Secure COTS

ENSURING EMBEDDED COMPUTING PRODUCTS AND SUPPLY CHAINS CAN BE TRUSTED

SMART Embedded Computing
www.smartembedded.com
January 2020

The security of COTS embedded computing products used in military and aerospace programs has become a focal point for military branches and prime contractors. This white paper addresses the issue of supply chain security, covering topics such as design authority, chain of custody and governance in supply chains.

It introduces the SMART Embedded Computing concept of 'Secure COTS', a holistic and cradle -to-grave approach that ensures SMART EC products and supply-chains can be trusted.

SMART™
Embedded Computing

Cybersecurity vulnerabilities and supply chain integrity are under the spotlight for global technology companies and users. Today's technology supply chain involves interfacing with vendors across many international borders. The current geopolitical climate has created a market discontinuity that dramatically affects US domestic critical infrastructure programs.

Securing the Supply Chain

The increasing complexity of global supply chains and associated interdependencies has raised questions for American military branches and those of allied nations worldwide.

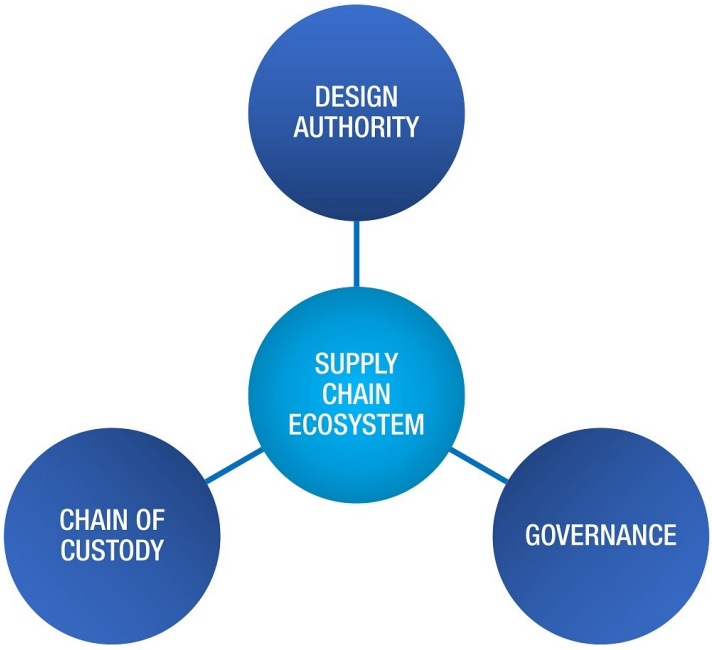
The Defense Industrial Base, which includes more than 100,000 private sector companies and their subcontractors, have historically made rational commercial decisions about their supply chains based on the golden triangle of price, delivery and performance.

These decisions haven't always accounted for the security aspects now under the spotlight.

Given the enormity of the implications, an effective supply chain security strategy must proactively minimize exposures throughout the entire product/system life cycle – from cradle (secure component design and manufacturing) to grave (ethical and secure e-waste disposal) and everything in between.

The 'Deliver Uncompromised' strategy is one of the Pentagon's responses, aiming to base even COTS contracts on security assessments in addition to cost and performance.

As the original strategy document states, *"Improved cyber and supply chain security requires a combination of actions on the part of the Department and the companies with which it does business. Through the acquisition process, DoD can influence and shape the conduct of its suppliers. It can define requirements to incorporate new security measures, reward superior security measures in the source selection process, include contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments."* (Source: Mitre Corporation)



Design Authority

While the DoD typically retains Design Authority over the architecture of complex systems that it purchases, COTS embedded computing platform suppliers such as SMART Embedded Computing (SMART EC) work collaboratively with military system architects to establish Design Authority principles, terms of reference, governance model, processes, roles and responsibilities and templates.

The contracted organization may be responsible for the design, but the authority for acceptance of a design remains with DoD.

SMART EC's internal design authority, system architects, are responsible for ensuring that the consequences of any design decision are understood. They maintain a consistent, coherent and complete perspective of the program design.

Chain of Custody

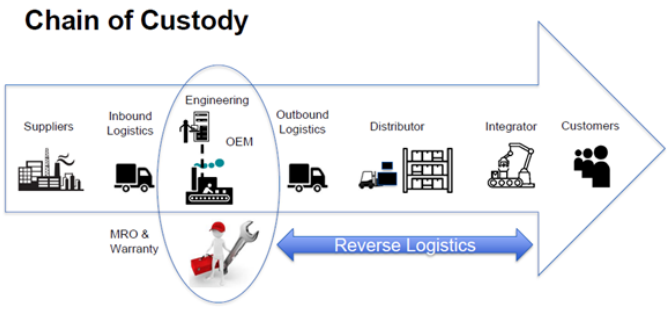
The concept of "chain-of-custody" originated in the legal context of handling evidence. In this context, chain-of-custody tracks everyone who has touched and processed the evidence.

But the concept of chain of custody is much more widely applicable.

Used with serialization and authentication, a chain-of-custody means knowing who has what, when

and where. It is a chronological documentation of all parties that come into contact with an item, and a history of all transactions.

It is useful in any context where sensitive information, or vulnerable goods, or valuable products are handled among many parties and the possibility of 'contamination' exists, which would have serious consequences.



Governance

The system of directing behaviors and decisions around procurement within an organization comes under the term of supply chain governance. It covers rules, organizational structures, policies and regulations that guide, control and lead supply chains.

This is the oversight function in comparison to the day-to-day role of supply chain management. SMART EC uses its quality processes, based on a total quality management approach, to drive integrity into all that we do. Every employee, supplier and customer is regarded as an essential part of the process.

We set an error-free performance standard, based on prevention and a 'right-first-time' attitude, and maintain a quality system in compliance with ISO standards and relevant international regulatory requirements. The use of statistical techniques commensurate with technological developments within the company is aimed at continuous quality improvement.

The objective and expectation is for customers to have full confidence in SMART Embedded Computing.

SMART EC Secure COTS

SMART EC employs a variety of control methods to ensure the security and integrity of our products from design through manufacturing and repair.

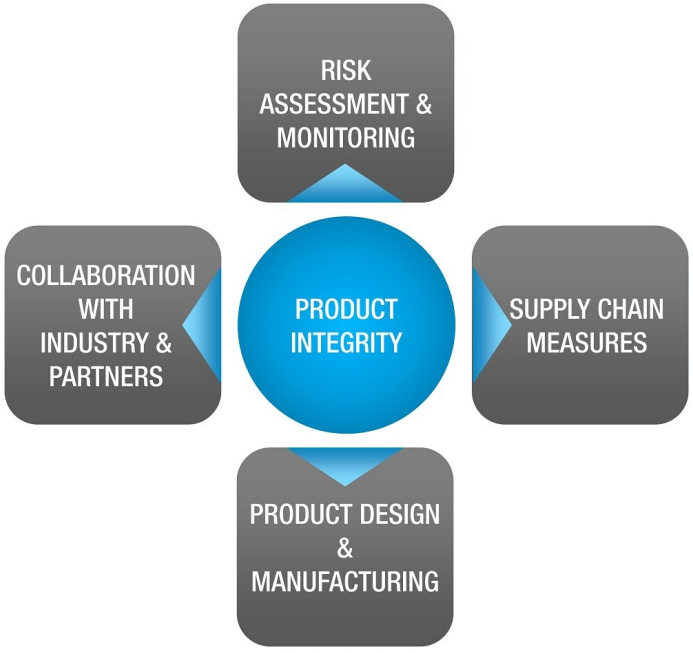
Formal quality management systems:

- SMART EC processes are ISO 9001 based
- Certified to ISO 9001:2015 standard
- Quality manual & procedures

We use a 'secure-by-design' approach to our technology planning and management, so security is considered at every stage of product development.

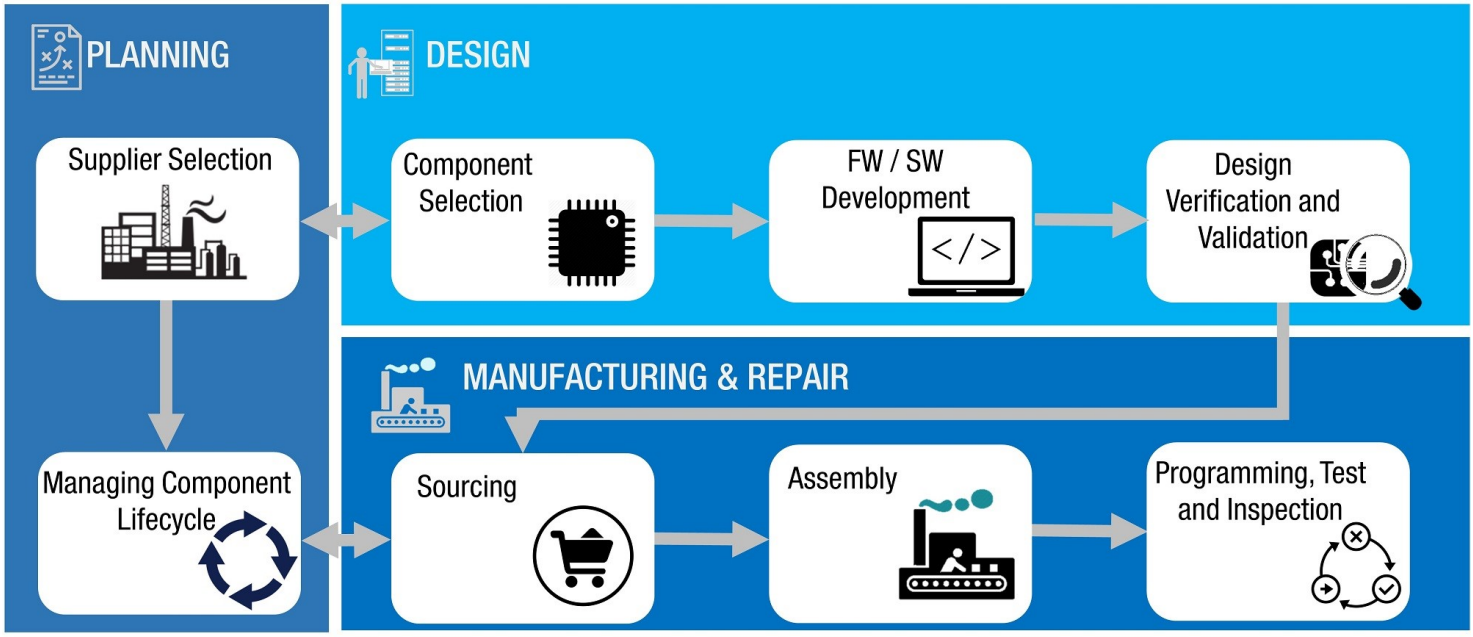
All design, supply chain management and repair is done internal to SMART EC, by SMART EC employees. All of our engineering is in-house, owned by SMART EC.

Where we use contract manufacturers or integrators, we have total control over the supply chain down to ownership of the bill-of-materials (BOM) and the suppliers to those subcontracted companies.



Supply Chain Security Measures

SMART EC has implemented thorough process controls over the product lifecycle.



Planning

Supplier Selection

There are so many suppliers of components these days that selecting the right suppliers can be a daunting but necessary step to secure the design of the product. Suppliers need to be audited, verifying that they follow standard design practices and verify their designs appropriately. Knowing where components are manufactured can be key.

Managing Component Lifecycle

To provide continuity of supply, it is essential to continually monitor component availability from suppliers. Manufacturers must evaluate change and end-of-life (EOL) notices, review them in detail for changes in specification, device packaging and manufacturing locations, and then find appropriate replacements for components that are no longer available and assure that replacements are from approved vendors and manufacturing locations.

Design

Component Selection

There are two aspects that feed into selecting the right components:

Firstly, selecting components that operate within the operational limits of the product. This assures that at the operational limits you have confidence the product will operate correctly and not cause any unknown side effects that may expose incorrect operation and a potential vulnerability.

Secondly, choosing components from a known validated supplier list as mentioned above.

The list of components used in the manufacture of products, otherwise known as a Bill of Materials (BOM), must be controlled through the use of system controls and processes, and any changes or substitutions authorized only by the design engineers.

Product Development

Adding in capabilities to assist application and system development to enhance the security of the solution encompasses a variety of areas and can involve both hardware and software components.

The first and most fundamental question with respect to software security is, *are we running the correct software or firmware?* This is where features such as Secure Boot or verified boot using Trusted Platform Modules (TPM) come in. There are two modes: measured boot and verified boot.

Measured boot uses digital signatures and verified boot uses TPM with RSA encryption keys for hardware authentication of software attempting to

run on the module. This methodology can also be used to secure the upgrade process for firmware or software.

Many system solutions now involve hosting a virtual machine manager of some form, such a KVM or VMware. Ensuring the security of applications running on these virtual machines (VMs) is vital. Features such as memory protection extensions in Intel processors allow VMs to create protected memory regions.

Quick Assist Technology (QAT) provides the ability for cryptographic and compression functions to use a hardware accelerator to assist application programs.

This functionality is an option on Intel processors that aids in cipher operations, hash authentication, public key functions and digital signature generation and authentication. SMART EC ATCA products now include options to include this feature.

Design Verification and Validation including Functional and Regulatory Compliance

Testing the product to ensure that it meets the requirements is key not only to determine that the product is operationally correct, but also to determine that nothing has been added to the design that was not intended. Design verification performs detailed low-level testing of a board's functionality, testing every circuit to ensure it is doing what is expected and nothing untoward is going on.

Regulatory testing such as EMI/EMC testing confirms that the product emissions are within limits, but also can check that nothing unexpected is being emitted.

In terms of software, running vulnerability test software and validating conformity to security technical implementation guidelines provides necessary confirmation that no vulnerabilities are left exposed.

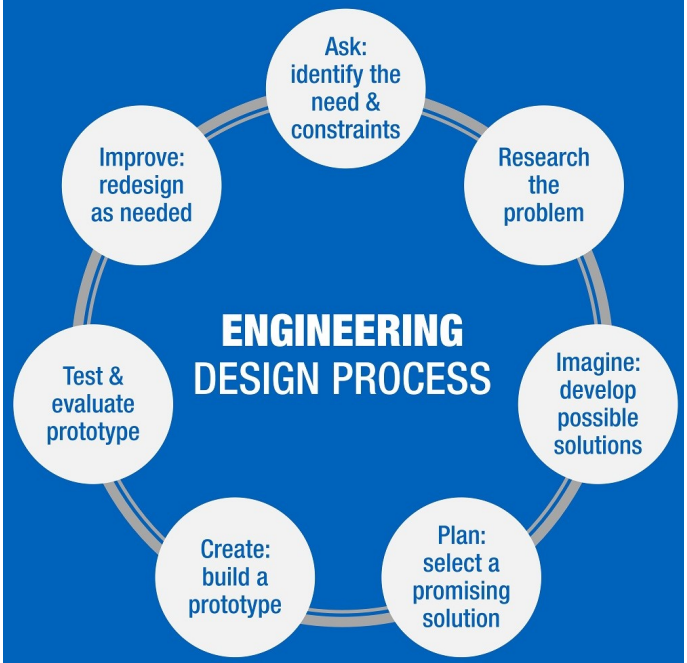
Manufacturing and Repair

Sourcing

All the design and functional testing is moot if you cannot guarantee that only the parts you have selected and specified make it onto the manufactured board. Ensuring that component sourcing only buys from the approved supplier list, not buying from "grey" market and brokers, is essential. Inspection of incoming components and materials during the receiving process

Secure COTS Engineering Design Process

- Marketing Requirement Document (MRD)
- Product Requirement Documents (PRDs)
- Planning: schedule, budget, resources
- Specifications
- Simulation: thermal, signal Integrity (SI)
- Implementation: coding, schematics, PCB layout, mechanical drawings
- Prototype builds
- Test and verification
- Functional, environmental testing, EMC testing, shock & vibration testing
- Product documentation and training
- Product release



is also necessary - only then do these components go into inventory.

Assembly

Only components and materials that are in controlled inventory are used in the manufacturing process. Having traceability from component lot numbers to board serial numbers provides a record and also enables tracking down boards if a component lot issue is identified at a later date.

Automated optical inspection and visual inspection need to be performed on 100% of all products and at the different stages of manufacturing assembly, product acceptance testing and packaging.

As part of the manufacturing process, software or firmware is often pre-programmed. By only using binary images created and validated by the design engineering team and stored on secure servers can you ensure that no modifications are being made to the intended functions. This is further secured by manufacturing tests confirming correct checksums for these images.

Test

Every product coming off the line needs to be put through rigorous manufacturing validation through the use of in-circuit testing and functional testing. Some products, mainly extended temperature rated units, may even have burn in test performed to ensure that they meet quality standards.

Repair

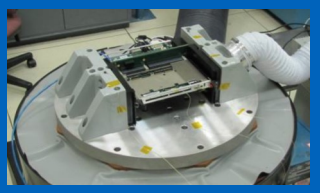
Making sure that product or warranty repair services are performed at company-owned locations or by trusted third-parties, which only use components originally specified and qualified from controlled inventory, along with re-testing using the original factory tests ensures that nothing post-manufacture can be added to the product and that the product meets the functional requirements. SMART EC's secure COTS products sold in the USA are repaired at company-owned locations.

SMART EC's Test Capabilities

Hardware Validation and Compliance

- Design reviews (EMC, safety, standards compliance)
- Environmental lab (on-site thermal, vibration, and humidity)
- Safety (on-site safety lab via CSA)
- EMC (on-site and A2LA accredited)

Integration, Interoperability and Verification



- Functional & conformance
- Interoperability verification
- Performance benchmarking
- Negative/exception verification
- Stress and stability verification
- Backward compatibility verification

Complex System Integration Services

- Blades (internal and 3rd party)

Manufacturing Location

Having flexibility in the geographic location of manufacturing facilities allows a supplier to balance best-cost, geopolitical concerns, product integrity, innovation, security of supply and other factors. Being able to manufacture in the USA, as SMART EC has the capability to do, can enhance a customer's confidence in the stewardship of its supply chain.

SMART EC's embedded computing business traces its heritage to Motorola Computer Group, Force Computers and Heurikon. We have a long legacy of manufacturing and integration in the USA. We were one of the inventors of VME and ATCA technology and continue to be a leading supplier of both technologies.

Our history of supplying COTS embedded computing platforms to military, aerospace and defense programs goes back many years. Some VME products have been available for almost 20 years, a principle that now extends to ATCA technology, which is planned to be in production through at least 2030.

Auditing

Many of the processes outlined in this whitepaper are great in theory, but unless they are correctly instituted and followed, the customer can't count on the benefits. It is crucial to have frequent process audits to ensure that the processes are being followed. To ensure timely verification, audits need to be performed at least annually.

SMART EC's design engineering and manufacturing processes and facilities are regularly audited, not only by internal teams, but also by customers from a range of markets, including military, rail, aerospace, telecom and industrial.

Conclusion

The security of COTS embedded computing products used in aerospace and military programs has become a focal point for military branches and prime contractors. There are two aspects:

1. The security of the products themselves, which SMART EC addresses in other published materials
2. The issue of supply chain security, addressed by this white paper

SMART EC has been a technology partner for network-centric compute infrastructure in aerospace and military programs for over 35 years. Our team has a dual focus:

1. Ensuring today's technology and our roadmap provides the functionality and performance customers need for their applications
2. Maintaining a world-class design and operations capability to ensure quality and security are built-in to our products, processes and culture.

For more information on secure COTS and supply-chain security, please contact us.

About SMART Embedded Computing

SMART Embedded Computing (SMART EC) is part of the SMART Global Holdings, Inc family of companies.

We are a global leader in the design and manufacture of highly reliable embedded computing solutions for a broad range of defense, industrial IoT (IIoT), edge computing, and communications customers.

Building on the acquired heritage of industry leaders such as Motorola Computer Group and Force Computers, SMART EC is a recognized leading provider of advanced computing solutions including application-ready platforms, single board computers, enclosures, blades, enabling software and professional services.

For more than 40 years, customers have trusted us to help them accelerate time-to-market, reduce risk and shift development efforts to the deployment of new, value-add features and services that build market share.

Our engineering and technical expertise is backed by world-class manufacturing, global sales offices and advanced worldwide logistics capabilities that can significantly reduce time-to-market and help customers gain a clear competitive edge.

Contact

+1 602-438-5720

info@smartembedded.com

www.smartembedded.com