SECURITY: THE KEY TO AFFORDABLE UNMANNED AIRCRAFT SYSTEMS

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

Cost efficiency and affordability will always be key design criteria for unmanned aircraft systems (UAS). Much discussion has focused on the use of open systems architectures (OSA) as a means of reducing costs. The U.S. Department of Defense (DoD) encourages the use of OSA through its Better Buying Power 2.0 initiatives, and the use of OSA is becoming commonplace in UAS designs, enabling the rapid migration of technology across multiple UAS platforms.

However, there is another design criterion that impacts costs and affordability even more than open architecture: security.

The move to a distributed control and data transfer system for unmanned operations introduces security challenges that are not present in traditional manned aircraft. These additional vulnerabilities must be addressed and resolved in order to minimize the total lifecycle costs of UAS.

Simply put, the cost savings benefits inherent in open systems can quickly be negated by a single security breach; conversely, what’s perceived as a higher cost for commercial software with proven security certification evidence may in fact help 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 a high-level overview of the unique security considerations for unmanned aircraft, along with a summary of security capabilities delivered by Security Profile for Wind River® Linux, VxWorks®, Security Profile for VxWorks, Aerospace Profile for VxWorks, Wind River VxWorks MILS Platform, and Wind River Simics®.

TABLE OF CONTENTS

Executive Summary ................................................................. 2
Security Concerns for Unmanned Systems .............................. 3
Creating End-to-End Security ................................................. 3
The Vital Role of Virtual Testing ............................................. 5
Conclusion ............................................................................. 6
SECURITY CONCERNS FOR UNMANNED SYSTEMS

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

In general, four key elements of UAS must be secured: the unmanned aircraft system, communications, the controller, and the payload. All four elements must be secured to create a completely secure, end-to-end solution.

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, and cannot impact any aspect of the operation of the vehicle and its payload. This is especially true as ground control stations move toward an open architecture approach with published services for UAS operations.

Moreover, the ground station must connect to back-end systems or the cloud to enable timely analysis and exploitation of data from intelligence, surveillance, and reconnaissance (ISR) payloads, further increasing security requirements.

Furthermore, developers need to ensure (and in many cases formally certify) that their end-to-end security remains intact over the life of the system, including changes in network topography and the addition or deletion of assets in the network. 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 systems, security must be built-in at multiple levels, from the design architecture to functions such as secure boot-up, secure operation, secure data transmission, and securing data at rest. Foundation software, such as the system boot environment and the operating system, must support a foundation for lifecycle security and the dynamics of changing asset insertion and deletion.

Figure 1: Unmanned aircraft systems environment

<table>
<thead>
<tr>
<th>Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Secure data link</td>
</tr>
<tr>
<td>• Satellite, tactical network, radio</td>
</tr>
<tr>
<td>• Reliable communications</td>
</tr>
<tr>
<td>• Secure communications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Infield control</td>
</tr>
<tr>
<td>• Headquarter control</td>
</tr>
<tr>
<td>• Program for autonomous mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Intelligence</td>
</tr>
<tr>
<td>• Surveillance</td>
</tr>
<tr>
<td>• Reconnaissance</td>
</tr>
<tr>
<td>• Tracking</td>
</tr>
</tbody>
</table>
Key capabilities required for each phase include:

- **Boot-up**: The system must prevent the execution of non-authenticated code or images. Nothing untrustworthy can ever be booted; only the signed software components will run.
- **Operation**: The system must protect against code tampering, malicious code injection, and unauthorized access.
- **Data in transit**: Network communications must secure data in transit and prevent attacks on the platforms and network channels.
- **Data at rest**: The system must safeguard data and prevent unauthorized access to onboard data at rest when the device is shut down.

This approach to security begins with establishing a “root of trust,” and builds upon this secure foundation to create a comprehensive lifecycle for building secure system components, encompassing the UAS, communications, payload, and the ground control station, and ensuring that only authorized individuals and trusted code, systems, and communications are utilized.

- **Advanced user management features**: A centralized, unified user management system makes it possible to assign privileges and manage users at run-time, implementing restrictions and controlling access to the device based on user credentials.
- **Support for key security-related interfaces**: Support for such interfaces 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, e.g., with AES, can safeguard data at rest.
- **Logging and audit trails**: Using logging and auditing systems, administrators can see exactly when the system has been entered, whether any data has been changed, and by whom.
- **A separation kernel**: This feature supports the Multiple Independent Levels of Security (MILS) architecture on multi-core processor architectures, so that exceptionally strong, multilevel security (MLS) systems and cross-domain solutions (CDS) can be delivered without compromising the performance of the system.
- **Integration with third-party products and technologies**: Complementary technologies provide value-added capabilities such as SSL visibility, content analysis, threat intelligence, and so on.

Under the umbrella of this lifecycle approach, many discrete technologies and methodologies must be employed to ensure that the system software fully maintains the root of trust. Specifically, the system software should deliver the following capabilities or features:

- **Digital signature verification**: Ensuring that only authorized code is running at boot-up and during run-time 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.

Simply put, when evaluating system software options with an eye toward increasing UAS affordability, the full range of security capabilities must be considered. 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 delivers on these core security requirements via Wind River Linux, the market-leading commercial-grade Linux solution for embedded device development, and VxWorks, the most widely deployed commercial real-time operating system.

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 gssecurity and PaX, and including features such as enhanced Address Space Layout Randomization (ASLR), memory sanitizing, and path-based security policy with zero run-time memory allocation

Figure 2: End-to-end security provided by Security Profile for VxWorks
• **Secure user space:** Secure-core and secure-platform options, built to take full advantage of run-time buffer overflow protection and including a suite of tools aimed at locking down, monitoring, and auditing a system, giving administrators more insight and more control of the system than ever before

• **Enabled Protection Profiles in the Common Criteria scheme:** Implemented as feature templates
  - Operating System Protection Profile and Validation Tools (OSPP)
  - General Purpose Operating System Protection Profile (GP-OSPP)
  - Labelled Security Protection Profile (LSPP)
  - Role-Based Access Control Protection Profile (RBAC-PP)

The inherent security advantages of VxWorks are supplemented by:

• **Security Profile for VxWorks:** Delivers a comprehensive set of security features to efficiently protect devices and data at every stage

• **Aerospace Profile for VxWorks:** Provides a collection of middleware developed to help manufacturers of aerospace and defense systems bring robust, differentiated products to market faster, while reducing risks and development costs

• **Wind River VxWorks MILS Platform:** Implements the industry-standard MILS architecture to provide an operating run-time environment designed for systems with high security, high assurance, and high performance requirements

• **Wind River VxWorks 653 Platform:** Provides robust partitioning in time and space to ensure fault containment in accordance with strict ARINC 653 requirements for Integrated Modular Avionics (IMA)

### THE VITAL ROLE OF VIRTUAL TESTING

The added security measures required for unmanned aircraft also contribute to the cost and complexity of security testing. This testing must be executed regardless of the pedigree of the system software components, and must continue 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)—forcing system security testing to be thorough, continuous, and dynamic to adapt to an ever-increasing threat landscape.

One option that can deliver enhanced security for UAS while also helping to reduce costs is virtualized (simulated) testing.

With simulation systems such as Wind River Simics, developers, testers, maintainers, and researchers use virtual target hardware in place of physical hardware for software development, debugging, testing, system integration, and deployment management. That means 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, racks of boards, even complete networks and systems-of-systems.

From a security perspective, these capabilities allow for a more comprehensive and efficient approach to understanding and addressing 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, so they can pinpoint root causes and potential solutions to security threats.

• **Validate and verify security issues:** Once maintainers identify flaws or vulnerabilities, they can fully test potential solutions to security threats, and make sure a solution does not impact the operational system before deployment to live systems.

• **Pause or rewind the test:** Testers can pause the simulation at any time and even run the whole simulation backward, which makes it possible to diagnose a flaw more 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, the hypervisor, and so on, so they can step through and understand exactly what the code is doing and how to fully protect against threats.

• **Inject faults:** Simulation enables testers to inject faults into the system safely without infecting the actual system under test, so they can study and respond to a wider variety of potential attack vectors.

• **Debug non-obtrusively:** With simulation, testers can inspect and modify the state of the entire target system, at any level. This is especially convenient when debugging low-level code such as firmware and hardware drivers.
With simulation, it becomes 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.

CONCLUSION

Ultimately, the selection of system software for affordable UAS development is a business decision, not just a technical analysis. By assessing how the system software addresses the full range of security issues in UAS development, it becomes possible to see clearly the business case for the use of commercial software based on open architecture systems and open standards.

By addressing the comprehensive array of security issues confronting UAS development teams, open-standards vendors such as Wind River are attempting to smooth the road to more affordable UAS—and further accelerate the cost savings, product innovation, commercial off-the-shelf safety and security evidence, and other benefits that will accrue to government organizations deploying next-generation unmanned systems.