WHITE PAPER

Next Generation Defense Electronics Manufacturing

Mercury Systems Advanced Microelectronics Centers

Introduction

Mercury Systems has pioneered a next generation defense electronics business model and supporting manufacturing infrastructure that addresses globalized supply chains in support of the aerospace and defense industries. This whitepaper describes why Mercury's proven approach to defense electronics manufacturing is necessary, how it works and how it benefits and enables prime contractors to win more business.

In so doing, this white paper answers a national defense imperative, succinctly stated by Army Chief of Staff, General Mark Milley's "How do we put technology into the hands of our soldiers (and by extension our airmen, sailors, marines, coast guard and first responders) faster."

USHA SHAH - VP/GM - US MANUFACTURING OPERATIONS
JOHN BRATTON - MANAGER OF PRODUCT AND SOLUTIONS
NOVEMBER 2017

mercury systems™

"Leading the race depends on who can out-innovate the fastest"

Technology is advancing faster than ever – the accumulated knowledge of mankind now doubles every 12 months. Nowhere is this knowledge advance more obvious than in the domains of computing and communications. For the defense industry, knowledge brings capability, opportunity and menace - as new and old, symmetric and asymmetric adversaries field increasingly sophisticated threats. Offsetting these threats requires responses that need to be even better and they need to be deployed quickly.

The commercial marketplace quickly replaced a relatively few wired telephones with billions of untethered wireless smartphones – it seems everyone has one regardless of where they are. Internet enabled, these smartphone-users communicate, share and access information anywhere and this has redefined what communication is. To maintain, or increasingly to re-establish a capability gap between our defense systems and peer, near-peer threats requires the defense industry to move as fast as the commercial marketplace. That is to say, innovate quickly and deploy better solutions, fast. And then do it again.

With the biggest defense re-calibration in decades underway, our national defense doctrine is pivoting towards:

- A full-spectrum model to deter potential adversaries
- Updated defense strategies, operational concepts and tactics
- Smart and essential technology innovations that leverage the best commercial solutions

That's not to say the commercial high-tech marketplace is a panacea. HTC and Blackberry (formerly Research In Motion) have transitioned from marketplace titans to near-also-ran in a few short years. It's one thing to lose marketplace stature; it's another to lose national defensive initiative.

The technology that changed the fortune of companies like HTC and Blackberry is the same technology that state and non-state actors around the world are using to field their own, often innovative threats to our national defensive posture. Deployment of our contemporary defense systems has to be competitive with the agile efficiency of the commercial marketplace to offset emerging threats that are evolving as quickly as technology itself.

Apple, Samsung, Amazon and Microsoft are also commercial high-tech companies. Unlike HTC and Blackberry they have found a business strategy that keeps them in front. These companies are innovators, and that's their focus. They leverage the best commercial manufacturing capabilities from world-class commercial contract manufacturers like Foxconn (China) and Asus (Taiwan) to offload their production to, while they maintain their core innovation focus. (Blackberry transferred their manufacturing to Foxconn in 2013 under new CEO John Chen which is enabling Blackberry to focus on its innovative software. This transition is seen as the mark of the beginning of Blackberry's turn around.)

New geo-political challenges create new opportunities where the winners will be the fastest innovators:

- Aging platforms - require modernizations at the speed of technology for new missions
- International and foreign opportunities - require secure, trusted and safe processing systems for information protection and mission autonomy
- Breakthrough technologies - low-risk game changing commercial technologies will define the future innovation winners

Since the early 1990s and Secretary of Defense William Perry's watershed COTS initiative, the DoD has strived to leverage the best commercial off the shelf (COTS) technology. The COTS initiative was originally affordability-centric, but is increasingly required for the performance, interoperability and quick reaction capability found in commercial marketplaces. To stay in front, defense electronics will need to be produced with the capability and velocity of commercial systems. Additionally, the defense industry has other special requirements and characteristics - regardless, as Defense Secretary Ash Carter said to the Senate Appropriations Committee, "Future success will go to the fastest innovators. Leading the race now depends on who can out-innovate (and deploy) the fastest."

Do more with less - better and quicker

The defense industry as a whole has cut manufacturing capacity, reduced headcount, lost engineers and has the headwind of an aging workforce, as newly minted professionals don't always see a career in defense electronics desirable. The need to stay "competitive" during times of uncertain and contracting military spending has preceded the fastest acceleration in technology and threat evolution in history. To stay in front, new approaches to defense electronic development and manufacturing have to be adopted.

Mercury recognized that the best commercial technology had to be deployed quickly and that a modified commercial business model was the vehicle with which to do it. Such a model could enable the DoD to retool and evolve more efficiently and effectively, if the model was made fully compatible with defense industry requirements. Mercury has systematized this approach with our next generation defense electronics business model.

Since 2001, when China joined the World Trade Organization, the US has lost nearly a third of its manufacturing jobs – China now produces 50% of the world manufactured output.

China's capability has become so great it is assumed by many US startups that China is where their products will be produced.

Meanwhile, other technically advanced nations including Germany and Japan have maintained a much stronger manufacturing capability.

Ref MForesight report MF-TR-2017-0201, funded by NSF and NIST.

Mercury's next generation defense electronic business model is a hybrid model. It combines the best innovation engines and investment strategies from the commercial electronics domain with efficient, scalable and affordable manufacturing and makes them suitable for defense applications. With the infusion of embedded product and infrastructure security, trust and defense grade miniaturization and rugged packaging, Mercury has created an enterprise that meets today's defense electronics innovation and deployment requirements. In effect the next generation defense electronics business model is doing more with less, and doing so better and quicker.

Mercury's next generation defense business model applies the best commercial practices of investing focused IRAD to solve anticipated future industry needs in domains such as embedded system security, dense packaging, greater reliability and processing power. We leverage the best commercial technologies, while building in trust, security, longevity and military grade ruggedness. Unlike commercial equivalents, Mercury is a dedicated defense electronics manufacturer that uses defense industry processes, documentation, testing and support practices. As such, Mercury may be regarded as an innovative commercial company and secure manufacturer that is focused on meeting the needs of a modern defense industry marketplace.

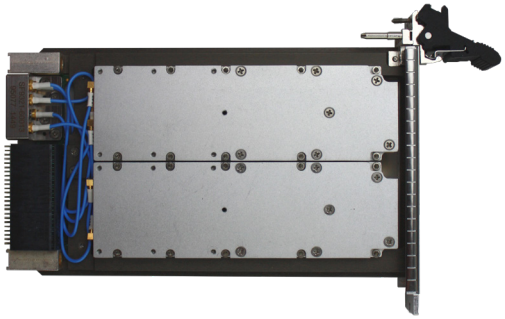
Maintaining our defense electronics leadership is pivotal to our national defense. For the prime defense contractors, electronics leadership is also fundamental to winning and retaining more business. "Leading the race now depends on who can out-innovate fastest" - this requires combining innovative technology breakthroughs with efficient manufacturing for deployment at the speed of technology.

The best world-class commercial manufacturers have capabilities that enable their customers to jump to the front of the deployment race through rapid, low-risk, low-cost of ownership manufacturing. These manufacturer capabilities enable their customers to focus on their true value - innovation. These capabilities are captured within Mercury's next generation defense electronics business model and similarly aid prime defense contractors to lead their deployment races while they remain innovation focused.

Precise, repeatable product performance, delivered using proven technology and low-risk processes, that scale from low, to high volume and that are offered with quick reaction capability and risk deferring fixed prices would differentiate any defense solution. Although an impressive list, it is not enough by itself for effective defense electronics production.

Intel Xeon-SP powered open system blades (3U, 6U OpenVPX and AdvancedTCA)

Prime contractors require industry specific capabilities that are seldom seen within the commercial domain. Primes require built-in security and trust in both the product and the producers' infrastructure. They require custom RF and digital processing pre-integration in the same box, solution miniaturization, defense grade ruggedness and longevity of supply/support. None of these traits are naturally characteristic of even the best commercial contract manufacturer. A bigger concern is that commercial contractors are becoming more and more globalized, exposing themselves to the risks of complex and intrinsically vulnerable supply chains. Vulnerabilities and comprises to these supply chains may be accidental, but increasingly they are not.



OpenRFM modules are compatible with OpenVPX

> ***"The DoD is interested in solutions that enable the use of commercial foundries while ensuring critical defense technologies and intellectual property (IP) are trusted (confidence there is no malicious content), assured (verified function with no extra functions), and protected (prevention of unauthorized disclosure)."***
>
> Broad Agency Announcement FA8650-18-S-1201, October 2017

Mercury's next generation defense electronics business model addresses these requirement-gaps, while leveraging the best commercial IP and business practices to deliver secure pre-integrated RF and digital processing solutions for defense applications.

Next generation defense electronics business model - Mercury's qualification

For over three decades Mercury has designed and manufactured the most powerful, contemporary embedded defense processing solutions. 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 architecture (MOSA) standard.

> ***"90%+ of respondents believe that business risk is increasing, with supply chain complexity being the largest concern, followed by cybersecurity, business model disruption and globalization."***
>
> Ref - MIT 2015 Global risk survey

Mercury's portfolio of engineering, manufacture and test span the whole sensor processing chain in both the RF and digital domains

Mercury is currently applying the discipline of standardization, interoperability and proven technology leverage in the RF domain, as we did in the digital realm, though OpenRFM. OpenRFM reuses 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 dissemination.

Prime contractors are shifting their focus and resources towards identifying and analyzing emerging threats from around the globe and across the electromagnetic spectrum. Their value lies in creating innovative command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) solutions that build in new threat awareness and mitigation or exploits the vulnerabilities in aggressor systems. They are staying in front of the innovation race by leveraging the best technical processing technology, which when deployed as part of open system architecture, enables relatively easy tech refreshes to stay in front.

Ease of system upgrades builds in future-proofing, enabling processing solutions to evolve, offsetting future threats and meeting future needs. An open architecture approach to system design and manufacture is enabling primes to differentiate themselves through responsiveness, lower program risk, greater affordability, interoperability, scalability, capability and sustainability – all of these features are increasingly DoD requirements.

To meet our defense objectives, deter 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."

Innovation That Leads: Mercury's resume of OSA firsts

- Embedded Intel Xeon-SP server-class processing
- OpenSAL DSP library
- Open multi-computing middleware
- Software defined agnostic fabrics
- OpenVPX (VITA 65) digital processing
- OpenRFM RF processing
- Air Flow-By (VITA 48.7), Liquid Flow-By cooling
- RACE, RACE++, Serial RapidIO switch fabrics
- Miniature DRFMs
- Secure Defense Grade SSDs

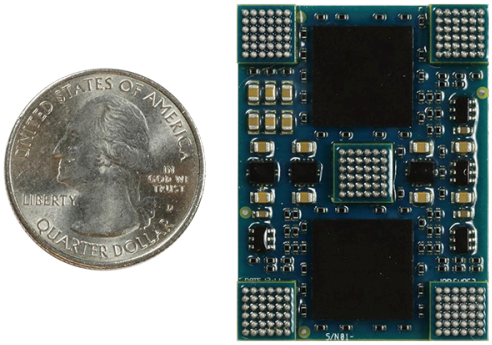
Leveraging focused IRAD

Mercury is fundamentally a commercial company that operates in the defense business. We continually invest 12-15% 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.

These investments have produced the broadest, most contemporary portfolio of embedded digital and RF processing capabilities and building blocks across the whole sensor processing chain. We build-in a layered and customizable, or turn-key security framework for system integrity which is fundamentally required for modern defense processing applications.

For certain deterministic, mission/safety-critical applications our processing solutions are built for the highest design assurance level (DAL) certification. These systems are delivered with their required safety artifacts to prove their designed-in flight safety certification qualification.

In recent years, using our next generation defense electronics business model, Mercury has made over $700M of focused investments, in a manner that any world-class high-tech company would recognize.



Dense and rugged system-in-package for greatest microelectronic density

We have made investments that differentiate our MOSA solutions by enabling them to cool themselves better for greater reliability, giving them greater processing density, developed system-in-package and 3D fabrication technologies for the greatest miniaturization and ruggedization. We have made investments that have delivered the most advanced, comprehensive built-in security and we have modernized and automated our Advanced Microelectronics Centers (AMCs). AMCs are Mercury's domestic design and manufacturing facilities and are pivotal for secure and trusted defense electronics manufacture. These world-class manufacturing facilities produce today's most advanced defense electronic solutions.

> ***"Prime contractors are developing next generation supply chains for flexibility, responsiveness, consistency, risk mitigation with built-in security and trust."***
>
> Ref MForesight report MF-TR-2017-0201, funded by NSF and NIST.

The traditional approach to outsourcing is the pursuit of the lowest cost option with acceptable quality. Shooting low usually unintentionally committed the organization to unplanned resource commitments and schedule delays as lowest requirements fell even marginally short. Globalization has rendered this model now unsustainable for defense electronics manufacture.

The new supply chain paradigm demands flexibility, responsiveness, consistency and risk mitigation which increasingly mandates built-in security and trust – collectively this is the real, new, actual cost of ownership. The DoD, Department of Energy (DoE) and National Institute for Standards and Technology (NIST) are all seeking data-driven, sustainable, flexible, local and collaborative supply chains that use proven technologies. They call these supply chains Next Generation Supply Chains. This approach builds in competitive advantage, trust, sustainment and flexibility and will increasingly be required by domestic defense contractors.

Trust and information protection

Trust is important for all vendor relationships and for defense prime contractors trust is critical, multifaceted and increasingly required by contract and mandate. A prime contractor needs to trust the products being produced for them and also trust all functions associated with the production of those goods, and in many cases to be able to prove that trust.

The prime contractor has to trust that their intellectual property (IP) and issued equipment is safe, won't be used to competitively disadvantage them, and it won't be used for espionage or product performance compromise. They require active devices used within their processing solutions to be trusted, from known and vetted sources and that the facilities used to produce their goods are secure, have a robust physical and cyber security posture. If there isn't a robust, demonstrable trust framework, everything else is for naught. Security is that important!

> ***In 2014 IBM, the last major US domestic manufacturer of data-center blades sold their x86 (datacenter servers) business to Lenovo (China) – Leaving the DoD without a trusted supplier for this critical piece of equipment.***

Mercury's facilities have a deep embedded trust culture that is rigorously maintained and is demonstrable. Mercury is an ethical, publically traded, US corporation whose next generation defense electronics business model is enabling prime contractors to win more business, which in turn grants Mercury financial and organizational stability – our customers can rely on Mercury for the long-term.

All Mercury defense processing solutions, whether designed and made with Mercury and/or Mercury's customer's IP are made, tested, coded and supported in the USA by US citizens/permanent residents. The devices used within these defense processing subsystems are sourced from trusted, approved suppliers via our actively managed supply chain. Devices are individually tracked and robust counterfeit screening is employed for additional, demonstrable traceability and trust.

Mandated trust and a robust cybersecurity posture

Cyber threats are increasing in frequency and sophistication, which is eroding trust due to the loss of the confidentiality and integrity of sensitive defense information. The DoD has responded to the severity of these threats by declaring traditional information assurance practices to be insufficient. They have gone on to prescribe a more rigorous set of security controls for use in safeguarding defense information.

> ***Program and technical information requires robust protection, and a prime must have full assurance that their supplier can provide a resilient cyber defense. This has become a critical requirement since many threat actors have now switched their attention from attacking the primes to focusing on their supply chains instead.***

In October 2016 "Safeguarding Covered Defense Information and Cyber Incident Reporting" (DFAR supplement 252.204-7012) directed prime contractors and their supporting subcontractors to provide "adequate security" for any covered defense information (CDI) in their possession. In this context, "adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized information access. In order to satisfy this requirement, a contractor must meet all 110 security requirements outlined in NIST SP 800-171r1…as a minimum.

These requirements are focused on the protection of CDI data as it is collected, developed, received, transmitted and stored in support of a contract. The requirements must be met by contractors who work with CDI as soon as practical but not later than December 31st, 2017.

The DoD makes it clear that the protection of CDI data is so critical that it trumps all other considerations. If an organization cannot meet these security requirements and be able to demonstrate their compliance, then defense suppliers are at risk of losing contracts.

Minimum requirements list for the protection of CDI data

- Compliance with DFAR 252.204-7012
- Security requirements listed in NIST SP 800-171r1 fully satisfied
- Secure, trustworthy, domestic facilities
- A written System Security Plan and Plan of Actions and Milestones

The security controls prescribed in NIST SP 800-171r1 include robust protections such as multi-factor authentication (e.g. password and fingerprint), FIPS-validated encryption, and a rigorous approach to privileged account management. These controls form the backbone of the robust security program required of all defense contractors regardless of size, if they are to work on government contracts involving CDI. However, the importance of these requirements is not universally appreciated, as they are often not fully implemented outside of prime contractors themselves.

Mercury had already fortified our operations by establishing a security program based on the Critical Security Controls which we established ahead of the published DFAR requirements. We perform most customer work in a protected enclave where the security posture exceeds the requirements of DFAR 252.204-7012.

Mercury's world class approach to cybersecurity protects our company, our customers, our nation's security interests and most importantly, the US and allied warfighters. We continue making key cybersecurity investments to improve our capabilities and strengthen our security posture. All the members of our security team are highly trained Certified Information Systems Security Professionals (CISSPs). We augment our dedicated team through our partnership with FireEye, whose expert analysts monitor our company networks 24/7, ready to respond to anomalies in real-time.

Best affordability for competitive advantage

A primary motivation to move to a subcontractor is to lower costs and risk transfer. Inherently, subcontractors are honed specialists with modest overheads making them more agile, focused and efficient. Mercury amplifies these advantages by applying our next generation business model which reduces risk and cost by:

SMT component placement and automated component inventory carousels

- Making investments to develop processes and applied capabilities that anticipate and intersect with our defense industry customers' future needs.
- Building in the defense industry's most robust, system-wide systems security engineering (SSE), cyber resiliency and trust for exportability
- Using an open systems architecture across the whole sensor and mission processing chains for scalability and tech refreshes – the ease at which future hardware can be seamlessly upgraded while protecting our customers' most valuable asset – their application software
- Designing our open system building blocks for interoperability and efficient manufacturability and test
- Leveraging the best commercial technology to "square" Mercury's IRAD. Mercury adds our focused IRAD on top of the best existing commercial technology, which was developed using a separate bucket of IRAD money, hence IRAD squared
- Investing in automated surface mount technology (SMT) fabrication, inspection and test lines for consistent, affordable board fabrication
- Investing in automated RF/mm-wave fabrication, assembly and test/tune lines for high yielding, precise, repeatable RF manufacture
- Applying proven IP and committing to its reuse through interoperable, open system architecture building blocks that lower risk and drive program velocity. This commercial approach to technology investment spreads development cost efficiently over many programs
- Reducing components by consolidating them in to single entities and/or by increasing the processing density so that less processing modules are required per solution

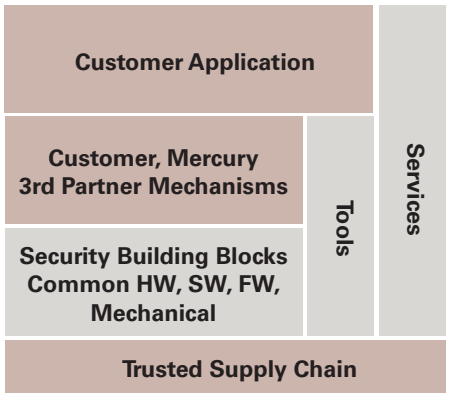
Collectively these capabilities enable prime defense contractors to field solutions quickly, build-in security and other product performance differentiation, while compressing program schedules, lowering risk and driving affordability.

Mercury's next generation defense electronics model helps primes to win more business by:

- Building in security for FMS and DFS
- Building for safety certification
- Reducing program risk
- Reducing costs
- Reducing development time
- Reducing product manufacturing time
- Enabling tech refreshes at the speed of technology
- Supporting whole program life cycles
- Building in competitive product differentiation
- Leveraging the best commercial technology

No more waivers - more business with built-in systems security engineering

Prime contractors are increasingly looking to export their defense systems via foreign military sales (FMS) and direct foreign sales (DFS) to generate additional revenue. From a strategic vantage point FMS and DFS equips our allies with compatible, interoperable capabilities that help to spread not just the financial load but also the defense load. Such technology transfers had typically required some degree of built-in security, but the requirement was often waived for expedience. When security was applied to mission critical applications it was oftentimes an afterthought and was subsequently bolted-on.



Secure mission and sensor processing architecture

The DoD has ruled that no more security waivers will be issued for FMS and DFS programs. Defense electronics that are going overseas will require built-in security or systems security engineering (SSE). Even allies like to look under the hood and not everyone is an ally. Systems security engineering counters nation-state reverse engineering efforts and is critical for FMS and DFS export programs.

BuiltSECURE™

Mercury processing solutions with BuiltSECURE technology counters nation-state reverse engineering with security engineering (SSE). BuiltSECURE is built-in SSE that enables turn-key or personalized security solutions to be quickly configured. The extensible nature of Mercury's SSE delivers system-wide security 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 has developed the broadest, most contemporary portfolio of security building blocks that work in conjunction with our built-in security framework to enable our customers to create their own personalized system-wide security or take a turn-key option off the shelf. The built-in security framework can be refreshed over time to counter new threat vectors. Our security framework is seamless across software, firmware and hardware. 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.

Recipe for best, proven commercial embedded security

Effective security systems engineering must be:

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

Mission critical applications must be safe

Most, if not all defense electronic solutions, require built-in security and some, especially if they are applied to aviation or vehicle autonomy are required to be safe and deterministic. 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. Such certification is required for safety/mission critical and flight safety processing functions such as fire control, avionics/vetronics and heads-up displays (HUDs). As sensors are making more decisions and platforms are becoming autonomous, safety critical processing is increasingly required.

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.

Safety-critical mission computer with embedded BuiltSAFE technology

Mercury applies a top down approach to building in DAL in to our open system architecture building blocks. We have more European Aviation Safety Agency (EASA), Federal Aviation Agency (FAA), Joint Aviation Authorities (JAA) and Transport Canada experience and the widest portfolio of building blocks, interfaces, software and safety certifiable fabrics/buses, making Mercury processing solutions that require flight safety certification the lowest risk.

The best partners work together

Prime defense contractors are seeking to partner with fewer, more capable tier-1 suppliers. They recognize that a few, really good suppliers are easier to manage, bring more to the table and are inherently more secure and trustworthy. Working with world class teir-1 suppliers enables prime contractors to build in quality using built-for-manufacturer and built-for-test manufacturing principles. And increasingly, prime contractors are recognizing that a supply chain is as strong as its weakest link. This is problematic, as it is difficult to see deeper than first tier level suppliers.

Mercury is a world class commercial manufacturing company operating within the defense electronics domain. We are organized to complement and augment our prime contractor customers' infrastructure and capabilities. Our program managers work closely with our customers, engaging engineering, QA, qualification and documentation specialists as required. We use similar tools as our customers for efficient information exchange. Mercury program and product managers actively oversee schedules, anticipate and mitigate program risks and manage component sustainment until end of product life. Working with our compliance, product management, QA and supply chain personnel, they drive program requirements down through Mercury's supply chain.

Mercury uses common defense industry tools for better customer engagement:

- PDM Vault/SolidWorks (Mechanical)
- CosmosWorks (Thermal simulation)
- Cadence/Allegro (PCB layout)
- Mentor (PCB schematics)
- HPVee/LabVIEW (Test automation)

Mercury program managers are often found onsite with our customers, championing deeper relationships and integration, highlighting program/product efficiencies and expanding our customers' capabilities. Program managers are responsible for the well-being of their customers' program. Mercury program managers maintain our customer score cards and are the customers' voice within Mercury.

Sustainment Mercury's processing solutions are developed with whole life cycle considerations built-in. Commercial items may have a 2-4 year product life cycle, whereas defense processing solutions more typically have a 15-20 year product life cycle. We carefully select devices from stable, world-class original equipment manufacturers (OEMs) that produce device configurations with enhancements for embedded applications (extended temperatures ranges, real-time functionality, etc.). Additionally, we seek components that are supported with OEM commitments of extended availability (7-10 years or longer).

Selected devices are continually monitored for proliferation of product change (PCNs) and end of life (EOL) notifications. This function is more complex than is immediately apparent but is critical for long-term defense program sustainment. Mercury has invested and established robust monitoring mechanisms that detect limited component availability and creates product sustainment options through alternative, acceptable component substitution, timely end of life buys and managed inventory.

Selected devices are sourced only from approved OEMs or their authorized distributors. Mercury has established and maintains a robust end-to-end supply chain management infrastructure using Society of Automotive Engineers (SAE) standards to detect fraudulent and counterfeit devices (AS5553B and AS6496 for electrical, electronic, electromechanically and processing components and assemblies).

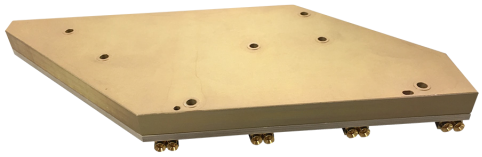
Automated, managed and environmentally controlled component storage and kitting

A robust device selection process, sourcing, tracking and monitoring goes a long way to mitigating the need to enter the gray market which many suppliers find themselves in when blindsided by diminished component supply. Although regulated by AS6081, the gray market is by definition a "lawless" place which is inherently more risky, leaving a supplier open to compromise. Mercury's consistently deploys a trusted supply chain without gray market content.

Trusted devices Mercury's supply chain is actively managed and permits only qualified supplier list (QSL) companies to supply only qualified product list (QPLs) devices. Critical devices may be monitored along the supply chain and throughout production. Their progress is documented through an assured custody chain process. Our assured custody chain process may be applied to classified and unclassified integrated circuits. For further integrity, silicon devices can be characterized through testing across a broad range of temperatures (-40 to +125oC). For exceptionally critical applications, we have developed a suite of techniques to eradicate rare silicon cell defects.

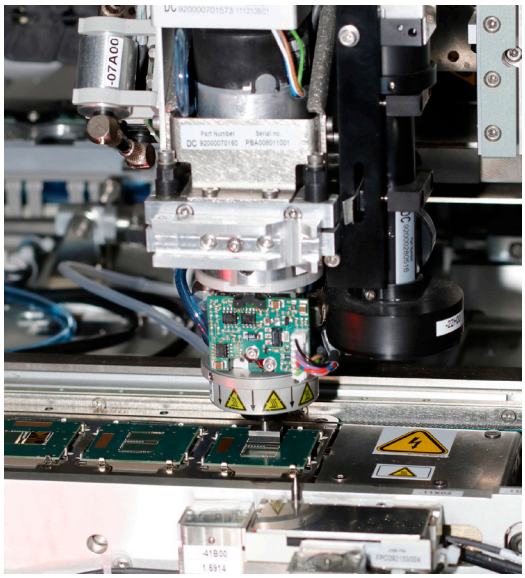
Responsive, scalable manufacturing – Built to print/specification

From new product introduction, to full rate of production, to sustainment, to end of product life, Mercury's next generation defense electronics business model prepares the enterprise to manufacture our customer's future processing requirements.



High-efficiency AESA Tx/Rx radar tile

Mercury applies the best, commercial, world-class manufacturing capabilities and augments them with in-house developed capabilities and processes that are tailored for defense electronics and RF manufacturing. Our manufacturing and test processes, with their supporting documentation and verifications are standardized and deployed across each of our AMCs. Multiple AMCs equipped with similar equipment, processes and work practices ensure our customers' program requirements can scale, while they have the assurance of supply.



Automated SMT die attach

Mercury AMCs are fully equipped design, NPI and secure scalable manufacturing centers. Each facility has full in-house processing capabilities enabling products to be produced under one roof for low-risk, manufacturing velocity. Mercury manufacturing domains includes:

Advanced Microelectronic Center (AMC) capabilities

Capability	Specifics
Fabrication	Package shrinking Multi-layer chip fabrication System-in-Package miniaturization SMT fabrication Device underfill and encapsulation
Digital	Memory miniaturization Secure solid state storage Custom defense microelectronics
Software coded in US	BIOS Ethernet stack SSD controller Software defined fabrics Cyber resiliency Secure hypervisor
RF	RF miniaturization Wire-bonding Hermetic sealing Testing and tuning Exotic dielectric material processing Thick and thin-film processing Integrated Microwave Assemblies (IMAs)
Screening qualification	Environmental (to Gun hardened) Space qualification (Radiation hardened)
Built-in product features	Built-in system-wide security Highest design Level Assurance (DAL-A) DO-254 (hardware) DO-178 (software) Best cooling 300W per 6U OpenVPX module Most powerful processing Intel SkyLake devices Fastest fabrics 40Gb/s, robust roadmap to 100Gb/s over copper backplane Most rugged packaging 100,000g gun-hardening Best SWaP performance 80% reduction microelectronic miniaturization
Services	Build-to-print Build-to-specification Processing subsystem pre-integration Guaranteed performance of software over hardware Innovative technology for product differentiation

Innovative technology for product differentiation

Mercury investments have produced robust capabilities for greater ruggedness, reduced size, weight and power (SWaP), robust built-in security and easier safety-certification and software porting. Mercury is able to focus a consistent and reliable stream of IRAD in to technologies that produce the most differentiated and powerful defense processing solutions available and the ability to manufacture them efficiently. Mercury is the only commercial company that consistently builds in differentiating innovation as a matter of course in all of our processing solutions.

Commercial contract manufacturers attach large pin devices with connectors or land grid arrays (LGAs) - neither approach meets with military ruggedness requirements.

To demonstrate Mercury's built-in product differentiation, consider the most powerful processing capability build to date – the Intel Xeon-SP (SkyLake) powered datacenter. Mercury is the only commercial company with the capabilities to ruggedly embed Xeon-SP devices for defense applications. Our captive capabilities enable the most powerful processing

technology to be taken to the tactical edge. Other manufacturers may offer more easily packaged mobile devices - Mercury is the only commercial company that reliably embeds Xeon-SP processors for full cloud capability anywhere.

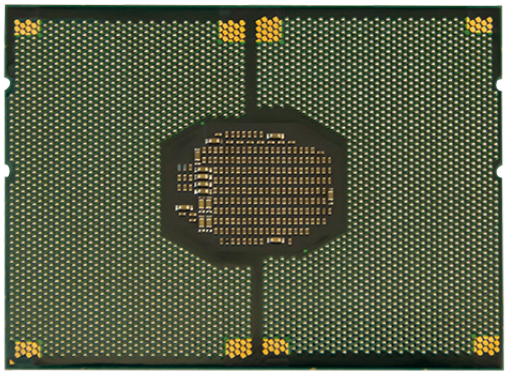
8 of the top 10 most compute-hungry military platforms are powered by Mercury processing solutions, including:

- Predator/Reaper and Global UAV platforms
- P-8 Poseidon, E-2D ISR platforms
- F-35 and F-22 5th generation fighters
- Gorgon Stare, "the unblinking eye-in-the-sky"

Ref - COTS Journal, January 2015

Embedding Xeon-SP processors for defense applications requires innovative design and robust manufacturing capabilities in four domains – Protective packaging, miniaturization, effective cooling and unrestricted pipes (I/O). Now in our fifth generation of Xeon-SP packaging, Mercury's sustained IRAD commitment meets these four requirements with:

Rugged packaging Xeon-SP devices are intended for benign environments which allow each device's thousands of I/O connections to be accessed with land grid arrays (LGAs). LGAs are cost effective for datacenters but unusable in defense applications due to shock and vibration (LGAs are not "hardwired"). Mercury has developed processes that solder each processor to its respective substrate/PCB ("hardwired"). We use tin/lead (SnPb) solder to mitigate gold embrittlement and reduce tin whiskers, both of which are features of modern commercial solders.

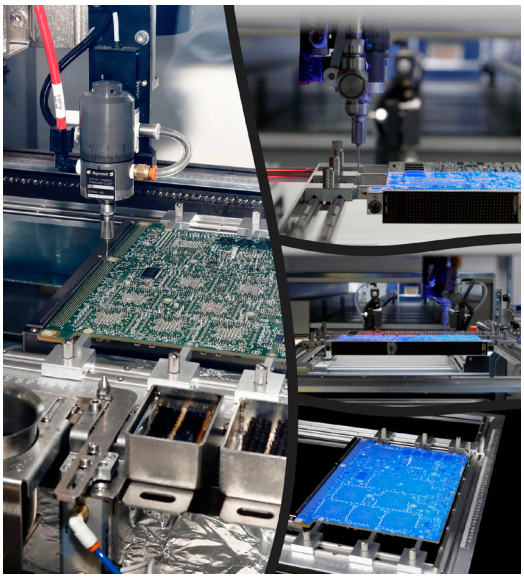


Intel Xeon SkyLake processor ready for rugged BGA substrate attach

Commercial devices invariably have gold plated terminations (ready for commercial solder reflow processing). Gold plating is notoriously a wide-tolerance process that produces gold films that vary from device to device and especially from device batch to device batch. Too much gold plating leads to gold embrittlement, which introduces inherent vulnerabilities in to the resulting circuit.

Mercury uses an effective wicking process to remove excess gold resulting in solder joints without problematic, long-term baked-in vulnerabilities derived from gold embrittlement.

Conformal coats protect circuits from moisture and abrasion and are a barrier to tin whisker growth. Mercury protects electronics with specialty coating including acrylic, parylene that supplements our baseline Mil-I-46058C and IPC-CC-830 compliant urethane coating. Mercury complies with the Government Electronics and Information Technology Association (GEIA) GEIA-STD-0005-2, Level 2B: standard for mitigating the effects of tin whiskers in aerospace and high-performance electronic systems.

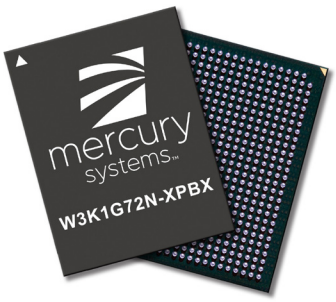


Conformal coating

Xeon-SP processors are intended for use in low-mechanical exertion, temperature-controlled environments and need to be prepared for rugged defense applications. The SnPb solder ecosystem is the most reliable for defense grade electronics but is generally less understood by commercial manufacturers, who by regulation (RoHS, WEEE) are not permitted to use it within commercial electronics intended for Europe. Mercury's defense industry focus means we use the more robust SnPb solder ecosystem. We have developed comprehensive capabilities to reprocess commercial gold-terminated devices and make them ready for SnPb solder reflowing. For especially harsh applications, we may also underfill our soldered devices with epoxy for additional reliability and security.

Soldering Xeon-SP processors to their substrate/PCBs requires the reflow of over 3,800 solder joints per device. The integral process of reflowing such complex devices requires rigorous verification. Mercury validates all our SnPb reflowed devices and underfill coverage with 3D X-ray inspection and automated visual inspection equipment for flawless quality and assurance of functionality.

Miniaturization is required to shrink the overall server package from a 19-inch rack server footprint, to a dense, defense grade open system OpenVPX format - a volume reduction of over 90%.



This miniaturization includes shrinking the vast amount of memory servers require. Mercury memory modules are soldered perpendicular to the PCB for cooling efficiency, density and ruggedization (essentially we are soldering in three dimensions instead of the usual two). For even greater packaging density, system memo-

ry is stacked as monolithic, multi-level entities. Stacked memory reduces their board footprints by nearly 80% without any performance or reliability degradation. Memory stacking enables huge memory resources to be placed close to the server-class Xeon-SP processors where board space is a premium. This technology is a subset of Mercury's overarching system-in-package (SiP) suite of fabrication capabilities. SiP technology miniaturizes electrical functionality across flip-chip, wire-bond, and surface mount technology (SMT) domains in to a single, rugged entity that in some applications may be gun-hardened to 100,000g.

Best cooling Mercury has developed the most effective and efficient conduction, air, liquid and hybrid cooling technology available for open system embedded processing. This cooling technology enables densely packaged Xeon-SP powered packages to operate reliably at full throttle for unrestricted, deterministic processing. Mercury cooling technology removes more heat to lower each device's temperature by several degrees, for a magnitudes increase in meantime between failures (MTBFs) and enables thermally dense devices, like Xeon-SP processors to be deployed in small packages.

Unrestricted fabrics As fabrics get faster and faster, modular open system compute architectures are facing bandwidth limits within their interconnects and backplanes. Mercury has developed backplane technologies that enable full, unrestricted fabric performance (currently 40Gb/s) across the largest processing subsystems and temperature ranges. This technology is scalable, giving Mercury a clear roadmap to 100Gb/s fabrics across copper backplanes, while still remaining fully OSA complaint. And, Mercury's optional FPGA-powered software approach to switch fabric implementation, removes the need to change hardware to implement future fabric upgrades.

All of these technologies are fully open systems compliant and/or enable open systems solutions to perform better and more reliably. Collectively they are making full Intel Xeon-SP cloud computing capabilities possible at the tactical edge. This enables our prime customers to leverage the full ecosystem of datacenter software, develop system roadmaps that track Intel's, build in product differentiation (no other commercial company can embed Xeon-SP processors) and grants them access the same suite of capabilities to cool, protect and pre-integrate their complementary IP.

Commercial electronics are produced for global consumption – one product configuration for everywhere. Access to the European market mandates (RoHS and WEEE) that electronic circuits, including solder must use less than 3% lead, eliminating the proven SnPb solder ecosystem for commercial manufacturers. This has created three defense electronics obstacles:

- Solder whiskers and gold embrittlement have re-emerged as significant quality problems associated with low-Pb solders
- Commercial electronics manufacturers are losing their capability to reflow SnPb solders
- Devices are no longer produced with SnPb compatible terminations

The ability to embed Xeon-SP devices or other equally challenging processing elements into defense grade applications gives Mercury's customers a clear and differentiated competitive advantage. This competitive advantage increases, as other Mercury manufacturing and pre-integration capabilities are introduced.

Mercury pioneered OpenVPX, the de facto embeded OSA for digital processing and we are doing the same in the RF processing domain with OpenRFM. OpenRFM leverages the reuse of the best technology enabling RF/digital solutions to be more quickly engineered with lower-risk.

Mercury's customers are able to take delivery of fully pre-integrated processing solutions across the whole sensor processing chain, in the RF and digital domains. We guarantee the performance of pre-integrated software to work across our pre-integrated hardware. We protect our customer's most valuable asset - their application software by using open middleware and fully open systems compliant hardware. This commercial approach enables defense processing subsystems to be upgraded at the speed of technology. As the hardware is refreshed, our open middleware (MPI/OpenMPI) supports our customers' application throughout the process.

What is *OpenRFM*™?

OpenRFM is a modular, open architecture that standardizes interfaces, hardware and protocols – it is ideally suited to EW and multi-spectral processing applications.

OpenRFM's benefits include:

- Affordability that is driven by high-channel density, modular design and pre-integration of proven RF and digital processing building blocks
- Sustainability though reuse of standardized technology that preserves our customer's application investment - making it "future proof"
- Flexibility of many system designs using common building blocks
- Interoperability driven by modular open architecture, standardized control plane and interfaces

OpenRFM's standard interface streamlines the production of integrated microwave assemblies by reducing their time and cost to test and tune.

Culture of quality for consistent outcomes

Mercury builds-in quality to our processing solutions, we validate quality with vigorous environmental screening, testing and inspection.

Training Mercury's AMCs have spirited LEAN/Six Sigma cultures. Staff throughout the manufacturing process maintain quality with peer-to-peer reviews, continuous improvement exercises and second-eye inspections. Every operator inspects the work performed by the previous operator before executing their own operation. In turn, this work will be inspected by the next process operator. Operators receive on-going cross-training and sustained re-training, giving them the insight and knowledge to effectively inspect work throughout the manufacturing process with a broad perspective of the complete fabrication process. Our highly cross-trained process operators enable us to level (LEAN manufacturing) shop floor loading for optimal product velocity, with the shortest wait times.

Six Sigma improves quality by removing the causes of production defects and minimizing variability in the manufacturing process. It uses statistical methods to improve quality with a goal of 3.4 defects (or less) per million.

Few (even high-volume, single product) manufacturers ever achieve this goal. Mercury applies Six Sigma tools for continuous improvement enabling Mercury to make ever better, more reliable and cost efficient products.

Mercury builds in quality along the whole manufacturing line, operator by operator, process by process. At critical product production steps, including final inspection, each product is formally inspected by dedicated QA personnel, who document their findings. Each dedicated quality inspector is trained to a minimum of IPC610 class 3 (acceptability of electronic assemblies).

Built-in quality Mercury has a sustained commitment to staff training and process development. Mercury products are designed for manufacturability and designed for test. We co-locate process engineers within all our AMCs. All manufacturing processes are carefully executed according to paperless work instructions. These work instructions rely primarily on illustrations to clearly and efficiently communicate the process steps, parameters and metrics.

Processes are systematically developed through structured design of experiments (DOEs) which run on the actual equipment they will be deployed upon. Processes are developed one variable at a time. Once a variable is optimized, it doesn't become part of the formal process until it has been turned-on/off three times. When process parameters are dialed in and proven, they are documented, which then require an engineering change order (ECO) to modify them.

Processes that require specific operating parameters to be established and maintained are monitored using statistical process control (SPC) tools. SPC lets operators see in real-time any process drift or variation. This real-time feedback enables the process to be realigned, usually without the loss of time or any product quality implications if it begins to drift. Tight SPC detects and flags process drift before it becomes problematic.

	Mercury AMC	Commercial Contract Manufacturer
Built-in product trust	✓	?
Trusted supplier infrastructure	✓	?
Built-in product security	✓	X
Secure supplier infrastructure	✓	?
Affordability (total cost of ownership)	✓	?
Defense industry compatible processes, tools	✓	X
Shared IRAD	✓	X
Built-in product differentiation	✓	X
Optimized and guaranteed software over hardware	✓	?
Pre-integrated RF/digital processing	✓	?
Regional, scalable, redundant manufacturing facilities	✓	?

Mercury manufacturing Vs. commercial contract manufacturing

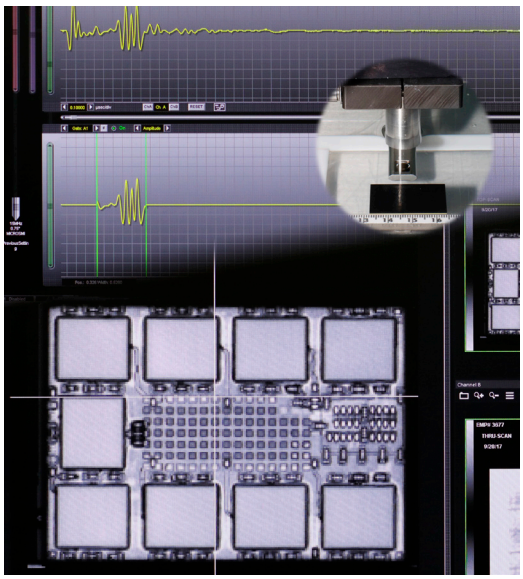
Test and inspection Every product Mercury produces is visually inspected. Inspections may be manual by trained inspectors, automatic using automated visual inspection equipment that systematically detects circuit and packaging defects. Deeper analysis or confirmation of process quality may be determined through cross-sectional analysis or scanning tools.

In-line automated visual inspection

Scanning inspection tools include X-ray, 3D X-ray, C-SAM ultrasonic scanning and Sonoscan which are placed either in-line with the processes they oversee or as part of an AMC's failure analysis lab. Failure analysis investigations are summarized using an 8D reporting format, a format that is compatible with our customer's documentation.

Mercury guarantees and optimizes the performance of our software over our pre-integrated hardware – Our customers have the knowledge and assurance that Mercury will not stop working until their processing solution is complete.

PCB fabrication and electrical circuit products are inspected to IPC 610 (assembly inspection) and IPC-J-STD-001 (solder) workmanship standards. Rework, should it be required is performed to IPC 7711/7721.



Confocal scanning acoustic microscopy (CSAM) inspection

2D and 3D X-ray inspection stations

Automatic electrical testing may be performed using a dedicated bed-of-nails to probe the circuit, or increasingly with flying-lead probes that removes the need for dedicated test.

RF testing and tuning may require dedicated test fixtures and programs. OpenRFM defines and standardizes RF interfaces and test protocols to reduce fixture cost/time, reduce test/tune duration and risk. OpenRFM brings a standardized approach to RF testing and tuning complex RF assemblies and is wholly scalable across all Mercury's AMCs.

Environmental screening Environmental screening is often overlooked as a critical defense electronics manufacturing asset by commercial manufacturers. In relatively, this function of defense manufacturing is oftentimes the most critical for a number of reasons. Firstly, depending upon the environmental tests required, their severity, complexity and duration, the process can be lengthy.

Secondly, many manufacturers don't have the full suite of tests required to stimulate or the ability to apply multiple stimulation combinations simultaneously.

Agile and scalable pre-integrated DRFM using MOSA building blocks

Thirdly, and this is especially applicable to larger product runs, most manufacturers simply don't have the number of test stations required to handle the volume of products at an elevated production rate. If there are insufficient test stations available, months can be added to the lead-time, as long duration environmental tests backup. Mercury has invested in dozens of comprehensive environmental workstations that effectively screen products to various MILSTDs and customer requirements without queue time, adding only the duration of the tests/screening themselves to the over product lead-time. Mercury environmental test stations effectively test/screen to MIL STD PRF-38534 (H and K) for hybrid microcircuits, STD PRF 38535 (M) for integrated circuits and MIL STD 883 for microelectronic devices.

World-class facilities for defense electronics manufacture

Mercury AMCs are private, secure, secret and trusted facilities that share common processes and documentation. Each facility performs all manufacturing in clean rooms with cleanliness rating of 10K or better for product reliability and performance, with "dirty" processes like device singulation performed just outside. All facilities are protected with backup power generation preventing power outages from adversely affecting production.

Each facility has all the processes required to build products in-house without transferring them to third parties for processing, inspection or other augmentation. Having all required manufacturing, testing and screening capabilities under one roof adds to product velocity, reduces security vulnerabilities and program risk. Only calibrated processes are performed on the products we produce. Mercury AMCs are AS9100, ISO 9001:2008, ISO 10012 certified.

QUALITY MANAGEMENT SYSTEM
AS9100
CERTIFIED

Device singulation (substrate dicing)

Trusted third party assurance

Key Mercury AMCs are Category 1A Trusted Supplier accredited for design services and manufacturing from the DoD's defense microelectronics activity (DMEA). DMEA was established by the Office of the Secretary of Defense (OSD) to act as the DoD center for microelectronics technology, acquisition, transformation, and support. DMEA is composed of highly specialized engineering facilities and microelectronic engineers that work in close partnership with major defense contractors and the semiconductor industry to provide support for fielded systems across all US military organizations.

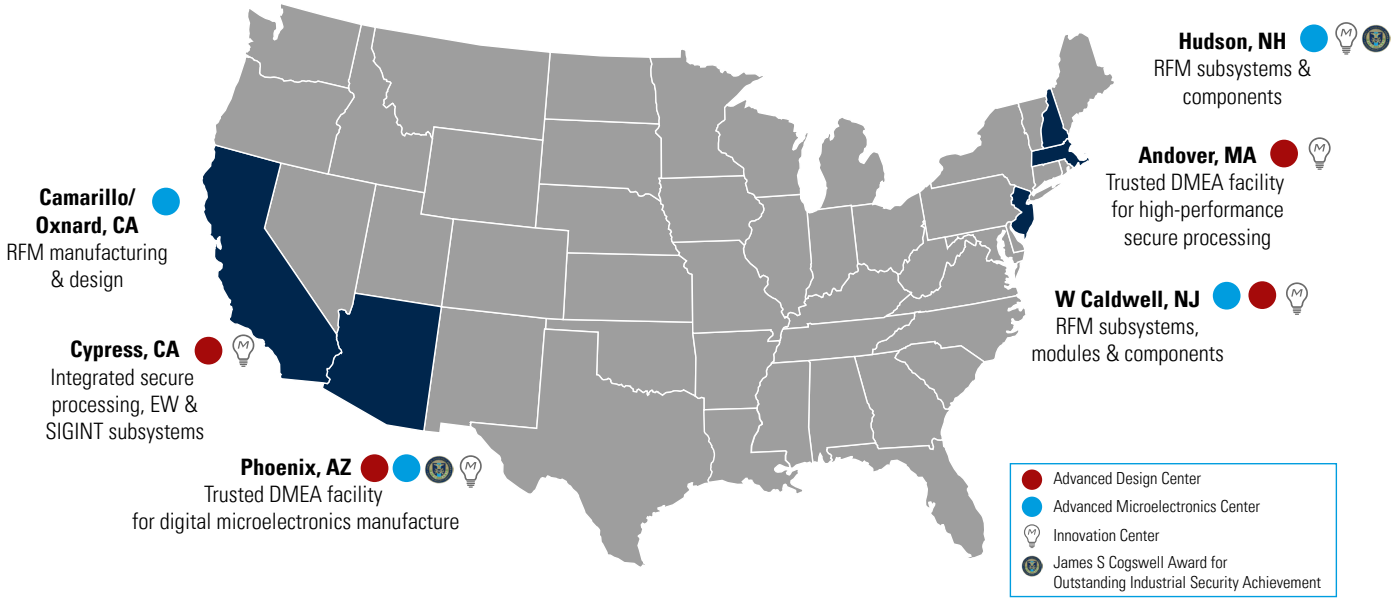
US military weapons are at risk from malicious insertions – When something is deliberately inserted into a system for a malicious purpose. Of particular concern are weapons currently in the field, which were not covered by the Pentagon's current procedures for mitigating supply chain risks.

Ref - Defense Science Board's cyber supply chain task force

Mercury AMCs have received Missile Defense Agency approval and are 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".

For the first time, prime contractors now have a secure and trusted supplier of digital microelectronics from a defense microelectronics activity (DMEA) accredited facility for design, assembly, test and broker services.

All domestic Mercury manufacturing facilities are rated superior or commendable by the Defense Security Service (DSS). Mercury's customers have presented us with awards for "outstanding achievement - excellent support - premier excellence - problem solving - affordability - competitive advantage."



Mercury AMC and Innovation Center locations

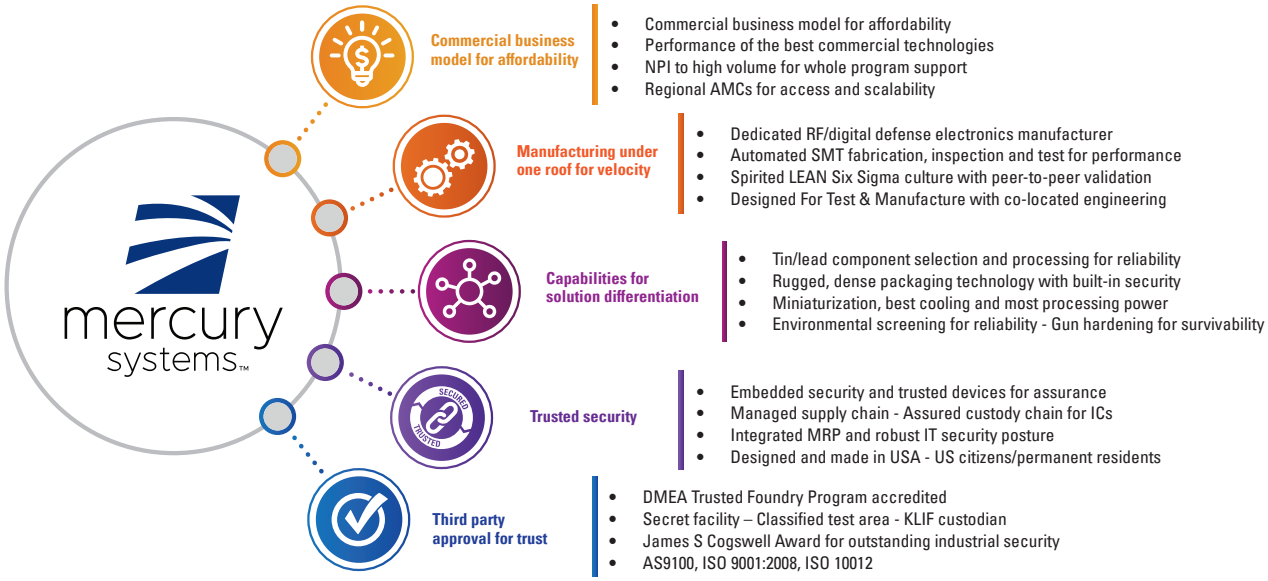
Summary

Mercury has pioneered a next generation defense electronics business model to enable the DoD to retool our defense capabilities efficiently with the best commercial technology, made secure and rugged for defense deployment. The model offsets the risk of globalized supply chains and is the vehicle to re-invigorate our defense posture and to mitigate current and future emerging national threats.

The best commercial technologies can now be applied to defense applications at the speed of technology itself. Our business model is creating innovative capabilities for next generation defense processing systems with the support of rapid deployment through secure world class manufacturing. Innovative technology deployed quickly is enabling defense prime contractors to win more business and field more elegant defense solutions.

The next generation business model anticipates future defense electronics requirements, invests in the technologies, capabilities and facilities necessary to manufacture these products when they are required. This model leverages the best commercial business practices and technology for the highest processing performance, interoperability, while driving affordability and program velocity. Mercury makes ready this technology for defense applications by building in trust and security while making them rugged and supporting them with long-term sustainability programs. Our open systems approach supports relatively easy tech refreshes that builds in future-proofing. This agile and practical approach to modern defense electronics manufacture enables the fielding of the best defense processing solutions quickly; we are "putting technology into the hands of our warfighters faster."

Mercury is proud of the capabilities we have developed. To demonstrate them, we have equipped our AMCs with Innovation Centers that display our pre-engineered defense electronics building blocks that span the whole sensor processing chain, in both RF and digital domains. Innovation Centers also introduce AMC manufacturing capabilities that produce the most differentiated, secure defense processing solutions available.



Innovation Centers

Mercury's Innovation Centers are located in Massachusetts, New Hampshire, Arizona, New Jersey, California and Switzerland and they showcase our solutions across the sensor and mission processing chain. Each Innovation Center also displays specific facility expertise including RF/mm-wave, digital processing and processing subsystem pre-integration. We encourage our customers to visit an Innovation Center, to see first-hand why Mercury's integrated defense manufacturing is an Innovation that Matters.

Table of Acronyms

AESA	Active Electrically Steered Array
AMC	Advanced Microelectronics Center
BBP3.0	Better Buying Power (rev 3.0)
DAL	Design Assurance Level
DFS	Direct Foreign Sales
DMEA	US Defense Department's Defense Microelectronics Activity
DoD	Department of Defense
DOE	Design Of Experiment
DoE	Department of Energy
DSS	Defense Security Service
EASA	European Aviation Safety Agency
EOL	End of Life
ERP	Enterprise Resource Planning
EW	Electronic Warfare
FAA	Federal Aviation Agency
FMS	Foreign Military Sales
GEIA	Government Electronics and Information Technology Association
HUD	Heads-Up Display
IMA	Integrated Microwave Assembly
IP	Intellectual Property
IRAD	Internal Research And Development
JAA	Joint Aviation Authorities
KLIF	Key Loading and Initialization Facility
MTBF	Mean Time Between Failure
NIST	National Institute for Standards and Technology
NPI	New Product Introduction
NSF	National Science Foundation
OEM	Original Equipment Manufacturer
OpenRFM	Open system architecture for RF processing
OSD	Office of the Secretary of Defense
Pb	Lead
PCB	Printed Circuit Board
RF	Radio Frequency
RoHS	Restriction of Hazardous Substances (EC directive)
SEA	Society of Automotive Engineers
SME	Small and Medium Enterprises
SMT	Surface Mount Technology
Sn	Tin
SnPb	Tin/Lead (solder)
SPC	Statistical process Control
SSD	Solid State Drive
SSP	System Security Plan
WEEE	Waste Electrical and Electronic Equipment (EC directive)

About the Authors

Usha Shah is Vice President and General Manager of US Manufacturing Operations for Mercury Systems, Phoenix, AZ. She is responsible for managing quality and supply chain organizations including development and achievement of P&L, operating and capital budgets, and five year strategic plan and execution. Usha earned her bachelor's degree in Physics and is a Six Sigma Master Black Belt. She also has a degree in an International Executive MBA in Practicing Management from McGill University in Montreal.

John Bratton is Manager of Product and Solutions for Mercury Systems, Andover MA. John has over 25 years of experience managing and promoting solutions within the embedded packaging, interconnect and RF domains. John earned his bachelor's degree in Mechanical Engineering from the North Eastern University of England and is a member of the IMechE and ASME.

3367.00E-1117-wp-manufacturing

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