Verocel Continues Involvement in IMA Certification

Integrated Modular Avionic (IMA) systems have become popular with the increase in computing power of modern processors, and there are many types of IMA systems in use today. Verocel continues to play a leadership role in certifying operating systems for IMA implementation, including training courses to assist companies planning to develop and certify IMA-based systems.

One of the motivations for IMA systems is a reduction of space, weight and power (SWaP). Instead of using a dozen individual processing units, each with their cooling and power requirements, a single larger processor can provide a dozen or more virtual boards that can support a dozen or more applications. This is the idea behind virtualization, which has become quite popular in enterprise data centers worldwide.

DO-297 provides development guidance and certification considerations for IMA systems. It describes an operating system that provides virtual processing boards as partitions. If the partitions of an IMA system are robustly partitioned, meaning that if it can be shown that the behavior of one partition cannot adversely affect the behavior of any other partition, then the applications loaded in each partition can be certified independently. Incremental certification provides significant benefits, as the certification evidence for the applications can be assembled as the system is integrated on the aircraft.

Most of the large transport planes use IMA systems and the trend is moving into the smaller aircraft, such as Unmanned Air Systems (UAS). They used to be called Unmanned Air Vehicles but the term has been broadened.

There is a big difference between IMA virtualization and the kind of enterprise virtualization provided by vendors such as VMWare™. A VMWare implementation provides an environment that emulates a complete processor as a virtualized platform. This virtualized platform can support multiple operating systems (e.g., Windows™ and Linux™) simultaneously along with applications that run on each OS. While this type of partitioning system does provide robust partitioning of memory, it strives to maximize throughput and improves average performance rather than providing strict deterministic time partitioning. As a result, these systems are not suitable in the safety-critical domains.

Multiple Independent Layered Security (MILS) provides robust partitioning of space and time, and provides very strict control over shared resources. The purpose of a MILS operating system is to provide very strict control over information flow. Many of the attributes of a robustly partitioned IMA system can be found in a well-implemented MILS system.

Verocel has been involved with IMA systems for many years, initially through membership of the committee that developed DO-297 and ARINC-654, which provides a standard API for an IMA system. Verocel also performed research for the FAA and co-authored a report and guidebook on the certification of an OS for IMA systems.

We are continuing with the certification of a deterministic hypervisor that is able to support robust partitioning, and we are developing certification evidence that will allow a MILS operating system to be used as an IMA platform.

We note the success of IMA systems to date, and foresee continued growth in the adoption of IMA platforms in future designs for safety-critical applications.

Verocel will soon be announcing the availability of a DO-297 course to support those companies that are planning to develop and certify IMA-based systems.