Position Paper for *National Workshop on Research on Transportation Cyber-Physical Systems: Automotive, Aviation, and Rail*
Chuck Howell, the MITRE Corporation, 21 October 2008

Among the many important issues that cut across the Automotive, Aviation, and Rail communities is their increasing reliance on Cyber-Physical Systems. The complexity and the consequences of failure of these transportation CPSs are both increasing. What has been clearly articulated for the Aviation goals for NextGen seems to be equally true for Automotive and Rail applications of CPS:

"Certification of software-intensive systems is particularly problematic primarily because of the gaps in our understanding of how to develop complex software systems. As a result of these gaps, certification of such systems today is largely based on adherence to specified processes, rather than on a systematic evaluation of the safety and quality of the systems themselves. This process-based approach to certification is likely a primary reason for excessive costs and time. An effective program must have as one of its primary goals the replacement of the process-based approach with approaches based on a systematic evaluation of the systems themselves."
"Visions of Automation and Realities of Certification", Hayhurst and Holloway, AIAA 5th Aviation, Technology, Integration, and Operations Conference 26-29 September 2005

Current tools and techniques for assuring and certifying software simply do not work for the complex mix of evolving ground and air safety-critical systems of systems anticipated for NextGen. As decision making is delegated increasingly to software (i.e., the software is increasingly autonomous), and as operational goals for NextGen rely on increased roles for software, dramatically improved effectiveness and efficiency of assurance techniques is an essential enabler that must be developed, demonstrated, and deployed. This is an important component of a research agenda for NextGen, and is recognized in the Aviation community as a broader concern that presents an opportunity for collaboration. This is called out explicitly in a 17 September 2008 response from the FAA to recommendations of the FAA Research, Engineering, and Development Advisory Committee (REDAC). The response cites an excerpt from the REDAC recommendations and then provides the FAA response:

<u>High Confidence Software Development Strategy</u>
There is an increasing reliance on software based system for high criticality applications both in aircraft systems and in ATC systems. The current software development and maintenance processes are cumbersome, expensive and incomplete. The FAA is not unique in this regard as other federal agencies and industries struggle with issues of software criticality. The REDAC suggests that this be a priority area both for FAA internal development and for inter-agency coordination.

<u>FAA Response</u>
We agree with the assessment of the REDAC of the importance of a software based system both in aircraft systems and in Air Traffic Management (ATM) systems. We also agree that the development of a strategy across the appropriate Government agencies is important and we will work with the appropriate Government agencies to develop a Government R&D strategy for high confidence software development and ensure high level internal support for the resulting strategy.

There are of course a range of topics that are important in a research agenda to support high confidence software development in critical transportation CPSs. For this workshop, I would like to suggest one issue of importance that could be a fruitful topic: the development and especially the review of assurance cases for these critical software intensive systems. Without adequate assurance (e.g., regulatory confidence that the risks of approving a system for deployment or sale are understood and acceptable), the adoption of the required CPSs will be crippled or stymied completely. Of course, if the measures required to acquire needed assurance are so burdensome as to effectively prohibit adoption of a CPS, it has the same effect. There is much research to be done to provide a clear pathway for effective and efficient assurance frameworks for transportation CPS.

The specific aspect I would suggest as a topic for the workshop is a focus on the review of interim and final assurance cases developed for a critical CPS. Currently the review of a safety case is largely handled as a document review: a team of experts reads a technical document, makes judgments about compliance with relevant standards and requirements, notes defects and gaps, may meet to consolidate comments, and provides the comments back to the "authors". This is essentially a peer review of a technical document. In order to elevate the efficiency and effectiveness of assurance case reviews, the assurance cases must be treated as "engineering artifacts", subject to rigor and disciplined technical scrutiny. There has been a little research in tools, notations, and techniques to support rigor and scrutiny in the review of assurance cases. For example, in the MITRE research on this topic that has just begun, we are focused on three aspects:

- extensive structural consistency checks for dependability cases (i.e., that they are well formed, rather than treating as just a volume of technical prose);
- incremental and role based team review of dependability cases, building on existing work in e.g., Phased Inspections (UVA) and Perspective Based Review (UMD);
- annotations to extend the natural language content of dependability cases, and the addition of checking rules to automatically ensure consistency with the annotations.

I would like to discuss the research that has been done at various institutions and prompt a discussion of what aspects of this challenge belong in a broader research agenda for assurance in CPS. Thanks for considering this topic.

Author Background

I'm Chief Engineer of the Domestic Security Division at the MITRE Corporation, and Principal Investigator of a MITRE Sponsored Research project on "Assurance for NextGen Software-Intensive Systems". My interests include techniques to calibrate and reduce residual doubt about the behavior of critical software intensive systems, and approaches to making large scale systems more robust (i.e., less fragile). I have participated on or led a broad range of Red Teams, Integrated Product Teams, and Independent Executive Review Teams for, among others, the ODNI Intelligence Collection and Requirements System, the Army's Maneuver Control System, real-time fault recovery in AWACS, the Seawolf Ship Control System, NASA Shuttle Flight Planning Software, software contributions to risk of inadvertent launch for the Missile Defense Agency, and the V22 Osprey Flight Management System. I was the MITRE Corporate representative on the IEEE Software Engineering Body of Knowledge Industrial Advisory Board. I was an invited presenter at a workshop organized by the National Academies of Science study of Certifiably Dependable Software and an invited participant at a workshop on Trustworthy Computing at the Naval Postgraduate School. I co-chaired the First Annual Assurance Case Workshop in Florence, Italy in 2004.

Contact information:
Charles Howell,
The MITRE Corporation, M/S T260
7515 Colshire Drive, McLean, VA 22102-7508
(703) 983-7615 / (703) 983-1405 (fax) / howell@mitre.org