chen direkten Zugriffen abzuschirmen. Sie haben die Eigenschaft, dass sie einen Manipulationsschutz besitzen, der sie vor Hardwareangriffen schützt. Direkte Manipulationen an der Hardware werden erkannt, worauf sich das HSM sperrt und das Auslesen des internen Speichers verhindert (*Bild 1*).

Um diese Manipulationen zu erkennen, werden diverse Sensoren in das HSM mit eingebaut, um zum Beispiel Druckänderungen, Lichtänderungen, extreme Temperaturänderungen oder Röntgenstrahlung zu detektieren. Somit können empfindliche Daten wie Schlüssel und Zertifikate in dem HSM sicher gespeichert werden. HSMs bieten überdies den Vorteil, dass sie speziell für Kryptografie-Algorithmen entwickelt werden.

Die kryptografischen Funktionen werden schneller ausgeführt als auf einem Anwendungs-Mikrocontroller. Lediglich die Anbindung über einen Bus kann die Geschwindigkeit begrenzen.

Um bestehende Systeme um HSMs zu erweitern, bieten sich Elemente an, die über SPI oder I²C angebunden werden. Durch diese Möglichkeit muss der Mikrocontroller des Systems nicht getauscht, sondern lediglich um das externe Element erweitert werden. Voraussetzung dafür ist jedoch, dass die Anwendungssoftware angepasst wird und das System mit der neuen Firmware aktualisiert wird. Bei der Neuentwicklung eines Systems sollte ein HSM direkt in der Designphase mit eingeplant werden (Security by design).

Security in Energienetzwerken

Im Rahmen des EU-Forschungsprojekts CONNECT (http://www.connect-ecsel.eu), an dem die Firma Mixed Mode als Mitglied des Infineon Security Circle Partner Network beteiligt war, wurde der OPTIGA Trust X als HSM zur Absicherung eines Smart-Grids genutzt (*Bild 2*). Die Wandlung des Energienetzes vom reinen Verteilnetz hin zum Smart-Grid ist ein unverzichtbarer Schritt, um die Klimaschutzziele zu erreichen und den Bedarf an fossilen Energieträgern deutlich zu reduzieren. Wesentliche Elemente dieses Wandels sind die Erweiterung des Energieversorgungsnetzwerks zur Zustandserfassung in Echtzeit, sichere Kommunikationsverfahren für den Austausch von Zustands-, Kontroll- und Steuerungsdaten sowie die effiziente Wandlung elektrischer Energie zur Verknüpfung von Verbrauchern, Speichern und Energiequellen.

Ein zentrales Thema dabei ist die sichere drahtlose und drahtgebundene Kommunikation für den Austausch der obengenannten Daten zwischen den beteiligten Sensoren und Aktoren in einer Liegenschaft sowie mit einer dahinterliegenden Backend-Infrastruktur, bestehend aus den Kommunikations-Netzwerkstrukturen vom Sensor beziehungsweise Aktor über zentrale Kommunikationsknoten zum Verbraucher und zum Versorger.

Security-Anforderungen betreffen in erster Linie:

- eingebettete, energieeffiziente Systeme,
- das Smart-Grid selbst sowie die
- drahtlose Vernetzung intelligenter Sensorknoten im Anwendungsfall des Wireless-Sensor-Network.

Abfangen und Manipulation der Daten im drahtlosen Sensornetzwerk muss zwischen den Sensorknoten und dem Gateway als neuralgischer Strecke verhindert werden. Diese Aufgabe übernimmt der OPTIGA Trust X, der etwaige Manipulationen der Hardware erkennt und verhindert, sowie als sichere Ablage für Schlüssel und Zertifikate dient. Die Kommunikation zwischen dem Gateway und dem Energienetz wird durch einen Communication-Hub umgesetzt, der auf einer Linux-Plattform basiert, deren Security ihrerseits durch ein HSM der Firma NXP gewährleistet ist. Die Sensordaten werden verschlüsselt vom Gateway über den Communication-Hub in das Energienetz eingespeist, wobei die Schlüssel selbst eben auf den HSM und damit für Angreifer unerreichbar liegen.

Der im drahtlosen Sensornetz eingesetzte OPTIGA Trust X von Infineon ist nach Common Criteria EAL6+ (high) zertifiziert und somit der geeignetste Sicherheitscontroller dieser Firma. Er unterstützt ECC256, AES128 sowie SHA-256 und besitzt vier Speicherplätze für Schlüssel sowie zwei für Trust-Anchor-Zertifikate. Als Turn-Key-Lösung bietet er die Möglichkeit, mit wenig Aufwand eine sichere Verbindung über TLS/DTLS aufzubauen.

Einsatz des HSM mit RIOT

Der Sicherheitscontroller wird in Verbindung mit dem Betriebssystem RIOT eingesetzt (*Bild 3*), das eigens für IoT-Geräte entwickelt wurde. Durch seine Modularität ist es mit verschiedenen Mikrocontrollern und Peripheriegeräten einsetzbar und lässt