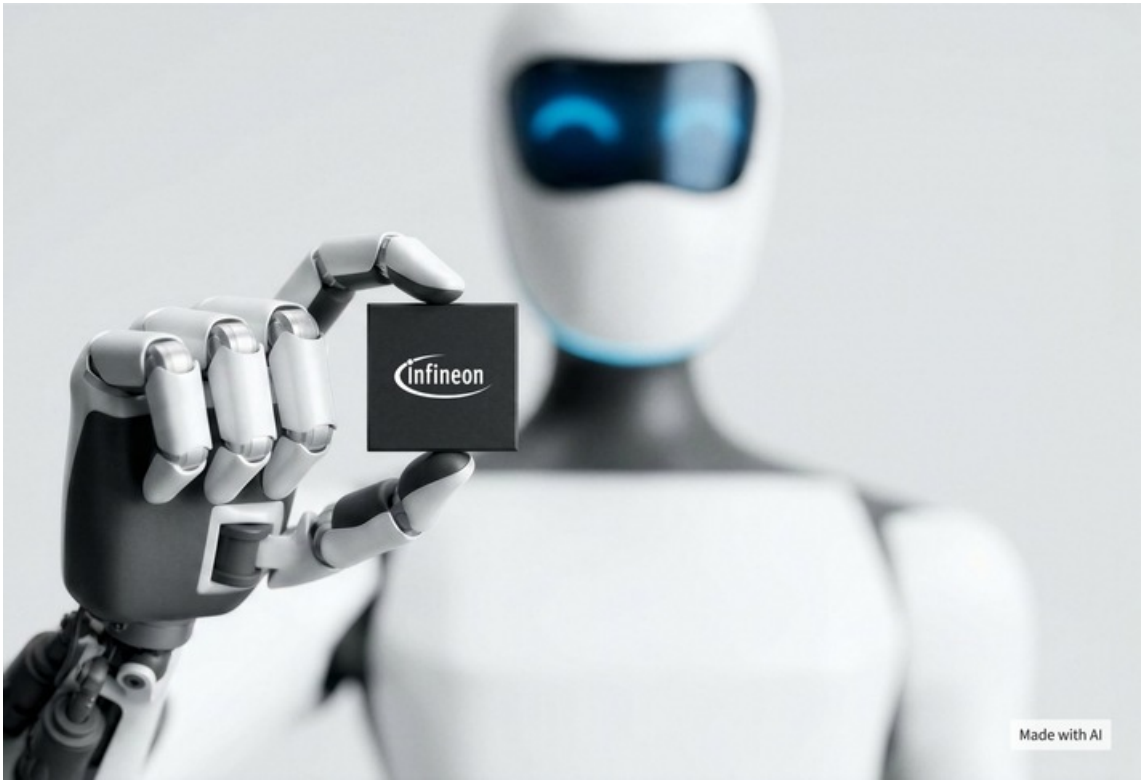
Infineon Technologies AG

03.06.2026 – 11:05 Uhr

Infineon stärkt Sicherheit für Physical AI mit zertifizierter TPM-Lösung und quantenresistenter Hardware-Sicherheit für NVIDIA-Robotikplattform Jetson Thor



München (ots) -

Die Infineon Technologies AG integriert sein Hardware-Sicherheitsmodul OPTIGA™ TPM SLB 9672 in die Rechenplattformen für Robotik und autonome Systeme Jetson Thor von NVIDIA. Das Modul sichert kryptografische Schlüssel direkt auf Chip-Ebene und schützt so die Systemintegrität gegen Manipulation und unbefugten Zugriff. Das Ergebnis ist eine zertifizierte, quantenresistente Vertrauensbasis, die sogenannte Root of Trust, auf der künftige Physical-AI-Systeme aufgebaut werden können. Da Roboter und autonome Maschinen zunehmend abgeschirmte Industrieumgebungen verlassen und in Fabriken, Logistikzentren und öffentlichen Räumen operieren, steigen nicht nur die Sicherheitsanforderungen, sondern auch die wirtschaftlichen Risiken. Ein Cyberangriff kann Betriebsunterbrechungen und Haftungsansprüche nach sich ziehen, die weit über einen klassischen Datenverlust hinausgehen. Für Hersteller und Betreiber von Robotersystemen ist die Wahl der Sicherheitsarchitektur deshalb keine rein technische Entscheidung. Sie beeinflusst die langfristige Wettbewerbsfähigkeit, die Zulassungsfähigkeit in regulierten Märkten sowie die Gesamtbetriebskosten über den vollständigen Produktlebenszyklus.

„Roboter, die die reale Welt wahrnehmen, analysieren und auf sie reagieren, sind nur so vertrauenswürdig wie die Sicherheitsbasis, auf der sie aufgebaut sind", sagt Dr. Stephan Zizala, Divisionspräsident Connected Secure Systems bei Infineon. „Das OPTIGA TPM von Infineon verankert eine hardwarebasierte Vertrauensbasis in der NVIDIA Jetson-Thor-Plattform, die sich bereits in Hunderten Millionen von Geräten weltweit bewährt hat. Damit erfüllt die Integration die besonderen Anforderungen industrieller Robotik: lange Lebenszyklen, Echtzeitfähigkeit und einen zuverlässigen Betrieb im großen Maßstab. Die darin integrierte Post-Quantum-Kryptografie stellt sicher, dass diese Grundlage nicht nur gegen aktuelle Bedrohungen gewappnet ist, sondern über die gesamte Lebensdauer jedes Roboters hinweg Schutz bietet."

„Physical-AI-Systeme agieren in der realen Welt, in der Sicherheit eine grundlegende Voraussetzung ist", sagt Deepu Talla, Vice President Robotics and Edge AI bei NVIDIA. „Das zertifizierte OPTIGA TPM von Infineon für NVIDIA Jetson Thor unterstützt Entwickler dabei, kryptografische Schlüssel zu schützen, die Integrität der Software zu verifizieren und Roboterflotten im großen Maßstab gesichert bereitzustellen. Dadurch entsteht eine

hardwarebasierte Vertrauensbasis – die Grundlage für gesicherte und resiliente autonome Systeme."

Der EU Cyber Resilience Act, der EU AI Act, die Norm IEC 62443 für industrielle Systeme sowie branchenspezifische Standards im Gesundheitswesen und in der Automotive-Industrie führen zu neuen Anforderungen an nachweisbare und auditierbare Sicherheit auf Hardwareebene. Dadurch entsteht eine durch regulatorische Vorgaben und Compliance-Anforderungen getriebene Nachfrage, die Infineon und NVIDIA gezielt adressieren können.

Die OPTIGA TPM-Technologie bietet eine physisch isolierte, nach FIPS und Common Criteria zertifizierte Lösung, die vom Anwendungsprozessor getrennt ist. Sie ermöglicht einen gemessenen Systemstart (Measured Boot) sowie eine Fernbeglaubigung (Remote Attestation), sodass Betreiber und Aufsichtsbehörden zu jedem Zeitpunkt des Betriebs eines Systems kryptografisch verifizieren können, ob der Software-Stack authentisch und unverändert ist. Darüber hinaus stellt sie hardwaregeschützten Speicher für proprietäre KI-Modellschlüssel, verschlüsselte Kommunikation sowie kryptografisch signierte Over-the-Air-Updates bereit.

Das OPTIGA TPM, das branchenweit erste TPM mit einem postquanten-gesicherten Firmware-Update-Mechanismus, wurde als Root of Trust konzipiert, die auch bei sich wandelnden kryptografischen Bedrohungslagen nicht kompromittierbar ist. Entwickler, die Physical-AI-Anwendungen auf der Jetson-Thor-Plattform von NVIDIA entwickeln, können sich auf die bereits in der Architekturphase verankerte hardwarebasierte Sicherheitsgrundlage verlassen und bleiben so gegen aktuelle wie zukünftige kryptografische Bedrohungen in Robotersystemen geschützt.

Die Roadmap zur vollständigen Post-Quanten-Sicherheit wird durch das OPTIGA TPM der nächsten Generation von Infineon abgerundet. Das TPM integriert Algorithmen wie ML-KEM und ML-DSA, die 2024 vom US-amerikanischen National Institute of Standards and Technology (NIST) standardisiert wurden. Unternehmen, die heute auf dem aktuellen OPTIGA TPM aufbauen, können künftig einen reibungslosen Übergang vollziehen. Für die Robotik-Branche ist dies über die technische Bereitschaft hinaus von Bedeutung. Die regulatorischen Rahmenbedingungen für Physical AI entwickeln sich bereits in Richtung einer verpflichtenden PQC-Konformität. Die zu Beginn getroffene Architekturentscheidung bestimmt daher, ob eine eingesetzte Roboterflotte diese Anforderungen über ihre gesamte Einsatzdauer hinweg erfüllen kann oder bei Inkrafttreten entsprechender Vorschriften mit kostspieligen Hardware-Eingriffen konfrontiert wird.

Humanoide Roboter sind auf eine Kette von Halbleiterfunktionen angewiesen, um gesichert und zuverlässig wahrzunehmen, zu denken und zu handeln – von der Sensorik über die Aktorik und das Energiemanagement bis hin zu Konnektivität und Sicherheit. Infineon adressiert all diese Funktionsbereiche mit einem breiten Portfolio spezieller Lösungen, wobei der geschätzte Halbleiteranteil pro humanoidem Roboter bei rund 500 US-Dollar liegt. Sicherheit ist kein optionales Merkmal, sondern die Grundlage moderner Robotik. Infineon baut den Schutzschild gegen die Bedrohungen von morgen. Sicherheitskomponenten, darunter TPMs, nehmen dabei einen immer größeren Anteil dieses Bestands ein, da die regulatorischen Anforderungen zunehmend an Bedeutung gewinnen. In Zusammenarbeit mit Ökosystempartnern wie NVIDIA unterstützt Infineon Roboterentwickler und -hersteller beim Übergang von Laboranwendungen zur Flottenbereitstellung in Industrie-, Gesundheits- und Logistikumgebungen.

Verfügbarkeit

Ein Referenzdesign für das OPTIGA TPM SLB 9672 ist verfügbar. Weitere Informationen sind erhältlich unter www.Infineon.com/OPTIGA-TPM-SLB9672, www.infineon.com/pqc und www.infineon.com/cra

Über Infineon

Die Infineon Technologies AG ist ein weltweit führender Anbieter von Halbleiterlösungen für Power Systems und das Internet der Dinge (IoT). Mit seinen Produkten und Lösungen treibt Infineon die Dekarbonisierung und Digitalisierung voran. Das Unternehmen hat weltweit rund 57.000 Beschäftigte (Ende September 2025) und erzielte im Geschäftsjahr 2025 (Ende September) einen Umsatz von rund 14,7 Milliarden Euro. Infineon ist in Frankfurt unter dem Symbol „IFX" und in den USA im Freiverkehrsmarkt OTCQX International unter dem Symbol „IFNNY" notiert.

Weitere Informationen erhalten Sie unter www.infineon.com

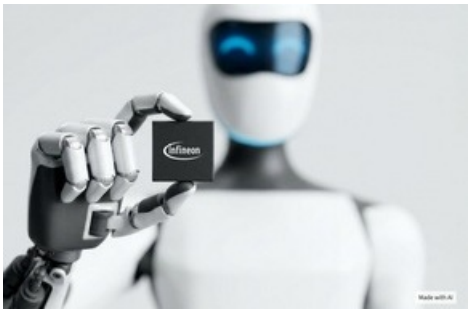
Diese Presseinformation finden Sie online unter www.infineon.com/presse

Follow us: Facebook - LinkedIn

Pressekontakt:

Michael Burner
Michael.burner@infineon.com

Medieninhalte



Mit Partnern wie NVIDIA hilft Infineon Robotikherstellern, den Schritt vom Pilotprojekt in die Serienproduktion zu schaffen. / Weiterer Text über ots und www.presseportal.de/nr/17888 / Die Verwendung dieses Bildes für redaktionelle Zwecke ist unter Beachtung aller mitgeteilten Nutzungsbedingungen zulässig und dann auch honorarfrei. Veröffentlichung ausschließlich mit Bildrechte-Hinweis.