Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems

Position Paper

Huáscar Espinoza, Alejandra Ruiz
Software Systems Engineering Unit
Tecnalia/European Software Institute
Zamudio, Spain
[firstname.secondname]@tecnalia.com

Mehrdad Sabetzadeh
Certus Software V&V Center
Simula Research Laboratory
Oslo, Norway
mehrdad@simula.no

Paolo Panaroni
Consulting Division
Intecs S.p.A.
Pisa, Italy
paolo.panaroni@intecs.it

***Abstract*— Safety assurance and certification are amongst the most expensive and time-consuming tasks in the development of safety-critical embedded systems. The increasing complexity and size of this kind of systems combined with the growing market demand requires the industry to implement a coherent reuse strategy. A major problem arises as typically a safety-critical product and accompanying safety evidence is monolithic, based on the whole product, and evolutions to the product become costly and time consuming because they entail regenerating the entire evidence-set. Another key difficulty appears when trying to reuse products from one application domain in another, because they are constrained by different standards and the full safety assurance certification process is applied as for a new product, thus reducing the return on investment of such reuse decision.**

This paper describes the current state on safety assurance and certification of embedded systems in the avionics, railway and automotive domains and then proposes some future directions for work in the area. In particular, we describe the need for a common certification framework that spans these different markets to improve mutual recognition agreement of safety approvals. We then discuss the need for new strategies focused on a compositional and evolutionary certification approach with the capability to reuse safety arguments, safety evidence, and context information about system components, in a way that makes certification more cost-effective, precise, and scalable.

Keywords: safety critical systems, safety certification, safety assurance, avionics, railway, automotive

I. Introduction

The innovation and productivity in the market of safety-critical embedded systems is curtailed by the lack of affordable safety assurance and (re)certification approaches. Major problems arise when evolutions to a system entail reconstruction of the entire body of certification arguments and evidence. Further, market trends strongly suggest that many future safety-critical systems will be comprised of heterogeneous, dynamic coalitions of systems of systems [11]. As such, they will have to be built and assessed according to numerous standards and regulations. Current certification practices will be prohibitively costly to apply to this kind of systems.

Another key difficulty appears when trying to share products between different application domains, because they are constrained by multiple standards and the full safety assurance certification process is applied as for a new product, thus reducing the return on investment of such reuse decision. The “high costs” per se is not the only issue, the pursuit of safety at any cost is often not balanced with other aspects such as scaling and prioritizing risks, the economic impact, and more significantly the restraint on innovation or just on product upgrading. This paper describes the current state of safety assurance and certification/qualification of embedded systems in the avionics, railway and automotive domains and proposes an ambitious work agenda, targeted by a new FP7 large-scale integrated project, called OPENCOSS (Open Platform for EvolutioNary Certification of Safety-critical Systems). This project will run for three and half years since October 2011 with a consortium of seventeen companies from nine countries. Some of these are Alstom Transport, Thales Avionics, Centro Ricerche FIAT, RINA, DNV, Intecs, AdaCore, Atego, Parasoft, ikv+, Altreonic, HPDahle and academic/research organisations such as University of York, Simula Research Labs, LaQuSo Labs, and Tecnalia/European Software Institute. The project is poised to make a significant and long-lasting impact on the way safety-critical embedded systems are certified and put into operation.

The next section gives a snapshot of four key challenges in safety assurance and certification of embedded systems by looking at domain specific issues, but also by looking at common issues in the different domains and levels of regulation. Section III describes five core directions for future work which will be addressed by OPENCOSS: (1) common certification language, (2) compositional certification, (3) evolutionary evidential chain, (4) transparent certification process, (5) compliance-aware development process. Section IV concludes with a brief summary of the central points addressed by the paper.

II. Current State and Challenges

Safety assurance and certification of safety-critical embedded systems is complicated by several factors, as we briefly describe below.

A. *Lack of precision and large variety of certification requirements*

Most safety standards aspire to precision. However, determining the degree of compliance with specified standards or practices for the different safety-critical market and technological domains is a challenging task.

For instance, the desire to make DO-178B (also known as the airworthiness standard), widely accepted in the avionics domain also made it imprecise, and evaluations have yielded very different results when conducted by different organizations or government agencies. There are very few detailed requirements for standards and checklists contained within DO-178B.

The aerospace industry is becoming increasing more reliant on software-based systems, with millions of lines of software code running onboard advanced planes and helicopters and on ground station platforms. The higher complexity and size of software combined with the growing market demand requires the industry to redefine its core and non-core activities, and to implement a coherent reuse strategy instead of relying exclusively on in-house-developed applications. For example, if the engine control computer from the automotive industry is to be reused in aerospace, the full certification process is applied as for a new product, thus reducing the return on investment of such decision. A second issue is interoperability. Aerospace applications are being more and more opened to “external” world, e.g., ground stations for flight planning, Ethernet for maintenance issues, air traffic management systems, customer information system. This introduces potential safety risks because not all elements of the chain are subject to a unified certification framework. While the aerospace industry is convinced of the benefits to share some development with other industries, it first and foremost requires a common certification framework, so that the certification results for a system or component originally developed for a different domain can be carried over to the aerospace domain.

In the railway domain, the European Railway Agency (ERA) has recently published the first draft for its recommendation on Common Safety Methods (CSM) [6]. CSM are methods describing how safety levels, achievement of safety targets and compliance with other safety requirements are assessed. Unfortunately, these recommendations contain only requirements, but no unified efficient methods to comply with the particular requirements. The current state of practice is to informally apply these recommendations, which heavily depends on the implicit assumptions and judgment of the particular independent safety assessors. This significantly complicates the certification process and hinders efficient re-use or adaptation of analyses. A second major complexity factor is that related subsystems need to be harmonised in their certification, e.g. the certification of the interlocking and the train control subsystems need to be closely aligned together. Similarly, the certification of the components in a subsystem, like axle counters and energy supply in the interlocking subsystem, need to be organised in a consistent way. Specific procedures have to be applied to ensure that the different inputs as well as results for the process of safety demonstration and certification are consistent, and in the correct order. Railways have a long established history with safety of signalling installations, and due to their national boundaries the process for safety approval can be quite different from country to country. This generates problems of cross-acceptance of safety approvals, being one of the main obstacles to borderless train interoperability within Europe.

In the automotive domain, the evolution is towards adopting automotive standards to reach a competitive advantage within the off-highway market. The safety requirements for machine construction are following a similar path. With the tighter regulations and increased customer expectations, safety standards such as the forthcoming ISO 26262 and software certification based on these standards are now seeing wide adoption in all these sectors. A key issue here is that safety standards are still maturing and complex to use and while driven by domain-specific needs, there are a lot of commonalities and hence significant overlaps between different safety aware processes. An example of effort in this direction is the Flanders’ Drive ASIL project [7]. This project was started in 2009 and has taken the major standards in automotive, off-highway and machine construction as input with the aim of defining a common standard for all these domains. The complexity for this effort can be measured by the fact that a semi-atomic analysis of the standard has identified close to 3000 process requirements that have to be met.

In a more general context, there are a variety of definitions of evidence, and how to evaluate it or derive it in regard the technology used, which makes cross-acceptance a difficult task. We also have a problem in understanding how to combine different evidentiary material when determining an overall evaluation of the evidence. To share products between industries, any best practices should be broadly shared and enforced due to the complexity and size of safety critical embedded systems.

B. *Lack of composable/modular view for certification*

Often, certification schemes are accused of being too process-centric, and not focusing enough on the product itself. In addition, they rely on a top down, bespoke, design approach. The process-centred certification approach does not translate effectively in a component-based (or systems-of-systems) environment. Modern engineering and business practices use massive subcontracting and Commercial Off The Shelf (COTS) component-based development that provide little visibility into subsystem designs.

In the aerospace domain, experience shows that despite the difficulties and costs incurred over the certification of COTS components, these components pose relatively few problems, and in most cases, with only minor negative impact. This observation suggests that the required levels of safety can be met by adopting broadly-used COTS products, thus laying the groundwork for a reuse strategy in aerospace system design.

In the automotive domain, ISO 26262 has introduced the concept of SEooC (Safety Element out of Context) where a component is evaluated against "presumed" operational context conditions. Once the component becomes part of a specific system in an actual operational context, the evaluation is optimised by comparing assumed context conditions against actual context conditions. This is in the right direction though it deserves to be investigated further.

Another important consideration is that safety assurance demands a systems perspective, in which the software is viewed as one component of many, working in concert with other components (be they physical devices, human operators, or other computer systems) to achieve the desired effect. Hence, a long term solution can only be found by taking a product-centred, composable/modular system view of the certification problem. This would imply that (a) certification approaches should be extended to use certification data in terms of the component/system interface only and, (b) they must address technology, policy and personnel issues in parallel.

C. High and non-measured costs for (re)certification

The lack of transparency in certification is a frequent problem in the current practice, in large part arising due to poor visibility into the architecture of systems, their design rationale, how components were verified and integrated, and finally how the system components and the system as a whole were certified. We take the view that a transparent certification cannot be achieved in isolation but only in tandem with transparent development and integration processes. Hence, it is essential to take a more holistic view towards transparency, consider the various stakeholders that play a role (e.g., suppliers, certifiers, integrators, operators, owners), and how each stakeholder anticipates benefiting from transparency.

Given the great number of certification schemes in the embedded system industry, it is rather surprising that there are no studies about the economics of certification. Furthermore, certification costs are not well-known within companies [1]. In order to gain deeper insight, we need to more accurately assess the cost of certification, and further identify the articulated and unarticulated benefits offered by a new certification approach. The metrics currently used in the certification process are those associated with development processes. New metrics are needed to assess both the efficiency and effectiveness of the new certification process.

The main prerequisite for achieving the level of transparency expected for safety-critical systems is then to answer the following questions: (1) What information is required by each stakeholder to achieve the required level of transparency and trust? (2) What is the best way to represent such information given the existing standards, practices, and technologies?

D. Lack of openness to innovation and new approaches

Standards and certification regimes play a major role in establishing and strengthening safety assurance processes in companies. However, the need to conform to a standard or obtain certification imposes unavoidable costs on a development organization. Standards tend to be slow-moving and conservative, and can be a barrier to innovation in both system design and in methods for assurance.

Indeed, when a safety-critical application and accompanying evidence is complete, evolutions to the software often become costly because they entail regenerating the entire evidence-set. How should the modified system be recertified as fit for service? A modified software-intensive embedded system is a new system, and local changes may affect the behaviour of unmodified parts of the system, through interactions with the modified code or even as a result of recompilation of unmodified code. The evidence for safety should therefore be re-examined whenever the system is modified and, if the evidence is no longer compelling, new evidence of safety should be generated and the safety case amended to reflect the changes. Recertifying embedded systems to meet even existing safety criteria is thus difficult and costly.

As a result, when an embedded system or subsystem receives the certification stamp, subsequent modifications are avoided. The effect in highly regulated domains (e.g., avionics) is that software either does not evolve or will do with difficulty as changes invalidate previous certification activities. In less-regulated domains (e.g., automotive), this can cause (authorized) developers to postpone or even renounce standard compliance. The process of re-certification of a previously certified system after modification (we can call it delta-certification) shall be clearly addressed by new approaches centred on certification and system evolution.

III. Directions

As an answer to the challenges identified in the previous section, we describe five technical objectives tackled by the OPENCOSS project.

A. Common Certification Language

The main enabler to improve mutual recognition agreement of safety approvals and to share abstract notions from different industrial markets is to define a common and industry-accepted "certification language". OPENCOSS aims at defining a Common Certification Language (CCL) to help reconcile two different views and conceptual approaches of the certification problem:

- The *safety case-based approach*, which promotes safety certification as a judgment based on a body of material that, explicitly, should consist of three elements: claims, evidence, and argument [5] [4]. The claims identify the adverse consequences to be considered and the degree of risk considered tolerable. Evidence comprises the results of analyses, reviews, and tests. The argument makes the case, based on the evidence, that the claims are satisfied. Specific safety-specific models are GSN [3], CAE [4], SACM [8], and Toulmin [9].
- The *standard-based approach.* The rationale behind certification standards is that the use of standard processes and compliance with predetermined objectives help avoid the common pitfalls of software development. The standard-driven way of ensuring

> quality is by imposing a level of rigor in the processes and workflows used to build the final system and by specifying the intermediate artefacts to be produced (requirements, specifications, test plans, etc.), the kinds of reviews, and analyses that should be performed, and the documentation that should record all of these. In the standards-based approach, the claims and the argument are largely implicit [2].

CCL shall provide a common language for these different approaches, where one specification in a given model can be expressed in the other. The goal is to provide a structured way for argumentative reasoning about safety requirements and constraints across multiple schemes. For instance, in the area of source code structural coverage, a clear uniform set of definitions have to be used. The MC/DC criterion used by ISO 26262 should be the same as the one proposed by DO178B/C.

CCL shall be implemented as a structured semi-formal domain-specific modelling language (DSML), which will act like a template or meta-model for safety certification specification. Using a common conceptual framework for different certification standards will also enable management of claims, evidences, and arguments in a common format, sharing patterns of certification assessment, and cost-effective re-certification between different standards. CCL and domain specific libraries shall be used to build a set of guidelines akin to “spell-checking”, in which a number of compliance checks are performed to assess the degree of compliance of embedded system products against safety-related standards.

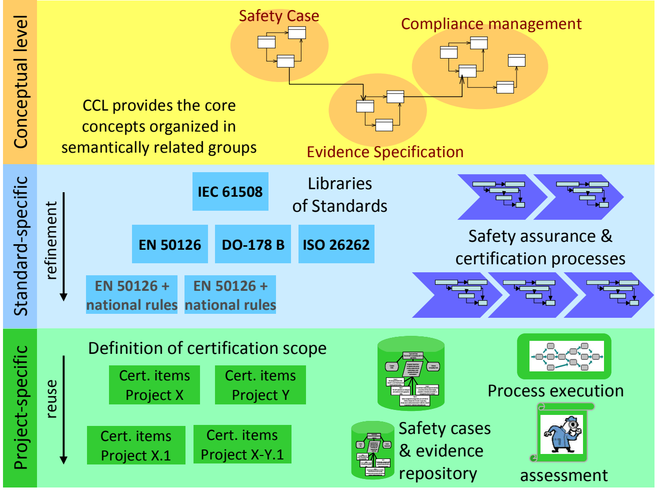

Fig. 1 - Layered approach based on the Common Certification Language

One major challenge for CCL is how to derive specific solutions from the general case in relation to the wide variety, partial inconsistency, semantic discrepancy and various “national flavours” of the existing standards across the avionics, railway, and automotive domains. As illustrated in Fig. 1, the proposed approach will follow a layered strategy to manage complexity. CCL shall identify shared safety principles and concepts as an "intersection set" of safety principles from different standards. This becomes the first layer, so called conceptual level. The second layer uses the CCL to build domain-specific libraries of certification models, which will act as a knowledge database, providing information about safety-related standards (e.g., EN50126, ISO 26262, DO-178 B/C). Any generic product could be first assessed against these libraries. Further standard library refinements enable more specific requirements, considering application domains and then even national aspects. Of course, the "cross acceptance" of the first layers is also a legal issue, OPENCOSS shall start from the technical point of view and point out some normative issue that should be addressed for making practicable in the actual regulatory schemes. The next layer defines project-specific certification activities, both from the process and the product-centric safety assurance perspectives. A new layer of reuse appears which is based on a compositional certification approach and a traceable evidential repository, as described below.

B. Compositional Certification

OPENCOSS shall rely on a compositional/contract-based certification approach. Understanding software safety demands a system-level perspective, in which the software is viewed as one component of many, working in concert with other components to achieve the desired mission. The key point is to understand how to capture each component’s contract and how to propagate the contracts for certification acceptance by other components.

In this approach, we plan to use safety case modules as basic composable specification. Each safety case module in an integrated system safety case and the associated system architecture produces and consumes a set of commitments. A commitment is an assumption, configuration, functional feature, or limitation (performance or behavioural), which is provided by a module [12]. The set of commitments for a given safety case can be identified as its contract. These commitments are also sometimes described as pre and post conditions. To use and ultimately approve or certify a module, the designer must be informed and have the ability to assess all the other modules in the system to determine if the module is consuming a commitment from another module or component.

The main principles of the approach are [13]:

- A change to a design element (e.g., component, RTOS) should only affect the corresponding safety case module, and not impact the entire safety argument.
- Safety case modules can be composed together if: (a) their Goals match and (b) their Context is compatible.
- Results can be recorded in a safety case contract.
- Establish a defined record of the inter safety case agreement.
- Change scenarios include: hardware vendor change, addition of a single application, addition of extra processing nodes, change of data bus.

The challenge in such systems is to assess not only the certifiability of each component or module, but also its certifiability once it is in an ‘integrated’ state. This is in line with the direction of SEooC introduced in ISO 26262. For example, if the safety argument relies, in part, on reasoning about the properties of subsystems/components, then the system build process should ensure that the system has been built out of the specific versions of each component for which there is evidence that the component has the necessary properties. Each step in developing the software needs to preserve the chain of evidence on which the argument that the resulting system is safe will be based. The mean to transfer a common frame for functional and design characteristics of a component from provider to integrator for the compatibility/gap analysis would bring a big benefit to the embedded system community for sharing components and increasing the safety by the broad service history.

C. Evolutionary Evidential Chain

OPENCOSS aims at defining an evolutionary evidential approach that will help having certification evidence readily available and up-to-date via safety certification management tools.

Traditional development processes follow a V-Model with system integration at the end of the project, and have the certification activities carried out as a separate activity. This approach is simply no longer viable for those aiming to develop evolvable and certifiable systems and is quite unrealistic even in more traditional approaches, where a set of iterations of the V-Model is normal procedure. A way to deal with this issue is to follow an evolutionary approach for certification, instead of separate and stand-alone after-the-fact procedures on final embedded system products. But in practice, at least with today’s technology, the costs of doing so would be high, and it will be impractical if we do not preserve the chain of evidence on which the safety arguments will be based.

The approach we intend to take in the OPENCOSS project for specification, collection, and management of safety evidence information is as follows. Using the common certification language described above, we provide precise specifications of the contents of safety standards by capturing the core concepts in the standards and the relations among these concepts. Such specifications will define, in a systematic way, the information requirements to demonstrate both compliance with the standards and to ensure that the safety chain of evidence is preserved.

Furthermore, the specification of evidence requirements for a standard, once tailored to a particular context of application, can be used to construct an evidence repository. Such a repository will store the development artefacts, process knowledge, hazard analysis data, safety audits, certificates, etc. This repository can be queried automatically for extracting the desired safety-relevant information and report generation. More importantly, the repository will provide a basis for managing the consistency of the evidence as the evidence evolves and for performing change impact analysis. We are going to take a number of steps to effectively handle the changes made to safety evidence: First, we will study and classify the various ways in which safety information can be manipulated within the constraints stipulated in the existing safety standards. We then use this classification for characterizing the potential side effects that each type of manipulation can have on the overall consistency of the safety evidence. Subsequently, we will define and compute minimal inspection plans for reviewing the potential side effects and dealing with any inconsistencies caused by a change. By following these steps, the safety engineers will be able to efficiently evolve the evidence repository.

D. Transparent Certification Process

The lack of performance metrics and certification efficiency and effectiveness estimations limits the capability to assess long-term costs, savings and benefits associated with safety-critical system development and subsequent recertification activities. OPENCOSS aims at tackling this limitation by providing the necessary infrastructure to follow a transparent certification process. The principle is to make the certification process explicit and interwoven with the development process, although highly independent and unconditioned from it. An explicit certification process will enable to produce specific metrics for safety-assurance and certification processes.

Such an infrastructure also intends to provide stakeholders (including customers and users) with information about the safety assessment process (e.g., times to carry out V&V (Validation & Verification) and certification tasks) and the assurance artefacts themselves (e.g., claims, arguments and evidence) as a way to improve credibility. It should address consistently potential cost savings achievable from re-use of previous certifications. For instance, compositional certification can improve re-certification over the total lifespan. On the other hand, a monolithic set of data may be cheaper upfront, but much more costly in the long term.

One possible approach to improving the transparency of the safety assurance and certification process is through the creation of certificates associated with the development artefacts [5]. A development or safety assurance team could benefit from a certificate management system to gather evidence in the form of log files, written documentation, information in team management software, or using means to record safety assurance metrics (efforts, costs, etc.). This certificate management infrastructure must provide an interface and infrastructure to create, maintain, and analyze software certificates. A certificate is a record of a safety assurance practice employed by developers and can be used to support traceability between code and the evidence of the safety assurance technique used. OPENCOSS devises a services platform for safety certificates life cycle (creation, configuration, validation, etc.), integration of evidence items with development and safety assurance tools (requirement specification, design, code generation, safety analysis, testing, etc), integration and management of metrics.

E. Compliance-Aware Development Process

Addressing the development workflow is one of the objectives of the OPENCOSS project. Cost-efficient system certification demands a continuous compliance-checking process by enhancing integration of certification goals and development workflow. The goal is to allow developers to assess where they are with respect to their duties to conform to safety practices and standards, and still to motivate them to see the effective progress of the work and level of compliance.

OPENCOSS aims at introducing an infrastructure to help keep certification evidence up-to-date. Such an infrastructure and the associated tooling will allow for faster certification by automating many of the laborious activities required for certification. From a process workflow standpoint, one can infer a temporal and causal dependency between processes, activities and artefacts. For example, editing a requirement shall always precede the verification of that requirement, and the production of the document containing the list of requirements shall always follow the editing and verification of requirements. It is thus possible to infer a set of rules which can be used to check automatically that the workflow has been followed and provide evidence of the level of compliance against safety assurance practices.

This is one field where agile approaches can be used. The question is on how we integrate agile approaches into the current standard-based approaches used in a critical system development. Agile processes when applied with rigour and discipline are not in contradiction with the goal of assuring safety [10]. On the contrary, a highly iterative process assuring at each step ("sprint", in agile terms) assuring safety may combine the benefits of an incremental approach with the rigour of a safety assessment. It is a challenge that the OPENCOSS project intends to tackle. The project will define common processes enabling partial automation of the certification across organisations, taking into account business constraints of the stakeholders participating in these processes.

IV. CONCLUSIONS

As we explained in the previous section, we have identified five key directions on evolutionary certification, which we believe constitute the essential ingredients in the engineering of future safety-critical systems. We can summarize them into two tangible expected results:

- A comprehensive *conceptual certification framework* for safety case creation, monitoring, assessment, maintenance, and evolution.
- An intelligent, automated, and highly customizable *safety certification management infrastructure* in support of the development processes and existing development and safety assurance tools.

The conceptual certification framework consists of (a) a common certification language to enable for certification items management in a common format, certification evidence management, certification assessment, and re-certification between different standards; and (b) a compositional certification method concretized in the form of a set of generic compositional certification rules. This method shall provide the composability rules of pre-certified blocks, for a systems-level certification composed of application components/systems with heterogeneous criticality.

The safety certificate management infrastructure shall maintain an evolutionary evidential chain linked to certification requirements, claims and arguments. In addition, the infrastructure shall provide a set of services to specify, enact, and deploy transparent certification processes interwoven (although independent) with development processes, as well as a set of configurable metrics to make the assurance and certification process available to selected stakeholders.

The OPENCOSS platform is planned to be realized as an industry-validated proof of concept of the abovementioned objectives. The project consortium will leave its further development and maintenance to a proper open-source community.

ACKNOWLEDGMENT

This paper's underlying vision has been extensively discussed in a series of meetings and extensive exchanges over a period of a year with participants of the OPENCOSS project.

REFERENCES

[1] Book: Software for Dependable Systems: Sufficient Evidence?, Daniel Jackson et al., Committee on Certifiably Dependable Software Systems, National Research Council, USA.

[2] Formalism in Safety Cases, John Rushby, Proceedings of the Eighteenth Safety-Critical Systems Symposium 2010.

[3] T. Kelly and R. Weaver. The Goal Structuring Notation: A safety argument notation. In Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, 2004.

[4] Adelard's ASCE. http://www.adelard.com/web/hnav/ASCE/, last accessed: Jan 2011

[5] E. Denney and B. Fischer. Software Certification and Software Certificate Management Systems. In Proceedings of 2005 ASE Workshop on Software Certificate Management, 2005.

[6] Preliminary Recommendation on the 1st set of Common Safety Methods (CSM), Issue 4.0, June 2007, European Railway Agency, to be published as Recommendation on the 1st set of Common Safety Methods

[7] Flanders' Drive ASIL project. http://www.flandersdrive.be/, last accessed: Jan 2011.

[8] OMG's Structured Assurance Case Metamodel. http://www.omg.org/technology/documents/modernization_spec_catalog.htm, last accessed: Jan 2011.

[9] Toulmin, Stephen. The Uses of Argument. Cambridge: University Press, 1958.

[10] R.F. Paige, R. Charalambous, X. Ge and P.J. Brooke. Towards Agile Development of High-Integrity Systems, in Proc. 27th International Conference on Computer Safety, Reliability and Security (SAFECOMP) 2008, LNCS, Springer-Verlag, Newcastle, UK, September 2008.

[11] Northrop, Linda, et al., "Ultra-Large-Scale Systems: The Software Challenge of the Future", Carnegie Mellon Software Engineering Institute, Ultra-Large-Scale Systems Study Report (2006).

[12] G. Despotou, M. Bennett, T. Kelly, "Evaluation and Integration of COTS in Evidence based Assurance Frameworks in Proceedings of 18th Safety Critical Systems Symposium (SSS'10), February 2010 (Proceedings published by Springer).

[13] G. Despotou, T. Kelly, "Investigating the Use of Argument Modularity to Optimise Through-life System Safety Assurance", In proceedings of the 3rd IET International Conference on System Safety (ICSS) 2008, 20-22 October 2008, NEC, Birmingham, U.K.