A Security Strategy for Avionics Systems

The Wind River Approach to DO-356A Certification

Massimiliano De Otto, CISSP
Senior Field Applications Engineer

WNDRVR

TABLE OF CONTENTS

1. INTRODUCTION

THE NEED FOR SECURITY IN AVIONICS SYSTEMS

It has taken nearly 10 years to complete development of a set of standards covering airworthiness security. This started with Boeing developing the Integrated Modular Avionics (IMA) environment on the 787 airliner. In order to support multiple independent applications at different safety levels, changes to the ARINC 653[1] specification and a new process for IMA certification in the form of RTCA DO-297[2]/EUROCAE ED-124[3] were required. This contained a novel design feature of a network architecture comprising flight-related safety control systems (the Aircraft Control Domain); airline business and administrative support (Airline Information Services Domain); and passenger entertainment, information, and internet services (Passenger Information and Entertainment Services Domain).

The FAA required that special conditions must be met[4] to ensure that avionics systems and data networks would be isolated and protected from unauthorized passenger domain systems access. It became clear that a system-level approach was needed to isolate applications from a security perspective to ensure safety, so the subcommittee (SC-216) was formed in 2007 to start work on what became RTCA DO-326/EUROCAE ED-202; now the group is working on the second revision, DO-326A[5]/ED-202A.[6]

The concept of these standards is to follow the existing processes familiar to avionics designers (from the ARP4754A[7] and DO-178C[8] process) and apply them to cybersecurity as it pertains to the airworthiness and safe operation of the aircraft. This idea led to a series of RTCA standards with DO-326A; DO-355;[9] DO-356A;[10] and EUROCAE ED-202A, ED-203A,[11] and ED-204A[12] respectively. These represent the high-level system approach, the initial requirements for an ongoing approach to continued airworthiness security.

The implementation of RTCA DO-356A is now regarded as an acceptable means of compliance for EASA with AMC-20 amendment 18.[13] The compliance to both formal security and safety standards will be an important asset for future avionics platforms.

This was a long-awaited step, since there are already examples of aircraft systems vulnerable to cyberattack. Stories that many thought would be seen only in movies are now reality. The AFuzion white paper on aviation cybersecurity[14] is a good introduction to the problem and the need for a security standard.

This paper outlines the principles behind avionics security and shows how Wind River® can help meet the objectives of DO-326A and DO-356A while maintaining strict compliance with DO-178C. The objective of a safe and secure platform is therefore achieved.

2. WIND RIVER ENGAGEMENT

As DO-355/ED-204 was the first guidance released that aligned across Europe and North America, Wind River did an early study of mapping between OS features in VxWorks® 653, a hypervisor-based ARINC 653 platform, and the DO-355 standard requirements.[15] This outlined where support could be provided by a COTS product solution and where it would be better custom built for a particular avionics platform. The latter is usually due to hardware features or nonstandard specifics for a unique application, for which Wind River offers various prepackaged solutions, such as the Security Assessment based on the Wind River Helix™ Security Framework or the Information Assurance Foundation customized security solution.[16]

In order to host multiple security classifications simultaneously, a secure isolation of domains is required, which introduces additional requirements into a safety-focused system. Originally this was achieved on single-core processors using a well-known concept in trusted computing, the so-called separation kernel (SK). The purpose of an SK is to provide data isolation, information flow, periods processing, and fault isolation to the OS platform. State-of-the-art multi-core processors provide the ability to implement the SK principles using virtualization technologies. This is the basis on which Wind River has designed the architecture of its family of safety products for multi-core: VxWorks 653 Multi-Core Edition[17] and Wind River Helix™ Virtualization Platform.[18]

3. A BRIEF OVERVIEW OF DO-356A

DO-356A, "Airworthiness Security Methods and Considerations," has the declared scope of protecting the airworthiness of an aircraft from any intentional, unauthorized electronic interaction that could compromise the safety of the aircraft itself. Physical security is not addressed by the document.

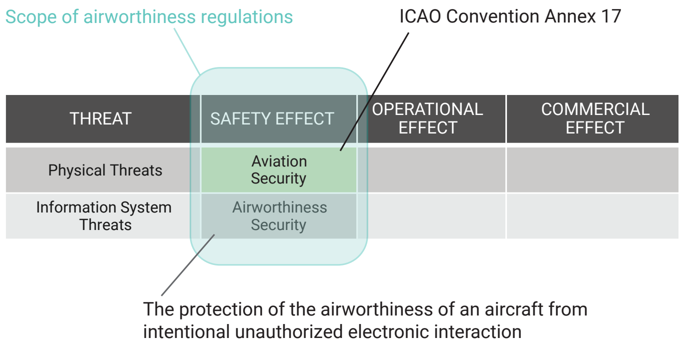

Scope of airworthiness regulations
ICAO Convention Annex 17
THREAT
SAFETY EFFECT
OPERATIONAL EFFECT
COMMERCIAL EFFECT
Physical Threats
Aviation Security
Information System Threats
Airworthiness Security
The protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction

Figure 1. Scope of airworthiness security

This scope must be addressed by implementing a process that:

- Identifies any electronic equipment ("asset") that needs to be protected
- Defines the perimeter of action ("scope") of the asset and its interaction with other assets; this may be one single element or a set of assets, as shown in Figure 2
- Identifies the potential attack surfaces for any asset
- Defines a threat level for that asset, including the impact on other assets caused by a security event
- Finally, defines a set of security measures and continuous monitoring activities for each asset: A security assurance level (SAL) is assigned to each security measure to classify the level of confidence in that measure against any attack to the asset being protected

Figure 2 is shown below as an example of a security scope.

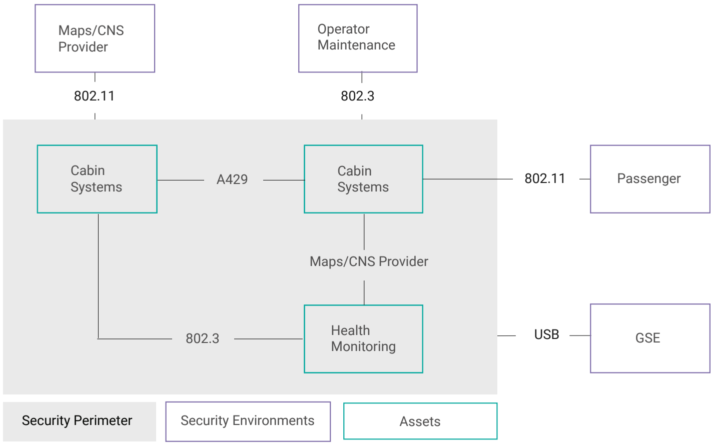


Figure 2. Security scope example

It is important to observe here that each asset may have a different SAL, and that in general more than one measure has to be applied. The number is not specified but must be adequate to avoid an impact on the safety of the aircraft. DO-356A defines a risk acceptability matrix to help determine the quantity and quality of security measures to apply, as shown in Table 1.

Table 1: Risk Acceptability Matrix

	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable

Security assurance levels are described in Table 2.

Table 2: Security Assurance Level Definition

Security Assurance Level (SAL)	Security Assurance Level (SAL)
3	Strongest security assurance for security measures. All security assurance objectives defined in this document are applicable.
2	Advanced security assurance for security measures. SAL 2 is similar to SAL 3 on security-specific assurance objectives but significantly less demanding on security-development assurance objectives.
1	Minimum security assurance for security measures. Appropriate for additional protection or hardening/resilience.
0	No protective effect. This level is limited to the initial assessment of the protection needs (as detailed in section 2.2 of DO-356A/ED-203A) and is applicable for systems and items that have no higher SAL assigned.

This process must be documented, and proper evidence must be produced; under this aspect DO-356A is very similar to DO-178C, since the output of its activities is a set of documents and reports that resemble closely the structure of a safety certification evidence. The full set of documents is described in DO-326A. It is worth mentioning the Plan for Security Aspects of Certification (PSecAC), which is analogous to the Plan for Software Aspects of Certification (PSAC) in DO-178C; like the PSAC, it is a living document evolving with the security process on a given system. Figure 3 shows this evolution:

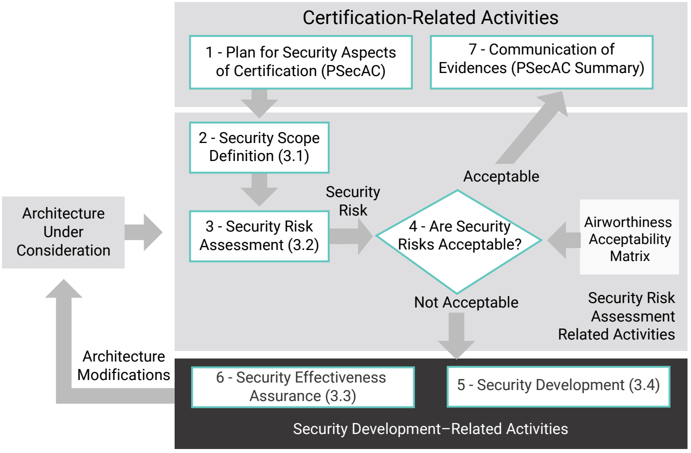

Certification-Related Activities
1 - Plan for Security Aspects of Certification (PSecAC)
7 - Communication of Evidences (PSecAC Summary)
2 - Security Scope Definition (3.1)
Acceptable
Security Risk
Architecture Under Consideration
3 - Security Risk Assessment (3.2)
4 - Are Security Risks Acceptable?
Airworthiness Acceptability Matrix
Not Acceptable
Security Risk Assessment Related Activities
Architecture Modifications
6 - Security Effectiveness Assurance (3.3)
5 - Security Development (3.4)
Security Development–Related Activities

Figure 3. Security process workflow (based on DO-326A)

4. DO-356A MAPPING FOR WIND RIVER PLATFORMS

The DO-356A standard primarily addresses the processes and objectives for formal compliance and validation. Section 5 of this document describes security architecture principles that also apply to software.

The DO-356A references the Common Criteria (CC)[19] as a non-avionics standard for formal security, including a traceability between its objectives and CC classes. It is therefore important to take the key concepts of the Separation Kernel Protection Profile (SKPP)[20] into consideration, even though the U.S. National Information Assurance Partnership (NIAP) sunset the SKPP, effective beginning June 1, 2011, and existing protection profiles were downgraded in the U.S. to EAL 2.[21]

This also means that the claim of prior protection profile validation, as proposed in section 2.8.3 of DO-356A, is not applicable to modern operating systems versions. However, although the SKPP has been sunset, the fundamental principles used to implement multiple independent levels of security (MILS) systems are still valid and can be applied to secure hypervisors on modern multi-core processors.

4.1. Wind River Platforms Overview

Wind River has a rich pedigree of reliable solutions for safety-critical needs. VxWorks 653 was introduced in 2003 and has been adopted by more than 500 programs worldwide.

VxWorks 653 is an ARINC 653–compliant OS that can be certified up to DO-178C DAL A; initially designed for single core processors, it is now available for multi-core processors responding to the market needs for faster, more compact, more efficient computing solutions. It is available for the Power Architecture®.

The increasing interest of the avionics world in Arm® architecture, along with the massive introduction of Arm-based solutions by semiconductor manufacturers, led to the introduction of Helix Platform, specifically targeting this architecture.

Both products share the same architecture (Figure 4) to implement the ARINC 653 concept of time and space partitioning:

- A hypervisor initializes the hardware and enforces a predefined configuration. It also schedules the partitions.
- One or more partitions host independent guest operating systems and applications. In other words, a partition is a virtual machine that hosts some aircraft functions performed by the system. The guest OS may be safety-critical (VxWorks Cert Edition), Linux, or RYO.
- A configuration vector contains the configuration information for the system (number partitions, resource assignment, scheduling slots) based on XML.

Both products are compliant to the ARINC 653 specification, Parts 1 and 2 (references [17] and [18] provide more details).

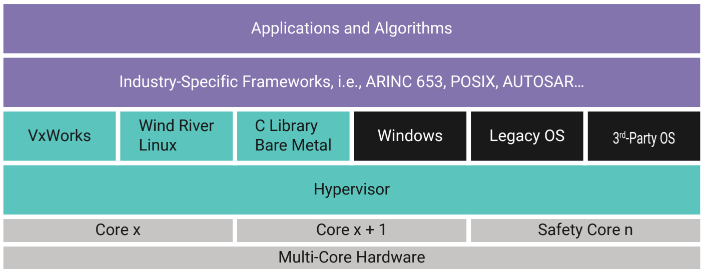


Figure 4. Notional architecture of Wind River hypervisor-based platforms

The following sections will analyze how this architecture is suitable for meeting the DO-356A requirements for a secure platform.

4.2. Separation Kernel Requirements

4.2.1. Data Isolation

Requirement: To ensure that a partition cannot access resources in other partitions, either directly or indirectly via a covert channel of communication

This requirement can be met using the memory management unit (MMU) present on any modern processor. The MMU prevents rogue pointer access from outside the partition boundaries. In addition, the most recent CPUs include a virtual I/O capability that prevents unallowed DMA operations from memory to devices, providing an even more robust isolation capability.

The Wind River family of partitioned operating systems takes full advantage of both, allowing robust space separation between the different virtual machines running on the processor.

4.2.2. Information Flow

Requirement: To allow only permitted information flows between partitions

This requirement states that a communications channel is connected only to the intended source and destination partitions, and that the information flows in one direction only (from source to destination).

In Wind River platforms, this is accomplished using the concept of the APEX channel as specified in the ARINC 653 standard. An APEX channel is a one-to-one connection between partitions; it can be enhanced by adding one-to-many connections and allowing scrubbing of a message buffer once it has been received, to prevent memory covert channels.

4.2.3. Periodic Processing

Requirement: To ensure that applications within partitions execute for the specified duration in the system schedule

In a platform hosting multiple applications and security domains, there is the potential for a rogue application to interfere with another application through variation in execution timing, known as a covert timing channel. A rogue partition may attempt to vary its own allocated execution period to cause an adverse effect on another application, or to detect and measure variations in its own execution speed (due to changes in cache contents caused by another application), or to detect and measure variations in the execution period of another application.

These covert timing channels can act as a semaphore, indirectly signaling a 0 or a 1 to another application. On a modern processor running at GHz speeds, this can create a covert channel of significant bandwidth, transmitting a large amount of information in a relatively short time. These covert channels can be significantly mitigated (but not completely eliminated) by the use of specific measures, including periods processing leveraging the frame scheduler of the Wind River platforms.

When running on a single core processor, an ARINC 653 time slot schedule with fixed minor frames is designed to prevent applications from overrunning their allocated time slot periods. If an application can cause its minor frame duration to overrun, this is known as jitter. It is possible for an ARINC 653 OS to implement a system-wide maximum jitter duration attribute, so that if an application partition tried to overrun or the partition context switch were not performed in a repeatable, deterministic way, a security event would be generated (indicating a potential covert timing channel).

Covert channels on multi-core processors pose a greater threat due to the simultaneous execution of multiple applications and security domains on different cores. This is beyond the scope of this paper.

4.2.4. Fault Isolation

Requirement: To ensure that a failure in one partition does not impact any other partition within the system

The implementation of data isolation contributes to fault isolation by preventing fault propagation or illegal accesses beyond a partition. However, a security system needs to be able to adapt its behavior and responses according to its threat environment. Therefore, a security management framework is required to enable security audit logging to be performed. This would enable recording and monitoring of individual security-related events and enable the appropriate action to be taken in response to an event of attempted security violation.

Wind River platforms implement an ARINC 653 health management framework to address safety-related events. This could potentially be extended to include support for security-related events.

4.3. Security Architecture Principles

Section 5.6 of DO-356A, "Security Architecture Principles at Aircraft Level," lists 14 principles that a good security design should implement to minimize the event of new, unpredicted risks being discovered during the assessment phase, forcing a redesign with a consequent increase in costs.

The idea is that these principles start from the aircraft and propagate downward to all the subsystems, including the assets as defined in the previous section.

Table 3: Security Architecture Principles

Architecture Principle	Applicable to OS	Comment
Defense in Depth	No	Layered protection is a system design principle. A hypervisor-based architecture, as implemented by VxWorks 653 and Helix Platform, can contribute to this principle. Any guest OS runs in a fully virtualized environment and is unaware that it is running on top of a hypervisor. Another factor that contributes to defense in depth is the careful choice and configuration of the guest OS(es) that will run in the system.
Integrity of Connected Equipment	Yes	Independent loading of a guest OS and applications occurs via independent build, link and load, custom partitions loader, cryptographic hash functions in the guest OS, and amendments via the Information Assurance Framework (see page 8).
Continued Airworthiness	Yes	This is support for incremental certification with independent build, link, and load and Wind River safety and security monitoring processes.
Prevent Bypass of Security Barriers	Yes	Kernel for the hypervisor and guest OS with a defined feature set and full DO-178C Level A traceability prevents backdoor introduction.
Keep Security Architectures as Simple as Possible	Yes	Separation between the hypervisor and guest OS and independent configuration vector reduces dependencies and interactions. The guest OS allows a minimized configuration and footprint.
Detection and Restoration	Yes	See Fault Isolation (page 6).
Attack Path Refinement at System Level	No	This is system-level activity.
Consider Security Process Specifics	Yes	A dedicated security test suite can be designed and applied at the system level.
Minimize External Interfaces	Yes	A configuration vector enables strict limitation of access to external interfaces with hardware device assignment and restricted communication between partitions.
Disable All Unused Interfaces	Yes	See the previous entry; the VxWorks guest OS allows fine configuration of software interfaces such as network protocols.
Independence and Isolation	Yes	ARINC 653 and DO-297 provide isolation and independence concepts as referenced in DO-356A.
Ensure Proper Error Handling	Yes	See Fault Isolation (page 6). Guest OS basic security measures might need hardening, as well as defensive programming techniques at the application level and BIT.
Least Privilege	Yes	ARINC 653 concepts provide permissions, but static configuration inhibits time-based privilege grants. There is no role concept in Helix Platform.
Control Access to Connections	Yes	Access control protection must be added where applicable; e.g., using authentication in network protocols or authentication on port/channel communication.

5. HOW WIND RIVER CAN SUPPORT YOUR PROGRAM

As seen in the previous section, almost all the security architecture principles are applicable from a software perspective. Wind River platforms are a good start for addressing them. The ideal set of features depends on the system under consideration, the SALs to be applied, and other factors.

The perfect mapping does not exist: Any system has its own unique requirements and, consequently, gaps and critical areas that need to be identified and addressed.

Wind River can solve the avionics security requirement by using a combination of products and services.

5.1. Security Assessment

Wind River Professional Services can perform a Security Assessment. At the end of this activity, customers receive a detailed written assessment of how to secure their systems, including:

- Identified assets
- Identified vulnerabilities of those assets

- A clearly defined security policy that describes:
  - A list of security implementations that will protect each asset from the listed vulnerabilities
  - A list of security-related log events that should be recorded
  - A list of responses to those security audit log events
  - A prioritized list of recommendations

The assessment can be customized and can include architecture review, help to develop the necessary documentation, and a customized protection plan.

A Security Assessment covers part of the formal activities described by DO-356A as "Certification Requirements." Wind River Professional Services can provide additional help to perform all the formal steps required to achieve such requirements:

- Security risk assessment activities
- Vulnerability identification activities
- Security refutation activities
- Security deployment activities
- Continued security effectiveness activities
- Requirements activities
- Design activities
- Implementation activities
- Security verification activities
- Security planning activities
- Security configuration management activities
- Tool security activities

5.2. The Information Assurance Framework

The Information Assurance Framework (IAF) is a set of GPL-free libraries specifically designed to enhance security of avionics systems by using processor hardware security capabilities to provide a broad set of security features. For example, in the IAF implementation on QorIQ architectures, these libraries use the SEC engine and provide:

- APIs for access to the SEC engine
- Software and workflow of secure boot and APIs for the trusted boot process
- Software for accessing the security monitor
- Software and workflow to enable the runtime integrity checker (RTIC)
- Software and workflow to enable the secure debug controller
- Software and workflow to enable the peripheral access management unit (PAMU)

Along with the IAF, Wind River Professional Services provides comprehensive documentation on how to use the libraries and a complete test suite to assess the system.

5.3. Security Hardening Guide and NIST SP 800-53 Mappings

The latest version of the Wind River leading RTOS, VxWorks, includes a "Security Hardening Guide" document. This document is based on the DISA General Purpose Operating System (GPOS) *Security Requirements Guide*[22] and provides a list of features mapping the requirements provided by that document according to the two categories of "Mandatory" and "Discretionary." Every time a given SRG requirement is not applicable, a rationale and possible mitigation actions at the system/design level are provided.

Using the "Security Hardening Guide" and the accompanying "Hardening Guide Approach Guide," Wind River customers can configure VxWorks to meet stringent security requirements for their applications and systems. These can be tailored according to the needs of the specific product.

Another capability provided to Wind River customers is the mapping of the NIST SP 800-53 controls[23] to Wind River products. This guidance helps define the applicability of security capabilities to systems, the implications of configuration decisions, and the division of responsibilities between system integrator and suppliers. Its broad applicability and recognition make NIST 800-53 a well-suited starting point for derivations to other industry security standards, providing a proven path to accountability with regulatory organizations. This is a valid help in reaching the "continuous monitoring" prescribed by DO-356A.

Most of the STIG SRG maps in turn to a NIST SP 800-53 requirement.

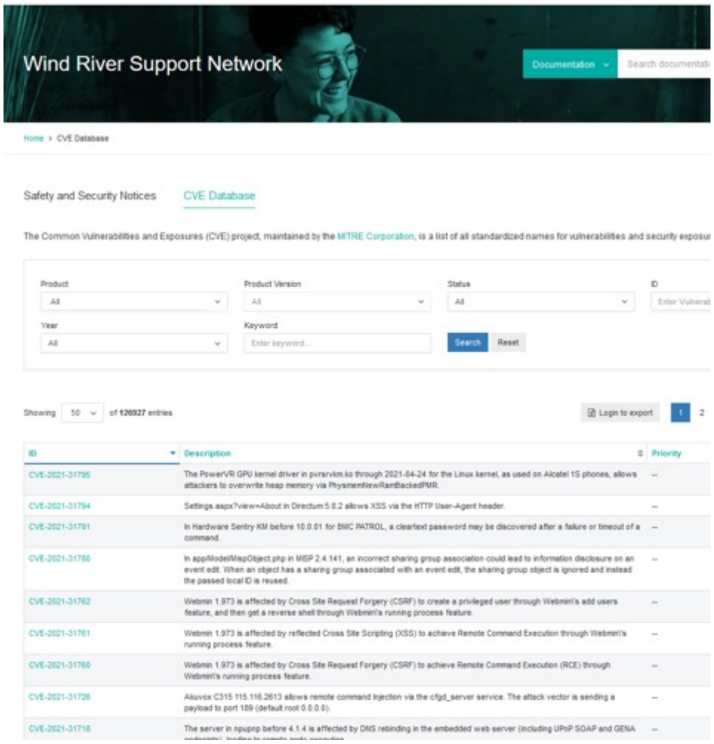
5.4. Wind River Security Shield

Wind River is committed to ensuring that its products are always protected against any vulnerability that might impact their functionality. Security Shield is an additional service provided to customers that offers these features:

- Constant monitoring of CVEs that are reported by researchers and security companies
- An alert service that notifies customers of any CVE that may impact Wind River products

- Determination of whether a CVE is impacting the customer
- Analysis of the possible impact on safety of the CVEs and common agreement on a mitigation strategy
- Access to the CVE database[24] maintained by the MITRE Corporation, with the possibility of searching for any CVE that might have an impact on a given version of a Wind River product

Wind River recognizes the importance of clear and accessible communication regarding security issues. Therefore, the last item on the above list, the CVE database, is publicly accessible through the Wind River web portal under the Security tab.[25]



The Common Vulnerabilities and Exposures (CVE) project, maintained by the MITRE Corporation, is a list of all standardized names for vulnerabilities and security exposu

Product: All
Product Version: All
Status: All
ID: Enter Vulnerab
Year: All
Keyword: Enter keyword...

Showing 50 of 126927 entries

ID	Description	Priority
CVE-2021-31795	The PowerVR GPU kernel driver in pvrsrvkm.ko through 2021-04-24 for the Linux kernel, as used on Alcatel 1S phones, allows attackers to overwrite heap memory via PhysmemNewRamBackedPMR.	—
CVE-2021-31794	Settings.aspx?view=About in Directum 5.8.2 allows XSS via the HTTP User-Agent header.	—
CVE-2021-31791	In Hardware Sentry KM before 10.0.01 for BMC PATROL, a cleartext password may be discovered after a failure or timeout of a command.	—
CVE-2021-31780	In app/Model/MispObject.php in MISP 2.4.141, an incorrect sharing group association could lead to information disclosure on an event edit. When an object has a sharing group associated with an event edit, the sharing group object is ignored and instead the passed local ID is reused.	—
CVE-2021-31762	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to create a privileged user through Webmin's add users feature, and then get a reverse shell through Webmin's running process feature.	—
CVE-2021-31761	Webmin 1.973 is affected by reflected Cross Site Scripting (XSS) to achieve Remote Command Execution through Webmin's running process feature.	—
CVE-2021-31760	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to achieve Remote Command Execution (RCE) through Webmin's running process feature.	—
CVE-2021-31726	Akuvox C315 115.116.2613 allows remote command injection via the cfgd_server service. The attack vector is sending a payload to port 189 (default root 0.0.0.0).	—
CVE-2021-31718	The server in npupnp before 4.1.4 is affected by DNS rebinding in the embedded web server (including UPnP SOAP and GENA	—

Figure 5. CVE database hosted on the Wind River website

6. CONCLUSION

Maintaining security is a continuous process throughout the lifecycle of a product. A system that can be considered secure in the present does not offer a guarantee that it will remain secure over time. New vulnerabilities, zero-day exploits, and attack methods are identified daily. Wind River can help address the challenges by providing a robust product based on a hypervisor and a rich set of additional services and continuous monitoring activities. Products built upon this foundation can be reliably designed to meet present and future security needs.

7. ACKNOWLEDGMENTS

The author is grateful to the following Wind River colleagues for their input into this white paper: Stefan Harwarth, Stéphane Le Merdy, Paul Parkinson, Alex Wilson, and Michel Chabroux.

8. REFERENCES

1. ARINC 653 Part 1 Supplement 5, "Avionics Application Software Standard Interface, Part 1, Required Services," ARINC,
2. DO-297, "Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations," RTCA, November 8, 2005
3. ED-124, "Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations," EUROCAE, June 2007
4. NM364 Special Conditions No. 25-356-SC, "Boeing Model 787-8 Airplane; Systems and Data Networks Security — Isolation or Protection from Unauthorized Passenger Domain Systems Access," Federal Aviation Administration (FAA), February 1, 2008
5. DO-326A, "Airworthiness Security Process Specification," RTCA, August 6, 2014
6. ED-202A, "Airworthiness Security Process Specification," EUROCAE, August 6, 2014
7. RP4754A, "Guidelines for Development of Civil Aircraft and Systems," November 1, 1996, SAE
8. DO-178C, "Software Considerations in Airborne Systems and Equipment Certification," RTCA, December 13, 2011
9. DO-356A, "Airworthiness Security Methods and Considerations," RTCA, June 21, 2018
10. DO-355A, "Information Security Guidance for Continued Airworthiness," September 10, 2020, RTCA
11. ED-203A, "Airworthiness Security Methods and Considerations," EUROCAE, June 2018
12. ED-204A, "Information Security Guidance for Continuing Airworthiness," EUROCAE, September 2020
13. AMC-20 Amendment 18, "General Acceptable Means of Compliance for Airworthiness of Products, Parts, and Appliances," European Aviation Safety Agency (EASA), June 24, 2000
14. "DO-326A/ED-202A Intro to Aviation Cyber-Security," AFuzion
15. A. Baker, P. Parkinson, "Cybersecurity Enhancements for a Safety-Critical ARINC 653 Avionics Platform," Aviation Electronics Europe, June 2018
16. Wind River Helix Security Framework and Information Assurance Framework, Wind River, September 2017
17. VxWorks 653 Multi-core Edition Product Overview, Wind River, October 2019
18. Helix Virtualization Platform Product Overview, Wind River, February 2019
19. Common Criteria portal
20. "U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness," Version 1.03, U.S. Government Information Assurance Directorate, June 29, 2007
21. "Publications and Future Support for Separation Kernels," National Information Assurance Partnership, May 11, 2011
22. Security Technical Implementation Guides (STIGs), public
23. NIST Special Publication 800-53
24. Common Vulnerabilities and Exposures (CVE) Database
25. Wind River Security Center

WNDRVR