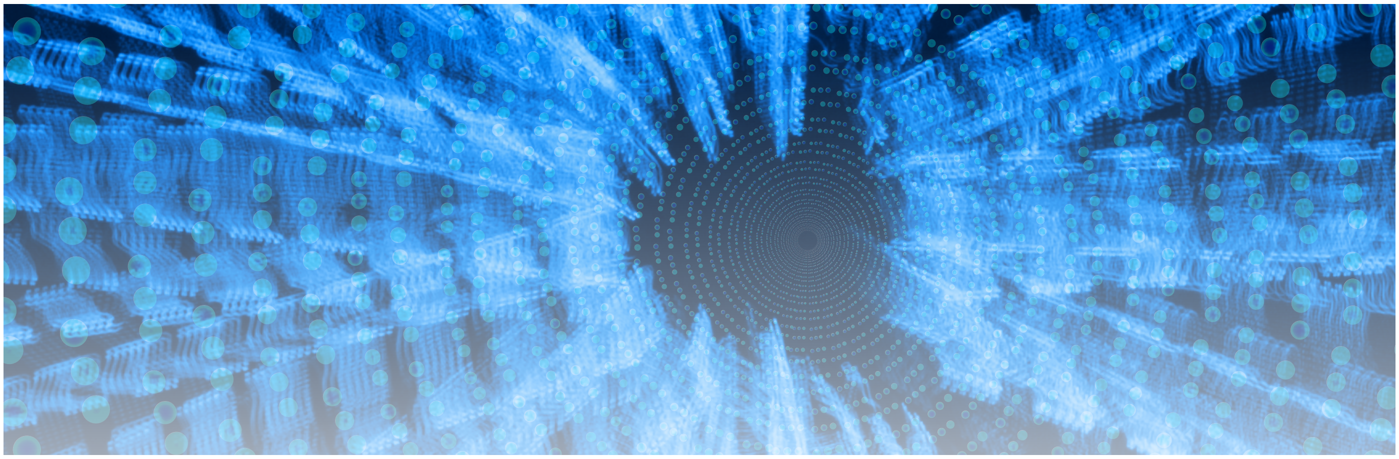
GENERAL DYNAMICS
Mission Systems

OKL4 Hypervisor

Real-Time Embedded Type 1 Virtualization Solution



- Guaranteed and Certifiable Separation
- Low SWaP
- System Reliability and Fault Tolerance
- Basic Integrity and Attestation
- Secure Messaging
- Distributed Power Management
- Tamper Proof VPN and DAR – Android

Overview

OKL4 Hypervisor designed by General Dynamics Mission Systems delivers a real-time embedded Type 1 virtualization solution using our proprietary OKL4 technology. Combined with Lightweight Execution Environments (LWEE) and proven commercial Linux, VxWorks or Android distributions, the OKL4 Hypervisor enables the ability to produce fully integrated, secure, and performance-optimized solutions with guaranteed separation. Applications, functions and processes running on separate dedicated operating systems and hardware can now be consolidated into one intelligent system, allowing for highly scalable and secure systems at a lower cost.

What is a Hypervisor?

A hypervisor is a small lightweight microkernel that utilizes virtualization to isolate and schedule multiple guest operating systems allowing them to run concurrently on a single SoC. Our Type 1, bare metal hypervisor runs natively on device hardware for maximum security and supports a number of proprietary and commercial guest operating systems.

The OKL4 Hypervisor utilizes the ARM MMU to provide guaranteed guest cell isolation enforced by hardware. Unlike other commercial hypervisors, the OKL4 Hypervisor uses a static isolation configuration and policy which can be verified at run time by our proprietary secure monitor. Sensitive functionality can be sequestered into dedicated, isolated virtual machines. Critical functions such as key management or VPN no longer need to run alongside public applications fully exposed to their vulnerabilities.

Securing Today's World

The OKL4 Hypervisor is designed for security. Guest cells are isolated from each other through the security of hardware virtualization and ARM Trustzone can be employed to host a secure monitor to constantly ensure this separation is operating correctly.

OKL4
HYPERVISOR

OKL4 Hypervisor

Low SWAP

OKL4 Hypervisor technology allows the reduction of multiple hardware SoCs into a single, multi-core SoC, saving significant size, weight and power (SWaP). Further, our proprietary hypervisor-based power management functionality allows for efficient management of system resources in hand-held power-sensitive environments. Reliably and securely consolidate your multi-component hardware into a single-SoC product using the OKL4 Hypervisor.

System Reliability and Fault Tolerance

Using OKL4 Hypervisor tools, applications running in guest cells are able to monitor guest cell operation and detect faults. OKL4 Hypervisor guest cells can be stopped, started, and rebooted. Plus, detached image loading can be performed from images stored in system memory or remote storage for on-the-fly software updates.

Our high performance round-robin priority scheduler allows efficient scheduling of all system components, complete with proper load balancing on all available SoC CPU cores. Low latency interrupt processing allows products to meet the tightest of real-time requirements.

Basic Integrity and Attestation

The OKL4 Hypervisor supports attestation, integrity, and signature validation of components running on its platform. Subsequent third-party vendor or customer-supplied solutions will be able to utilize the following OKL4 Hypervisor mechanisms:

- Ability to inspect the memory of other virtual machines, where access control is granted in the system specification.
- Remote attestation for verification of the integrity and security of the operating kernel software.
- General Dynamic's proprietary secure boot technology allows for trusted boot anchored in a hardware root of trust.

Secure Messaging

Inter-VM messaging can be designed to be completely secure – even the hypervisor itself cannot access the data. Message exchanges between two virtual machines are guaranteed private with data isolation enforced by hardware.

Hypervisor Based Power Management

The OKL4 Hypervisor has full support for the extensive power management capabilities of SoCs such as the Xilinx MPSOC Zync Ultrascale^{+}. This allows the use of a secure hypervisor without compromising power management. Control and monitor power management from individual virtual machines including support for CPU suspend as well as dynamic voltage and frequency scaling.

Tamper Proof VPN and DAR – Android

Most current Virtual Private Network (VPN) and Data-at-Rest (DAR) solutions are implemented within the Linux or Android system stack. Running alongside public applications, these components are exposed to the risk of being bypassed or having their private secret keys compromised.

Tamperproof and Non-Bypassable VPN and DAR encryption

Using the OKL4 Hypervisor, these sensitive components can be separated and isolated into dedicated virtual machines. In doing so, these components become non-bypassable and provide the only gateway between the OS system stacks and storage and the actual physical devices:

- Network devices for VPN
- Storage for DAR

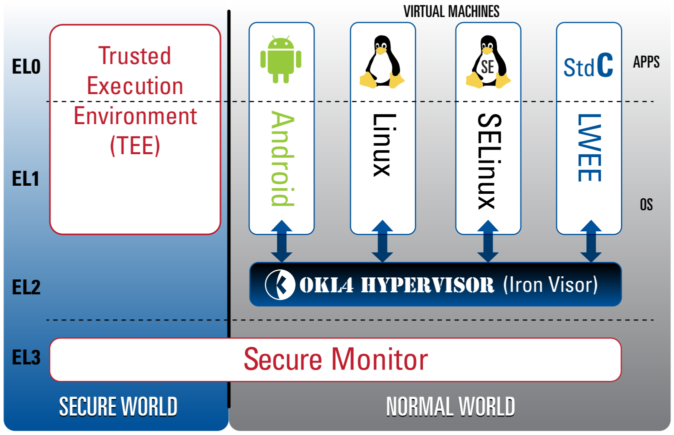
This makes non-bypassability a property of the platform configuration and tamperproof is inherited from the OKL4 Hypervisor's guaranteed domain isolation.

System Security

OKL4 Hypervisor technology can be paired with an ARM Trustzone Secure Monitor for a complete security solution. Periodic and selective invocation of the secure world functionality can provide operation guarantees by measuring the kernel's static data objects. Any compromise in the system kernel can be quickly detected and dealt with by methods dictated by the specific system.

Virtual Services

Our proprietary Virtual Services allow for the virtualization of hardware devices and enables secure sharing between guest virtual machines for device components such as Ethernet, Block and input devices. Dedicate system components to specific virtual machines or securely arbitrate access to the devices – the choice is up to you.



GENERAL DYNAMICS
Mission Systems

OKL4hypervisor@gd-ms.com • www.GDMissionSystems.com/OKL4
US & Canada: 1-877-449-0600 • Global: Your AT&T Country Code + 877-466-9467 • DSN: 312-282-1048