WHITE PAPER

The Military Digital Convergence

Converged digital processing enables next-generation military platforms

IKE SONG
VICE PRESIDENT & GENERAL MANAGER, MERCURY MISSION SYSTEMS
MAY 2018

mercury systems™

Introduction

Commercial digital convergence has created converged media, information systems, smartphones and autonomous vehicles. Digital convergence now has a proven roadmap behind it and is enabling new technology breakthroughs in processing domains everywhere.

Military digital transformation enables platforms to shrink and become more capable and adaptable for mission autonomy. This transformation needs digital convergence architecture to leverage billions of investment dollars made by the commercial sector and coincides with other prevailing trends to make the convergence inevitable.

This white paper describes what digital convergence is, why its benefits are required and why it will become increasingly needed for military applications if we are to maintain a superior defense posture. Early adoption is underway within unmanned land, sea and air platforms, including UAVs. The latter is where the military digital convergence is accelerating the fastest, as extreme-SWaP performance, among other requirements are the prerequisite to success.

How the pilot got us here

Since the Wright Brothers first free-powered flight in 1903, air vehicles have relied upon discrete, analog sensors to supply the information required by their pilots. These sensors and their dashboard-clustered indicators may be regarded as the first and the analog approach to platform situational awareness. The evolution of electronics and more recently, digital processing has augmented these sensors, giving them greater capability.

Fundamental air speed, altitude, pitch/bank, direction and temperature instruments are increasingly being complemented with newer radar, electro-optical/infrared (EO/IR) and other electronically enabled sensors for environmental awareness, threat detection, intelligence, surveillance and reconnaissance (ISR). Although smarter, each sensor is often developed as the response to a specific threat or technology opportunity and consequently becomes a standalone proposition. Sensor integration into existing platforms is a best-fit affair and is characterized as being "siloed" and bolted-on. The absence of a holistic, scalable, refreshable architecture with the ability to efficiently share common resources has meant that each additional siloed sensor relied upon its own proprietary processing chain, comprising of signal acquisition, digitization, processing, exploitation and dissemination functions.

Sensor processing chain

Electronic integration of sensors is implemented via platform data busses, most notably MILSTD-1553 and ARINC-429. Platform processing evolution has developed one program at a time and over countless technical insertions. The result has been the creation of ad-hoc platform processing topologies, which are most suitably described as distributed and federated, comprising of data busses that connect a grid of siloed sensors.

As platforms have become more complex and the array of effectors they can implement has grown, electronics and computers have come to aid the pilot here too. Mission and flight computers help the pilot execute a host of critical functions from avionics, to countermeasures, and to fire control. These effectors, like sensors have evolved and been introduced over time and for similar reasons. Both are integrated into platforms in a distributed, federated manner, which has become the de facto sensor and mission processing architecture for military platform processing.

> ***"Threats are evolving faster than our architectures and processes can respond to" -*** *Dr. Ilya Lipkin, Sensor Open Systems Architecture (SOSA)*

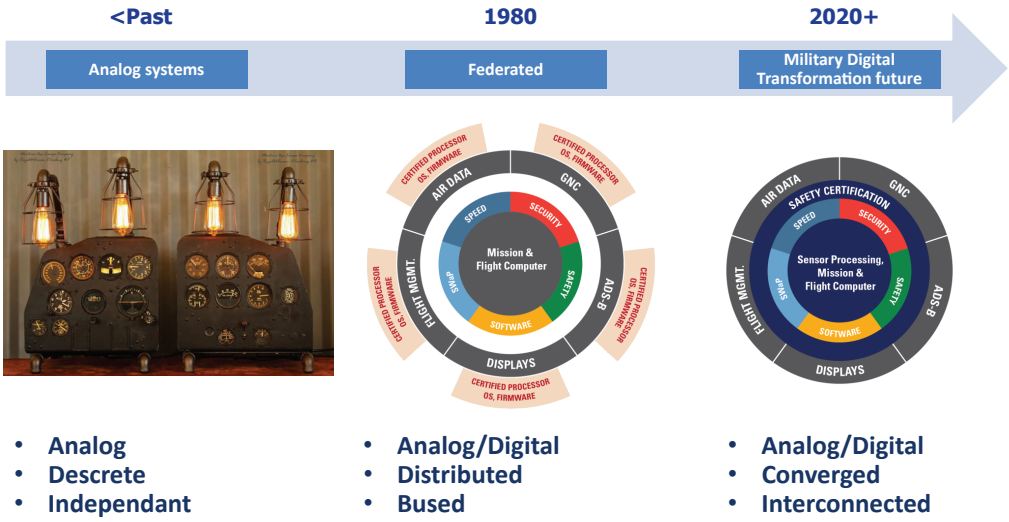
Meanwhile, commercial enterprises have invested billions of dollars defining platform processing architectures that are delivering driverless cars and other platforms that will ultimately dominate many aspects of the autonomous domain with their IP – and they are not using a federated approach to accomplish their missions.

Unmanned vehicles developed for military applications opened the door to this commercial autonomy revolution. Disadvantaged by being first and having to react to a myriad of unforeseeable global threats, military leaders realize that the roadmap they started needs a major recalibration to remain vibrant and effective.

> ***"We spent millions taking a sensor from one platform and integrating it into another…and we do it over and over again".*** *Major prime contractor program manager.*

As in other commercial processing domains, digital convergence will redefine the game as autonomous vehicles from many enterprises and other nations become increasing prevalent. If the same technology can be made ready for defense applications, then agile, adaptable, efficient platform processing will enable autonomous military vehicles to have all the capabilities the best commercial technology has to offer.

Commercial enterprises are focusing their IRAD to develop agile, adaptable and holistic platform processing architectures. Guided by the hindsight obtained by being second to the unmanned vehicle challenge, their platform autonomy solutions emphasize performance, size, weight & power (SWaP), affordability and upgradability which they are achieving through digital convergence. A similar approach, modified for military applications will return the technology initiative back to our military solutions.



- **Analog**
- **Descrete**
- **Independant**

- **Analog/Digital**
- **Distributed**
- **Bused**

- **Analog/Digital**
- **Converged**
- **Interconnected**

Evolution of platform processing, from analog, to federated to digitally converged

The power of digital convergence

In the fall of 2000, the Sharp Corporation released their J-SH04 into the Japanese market. This was the first cellphone with a built-in camera. Seven years later in the US, Apple Inc. released their cellphone with a camera – The iPhone®.

An example of commercial digital convergence – The smartphone

Who, when first learning of a camera sensor being integrated into a telephone considered it a must-have device or even if it was particularly practical? Some may have considered the combination a distraction as size, weight and power all increased, as did the phone's sticker price and complexity. Although the vast majority of us didn't know it then, digital convergence in the communication domain had started. Almost immediately innovation accelerated and now, a decade after Apple announced the iPhone, commercial digital convergence has redefined just about every aspect of our lives.

> ***"If the military doesn't move forward with driverless technology it risks re-experiencing what it did with mobile devices. Warfighters will wonder why they have the technology at home, but as soon as they pass through their base gates, they go back in time a decade."*** *National Defense Magazine, March 2017*

Today, the iPhone and its peers are rugged, miniaturized smart devices that collect sensor data (camera, gyroscope, GPS, etc.), communicate with the world via the Internet, cellular network, and Bluetooth and it is all made possible through adept, converged and miniaturized processing. These devices output to a grid of affects that includes navigation, entertainment, organizers and a secure means of payment, to name a few. An idea that started half-a-world away, less than two decades later has changed information sharing, communication, what is possible and the lives of nearly everyone, everywhere.

Collectively the capabilities delivered by digitally converged smartphones nullify the original nay-sayers' concerns of size, complexity, affordability and desirability. This is the power of digital convergence.

Now that the digital convergence roadmap has been established, other industries are applying a similar strategy to profoundly transform their domains. Whether it is in the industrial internet of things (IIoT), smart buildings or automated distribution systems, digital convergence is everywhere. However, nowhere is this transformation more apparent than in the domain of autonomous cars and smart vehicles.

> ***"The convergence of new technologies may allow autonomous, small, smart and cheap weapons based on land, sea, or air to dominate combat."*** *– CATO Institute*

For autonomous vehicles to deliver their promise of safe, efficient travel it requires a convergence of extensive sensing, cognitive decision making and safe effector implementation. With big financial bets being placed by Google, Apple, Amazon, Uber, Tesla and the automobile industry as a whole, the momentum of innovation has become unstoppable. With a proven technology roadmap, the availability of powerful processors and sensors, vehicle autonomy has passed its technological event horizon. Many next-generation flying taxi startup companies are working towards similar commercial solutions that fly without pilots.

Military digital convergence concept

Digital transformation is not a new concept in defense. It has its roots in the digitization of sensor technologies. This transformation needs next-generation architecture that converges the C4ISR data on and off military platforms. What's new is the amount of data being collected by an ever-growing fleet of interconnected platforms and the promise of that data to facilitate new missions both on and off platform. Military digital convergence is the roadmap to realizing that promise.

Group 3 UAV

> ***Sensor processing characteristics***
>
> *Sensor processing subassemblies are powerful, real-time processing engines that turn the large data streams from complex sensors like radars and EO/IR focal planes in to information. Sensor processing is required to be trusted and secure to prevent malicious content and making them resilient to reverse-engineered and unauthorized data access efforts. Security hardening has often been side-stepped through DoD waivers in the interest of expedience. In 2016, the DoD stated that security has become so paramount that waivers for systems going oversees will no longer be issued. Processing security and trusted data in the modern world is so important, it trumps everything and it has to be built-in to every military processing subsystem.*

The main thesis of digital convergence is centralizing the compute resources of all the avionics sensors into a combined mission and flight computer. The result is a software-defined architecture that is independent of the hardware. This centralized processing hardware can be upgraded much more frequently than the sensors to accommodate enhanced processing techniques and expanded mission profiles. The software that runs on the central computing resources would be similar to an app running on a smart phone.

Mercury OpenVPX mission computer (ROCK-II)

Mission computing characteristics

Mission and flight computers must be proven to be intrinsically safe to meet commercial flight safety requirements if they are to be operated in commercial airspace. Regulated by the European Aviation Safety Agency (EASA), Federal Aviation Administration (FAA), Joint Aviation Authorities (JAA) and Transport Canada, compliance to this requirement is certified to various Design Assurance Levels (DAL) depending upon the level of system criticality. Mission processing is characterized by its high reliability and determinism, which collectively constitutes inherent safety. Safety is mandated for mission-critical applications (e.g. avionics, vetronics, fire control, displays, etc.) and has to be certified for compliance.

The hardware architecture of the central compute resource would include the redundancy required for flight safety certification. The system would be segmented into different zones, each of which could have a different level of safety and security.

Distributed, federated platform processing limits

Technology is advancing faster than ever and the pace will continue to accelerate. Today's federated approach to platform processing is insufficiently agile to offset fast evolving challenges and doesn't meet SWaP performance requirements, especially in regards to smaller UAVs. Further, the federated approach is inherently complex, intrinsically risky, slow to deploy and is difficult to make safe and secure.

Five key conditions limit the federated platform architecture and each one of them is becoming increasingly expensive to accommodate:

- **Sensors** are predominantly, siloed capabilities requiring custom integration into their respective platforms. There are few standard interfaces, protocols or interoperability considerations built in to them and they are not easy to reuse.
- **Duplication** as each siloed sensor invariably has many support functions that are duplicated between sensors, including positioning navigation, timing, analog/digital conversion and processing.
- **Security** is implemented to varying degrees across the platform's processing subassemblies, with technologies from multiple vendors. This creates large attack surfaces and many needless seams and nodes. Making these complex networks and processing resources secure is inherently complicated and difficult.
- **Safety** certification is required for most mission and flight computer functions to prove that they are intrinsically safe and reliable. With so many standalone sensors and processing subassemblies, safety certification is also needlessly complicated and difficult to implement.
- **Performance** is restricted as data is limited to the platform's data bus and proprietary sensor I/Os, many of which are antiquated, putting a cap on platform processing capability and bandwidth. Compute refreshes are further hindered limiting the platform's processing ability to execute new missions.

The federated approach to platform processing is buckling faster, and as technology evolution accelerates and commercial solutions become available, it becomes evermore ineffective making a dominant defense posture increasingly elusive.

"The modern consumer electronics industry moves at a breakneck pace. Each generation of smartphone brings such startling innovation that we forget what was deemed impossible just a few years prior. By contrast, aviation moves at a broken pace. Safety is rightfully paramount, but well-intentioned regulation has overburdened development processes." *Ryan Braun, Chief Operating Officer, uAvionix Corporation*

Technology and threat countermeasure evolution has enabled analog platform processing to morph into today's federated architecture, delivering improved capability along the way. The evolution has largely been implemented through the introduction of processing subsystems behind smarter sensors and the addition of mission and flight computers to aid the pilot to utilize the array of mission effectors and countermeasures. Without a holistic, top-down approach to implementing and integrating these functions, the result has been a dramatic increase in duplication and complexity, while performance and capability are progressively becoming missed opportunities.

Analog and federated architectures

A typical airframe now has more than fifteen discrete sensor and mission processing subassemblies on it. For reliability and flight certification, each of these processing subsystems may have one or more similar redundant backup units, meaning an airframe today may be loaded with over thirty processing subassemblies, many have a lot more.

Event horizon for military digital convergence

Sensor integration requirements have become so complex they are limiting platform capability and performance in all domains. In effect, the tail is wagging the dog.

As technology developments come online from the commercial sector and the modern threat environment gets increasingly technologically sophisticated, the need to deploy automatous platforms as a force multiplier is becoming an imperative. The DoD's embrace of modular open system architectures (MOSAs) for affordability, scalability, interoperability and capability will aid the transformation from a federated processing architecture to digitally converged platform processing for next-generation missions.

For the DoD, the transition from federated to digitally converged will require the integration and certification of four critical commercial technologies: multicore microprocessors and operating environments, a verifiably secure-to-safe boot pipeline, mixed assurance display and I/O processing, and finally software-defined PNT. Multicore microprocessors are the backbone of digital transformation across many industries. The ability to rapidly segment and deploy processing resources to a variety of applications simultaneously is a fundamental building block of convergence.

The challenge in safety-critical applications is to ensure that the segmentation of processing resources can be verified to a particular Design Assurance Level (DAL) in both hardware and software. Software segmentation is governed increasingly by a basket of commercial technologies known as hypervisors, but there are only a handful of hypervisors that can be certified for safety-critical operation.

Convergence both concentrates the security risk while simplifying the implementation, management, and upgradeability of a safety-critical platform. As such, the DoD will need access to a composable security architecture where components can be segmented in time and space to facilitate a secure-to-safe transition before safety-critical operation.

Digital convergence aggregates the processing associated with remote applications, creating efficiencies that benefit the platform and its mission. For the revolution in autonomy, the critically important remote applications to be converged are sensors. To reap the benefits of commercial sensor technology, the mixed assurance capabilities need to extend into the I/O architecture. Finally, PNT is one of the most important building blocks to the future of autonomy and a digitally converged architecture in avionics. As platforms incorporate more and more sensors to improve situational awareness and safe operation, the fusion of that information with PNT will foster the development of software-defined PNT solutions that are reliable and robust enough while being much more cost-effective than today's distributed PNT subsystems.

A digitally converged future can be depicted as a "grid" of critical onboard functions that share a common resource -- a converged flight control and mission processor. The concept of a grid is used to depict the importance of peer relationships between critical sensor and mission functions such as sensors, weapons, data storage, displays, and communications. A sensor and mission processing grid generates a fused perspective that can be used to execute missions, and the converged flight control and mission processor is responsible for fusing the sensor data safely and securely to effect an outcome. As such, the grid encompasses three classes of processing functions: sensors, effectors, and C4I. Each class of processing has unique safety and security requirements. Hence, the need for a composable approach to a next-generation, safe-secure processing architecture.

There are no overarching standards bodies governing the sensor and mission processing grid, but a handful of critical ones are attempting to address aspects of the interoperability and verification challenge. The Sensor Open System Architecture (SOSA) Consortium defines the architecture, electrical/mechanical, hardware, software and interfaces for radar, SIGINT, EO/IR, EW, PNT and comms processing. It has been adopted by the US Army, Navy and Air Force and has interoperability with FACE, OMS, SPIES, MORA, Redhawk, CMOSS, VICTORY and VITA standards. Unlike previous open system architectures (OSAs), SOSA builds in robust security and is packaged within a business model to ensure that DoD, warfighters, prime contractors and industry all get what they want and need for success.

The SOSA approach decomposes existing infrastructures and recomposes them as more capable and adaptable solutions made from common, interoperable building blocks. The effectiveness of this approach is defined by the benefits it delivers which are measured in terms of the time taken to implement new missions – from the current months and years to weeks, even days depending upon the type of mission.

The SOSA Consortium is creating open system reference architectures applicable to military and commercial sensor systems and a business model that balances stakeholder interests. The architectures employ modular design and use widely supported consensus-based, nonproprietary standards for key interfaces that are expected to:

- Reduce development cycle time and cost
- Reduce systems integration cost and risk
- Increase commonality and reuse
- Reduce sustainment and modernization cost
- Support capability evolution and mitigate obsolescence
- Enable technology transition
- Facilitate interoperability
- Isolate the effects of change

A key part of SOSA's success has been the ability to decouple the sensor from its siloed infrastructure as required by the decomposition phase of implementation. Subsequent recomposing of the sensor as a decoupled, plug-in line replacement unit (LRU) enables platforms to be upgraded as required and for technology to be relatively easily reused. Sensors have

lifetimes spanning decades, whereas processing resources more closely follow Moore's law and require refreshing every few years. Decoupled LRUs can be refreshed independently of each other enabling both sensors and processors to be upgraded as determined by their respective life cycles. At the time of this whitepaper, the first SOSA implemented LRU sensors have been delivered by two leading sensor manufacturers who recognized the efficiency of this approach.

SOSA successfully decouples sensing from the processor, but the sensor and mission processing grid encompasses other processing functions including effectors and C4I. This white paper introduces and discusses a next-gen processing architecture that successfully decouples all three.

Autonomous military platforms

Digital convergence decomposes a platform's sensor and mission processing components and recomposes it as a harmonized, single entity of pre-architected, interoperable building blocks, or LRUs. This top-down approach enables processing resources and decoupled sensors to be scaled, quickly reconfigured for new missions, facilitate simpler hardware technology refreshes and makes platform miniaturization possible through big jumps in SWaP performance.

Digital convergence allows platform providers and integrators to implement, upgrade and scale their solutions quickly in a low-risk environment leaving sensor providers to focus on their value proposition by continuously optimizing SWaP. DoD gets more affordable, scalable and interoperable platforms that are more capable and easier to keep current with the most contemporary technology. Our warfighters get quick access to the best commercial technology to keep them safe while restoring our national defense initiative.

Benefits of Digital Convergence

Better performance, more features:

- Fewer sensors, support devices & computers for big jumps in SWaP performance
- Simpler sensor implementation architecture for faster and higher DAL certifications
- Single computing node for greatly reduced cyber-attack opportunity
- Protect all critical information in a single area with secure boot

More computing power:

- Increased capacity and functionality from sensor fusion and machine learning
- Tech refreshes increase capability for all sensor, mission and flight computers at determined time frame

Lower costs and risks:

- Cost efficiency through consolidated computing
- Safety and security in one system
- Decoupled sensors for mission agility, upgradability and reuse
- Timely upgrades through decoupled processing and sensors
- Reduced risk, development and deployment time through common, proven architecture, platform independence & centralized control

Digital convergence enables platform integrators to concentrate their engineering resources enhancing capabilities and the selection of better LRU payload configurations. Rather than debugging sensor ports to the compute environment, platform integrators can develop their applications and offer solutions that feature software-defined solutions for the greatest mission capability and agility.

Gray Eagle UAV EO/IR (camera) gimbal

Digitally converged platforms are versatile. Existing sensors (e.g. a camera) may be upgraded (from surveillance to weapon control) by refreshing its processing capability and safety certification. As in the commercial domain, digital convergence enables capabilities to augment. Augmentation includes sensor fusion where, for example, a radar display may include IFF, weather and EO/IR camera imagery superimposed over it providing a much richer situational awareness.

Digital convergence centralizes the processing needs of platform mission and sensor processing functions for greater processing performance and ease of upgradability. Centralized processing increases SWaP performance by magnitudes as inefficient and duplicated processing resources are recomposed as scalable, agile, adaptable single entities composed of interoperable LRUs. A single processing entity, which may be duplicated for reliability (redundancy) is simpler to flight safety certify and harden for security than a much more complicated, multi-node, federated solution.

With convergence, though, there is some risk to determinism and therefore precision. Design Assurance Level (DAL) defines the process of demonstrating that hardware (DO-254) and software (DO-178) will operate in a precise and predictable manner. In effect, they are and can be shown to be intrinsically safe and reliable by the European Aviation Safety Agency (EASA), Federal Aviation Administration (FAA), Joint Aviation Authorities (JAA) and Transport Canada. The technology being developed for commercial autonomous vehicles, the availability of segmented processors and memory, multi-safety and security partitioned processing subassemblies and decoupled sensors means the major hardware ingredients required for digital convergence are currently accessible and will become increasingly capable and available.

Autonomy has drastically augmented the need for on-board sensors and by extension the amount of sensor processing. The future of "smart" missions depends on on-board processing keeping pace with the commercial pace of change in technology, including the revolution in cognitive computing. Processing resources should be separable, scalable, safe, and secure.

To implement a military digital convergence requires a holistic, top-down approach to fuse secure and trusted sensor processing with mission processing. Mission processing needs to be safe, reliable and deterministic and shown to be so which is a public affair (third party verification). The ability to seamlessly fuse together varying levels of security and safety certification into a single processing unit is pivotal for digital convergence, and by extension viable autonomous military platforms.

Mercury's military digital convergence qualification

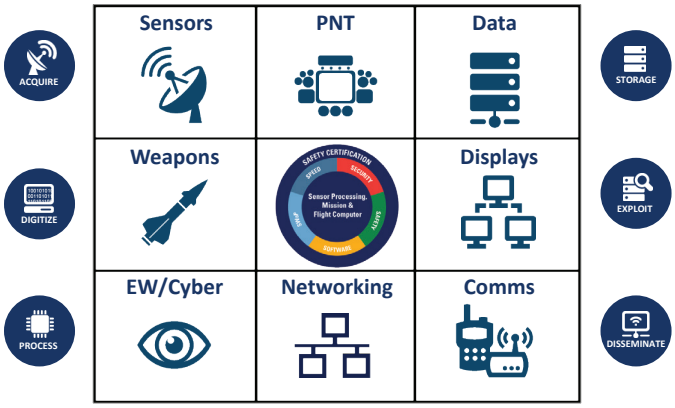
Innovation that scales and adapts

For over three decades Mercury has designed and manufactured the most powerful, contemporary embedded sensor and mission processing solutions for the defense and avionics industries. Mercury pioneered an open system approach to building these systems, first with the creation of real-time switch fabrics (RACEway, RACE++ and Serial RapidIO) that ran on then industry de facto embedded processing open system architecture (VME). More recently, Mercury led the creation and adoption of OpenVPX™ (ANSI/VITA 65-2010), which has become the follow-on and current de facto rugged embedded digital processing modular open system architecture (MOSA) standard.

"Affordable mission effectiveness through systematic reuse of technology." - *Dr. Ilya Lipkin, Lead Manager for SOSA*

OpenRFM™ OpenVPX

Mercury is applying the discipline of standardization, interoperability and proven technology reuse in the RF domain, as we did in the digital realm, though OpenRFM™. OpenRFM leverages the best, proven technology enabling RF/digital solutions to be quickly engineered, manufactured and tested for lower-risk and greater program velocity. For the first time OpenRFM (RF), combined with OpenVPX (digital) has standardized the design, interoperation and the manufacture of processing solutions across the whole sensor processing chain - from RF acquisition to digital processing and back to RF/analog/digital dissemination.



Mapping the sensor chain to the mission processing grid

Mercury's next generation defense electronics business model

Mercury is following the digital convergence roadmap and applying our next-generation defense electronics business model to produce processing solutions that leverage the best commercial technology, making it ready for military applications. We are connecting the grid of sensors with the grid of effectors in one open system processing box. This removes the limits of the federated approach and vastly reduces the number of processing subsystems on a platform.

Military Digital Transformation - Five Keys to Success:

- Don't fear security
- Exploit multicore processors and Moore's Law – Refresh at the speed of technology
- Deploy safe Ethernet
- Integrate entire platform, from sensors to mission management
- Greater on-board video processing and exploitation

Mercury's next-generation defense electronics business model enables us to function with the agility of a commercial company while equipping us with the practices and infrastructure that compliments a modern defense industry. We consistently invest up to 13% of our gross revenues into focused IRAD. We anticipate future defense electronics requirements and develop technologies and capabilities that intersect with these needs so we have the technology and manufacturing capabilities ready. Our investments have produced the broadest, most contemporary portfolio of pre-engineered digital and RF interoperable building blocks across the whole sensor and mission processing chains.

Mercury technology investments for military digital transformation

- Industries' most proven embedded security – BuiltSECURE™
- Top down approach to highest level safety certification - BuiltSAFE™
- Secure and deterministic Ethernet – Secure 1553/ARINC bus
- CANGuard™ – Secure CAN controller area network – Secure SSDs & memory
- Broadest, most contemporary portfolio of interoperable OSA building blocks
- Most I/O interfaces
- Innovative safety critical solutions – CPU rendered graphics
- Open software, middleware and APIs for relatively easy tech refreshes
- Best open system cooling for reliability, performance and processing density
- Rugged, RF/electronic miniaturization with SiP & substrate-stacking for extreme SWaP
- System management and efficient power management
- Long life cycles and product support
- OSA (VME, OpenVPX, VNX), hybrid and custom architectures
- Secure, trusted DMEA facilities and robust IT cyber posture

Built-in security and trust

Mercury builds in a layered and customizable or turnkey security framework for system integrity required for modern defense processing applications. Our proven built-in security framework spans software, firmware and hardware and is configurable with trusted third-party and our customer's own IP enabling the creation of private and personalized system-wide security. Although fully customizable, many of our customers rely on our proven built-in system security engineering, cyber resiliency and trust stance to produce a robust turn-key layered security solution.

BuiltSECURE™

Mercury processing solutions with BuiltSECURE technology counter nation-state reverse engineering with systems security engineering (SSE). BuiltSECURE is built-in SSE that enables turnkey or personalized security solutions to be quickly configured. The extensible nature of Mercury's SSE delivers system-wide security which evolves over time, building in future-proofing. As countermeasures are developed to offset emerging threats, Mercury's security framework keeps pace, maintaining system-wide integrity.

Mercury building blocks are built with systems security engineering (SSE), cyber resiliency and trust embedded into them. Our holistic security approach is built-in and not bolted-on and forms our BuiltSECURE portfolio of building blocks. This portfolio includes processing (server-class CPU, ASICs, GPU, Atom and FPGA devices), switching, storage, memory, Ethernet, 1553/ARINC and CANbus solutions, all of which have embedded BuiltSECURE technology.

Built-in security is mandated by SOSA and Mercury is jointly chairing The Open Group's security subcommittee to define its implementation within the standard.

Key Mercury Advanced Microelectronics Centers (AMCs) are Category 1A Trusted Supplier accredited for design services and manufacturing from the DoD's defense microelectronics activity (DMEA). Our Phoenix facility has received Missile Defense Agency approval and is one of a very few select entities with trusted key loading and initialization facility (KLIF) programming authorization. Mercury's facilities are continually audited by the DoD and our customers. We have received three James S. Cogswell Awards for "outstanding industrial security achievement".

Built-in flight safety certification

Mercury deterministic safety-certifiable processing solutions are built with a top-down approach for scalability, interoperability and ease of subsystem configuration and safety certification. This built-in approach to safety-certification is the basis of our BuiltSAFE portfolio of pre-engineered DAL building blocks for subsystem pre-integration. BuiltSAFE building blocks include CPUs and CPU-rendered graphics, safe OpenGL, deterministic Ethernet and the most I/O interfaces in the industry. Mercury is executing a roadmap to certify Intel multi-core devices (Apollo-Lake). We have the most EASA, FAA, JAA and Transport Canada safety agency experience for the lowest certification risk.

BuiltSAFE™

Mercury processing solutions with BuiltSAFE capabilities bring the highest level of flight safety assurance to aerospace and defense applications. Our proven, reusable Design Assurance Level (DAL) certified artifacts for mission computing, avionics, networking and datalink comms processing save time and cost while decreasing risk.

Inherently refreshable and reusable

Our pre-engineered subsystem building blocks are inherently refreshable being made compatible with prevailing standards, many of which Mercury made significant contributions to or pioneered. Mercury processing solutions comply with SOSA, FACE, OpenVPX, VME, VNX, hybrid and customer architectures. Our software, operating systems and APIs are open system compatible (MPI/OpenMPI) enabling relatively easy technology refreshes of both hardware and software.

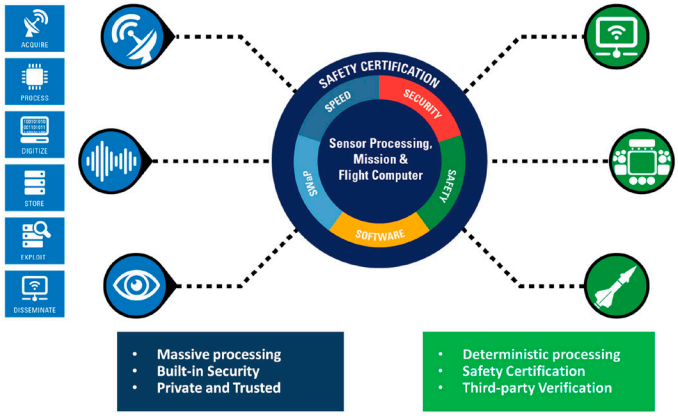
Greatest SWaP performance

Digital convergence dramatically reduces the number of platform processing boxes required from many to potentially one (logical digital convergence conclusion without redundancy). Using already rugged, SWaP efficient architectures including OpenVPX and VNX, we add further miniaturization at the board level with system-in-package and 3D fabrication techniques. This produces extreme miniaturization giving our processing solutions the highest functionality density available. Fewer boxes with the highest processing density enable not only autonomous platforms but also small autonomous platforms including UAVs.

Digitally converged processing subsystem pre-integration

Mercury is the only commercial company with whole sensor and mission processing expertise. Our focused IRAD has produced the broadest and most contemporary portfolio of interoperable building blocks in the RF and digital domain, across hardware, software and firmware. Depending upon a building block's functionality it may feature the industry's most robust built-in security or be produced with the highest level of flight safety certification (DAL-A) in mind.

Mercury's security pedigree is reflected in SOSA's confidence in our abilities and our chairmanship of the standard's security subcommittee. Our extensive flight agency program experience testifies to our safety certification qualification.



Connecting the sensor and effectors grids together

Mercury's pre-engineered processing solutions include multi-safety zone chassis that enable different safety levels to be integrated in a single processing box. Mercury is a systems integration company and has made the investments necessary to pre-integrate our proven pre-engineered processing building blocks to deliver digitally converged processing solutions for autonomous military platforms.

Summary – Innovation that converges

Autonomous commercial vehicles are emerging and may soon be commonplace. The availability of this technology will necessitate a digital convergence in the military domain.

> ***"Autonomy is the future of where we're going and it really ties into manned-unmanned teaming."-*** *Lt. Gen. Robert Walsh, Marine Corps Combat Development Command*

The enabling technology has come of age through the investments made in the commercial sector using the proven digital convergence roadmap which is exemplified by the smartphone. To miniaturize military platforms, make them smarter and autonomous and to fundamentally keep them up to date with a modern threat environment demands capabilities that can only efficiently be delivered through military digital convergence.

Mercury is making commercial technologies safe for military and aerospace applications

- From avionics I/O to platform networking, from storage to graphics processing
- Recognized experts in certified multicore solutions and graphics processing
- Design, certification and reverse engineering services
- Transform of technology building blocks into safe deployable solutions
- Built-in security foundation, tailored to deliver the right amount of security

…delivering on the promise of certifiable COTS

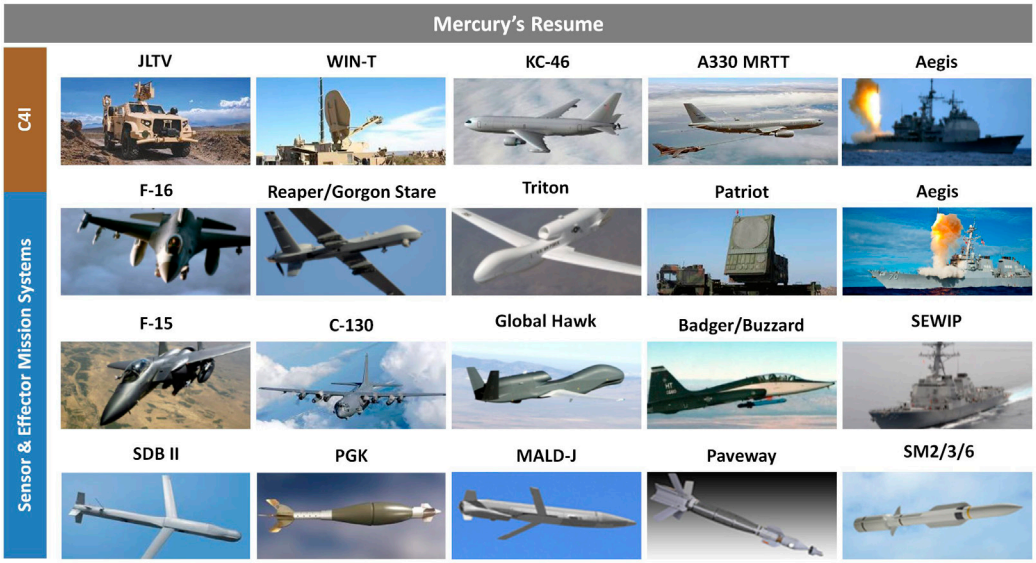
Coinciding with the availability of the required technology, SOSA is gaining traction within all branches of the military. Currently SOSA is seeking programs of record for decomposition into SOSA-certifiable open system building blocks. Two sensor manufacturers have supplied SOSA programs with decoupled sensors. Further, the PCI Industrial Computers Manufacturers Group (PICMG) oversees the industrial internet of things (IIoT) standards/specifications and is driving towards decoupled sensors that will be made in volume for their industrial solutions. IIoT is becoming the industrial internet of sensors.

Mercury Systems is a commercial company that has positioned itself and made the investments necessary to deliver the best commercial technology ready for military applications. Our investments and portfolio of capabilities enable the military digital transformation through converged sensor and mission processing solutions that feature robust system integrity and segmented safety zones in the same processing box.

> ***"We're looking at everything, like dropping off smaller autonomous unmanned systems that release from another autonomous unmanned capability…that impacts the EMS with jamming."-*** *Lt. Col. Dan Schmitt, Marine Corps Warfighting Laboratory*

Military digital convergence has begun. Small UAVs will be the vanguard platforms that usher in the technology. Mercury has prepared to meet the requirements of this wave of technology with innovation that converges.

> ***Mercury is helping to certify UAVs for civilian airspace operation all the way to DAL-A including high-altitude, long endurance platforms involving four safety-critical audits by the FAA and EASA. We are helping the world's largest helicopter company bring video directly onto flight critical display and we're doing the same thing for commercial aviation with HUDs.***



Mercury's platform processing resume

About the Author

Ike Song is the VP and General Manager of Mercury Mission Systems (MMS), where he is responsible for managing the MMS product line business both in the US and Europe including M&A.

Prior to joining Mercury, Mr. Song served as Vice President of Mission Solutions within Northrop Grumman's Land and Avionics C4ISR Division, where he managed strategic direction and operations for his business unit. He also held roles as Director of Strategic Programs and Business Development and Director of Western Region Technology Center. Mr. Song has also held positions at NP Photonics, Solus Micro Technologies, and Litton Guidance and Control Systems.

Song holds bachelor's and Master of Science degrees in engineering from the Massachusetts Institute of Technology and an Executive M.B.A. degree from the University of California at Los Angeles. He has also completed the General Management Program at Harvard Business School. Song has three patents and numerous trade secret and merit awards.

Song has served on the Board of Directors for the Vertical Lift Consortium. He was a 2012 National Association of Asian American Professionals (NAAAP) 100 winner for his leadership and professional achievements.

About Mercury Systems, Inc.

Mercury Systems (NASDAQ:MRCY) is a leading commercial provider of secure sensor and safety-critical processing subsystems. Optimized for customer and mission success, Mercury's solutions power a wide variety of critical defense and intelligence programs. Headquartered in Andover, Mass., Mercury is pioneering a next-generation defense electronics business model specifically designed to meet the industry's current and emerging technology needs. To learn more, visit www.mrcy.com.

Table of Acronyms

AMC	Advanced Microelectronics Center
API	Application Program Interface
DMEA	Defense Microelectronics Activity
FMS	Foreign Military Sales
GPS	Global Positioning System
HUD	Heads Up Display
I/O	Input/output
IFF	Identification, Friend or Foe
IIoT	Industrial Internet of Things
IP	Intellectual Property
IRAD	Independent/Internal Research And Development
ISR	Intelligence, Surveillance & Reconnaissance
JAA	Joint Aviation Authorities
KLIF	Key Loading and Initialization Facility
LRU	Line Replacement Unit
MORA	Modular Open RF Architecture
MOSA	Modular Open System Architecture
OMS	Open Mission Systems
PICMG	Pci Industrial Computers Manufacturers Group
PNT	Positioning Navigation & Timing
RF	Radio Frequency
SIGINT	Signal Intelligence
SOSA	Sensor Open System Architecture
SSE	Systems Security Engineering
SWaP	Size, Weight & Power
UAV	Unmanned Aerial Vehicle
VICTORY	Vehicle Integration for C4ISR/EW Interoperability
VITA	VME International Trade Association

3399.00E-0318-wp-digital-transform

mercury systems™

INNOVATION THAT MATTERS™

CORPORATE HEADQUARTERS
50 Minuteman Road • Andover, MA 01810 USA
(978) 967-1401 • (866) 627-6951 • Fax (978) 256-3599

MADE IN AMERICA