



INNOVATION THAT MATTERS™



Corporate Headquarters

50 Minuteman Road
Andover, MA 01810 USA
(866) 627-6951 • (978) 967-1401
www.mrcy.com



Mercury Systems, Innovation That Matters, Air Flow-By and OpenRFM are trademarks and Ensemble is a registered trademark of Mercury Systems, Inc. Other product and company names mentioned may be trademarks and/or registered trademarks of their respective holders. Mercury Systems, Inc. believes this information is accurate as of its publication date and is not responsible for any inadvertent errors. The information contained herein is subject to change without notice.
Copyright © 2017 Mercury Systems, Inc. 3286.01E-0317-BR-capabilities



CORPORATE CAPABILITIES



WELCOME TO MERCURY SYSTEMS

Dear Customer,

Welcome to our overview of Mercury Systems. Our goal is to be the leading commercial provider of secure sensor and mission processing subsystems.

The DoD and the entire defense industrial base live in an increasingly challenging environment. With a backdrop of unrelenting geopolitical tensions around the globe, a defense industry that is in transition, and a domestic political environment that adds an additional element of uncertainty, Mercury Systems has adopted a pragmatic Next Generation Business Model that is in touch with these times. Our Next Generation Business Model is simple. We combine three key components to drive towards your success:

First, we quickly and affordably adopt commercially-available technology in support of critical programs and missions. Second, Mercury innovation is central to our business model as we invest up to 15% of our revenue in internal R & D. Third, we leverage this internal R & D and commercially available technology towards the development of pre-integrated subsystems so that our customers can use open application programming interfaces to easily and quickly configure solutions to meet mission specific requirements. All while reducing cost and time to market.

Mercury Systems has a long history of driving modular open systems architectures. With thirty five years of technology leadership within the high-performance embedded computing industry, we have pioneered many of the defense industry's current and emerging open standards.

This includes OpenVPX™ and AdvancedTCA®. Most recently we launched OpenRFM™, an open, standardized and scalable approach that combines digital and RF processing. Within the RF domain, we've invested in modern, scalable and efficient manufacturing by establishing Advanced Microelectronics Centers covering both the Eastern and Western United States. We have state-of-the-art DMEA-accredited trusted manufacturing facilities that provide industry leading capabilities in custom micro-electronics design and manufacturing. We believe that our engineering, design and manufacturing capabilities give Mercury Systems a footprint that allows us to deliver leading embedded secure processing, secure storage, and RF solutions. Our pre-integrated solutions support programs and missions that require advanced radar, Intelligence Surveillance Reconnaissance, Electronic Warfare, and guided missiles and precision-guided munitions capabilities.

We have recently added additional capabilities to better serve our customers in the areas of mission computing, safety-critical avionics and platform management. Mercury now offers subsystems deployed in applications certified to the highest levels of design assurance, DAL-A, for both DO-254 and DO-178. These solutions complement our already broad portfolio of contemporary technologies in support of the defense industry.

All of these capabilities leverage our growing expertise in embedded security. We are currently in our fourth-generation of secure solutions. Secure solutions that can provide a modular, affordable foundation in support of secure architectures. We have thoughtfully built our secure capabilities around four key elements.

- **Security solutions must be “built-in” not “bolted on.”**

The concept is key to making sure technology building blocks can be leveraged effectively even as they are integrated and customized to meet customers' needs.

- **Secure solutions must be domestic.**

Much of the IT industry, which the defense industry has come to depend on, is sourced outside of the US, sometimes in countries that are potential adversaries. We engineer, develop and manufacture all of our secure solutions domestically.

- **Secure solutions must be upgradable.**

We provide secure building blocks that are standardized and can be used, in a repeatable way, by our customers who then can affordably include them as part of their own secure architectures.

- **Secure solutions must be integrated.**

As part of creating “built-in” solutions, it is essential to know what the source is and how it is being used. As multiple technologies are integrated into a secure platform it is essential that common APIs and software code have a known and controlled source and can provide clear and known user authentication, information assurance, tamper monitoring and resistance, and secure run-time operation.

All of our security work is done by a team of skilled professionals that we believe is among the deepest pool of talent the industry has to offer.

I hope you find the information in this brochure helpful. We look forward to partnering with you on the challenges and opportunities that lie ahead.

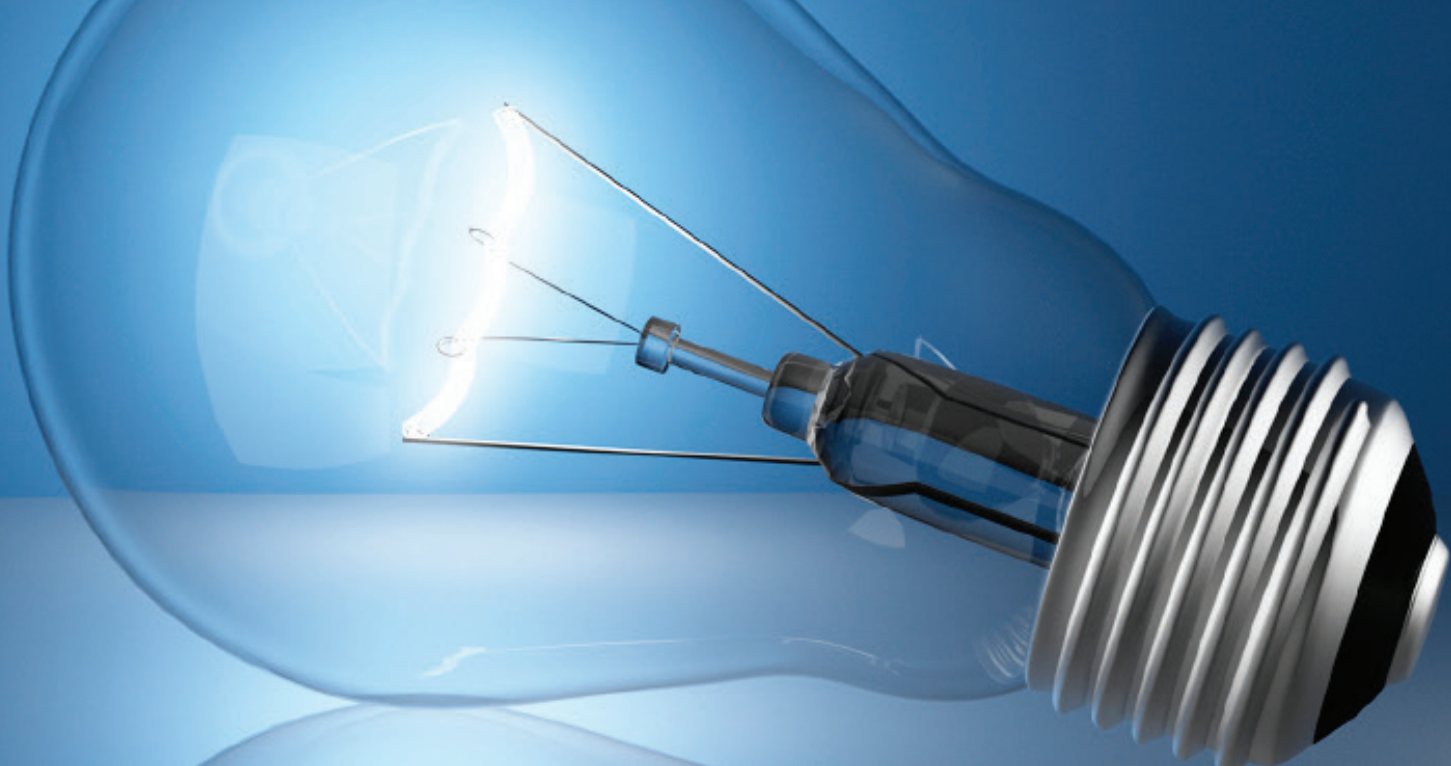
Sincerely,



Mark Aslett
President and
Chief Executive Officer



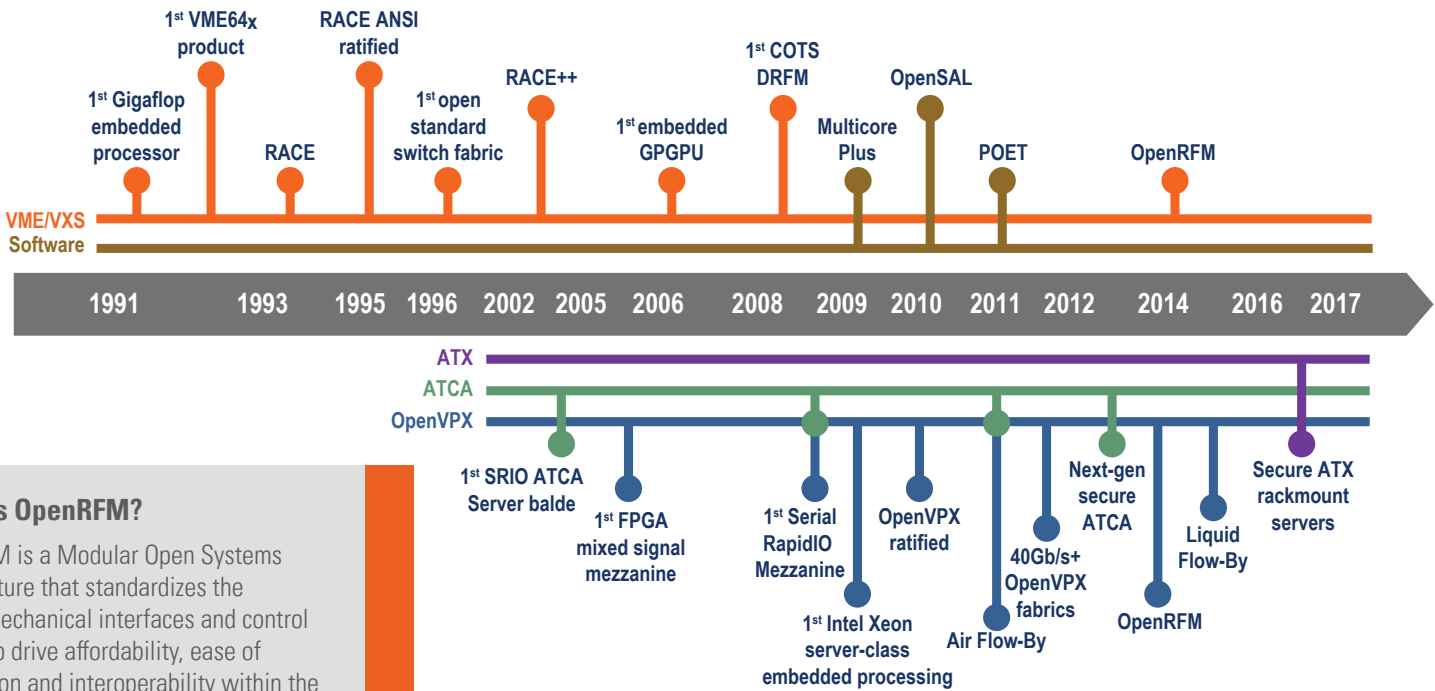
INNOVATION THAT MATTERS™



To meet our defense objectives, deter our adversaries and defeat terrorism we need the rapid deployment of agile, capable and trusted commercial technology. Recognized by the DoD, this realignment is captured and promoted by the DoD's Better Buying Power 3.0 (BBP3.0) under the overarching theme of "Achieving Dominant Capabilities through Technical Excellence and Innovation."

To remain dominant, our defense solutions need agile and superior capabilities that are interoperable and affordable. Increasingly, in a

globalized world, these solutions must be secure, trusted and certified for flight safety. BBP3.0 addresses this by highlighting the need to leverage the best commercial technology through open architectures. It is by leveraging breakthroughs in commercial technology that defense innovations will be born. This is consistent with Mercury's next-generation defense electronics business model and as stated in a DoD Defense Appropriations Testimony before Congress "Leading the (technology) race now depends on who can out-innovate fastest."



What is OpenRFM?
OpenRFM is a Modular Open Systems Architecture that standardizes the electromechanical interfaces and control planes to drive affordability, ease of integration and interoperability within the RF/microwave domain and is ideally suited to EW applications.

NEXT GENERATION DEFENSE ELECTRONICS BUSINESS MODEL

Mercury is pioneering a next generation defense electronics business model. We are the leading provider of secure and safety-critical processing subsystem solutions.

Our next-generation defense electronics business model drives affordability and program velocity that wins our customers more business. Our business model is built on three foundational elements:

- Quickly and affordably adopt the best commercial technology in support of defense programs and missions
- Invest our own funds in R & D to complement the Pentagon's, prime contractors', defense and non-profit labs' own initiatives
- Create secure pre-integrated processing subsystem building-blocks that can be rapidly pre-integrated into critical defense programs

This model complements the DoD's drive to modernize and streamline defense procurement and the prime-contractors' increasing need to be efficient and affordable platform integrators. We pre-integrate our solutions to drive down overall platform integration costs. We then rapidly customize these solutions for multiple platforms, leveraging scalable manufacturing resources to lower both cost and risk.

We have driven the creation and leveraged the use of Open Systems Architectures (OSAs), ushering in the adoption and ANSI/VITA ratification of OpenVPX™ for digital processing in 2010 and launching an emerging open architecture, OpenRFM™ for RF/microwave processing in 2014. We build modularity, usability and security in to all of our processing subsystem building blocks. Today we have the most contemporary and largest portfolio of embedded processing solutions from tactical servers, digital and RF/microwave building blocks, pre-integrated processing subsystems and new secure-rackmount and AdvancedTCA® server blades.

Mercury is the better alternative for low-risk, affordable, commercially developed processing subsystems.

- A commercial company within the defense industry
- 13% - 15% of revenue invested annually on applied R&D
- Collaborative engineering and program management
- Open systems architecture for sensor and mission processing
- One-stop-shop for trusted, secure and safe processing subsystems
- Scalable RF/microwave and microelectronics manufacturing
- Quick Reaction Capability and proven high-TRL solutions

CAPABILITIES

Mercury is the leading commercial provider of secure sensor and mission processing subsystems

Secure Processing and Storage

Security of critical defense platforms and missions has never been more important – it’s a must-have. Mercury’s built-in fourth generation security framework and building blocks complement our customers’ secure architectures, enabling the creation of their own private and personalized system-wide security.

Our processing, memory and storage solutions build in the industry’s most robust security. These solutions are designed, coded and manufactured in secure, domestic facilities, using trusted devices from managed supply chains for the highest level of system integrity.

Mission Computing

Mercury Systems brings the highest level of flight-safety assurance to the secure processing domain for 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, and reduce risk.

Our safety-critical processing subsystems are produced in AS-9100 facilities and deployed in applications that are certified to the highest levels of design assurance, DAL-A for both DO-254 (hardware) and DO-178 (software). For low-risk interoperability, Mercury’s deterministic safety building blocks are OpenVPX, VME and CompactPCI compatible.

C4I Processing

Our rugged secure ATX rackmount servers and AdvancedTCA server blades are designed to drive the most powerful military processing applications, addressing the US defense market’s need for affordable, reliable and trusted US-made technology. These servers have security and ruggedness built in and are ideally suited for next-generation radar, large mission, ground/ naval/air C4I processing applications requiring system integrity.

An open system middleware framework with sustained Mercury support protects customers’ application investments. This framework enables our customers to easily port their applications to refreshed hardware thereby preserving their most valuable asset, their software. Secure servers are open systems compliant, making them application-ready and an extremely low-risk adoption proposition for new and current applications requiring server-class processing and robust system integrity.

RF/Microwave Solutions

Our Advanced Microelectronics Centers (AMCs) include trusted DMEA facilities to manufacture our secure RF, microwave and millimeter-wave and miniaturized, mixed signal processing solutions. Our highly automated, world-class manufacturing capabilities enable us to produce highly-repeatable build-to-print/spec Integrated Microwave Assemblies (IMAs), components, high-power EW amplifiers, switch matrices and other RF/microwave devices. In the embedded digital processing domain, Mercury drove interoperability and affordability with OpenVPX - we are now doing the same within the RF/microwave domain with OpenRFM.



Radar Solutions

Mercury’s rugged and dense Ensemble® 3U and 6U OpenVPX and AdvancedTCA radar compute building blocks feature the most efficient cooling technology and fastest, software-defined switch fabrics to deliver the greatest embedded signal processing capability in the industry today. These building blocks are optimized for SWaP performance and processing density, leveraging such processing power as Intel® Xeon®-E server-class processors. Scalable Ensemble processing subsystems with their streaming, low-latency processing power and performance software are ideally suited to next-generation radar’s compute-intense, streaming, real-time signal processing requirements.

Mercury leverages scalable, highly-automated manufacturing/test resources with advanced RF/ microwave simulation and packaging to produce affordable and SWaP-efficient antenna tiles for next-generation AESA radar arrays. We have applied our DRFM and radar domain expertise to produce radar environmental simulators that exercise the most contemporary radars and develop new techniques to thwart emerging tactical threats.

Electronic Warfare Solutions

From signal acquisition (tuners, filtering), to digitization (AD/DA converters), processing and electronic countermeasures (DRFMs), our rugged, coherent EW building blocks have exceptional SWaP utilization and the greatest spectral-efficiency. Mercury’s modular open system approach to EW subsystem development reduces program risk and time-to-solution and market, while promoting affordability.

Mercury leverages the best commercial technologies to create cognitive, low-latency EW solutions across the spectrum. Our small form-factor building blocks enable the quick configuration of agile and sophisticated EW solutions. Mercury’s EW pre-integrated solutions span digital and RF/microwave domains including spoofing DRFMs, signal jamming and entirely self-contained EW LRUs. OpenRFM neatly manages RF/microwave and digital processing convergence within the EW domain.

Intelligence, Surveillance and Reconnaissance Processing

Modern ISR sensors require greater processing power and capability. Mercury ISR/IMINT solutions integrate powerful parallel processing GPGPUs and general server-class processors to deliver unequalled image processing and real-time information exploitation capability in low-SWaP packages. Our advanced air/ liquid cooling technology ensures reliable, full-throttle deterministic processing from pre-flight ground preparation to extended high-altitude loiters.

Mercury pre-integrates processing and RF/microwave building blocks to support ISR programs requiring quick reaction capabilities and special missions. Our capabilities deliver affordable specialized performance in the domains of SIGINT and EW that augment EO/ IR national assets in such roles as target identification. Mercury ISR solutions have low-SWaP profiles, mission agility and are supported by full in-house design, qualification, tuning and manufacturing capabilities.

Guided missile and precision-guided munition solutions

Mercury applies off set technologies to maintain the dominance of our precision-guided munition solutions, mitigating emerging threats. Modern kinetic assets have to be secure, mission-tailorable, with longer reaches, and smarter to confidently intercept threats anywhere.

Modern munition guidance, navigation and control systems require secure, dense mixed-signal processing and high-frequency RF (mm) technology in protective packaging. Mercury’s dense system-in-package (SiP) and multi-layer memory stacking technologies deliver the highest mixed-signal processing density and performance. Our gun-hardened guided munition solutions, with built-in security and EW capabilities are smarter than ever.

The Only Commercial Company with Capabilities Across the whole Sensor and Mission Processing Chain

We continue to build our capabilities across the entire sensor and mission processing chain, from signal acquisition to dissemination, and everything in between. Mercury processing subsystems are deployed on some of the world's most important military platforms, executing critical sensor, decision and mission processing operations.

SOME MAJOR PLATFORMS AND PROGRAMS SUPPORTED:

- Patriot BMD
- SEWIP, AEGIS BMD
- B-1B, F-15, F-16, F-22, F-35
- Triton, Global Hawk
- Predator, Reaper, Gorgon Stare
- AH-64 Apache
- P-8 Poseidon MMA, KC-46
- Paveway, MALD-J, SDB-II

New performance-optimized OSA building block innovations for the sensor and mission processing chain

Mission Computing

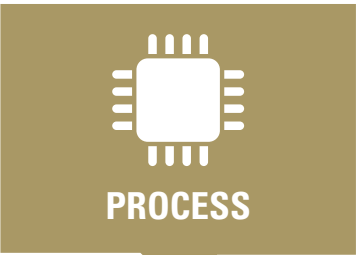
Mercury is bringing the highest level of DAL flight-safety assurance to the secure sensor processing domain. Mercury's decision-making mission computing solutions enable the effects grid to connect to the sensor grid using open system architectures.



- Missile and precision munition guidance subsystems
- Pre-integrated AESA Rx/Tx modules
- Fastest, high-dynamic range and most agile wideband tuners



- Scalable SW-Defined Radios across multiple form-factors
- Small form-factor, spectrally efficient ADCs and DACs
- High isolation and switching frequency switch matrices



- Secure AdvancedTCA processing ecosystem for data-center performance
- Secure rackmount ATX server processing ecosystem for affordability
- Industry leading air and liquid cooling for dense, reliable and unrestricted processing power



- Secure, rugged Solid State Drives
- Secure, rugged, high-density memory
- Rugged, System-in-Package miniaturization



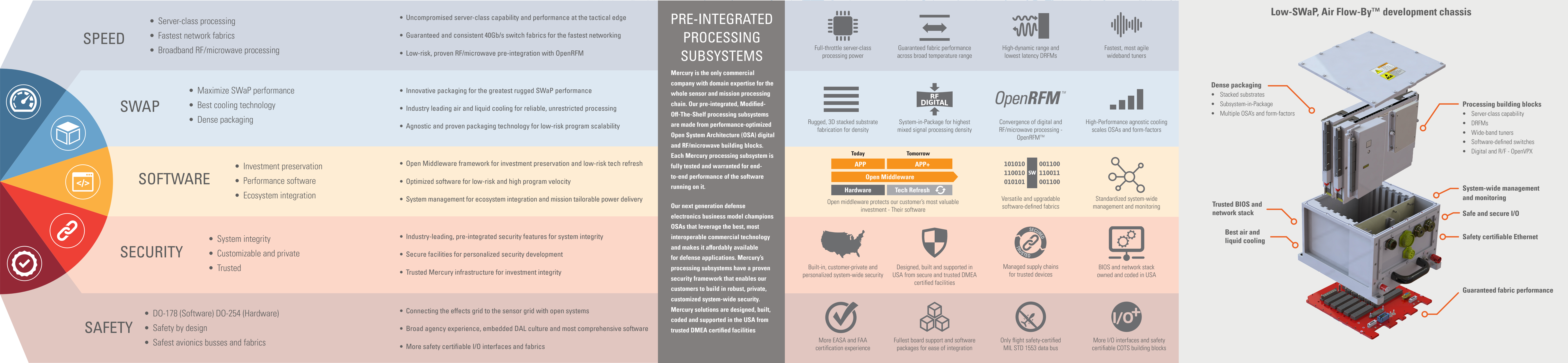
- Safety-certifiable building blocks for avionics, platform management and mission processing
- Guided missile solutions with EW capability
- Software framework for customer technique generation



- Safety certifiable building blocks for networking and datalinks
- Broadband high-power GaN-based power amplifiers
- High-dynamic range, low-latency DRFMs

ANATOMY OF A SUBSYSTEM

Mercury is the only commercial company that designs and builds rugged, pre-integrated processing subsystems for sensor and decision making applications with proven built-in security.





MISSION COMPUTING

Mercury Systems designs and manufactures deterministic processing modules and subsystems that have been deployed in applications certified to the highest Design Assurance Level, DAL-A, for both DO-254 (hardware) and DO-178 (software). Our mission computing solutions are found in commercial and military, manned and unmanned platforms.

Our real-time flight-safety building blocks are made to rugged 3U and 6U VME/VXS, OpenVPX and CompactPCI Open Systems Architectures (OSAs). Solutions may be modified (MOTS) or right off the shelf (COTS). Both are supported by our teams of experienced engineers who number over half of Mercury Mission Systems' staff.

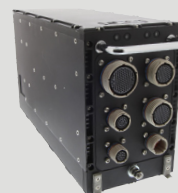
Our expertise and experience has been acquired over three decades and is built-in to our Avionics Series of flight-safety certifiable building blocks for processing, avionic I/O, video, avionics-certifiable Ethernet and rugged packaging. These safety building blocks are in their third generation (with backward compatibility) and designed with a top-down approach for interoperability and ease of pre-integration in to our safety certifiable processing subsystems.

Key components used with our Avionics Series of safety building blocks are carefully selected for determinism, performance, reliability and sustainability. CPUs and other critical devices that may evolve quickly over time are mounted to mezzanines to ease future tech refreshes and recertifications. We commit to maintain and support established products and facilitate migration to new product generations with full backwards-compatibility.

To extend product life we have developed multiple management techniques including stocking, multi-sourcing and utilizing FPGAs to mitigate specific device dependence. Whatever your strategy, we are at your side to extend the lifetime of your solutions.

DAL-certifiable development chassis

- Certifiable to DAL-A
- Multiple safety-segmented zones for program velocity
- COTS safety-certifiable processing and I/O modules
- Safety-certifiable fabrics and avionics busses



SYSTEM INTEGRATION AND SOFTWARE

Mercury is the only commercial company with domain expertise across the whole sensor and mission processing chain. Our investments have produced the largest, most contemporary portfolio of embedded processing building blocks powered by the best commercial technology. These proven, interoperable digital and RF/microwave/mm-wave processing elements have a common robust built-in security foundation which spans 3U and 6U OpenVPX, secure AdvancedTCA and rackmount ATX architectures.

The key to program success and winning the innovation race is to be able to leverage the best, trusted commercial technology, quickly. Mercury's pre-integrated processing subsystems are agile configurations of proven, high-TRL Modified-Off-The-Shelf processing building blocks. Their built-in security framework creates higher product differentiation, drives greater program velocity, while lowering risk.

We guarantee and optimize the functionality of software over our pre-integrated digital and RF/microwave/mm-wave processing subsystems. Trusted devices and built-in, customer private and personalized security enables our customers to deploy their solutions anywhere.

Mercury's open middleware preserves our customers' valuable software. Our open approach and Mercury's consistent, multi-decade middleware support enables our customers to refresh their applications at the speed of technology. Further, our suite of software is optimized for low-latency processing applications and includes such innovations as software-defined switch fabrics for ease of upgrade.

Low-SWaP, Air Flow-By chassis

- Secure, rugged OpenVPX architecture
- Best cooling – Fastest, SW defined fabrics
- Largest portfolio of processing modules
- System-wide management and monitoring





SECURITY

The issue of security in support of critical defense platforms and missions has never been more important - today security is a “need to have” as the very effectiveness of the defense platform becomes dependent on the level of security afforded it.

Systems have been and will continue to become interconnected at an astonishing rate. Sometimes the connections are by design and sometimes they happen in an ad hoc manner. These interconnections pose a security risk due to data aggregation/linking, threat/vulnerability mismatches (or “seams”), and a lack of defensive countermeasure interoperability and integration. Even the best designed and scrutinized secure defense platform may become vulnerable because of an interconnection created outside of the parameters of the original design. For this reason, electronic systems deployed for use in military applications should employ built-in security including encrypted data-at-rest, secure start-up, user authentication, tamper monitoring and reporting, and secure run-time operation. Built-in security is the most effective and versatile approach to meeting these evolving requirements and is the approach Mercury uses with our system-wide, extensible security building blocks that further reduces risk and supports greater affordability.

For over a decade, Mercury has been developing security building blocks across the whole sensor processing chain that is complementary to our customers’ secure architectures. Our building blocks and security principles are grouped in to four fundamental domains:

- **Designed-in security:** First and foremost, for defense platforms to be secure against today’s advanced threats, the security must be “built-in” and not “bolted-on.” This is necessary to address the seams in security implementations that form within a single platform due to the interplay between legacy and contemporary security policies as well as between the various security disciplines. Mercury’s fourth-generation secure building blocks can be stitched together to defeat new threats, even as they are integrated and customized during subsequent stages of integration.
- **Domestic solutions:** Domestic supply chains come with the enforceable regulation and oversight of the suppliers and the consequence of US law should participants in that supply chain misbehave. Much of the broader IT industry, which the Department of Defense has become dependent on, is now manufactured and sourced outside of the US, either in places where supply chains are hard to track, or even worse, in locations where there is the risk of a compromised solution. The potential for bad actors is significantly reduced when the supply chain has motivation to police itself at a high standard as it does in the US. We engineer, develop and manufacture all of our secure solutions domestically.

- **Extensible:** While the security community can attempt to “future proof” architectures through rigor and expertise, the unpredictable nature and deployment speed of threats against defense platforms require that ways to quickly update and improve security capability are designed in. Mercury’s secure building blocks are standardized and can be used, in a repeatable way, by our customers who then include them in their secure architectures. This approach allows our customers to be in control as they build their secure processing platforms using and re-using our technologies as needed. It also enables the replacement of building blocks as new security methods become preferred and/or new building blocks to be added as threats emerge.
- **Interoperable and integrated:** The challenge with the maturing security disciplines of information assurance, anti-tamper, cyber-defense, and supply chain risk management is that adversaries will seek to attack the seams in these disciplines. This becomes more pronounced as policies in these disciplines are tailored across user communities and implemented to varying degrees across defense platforms. The attack vectors are uninhibited by the siloed walls of any particular security discipline and hence security practices should overcome these confines. As multiple technologies are integrated into a single interconnected platform it is essential that standard interfaces are utilized for interoperability in areas of encrypted data-at-rest, secure start-up, user authentication, tamper monitoring and reporting, and secure run-time operation. Mercury’s built-in approach facilitates system interoperability and integration.

Systems and networks in support of key defense platforms continue to become more complex. Today security is a “must have” to the effectiveness of defense platforms and must be prioritized as such to meet the increasingly challenging demands of the warfighter. Mercury has the broadest, deepest commercial portfolio of embedded security building blocks, extensible framework and customizable mechanisms that enable our customers to build in robust, private and personalized security for the highest level of system integrity.

Mercury’s secure processing subsystems are built using trusted devices from managed supply chains and run trusted software, where our fabric network stacks and Basic Input/Output System (BIOSs) are coded within secure Mercury facilities.

Secure Solutions must be:

- Built-in, not bolted-on
- Domestic for uncompromised supply
- Extensible for customer control
- Interoperable and integrated for seamless protection

ONE MERCURY

Headquarters

Mercury Systems is headquartered in Andover, Massachusetts within a secure and Defense Microelectronics Activity (DMEA) accredited, state-of-the-art facility. Our headquarters incorporates a world-class design and engineering capability and Innovation Center that demonstrates sensor and mission processing innovations to customers.

It is from our headquarters that we drive our One Mercury next-generation defense business model that efficiently leverages our capabilities across the whole sensor and mission processing chain, delivering innovation at the speed of technology. Our business model enables our customers to leverage the best commercial technology for performance, confident that security and trust is built-in. Mercury’s flight safety and sensor processing capabilities are enabling our customers to connect their effects grid to their sensor grid through affordable open systems architectures.



Innovation Centers

Mercury’s Innovation Centers located in Massachusetts, New Hampshire, New Jersey, California and Switzerland showcase our solutions across the sensor and mission processing chain. Each Innovation Center also displays specific facility expertise, be it RF and microwave digital processing or solution pre-integration. We encourage our customers to visit an Innovation Center, to see firsthand why Mercury solutions are Innovation that Matters.

Trusted Mercury infrastructure for investment integrity

- Best security practices applied across enterprise
- Trusted board support and development
- World-class infrastructure and IT security posture



Advanced Microelectronics Centers (AMCs):

To meet our customers’ need for precise, repeatable RF and microwave and digital processing solutions, Mercury has invested in redundant, scalable Advanced Microelectronic Centers (AMCs). Our AMCs are dedicated to the production of defense industry subsystems within world-class, domestic manufacturing environments. We operate scalable AMCs in New England, New York metro area, Southern California and a trusted DMEA facilities in the Southwest, which has Missile Defense Agency approval and AS9100 certification. Each AMC offers onsite Program Management and co-located product and process engineers for the smooth on-boarding of build-to-print, build-to-specification military processing subsystem production.

Mercury consistently makes investments in our state-of-the-art manufacturing and test capabilities enabling our customers to benefit from the most efficient and contemporary processing technologies for greater solution performance and lower program risk. Our rigorous Highly Accelerated Stress Screening (HASS) processes assure our solutions, which are engineered with extended temperature, stock and vibrational resilience, function unconditionally right of out of the box.

From simulation to fully automated manufacturing, to precise RF and Microwave tune and test, Mercury’s AMCs are the better alternative for trusted, secure defense processing subsystem manufacturing.

**Mercury has been
awarded two Cogswell
Awards for Industrial
Security and Excellence**

