Standards roulette: which one to use for safety-critical software and hardware development?

By TAMMY REEVE, Founder & CEO of Patmos Engineering Services, Inc and Airworthiness Certification Services LLCs. For more details about her, read "About the author" on the last page of this article.

For this year's Aerotech 2023 in March, I will be presenting on a commercial aerospace FAA and EASA harmonized published guidance for airborne electronic hardware, "What's new with Airborne Hardware Design Assurance for Aviation? Newly released FAA AC20-152A harmonized with EASA."

This presentation focuses on accepted means of compliance to the FAA and EASA certification regulations for commercial aircraft of all sizes, including propulsion. As the title suggests, it will address hardware aspects of these systems performing as intended with a safety-critical level of reliability.

So, what is reliability in a complex custom hardware or software design? How does one measure the error-free nature of a custom design in a field programable gate array (FPGA) or complex software program used in critical functions of aircraft operations? In answer to these questions, many papers have been written.

Government (military and civil) have the responsibility for keeping the public safe and securing our safety. To do so, it relies on

Airbus

Standards cover aircraft from stem to stern, including electronics. Shown is the Airbus A350 XWB cockpit touchscreen.

industry standards to carry out the laws put in place via legislation. Industry standards are written by many organizations, SAE being just one...albeit an important one. ISO, ASTM, IEE, RTCA, and many others use industry experts under working groups to write best practices standards — many times in cooperation with government agencies — to ensure public safety in critical aircraft, automotive, naval, nuclear, medical, and other public services or potential public-impacted areas of life.

Which standard is the one to use? What do you do when there are competing standards for demonstrating reliability of hardware or software aspects of certification of safety-critical systems? Choosing the correct standard for the industry you will be developing for is

important. Most of the regulating industries align themselves with a standard they believe is sufficient for demonstrating the level of rigor (reliability) for the safety-critical systems. So, find out what the industry regulator you will be working with accepts.

For airborne software and hardware, the civil authority is the FAA in the U.S. and EASA in the E.U. Other countries have their own regulating body for airborne civil aircraft. In the U.S., civil avionics related to safety-critical systems are certified under the regulatory laws published in the Code of Federal regulations (CFRs). EASA in the E.U. has similar regulations called certification standards (CS).

Both EASA and the FAA acknowledge industry standards that they consider acceptable means of compliance (MOC) via an Advisory Circular document. AC20-152A/AMC20-152A is currently the document that acknowledges the RTCA standard DO-254 as a MOC for airborne hardware aspects of certification. AC/AMC20-115D acknowledges RTCA standard DO-178C as a MOC for airborne software aspects of certification. Similar ACs/AMCs acknowledge ARP4754A/ARP4761, DO-160G, for environmental testing and systems and safety development.

There are alternative MOC accepted as well, but they require closer interactions and support from the regulating body. This can increase risk, schedule, and costs. It is very important in the civil aviation certification program to read the AC/AMC first before jumping in reading the industry standard. The AC/AMC provides tailoring and is the regulator's opinion on how to use the industry standard for regulatory approval.

To Learn more about the industry standards and use for safety-critical systems for airborne hardware and software, attend AeroTech 2023 and see my presentation. Or, reach out to Tammy@patmos-eng.com for support. ■

S-18 Committee members on the move

The "Move with SAE Mobilus" program recently featured three members of the SAE S-18 Aircraft and System Development and Safety Assessment Committee to talk about, among other things, planned revisions of ARP4754A/ARP4761. The January 18 interview featured with Bob Voros, System Safety Manager at Merlin Labs; Andrew Wallington, Boeing Enterprise Safety & Mission Assurance; and Cory Laflin, Engineering Process Improvement Specialist at Textron Aviation.

About the Author

Tammy Reeve, Founder & CEO of Patmos Engineering Services, Inc. and Airworthiness Certification Services LLCs, is an independent FAA DER and a software and digital hardware engineer who works with companies in safety-critical development, both commercial and military, in meeting design and compliance requirements for the government regulators. She is an active member of SAE and serves on several committees, including AeroTech, WG34 Machine Learning and AI, S-18UAS, RTCA Forum for Aeronautical Software RTCA WG-117 SG-1 Low Risk Software. She is a recipient of the SAE Cordell Breed Award.