GSAW 2014 Tutorial J:

Secure Cloud Computing for Resilient Ground Systems

Length: Half day

Overview:
Cloud Computing holds many promises for Ground Systems, including the potential to significantly reduce computer hardware and software development time from years/months down to weeks/days and to significantly reduce fielding costs by leveraging proven Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) foundations from major service providers. The ability to rapidly construct or adapt ground system capabilities via Software-as-a-Service (SaaS) may be an important step in moving away from the more rigid or brittle architectures of the past in an effort to field more resilient and adaptable systems in the future. But these promises are clouded (pun intended) by stark realities– are such capabilities sufficiently reliable and trustable, when major portions of the ground systems software and computing infrastructure are provided by commercial companies? Will systems be resilient to real-world conditions? Will overall operational availability be limited by reach-back communication channels? What about Cyber Security, and the threat of attack or information exploitation by global entities via the cloud? For ground systems that must be certified and accredited for information security (e.g. defense, health care, and financial systems), how can assurance be proven when ground systems are reliant on cloud-based services? Can cloud-based ground system components developed by dissimilar organizations for dissimilar operational needs be coordinated in complex System-of-Systems applications, especially those with safety-of-life implications? And perhaps most important of all: is cloud computing effective in ground systems architecture, or is it mostly marketing hype?The tutorial draws from the experience of Network Centric Operations Industry Consortium (NCOIC), which has been examining these topics for a number of critical applications. The NCOIC is a global organization focused on industry neutral approach to adoption of net-enabled capability and system interoperability. It consists of 55+ members/organizations representing 12 countries, operating in a wide range of domains, including Aerospace/Defense, Information Technology and Service Providers, Air Traffic Management and Academia. The Industry/Government partnership provided by the NCOIC is international in scope, with the intent of meeting Customer needs to increase system interoperability and increase value-for-money (e.g. increase the capability of both new and existing systems, lower their cost, keep up with technology and administrative efforts, and reduce risk). The NCOIC also recognizes Industry needs to maintain product lines and grow into new business areas (e.g. keep existing products relevant, acquire new business within core product lines, and acquire entry into new markets).

Instructor: Kenneth Cureton, Network Centric Operations Industry Consortium (NCOIC), University of Southern California

Biography:
Kenneth Cureton is a Technical Council Chairman Emeritus of the Network-Centric Operations Industry Consortium (NCOIC). An active member since 2004, he has served in various technical leadership capacities. Cureton has been actively involved in “voice of industry” design efforts to support the National Geospatial-Intelligence Agency (NGA) Cloud Computing dissemination of geo-spatially tagged data for emergency management systems, the US Federal Aviation Administration (FAA) Next-Generation Air Traffic Management System, the Australia Defence Organization (ADO) Single Integrated Environment, the North Atlantic Treaty Organization (NATO) Allied Mission Network, and other national and international systems. Mr. Cureton is also an Industry Lecturer at the University of Southern California (USC) and currently presents two televised/webcasted Masters-level Engineering classes: SAE 574 (Net-Centric Systems Architecting and Engineering) since 2003, and SAE 550 (Systems Architecting and the Political Process) since 1996.

Description of Intended Students and Prerequisites:
Attendees should be familiar with the general intent and use of various Ground Systems, ideally with experience with their required capabilities and real-world limitations. Some experience in use of software applications on such systems is highly desirable, but detailed hardware/software design experience is not necessary. General familiarity with Cloud Computing principles (for example, from attendance at the morning tutorial) is highly desirable. No specific ground system category is covered, but the assumption is that participants will be more interested in complex, large-scale networked applications rather than stand-alone, single-function systems.

What can Attendees Expect to Learn:
This tutorial explores the need for assured operation and trust in ground systems that leverage cloud computing technology, with specific emphasis on Cyber Security, Resiliency, and Interoperability of ground systems through the cloud. A hand-on workshop exercise is provided to reinforce these concepts and help attendees assess the benefits and risks of applying Cloud Computing in current and future ground systems.