Position Paper

October 5-6, National Workshop on Aviation Software Systems: Design for Certifiably Dependable Systems

Scott Beecher
&
Jim Krodel
Pratt & Whitney Aircraft

August 31, 2006

Background / Topic

Certification is a process by which an assessment can be made as to the acceptability of a system in a particular domain. Various domains (aerospace, automotive, medical, nuclear, etc.) have an assortment of certification criteria. Systems containing software and associated components can assume various levels of risk, yet a predominate attribute of many 'certification' domains is safety and the associated costs vs. testing these safety attributes. Current safety practices include basic hazard analysis, fault tree analysis and failure mode accommodations which are used to develop a set of requirements and criteria necessary for the development and deployment of a safe system.

A rapidly growing trend in embedded software systems in safety critical domains is to develop highly integrated systems with a multitude of hardware and software of components or modules. In question is not only the pedigree of these components/modules but also their intrinsic architecture. The certification or approval processes applied today to highly integrated systems may not be sufficient since they fundamentally and overwhelmingly inspect and verify results to requirements and as such can break down from a both a certification and business perspective. Other approaches to certification for these highly integrated systems must be considered.

Important Challenges

Each component in an integrated, composable or networked system and the associated system architecture produces and consumes a set of commitments. A commitment is an assumption, configuration, functional feature, or limitation (performance or behavioral), which is provided by a component or module. The set of commitments for a given component can be identified as its system contract. To use and ultimately approve or certify a component or module, the designer must be informed (to some degree) and have the ability to assess all the other components or modules in the system to determine if the module is consuming a commitment from another module or component. The system's component contracts must be shared with all other system components, understood and accepted or "signed". Likewise, it must produce and establish its own set of commitment expectations, which this contract is then shared and must be accepted by other modules and components. The challenge of 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.

An approach to address this issue in complex systems is to understand how to capture each component's contract and how to circulate the contracts for acceptance by other components. A further challenge is the identification of the necessary contractual information and how it is captured.

Important Information Technology Research Needs

1. The certification of highly composable, integrated embedded systems should include a method of authentication for the consumer of commitments and the producer of commitments necessary for an effective system development and fabrication. This may come in the form of property or commitment traceability and how the system integrator designer can establish and trace the necessary commitments for proper certification. Research is further needed to determine an acceptable system response to components that break their contract.

2. With increasing complexity stemming from integrating such systems the module and component developer as well as the system integrator can longer develop systems utilizing today's rudimentary tools and analyses. Developers must increasingly rely on a suite of support tools. Recent studies have shown the benefits of such model driven engineering tools (e.g. domain-specific modeling languages). For very large systems, the developers and integrators can be stymied by the large set of commitments to be observed while developing such systems. These contracts become immense and in their "small print" they cover spatial, temporal, performance and behavioral aspects as well as asset management. Therefore, a heavy reliance on the pedigree and confidence in the tool occurs (i.e. the tool suite can be viewed as a virtual developer).

System certification can be viewed as both process and product based and the determination of the acceptability of the system in a certification sense must now consider the virtual developer in the form of tools. This requires a set of tools that have a known pedigree. As such, the certification reliance of tools used in the synthesis of highly integrated systems must be studied. Simultaneously a mechanism is needed for accommodating changes in the safety assessment during synthesis of the system as the system grows by adding features or functionality.

As a result, an approach for an incremental approval process towards certification is needed. Incremental methods may be an application for formal or object-oriented methods in this area.

Possible Roadmap (5-10 years)

Changes in product certification are typically lethargic. Domains with successful certification practices are reluctant to change for obvious reasons, yet large complex composable embedded systems will continue to be a challenge for certification authorities. Certification requirements that do not evolve with the technology effectively block the use of these effective and powerful systems. One approach would be to provide a high confidence method of reliance on tool pedigree, followed by a composable certification approach supported by tools certified with such a pedigree. The tool certification approach must include an understanding of how to manage component commitments or contracts.

Near term research in ‘trusted tools’ used for development of certifiable highly composable embedded systems is needed. A determination as the necessary criteria of tool acceptability and completeness of commitment coverage is needed.

Longer-term research is needed to develop a ‘certification by development method’ technique. That is, new embedded software development methods are needed whereby the resultant system has a known certification pedigree due to the system composition method used. We need to know not only how to develop such an approach, but in parallel we need to develop a method by which certification authorities can accept certain certification credit from the composition method used.

Biography:
Scott Beecher – Embedded Software Engineer, Pratt & Whitney Jet Engines

Mr. Beecher has over 25 years of experience in embedded aerospace software systems development.

Currently Mr. Beecher is a candidate for FAA designated engineering representative (DER) and is project lead for F100 engine embedded control and diagnostic software as well as various ground support maintenance systems for both commercial and military applications. Mr. Beecher has been involved with the Pratt & Whitney SEPG, CMMI assessments and has taught various college computer science classes. He is currently on the advisory board to the University of Connecticut’s Computer Science and Engineering department and is a member of RTCA’s special committee 205.

He holds a B.S. in Computer Science Engineering from the University of Connecticut and a Masters in Computer Science and in Business Management from Rensselaer Polytechnic Institute.

Contact Details
Speaker:
Scott Beecher, Embedded Software Engineer, candidate DER
Controls and Diagnostics Systems
Pratt & Whitney Aircraft
MS-182-22
400 Main Street
East Hartford, CT 06108 USA
1-860-565-7022 voice
1-860-755-6012 fax
scott.beecher@pw.utc.com

Jim Krodel – Fellow Control Systems Verification and Validation, Pratt & Whitney Jet Engines

Mr. Krodel has over 30 years of experience in the aerospace software domain. He has held several technical and managerial positions in software development of embedded systems including software for the full authority digital electronic engine control (FADEC) for the Pratt & Whitney PW4084 jet engine propulsion system on the Boeing 777 aircraft. Jim is a Designated Engineering Representative (DER) for software recently has conducted several studies relating to COTS software in the integrated avionics domain.

Jim is currently chairman of RTCA's special committee 205, which is amending the RTCA;s DO-178B "Software Considerations in Airborne Systems and Equipment Certification" which is recognized by the FAA as an acceptable means for certifying systems with software.

He holds a Masters in Computer Science from the University of Connecticut and has been a research affiliate lecturer on systems and software development in aerospace systems at the Massachusetts Institute of Technology, Cambridge, MA

Contact Details

Speaker:
Jim Krodel, Fellow Control Systems Verification and Validation, DER
Controls and Diagnostics Systems
Pratt & Whitney Aircraft
MS-162-44
400 Main St.
East Hartford, CT 06108 USA
1-860-565-8886 voice
1-860-622-3065 fax
james.krodel@pw.utc.com