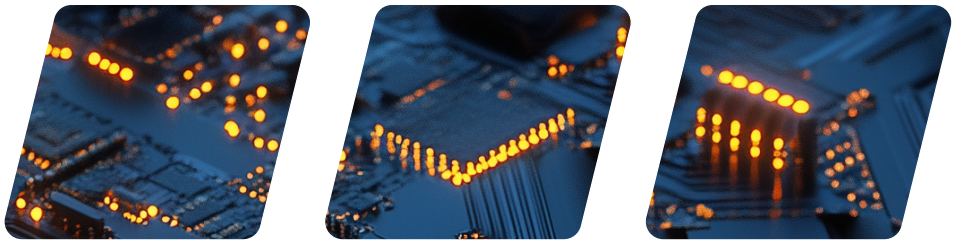
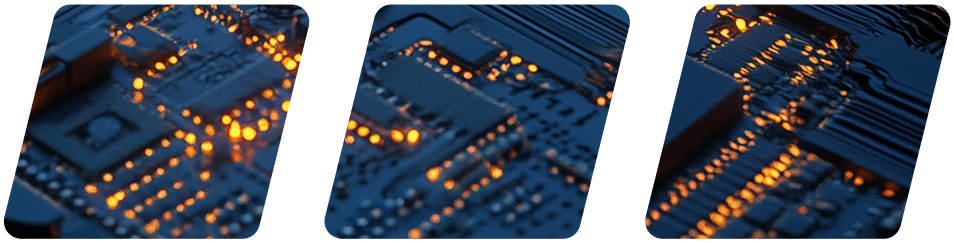


Securing the Future of Humanoid Robotics with TPM-anchored FPGAs with Post-quantum Cryptography



White Paper

Authors:
Eric Sivertson, VP of Security Business, Lattice Semiconductor
Steve Clark, Security Technologist, SEALSQ

DISCLAIMERS

Lattice makes no warranty, representation, or guarantee regarding the accuracy of information contained in this document or the suitability of its products for any particular purpose. All information herein is provided AS IS, with all faults, and all associated risk is the responsibility entirely of the Buyer. The information provided herein is for informational purposes only and may contain technical inaccuracies or omissions, and may be otherwise rendered inaccurate for many reasons, and Lattice assumes no obligation to update or otherwise correct or revise this information. Products sold by Lattice have been subject to limited testing and it is the Buyer's responsibility to independently determine the suitability of any products and to test and verify the same. Lattice products and services are not designed, manufactured, or tested for use in life or safety critical systems, hazardous environments, or any other environments requiring fail-safe performance, including any application in which the failure of the product or service could lead to death, personal injury, severe property damage or environmental harm (collectively, "high-risk uses"). Further, buyer must take prudent steps to protect against product and service failures, including providing appropriate redundancies, fail-safe features, and/or shut-down mechanisms. Lattice expressly disclaims any express or implied warranty of fitness of the products or services for high-risk uses. The information provided in this document is proprietary to Lattice Semiconductor, and Lattice reserves the right to make any changes to the information in this document or to any products at any time without notice.

INCLUSIVE LANGUAGE

This document was created consistent with Lattice Semiconductor's inclusive language policy. In some cases, the language in underlying tools and other items may not yet have been updated. Please refer to Lattice's inclusive language FAQ 6878 for a cross reference of terms. Note in some cases such as register names and state names it has been necessary to continue to utilize older terminology for compatibility.

ABSTRACT

Humanoid robots are rapidly transitioning from research prototypes to real-world deployment in factories, healthcare facilities, logistics operations, and public environments. As these systems increasingly operate alongside humans, safety and security become inseparable requirements. A cyber-compromised humanoid is not just a data breach; it is a direct physical safety risk with long-term regulatory, legal, and operational consequences. This white paper examines why traditional, bolt-on security approaches are insufficient for humanoid platforms and argues for a hardware-native trust architecture anchored at the edge. It demonstrates why Trusted Platform Module (TPMs), Field-Programmable Gate Arrays (FPGAs), and post-quantum cryptography together form a foundational requirement for safe, scalable, and commercially viable humanoid robotics.

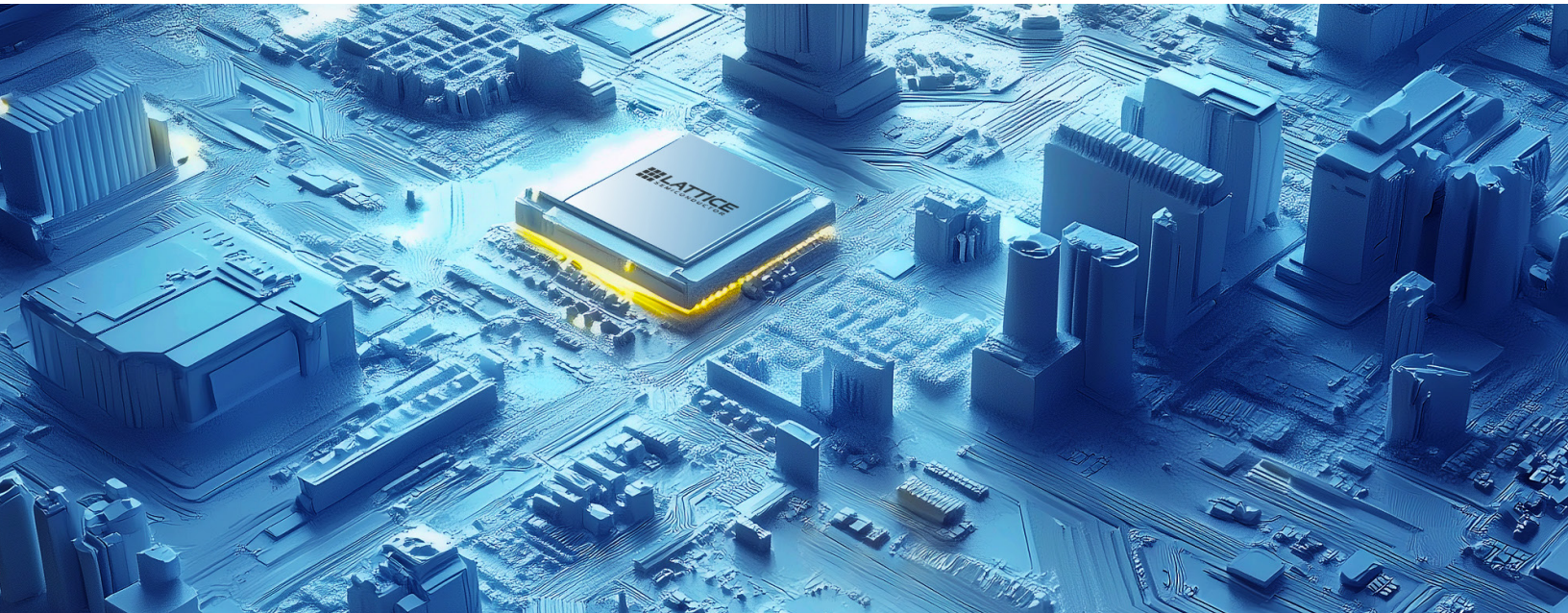


TABLE OF CONTENTS

Introduction

Humanoid robots are no longer laboratory curiosities. They are rapidly entering factories, warehouses, healthcare facilities, and service environments as the ultimate expression of physical AI—embodied systems that sense, reason, act, and collaborate with humans in shared spaces. Yet with this capability comes unprecedented responsibility. A compromised humanoid is not merely a cybersecurity incident; it is a physical safety failure with potential for harm, data exfiltration, regulatory violations, and cascading systemic risk.

Safety and security in humanoids are inseparable. Traditional bolt-on approaches are not sufficient. What is required is hardware-native trust anchored at the edge: deterministic control, immutable Root of Trust (RoT), cyber resilience, standards-compliant attestation, and future-proof cryptography.

Lattice Semiconductor and SEALSQ have delivered exactly that solution. Through their collaboration on a unified TPM-FPGA architecture, Lattice's low power, secure FPGAs are combined with SEALSQ's QS7001[1] and QVault TPM[2]-based secure Root of Trust. The result is a programmable, quantum-resistant security foundation purpose-built for humanoid platforms—delivering real-time deterministic motor and sensor control, hardware-enforced cyber resilience, and protection against both today's threats and tomorrow's quantum attacks.

This white paper, written from the perspective of designers who have developed and deployed humanoid systems, details why this integrated approach is not optional but essential for safe, scalable, and commercially viable humanoid deployment.

The Humanoid Imperative: From Prototype to Production

The humanoid robotics market is accelerating toward an inflection point in 2026–2027. Leading platforms from Tesla (Optimus), Boston Dynamics (Atlas), Figure AI, Agility Robotics, and others are transitioning from research prototypes to early commercial deployments in manufacturing, logistics, and service sectors.[3] See Figure 1. Analysts project a market size approaching $6–6.5 billion by 2030 with exceptional CAGR.[4]

These systems demand sub-microsecond motor control loops, dense multi-modal sensor fusion, real-time perception, and power efficiency under strict thermal and battery constraints. FPGAs excel here because they implement functionality directly in hardware—delivering true determinism that instruction-based processors (CPUs, GPUs, and MCUs) simply cannot match within a single clock cycle.

Yet technical feasibility is only half the battle; trust is the other half. Enterprises will not deploy fleets of humanoids at scale without ironclad guarantees of safety, security, and privacy. Víctor Mayoral-Vilches, Founder and CEO of Alias Robotics, says it succinctly, "Robots are only safe if secure."[5]

Figure 1: Robotic Worker Operating in a Smart Factory

Safety and Security: Two Sides of the Same Coin

In humanoid systems, safety and security cannot be decoupled. A robot designed for safe, precise motion can still become a weapon if cyber-compromised. Conversely, a system that shuts down at every anomaly may fail to maintain stable locomotion or execute emergency stop protocols.

Traditional IT or industrial-robotics security models fall short. Humanoids operate in dynamic, human-shared environments with persistent multi-modal sensor streams, distributed edge nodes (joints, fingers, and actuators), and long operational life cycles measured in decades. The key risks include:

- Physical harm resulting from hijacked actuators or locomotion
- Exfiltration of proprietary enterprise data or private human interactions
- Botnet formation across fleets once a single vulnerability is discovered
- Privacy violations under GDPR, CCPA, or emerging AI regulations
- Supply-chain tampering or firmware rollback attacks

These threats are amplified by the “harvest now, decrypt later” quantum risk. Humanoids deployed today will still be operational when large-scale quantum computers arrive. Classical cryptography such as RSA and ECC will be obsolete. Post-quantum cryptography (PQC) must be baked in at the hardware level from day one.

The TPM-anchored FPGA Solution: Hardware Root of Trust at the Edge

The Trusted Computing Group’s (TCG) TPM specification provides the industry-standard foundation for attestation, secure boot, key storage, and cryptographic identity. When anchored to a programmable FPGA that acts as the system’s first-on/last-off component, the TPM becomes a dynamic, real-time cyber-resilience platform rather than a static discrete chip.

Lattice FPGAs deliver this foundation through:

- Hardware Root of Trust (HRoT) with immutable secure boot and dual-boot capabilities
- Built-in support for NIST 800-193 Platform Firmware Resiliency (PFR), Device Identifier Composition Engine (DICE), and Zero Trust architectures
- Parallel fail-safe mechanisms (lock-step redundancy and continuous attack-surface validation)
- Deterministic control for motor drivers, joint actuators, and sensor interfaces

SEALSQ’s QS7001 and QVault TPM products elevate this further by embedding NIST-selected PQC algorithms—CRYSTALS-Kyber (ML-KEM) for key encapsulation and CRYSTALS-Dilithium (ML-DSA) for digital signatures—directly into a tamper-resistant hardware RoT. This unified TPM-FPGA architecture enables:

- Quantum-resistant secure boot and runtime attestation
- Hardware-enforced firmware updates and policy enforcement
- Per-node cryptographic identity across every joint and actuator
- Real-time cyber-resiliency

A joint TPM-FPGA solution proof of concept demonstrated by Lattice and SEALSQ integrates a Lattice MachXO4™ secure FPGA with SEALSQ’s PQC-based QS7001 and QVault TPM RoT. It demonstrates the feasibility of embedding TPM-class post-quantum capabilities into programmable hardware, creating a reference design for edge systems where power, size, and determinism matter most. Together, Lattice’s broader security portfolio, including the Lattice Sentry™ solution stack and Lattice Mach™-NX FPGA devices, combined with SEALSQ’s QS7001 and QVault TPMs, provide a complete, standards-aligned path to trusted physical AI.

Why FPGAs + TPM + PQC Is the Only Viable Path for Humanoids

From a humanoid system designer's perspective, the benefits are immediate and measurable. TPMs provide a critical foundation for end-to-end attestation and cyber resilience, but they cannot stand alone. By integrating SEALSQ QVault TPM with Lattice MachXO4 FPGAs, designers gain a scalable path to quantum-resistant security that supports a wide range of applications. See Table 1 for key advantages enabled by the joint solution.

Table 1: Key Advantages of Lattice FPGAs with SEALSQ TPM and PQC for Humanoid Systems

Determinism Meets Security	Cyber Resilience at Every Node	Quantum Readiness Today	Compliance and Liability Reduction	Power and Form-Factor Efficiency
▪ Critical control loops (balance, grasping, & locomotion) execute in hardware with single-cycle predictability ▪ Continuously attested and protected by TPM policies ▪ No instruction-pipeline jitter ▪ No security overhead that compromises real-time performance	▪ Multiple FPGAs can operate in lock-step across the humanoid's body ▪ A compromise in one joint is isolated and mitigated without cascading to the entire system ▪ Real-time monitoring and mitigation exceed what discrete TPMs or software-only solutions can achieve	▪ Low power, small FPGA with dual-boot, integrated lockable flash ▪ Future-proof the entire platform against quantum threats for years, without costly redesigns	▪ Meets or exceeds NIST, TCG, Radio Equipment Directive (RED), and Cyber Resilience Act (CRA) requirements ▪ Provides auditable cryptographic identity and attestation logs essential for insurance, regulatory approval, and enterprise deployment	▪ Low power, small Lattice FPGAs ensure security does not compromise battery life or thermal budgets, which is critical for untethered, mobile humanoids

Proof of Concept and Availability

The joint TPM-FPGA proof of concept with embedded PQC is available for evaluation. It provides a drop-in reference design for humanoid developers moving from prototype to production with built-in quantum resilience.

Conclusion: Trust Is the New Dexterity

Humanoid robotics will succeed not because the hardware can walk and grasp, but because enterprises and consumers trust that it will do so safely, securely, and privately—today and for decades to come. By anchoring every critical control point to a TPM-FPGA architecture with native post-quantum cryptography, Lattice Semiconductor and SEALSQ deliver that trust at the silicon level. This is not incremental security; it is foundational resilience engineered for the unique demands of embodied AI. Developers and manufacturers can now move humanoids from pilot to production with a proven, quantum-ready solution. The era of trusted physical AI has arrived.

References

[1] SEALSQ, https://www.sealsq.com/semiconductors/platforms/quantum-shield/qs7001

[2] SEALSQ, https://www.sealsq.com/products/secure-element/tpm/qvaulttpm

[3] Future Markets, https://www.futuremarketsinc.com/humanoid-robots-market-report-2026-2036/

[4] ABI, https://www.abiresearch.com/news-resources/chart-data/humanoid-robot-market-size-outlook (Also detailed in their Global Robotics Market Outlook: https://www.abiresearch.com/blog/global-robotics-market-outlook)

[5] IEEE Spectrum, https://spectrum.ieee.org/unitree-robot-exploit

READY TO LEARN MORE?

Learn more and evaluate the unified TPM-FPGA solution:
Visit Lattice Semiconductor at **www.latticesemi.com** or contact your Lattice representative.
Visit SEALSQ at www.sealsq.com.

TECHNICAL SUPPORT ASSISTANCE

Submit a technical support case through **www.latticesemi.com/techsupport**.
For frequently asked questions, please refer to the Lattice Answer Database at **www.latticesemi.com/Support/AnswerDatabase.**

V.2 WP0053