Thema:
Sichere Elektronik für die digitalisierte und vernetzte Produktion (SichEl)

Fördernummer:	BMWK/IGF-Nr. 20690 N
Laufzeit:	01.06.2019 – 31.05.2022
Schwerpunkte DFAM:	Security by Design, Security und Safety als Qualitätsmerkmal, Juristische Aspekte, Security

Forschungseinrichtungen:

- Fraunhofer-Institut für Mikroelektronische Schaltungen und Systeme IMS, Prof. Dr.-Ing. Rainer Kokozinski
- Hochschule Offenburg, Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK), Prof. Dr.-Ing. Axel Sikora

Kurzbeschreibung:

Der Trend hin zu fortschreitender Digitalisierung industrieller Produktionsanlagen bringt neue technische Herausforderungen mit sich. Bislang isolierte Geräte werden zunehmend miteinander vernetzt, was dazu führt, dass das Gesamtsystem von außen angreifbar wird. Gängige Sicherheitskonzepte wie verschlüsselte drahtlose Kommunikation oder die Sicherstellung der Geräteintegrität spielen für KMU eine immer größere Rolle bei der Entwicklung von Hardware- und Softwarelösungen. Das derzeit primäre Ziel ist dabei die Integration von softwarebasierten Security-Algorithmen, die zur Ver- und Entschlüsselung der Nutzdaten innerhalb eines vernetzten Systems eingesetzt werden. Die einzelnen Geräte verfügen i.d.R. über einen nichtvolatilen Speicher, der vom Gerätehersteller während des Produktionsprozesses mit einem einzigartigen digitalen Schlüssel beschrieben wird. Eine andere Möglichkeit bieten sog. Physical Unclonable Functions (PUFs), Hardwarestrukturen, deren unkontrollierbare herstellungsbedingte Variationen als physikalischer kryptografischer Schlüsselspeicher genutzt werden. Ein entscheidender Vorteil von PUFs ist deren Unvorhersagbarkeit der Schlüssel, da die resultierende Bitfolge auf den einzigartigen Merkmalen jeder einzelnen Geräteinstanz beruht. Darüber hinaus entfällt der Schritt der Speicherinitialisierung mit dem einzigartigen Schlüssel durch den Gerätehersteller, wodurch ein weiterer potentieller Angriffspunkt eliminiert werden kann. Ziel dieses Forschungsprojekts ist es, einen integrierten PUF-Baustein zu entwickeln und dieses KMUs zur Verfügung zu stellen. KMUs können diesen PUF-Baustein in ihre Hardwaredesigns integrieren und so vom höheren Sicherheitsstandard profitieren.

Nutzen:

- Die Firmware in Geräten kann durch Angreifer nicht ausgelesen / kopiert werden
- Geräte-IDs können nicht gefälscht werden, Rückverfolgbarkeit des einzelnen Teils ist gegeben
- Es entstehen keine Zusatzkosten durch spezialisierte Krypto-Bausteine