A look at the ARINC 653 Supplement 3 enhancements to allow for incremental load and certification of payloads

Wilson, A; Parkinson, P; Kinnan, L; Downing, C
Wind River

The ARINC 653 standard has been around for a number of years, going from it's inital release to Supplement 2 enhancements in 2006/2007. The standard has been developed by leading experts in the Aerospace industry including contributions from Airbus and Boieng, culminating in it's adoption in leading edge Aircraft designs such as the Boeing 787 Dreamliner and Airbus A380.

Wind River has been working on a solution with GE Aerospace with the goal of deploying a commercial off the shelfs (COTS) solution for the Aerospace industry for this standard. During this development, the ARINC 653 standard itself not only matured, but led to further research into how to build IMA systems under EUROCAE Working Group 60 (RTCA SC 200).

This resulted in the publication of DO-297 which provides guidelines for an approach to incremental certification, which then led to additional work under ARINC 653 supplement 3. Wind River has been working with GE Aerospace and Boeing on the XML schema and incremental link/load of applications under the ARINC 653 standard with a result of the proposed changes to the ARINC 653 XML schema under Supplement 3.

This presentation will go through the current status of the XML Schema and the proposed modification to the standard in order to follow the guidelines proposed by DO-297, which led to the work on the 787 Dreamliner being able to run multiple applications, linked and loaded individually, at different levels of safety certification, on the same Core Computing Platform.

The core concept of DO-297 is to make sure the IMA Systems development is cleanly separated into well defined roles, namely the Certification Authority, the Certification Applicant, the Systems Integrator, the Platform Provider and the Application Developer. By providing clean roles for each of these phases the IMA system can be built up with a number of components, each tested and certified in isolation before moving to the next phase. This allows applications to be built and tested seperately from each other and from the core computing system. This is critical to allowing not only the appplications providers to be able to work seperately, but to allow application to run at different levels of criticality.

The presentation will include not only the concepts invloved in this role based development, but how these roles effect the development process and tools environment, as well as the resulting runtime components.

It will also look at some of the proposed features in ARINC 653 that would and could be used to benefit space based applications, including incremental load of applications using the partition restart capabilities without having to restart the entire system. This includes the ability to incrementally test, certify, link, load and schedule the application in isolation of the main system, giving huge benefits to system updates and increasing the reliability of the system, and the p[ortability of the application itself across different IMA platforms.