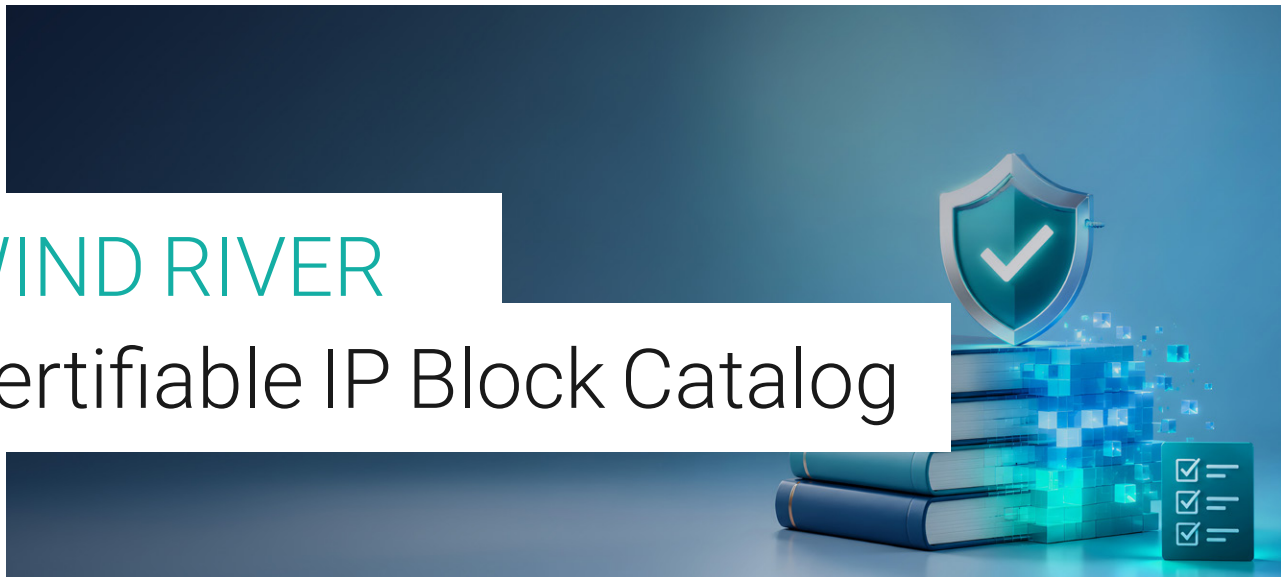

WIND RIVER
Certifiable IP Block Catalog

Wind River provides certifiable IP blocks that are prebuilt, pre-documented, and pre-verified software components for safety- and security-critical embedded systems, with DO-178C DAL A certification evidence. These blocks accelerate certification programs while reducing integration risk and program cost. This catalog provides technical specifications and key differentiators for each available block, supporting evaluation by certification engineers, system architects, and program technical leads.

To see how Wind River certifiable IP blocks have accelerated certification for real programs, see the Certifiable IP Blocks Solution Brief.

BLOCKS IN THIS CATALOG:

- **Curtiss-Wright VPX3-1708 Reference BSP** — Two-level board support package for ARINC 653 systems
- **Curtiss-Wright VPX3-1708 Secure Boot Loader** — Authenticated boot with hardware-anchored chain of trust
- **Information Assurance Foundation (IAF)** — Data protection, integrity, and trusted boot services
- **RTNET Cert** — Deterministic TCP/IP network stack for safety-critical systems
- **High Reliability File System (HRFS)** — Power-loss-safe transactional file system

DO-178C COMPLIANCE ARTIFACTS

A complete DO-178C DAL A compliance artifact set is available for each block through Wind River Professional Services. Each set contains the data required to meet the objectives of all four DO-178C phases — Planning, Requirements and Design, Verification, and Completion — spanning the full evidence chain from the Plan for Software Aspects of Certification (PSAC) through the Software Accomplishment Summary (SAS) including high- and low-level requirements, compliant source code, review data, and complete test cases, procedures, and results.

CURTISS-WRIGHT VPX3-1708 REFERENCE BSP

Two-Level Board Support Package for ARINC 653 Systems

A complete two-level board support package for ARINC 653 systems on the Curtiss-Wright VPX3-1708 single-board computer: a Module OS BSP supporting the Helix Virtualization Platform hypervisor level, and a Partition OS BSP providing the RTOS and full device driver suite for VxWorks guest partitions. A DO-178C DAL A evidence license is available through Wind River Professional Services.

Key Differentiators

- **Complete Two-Level Coverage** — Purpose-built BSPs for both the hypervisor (MOS) and partition (POS) levels of an ARINC 653 system
- **Comprehensive Driver Suite** — Storage, buses, timing, DMA, and discrete I/O drivers for the full VPX3-1708 device complement
- **Integrated with Catalog Blocks** — RTNET, HRFS, and IAF are pre-integrated — the certifiable stack composes out of the box; production use requires a separate license for each
- **Per-Component Evidence** — Every component carries dedicated DO-178C artifact documentation, supporting focused delta certification

Specification	Value	Notes
Target hardware	Curtiss-Wright VPX3-1708 SBC	NXP LX2160A SoC (Arm Cortex-A72)
Operating environment	Helix Virtualization Platform (ARINC 653)	VxWorks 7 partition operating system
BSP STRUCTURE		
Module OS (MOS) BSP	Hypervisor level	Board configuration, common execution environment, device drivers
Partition OS (POS) BSP	Partition level	Board configuration, processor support library, full device driver suite
Evidence structure	Per-component	Each component carries its own DO-178C artifact documentation
MOS BSP CAPABILITIES		
System services	Interrupts, system clock, ROMFS	—
Memory protection	SMMU support	System Memory Management Unit configuration
Health monitoring	EDR/HM events	Error Detection and Recovery integrated with HVP Health Monitor
POS BSP DEVICE SUPPORT		
Storage	NVMe SSD, NOR Flash, MRAM	Plus HRFS and extended block device support
Networking	Ethernet	Allows the DPAA2 Management Complex (MC) two SFC and one RJ-45 devices to be assigned to different partitions; integrates with RTNET Cert
Buses & I/O	PCIe, I2C, SPI, FlexSPI, GPIO, discrete I/O, serial	Includes non-transparent bridge (NTB) over PCIe
Timing	RTC, elapsed time counter, timers, clock subsystem	—
Data movement	DMA engine	—
Application loading	APEX loader	ARINC 653 Application Executive loader/launcher
INTEGRATION & COMPLIANCE		
Security	IAF components included	Trusted Boot Engine, key database, and hardware security engine support
File system	HRFS included	Transactional file system support in the partition OS
Safety certification support	DO-178C DAL A	Evidence license available through Wind River Professional Services

CURTISS-WRIGHT VPX3-1708 SECURE BOOT LOADER

Hardware-Anchored Authenticated Boot

A certifiable secure boot loader occupying the final user-level stage of the Arm Trusted Firmware boot chain on the NXP LX2160A. Every image is signature verified through the Information Assurance Foundation (IAF) before execution, with boot media accessed through the transactional HRFS file system — extending the chain of trust from silicon to operating system. IAF and HRFS are integrated into the SBL and licensed separately for production use; customers develop their own boot application — the SBL element implementing customer-specific image location, load, and verification. DO-178C DAL A evidence is available through Wind River Professional Services.

Key Differentiators

- **Authenticated Boot Path** — No image executes without IAF signature validation; encrypted image support included
- **Minimal-Footprint Staged Design** — A small hardware-initialization loader launches a VxWorks-kernel-based boot application — capability without bloat at the most safety-critical boot stage
- **Power-Loss-Safe Media Access** — Boot images read through HRFS, eliminating file system corruption as a boot-failure mode
- **Boot-Time Health Awareness** — Onboard temperature and voltage monitoring with error detection and logging from the first instruction
- **Per-Component Evidence** — Every component carries dedicated DO-178C artifact documentation

Technical Specifications

Specification	Value	Notes
BOOT ARCHITECTURE		
Boot chain position	BL3.3	Final user-level stage of the Arm Trusted Firmware boot flow
Loader design	Two-stage	Minimal hardware-init loader launches a VxWorks-kernel-based boot application
Boot source	QSPI NOR Flash	Loader stage; payload images loaded from NVMe
SECURITY		
Image authentication	Signature validation via IAF	Every image verified before execution
Encrypted images	Supported	Decryption via IAF during load
Image format	Signed ELF	Loaded from NVMe to RAM
RELIABILITY		
File system	HRFS	Transactional, power-loss-safe access to boot media
Error handling	Detection and logging	Boot-time error detection with exception level handling
Health monitoring	Temperature and voltage	Onboard sensor monitoring during boot
PLATFORM & COMPLIANCE		
Target hardware	Curtiss-Wright VPX3-1708 SBC	NXP LX2160A SoC (Arm Cortex-A72)
Safety certification support	DO-178C DAL A	Evidence available through Wind River Professional Services

INFORMATION ASSURANCE FOUNDATION (IAF)

SEC Engine Access

The Information Assurance Foundation (IAF) provides applications the interfaces to securely handle data and verify its integrity using the processor's on-chip security engine (SEC engine) for cryptographic and hashing operations. A library rather than a standalone application, IAF is pre-integrated into the Curtiss-Wright VPX3-1708 SBL and BSP — binding cryptographic functions to a write-protected Black Key Database (BKDB) in non-volatile memory — and is licensed separately for production use. IAF is operating-system independent and processor specific, with DO-178C compliance artifacts provided through Wind River Professional Services.

Key Differentiators

- **Hardware-Backed Crypto —** The NXP SEC engine offloads all RSA/ECC operations — zero CPU overhead for key verification
- **Tamper-Proof Key Storage —** BKDB is hardware write-protected after provisioning; cannot be modified at runtime
- **Pre-Kernel Enforcement —** Verification runs before the OS loads — no software bypass path exists
- **Dual-Image Resilience —** Built-in primary/secondary image fallback with independent verification callbacks
- **Certifiable Architecture —** DO-178C Level A design with full function header block (FHB) traceability and MISRA-C conformance

Technical Specifications

Performance figures measured on CW VPX-1708 with NXP QorIQ ARMv8 processor.

Specification	Value	Notes
PERFORMANCE		
Boot-time overhead	< 50 ms	IAF initialization on CW VPX-1708
BKDB read latency	< 1 ms	SPI Flash at 50MHz
RSA-2048 signature verify	< 5 ms	Hardware accelerated via the on-chip SEC engine
KEY STORAGE & CRYPTOGRAPHY		
NVRAM region size	64 KB	Dedicated TBE region on SPI Flash
Max key entries	100+	Depending on key format
Key type	Public keys (RSA/ECC)	Algorithm agnostic at API level
Crypto engine	NXP SEC engine (CAAM)	Hardware-offloaded cryptographic and hashing operations
Supported algorithms	RSA, ECC, SHA-256, SHA-512	FIPS-validated hardware module
Key write-protection	Hardware (SPI Flash WP)	Applied post-provisioning; BKDB immutable at runtime
BOOT RESILIENCE		
Image slots	2 (Primary + Secondary)	Independent verification paths for each image
Fallback behavior	Automatic	Falls back to secondary if primary verification fails
Bypass path	None	IAF runs pre-kernel; OS cannot skip verification
PLATFORM & COMPLIANCE		
Operating system support	VxWorks 6.9, VxWorks 7, VxWorks 653, HVP	OS-independent design with per-OS implementations
Processor support	NXP Power Architecture and Arm with SEC engine	DO-178C compliance artifacts available for the NXP LX2160A SoC
Safety certification support	DO-178C Level A, IEC 62443-4-2	Full requirements traceability
FIPS alignment	FIPS 140-3	Via the SEC engine hardware crypto module
NIST alignment	NIST SP 800-193	Platform firmware resiliency — protection, detection, recovery
Debug/provisioning backdoors	Disabled	Key loading and test interfaces removed from production build

RTNET CERT

Real-Time Network Stack for VxWorks

A deterministic TCP/IP network stack built for safety-critical embedded systems — typical applications include onboard networking between compute nodes, such as a flight control computer communicating with control surfaces. RTNET provides standard socket-based IPv4 networking with DO-178C DAL A certification artifacts provided through Wind River Professional Services.

Key Differentiators

- **DO-178C DAL A Certification Artifacts —** Each of the stack's three components carries dedicated certification evidence, integration-ready for program use
- **Deterministic by Design —** Kernel-resident, pre-allocated buffer pools, static API-based configuration — no runtime surprises
- **Standards Conformant —** 30+ RFC conformance across TCP, UDP, IPv4, ICMP, and ARP using the standard socket API
- **Flexible Deployment —** Runs natively on VxWorks 7 or within an ARINC 653 partition on Helix Virtualization Platform — including multiple partitions per system

Technical Specifications

Values reflect the current certifiable configuration of RTNET. The certifiable scope is deliberately bounded; features outside the current scope are listed explicitly below.

Specification	Value	Notes
PROTOCOL SUPPORT		
Protocols	IPv4, TCP, UDP, ICMP, ARP	Over Ethernet
Stack scope	Host only	Routing-stack portions of RFCs not applicable
RFC conformance	25+ RFCs	Full conformance for core TCP/UDP/IP/ICMP/ARP; detailed conformance table available on request
ARCHITECTURE & DETERMINISM		
Components	3 (END, NET_BASE, RTNET)	Device interface, buffer management, and network stack — each with dedicated DO-178C artifacts
Execution space	Kernel	Certifiable configuration is kernel resident
Buffer management	Pre-allocated pools	Network buffer pools sized at initialization
Error handling	EDR integrated	Fault conditions raise Error Detection and Reporting exceptions
CONFIGURABILITY		
Socket descriptors	Configurable maximum	Set via configuration API at initialization
MTU	Variable	Per-interface configuration
Routing table (FIB) capacity	Configurable	Set at initialization
Configuration method	API based	Static configuration via initialization APIs
CURRENT CERTIFIABLE SCOPE		
IPv6	Outside current scope	IPv4 only; IPv6 frames are dropped
Multicast/IGMP	Outside current scope	Unicast operation
User-space (RTP) operation	Outside current scope	Kernel resident only
Virtual Ethernet/Virtual Switch	Outside current scope	—
PLATFORM & COMPLIANCE		
Processor support	Arm Cortex-A53, Cortex-A72	Reusable across platforms on these architectures
Deployment environments	VxWorks 7 (native), Helix Virtualization Platform	HVP: runs within an ARINC 653 partition; multiple partitions supported
Safety certification support	DO-178C DAL A	Certification artifacts provided through Wind River Professional Services

HIGH RELIABILITY FILE SYSTEM (HRFS)

Highly Reliable File System for VxWorks

A transactional, power-loss-safe file system for embedded systems where data integrity is non-negotiable. Every write is either fully committed or fully discarded — automatically, with no possibility of corruption reaching the application. HRFS is included in VxWorks; DO-178C compliance artifacts and the corresponding source version are provided through Wind River Professional Services.

Key Differentiators

- **Zero Corruption on Power Loss —** No logically inconsistent state possible; recovery is automatic with no manual intervention
- **Deterministic, Bounded Recovery —** Replays at most 7 inode journal entries — milliseconds, not a scan that scales with disk size
- **Drop-In POSIX Compatibility —** open(), read(), write(), and related APIs work unmodified through the VxWorks VFS layer
- **Certifiable CERT Build —** Bounded-memory, deterministic build supports DO-178C, IEC 61508, and ISO 26262 programs

Technical Specifications

Values reflect distinct build and block-size configurations — the applicable figure depends on which HRFS configuration is deployed.

Specification	Value	Notes
CAPACITY & FILE SIZE		
Max disk size	8 GB – ~32 TB	Block-size dependent (512 B–32 KB blocks)
Max file size — CERT build	only bounded by disk capacity	Fixed at config time for bounded-memory determinism
Max file size — Standard build	only bounded by disk capacity	Block-size dependent; ~4 TB at 4 KB blocks
Metadata overhead	~1.6%	Measured on 64 MB volume/4 KB blocks
FILE SYSTEM LIMITS		
Max open files — CERT pool max	128	Fixed handle pool in CERT build
Max filename/pathname length	251 characters	—
Max hard links per file	65,535	2^{16} limit
Max inodes per volume	~4 billion	2^{32} inode numbering
Reserved blocks	16	Reserved for delete/truncate on a full disk
RELIABILITY & REAL-TIME BEHAVIOR		
Inode journal entries per transaction	7	Bounded — no dynamic growth
Transactions in flight	2	Double buffered; eliminates write-stall bubbles
Journal replay time on recovery	Milliseconds	Bounded to max 7 inodes — not disk-size dependent
PLATFORM & COMPLIANCE		
Supported media	SATA/AHCI, NVMe, SD/MMC/eMMC, raw NAND/NOR, RAM disk	Via XBD block device abstraction
Block size range	512 B – 32 KB	Must be a power of 2
Safety certification support	DO-178C (Read-Only), IEC 61508, ISO 26262	Safety (cert) build is read only; compliance artifacts cover the safety build. A read/write build is available for development.
Encryption/Compression	Not supported	—

WNDRVR

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the digital transformation of mission-critical intelligent systems that demand the highest levels of security, safety, and reliability.