Next-Generation MachXO3D FPGAs Make Automotive Space Secure

Instant-On Single-Chip MachXO3D FPGAs Bring Enterprise-Level Security to the Automotive Domain

A Lattice Semiconductor White Paper.

September 2020

Learn more:

www.latticesemi.com

Contact us online:

www.latticesemi.com/contact
www.latticesemi.com/buy

TABLE OF CONTENTS

We live in a highly connected world that is subject to cyberattack from a myriad of sources. In 2018 alone, attacks on hardware rendered over 3 billion systems of all types open to data theft, improper operation, and other security threats[1].

In the case of automobiles, security problems are exacerbated by today's smart and connected cars. A cyber attack causing loss of control could potentially harm the passengers in the targeted automobile, nearby vehicles, pedestrians, and property in the vicinity.

Not surprisingly, automotive designers and manufacturers are desperately looking for ways to secure their systems. As discussed in this paper, one solution is to employ MachXO3D™ FPGAs from Lattice Semiconductor.

Not Your Grandmother's Automobiles

Always in flux, the automotive market has changed dramatically over recent years, and these changes are increasing at an exponential rate.

Computers in the form of microprocessor units (MPUs) and microcontroller units (MCUs) started to find their way into cars in the late 1970s and early 1980s. Initially, these acted as sophisticated engine control systems and only appeared in high-end vehicles. By the mid-1990s, all cars had processors monitoring their sensors, controlling their engines, and managing interactions between various in-car systems.

A typical car, circa 2020, contains around 50 computers, while high-end vehicles can contain 100 or more or more. Today's automobiles are equipped with things like GPS, Bluetooth, Wi-Fi, and cellular communications, along with advanced safety systems including lane departure warning and collision warnings. Many automotive applications employ sensor fusion between radar, lidar, and machine vision systems powered by artificial intelligence (AI) and machine learning (ML). Some vehicles have the ability to parallel park themselves at the touch of a button, with more capabilities of this type on the way.

There's also a surging interest in electric vehicles (EVs), and the world's major automobile manufacturers are now investing heavily in such vehicles. Furthermore, there is an increasing interest in hydrogen-powered cars, with at least three models publicly available and multiple companies working to develop new vehicles.

Feeling Insecure?

In addition to boasting 50 to 100+ computers, today's automobiles are becoming increasingly connected to the outside world. In this context, the term "connected" refers to a vehicle that can communicate bidirectionally with other systems outside of itself. This allows the car to share internet access and data with other devices both inside and outside the vehicle.

The first automaker to bring connected features to the market was General Motors with OnStar in 1996. Remote diagnostic capabilities were introduced in 2001. By 2003, connected car services included vehicle health reports, turn-by-turn directions, and network access devices. Data-only telematics were first offered in 2007, and by 2017 fleet operators saw the first deployments of predictive intelligence capabilities.

In the context of a software environment, the term "attack surface" refers to the sum of the different points where an unauthorized user can try to enter data or extract data from an environment, or take control of that environment. The problem is that having connected cars boasting 50 to 100+ computers provides a large attack surface to hackers and other "bad actors."

A large part of the security solution is to establish a root of trust (RoT). According to the National Institute of Standards and Technology (NIST):

> *Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are currently rooted in software that, along with all underlying components, must be trustworthy. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon those components. Stronger security assurances may be possible by grounding security mechanisms in roots of trust. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.*

Unsecured systems can lead to data and design theft, product cloning, and overbuilding. Even worse, systems lacking sufficiently robust security leave themselves open to device tampering or hijacking.

There are only a handful of FPGA vendors, most of whom are focused on providing ultra-high levels of capacity, capability, and performance. These are the devices that are used in large telecommunications infrastructure, server farms, data centers, and such. By comparison, Lattice Semiconductor is the only FPGA vendor focused on the low to mid-range FPGA space, which is the "sweet spot" for many automotive applications. Furthermore, Lattice offers the only low-power FPGA at <10k look-up tables (LUTs) that is equipped with a NIST-certified Immutable Security Engine.

Introducing the MachXO3 FPGA Family

Lattice offers a variety of FPGA technologies. One example of FPGAs that are ideal for deployment in automotive applications is the MachXO suite of devices.

The original MachXO family was presented to the market in 2005. The MachXO2/ZE™ families were introduced in 2010, followed by the MachXO3L/LF™ families in 2013 and the MachXO3D™ family in 2019. Throughout this evolution, each new generation maintained all of the customer-driven features provided by previous generations while adding increased capacity and functionality.

Like all previous generations of MachXO FPGAs, MachXO3™ devices offer a highly desirable combination of low power, substantial LUT resources, and large numbers of input/outputs (I/Os). These are coupled with instant-on and hot-socketing capabilities, along with background programmable internal flash configuration memory and the ability for in-field logic updates. This makes MachXO3 devices ideal for glue logic, bus bridging, bus interfacing, motor control, power-up control, and myriad other control logic applications. Furthermore, with their hundreds of I/Os, MachXO3 FPGAs are perfect for a wide range of applications that require general purpose I/O expansion, interface bridging, and power-up management functionality.

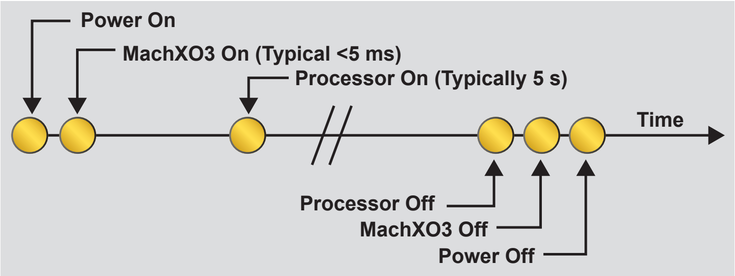

Figure 1: Dominating the platform control arena, MachXO3 FPGAs are the system's first-on, last-off devices.

Offering up to 9400 LUTs and 384 I/Os, the MachXO3LF family provides a range of capacities to suit each design scenario. Available with 3.3/2.5 V core or low power 1.2 V core, this family offers multiple I/O banks (up to six) that support hot socketing along with a wide range of signaling standards, and voltages, all coupled with per-pin programmability. An extended (junction) temperature range of -40°C to +125°C addresses the needs of harsh automotive environments, while AEC-Q100 Grade 2 certification[2] meets established industry standards for automotive quality.

In addition to their flash-based configuration memory, the MachXO3LF family also provides up to 448 kilobits of user flash memory (UFM). Furthermore, on power up, the configuration data is copied from the flash configuration memory into SRAM-based configuration cells (not to be confused with any blocks of user SRAM memory). This operation is performed in a massively parallel fashion taking less than 5 ms to perform. A huge advantage of this approach is that the device can continue to function using its SRAM-based configuration while a new configuration is loaded into the flash configuration memory. Once the new configuration has been loaded, the device can be paused under program control, the outputs locked, the new configuration copied into the SRAM configuration cells, and the device released to continue operation.

As the structures on integrated circuits get smaller and smaller with each new process node, one issue that affects all of today's electronic devices is that of radiation. A very common radiation-induced effect is that of a single-event upset (SEU) in which an energetic radioactive particle strikes a sensitive node in the circuit causing it to change state; for example, a register bit or a memory cell flipping from a 0 to a 1, or vice versa. Since SEUs can be corrected, these are classified as being "soft errors." The SEU problem is more acute in the case of FPGAs, which also have their configuration cells to contend with.

Not surprisingly, automotive applications are considered to be safety critical. In order to address radiation effects -- and also to address electrically noisy environments, such as those found in automobiles -- the MachXO3LF family supports soft error detection (SED), soft error correction (SEC) and soft error injection (SEI).

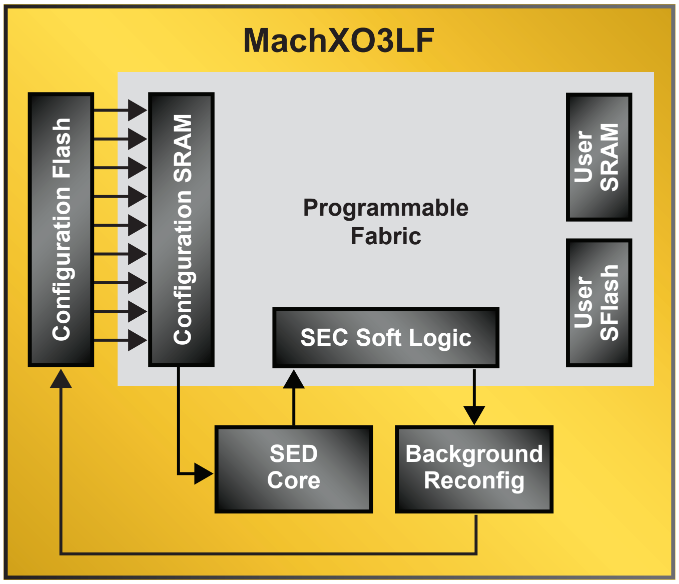

Figure 2: Simplified block diagram of the MachXO3LF illustrating the soft error detection and correction process.

Created as a hard core on the silicon die, the SED module calculates the cyclic redundancy check (CRC) of the SRAM configuration bits, compares this calculated CRC with the existing CRC associated with the current configuration, and flags an error if a mismatch occurs. Responding to this flag, the SEC soft core implemented in the programable fabric triggers the background reconfiguration core to update the SRAM configuration cells from the primary configuration stored in the configuration flash (this reconfiguration does not interrupt any unaffected sections).

Last, but not least, the SEI capability allows the user to emulate soft error events by injecting faults via JTAG, I^{2}C, or SPI directly into targeted SRAM configuration cells without modifying the CRC.

Introducing the MachXO3D FPGA Family

The automotive industry is basing its approach to security on that taken by the server industry, including such things as supply chain security, secure boot (ensuring that code launched by firmware is trusted), and platform firmware resiliency.

As discussed earlier, MachXO3LF automotive FPGAs offer the best-in-class programmable logic devices for the flexible deployment of robust automotive applications. In addition to vastly increased flash that offers up to 2,693 kilobits of UFM, MachXO3D automotive devices add hardware security features that bring NIST-level security to automotive systems. In fact, the MachXO3D is the only FPGA at <10K LUTs that is equipped with a NIST-certified Immutable Security Engine.

In addition to enabling hardware root of trust in the form of the system's first-on, last-off device, the MachXO3D's Immutable Security Engine also enables pre-verified cryptographic functions such as ECDSA, ECIES, AES, SHA, HMAC, TRNG, Unique Secure ID, and public/private key generation. The Immutable Security Engine -- along with Lattice's recently introduced firmware security solutions stack, Lattice Sentry™ -- supports security throughout the product lifecycle, including device manufacturing and transport, platform manufacturing, installation, operation, and even decommissioning. It also enables comprehensive protection against a variety of threats by providing data security, equipment security, data authentication, design security, and brand protection.

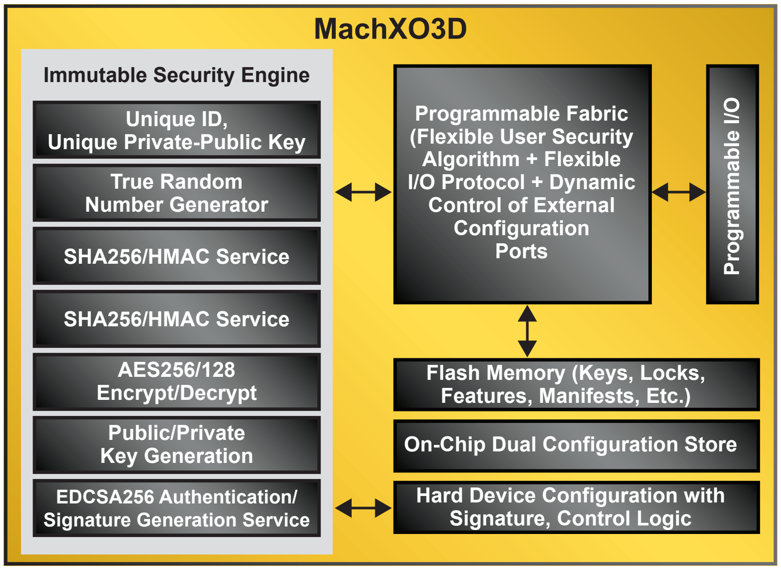
MachXO3D
Immutable Security Engine
Unique ID, Unique Private-Public Key
True Random Number Generator
SHA256/HMAC Service
SHA256/HMAC Service
AES256/128 Encrypt/Decrypt
Public/Private Key Generation
EDCSA256 Authentication/ Signature Generation Service
Programmable Fabric (Flexible User Security Algorithm + Flexible I/O Protocol + Dynamic Control of External Configuration Ports
Programmable I/O
Flash Memory (Keys, Locks, Features, Manifests, Etc.)
On-Chip Dual Configuration Store
Hard Device Configuration with Signature, Control Logic

Figure 3: The MachXO3D secure control FPGA is the system's first-on, last-off, root-of-trust programmable logic device.

As defined by NIST SP 800 193, platform firmware resiliency (PFR) involves protection, detection, and recovery. Protection includes protecting the platform's firmware and critical data from corruption and ensuring the authenticity and integrity of any firmware updates. Detection includes cryptographically detecting corrupted platform firmware and critical data, both when the system is first powered on and following any in-system updates. Recovery includes initiating a trusted recovery process and restoring and corrupted platform firmware and critical data to its previous value.

MachXO3D devices fully address PFR requirements by providing features such as a secure dual-boot capability. The combination of the MachXO3D's programmable logic, Immutable Security Engine, and secure dual-boot configuration block provides flexibility during design implementation and enables secure updates after the system has been deployed. In addition to providing hardware root of trust by design, the use of on-chip logic dramatically minimizes the cyberattack surface area.

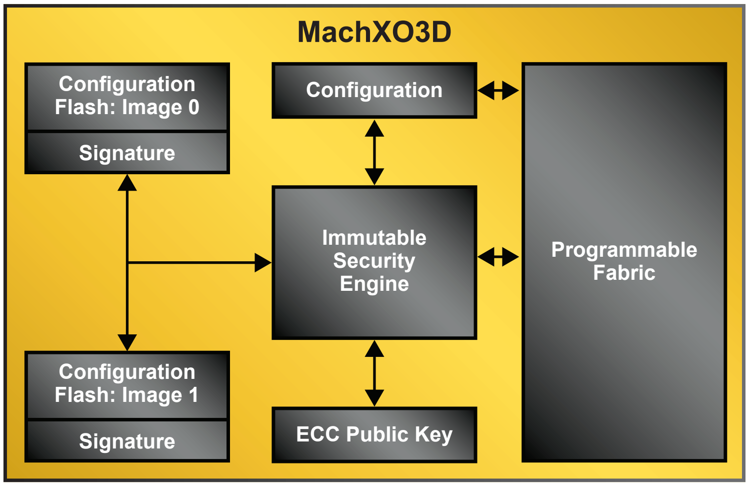
MachXO3D
Configuration Flash: Image 0
Signature
Configuration
Immutable Security Engine
Programmable Fabric
Configuration Flash: Image 1
Signature
ECC Public Key

Figure 4: The MachXO3D's dual-boot capability fully addresses the requirements of NIST SP 800 193 for platform firmware resiliency.

As part of supporting NIST PFR requirements, the MachXO3D enables secure on-the-fly system updates by employing self-detection, self-recovery, and self-protection. In the case of self-detection, the existing on-chip configuration image is authenticated by the security engine prior to boot using a public key that is securely stored on-chip. With regard to self-protection, if the authentication of a newly downloaded image fails, the security engine automatically reverts to the existing authenticated "golden image". In the case of self-protection, in addition to preventing the device from configuring itself using a compromised image, the programmable fabric logic controls access from the programming ports, a lock policy ensures separate access rights for each flash store, and the security engine blocks attack from all configuration ports while a new image is "in-transit" (in the process of being loaded into the configuration flash).

Typical Use Cases

The following provides brief overviews of three typical automotive use cases for MachXO3 and MachXO3D FPGAs: battery management, root of trust, and hardware-based secure boot.

- **Battery Management:** Many of today's systems, including electric vehicles, have multi-cell batteries. It is required that each cell in the battery array is charged to the right amount to extend the life of the battery. Any overcharging or undercharging of these cells will reduce the battery life.

  A battery management system performs a variety of tasks, including protecting the battery from operating outside its safe operating area, monitoring its state, calculating secondary data, and reporting that data.

A MachXO3-based battery management system (BMS) is a controller that oversees the charge and discharge processes and provides intelligent cell balancing for charge equalization for each battery cell. Additionally, the BMS provides real-time battery information like the state of charge (SOC) and state of health (SOH) of the battery to help the vehicle's application processor (AP) provide up-to-date information to the driver.

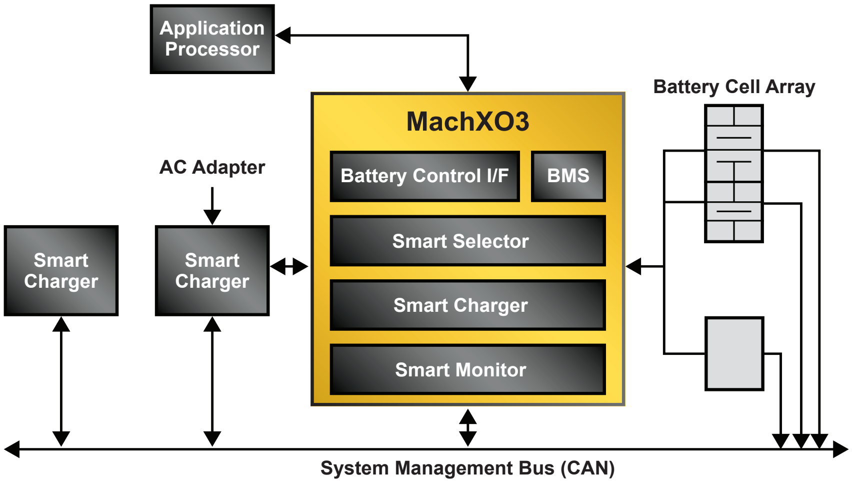

Figure 5: MachXO3-based battery management system.

Using a MachXO3D FPGA to implement the BMS adds an additional layer of security to the system, thereby preventing the hacking of intelligent batteries to push them beyond their safe limits, which could potentially cause permanent damage or catastrophic failure to the batteries and the vehicle.

- **Chain/Root of Trust:** Hardware root-of-trust (RoT) is the first link in chain of trust that protects the entire automotive system, including any engine control units (ECUs).

  Commencing with the component supplier, the automotive system supply chain also includes Tier 2 system developers, Tier 1 system integrators, OEM car manufacturers, distribution and shipping, dealerships, and the end customers. Throughout this supply chain, there are number of attack points where the system can be hacked with the possibility of compromised firmware being uploaded.

  The Lattice SupplyGuard™ supply chain security service provides customers with factory-locked ICs. These can only be programmed using a configuration bitstream that has been developed, signed, and encrypted by the intended customer.

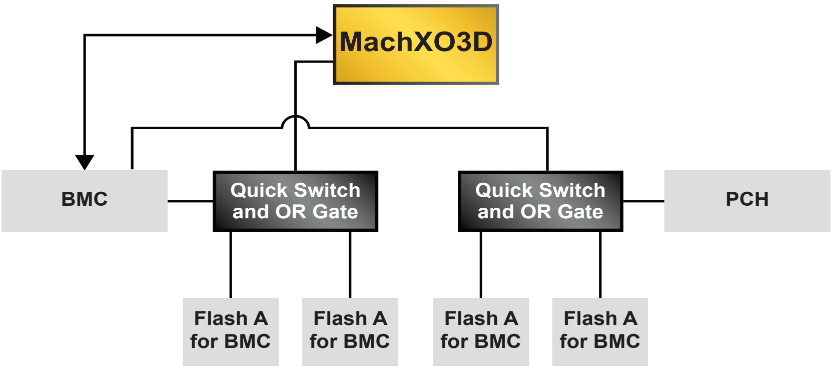

Figure 6: MachXO3D-based chain/root of trust.

Additionally, the MachXO3D FPGA's dual-boot capability supports key-based encryption and a highly secure golden image to which the system can always default. The combination of the instant-on MachXO3D, the golden image, and Lattice SupplyGuard provides end-to-end supply chain protection.

- **Hardware-Based Secure Boot:** The MachXO3D FPGA is the first device to turn on and the last device to turn off in an automotive system. Upon system powerup, the MachXO3D self-checks to make sure only authenticated firmware is running on it. The MachXO3D also checks the firmware associated with other devices in the system.

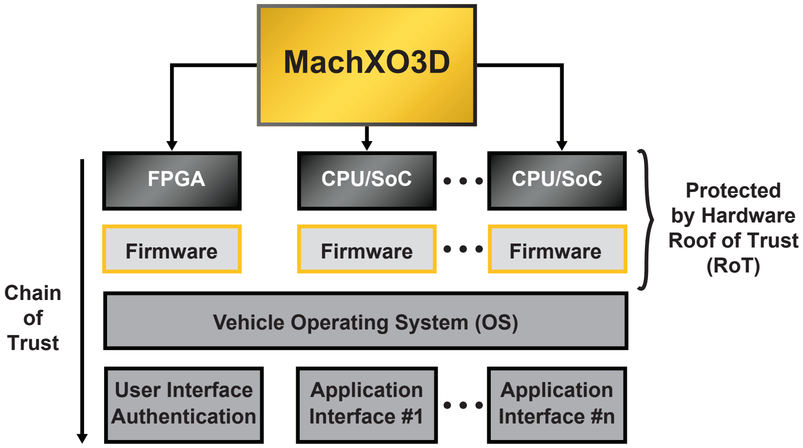

Figure 7: MachXO3D-based secure boot.

Compliant with NIST SP 800 193 Platform Firmware Resiliency (PFR) guidelines, the MachXO3D FPGA's hardened secure configuration block enables the device to protect, detect, and recover itself from malicious attacks. Furthermore, the massively parallel processing capability of its programmable fabric gives the MachXO3D the ability to protect, detect, and recover multiple platform firmware elements at the same time.

Conclusion

The flash-based configuration of MachXO3 FPGAs provides "instant-on" capabilities that allow them to be the platform's first-on, last-off devices and dominate the market for system control and power management functionality.

Automotive applications are considered to be safety critical. In order to address radiation effects -- and also to address electrically noisy environments, such as those found in automobiles -- the MachXO3LF family supports soft error detection (SED), soft error correction (SEC) and soft error injection (SEI).

In addition to vastly increased flash that offers up to 2,693 kilobits of UFM, MachXO3D automotive devices add hardware security features that bring NIST-level security to automotive systems.

MachXO3D FPGAs enhance security with hardware root of trust capabilities. Using MachXO3D FPGAs, OEMs and automakers can simplify the implementation of robust, comprehensive, and flexible hardware-based security for all system components. MachXO3D FPGAs can protect, detect, and recover themselves and other components from unauthorized firmware access at system run time. Furthermore, in conjunction with Lattice SupplyGuard, MachXO3D FPGAs can protect a system from malicious activity at every stage of that system's lifecycle, from the point of manufacturing all the way to its end-of-life (EOL).

In addition to security, an FPGA's ability to perform operations in a massively parallel fashion makes these devices of interest for a wide variety of advanced driver-assistance systems (ADAS), which are electronic systems that assist drivers in driving and parking functions. Many ADAS systems demand real-time response, but MCUs are too slow, while custom System-on-Chip (SoC) devices are too expensive and time-consuming to develop. Also, algorithms implemented as hardware accelerators in an SoC are effectively "frozen in silicon," which is unfortunate at a time when many standards and protocols are evolving and in flux. The solution is FPGAs, which are as flexible as you can get, and which can be reconfigured to address evolving standards, protocols, and functional requirements.

MachXO3D FPGAs offer the perfect combination of functionality and security for today's evermore complex and connected automotive applications.

References

[1] https://www.technologyreview.com/2018/01/05/146411/at-least-3-billion-computer-chips-have-the-spectre-security-hole/

[2] Full certification is anticipated by Q1 2021

Learn more:

www.latticesemi.com

Contact us online:

www.latticesemi.com/contact
www.latticesemi.com/buy