



Software Engineering Collaborator's Information Exchange (SECIE)

January 19, 2010, 11 am - Noon EST

Structured Assurance

T. Scott Ankrum

Senior Software System Engineer, MITRE Corporation

Dr. Alfred Kromholz

Software Engineering Center, MITRE Corporation

Abstract:

For safety-, mission-, or security-critical systems, there are typically regulations or acquisition guidelines requiring a documented body of evidence to provide a compelling justification that the system satisfies specified critical properties. Current frameworks suggest the detailed outline of the final product but leave the truly meaningful and challenging aspects of arguing assurance to the developers and reviewers.

We began with two major hypotheses. We selected a software notation suitable for building structured safety cases and applied it to three disparate assurance standards. Each of the three standard mapping efforts is discussed, along with the problems we encountered. In addition to the standards, we used the notation to structure an assurance case for a practical security-critical system, and we describe the lessons learned from that experience. We conclude with practical options for using our mappings of the standards, including a methodology for attaining high assurance levels based on an extension of the familiar V-chart structure, and how well our initial hypotheses are borne out by the project.

Bio

T. Scott Ankrum has been a project manager, software designer and developer and has over 30 years of experience in many aspects of computing, from mainframe systems to distributed systems development and client/server design. He has managed projects and led development teams, and has been personally involved in software development from requirements definition to final testing. Mr. Ankrum is Senior Software System Engineer at the MITRE Corporation, working in software development process improvement and requirements management, and where he led the Assurance Frameworks research task. He holds a B.S. degree in Computer Science from American University and a Master of Software Engineering degree from the University of Maryland. He is a member of the Association for Computing Machinery (ACM), the IEEE Computer Society, and a senior member of the American Society for Quality (ASQ). He is currently the chairman of the local ASQ Software SIG.

Alfred Kromholz received a Bachelor of Electrical Engineering from Cornell University, with a side concentration in European languages and literature. After working for several years on the Apollo program, he went on to a master's degree in Classics and a PhD in ancient culture, both involving extensive computational analysis. After spending a dozen years in the Near East combining work in computers and anthropology, he returned to the US to join the space station program, where he focused on systems integration, interactions of technology and society, and organizational culture change.

Dr. Kromholz has been with MITRE's Software Engineering Center for 10 years, during which he has worked in a wide range of areas, including both civilian sector (IRS, Department of Homeland Security, Department of Energy) and DoD (DISA, Defense Logistics Agency, Army and Navy/Marine Corps). His efforts tend to concentrate on program infrastructure and organizational improvement- change and configuration management, quality assurance, requirements management, the "ilities" - and on optimizing relationships among products, processes, and, above all, people.