Solution Brief

USING FPGAs TO NAVIGATE EVOLVING REGULATORY REQUIREMENTS FOR CYBERSECURITY

Achieve Cyber Resilience and Enable Compliance with Key CNSA, NIST, CRA, and EU Regulations for Enhanced Security and Trust

Overview

The cyber threat landscape is showing no signs of slowing down. As cybercriminals develop more sophisticated techni ques and target a wider range of organizations, traditional security measures are becoming increasingly insufficient – and costly. The urgency for cyber resilience is rising as threats accelerate in volume and velocity across a widening attack surface. In response, global cybersecurity regulatory frameworks are rapidly evolving with several new requirements about to come into effect.

This surge in new regulations and standards is intended to help organizations address critical vulnerabilities and build resilience while creating accountability for data breaches. Keeping pace with the evolving regulatory environment is a challenging undertaking for developers with complex design processes and legacy infrastructure. Leveraging field programmable gate array (FPGA) technology will be key for organizations to effectively protect systems from sophisticated attacks and remain compliant with new requirements.

Cybersecurity Guideline Requirements

While there are a large number of cybersecurity regulations, standards, and frameworks for different markets, they all require similar capabilities. Lattice FPGAs provide critical security features to enable system designers to achieve compliance with these security frameworks. The inherent flexibility of FPGAs makes them adaptable to ensure ongoing compliance as regulations evolve.

Device Cybersecurity Requirements

The Cybersecurity Standards & Regulations provide a set of security principles and practices that must be followed. They also define a set of capabilities that must be supported at the device level. See Tables 1 and 2. Cybersecurity guidelines require device manufacturers to:

- Have a process that considers security from the start
- Make sure devices are secure and verify security via testing
- Monitor and address post-market cybersecurity vulnerabilities
- Support a firmware update process for in-field devices to address identified vulnerabilities

KEY CHALLENGES

- Modern systems cannot be secured with point solutions or by adding a single layer of security
- Organizations need a holistic approach to protect modern systems against cyber threats
- Security solutions must be updatable to stay ahead of evolving attacks and new regulatory requirements
- Strong locking and tamper detection is needed to prevent malicious malware installations or code modifications

LATTICE SOLUTION

- Secure Boot
- Platform Firmware Resilience
- Device Identifier Composition Engine (DICE)
- Secure enclave
- Cyber Resilience Act (CRA) compliance
- Regulatory compliance
- Identity, encryption, and authentication
- Agile Post-Quantum Cryptography
- Denial of service attack resistance
- CNSA 1.0 and Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) compliance

Table 1: FDA Guidelines

FDA GUIDANCE: DEVICE CAPABILITIES	
Authentication Authorization	Secure authentication
Confidentiality	Secure data transfer and data encryption
Data, Code, and Execution Integrity	Secure Boot and secure updates
Event Detection and Logging	Detect and log security events
Resiliency and Recovery	Detect attacks and unauthorized changes to code and data, then initiate recovery
Updates and Patches	Authenticate code, sign firmware and field updates

Table 2: Regulations & Standards Driving Security Requirements

REGULATION	SCOPE/TARGET	KEY REQUIREMENTS
CISA Mandates and NIST Guidelines	US critical infrastructure	Zero Trust, HRoT, Secure Boot, PFR
CNSA 2.0 and Executive Order 14144	US national security systems	Post-Quantum Cryptography (PQC)
Quantum Computing Cybersecurity Preparedness Act	US government agencies and their suppliers	PQC, crypto agility
EU Cyber Resilience Act (CRA)	Hardware and software product creators selling into the EU	Cyber resilience, secure updates, hardware-based security, PFR
FDA Cybersecurity in Medical Devices Guidance	Medical device manufacturers	Secure Boot, secure updates, cyber resilience, device identity, encryption
ETSI, CISA, ENISA	Critical infrastructure	Zero Trust, cyber resiliency, supply chain security

National Institute of Standards and Technology (NIST) 800-193 Platform Firmware Resiliency (PFR)

NIST 800-193 PFR guidelines describe the principles of supporting platform resiliency. PFR guidelines are based on the security principles of:

- **Protection:** Ensuring the integrity of platform firmware code and critical data by providing a process for ensuring the authenticity and integrity of firmware updates.
- **Detection:** Detecting when platform firmware code and critical data have been corrupted, or otherwise changed from an authorized state.
- **Recovery:** Restoring platform firmware code and critical data to a state of integrity in the event firmware code or critical data are detected to have been corrupted, or when forced to recover through an authorized mechanism.

Lattice FPGAs provide an ideal platform to implement PFR functionality to protect firmware for other components in the system.

Implementing PFR enables organizations to combat attacks in real-time by proactively monitoring data traffic for malware. When a malware attack is detected, the FPGA can load a recovery image of the authorized firmware. The recovery image overrides the unauthorized version, providing a quick recovery. This helps alleviate in-system firmware attacks by providing efficient protection, detection, and recovery capabilities.

Hardware Root of Trust

The inherent flexibility of FPGAs makes them an ideal solution for real-time hardware Root of Trust (HRoT) devices. An HRoT solution can deliver enhanced zero trust authentication of server platforms and other connected device applications to secure a system's end-to-end attack surface. FPGA-powered HRoT devices can be tailored to specific security needs, allowing developers to implement security features like encryption of configuration data or implement attestation flows. This flexibility empowers designers to create a more robust HRoT environment suited to the unique security requirements of their applications.

Unlike traditional processors where firmware resides in software memory, FPGAs store code in a separate hardware component. This makes it physically challenging to access and modify the firmware directly. This hardware-based trust protects from AI-based attacks on security implemented through software only. FPGAs may also contain dedicated security engines hardened in silicon with secure, immutable unique IDs. The security engine is used to ensure that the system's core functions and components are verified as genuine and unaltered, mitigating the risk of unauthorized access or malicious tampering.

Lattice FPGAs enable HRoT capabilities to ensure the security of FPGA bitstreams, firmware, software, and device configuration. This provides virtually instant detection against multiple types of attacks and compliance with security standards. See Figure 1.

Figure 1: Cyber Resiliency Specifies Using a Hardware Root of Trust Device to Perform Detect, Protect, and Recover Functions

Detection	Protection	Recovery
Cryptographically detect corrupted platform firmware & critical data At Power-On After In-System Updates	Protect platform firmware & critical data from corruption Ensure authenticity & integrity of firmware updates	Restore corrupted firmware & critical data to a known good value Initiate trusted recovery process

Platform Root Of Trust

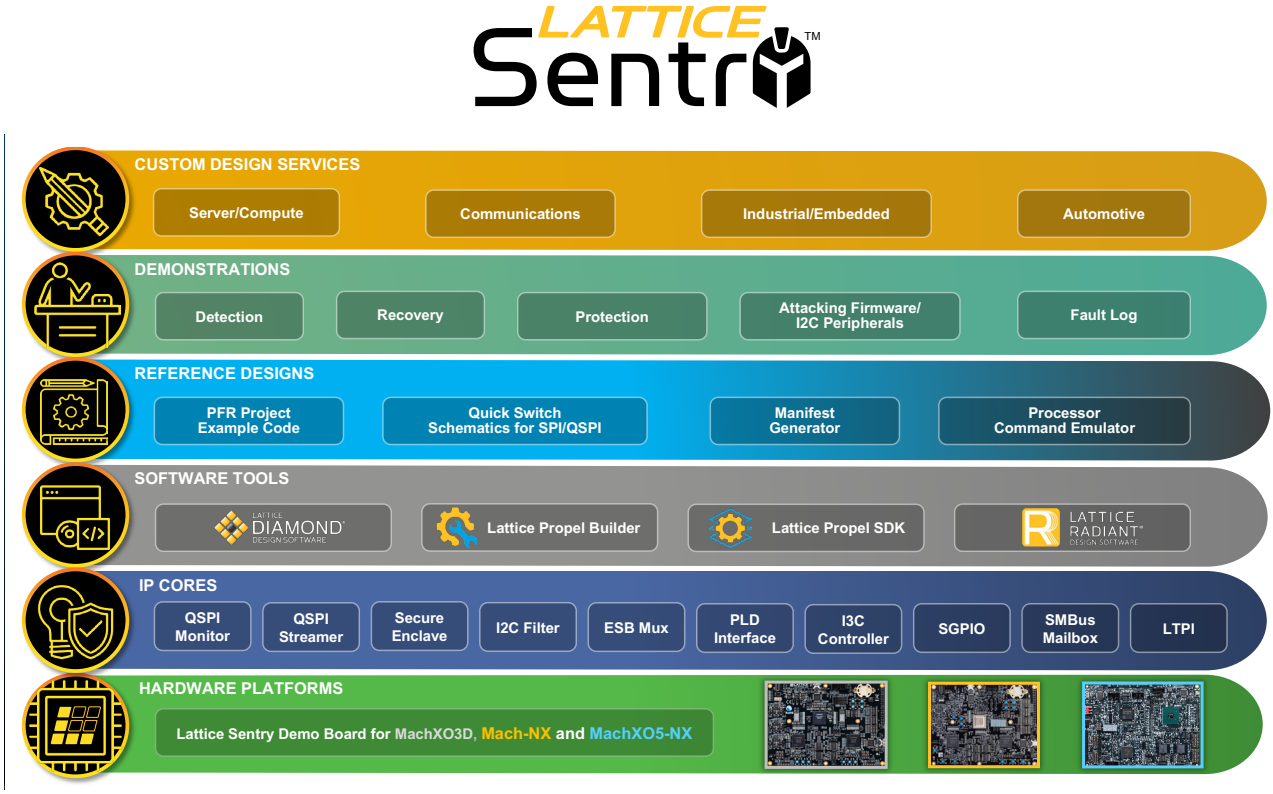
Lattice FPGAs can also be used to implement Platform Root of Trust functionality. Operating as the “first on, last off” device, the FPGA can authenticate Basic Input Output System (BIOS) or Baseboard Management Controller (BMC) flash and firmware before handing over control during the boot process.

Cyber Resiliency

Achieving cyber resilience and meeting stringent regulatory requirements like the Cyber Resilience Act (CRA) requires security at the device, system, and supply chain levels. This requires multiple layers of protection, which can only be achieved by implementing multiple security features to protect against sophisticated, multi-stage attacks.

The Lattice Sentry™ solution stack helps minimize in-system firmware attack vulnerabilities by providing real-time, dynamic protection, detection, and recovery capabilities to programmable components in a system. See Figure 2. It also enables next-generation hardware Root of Trust solutions complaint with NIST PRF guidelines (NIST SP 800-193) and supports both classical and PQC authentication. Building on this system-level protection, Lattice RoT FPGAs strengthen foundational security elements required for CRA certification.

Figure 2: Lattice Sentry Solution Stack



Regulatory Requirements Driving PQC Adoption

Why PQC is Important

Quantum computers will break RSA and ECC encryption, undermining the integrity of virtually all of today's security systems. Without quantum safe cryptography, all information that is transmitted on public channels is vulnerable to eavesdropping.

Even encrypted data that is safe against current adversaries can be stored for later decryption once a practical quantum computer becomes available. Furthermore, quantum computers will allow forging of RSA and ECC signatures, making it impossible to detect if data has been tampered with.

NIST

On August 13, 2024, the U.S. NIST marked a significant milestone in cybersecurity by finalizing the first set of PQC standards. NIST has approved four principal algorithms designed to secure digital communications against the threat posed by quantum computers.

- **ML-KEM (CRYSTALS-Kyber):** A key encapsulation mechanism for secure key exchange
- **ML-DSA (CRYSTALS-Dilithium):** A robust digital signature algorithm
- **SLH-DSA (SPHINCS+):** An alternative digital signature algorithm
- **FN-DSA (Falcon):** An additional alternative digital signature algorithm, the standard for FN-DSA has not yet been released

PQC Initiatives Around The World

National governments and international standards bodies are working on guidance and regulations defining PQC algorithm requirements and adoption timelines. These standards define both the PQC algorithms to be used and the timelines for adopting PQC algorithms. The NIST PQC standards provide the foundation for the algorithms used throughout the world. Even those countries that are considering using algorithms other than those defined by NIST are still heavily influenced by the NIST algorithms. In some cases (France and Germany), they are adopting both the algorithms specified by NIST and some of the algorithms NIST considered but did not standardize. In other cases (China), they are adopting the NIST algorithms, but with slight changes to create country-specific versions of the algorithms. See Table 3.

CNSA 2.0 & Global PQC Requirements

On September 7, 2022, the NSA released the CNSA 2.0 ("Announcing," 2022) requirements. This document specifies the encryption algorithms to be used in systems related to national security. CNSA 2.0 mandates the use of:

- XMSS/LMS for code signing
- ML-DSA (CRYSTALS-Dilithium) for digital signatures
- ML-KEM (CYRSTALS-Kyber) for key exchange

CNSA 2.0 requirements also define timelines for adopting PQC algorithms, with requirements for adoption beginning in 2025. ANSI, BSI, and other global security organizations are also publishing timelines and requirements for PQC adoption.

Crypto Agility

The development of PQC is still evolving. It is therefore crucial that cryptographic solutions maintain a high degree of agility to adapt to new standards. Crypto agility is essential to allow systems to swiftly integrate advancements in cryptography to ensure ongoing security against emerging quantum threats.

Lattice FPGAs are poised to play a pivotal role in navigating this complex environment. Their unique capabilities directly align with the demands of emerging regulations that prioritize flexibility and resilience. This makes Lattice FPGAs ideal for implementing crypto agility. As new standards evolve, FPGAs can be reprogrammed to implement new or updated algorithms.

Why Lattice FPGAs

Flexibility and Reprogrammability

Lattice FPGAs are inherently flexible solutions. This enables them to be reprogrammed and retrofitted to align with evolving regulations and standards without the need for removal from host devices. As a result, developers can efficiently deliver new security features and updates to FPGA-based architectures without new tape outs or device switch outs. This flexibility also increases FPGA's longevity compared to other types of semiconductors, for added cost savings.

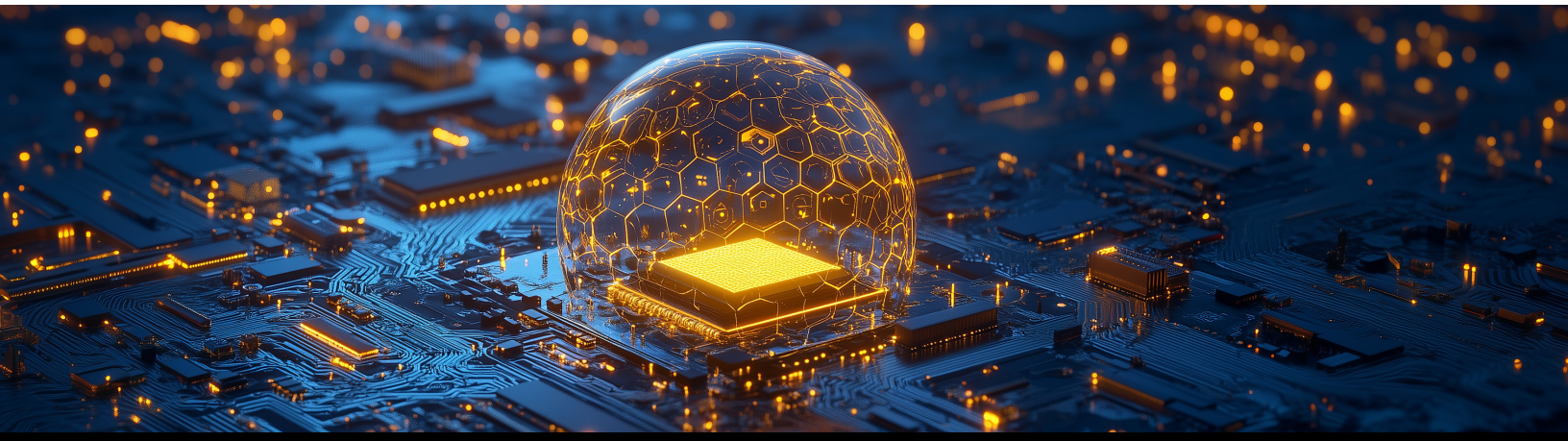
Built-in Security Features

Many FPGAs also provide built-in security features such as encryption and authentication mechanisms that help safeguard data during processing. By incorporating Lattice low power FPGAs into data processing infrastructure, organizations can strengthen their data security posture and mitigate risk. Security updates can be quickly delivered, helping organizations ensure compliance with constantly evolving government regulations.

Lattice FPGAs also provide side-channel attack (SCA) resistance and tamper detection for protection from side channel and physical attacks.

Table 3: PQC Initiatives Around The World

COUNTRY/REGION	PQC ALGORITHMS UNDER CONSIDERATION	PUBLISHED GUIDANCE	TIMELINE FOR ADOPTION
Australia	NIST algorithms	ASD/ACSC (2023)	Implementation started in 2025–2026
Canada	NIST algorithms	Cyber Centre (2021)	Implementation started in 2025
China	China specific	CACR (2020)	Planning started now
European Union	NIST algorithms	ENISA (2022), European Commission (2024)	Planning and implementation started now
France	NIST, FrodoKEM, LMS, XMSS	ANSSI (2023)	Implementation started in 2025
Germany	NIST algorithms, LMS, XMSS, FrodoKEM, ClassicMcEliece-KEM	BSI (2022)	Implementation started in 2025
Japan	Monitoring NIST	CRYPTREC (2022, 2024)	Planning started now
New Zealand	NIST algorithms	NZISM (2022)	Planning started now
Singapore	Monitoring NIST	MCI (2022), Monetary Authority of Singapore (2024)	Planning started now
South Korea	KpqC	MSIT (2024)	Additionally, South Korea–specific algorithms to be selected in 2024
United Kingdom	NIST algorithms, LMS, XMSS	NCSC (2023)	Implementation started now (2025)
United States	NIST algorithms, LMS, XMSS	CISA (2021, 2022, 2023) NIST (2023) NSA (2022, 2024) White House (2022, 2024) Congress (2022)	Implementation startedin 2025; required to begin in 2025



Ready to Learn More?

To learn more about Lattice low power FPGA-based solutions for compute, communications, industrial, and embedded applications, visit **www.latticesemi.com** or contact us at **sales@latticesemi.com**.