WIND™

Security: The Key to Affordable Unmanned Aircraft Systems

By Alex Wilson, Director of Business Development, Aerospace and Defense

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Cost efficiency and affordability will always be design criteria for the unmanned aircraft system (UAS). There has been much discussion focused on the use of open systems architecture (OSA). One advantage of this approach is to reduce costs. The U.S. Department of Defense (DoD) encourages the use of OSA through its Better Buying Power 3.0 initiatives. UAS designs based on OSA enable the rapid migration of technology across multiple UAS platforms.

Open systems architectures will not solve all of the challenges associated with building UASes, however. Security is another factor that has an effect on affordability.

In a UAS, the flight control loop extends from the aircraft through the data link to the ground control station. There is also a data link for any payload information. This distributed control and data transfer system introduces security challenges that are not present in traditional manned aircraft. Vulnerabilities exposed by this distributed architecture must be addressed and resolved to minimize the total lifecycle costs of UAS.

The cost saving benefits inherent in open systems are negated by a single security breach. Higher cost is often associated with commercial software — however, commercial software with proven security certification evidence helps reduce the total cost of a project and protect the value of missions. Both approaches are valid, and both must account for security vulnerabilities before they can deliver true cost savings.

This paper provides an overview of the security considerations for unmanned aircraft, along with a summary of security capabilities delivered by Wind River® technologies such as VxWorks®, Wind River Linux, and Wind River Simics®.

TABLE OF CONTENTS

SECURITY CONCERNS FOR UNMANNED SYSTEMS

Security technology for manned avionics systems is well understood. A great deal of existing technology can be leveraged in UAS development. However, there are a few differences that require security mechanisms designed for UAS applications.

To secure a UAS, you have to break the system down into four components, as shown in Figure 1:

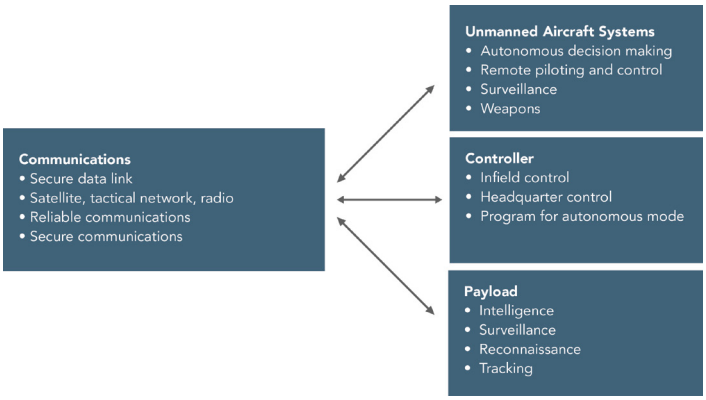

Figure 1. Unmanned aircraft systems environment

Communication and mission data links in UAS are networked distributed systems. The data link must be secured to ensure that would-be attackers cannot gain access to the control communications or the mission data. This prevents the unmanned aircraft and its payload from compromise.

This is especially true as ground control stations move toward an open architecture approach with published services for UAS operations.

The ground station connects to back-end systems or the cloud to enable timely analysis and exploitation of data from intelligence, surveillance, and reconnaissance (ISR) payloads, which increases security requirements. Ground stations are also based on OSA, with published interfaces to UAS operations. It is vital that these are built with security from the ground up.

Developers ensure, and in many cases formally certify, that their end-to-end security remains intact over the lifecycle of the system. This lifecycle approach includes changes in network topography and the addition or deletion of assets in the network. This must cover the design, deployment, operations, and decommissioning of the UAS. Security must be present in all aspects of the system, from the UAS to the network controlling the UAS to the feed of intelligence to decision systems.

CREATING END-TO-END SECURITY

For unmanned aircraft systems, security should be built in at multiple levels, as shown in Figure 2. This approach to security begins with establishing a "root of trust." It builds on this foundation to create a comprehensive lifecycle approach for building secure system components, encompassing the UAS, communications, payload, and the ground control station. This ensures that only authorized individuals, trusted code, trusted payload systems, and communications are used.

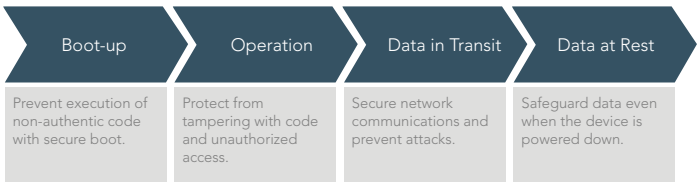

Figure 2. End-to-end security provided by the VxWorks product family

Foundation software, such as the system boot environment and the operating system, support a foundation for lifecycle security and the dynamics of changing asset insertion and deletion.

Security technologies and methodologies are employed to ensure that the system software fully maintains the root of trust. The system software should deliver the following capabilities or features:

- **Digital signature verification:** Such verification ensures that only authorized code is running at boot-up and during runtime operations. The digital signature will typically be based on the X.509 ITU-T standard for public-key cryptography and will generate root keys and certificates for developers to ensure code authenticity.
- **Support for encryption and decryption of data:** Encryption capabilities such as SSL secure the data link and protect IP, and decryption can help thwart attacks that attempt to hide in encrypted data, such as advanced malware threats.
- **Advanced user management features:** A centralized, unified user management system assigns privileges and manages users at runtime. This implements restrictions and controls access to the device based on user credentials.
- **Support for security key interfaces:** Support for interfaces such as SSL and cryptography libraries, as well as IPsec and Internet Key Exchange (IKE), can enable state-of-the-art encryption and effectively secure network communications.
- **Encrypted containers:** Containers strongly encrypted, for example with AES, can safeguard data at rest.

- **Logging and audit trails:** Administrators can see exactly when the system has been entered, whether any data has been changed, and by whom, by using logging and auditing systems.
- **Integration with third-party products and technologies:** Complementary technologies provide value-added capabilities such as SSL visibility, content analysis, and threat intelligence.

Security capabilities based on the UAS lifecycle must be considered, when evaluating affordability. Any lapses in system security can result in costs and penalties that far outweigh the costs of acquiring and operating the system software.

WIND RIVER SOLUTIONS

Wind River delivers on these core security requirements via Wind River Linux and VxWorks.

Wind River Linux security is enhanced by:

- **Certification-ready platform:** *Evaluated Configuration Guide* and documentation to help certify devices for EAL
- **Yocto Project compatibility:** Open source solution based on the Wind River Linux Yocto Project Compatible platform
- **Hardened kernel:** A security-focused kernel including grsecurity and PaX, and including features such as enhanced address space layout randomization (ASLR), memory sanitizing, and path-based security policy with zero runtime memory allocation
- **Secure user space:** Secure-core and secure-platform options, built to take full advantage of runtime buffer overflow protection and with a suite of tools aimed at locking down, monitoring, and auditing a system. This gives administrators more insight and more control of the system than ever before.

VxWorks security is shown in Table 1:

Table 1. VxWorks security capabilities

Design	Boot	Data in Use	Data in Transit	Data at Rest
• Secure Development Processes • Signed binary delivery • IEC 62443 • IEC 27034	• Secure boot/load • Measured boot/load • Signed binary application authentication • Digital certificates/PKI • Remote attestation	• Secure Partitioning • Cryptography • User authentication / manage-ment • Auditing/logging	• Network security • SSL/SSH • IPSEC/IKE • Firewall	• Encrypted storage • Sanitizat-ion

THE ROLE OF VIRTUAL TESTING

The added security measures required for unmanned aircraft contribute to the cost and complexity of security testing. This testing must be executed regardless of the pedigree of the system software components. It continues through the life of the product. The number and sophistication of security exploits is increasing from targeted malware to "zero-day attacks" to advanced persistent threats (APTs). This forces system security testing to be thorough, continuous, and dynamic to adapt to an ever-increasing threat landscape.

Virtualized (simulated) testing can deliver enhanced security for UAS while also helping to reduce costs.

Wind River Simics allows developers, testers, maintainers, and researchers to use virtual target hardware in place of physical hardware. They can run the complete target software stack on a simulated system. They can simulate systems of virtually any size, from processors and memory to complete boards and devices to racks of boards, as well as to complete networks and systems-of-systems.

From a security perspective, these capabilities allow a more comprehensive and efficient approach to understand and address security vulnerabilities than is possible via traditional methods. For example, developers, maintainers, and researchers can do the following:

- **Replicate conditions that caused issues:** Once developers identify flaws or vulnerabilities, they can reproduce the conditions that created them as often as needed. This allows them to pinpoint root causes and potential solutions to security threats.
- **Validate and verify security issues:** Once maintainers identify flaws or vulnerabilities, they can test potential solutions to security threats. This allows them to make sure a solution does not impact the operational system before deployment to live systems.
- **Pause or rewind the test:** The simulation can be paused at any time and run backward. This makes it possible to diagnose a flaw completely and target the remedy to the specific vulnerability.
- **Analyze the entire system:** Testers can examine every facet of the entire system, not just the application software but the operating system, the firmware, and the hypervisor. They can step through and understand exactly what the code is doing and how to protect against threats.

- **Inject faults:** Simulation enables testers to inject faults into the system safely without infecting the actual system under test. This method allows them to study and respond to a wider variety of potential attack vectors.
- **Debug unobtrusively:** With simulation, testers can inspect and modify the state of the entire target system, at any level. This is convenient when debugging low-level code such as firmware and hardware drivers.

With simulation, it is possible to take a comprehensive, holistic approach to uncovering and resolving security threats and accelerate every phase of developing, testing, and deploying security-sensitive unmanned aircraft systems.

CONCLUSION

The selection of system software for affordable UAS development is a business decision, not just a technical analysis. It is possible to see the business case for the use of commercial software based on open architecture systems and open standards. The business case has to assess how the system software addresses the full range of security issues in the UAS lifecycle.

Wind River is supplying open standards–based systems with commercial off-the-shelf safety and security evidence. Affordable UAS development can be achieved through the use of commercial off-the-shelf solutions. This approach also allows developers to focus on innovation to give them a competitive advantage. Government organizations deploying next-generation UAS can benefit from this and field more affordable innovative platforms.