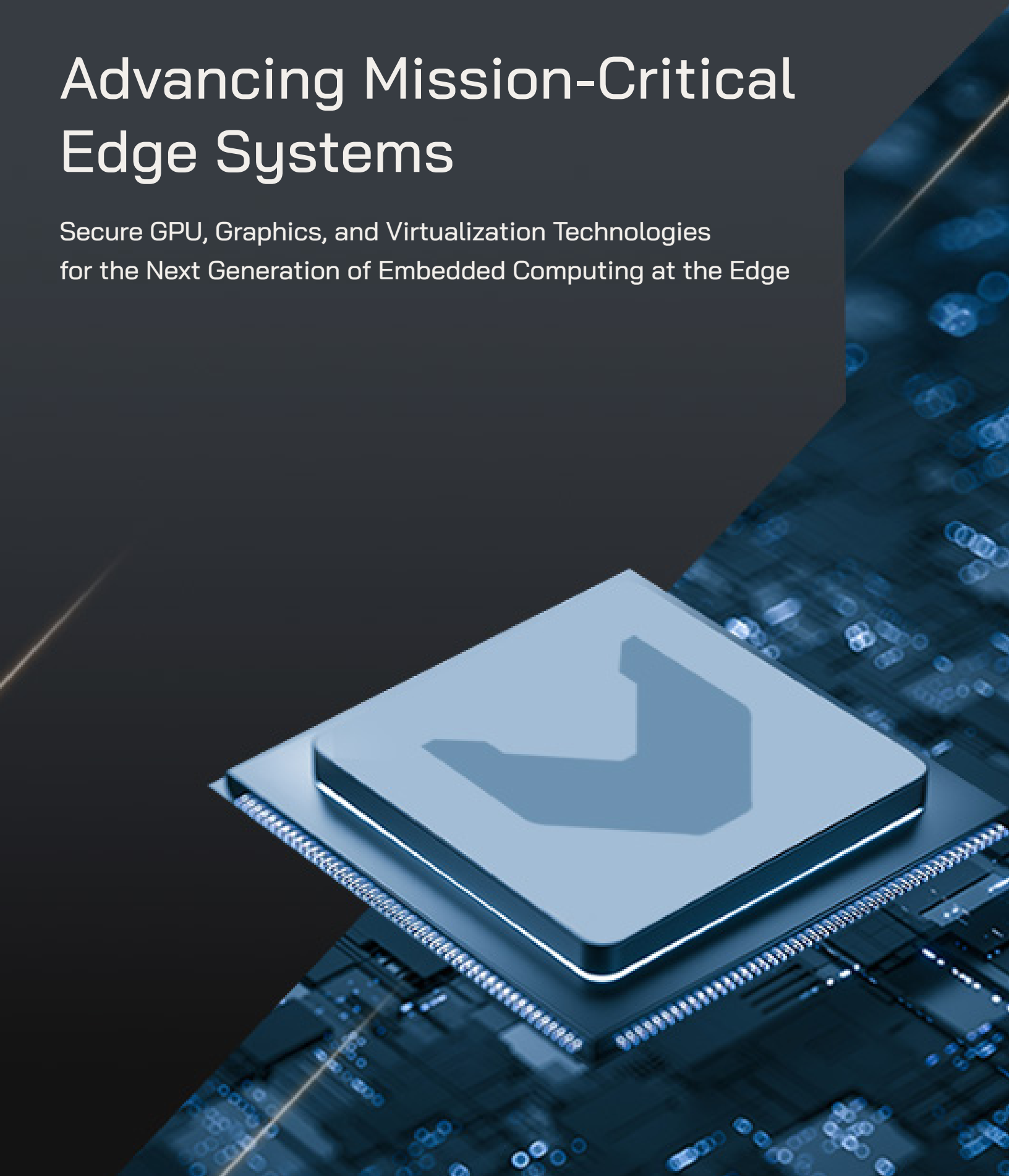
LYNX

Advancing Mission-Critical Edge Systems

Secure GPU, Graphics, and Virtualization Technologies
for the Next Generation of Embedded Computing at the Edge



Across aerospace, defense, automotive, industrial automation, and autonomous platforms, the next generation of embedded systems is being defined by a single challenge: delivering uncompromising performance and certifiable safety on the same piece of silicon. This paper outlines how our patented technologies in secure virtualization, GPU determinism, and graphics interoperability address that challenge, and why our intellectual property portfolio matters to the engineers and organizations building these systems.

The Convergence at the Edge

Modern mission-critical edge systems are evolving rapidly. What used to be a federated collection of single-purpose boxes is becoming a software-defined platform, where a single compute node consolidates workloads that previously lived on separate hardware.

These platforms now routinely combine:

- High-performance multi-core CPUs
- GPU acceleration for compute and rendering
- Advanced graphics stacks driving certifiable displays
- AI inference and multi-sensor fusion
- Hardware-assisted virtualization
- Deterministic, real-time execution

And they are expected to deliver, simultaneously:

- High throughput and low latency
- Strict safety certification (DO-178C, ISO 26262, IEC 61508)
- Secure isolation between mixed-criticality domains
- Predictable, repeatable execution under load
- Decade-plus lifecycle support

Meeting all these requirements on a single platform is not a matter of bolting safety features onto a general-purpose stack. It requires foundational technology, designed from the kernel up, for isolation, determinism, and graphics integrity. That is the problem space our patent portfolio addresses.

Why Our Intellectual Property Matters

Patents in this domain are not trophies. They are evidence of solved problems. Problems that program managers, certification authorities, and systems integrators encounter every day, and that off-the-shelf desktop or mobile software stacks are not designed to handle.

Our portfolio provides three concrete forms of value to customers and partners:

Technical Assurance

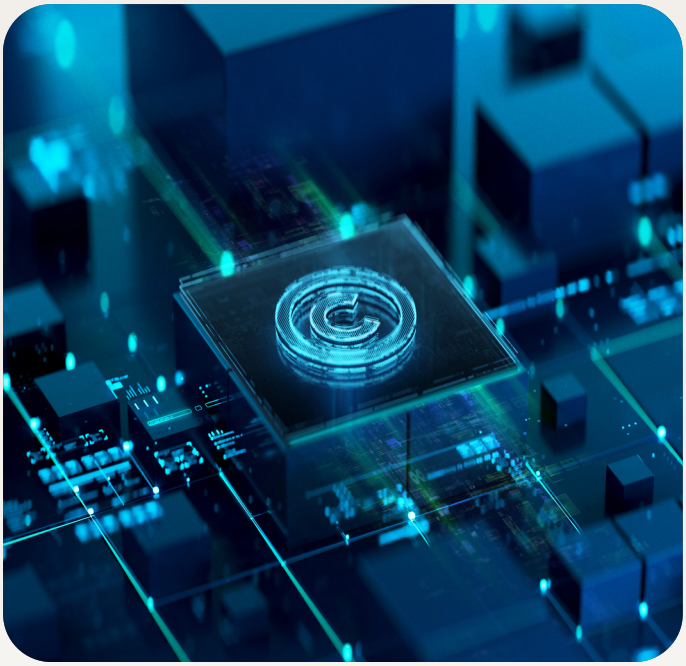
Each granted patent represents a documented, reviewed, and protected approach to a hard problem in secure or deterministic computing. When an integrator builds a safety case on top of our platform, they are building on mechanisms that have been formally described, examined, and recognized as novel.

Supply-Chain and Program Risk Reduction

Long-lifecycle programs, such as aircraft, ground vehicles, industrial systems, cannot tolerate foundational technology that may disappear or be reinvented mid-program. A defensible IP portfolio is a signal of durability: the underlying technology is protected, attributable, and supportable across the life of the program.

Architectural Differentiation

Many problems in this space have superficially similar solutions until you look closely. Our patents define how we approach separation, virtualization, GPU determinism, and graphics API translation in ways that competing implementations do not. That is what allows our customers to ship systems that meet requirements others cannot meet at all.



Enabling Modern GPU and Graphics Infrastructure

Graphics and GPU compute are no longer cosmetic features of embedded systems. They drive primary flight displays, digital cockpits, situational awareness, perception pipelines, and synthetic vision. They must be modern enough to use current GPU hardware, and stable enough to be certified.

Our graphics-related patents address a recurring tension in this market: how to move embedded software onto modern, programmable GPU architectures, particularly Vulkan, without abandoning the OpenGL-based applications, tools, and certification artifacts that customers have invested in for decades.

US 10,497,083 B2 OpenGL on Vulkan Driver Architecture

Systems and methods for using an OpenGL API with a Vulkan graphics driver

As embedded and safety-critical systems migrate toward Vulkan-based graphics architectures, many existing applications still depend on OpenGL compatibility. This patent describes how an OpenGL API can operate efficiently over a Vulkan graphics driver, letting organizations modernize their graphics stack while preserving compatibility with legacy and certifiable software environments.

Key Innovation Areas:

- OpenGL-to-Vulkan interoperability
- Translation and abstraction layers between APIs
- Graphics API compatibility for legacy applications
- Vulkan-based GPU software architectures
- Embedded graphics portability across hardware generations

Reference: https://patents.google.com/patent/US10497083B2

US 10,255,651 B2 Shader-Based Emulation of Fixed-Function Graphics Pipelines

Methods and systems for generating shaders to emulate a fixed-function graphics pipeline

Modern GPUs are built around programmable shader architectures, but a large body of embedded and legacy applications still depends on fixed-function graphics behavior. This patent covers systems for dynamically generating shaders that emulate fixed-function pipelines, enabling legacy compatibility on modern silicon and eliminating dependencies on obsolete hardware features.

Key Innovation Areas:

- Legacy graphics compatibility on modern GPUs
- Modernization of embedded graphics stacks
- Migration paths to programmable GPU architectures
- Reduced dependency on obsolete hardware features

Reference: https://patents.google.com/patent/US10255651B2

US 2019/0073741 A1 EGL Integration with Vulkan Graphics Infrastructure

Systems and methods for using EGL with an OpenGL API and a Vulkan graphics driver

Mission-critical systems require robust interoperability between graphics APIs, display systems, and underlying GPU drivers. This application addresses EGL integration, context and surface management, graphics resource coordination, and Vulkan-based rendering environments, technologies directly relevant to avionics displays, automotive digital cockpits, industrial visualization, and embedded HMI systems.

Key Innovation Areas:

- EGL integration with modern Vulkan drivers
- Context and surface management
- Graphics resource coordination across subsystems
- Display and HMI integration for embedded platforms

Reference: https://patents.google.com/patent/US20190073741A1

US 2021/0109796 A1 Deterministic Execution for Safety Critical Workflows

Methods and systems for time-bounding execution of computing workflows

GPUs and heterogeneous compute platforms are increasingly used in environments where unbounded latency is unacceptable. This patent application addresses time-bounded workflow execution, predictable scheduling, and deterministic compute infrastructure, a foundation for using modern accelerators in autonomous systems, safety-critical AI, and mixed-criticality platforms without sacrificing certifiability.

Key Innovation Areas:

- Time-bounded execution of compute workflows
- Predictable scheduling on heterogeneous hardware
- Bounded latency for accelerated workloads
- Deterministic infrastructure for certifiable edge AI

Reference: https://patents.google.com/patent/US20210109796A1

Secure Virtualization and Separation Kernel Technologies

Modern edge systems increasingly consolidate workloads that used to live on separate hardware: safety-critical control software, AI inference, graphics rendering, networking stacks, and general-purpose operating systems, all sharing the same processor.

This convergence creates real value, but it also creates real risk. A failure or compromise in a non-critical partition cannot be allowed to propagate into a safety-critical one. A high-throughput workload cannot be allowed to starve a deterministic one. And the architecture must be auditable enough to support certification.

The technical answer is not a heavier operating system. It is a smaller, more rigorously designed layer beneath the operating systems, a separation kernel hypervisor that enforces isolation directly against the hardware.

The technical answer is not a heavier operating system. It is a smaller, more rigorously designed layer beneath the operating systems, a separation kernel hypervisor that enforces isolation directly against the hardware.

Our broader portfolio covers innovations across this layer, including:

- Separation kernel hypervisors
- Secure virtualization and domain isolation
- Trusted execution environments
- API interception and behavioral monitoring
- Rootkit detection and prevention
- Mixed-criticality system architectures
- Boot-time integrity and anti-fingerprinting

US 10,061,606 B2 Secure Domain Isolation

Systems and methods of secure domain isolation involving separation kernel features

Covers the mechanisms by which independent computing domains can share hardware while remaining provably isolated from one another, a prerequisite for consolidating mixed-criticality workloads on a single platform.

Reference: https://patents.google.com/patent/US10061606B2

US 11,861,005 B2 Hardware Virtualization and Hypervisor Security

Systems and methods involving features of hardware virtualization such as separation kernel hypervisors, rootkit detection/prevention, and/or other features

Addresses the architecture of separation kernel hypervisors together with the detection and prevention of rootkit-class threats. The combination is central to building platforms that are both certifiable and resilient against modern attack techniques.

Reference: https://patents.google.com/patent/US11861005B2

US 10,051,008 B2 API Interception and Virtualization Monitoring

Systems and methods involving aspects of hardware virtualization such as hypervisor, detection and interception of code or instruction execution including API calls

Covers the ability to observe and intercept code and API execution at the virtualization layer, enabling powerful security monitoring, policy enforcement, and forensic capabilities without modifying guest operating systems.

Reference: https://patents.google.com/patent/US10051008B2

What Our Portfolio Enables

Read individually, each patent solves a specific engineering problem. Read together, they describe a coherent platform architecture for the next generation of embedded computing: one in which a single, certifiable foundation supports modern GPUs, modern graphics APIs, modern accelerators, and modern security expectations, without forcing the customer to choose between performance and assurance.

Concretely, this is what the portfolio supports:

- **Avionics and Defense Displays —** Modern Vulkan-class rendering with OpenGL compatibility, deterministic frame timing, and certifiable display architectures.
- **Software-Defined Vehicles —** Mixed-criticality consolidation of ADAS, infotainment, and safety functions on shared silicon with strong isolation.
- **Industrial and Robotics Platforms —** Deterministic real-time control alongside AI workloads and high-throughput networking on the same node.
- **Autonomous Systems —** GPU-accelerated perception and AI inference with bounded execution and rigorous separation from flight or vehicle control.
- **Secure Edge Infrastructure —** Trusted execution, behavioral monitoring, and resistance to rootkit-class threats at the hypervisor layer.

The systems being built today on these patented technologies are expected to operate for fifteen, twenty, or thirty years. A patent portfolio of this depth is not just protection, it is a commitment to the customers and programs that depend on these platforms over the long term.

Portfolio Index

The table below lists representative granted patents and applications from our portfolio across the United States, Europe, and other jurisdictions. Family members and continuations are listed individually where they reflect distinct grants.

Title	Patent No.
Systems and Methods Involving Anti-Fingerprinting, Separation Kernel Hypervisors, Hypervisor Guest Context, and/or Other Features	US 8,745,745
Systems and Methods for Using an OpenGL API with a Vulkan Graphics Driver	US 9,607,151
Methods and Systems for Generating Shaders to Emulate a Fixed-Function Graphics Pipeline	US 9,218,489
Systems and Methods for Using EGL with an OpenGL API and a Vulkan Graphics Driver	US 10,061,606
Methods and Systems for Time-Bounding Execution of Computing Workflows	US 9,129,123
Systems and Methods of Secure Domain Isolation	US 9,575,824
Systems and Methods of Secure Domain Isolation	US 10,671,727
Systems and Methods of Secure Domain Isolation	US 9,390,267
Systems and Methods Involving Features of Hardware Virtualization Such as Separation Kernel Hypervisors	US 10,095,538
Systems and Methods Involving Features of Hardware Virtualization Such as Separation Kernel Hypervisors	US 11,782,766
Systems and Methods Involving Features of Hardware Virtualization Such as Separation Kernel Hypervisors	US 9,940,174
Systems and Methods Involving Features of Hardware Virtualization Such as Separation Kernel Hypervisors	US 8,745,745
Systems and Methods Involving Features of Hardware Virtualization Such as Separation Kernel Hypervisors	US 9,607,151
Systems and Methods Involving Features of Hardware Virtualization Such as Separation Kernel Hypervisors	US 9,218,489
Systems and Methods of Secure Domain Isolation Involving Separation Kernel Features	US 10,061,606
Systems and Methods of Secure Domain Isolation Involving Separation Kernel Features	US 9,129,123
Systems and Methods of Secure Domain Isolation Involving Separation Kernel Features	US 9,575,824

Title	Patent No.
Systems and Methods Involving Features of Securely Handling Attempts to Perform Boot Modification(s) via a Separation Kernel Hypervisor	US 10,671,727
Systems and Methods Involving Features of Hardware Virtualization, Hypervisor, Pages of Interest, and/or Other Features	US 9,390,267
Systems and Methods Involving Features of Hardware Virtualization, Hypervisor, Pages of Interest, and/or Other Features	US 10,095,538
Systems and Methods Involving Features of Hardware Virtualization, Hypervisor, APIs of Interest, and/or Other Features	US 11,782,766
Systems and Methods Involving Features of Hardware Virtualization, Hypervisor, APIs of Interest, and/or Other Features	US 9,940,174
Systems and Methods Involving Features of Hardware Virtualization, Hypervisor, APIs of Interest, and/or Other Features	US 10,789,105
Systems and Methods Involving Features of Hardware Virtualization, Hypervisor, APIs of Interest, and/or Other Features	US 9,213,840
Systems and Methods of Processing Data Associated with Rapid Snapshot and Restore of Guest Operating System States	US 9,208,030
Systems and Methods of Processing Data Associated with Rapid Snapshot and Restore of Guest Operating System States	US 8,782,365
Systems and Methods Involving Hwardware Virtualization Such as Separation Kernel Hypervisors, Rootkit Detection/ Prevention, and/or Other Features	US 11,861,005
Systems and Methods Involving Aspects of Hardware Virtualization Such as Hypervisor, Detection and Interception of Code or Instruction Execution Including API Calls	US 9,203,855
Systems and Methods Involving Aspects of Hardware Virtualization Such as Hypervisor, Detection and Interception of Code or Instruction Execution Including API Calls	US 10,051,008
Systems and Methods Involving Aspects of Hardware Virtualization Such as Hypervisor, Detection and Interception of Code or Instruction Execution Including API Calls	US 9,648,045
Systems and Methods Involving Anti-Fingerprinting, Separation Kernel Hypervisors, Hypervisor Guest Context, and/or Other Features	US 11,782,745

About This Paper

This document summarizes selected innovations from our intellectual property portfolio relevant to mission-critical edge computing. Patent numbers, titles, and abstracts are provided for reference; for full claims and legal scope, consult the published patent documents on the United States Patent and Trademark Office, the European Patent Office, or Google Patents.

Ready to Revolutionalize Your Mission-Critical Systems?

Contact Lynx today to learn more about how we can empower your success and help you Seize the Edge in every mission-critical endeavor

edge@lynx.com

www.lynx.com