WHITE PAPER

AMI Tektagon™ Firmware and Lattice Semiconductor FPGA → Serious Firmware Protection

Firmware presents "a large and ever-expanding attack surface."

ABSTRACT In many modern computer security approaches, securing the firmware layer is often overlooked. However, firmware could be a single point of failure in digital devices and one of the stealthiest ways for an attacker to gain control of a system. An attacker with access to a device's firmware can potentially bypass authentication and encryption mechanisms, modify the core functionality of a device, and plant persistent malware."

Because of this lack of attention, firmware attacks are much more dangerous than OS-based attacks since firmware is invisible to OS-based security solutions.

A Zero Trust strategy begins at power up with trusted platform firmware. Not paying attention to platform firmware, could put an enterprise's entire system at risk. Becoming educated about the risks of unsecured firmware and taking steps to protect the system against exploitation is critical to maintaining a secure environment.

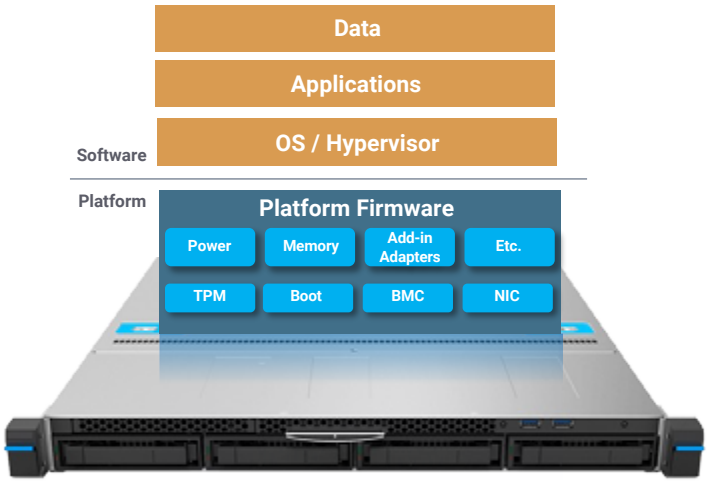
The bottom line --- do not take firmware resiliency for granted.

THE PROBLEM

When it comes to cyberattacks, most security experts do not consider firmware as a critical vulnerability. However, firmware-based cyberattacks are on the rise because they provide an additional system entry point for hackers.

According to a report commissioned by Microsoft, 83% of businesses have experienced a firmware attack in the last few years [1]. Additionally, the Cost of Data Breach Report 2021 commissioned by IBM says that 2021 had the highest average data breach cost in 17 years [2]. With cyberattacks on the rise, it is important to be aware of all potential vulnerabilities - including firmware. Understanding how firmware-based attacks work and taking steps to protect system firmware, can help keep a business safe from these costly and damaging attacks.

Root of Trust must be Trustworthy



Are you aware of ALL the firmware running on your platform?

It's essential for every platform to be trusted at boot time.

Platform trust requires validated firmware.

Firmware Security

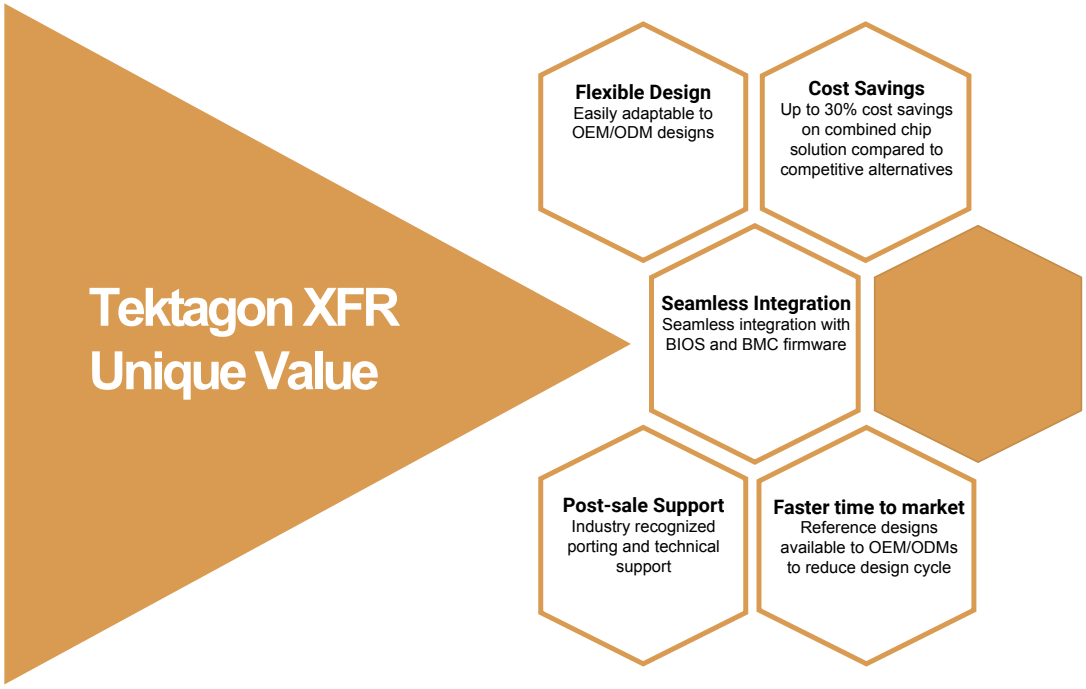
Firmware security must be taken seriously and is critical for complete data center security. With the increase of firmware in the data centers comes an increase in attack surfaces, which drives interest in firmware security to new highs.

Firmware security is the most important security layer. If the platform firmware is compromised in any way, hackers can gain full control and the entire system cannot be trusted. With security breaches becoming more prevalent at the firmware level, organizations must have a system to validate their platform firmware

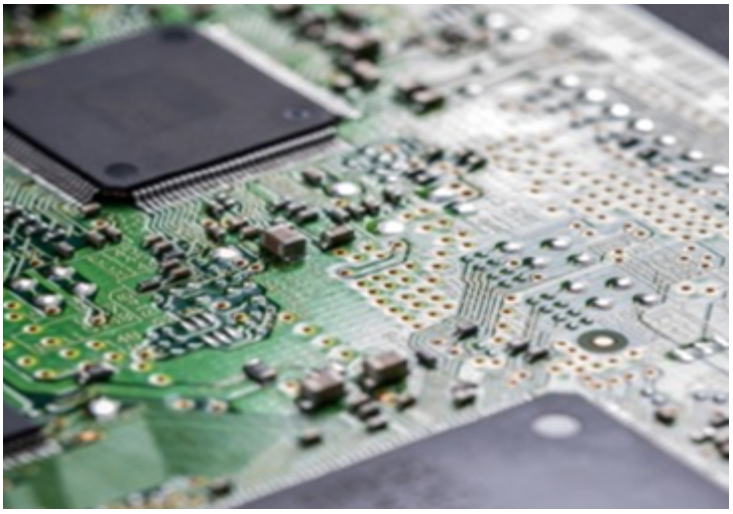
For any platform, the root of trust must be trustworthy. Users must be aware of all firmware running on their platform. To have this trust, it is essential for every platform to be trusted at boot time by validating firmware using a Platform Root of Trust (PRoT).

THE SOLUTION

AMI Tektagon™ XFR and Lattice



AMI Tektagon and Lattice



The Need for Tektagon XFR

- Firmware attacks are becoming more common
- Attackers want a persistent foothold on platform
- If platform firmware is compromised, the entire firmware is compromised
- Compromised firmware may be impossible to detect without specialized hardware
- NIST compliance may be required for some contracts

Tektagon XFR from AMI is hardware-based Platform Root of Trust (PRoT) security solution that detects and protects firmware compromises on computing ecosystems worldwide.

When necessary, Tektagon XFR can recover a golden image of the platform firmware to restore integrity of the platform and can help prevent unauthorized access into the organization's infrastructure and contribute to protect business data.

AMI's Tektagon Platform Root of Trust portfolio of products can secure firmware to meet the platform security challenges.

Tektagon products are designed to secure platform firmware by providing three things:

- Detect when platform firmware code is compromised or corrupted
- Recover and restore firmware and authenticate the recovery image
- Monitor and block unauthorized transactions

While being silicon agnostic, partnering with Lattice Semiconductor provides flexibility to AMI customers. The Lattice MachXO3D field-programmable gate array (FPGA) is available today with a minor PCB revision (See Appendix) [3]. Keeping the Platform Root of Trust firmware independent from the FPGA ensures the firmware is not locked to a specific silicon vendor. However, implementing the AMI+Lattice solution:

- Provides high integration with AMI's Aptio UEFI firmware and MegaRAC Baseboard Management Controller (BMC) firmware
- Provides superior Serial Peripheral Interface (SPI) filtering
- Enables fast firmware updates through flexible memory organization
- Requires no FPGA development knowledge since Tektagon XFR firmware development is separate from the power sequencing development

Providing cyber protection from the moment that power is applied to a system mandates a need for a hardware-based Root of Trust upon which to build a cyber security strategy. Lattice Semiconductor has provided this HRoT in their MachXO3D product which contains an immutable hardware-based security block providing enhanced levels of protection. The HRoT is the beginning of the establishment of Chain of Trust (CoT) as the system continues to build upon lower levels of trust to fully bring up the system in a protected manner.

The best way to describe the Lattice Platform Firmware Resilience (PFR) architecture is one of zero trust. For that reason, the RoT must be an HRoT. For quite a while, FPGAs from all vendors have had write protect and encryption but these have been primarily focused on copy protection and secondarily on memory corruption. That level of protection has been pressed into service for both FPGA and microprocessor PFR solutions including the MAX10. As cyber-attacks have gotten more sophisticated, there is concern those FPGA protections are now insufficient. The problem is "What if somebody properly does something improper?"

To address this issue, Lattice created the XO3D with the Embedded Security Block (ESB) to provide a hardware based, immutable security mechanism that is active from the moment of power on of the device. The Lattice XO3D does not even trust itself at that point and that is what zero trust means. Before the FPGA is even allowed to configure its logic, the encrypted, signed configuration images must pass security checks. Unique keys in every device mean that the images and signatures for no two devices need be the same. It eliminates design cloning and provides mechanisms to track the device and its image through the whole manufacturing and deployment process. Well beyond simple copy protection, a Chain of Trust must be built within the FPGA before it is even allowed to begin operation.

Subsequent levels of the CoT are developed as implemented per PFR. BMC and Platform Controller Hub (PCH) BIOS images are checked by the firmware running in the FPGA. Successful security checks there allow the BMC and PCH to begin operation and then the CoT can extend to even higher levels. This high-level process is the same whether one is looking at a MAX10 or Lattice solution.

Both the MAX10 and Lattice XO3D solution include processor blocks to implement the PFR operations related to the BMC and PCH BIOS images. The MAX10 uses the NIOS2 soft core processor on an Avalon bus structure and the Lattice device uses a RISC-V processor on an AMBA AHBL/APB bus structure. The MAX10 peripherals are then going to be Avalon based and the Lattice peripherals AHBL or APS based. Conceptually, they should be very similar.

See Appendix for Key Differences

SOLUTION ARCHITECTURE

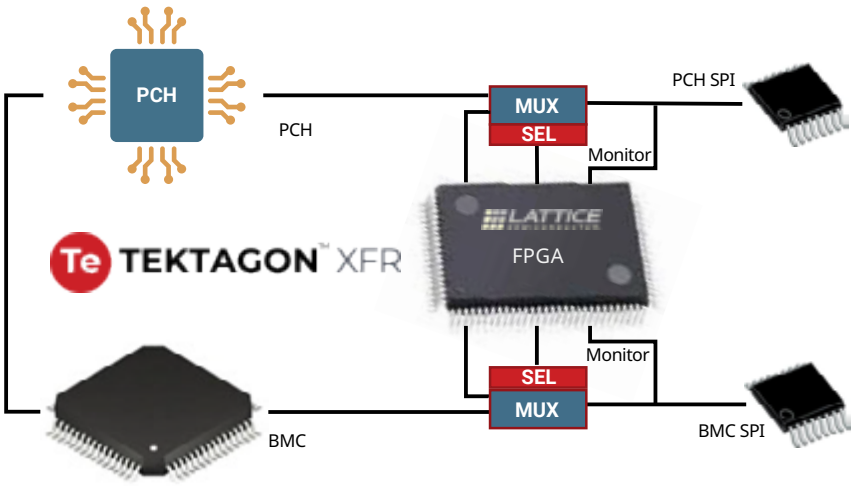
Tektagon XFR Key Features

- Utilizes Lattice FPGA to provide an independent HRoT with maximum flexibility
- Fully-featured solution
- Secure firmware update of recovery image
- Configurable modular code
- Capable of DC-SCM module implementation
- Flexible runtime flash protection
- PRoT for BIOS/BMC and other system firmware
- SMBus monitoring for peripheral firmware protection
- NIST SP 800-193 Compliant PFR
- Compatible with Intel®, AMD®, ASPEED®, Arm®, RISC-V® and other silicon vendors
- Great fit for general server and CP Market

For the ultimate in security, choose the Tektagon XFR platform from AMI. This design option offers a robust chain of trust, including real-time I2C bus monitoring and SPI monitoring of both BIOS and BMC SPIs. That means there are no gaps in security - users can be sure that all transactions on the SPI bus are monitored and protected. Plus, it is a great fit for the general server and cloud services provider (CSP) market. Tektagon XFR provides the peace of mind that comes from knowing the system is secure from end to end.

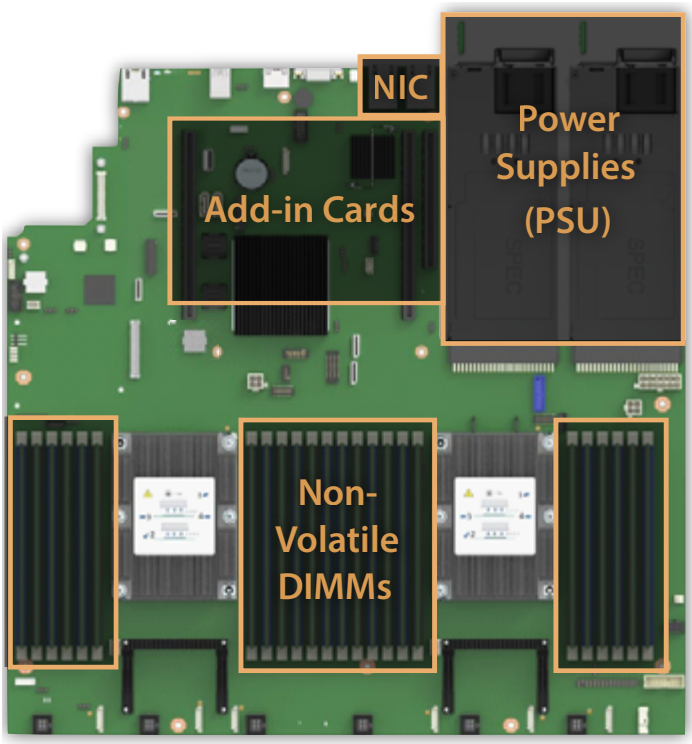
Minimizes Gaps in Security

- Tightly knit, secure Root of Trust (RoT) solution
- Offers robust chain of trust, including real-time I2C bus monitoring and SPI monitoring of both BIOS and BMC SPIs
- Monitors all transactions on the SPI bus during runtime to ensure no malicious read/write commands are executed

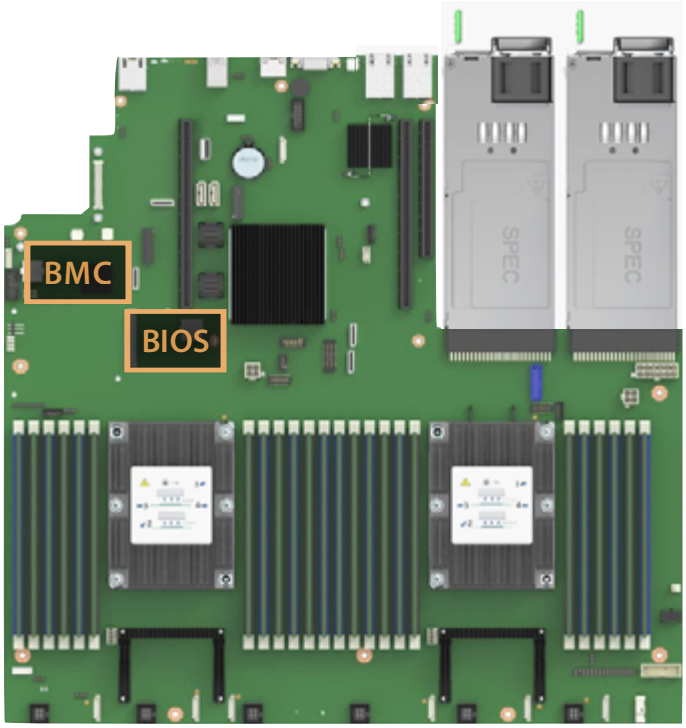


Tektagon Secures the Entire Platform Firmware

What Does Tektagon XFR Secure?



What Does Tektagon XFR Secure?



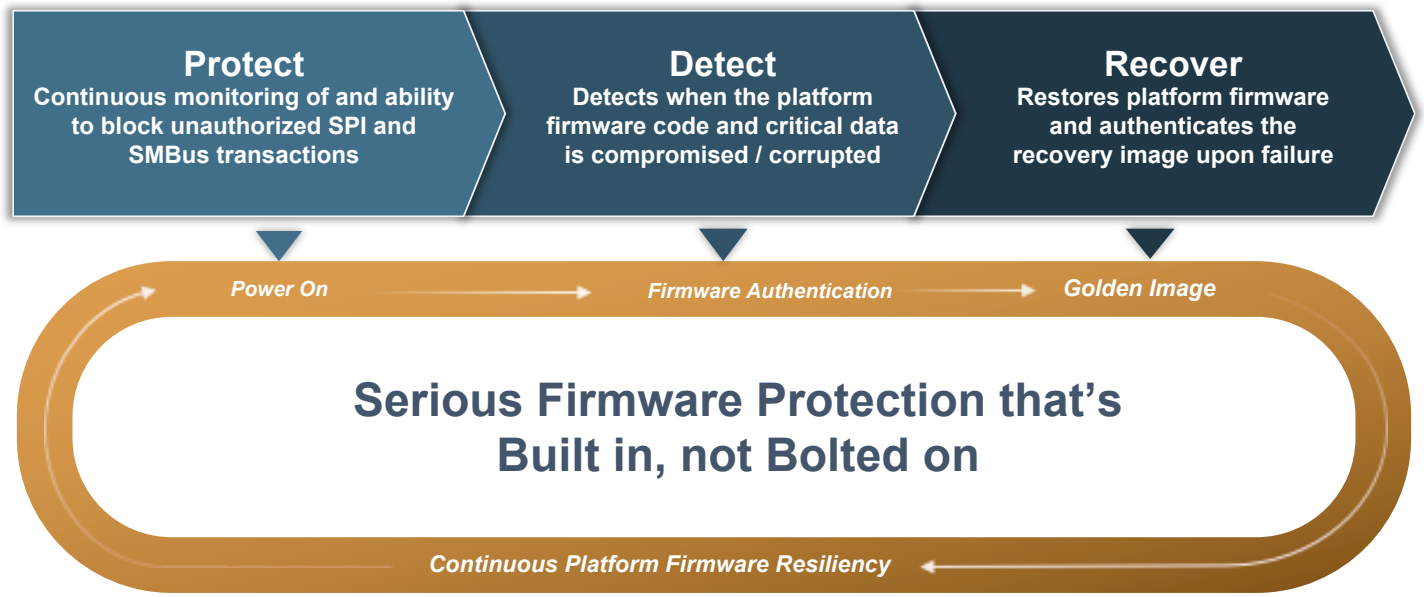
Utilizing the AMI's HoT engine, Tektagon XFR validates BMC and BIOS firmware.

Tektagon XFR can also monitor andsecure other firmware accessible by the BMC, including:

- Add-in Cards
- Power Supplies
- NIC
- Non-volatile DIMMs

NIST SP-800-193 Compliant

Tektagon XFR: NIST SP 800-193 Compliant



CONCLUSION

As the saying goes, "The best offense is a good defense." The same can be said for cybersecurity. In today's digital world, there are more devices and more data than ever before. And with those increases comes more vulnerabilities. Cybercriminals are becoming more sophisticated and realize that firmware is the soft underbelly of cybersecurity. It is analogous to the door in the basement of a large building or air handling ducts that no one thinks about securing. Beyond cybersecurity, Platform Firmware Resilience allows companies to quickly respond to attacks as they happen.

Firmware vulnerabilities can act as a gateway for cybercriminals to access sensitive information and wreak havoc on an organization. While firmware can be a risk, it can also be an enabler of security. By thinking more thoroughly about firmware security and creating a resiliency plan, organizations can protect themselves from potential attacks.

A Zero Trust strategy really does begin with firmware – and AMI Tektagon XFR and Lattice can provide the ultimate security solution.

APPENDIX KEY DIFFERENCES:

On SPI interfaces, the MAX10 puts its SPI Master on separate pins than the SPI Monitor (see Figure1). The Lattice XO3D routes its SPI Master pins through the SPI Monitor so pins are shared. The result is a savings of 4-7 pins on the Lattice implementation and elimination of external multiplexing of the FPGA SPI Master.

Both MAX10 and Lattice XO3D seek to filter unwanted FLASH operations by modifying the SPI transaction to make it illegal. When SPI Monitor filtering occurs, the MAX10 completely impacts this function by truncating the chip select to the SPI FLASH to block the offending function. This works well for multibyte instructions but is problematic for single byte instructions. What the MAX10 does for those single byte instructions is make the decision to truncate the chip select after the first 6 bits of the instruction, presuming the values of the last two bits. For Quad-SPI (QSPI) interfaces, the MAX10 would need to make that decision after the first 4 bits of the instructions. The Lattice XO3D SPI Monitor also uses chip select truncation for multibyte instructions but adds a second mechanism that stretches the chip select and adds additional bogus clock cycles. This allows the monitor and filtering to look at all 8 bits of the instruction, whether in Security Support Provider Interface (SSPI) or QSPI modes, before making the decision to take action.

The above difference in SPI monitor/filter function then results in slight differences to how the high-speed multiplexors are connected. In general, the SPI filtering functionality of the MAX10 happens inside the MAX10 and the multiplexors are used to select between the MAX10 SPI Master or the BMC/PCH. In the Lattice XO3D implementation, the multiplexor becomes an integral part of the filtering due to speed constraints.

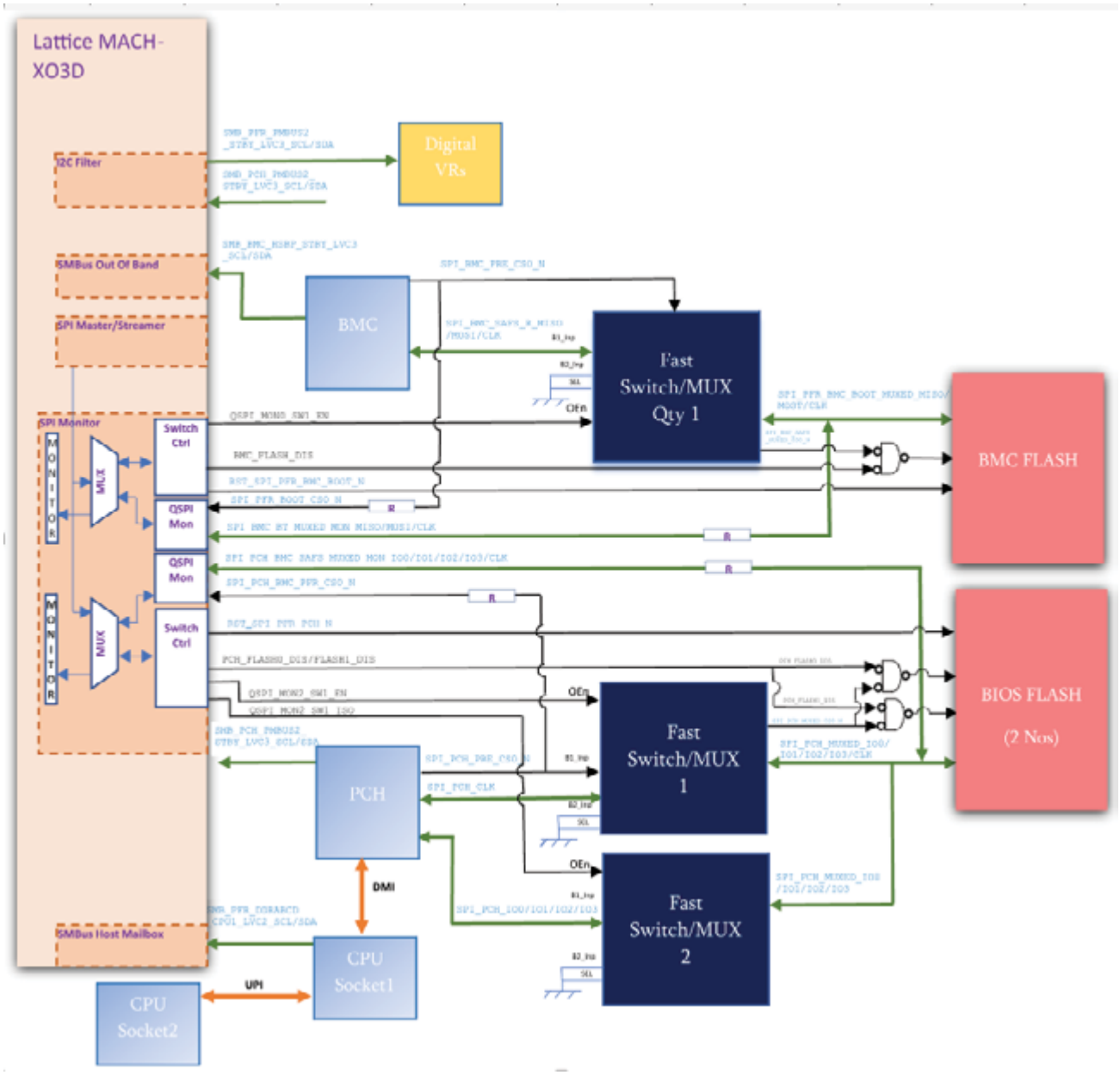


Figure 1. Key Lattice MachX03D connections.

References

[1] 83% of businesses have experienced firmware attacks recently (windowsreport.com)

[2] Cost of a Data Breach Report 2021 | IBM

[3] https://www.latticesemi.com/Products/FPGAandCPLD/MachXO3D

For more information please visit the request form at ami.com/contact