Solution Brief

Edge Computing
Military and Defense

Rugged, High-Performance Processing and Advanced Security for Defense Missions at the Edge

Using Intel® technology, Mercury's rugged edge servers and OpenVPX subsystems deliver superior performance and ironclad security in harsh military settings worldwide.

From ship sensors to satellite telemetry and underground transportation surveillance, access to an ever-widening array of data streams is important for defense operations. Military and security personnel depend on being able to capture, analyze, and gain insight from massive volumes of data as quickly as possible.

Staying on top of the demand to capture and analyze data at the edge requires military computer systems to deliver high-performance edge computing in an array of harsh environments—whether on land, at sea, in the air, or in space. And in many cases, edge computing systems must be lightweight and compact to accommodate extreme space constraints while remaining resilient to g-force, altitude, dust, corrosion, sand, humidity, salt fog, temperature extremes, and even impact.

Mercury Systems is partnering with Intel to develop high-performance, ruggedized edge computing solutions capable of bringing computational power where it's needed: close to the data source. Using the latest Intel® Xeon® Scalable processors and Intel® Distribution of OpenVINO™ toolkit, Mercury Systems has created servers and OpenVPX systems that allow mission-critical edge computing tasks to be carried out under the harshest of environmental conditions.

> *"Intel provides our solutions and customers high-performance processing, storage, and security capabilities. Our partnership allows us early access to the latest Intel® technologies, allowing us to design and deliver the most advanced, secure, dense, and compact solutions with greater performance to our customers."*
>
> —Brian Perry, President/EVP – Processing for Mercury Systems

Challenge: Achieving both performance and security in a single rugged system

To meet defense industry requirements, edge computing servers and OpenVPX systems must perform reliably in a wide range of environments and be optimized for size, weight, and power (SWaP) and cooling. However, many solutions on the market today fail to deliver the high performance required without sacrificing security—and those designed for high security often lack in performance.

Consider also the fast-evolving security requirements of defense applications. To safeguard vitally important intellectual property and confidential data against all threats, edge computing systems must have built-in mechanisms to help prevent data losses and breaches, even in the most remote locales. Mercury Systems' rugged servers and processing subsystems, featuring motherboards designed and manufactured in the US, help safeguard against current and emerging threats to multidomain operations with cryptography, secure boot, and advanced physical protection.

Key industry needs

Exceptional computing performance: Defense applications require rapid, mission-critical decision-making, which makes high-performance computing a must. Rugged edge servers and OpenVPX subsystems must support state-of-the-art artificial intelligence, machine learning, and other compute-heavy applications.

High security: Securing military intellectual property and confidential data from theft or cyberattacks is of paramount importance. To achieve the protection needed, defense computer systems must deliver the highest levels of embedded hardware and cybersecurity features without impacting performance.

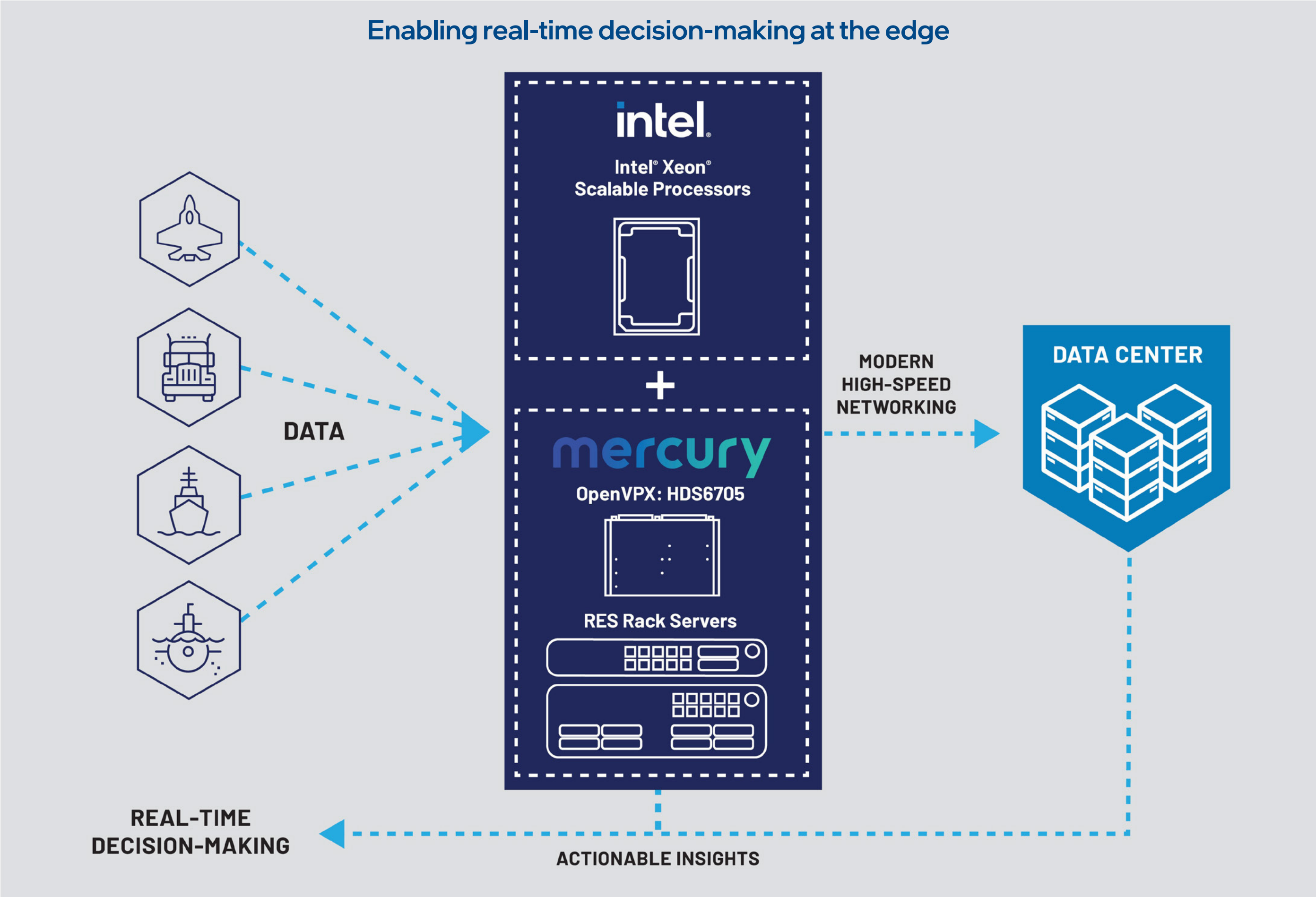
Resilience: Defense edge computing systems can be deployed anywhere in the world for a myriad of use cases. Accordingly, they must be engineered to perform optimally on-site, in the harshest temperatures and weather conditions, all while meeting SWaP specifications.

Mercury Systems' rugged edge servers and OpenVPX subsystems accelerate heavy-compute applications reliably and securely wherever defense missions take them worldwide.

Solution: Mercury delivers both high performance and security without compromise

Mercury Systems' rugged edge servers and OpenVPX subsystems stand apart from the rest by delivering on all fronts. Whether operating separately or in tandem, these lightweight, compact, low-power solutions accelerate compute-heavy applications and perform optimally in the world's most remote and unforgiving environments. As a result, they help enable decision-making in real time while delivering the built-in security and environmental protections required for these and other C5ISR (Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance) mission-critical applications:

- Artificial intelligence (AI)
- Big data analytics
- Sensor processing and fusion
- Image processing
- 5G based
- Signals intelligence (SIGINT)


Enabling real-time decision-making at the edge
intel
Intel® Xeon® Scalable Processors
+
mercury
OpenVPX: HDS6705
RES Rack Servers
DATA
MODERN HIGH-SPEED NETWORKING
DATA CENTER
REAL-TIME DECISION-MAKING
ACTIONABLE INSIGHTS

Mercury's rugged edge compute solutions securely accelerate many different compute-intensive applications on surface, subsurface, airborne, space, and ground-based platforms. They also can help ensure system-wide security by employing cryptography, secure boot, and physical protection.

System integrity is cemented with advanced environmental protections. Peak performance, regardless of dust, vibration, extreme temperatures, or other environmental hazards, is provided through single and hybrid cooling approaches, thermal management, and rugged packaging. This comprehensive approach to system security and integrity allows Mercury edge computing systems to protect critical data while maintaining uptime and performance anywhere they are deployed.

Mercury solutions are also backed by end-to-end security services from the company's systems security engineering teams, including vulnerability assessments, technical training, and product-specific protection schemes based on Intel® Software Guard Extensions (Intel® SGX) technology.

Because Mercury's rugged edge servers and OpenVPX subsystems are manufactured exclusively in the US in AS5553-compliant, IPC-1791- and ISO9001-certified manufacturing facilities, with motherboards and OpenVPX subsystems manufactured in DMEA-accredited facilities, their embedded security protections meet the defense industry's strictest compliance standards.

Mercury Systems' rugged edge servers

Mercury Systems' rugged OpenVPX subsystems

Mercury's rugged edge servers and OpenVPX subsystems are designed to address computing, reliability, space, and security challenges found at the tactical edge and to tackle the most challenging workloads in the most remote environments.

Rugged edge servers

- High-performance big data processing with the latest data center technologies
- Lightweight, 1U–4U, and portable form factors with depth as short as 13"
- Designed and tested to military and industrial environmental standards
- Includes up to 512 terabytes of storage
- Built-in cryptography, secure boot, and advanced physical protection security feature options

OpenVPX subsystems

- Highest AI-enabling processing performance available in OpenVPX
- Open architecture for rapid development, testing, deployment, and modernization
- Built-in cryptography, secure boot, and advanced physical protection
- SWaP-optimized, MOTS+ extreme environmental protection

OPERATIONAL METRICS

Solution	Temperature	Shock	Vibration	Altitude
Rugged edge servers	0°C to +50°C operating -40°C to +71°C storage	X, Y, Z axes 20 g | 11 ms, 1/2-sine pulse (3 positive, 3 negative)	4-33 Hz Sinusoidal Sweep and Dwell	12,500 feet above sea level
Rugged OpenVPX subsystems	-40°C to +100°C operating -55°C to +105°C storage	Z axis 50 g | X,Y axes 80 g | 11 ms, 1/2-sine pulse	0.1 g2/Hz peak | 10G peak to peak | 5–2000 Hz 1 hr/axis	70,000 feet above sea level

Results: Mercury Systems' solutions in action

While Mercury Systems' compute solutions enable secure, real-time, mission-critical decision-making at the edge, they offer other essential benefits as well. For example, in a recent ground radar processing application, Mercury Systems' new RES XR7 rugged rack servers reduced a customer's computing footprint by 36 percent, condensing its 13U rackmount server stack into a 9U rackmount server stack. This transition resulted in even higher system performance as well, thanks to embedded 3rd Generation Intel Xeon Scalable processors and E1.L Intel® SSDs based on enterprise and data center SSD form factor.

Intel Xeon Scalable processors also power Mercury Systems' SWaP-optimized OpenVPX multiprocessing modules. These rugged modules enable multifunction, data center–caliber compute capabilities for applications that must run remotely in the harshest SWaP-constrained environments. As a case in point, Mercury Systems' HDS6705 6U OpenVPX multiprocessing modules measure just 233 mm x 160 mm and are rugged enough to operate inside the nose cone of jets, withstanding severe shock, vibration, and temperature changes while continuing to deliver data center–class processing capabilities. To ensure peak performance when running the most sophisticated C4ISR applications at the edge, OpenVPX multiprocessing modules can be combined with a complementary portfolio of plugin storage, networking switches, GPU boards, other custom electronics, and software to meet mission requirements.

Intel is meeting the evolving needs of security professionals

Intel provides Mercury Systems and its customers the high-performance compute, storage, and security capabilities needed for even the most challenging defense applications. Embedded with 3rd Generation Intel Xeon Scalable processors, Mercury's RES XR7 rugged rack server line reliably accelerates compute-heavy programs that help customers make rapid decisions with confidence wherever they are located. The processors' Intel® Advanced Vector Extensions 512 (Intel® AVX-512) helps accelerate AI workloads for image analysis, audio/video processing, and cryptography. Intel® Deep Learning Boost (Intel® DL Boost) further extends Intel AVX-512 with a new instruction set that increases inference performance on lower-precision data types, such as those used in workloads for image classification, speech recognition, and object detection.

The use of the Intel Distribution of OpenVINO toolkit enables customers to implement a write-once, deploy-anywhere approach to deep learning when using Mercury's systems. Using OpenVINO, Mercury customers can optimize AI applications on Intel® hardware, helping derive even more value from Intel DL Boost.

Ultimately, 3rd Gen Intel Xeon Scalable processors deliver hardware-enabled security to protect data and system integrity all the way down to the chip level. Here's how:

Intel Software Guard Extensions (Intel SGX) helps protect workloads at runtime by creating isolated memory enclaves. This helps make systems more resistant to malware and privileged software attacks.

Intel® Total Memory Encryption (Intel® TME) enables full physical memory encryption. This helps defend against hardware-level attacks such as cold boot, freeze spray, and DIMM removal.

Secure Boot with Converged Boot Guard and Trusted Execution (CBnT) is a fusion of two powerful boot sequences: Intel® Boot Guard and Intel® Trusted Execution Technology (Intel® TXT). These technologies help establish a secure boot and provide the foundation for safe computing.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) provide accelerated data encryption that doesn't impact system performance.

Conclusion: Driven by Intel technology, Mercury's rugged servers and OpenVPX systems are reshaping the industry

Defense missions are mired in complexity and can evolve quickly. Mission-critical decisions must be made as fast as possible and based on real-time data. This requires resilient, high-performance edge computing systems that can be protected by advanced built-in security.

Powered by the latest Intel Xeon Scalable processors, Mercury Systems' rugged edge servers and OpenVPX subsystems deliver the unparalleled performance and security workload-heavy applications require. By reducing latency, maximizing bandwidth, and delivering real-time data and intelligence at the edge, these systems empower customers with the insights they need to make pivotal decisions in the field faster. In partnership with Intel, Mercury Systems has redefined what's possible at the tactical edge, transforming defense missions and helping to safeguard military personnel and assets.

About Mercury Systems

For 40 years, Mercury Systems has delivered military-proven commercial innovations for industrial and aviation applications, as well as safety-critical mission computing for both piloted and autonomous commercial airborne systems. Mercury's trusted portfolio of product solutions and subsystems are purpose-built to meet or exceed the most pressing high-tech needs for these and other edge computing use cases: 1) processing time-sensitive mining data; 2) real-time media broadcasting; 3) surveillance for law enforcement; 4) electronic medical records systems; 5) surveillance for the transportation industry; 6) sensor processing for the oil and gas industry; and 7) processing data in real time for aircraft engine assessments.

mrcy.com

Learn more

Explore Mercury rugged edge servers ›

Read about Mercury OpenVPX subsystems ›

Intel Xeon Scalable processors

With 3rd Gen Intel Xeon Scalable processors, you get high performance, expansive memory bandwidth, and hardware-enabled security features to facilitate and enhance your AI and IoT deployments.

Explore the range of processors ›

Intel Distribution of OpenVINO toolkit

The Intel Distribution of OpenVINO toolkit is free software for developers that accelerates performance, deep learning, and computer vision inference from edge to cloud. This toolkit gives developers access to libraries, frameworks, and pretrained artificial intelligence models to achieve faster time to market for AI vision solutions. It supports heterogeneous processing and asynchronous execution across multiple types of Intel® processors.

Learn about and download the toolkit ›

intel. + mercury

Notices and disclaimers

Intel® technologies may require enabled hardware, software, or service activation.

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

No product or component can be absolutely secure.

Your costs and results may vary.

1221/LM/CMD/PDF