So, how should we determine the LOR? Gill said, "There is not a one-size-fits-all solution." Because each system is unique, there will always be a need to tailor the LOR process. Sometimes, there are valid reasons for a system to not follow common processes and standards because in the tailoring process, some steps may not apply and accepted alternatives may be used in their place. Subsequently, there will also be thresholds associated with criticality and LOR because of the signature authority associated with a system or program. In any case, the process must result in a balance between technical risk and cost, and schedule risk. A good place to begin the LOR process is with functional hazard analysis (FHA), failure modes and effects criticality analyses (FMECA) and other safety analyses.
ISSC 2009 Recaps

A Summary of the Levels of Rigor Workshop from the ISSC 2009

by Jeffrey Richards

Dr. Janet Gill and Josh McNeil, Presenters

Pages 1 | 2

McNeil continued the workshop by discussing some of the standards that are available for safety professionals to use on their programs. Some are required and some are suggested as guidance depending on the SOW. He also discussed how to handle previously developed (legacy) systems. McNeil pointed out that “there is give and take but, ultimately, the SSWG has to determine what is best for their program.” Gill added that the safety lead must be aware that “mitigation by expert opinion is not acceptable and proper evidence should always exist when making decisions.”

McNeil went on to say that “sometimes requirements cannot be properly tested, and those requirements need to be really scrutinized by a larger group of experts — you cannot test safety into a system.” Although testing does provide evidence and does exercise the software to help identify problems, there still needs to be a level of confidence based on development. “CMMI certifications do buy some credibility, but certifications alone cannot guarantee properly developed and tested software,” McNeil said.

According to McNeil, the use of safety cases is a technique that can aid safety professionals with their analysis of the system. They are widely used in Europe and can provide a firm foundation of evidence. McNeil said, “Safety cases may be a process that will need to be adopted for future systems developed in the U.S.” The safety professional must determine the safety arguments of the system and build a case similar to one that would be presented in a court of law. Safety cases can be started using documents that may already exist such as the safety assessment report (SAR).

Gill and McNeil concluded the workshop by emphasizing that standards may require four LOR categories, but there will always be exceptions to the rule because each system is unique. The safety engineer and SSWG must be vigilant and obtain as much evidence as possible when assessing criticality and then applying the appropriate LOR.

About The Author

Jeffrey Lee Richards is a software safety engineer APT Research, Inc. in Huntsville, Alabama. He received his Bachelor of Science degree from the University of North Alabama in computer science with a minor in mathematics. He has more than 10 years experience in software that includes embedded, desktop application and Web application development. Richards is currently providing software and software safety support to the PEO Aviation office through the Software Engineering Directorate (SED). He can be reached at jrichards@apt-research.com.

For more information about the ISSC 2009, including technical summaries, speaker bios and a photo slideshow, please visit http://www.system-safety.org/~issc2009/index.html.