räts. Apple will die Apple Watch damit ausstatten.

Zu den weiteren Produkten, die auf Basis von Silicon Photonics entwickelt werden, zählen elektronische Nasen, optische Kohärenztomografie-Systeme (sie funktionieren ähnlich wie medizinische Ultraschallgeräte, basieren aber auf Licht statt Schall), Diagnosegeräte für die Erkennung von Erkrankungen am Herzen und an den Blutgefäßen. Außerdem wird das Gebiet der optischen Transceiver weiterwachsen, beispielsweise um in Datenzentren verschiedene High-Performance-Computing-Elemente über Lichtwellenleiter zu vernetzen.

Intel, mit einem Marktanteil von 53 Prozent auf dem Sektor der optischen Transceiver eines der führenden Silicon-Photonics-Unternehmen, hat in wenigen Jahren bereits 3 Mio. 100G-Transceiver ausgeliefert. Mithilfe ihrer CWDM4-100G-Technologie kann Intel als erstes Unternehmen der Welt bereits Distanzen von 10 km überbücken.

Insgesamt wächst das Ecosystem rund um Silicon Photonics, die Zahl der Foundries und Packaging-Unternehmen nimmt zu, genauso wie die Zahl der Unternehmen, die Module auf Basis von Silicon Photonics entwerfen. (ha) ■

Debugging

Mehr Sicherheit für Cypress-SoC

Der Halbleiterhersteller Cypress weitet die Lizenzierung für das Embedded-Dateisystem „emFile“ von Segger auf seine Hardware-Plattform PSoC 6 aus. Somit stehen Entwicklern umfangreiche Sicherheitsfunktionen zur Verfügung. Alex Gruener, CTO, und Dirk Akemann, Partner Marketing Manager von Segger, sprechen über den Deal.

Markt&Technik: Gerade im Zuge des Entwickelns von IoT-Geräten wird Sicherheit immer wichtiger. Wie unterstützen Sie Entwickler, Ihr Design sicher zu gestalten?
Alex Gruener: Sicherheit und Kryptografie sind essenziell für alle Embedded-Systeme, speziell jedoch für vernetzte IoT-Anwendungen. Ob Entwickler ihre IP vor Fälschungen, ihre Geräte vor Manipulationen oder die auf den Geräten gesammelten Daten vor dem Ausspähen schützen wollen, die Bedrohungen sind vielfältig. Wir haben daher umfangreiche Kryptografie- und Sicherheits-Bibliotheken von Grund auf für Embedded-Systeme entwickelt. Die resultierenden Bibliotheken sind sehr schnell und verbrauchen wenig Speicherressourcen.

Können Sie das noch etwas detaillierter ausführen?
Gruener: Wir bieten eine komplette Ende-zu-Ende-Anwendung. Unsere Kunden haben Zugriff auf ein umfassendes IoT-Paket, das alle Bereiche von Entwicklungswerkzeugen bis zu Standard-Firmware-Komponenten abdeckt. Software-IP-Komponenten wie „emSSL“ Transport Layer Security (TLS), „emSSH Secure Shell“ oder „emSecure Digital Signature Suite“ – um einige zu nennen – können als Grundlage für sicher verbundene IoT-Geräte zum Einsatz kommen. Unsere Software funktioniert auf praktisch jeder MCU. Hierfür arbeiten wir mit allen großen Halbleiterherstellern zusammen.

Dirk Akemann, Partner Marketing Manager bei Segger

„Unsere Supply Chain ist stabil.“

Ihre Bibliothek „emFile“ hat kürzlich neue Funktionen bekommen. Können Sie diese kurz erläutern?
Dirk Akemann: emFile ist eine Dateisystem-Bibliothek, die es einer Embedded-Anwendung oder einem System ermöglicht, Daten sicher und zuverlässig auf jeder Art von Speichergerät zu sichern. Stichworte sind Ausfallsicherheit, Datenverschlüsselung, RAID-1- und RAID-5-Unterstützung und ECC-Fehlerkorrektur. emFile kommt weltweit auf mehreren Millionen Geräten zum Einsatz. Gerätetreiber sind zum Beispiel für NAND- und NOR-Flash, SD/SDHC/SDXC/MMC-Karten oder eMMC-Speichergeräte verfügbar. Außerdem unterstützt emFile die gängigen Dateisysteme FAT12/16/32 und das Segger-Dateisystem EFS (Embedded File System), das speziell für die Anforderungen moderner Embedded-Anwendungen entwickelt wurde.

Wie gewährleistet Journaling zusätzliche Sicherheit für das Dateisystem?
Akemann: emFile Journaling ist eine zusätzliche Komponente, die auf dem Dateisystem sitzt und die Dateisystemschicht ausfallsicher macht. Dateisysteme ohne Journaling-Unterstützung – zum Beispiel FAT und EFS – sind nicht ausfallsicher. Journaling bedeutet, dass ein Dateisystem alle Änderungen protokolliert, bevor sie in das Hauptdateisystem übertragen werden, und somit die Konsistenz des Dateisystems gewährleistet.

Können Sie den technischen Hintergrund erklären?
Akemann: Ein Datenverlust kann entweder in der Treiberschicht oder in der Dateisystemebene auftreten. Die Treiberschicht ist in der Regel ausfallsicher, sodass der einzige Ort für typische Datenverluste die Dateisystemschicht ist. Journaling gewährt der Dateisystemschicht zusätzliche Sicherheit.

Das Ziel der zusätzlichen Schicht ist es, zu garantieren, dass das Dateisystem nach einem