAA, for example, auditing of the product and the associated artifacts is also undertaken by DERs.

In practice, the distinction between these three elements of certification is frequently not sharp, and the details of how they are conducted varies both between regulating agencies and between individual certification processes.

The structure of CLASS enables a refined version of these three elements. The safety case combines and structures many items that would normally be identified and elicited separately as part of existing certification mechanisms. By definition, the safety case documents the rationale for belief in the adequacy of the safety of the subject system. In addition, if implemented as expected, the CLASS Analysis Framework eliminates indirect evidence about the subject system, and so the doubts in the properties of a system that are engendered by indirect evidence are avoided. Finally, the CLASS monitoring mechanism provides a high level of confidence that the expected properties established by the Analysis Framework will be true.

The four pillars upon which certification in CLASS is based are:

- CLASS makes the existence of the safety case explicit and requires that the safety case have certain properties.
- CLASS assurance analysis allows prediction of the properties that are expected of both the subject system and the system safety case (the SSCP).
- CLASS monitoring allows confidence in the predicted properties of the subject system and the system safety case.
- CLASS facilitates certification activities and the associated development of artifacts throughout the lifecycle by making provision for lifecycle certification activities supported by:
  - the basic definition of CLASS,
  - the lifecycle monitoring concept,
  - the comprehensive mechanism for assembling system artifacts (the SIR), and
  - the explicit lifecycle availability of the safety case.

From the perspective of a regulating agency, CLASS certification is broken into two parts both of which are auditing activities and both of which would be undertaken by an expert designated by the regulating agency:

- Auditing of the instanceCLASS for the subject system. This auditing is facilitated by the results of monitoring undertaken during development.
- Auditing of the safety case for the subject system. This auditing is essentially in place to determine whether the safety case is compelling.

These audits are supported by the CLASS Analysis Framework and the content and organization of the system safety case.

3 The Filter Model

The *Filter Model* of certification was developed by Steele and Knight [1]. The Filter Model characterizes the certification process itself as a safety-critical system in which certifying a system that should be rejected is treated as a *certification accident*. The four possible outcomes of certification are shown in Figure 1. Clearly, rejection of an acceptable system is undesirable, but certification of an unacceptable system could have serious safety consequences and that case is the initial focus of the CLASS certification mechanism.

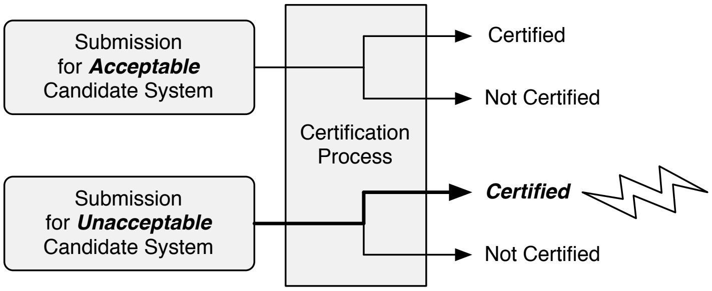
Submission for ***Acceptable*** Candidate System
Submission for ***Unacceptable*** Candidate System
Certification Process
Certified
Not Certified
Certified
Not Certified

Figure 1: The Four Possible Outcomes of Certification

Since the Filter Model bases analysis of certification on the treatment of certification as a safety-critical process itself, all of the tools of safety engineering can be applied immediately to certification. For example, since incorrectly certifying a system is considered an "accident", safety-engineering techniques such as hazard analysis and fault-tree analysis can be applied to certification. Such techniques identify the ways in which any given certification process could allow a defective system to pass through certification.

The Filter Model structures the certification process as a filter (hence the name). The goal of the filter is to identify faults in the system being certified. The filter that is a certification process is structured as a series of planes, each of which targets a prescribed set of faults that might be present in the subject system. The union of the fault classes targeted by the various planes in the filter should be the entire set of possible faults in the system being certified.

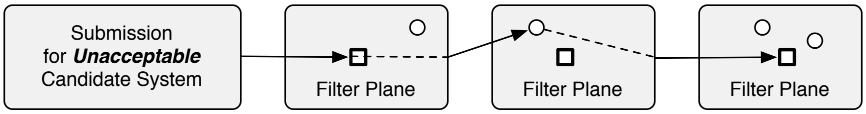

Figure 2: Instance Certification Filter

The structure of the filter concept is shown in Figure 2. Each plane in the filter has a path through which an acceptable system should pass. This notion is illustrated in the figure by the small squares at the center of each plane.

Inadequacies in any filter plane could allow an unacceptable system to pass and lead to certification of that unacceptable system, *i.e.*, a certification accident. Such inadequacies are shown in the figure as small circles located at different points in the various planes. An unacceptable system is shown passing through a defect in the second filter plane in the figure.

The sufficiency of any certification process lies in the degree of freedom of the various planes from these inadequacies. Application of safety-engineering assessment techniques to any specific instance of the CLASS certification process, techniques that are usually applied to the determination of residual risk, allows assessment of certification and offers the possibility of correction of weaknesses.

The results of applying the Filter Model can be codified in the form of a standards. Thus, instanceCLASS can be developed for any given application with a unique standard-like guidance document. To the extent that systems share common certification goals, as is likely in the aerospace domain, a generic standard could be developed for metaCLASS from the Filter Model.

4 The Dialectic Model

The Filter Model is conceptual. Although not acknowledged as such, in present practice, as noted by Steele and Knight [1], the filter concept is realized by standards that effectively transfer the responsibility for, location of and operation of the filter from the certifying organization to the development organization. This transfer explains the origin and role of standards, and provides a basis both for the definition of and assessment of standards.

In CLASS, the entity being subject to filtering has switched from various forms of documentation about the subject system to the associated safety case. The safety case is the rationale for belief that the subject system is adequately free of faults as appropriate for the operation of that system. Prevention of certification accidents (in the sense of Steele and Knight), therefore, rests upon determination of the adequacy of the safety case. Thus, realizing the Filter Model in CLASS requires a filter that will detect faults in the safety case and its use. The safety-case filter has to establish freedom from faults in two dimensions:

- Completeness and validity of the argument.
- Adequacy of the argument to the extent that the argument engenders confidence in the top-level goal.

In the CLASS certification filter, shown in Figure 3, is based on a certification concept developed by Graydon, Knight and Green [2] (hereinafter referred to as GKG).

The detection of faults by the GKG approach to certification is broken down into two major phases. In the first phase, a variety of qualities are established by inspection. The set of qualities are the definition of *completeness* and *validity*.

The inspections that establish the various properties are based on a technique called *Phased Inspection*. This technique was developed by Knight and Myers for rigorous inspection of software [3]. Phased inspections are well suited to inspection of safety arguments and the other elements of a safety case because of their rigor and comprehensive structure, as well as minimizing rework by timely capture of problems.

In the second phase, a set of *challenges* are applied to the argument by a team consisting of an advocate for the argument and a challenger using a structure called a *dialectic*. The intent of the dialectic is to conduct a structured discussion in order to reach agreement about the argument's *adequacy*. The challenges are accumulated over time as experience is gained in the domain of interest.

5 Large Safety Cases

Large safety cases are inevitable in modern aviation systems, and certification must take that into account. In CLASS, scale is dealt with by using two complementary techniques:

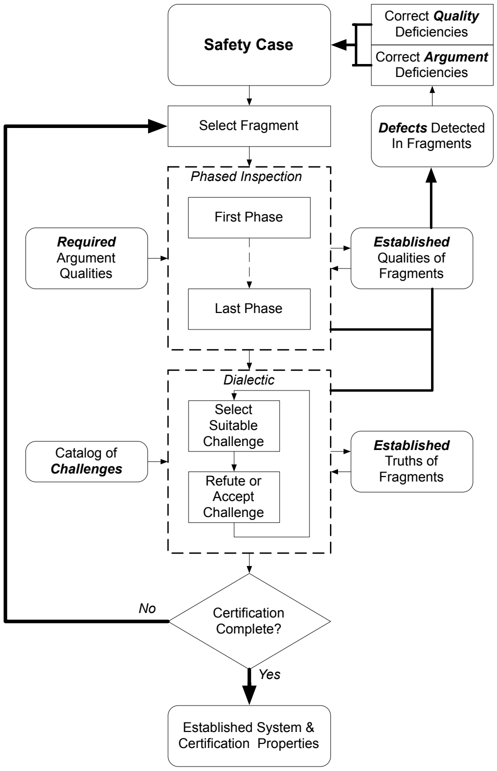
Safety Case
Correct *Quality* Deficiencies
Correct *Argument* Deficiencies
Select Fragment
Defects Detected In Fragments
Phased Inspection
First Phase
Last Phase
Required Argument Qualities
Established Qualities of Fragments
Dialectic
Select Suitable Challenge
Refute or Accept Challenge
Catalog of *Challenges*
Established Truths of Fragments
No
Certification Complete?
Yes
Established System & Certification Properties

Figure 3: Proposed CLASS Safety Case Analysis Mechanism

- The CLASS process structure that enables the construction of large systems using teams that operate relatively independently allows different system elements and associated safety case elements to be developed separately. Materials necessary for certification can be prepared separately.
- The modularity of the system safety case incorporates a contract/guarantee model of safety-case modules. The filter and dialectic models instantiated for the system of interest are used to derive sub-filters with each sub-filter tailored to an argument module in a particular domain. In essence, this approach corresponds to partitioning the overall safety case into separate assurance cases for the various technical domains and certifying each separately.

By combining these techniques, operating within the CLASS process model, and employing the CLASS monitoring mechanism as intended, large system safety cases can be accommodated in system certification.

6 Stakeholder Certification Considerations

In practice, many details have to be addressed in order to ensure that the pragmatic issues are addressed properly. The theory and principles of certification are not sufficient to allow development of the CLASS certification mechanism. For example, details such as document formats, presentation forms, content ordering, media used and so on have to be addressed. In this section, these details are elaborated from the perspective of the system stakeholders.

For the system stakeholders, the following pragmatic requirements of certification have to be addressed:

1. **Completeness**. A safety case must be complete in order to be suitable for any subsequent purpose such as certification. A safety case is complete only if it is suitable for the operational context within which the system is expected to operate.
2. **Technology Used**. Technology used in development must lend itself to providing repeatable, auditable and sufficient evidence for the safety claim on which the safety case rests.
3. **Confidence in Claims**. There must be defensible reasoning and justifiable basis for asserting adequate confidence in the safety claim.
4. **Certifiability**. In cases where systems have to be certified before use by a regulating agency, the safety case has to be acceptable to a regulating agency and the process whereby the agency makes that determination must effect a suitable degree of certification.
5. **Proof of Competence**. Whether or not certification is required, motivated by a desire to minimize accidents or product recall, the system developers create a safety case to detect any deficiencies in engineering. This provides an opportunity to conduct complementary engineering activities to complete a robust safety case.

Each of the purposes listed above has many variants thereby making a single detailed CLASS certification process impractical. Thus, certification reflects the instanceCLASS/metaCLASS distinction. The overall structure of the certification process is shown in Figure 4.

At the metaCLASS level, certification relies upon the *Filter Model* [1] (see Section 3). The basic the process used to implement the Filter Model is based on the *dialectic model* [2] (see Section 4. Finally, both the theory and the process of CLASS certification are informed by relevant *regulation*.

At the instanceCLASS level, the instantiation of the certification mechanism is informed by the subject system. As shown in Figure 4, the instanceCLASS assurance mechanism combined with the progression of real-world requirements over time have to reassess the safety case as necessary. Coordination over time is undertaken by the Safety Information Repository. The details of what triggers re-certification and what is required to properly assess the safety case when recertification is triggered are determined by the certification constraints that derive from regulation.

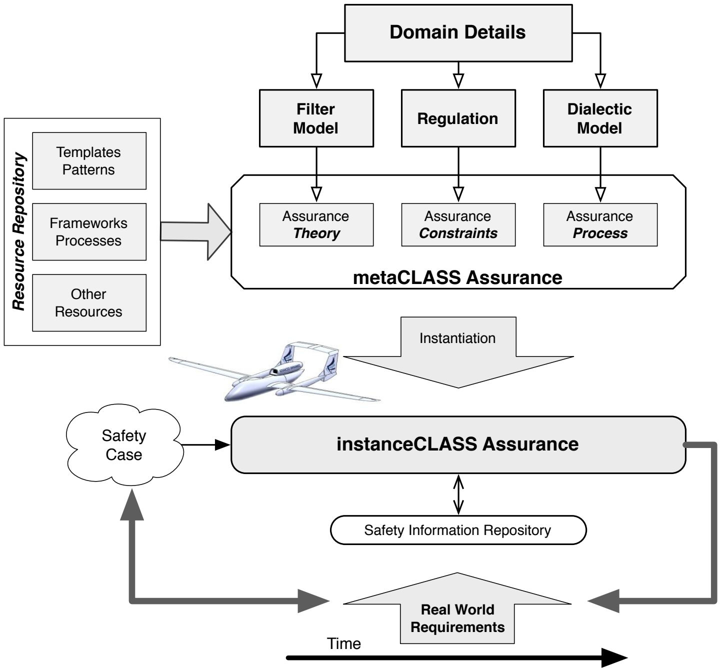

Figure 4: Certification Approach Overview

7 FAA Certification Considerations

The safety and assurance case paradigm can be expected to be used in design assurance of new and modified systems, reapplied when there are changes in environment (operation, training or maintenance), and reviewed in investigating incidents and accidents. In fact one of the advantages of the safety case approach is that it can be used from commissioning of the system all the way to decommissioning of the system, airborne as well as ground systems as an integral whole.

The FAA has different roles in different domains. As a regulator, the FAA is more focused on "auditing" the development of airborne systems. In this case, the cost and schedule risk is borne by the industry. However, for ground systems, the FAA is frequently the acquirer. This forces the FAA to balance cost, schedule, and the extent of assurance required to meet both real and perceived safety risks. "Certification" does not exist on ground systems although attempts have been made to introduce the concept of "Type Certification" of ground systems much like Type Certification of airplanes and engines. There is a general application of IEEE 12207: Standard for Information Technology – Software Life Cycle Processes for the full lifecycle of ground systems, but the rigor and details of application are not as closely monitored with competing demands of cost and schedule.

There are some safety assessment problems with ground systems that communicate directly with airborne systems. In most cases, the safety considerations are separately analyzed, assessed and determined for the airborne systems and the ground systems even in cases where the there is a tight functional link between the airborne and ground systems. The FAA has made some progress in these cases through the application of RTCA DO–264 Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications. This document, originally conceived for datalink system definition and assurance, has now been applied to a wide range of NAS-wide[2] systems (e.g., ADS-B). DO–264 requires the development of a comprehensive definition of the operational environment and then requires the development of safety and performance requirements based on that definition.

[2] National Airspace System

Comprehensive application of this approach has been slow and is not yet routine.

There is another challenge for the introduction of any new method, tool or technology into considerations of "certification". Ideally, all parties involved in the dialogue are fully engaged, understand the conversation, can ask intelligent questions, make knowledgeable decisions, and can come to evidence-based conclusions. A goal-based method such as a safety case dictates that all parties are thinking in a paradigm different from a checklist mentality, a mentality that sometime permeates an objective-based paradigm. When either the developer or the regulator does not understand the method/technology/paradigm, they usually tend to be extremely conservative to compensate for the lack of knowledge and fear of unsafe conditions. This situation can lead to the application of limited resources in areas that would not otherwise receive such a high level of scrutiny, thus defeating the graduated system that is now in place.

7.1 Certification Approach

The goal in CLASS is to develop a certification approach using safety cases that would be consistent with the FAA principles.

7.1.1 Traits of Regulatory Approvals

The following list includes some of the traits of the current FAA methods for "finding compliance" of airborne systems.

1. Developers and the FAA work with the focus on compliance to all applicable FAA regulations (14 CFR).

2. Graduated effort that depends upon the graduated levels of safety and risk.

3. The system safety assessment is rooted in past experiences of accidents and incidents as well as vulnerabilities of specific functionality, reliability of materials and components used, geometry of positioning on the aircraft (zonal safety), non-interference principles, operating conditions (temperature, pressure, flammability, exposure to dirt/sand *etc*.,), common cause failures, *etc*. Special attention is given when new and novel functionality or materials are used since there is no tribal knowledge to back up the analyses.

4. Review of plans at the outset to assess whether the plans completely and correctly address all compliance concerns.

5. Graduated level of involvement by the FAA depending upon several risk factors such as experience level of the developer, complexity of the project, design assurance level, novelty of technology *etc*. coupled with continuous involvement of independent observations by a quality engineer.

6. Independent set of audits/reviews of engineering accomplishments throughout the project so that corrections can be made without having to undo work already completed.

    - Requirements are exactly implemented; components of this item are the tight configuration management to ensure to the extent possible that: *as specified = as built = as tested = as delivered*, avoidance of errors, examining/fixing all possible sources of errors, tracking/resolving all known errors *etc*. Open problems are also reviewed for safety and workaround.
    - No "extraneous" functions are introduced (robustness testing, structural coverage).

7. Assure that "Type design data" is available at the aircraft or engine level from all component development efforts.

8. Prior to fielding a system, its maintenance characteristics, human factors as well as its interaction with other systems, and importance to operation must have been analyzed. These factors are grouped under continued certification considerations (maintenance and training) as well as minimum equipment required to be operational for a flight (Master Minimum Equipment List).

9. In most cases, the applicant makes a “statement of compliance” to state that the work that has been done is compliant.
10. Assure that there are clear delineations between different gradations of activities for different gradations of design assurance so that the regulator is focused on what exactly is needed for compliance. For a safety case, this issue raises the question of how robust an argument is needed for level A as opposed to level D.
11. Compliance finders (e.g., DERs, ODA unit members) are expected to go through initial training and recurrent training to learn and keep up with changing regulations or application of regulations.
12. Recently, the FAA has introduced an ICAO initiative call *Safety Management Systems* where safety is introduced and nurtured as a cultural component of organizations that work in aviation. Further, the FAA has been promoting an “Accountability Framework” that puts the responsibility on the applicant who emphatically should not depend on the FAA to make the case of correctness or safety or compliance.
13. The FAA also coordinates with other regulatory bodies to assure recognition of compliance as needed in other parts of the world.
14. Certification of the equipment, or more specifically the configuration and interaction between equipment may be indirectly tied to certification of the operating rules.
15. Instructions for Continued Airworthiness come into play for systems with specific Certification Maintenance Requirements.
16. Change Impact Analyses are conducted any time system updates are made.
17. The general sentiment is “Aviation in itself is not inherently dangerous. But to an even greater degree than the sea, it is terribly unforgiving of any carelessness, incapacity or neglect.”

7.1.2 Traits of Applicant Methods

The following are the generalized traits (they might not be universally true) of current methods used by applicants in order to “show” compliance:

1. Choose methods that lend themselves to planning, procedures and standardized methods that give an idea of whether the resulting product will be compliant – audits are always performed against plans/procedures/ standards.
2. Choose methods that leave a trail of evidence as a consequence of activities that can be examined by a third person.
3. Implement an independent quality system that gives the applicant full control of compliance activities and a basis for making the compliance statement – self disclosed statement of responsibility.
4. Assure that data needed for maintenance and continued compliance is indeed controlled.
5. Assure that data used for compliance establishment is controlled and available in case of incidents and accidents.
6. Optional: make data/access easy to review.

7.2 Designated Engineering Representatives and Aircraft Certification Offices

We can only speculate about the future in light of moves that the FAA has been making to place the responsibility for safety squarely in the hands of the applicants by even giving the approval authority to the applicant Organization Designation Authorization.

We cannot be sure what the role of Aircraft Certification Offices (ACOs) would be when all of the applicants have their own ODAs. Further, no real constraints have been placed on ODA unit members, equivalent of DERs. Currently, ODAs are making use of DERs as their unit members.

The FAA reviews each DER and his/her work every year; if the DER has not performed any of the “find compliance” activities, the FAA has the authority to terminate the DER’s license. DERs working within an ODA have the disadvantage that this experience does not qualify for the FAA’s annual review. Further, since DERs who work on ground systems, space systems and TSOs are not qualified for the FAA’s annual review, some of the DER work force will surely be terminated due to inactivity in years to come.

ODAs will be populating their units with non-DERs. This might lead to an erosion of the skill base. There is also a concern of ‘polluting’ the compliance-finding workforce by mixing this activity with project management as well as other cost and schedule driven aspects.

7.3 Big Picture Considerations

The overall goal of the FAA’s certification process is to ensure that only safe systems are fielded and fielded systems continue to be safe. The current DER/ODA-based compliance finding activity to support this goal (although “safety” is not used in the certification standards for legal reasons) is based on objective-based standards has evolved over time and is ever expanding.

Each new technology introduces additional items that need to be planned for, implemented, and verified to demonstrate correctness of implementation and appropriateness for use. As a result, design assurance activity continues to increase at the software level, hardware level, avionics level, aircraft level, multiple aircraft level and airspace level. In addition, every new incident or accident may add yet more items that need to be checked or protected against.

At the same time, the need for clarity and clear evidence that oversight has been adequate is driving an ever more prescriptive, ‘by the book’ mentality in terms of documenting compliance finding. This too increases the overall workload and tends to shift the focus of oversight to those things that are relatively easy to check and away from those things that are hard to check (or at least hard to document conclusively).

This path is not sustainable over the long run as complexity and cost will ultimately lead this system to fail. For example, DO–178C’s introduction of multiple technical supplements, while at the same time maintaining the core document almost unchanged, continues the status quo for compliance demonstration and compliance finding without acknowledging the increased complexity and interdependencies inherent in modern avionics development.

From the DER’s perspective, one of the possible benefits that could be realized from safety/assurance cases is better prioritization of compliance demonstration and compliance finding activity. The software type, its role within the broader system of systems, and consideration of other technology present in the design could allow for the safety cases to only callout DO–178C-like compliance for certain elements of the software application. This would afford more flexibility in approach for those system/software aspects that can be demonstrated as being correct via some other means or for which direct demonstration is not as important due to other elements present in the system.

It is imperative that any guidance for using safely cases clearly note the necessary and sufficient acceptance criteria. For this to work, personnel qualifications are likely to take on a bigger role as engineering judgment based on sound logical decision making will be required. All of the approaches to safety and assurance cases of which we are aware require a level of knowledge and structured reasoning that are not necessarily the norm across the workforce currently involved in design assurance today. This statement holds true for both the regulator and industry.

References

[1] P. Steele and J. Knight, “Analysis of critical system certification,” in *High Assurance Systems Engineering Symposium*. IEEE, 2014.

[2] P. Graydon, J. Knight, and M. Green, “Certification and safety cases,” in *International System Safety Conference*, ISSC. International System Safety Society, September 2010.

[3] E. Myers and J. Knight, “An improved software inspection technique and an empirical evaluation of its effectiveness,” *Communications of the ACM*, vol. 36, no. 11, pp. 50–61, November 1993.