Safety and Security Requirements are Merging for UAS

Imagine the embarrassment of the US Forces when an Unmanned Air System (UAS) was broadcasting video images in Iraq earlier this year. These images were picked up on the ground by someone unknown and broadcast to YouTube. The images could have been very sensitive, and could easily have compromised US troop security. The UAS pictured here, the Fire-Scout, was involved in an incident taking place in the Washington, D.C., airspace.

Another scenario may have been less dramatic but more sensitive and critical if passwords, mission plans, troop positions or other such information had been broadcasted by the UAS or by the Control Segment used to fly the UAS.

Two other instances of UASs misbehaving have been reported within the past year.

- Operators lost the control link with a Northrop Grumman MQ-8B Fire Scout during an Aug. 2 test flight from a Naval Air Station Pawtuxet River, Md., facility. The unmanned aircraft entered National Capital Region airspace. When the Fire Scout was about 40 miles from Washington, D.C., operators shifted to another ground control station and were able to re-establish the control link and direct the aircraft to Webster Field in Maryland. The problem was identified as a "software anomaly," and a modification has been developed to correct the issue.
- In Sept. 2009, an F15 was ordered to shoot down a REAPER UAV that had lost its control link in the south of Afghanistan. All efforts were made to re-establish the link before a decision was made to shoot down the UAV over an unpopulated area prior to it crossing into Tajikistan. The F15 fired on the REAPER and destroyed its engine, however the link was re-established and the controller was able to guide it into a mountain in RAGH District. There were no sensitive items on board the REAPER but it did go down with its ordnance (Hellfire and GBU-12). You never want to shoot down a perfectly functional UAS!

UASs are becoming increasingly more capable, and they must be able to support both safety critical as well as information security requirements. Software developed by many different suppliers is provided to a system integrator that loads and connects the components. While the component developers can ensure the safety and security properties of their own components, the system integrator must construct the system in a way that preserves these properties.

One way that this may be accomplished is to develop a platform that is able to run many applications at different security levels and with different criticality levels, while preserving the properties established. Such a platform has been developed by Wind River and is called the MILS platform (Multiple Independent Levels of Security).

VEROCEL is contributing its software verification expertise to provide evidence for the MILS platform required by the safety and security authorities. There are many certification objectives in the two domains that overlap. The resulting platform may be used in combination with other middleware components to provide the information assurance infrastructure that is able to support both safety and security requirements.

As our systems become more distributed they also become more interconnected. A platform must be able to protect the certification work and enforce its interconnections; this is a vital component in the future of safety critical and secure systems.

More on this topic in future newsletters.