FEATURE ARTICLE

WIND RIVER

Software for UAS

Big Changes Lie Ahead

By Chip Downing

Our Unmanned Aircraft Systems (UAS) industry is growing up fast, and, with over 200 UAS projects globally, will prove to be one of the most prolific eras ever for aerospace. As these airborne devices are deployed into defense, commercial, and public safety programs the unit volumes and supporting ground systems will grow by orders of magnitude. However, for this to occur, big changes are needed in one of the most challenging components of a deployed UAS: software. Three aspects of this challenge are:

Safety	Safety certification with the government agencies FAA and EASA
SWaP	Reducing space, weight and power (SWaP) by combining applications from multiple vendors onto shared hardware platforms
Security	Multiplexing multiple levels of classified information, coalition partners, or other domains securely.

Safety

One of the difficult days for traditional R&D engineers working on UAS programs is to find out that the program is so successful that customers want to deploy the system from un-controlled airspace into controlled airspace. Just like commercial manned aircraft today, UAS activities in controlled airspace will need to comply with US Federal Aviation Administration (FAA) and European Aviation Safety Agency (EASA) safety regulations for controlling and separating aircraft, hot air balloons, and other objects, like skydivers, in this shared zone. Current guidelines ask for UAS programs to show an equivalent level of safety to their manned counterparts – but what is an equivalent level of safety?

For software on airborne systems, the global commercial avionics industry has developed a standard known as RTCA DO-178B / EUROCAE ED-12B, with RTCA (www.rtca.org) managing the North American standard, and EUROCAE (www.eurocae.org) managing European standard for software deployed on aircraft flying in «controlled airspace». DO-178B and ED-12B are identical standards, and these standards, currently in their third revision, have an excellent track record for safety. Similarly, airborne hardware systems need to comply with a separate safety specification, RTCA DO-254/EUROCAE ED-80.

All systems on an airborne vehicle do not impact safety equally – some systems, like flight control systems, are quite critical to continued safety of flight. Other components, like cabin lighting systems, may have little or no effect on safety of the entire aircraft. With this in mind, DO-178B created separate safety levels to reflect the relative criticality of an individual system. These range from Level A (highest criticality) to Level E (lowest). Certification authorities set the required level after analyses of safety impact of failure of the systems on the entire aircraft. UAS engineers can then focus on the quality of the most critical systems, and are therefore relieved from the entire Level A certification burden as these levels decrease.

DO-178B software certification packages for COTS components are nontrivial investments, currently averaging $60-100 per line of software code. For example the DO-178B package for the ARINC 653 operating system from Wind River, VxWorks 653, contains more than 65,000 files to support the highest safety certification Level A. Developing this certification evidence cost millions of dollars, and would be cost-prohibitive if borne by a single program. As a COTS component the costs for each program are a fraction of this investment. Further, safety certification officials on many different projects have reviewed this COTS certification package, increasing its inherent quality and reducing risk for all programs.

SWaP

As the demand for more capability increases on individual UAS, the volume of application software increases. This creates a pressure to reduce hardware size, weight, and power (SWaP) and cabling by combining software applications on fewer and smaller hardware platforms. To address this demand, systems integrators are requiring systems suppliers to share computer hardware resources with other vendors on the aircraft. This concept, embodied in the ARINC 653 specification, originally pioneered by Boeing and Honeywell on the Boeing 777, is now a core requirement of almost all new unmanned and manned production aircraft, including the Northrop Grumman X-47B UCAS-D, the European nEUROn UCAS, the Boeing 787, and the Airbus A380, Airbus A400M, and Airbus A330 MRTT aircraft, to name a few.

Sharing hardware resources among different (perhaps competing) software suppliers creates friction in the supply chain. To reduce this friction, the avionics industry created the RTCA DO-297/EUROCAE ED-124 specification that describes the exact roles *application developers*, *platform provider*, and *systems integrator* must each play for clean and safe integration of all of these components. In turn, COTS vendors like Wind River have responded with operating systems such as VxWorks 653 that support *role-based partitioning* of applications during execution and throughout the development lifecycle (debug, test, certification, and later change and recertification).

But, even with the availability of partitioning operating systems and with DO297/ED-124 helping to define the «ground rules» of integrated modular avionics (IMA), moving to this method of sharing hardware resources continues to be a challenge.

Security

In this highly connected, yet vulnerable world, the demand for security is increasing in all systems, especially those that contribute to national defense. This is especially true for unmanned systems, which require very high

functionality in relatively small space and power, and yet must be extremely robust, reliable, and defended against hostile threats, all with very high assurance of security.

As with complex, hardware-constrained *safe* systems that comingle software components with different *safety criticality levels*, complex, hardware-constrained *secure* systems comingle components from different *security domains*.

In the past, system builders used separate hardware elements to create so-called «air gap» security. Now, at the operating system level, the same partitioning approach taken to safely run multiple applications on a single processor is being extended to *securely* run multiple applications from different security domains through an emerging system architecture called *MILS* for *Multiple Independent Levels of Security*.

To show that such systems are highly secure, COTS software vendors use the international security standard *Common Criteria for Information Technology Security Evaluation*, ISO 15408. Like DO-178B safety levels, Common Criteria ranks different security levels, from EAL7 (highest) to EAL1 (lowest). In the United States, Common Criteria is now *required* by the US Department of Defense for COTS components in system requiring information assurance.

The benefits of MILS for implementing highly secure systems are compelling when implemented correctly – dramatically lower development and certification time and cost throughout the lifecycle, and lower system bill-of-material costs through hardware consolidation. Harnessing the power of MILS is a challenge for both software component vendors and systems builders. COTS software component vendors with highly successful DO-178B-certified ARINC 653 avionics platforms are ably positioned to assist defense system builders with this powerful technology.

Putting it all together – Communications and S&A

How will unmanned aircraft systems be able to intermix with the already crowded NAS and show an equivalent level of safety? It will not be with today's technology. Manned flights have managed to remain reasonably safe over the last century by using relatively simple radio communications, and radar in more congested areas, with human oversight. For semi-autonomous and autonomous unmanned flights in the NAS, improvements in communications and sense-and-avoid (S&A) technologies need to be developed and deployed.

Communications

The use of simple radios and radars, human-based separation, and pre-defined airways will not offer the margin of safety required for continued safe mixed manned/unmanned flights in an airspace growing in complexity and congestion. Supplemental communications channels need to be robustly deployed on tomorrow's manned and unmanned aircraft. In addition, these new communications systems must move from traditional federated systems into more compact, ARINC 653 partitioned systems with reduced SWaP. For true communications security, UAS of tomorrow must deploy advanced MILS-based systems to handle the multiple channels of communication and control that will be required to securely enable safe flight in the mixed airspace of tomorrow. And these systems will need to be both DO-178B and Common Criteria-certified at high levels.

S&A – Sense and Avoid

Although «See and Avoid» has successfully served our manned operations in NAS for decades, the mixed airspace of tomorrow will require very accurate, affordable, and widely deployed «Sense and Avoid» (S&A) systems for safe flight in both UAS and also manned systems that are required to avoid the often smaller and harder to see UAS systems.

Although challenging to develop, these systems will prove their value, and will quickly move into the manned marketplace, similar to other navigational aids, as volume and quality increase and prices decrease. However, for these devices to achieve wide acceptance in both manned and unmanned platforms, like communications systems, they need to be certified at the highest levels.

Summary

As UAS mature from exotic to commonplace usage they face significant technological challenges. The safety and security demands of this industry are far above that required of UAS development engineers in the past. Similar to the understanding that evolved from the use and maturation of avionics safety standards, over time the demands for further scrutiny and increased certification complexity will appear. RTCA Special Committee 203 and EUROCAE Working Group 73 are striving to create certification standards for UAS and minimize the immediate safety certification burden for pioneering organizations. However, as time, complexity, incidents, accidents, and this industry evolve, these communication and S&A systems will be forced to increase their criticality levels to a point that may exceed that of manned aircraft. When this evolution occurs, companies supporting this increased rigor will become the true technology leaders for the next generation of manned and unmanned aircraft and safe and secure airspace utilization.

Chip Downing