RUNSAFE SECURITY | LYNX

Integrating RunSafe Protect with the LYNX MOSA.ic RTOS

RunSafeSecurity.com

Table of Contents

Executive Summary

Safety- and security-critical systems—from aircraft avionics to medical devices—are under growing pressure. They must operate flawlessly in the harshest environments, comply with the world's most stringent certification requirements, and withstand increasingly sophisticated cyber threats. At the same time, these systems are built on decades-old codebases that cannot be rewritten overnight. While in the business and consumer computing industries vulnerabilities can be resolved as rapid updates pushed out from the cloud, this approach is not viable in high-reliability edge computing systems. Changes to the codebase require a recertification effort and safety-critical embedded software is rarely (if ever) designed to support that type of simple "patching" process.

This white paper introduces a breakthrough integration: **LYNX MOSA.ic™** and **RunSafe Protect™,** the industry's first **DAL-A certifiable, memory-safe RTOS platform.** Together, these technologies establish a defense-in-depth foundation for mission-critical systems.

- **LYNX MOSA.ic** provides a partitioned, modular software framework for mixed-criticality embedded workloads that enforces safety and isolation in multi-core processors at the system level.
- **RunSafe Protect** delivers DO-178C-ready runtime memory safety that can, without source code changes or performance loss, protect against threats posed by the most dangerous class of software exploits.

By essentially changing memory address locations on every boot-sequence, the addition of RunSafe Protect to LYNX MOSA.ic dramatically mitigates security vulnerabilities by preventing access to the software stack. The result is a safety-certifiable cybersecurity solution that protects against both known and emerging unknown threats after the edge computing system has been field-deployed.

In this white paper, we will cover:

- The cybersecurity imperatives facing today's embedded systems
- Why memory safety remains the most urgent and difficult challenge
- How LYNX MOSA.ic and RunSafe Protect address certification, performance, and security in tandem
- The integration benefits of the industry's first DAL-A certifiable, memory-safe RTOS platform
- Real-world deployment examples that demonstrate operational impact

Cybersecurity Imperatives in Embedded Systems

The Critical Nature of Embedded Systems

Embedded systems are the backbone of mission-critical infrastructure, powering everything from aircraft avionics and defense platforms to industrial automation, medical devices, and transportation networks. These systems operate in environments where failure is not an option. Reliability, safety, and security are paramount. Lynx and RunSafe understand the embedded world deeply, with their software deployed for decades in some of the most demanding applications and austere environments.

Vulnerabilities in embedded systems can compromise national security, endanger human lives, and disrupt essential services. As such, embedded platforms must be engineered with resilience at their core, capable of maintaining operational integrity even under adversarial conditions.

Certification and Performance Mandates

Safety-critical systems demand not only uncompromising reliability but also strict adherence to industry certification standards. Lynx addresses these imperatives through a trio of purpose-built commercial technologies:

- LynxSecure, a separation kernel hypervisor that immutably partitions hardware resources to isolate workloads and enforce security policies;
- LynxOS-178, a natively POSIX, ARINC 653-partitioning hard real-time operating system certifiable to DO-178C Design Assurance Level A; and
- LynxElement, a natively POSIX-compatible unikernel designed for deterministic execution and simplified multicore timing analysis, certifiable to DO-178C DAL-A.

Together, these components form a modular and certifiable foundation for embedded systems across aerospace, automotive, industrial, and medical domains. By minimizing attack surfaces, preserving real-time determinism, and supporting reusable certification artifacts, Lynx enables developers to meet rigorous safety and performance mandates without compromising system integrity or development velocity.

Addressing Long-Standing Vulnerabilities in Embedded Software

While embedded software underpins critical systems that power our daily lives, there are inherent code weaknesses that can cascade into widespread disruption, making secure embedded software essential to the functioning of modern society.

Among the most persistent and dangerous flaws are memory safety vulnerabilities, such as buffer overflows. Memory safety flaws consistently rank in MITRE's Top 25 Most Dangerous Software Weaknesses, while CISA and the NSA have warned that they pose a serious threat to national critical infrastructure. The scale of the problem is underscored by industry leaders: both Google and Microsoft report that nearly 70% of their native code vulnerabilities trace back to memory-related flaws.

A widely cited solution is to rewrite code in memory-safe languages like Rust. While effective in principle, this approach is rarely feasible for embedded systems. Legacy codebases are too vast, too costly, and too tightly bound by long product life cycles and rigorous certification requirements to allow for wholesale rewrites. What's needed are immediate, certifiable defenses that can be deployed without disrupting mission-critical operations.

This is where runtime code protections play a critical role. By neutralizing attackers' ability to discover and exploit memory safety weaknesses, defenses like RunSafe Security's Load-time Function Randomization (LFR) provide an actionable and effective way to secure embedded systems today, ensuring resilience without waiting years for a complete language migration.

Industry Context: Why Lynx and RunSafe Matter Now

There are two forces driving the world of embedded security: regulatory and industry mandates and the need to balance security, performance, and certification.

First, embedded systems operating in safety- and security-critical domains are subject to increasingly stringent oversight from regulatory bodies such as NIST, CISA, FAA, and EASA. These organizations mandate the adoption of Secure by Design principles, emphasizing proactive security measures like vulnerability detection and remediation, runtime exploit mitigation, and compliance with standards including DO-178C, DO-297, DO-330, ISO/SAE 21434, and the NIST SP 800 series.

Second, for embedded systems, especially in mission-critical domains, three imperatives must coexist: strong security, uncompromised performance, and certifiability. Yet achieving all three simultaneously has long been a challenge.

- **Performance cannot be sacrificed.** Real-time systems in aviation, defense, transportation, and industrial environments rely on deterministic operation. Even small performance hits can disrupt critical functions.
- **Legacy codebases can't simply be rewritten.** Code rewrites into memory-safe languages or disruptive retrofits are not realistic options for most operational systems. These environments demand continuity, stability, and decades-long lifecycle support.
- **Certification is non-negotiable.** Any solution must align with rigorous safety and security standards—from DO-178C in aviation to ISO 26262 in automotive—without slowing down development timelines or jeopardizing approval.

What's emerging across the industry is a shift toward composable security solutions: technologies that harden systems without requiring invasive code changes or introducing performance penalties, and that can be integrated in ways consistent with certification pathways.

This shift points directly to why Lynx and RunSafe's partnership matters, and how their integration delivers a composable, certification-friendly approach to embedded security.

Strategic Synergy of LYNX MOSA.ic and RunSafe Protect

The integration of LYNX MOSA.ic and RunSafe Protect delivers the industry's first DAL-A certifiable, memory-safe RTOS platform, uniting safety, security, and operational efficiency in a single solution.

- **LYNX MOSA.ic:** Partitioned, modular architecture for mixed-criticality embedded systems.
- **RunSafe Protect**: DO-178C-ready memory safety, defending against runtime exploits without source code changes or performance loss.

Together, they create a defense-in-depth foundation that neutralizes both system-level and code-level threats while preserving real-time determinism and simplifying certification.

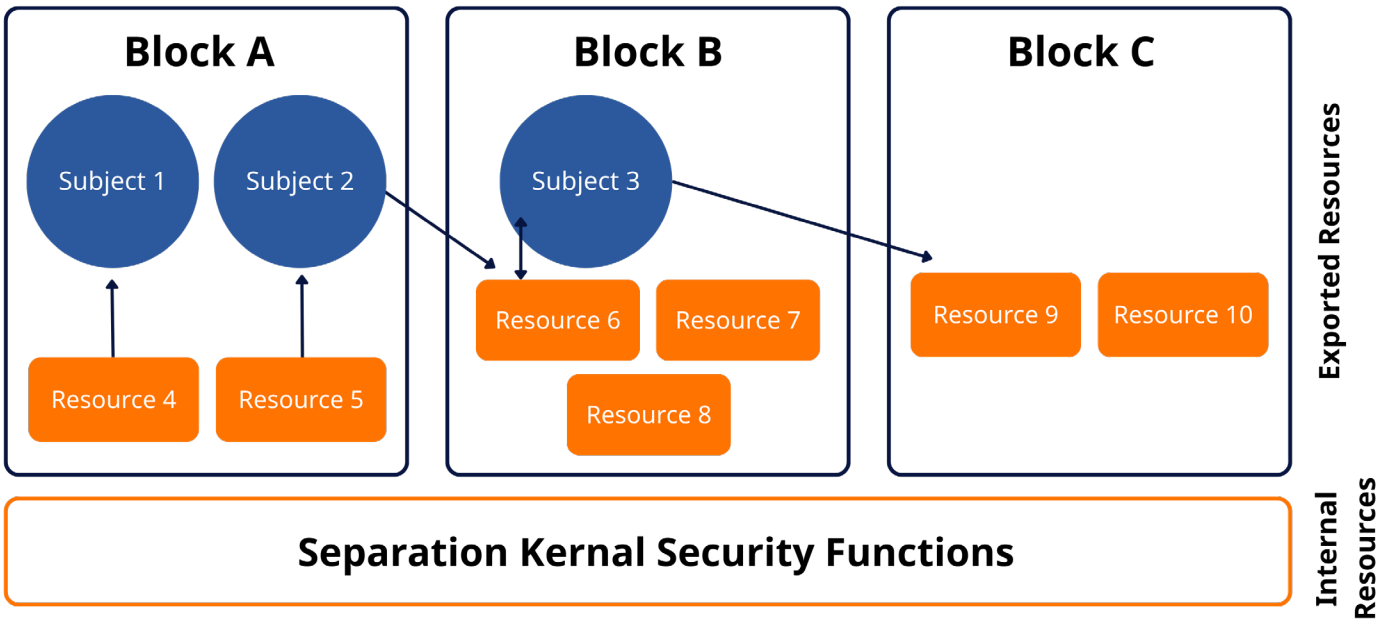
Technical Background: LYNX MOSA.ic

Modular Architecture for Mission-Critical Systems

LYNX MOSA.ic is a modular software framework that enables multiple applications to run concurrently in edge computing devices without compromising system reliability, security, or performance. It can be used to consolidate mixed-criticality workloads on multicore processors by providing robust separation between critical and non-critical functions.

LYNX MOSA.ic redefines traditional multicore architectures to enable developers to construct application-specific software stacks rather than relying on monolithic designs. This modularity allows for precise control over system complexity, scalability, and certification readiness. Acting as an "Integration Center," MOSA.ic unifies diverse tools and runtime environments including bare-metal, RTOS, unikernel, and Linux within isolated virtual machines managed by the LynxSecure™ separation kernel.

This architecture empowers developers to streamline integration, reduce development costs, and accelerate certification timelines across aerospace, defense, industrial, and automotive domains.



Cybersecurity Built into the Core

Security is not an afterthought in MOSA.ic. It's foundational. The platform enforces Secure by Design principles through hardware-enforced partitioning, tickless scheduling, and virtualized subjects running on multiple cores, all orchestrated by the LynxSecure™ hypervisor.

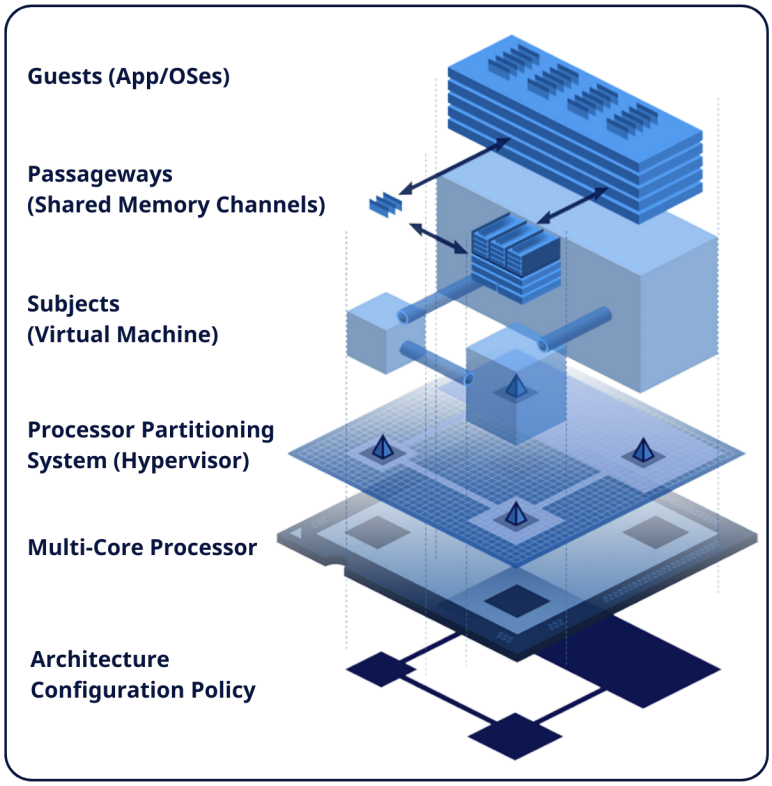
LYNX MOSA.ic provides built-in support for generating Software Bills of Materials (SBOMs), giving teams visibility into their software components. For organizations looking to strengthen their security posture, MOSA.ic.SCA is a premium add-on that integrates advanced Software Composition Analysis (SCA) tools. It enables automated vulnerability scanning within CI/CD workflows, helps manage Common Vulnerabilities and Exposures (CVEs), and continuously monitors for emerging threats across the software supply chain. These capabilities enable proactive risk mitigation and compliance with mandates such as DO-178C, ISO/SAE 21434, and NIST SP 800 series.

By embedding security into the development lifecycle and runtime environment, MOSA.ic ensures that systems remain resilient against both known and emerging threats.

Real-World Applications: Mixed-Criticality

LYNX MOSA.ic is engineered to support mixed-criticality systems, where applications of varying safety and security levels must coexist on shared hardware without interference. This is especially vital in platforms where flight-critical avionics, classified mission software, and real-time GPU powered displays systems must operate in parallel.

MOSA.ic's architecture, powered by the LynxSecure™ hypervisor, enables hardware-enforced partitioning that isolates workloads into virtual machines with tailored resource and access controls. This ensures that high-assurance applications meet DO-178C standards while allowing less critical components to run independently without compromising system integrity or certification.



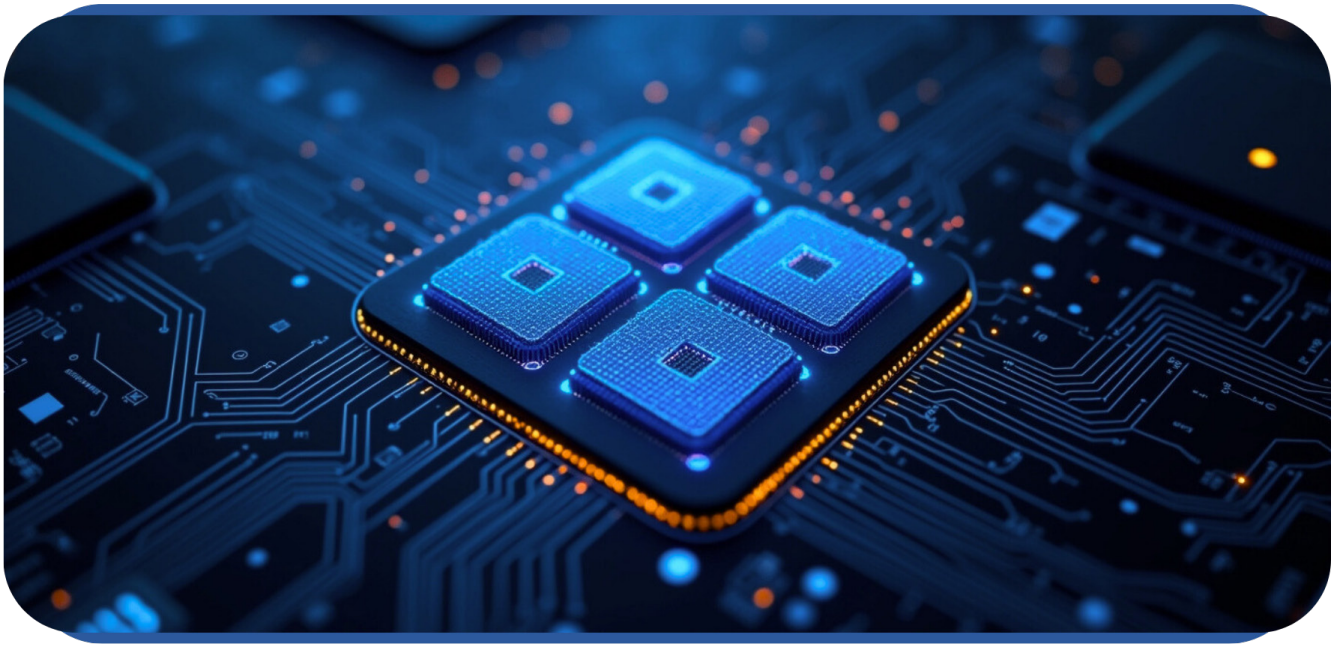
© Lynx

MOSA.ic enables secure data separation and controlled interaction between domains of differing sensitivity. For example, in defense systems, MOSA.ic could allow sensitive operations to run alongside mission applications and logistics software, each within its own isolated environment.

This capability is critical for platforms such as mission computers that leverage MOSA.ic to support bare-metal, unikernel, and RTOS applications across multiple processor architectures. By enabling isolated virtual machines with secure inter-subject communication, MOSA.ic facilitates controlled data exchange while maintaining strict boundaries between domains.

The platform's flexibility also extends to unmanned systems and edge computing environments. One program used MOSA.ic to transform a monolithic mixed-criticality stack into a modular, scalable architecture that improved performance and integration on multiprocessor system-on-chip (MPSoC) hardware.

LYNX MOSA.ic's modularity allows developers to deploy AI-based analytics, sensor fusion, and control logic in isolated partitions, ensuring real-time responsiveness and cybersecurity compliance.



Technical Background: RunSafe Protect

RunSafe Protect is a patented cyber hardening solution designed to defend software against memory corruption exploits, the single most damaging category of vulnerabilities in modern computing. Instead of relying solely on patching, scanning, or runtime monitoring, Protect introduces a proactive defense mechanism called Load-time Function Randomization (LFR) that disrupts the predictability attackers depend on when chaining memory corruption vulnerabilities into reliable exploits.

By ensuring that every program load results in a unique, randomized memory layout, Protect makes file-less attacks like Return-Oriented Programming (ROP) and Jump-Oriented Programming (JOP) attacks virtually impossible to execute at scale. **As a result, RunSafe is able to prevent memory corruption-based attacks, including zero days, targeting 86 of MITRE's Common Weakness Enumerations.**

How LFR Is Different

Unlike legacy mitigations such as Address Space Layout Randomization (ASLR), which shifts the base address of an entire program, LFR works at the function level, delivering far greater memory diversity and resilience. The defense persists across distributed systems as well. Because every protected binary loads differently on each execution, attacks cannot be replicated reliably across devices or environments.

This undermines one of the most powerful tools of adversaries: the ability to scale a single vulnerability into a widespread breach.

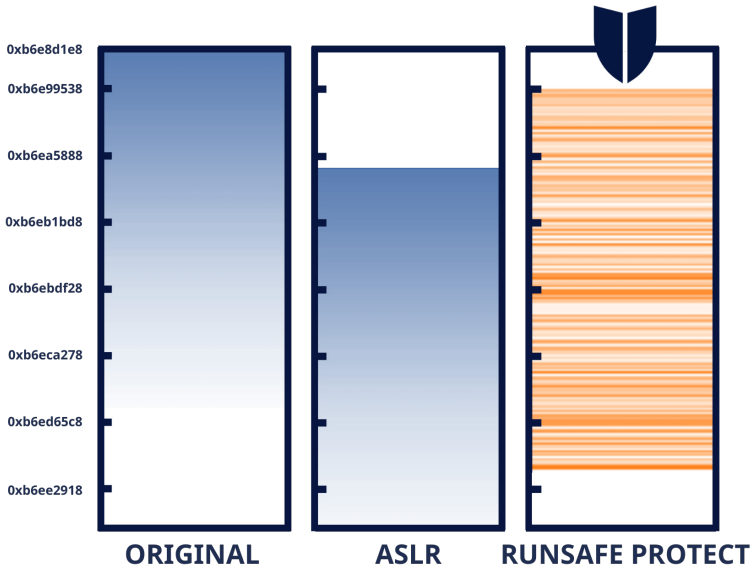


Figure 1: Change in memory diversity with Protect's LFR

At its core, Protect operates as a build-time and load-time defense, requiring no modifications to source code, compilers, or linkers. It integrates seamlessly into existing development pipelines, from enterprise DevSecOps workflows to embedded system builds such as Yocto, Buildroot, VxWorks, and QNX.

During compilation, Protect embeds metadata into binaries that enables RunSafe Protect to rearrange functions dynamically when the program is loaded.

This maintains the intended logic and performance of the application, while simultaneously multiplying the entropy of its attack surface by factorial orders of magnitude. For example, even a program with 30 functions (less than 1/6th of the number of functions in an average program) has over 10^{32} possible layouts, ensuring that an attacker cannot craft a reusable exploit.

Crucially, Protect achieves this security enhancement without degrading performance or disrupting workflows. Benchmark tests (SPEC CPU2006) show negligible overhead—typically less than 1%—and no runtime penalties once execution begins. Because the binary maintains its checksum and digital signatures post-compilation, protected programs can be distributed and validated using the same supply chain and secure boot processes already in place.

This ensures compliance with federal and industry mandates, while reducing the operational cost and complexity of vulnerability management.

In short, RunSafe Protect transforms software binaries into self-defending assets. By embedding LFR directly into compiled code, it removes the attacker's ability to weaponize memory vulnerabilities—whether zero-day or known—and enables organizations to protect critical infrastructure and mission-critical systems with a solution that is simple, scalable, and enduring.

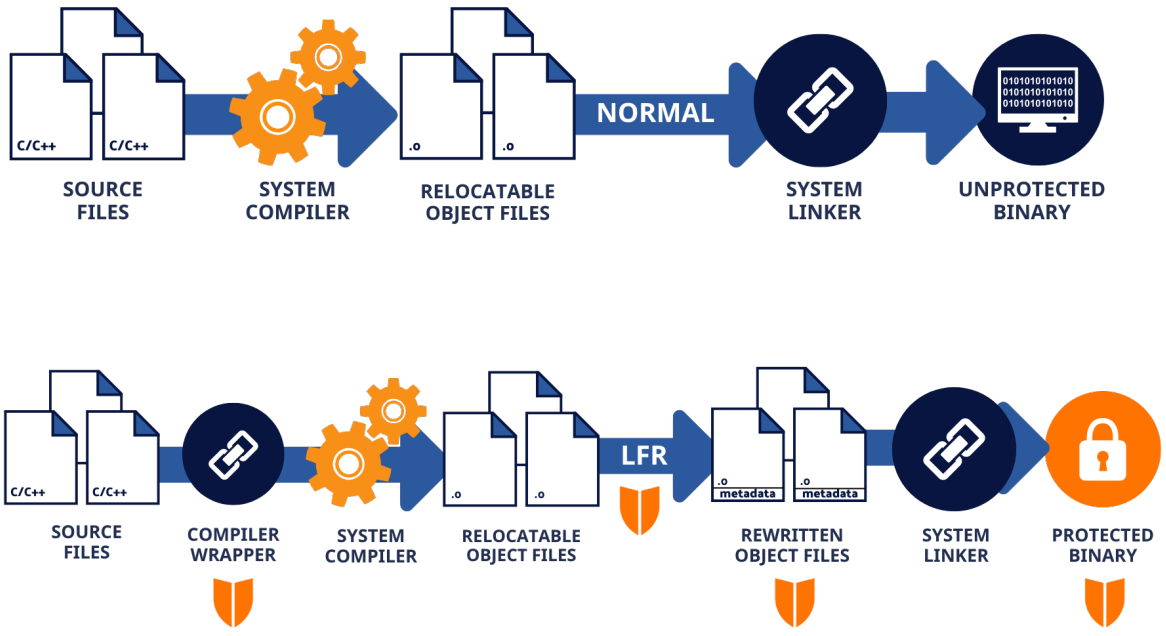


Figure 2: Change in build process to add Protect's LFR

Integrated Solution: LYNX MOSA.ic and RunSafe Protect

The integration of LYNX MOSA.ic and RunSafe Protect creates the industry's first DAL-A certifiable, memory-safe real-time operating system platform. This partnership delivers complementary layers of protection that address security threats at both the architectural and code execution levels.

LYNX MOSA.ic provides the foundational security architecture through hardware-enforced partitioning and isolation while RunSafe Protect adds dynamic memory protection that operates transparently within each partition. Together, they establish a comprehensive defense-in-depth strategy that neutralizes both system-level and code-level attack vectors without compromising performance or certification requirements.

Integration Benefits: The First Memory-Safe RTOS

Unified Certification Path

The integration enables a streamlined path to DO-178C DAL-A certification by combining:

- LYNX MOSA.ic's proven certification artifacts and test suites for system-level safety
- RunSafe Protect's comprehensive DO-178C certification package, including:
  - **Complete Traceability Package:** RunSafe provides integration materials including plans, standards, requirements, the traceability matrix, and verification testing on the target platform for both DO-178C and DO-330.
  - **Parameter Data Item Management:** The seed value used for load-time memory relocation is treated as a Parameter Data Item under DO-178C.
  - **Deterministic Functionality:** Memory relocation is deterministic for any given 64-bit seed value, ensuring predictable behavior while maintaining security through randomization.
- Integrated documentation that demonstrates comprehensive security coverage
- Reduced certification complexity through pre-qualified security components

Operational Efficiency

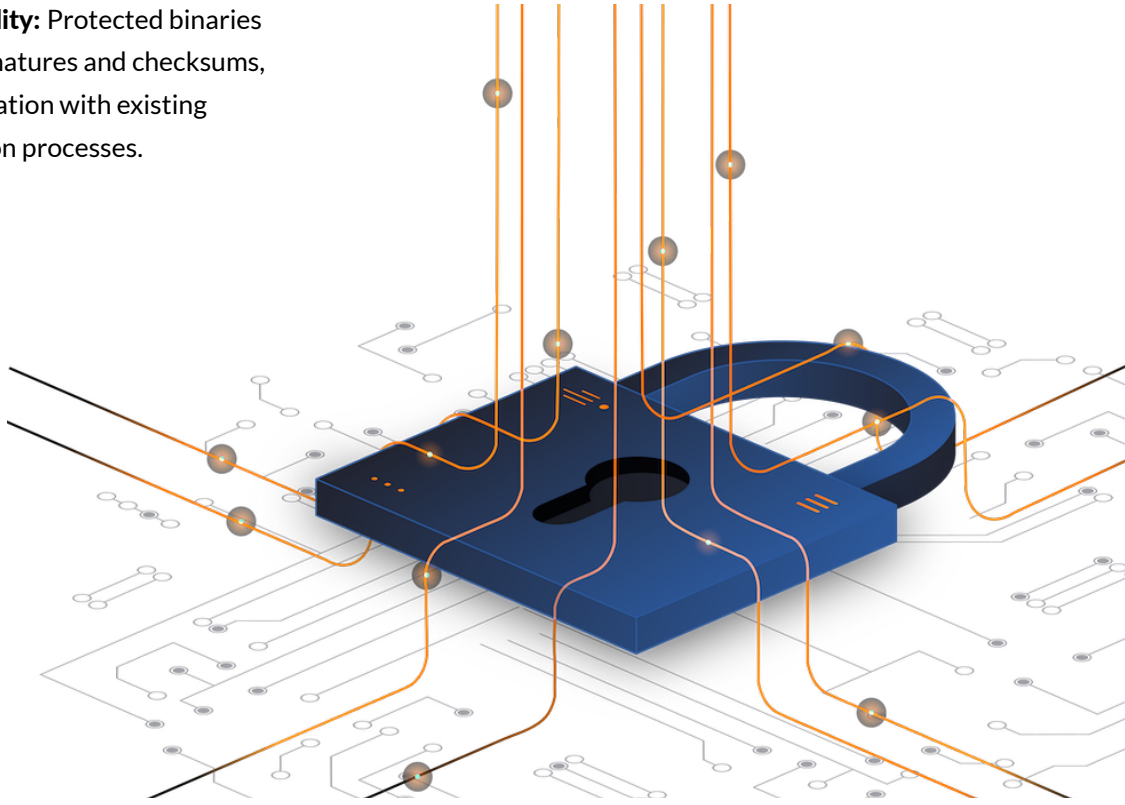
The combined solution delivers operational advantages that traditional security approaches cannot match:

- **No Performance Trade-offs:** Both technologies are engineered to maintain real-time determinism. MOSA.ic's tickless scheduling and hardware partitioning, combined with Protect's sub-1% runtime overhead, ensure that security enhancements do not compromise mission-critical timing requirements.
- **Zero Code Modification:** Development teams can integrate both solutions without rewriting existing codebases. MOSA.ic virtualizes existing applications within secure partitions, while Protect instruments binaries during the build process without source code changes.
- **Supply Chain Compatibility:** Protected binaries maintain their digital signatures and checksums, enabling seamless integration with existing validation and distribution processes.

The integration marks a paradigm shift in embedded security, enabling mission-critical systems to achieve:

- **Comprehensive Protection:** Architectural + memory-level security in one platform
- **Certification Ready:** DAL-A certifiable security meeting the highest safety standards
- **Performance Maintained:** Real-time determinism across all protections
- **Developer Friendly:** No rewrites, minimal workflow changes, familiar practices

As cyber threats intensify and regulations tighten, the combined platform offers a future-proof foundation that scales security without sacrificing safety, performance, or certification.



Real-World Deployment Example

Runtime Application Security in Resource-Constrained Defense Systems

Customer Challenge & Environment

A leading defense prime faced a critical challenge: implementing runtime application protection for a mission-critical embedded system operating under stringent Size, Weight, and Power (SWaP) constraints. The target platform required robust defenses against memory-based vulnerabilities, including code injection, memory corruption, and unauthorized access, while also maintaining deterministic real-time performance essential for operational success.

Traditional endpoint security solutions were unsuitable due to their resource-intensive nature and inability to function effectively within constrained embedded environments. This created a significant gap between the system's security requirements and the technical feasibility of deploying conventional solutions.

Technical Integration Challenges

The core complexity of this deployment involved delivering runtime memory protection that could be certified to DO-178C within an embedded system characterized by limited computational resources and strict real-time constraints. Lynx's MOSA.ic platform provides the modular and certifiable components such as the LynxSecure Hypervisor to host the virtualized embedded operating system, LynxOS-178 in this case, which provided the foundational real-time capabilities and hardware abstraction necessary for the defense application.

Integrating RunSafe's specialized runtime application security solution, which uses Load-time Function Randomization (LFR) to dynamically relocate software functions in memory, simplified coordination to ensure comprehensive protection without exceeding SWaP limitations. Unlike traditional ASLR, LFR offers fine-grained memory layout randomization without incurring runtime performance penalties, which makes it ideal for embedded systems.

Key challenges included minimizing the security layer's memory footprint and CPU overhead, maintaining full visibility into application behavior, enforcing process isolation, and enabling real-time threat detection. These objectives had to be met without compromising deterministic system response or violating operational constraints.

Integrated Solution & Partnership Value

The successful integration leveraged Lynx's OS kernel-level hooks and optimized memory management to enable RunSafe's security solution to monitor runtime application behavior with minimal system overhead.

This close partnership delivered a unified solution. Lynx's deep integration with the hardware platform optimized the performance of RunSafe's Protect security layer, which mitigated threats from both known and unknown vulnerabilities. The result was a secure, real-time embedded system that met the defense prime's mission-critical requirements and ensured operational integrity without compromising timing or resource constraints.

Conclusion

The integration of LYNX MOSA.ic and RunSafe Protect marks a paradigm shift in embedded security: the first platform to combine certifiable safety, uncompromised performance, and runtime memory protection into a single, integrated RTOS. For aerospace, defense, automotive, industrial, and medical domains alike, this means the ability to deploy systems that are resilient against today's threats and ready for tomorrow's regulatory demands.

With Lynx and RunSafe, organizations don't have to choose between security, performance, and certification.

Learn more about Lynx and RunSafe

To explore how this solution can harden your mission-critical systems, streamline certification, and future-proof your security posture, contact Lynx and RunSafe for a technical briefing.

RunSafeSecurity.com

571.441.5076

Sales@RunSafeSecurity.com

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security protects embedded software across critical infrastructure, delivering automated vulnerability identification and software hardening from build-time to runtime to defend the software supply chain and critical systems without compromising performance or requiring code rewrites. The RunSafe Security Platform includes the authoritative build-time SBOM generator for embedded systems and C/C++ projects, automated vulnerability identification and risk quantification, patented memory relocation techniques to mitigate memory-based vulnerabilities, and pre-hardened open-source packages and containers for immediate protection.

Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace and defense, energy, operational technology, industrial automation, transportation and automotive, medical device, and high-tech manufacturing verticals. For more information, visit RunSafeSecurity.com.

ABOUT LYNX

LYNX is a leader in delivering scalable, safe, secure, resilient, and certifiable software solutions for mission-critical edge platforms and secure edge computing solutions for the aerospace, defense, automotive, medical, and commercial sectors. By leveraging decades of expertise and modular, open-architecture technologies, LYNX empowers organizations to develop and deploy advanced real-time platforms that meet the highest performance, safety, and security standards. For more information, visit, www.lynx.com.