# Wanted: A Systems View on Certification

Jayakanth Srinivasan, Ricardo Valerdi, Kristina Lundqvist
Massachusetts Institute of Technology

A number of panel studies have addressed the software aspects of certification for aerospace systems. These studies have highlighted the limitations of the current paradigm of certifying the development process[1] in creating dependable products. Additionally, this approach does not translate effectively in a systems-of-systems environment. While the need to develop more efficient processes for complex systems has been recognized as a national priority[2], product and performance-based certification approaches remain unproven, and have received little research attention. The problems associated with certification arise from an intertwining of technology, policy, and personnel factors.

The core technologies for the development of hardware and software are evolving at a much faster rate than the current technology refresh cycle of aerospace systems. As the technology becomes obsolete, so does the policy associated for certifying it. Additionally, the knowledge gap between what policy makers know and what they need to know in order to be both efficient and effective widens. The current certification standards are either ambiguous (as is the case of DO-178B[3]) or have been voided (as in the case of military standards like DoD-STD-2167). We believe that a long term solution can only be found by taking a systems view of the problem, and addressing technology, policy and personnel issues in parallel.

**Challenge 1: Matching technology refresh rate to the rate of evolution**

Giant strides have been made in the technology and processes associated with the development of hardware and software. In the case of software, agile development approaches provide a means of rapidly and incrementally delivering working software in an environment of unstable requirements. Agile approaches have been used largely in non-mission critical applications. The question is on how we integrate agile approaches into the current plan-based approaches used in a mission critical environment. A corollary to managing agile development revolves around how we apply these approaches to carry out certification effectively in an incremental development model. Hardware-Software codesign approaches now provide us with the added flexibility of implementing traditional software components in hardware. Do we treat these components as software or hardware? The preliminary response[4] to this challenge in the form of a position paper, by the Certification Authorities Software Team has raised more interesting questions.

---

[1] Computer Science and Telecommunications Board, "Summary of a Workshop on Software Certification and Dependability", National Academies Press, October 2004.
[2] National Research Council, "Decadal Survey of Civil Aeronautics: Foundation for the Future", National Academies Press, June 2006
[3] Hayhurst K.J., et.al., "Streamlining Software Aspects of Certification: Report on the SSAC Survey", NASA Technical Report, NASA/TM-1999-209519, August, 1999.
[4] CAST, "Clarifications on the Use of RTCA Document DO-254 and EUROCAE Document ED-80, Design Assurance Guidance For Airborne Electronic Hardware", June 2006.

**Challenge 2: Articulating the value of certification**

The expected value of certification is in providing increased confidence in the fielded system; however, it currently is a necessary "bureaucratic" evil. In order to gain deeper insight we need to accurately assess the cost of certification, as well as to identify the articulated and unarticulated benefits derived from the certification process. 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 certification process. We believe that more research needs to be carried on how value-based methods can be effectively applied.

**Challenge 3: Bridging the growing knowledge gap**

A key challenge facing us today is in educating policy makers on emerging technologies and enabling them to create more effective guidance for certification. In parallel, undergraduate and graduate students have to be trained in both the software and system aspects of development.

Given the research funding for software engineering has remained relatively stable, or declined[5], to support a rigorous research program addressing all three issues, increased funding is essential. The research will have to be a collaborative project involving government, industry and academia, to get a balanced view of all stakeholder needs.

The five year roadmap that we see is detailed below:

Year 1: Develop a value stream map of the certification process. Gather new data on the current state of certification processes to supplement SSAC[3] data. Gather practices from both troubled and successful certification efforts.

Year 2: Focused research on the three areas of value-based metrics, new certification processes, and training needs.

Year 3-4: Pilot value-based certification and develop new training programs and associated academic curricula.

Year 5: Transition learning into policy and practice, through workshops, publications and classroom teaching.

[5] Baldwin K., "NDIA Top 5 Software Issues Workshop Address", August 24, 2006, Slide 2.

**Author Bios:**

Jayakanth “JK” Srinivasan is a Research Associate with the Lean Aerospace Initiative at MIT. He is currently the research lead for the Enterprise Integration enabled by IT cluster, focusing on IT Architectures and Lean Software Development. JK has an undergraduate degree in Computer Engineering and graduate degrees in Avionics and Aeronautics and Astronautics respectively. He can be reached via email (jksrini@mit.edu) or phone (617-253-0672)

Ricardo Valerdi is a Research Associate with the Lean Aerospace Initiative at MIT. He is currently the research lead for the Enterprise Cost and Metrics cluster. Ricardo received his doctoral degree in systems engineering from USC in 2005, where he created for the COSYSMO model for systems engineering cost estimation. He can be reached via email (rvalerdi@mit.edu) or phone (617-253-8583)

Kristina Lundqvist is an Assistant Professor in the Department of Aeronautics and Astronautics at MIT. She currently serves as the Director of the Embedded Systems Laboratory. Her research focuses on the creation of frameworks, tools and processes for the rapid design, development and evolution of dependable software-intensive systems. She can be reached via email (kristina@mit.edu) or phone (617-452-2550)