

Thema: Prozesse und Kommunikationsprotokolle für ein Security Lifecycle Management in industriellen Feldbusgeräten und -systemen (FieldPKI)



Fördernummer: BMWK/IGF-Nr. 21752 N

Laufzeit: 01.04.2021 – 31.03.2023

Schwerpunkte DFAM: Produktinnovation, Produktqualität, IT-Security & Vernetzung

Forschungseinrichtung:

- Hochschule Offenburg, Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK), Prof. Dr.-Ing. Axel Sikora
- Fraunhofer Institut für Integrierte Schaltungen (IIS), Nürnberg, Prof. Dr.-Ing. Albert Heuberger

Kurzbeschreibung:

Durch die zunehmende Vernetzung der industriellen Automatisierungstechnik sowohl bei Anlagensteuerungen als auch mit Produktionsplanungssystemen und externen Kommunikationspartnern sind ähnliche Schutzmaßnahmen gegen Angriffe wie bei gängigen Internetanwendungen erforderlich. Eine zentrale Rolle für die Schutzziele Authentisierung und Identifizierung spielt dabei eine Public Key Infrastructure (PKI). Im Projekt werden Kommunikationsarchitekturen unter Nutzung einer PKI und von Software- und Hardwaremodulen beschrieben, die für Entwicklung und Betrieb industrieller Automatisierungs- und Kommunikationslösungen benötigt werden.

Lösungsweg: In einer optimierten PKI lassen sich z.B. mit dem Transport Layer Security (TLS) Protokolls auch über Feldbusse sichere Ende-zu-Ende-Tunnel aufbauen, die durch kryptographische Methoden vor unberechtigtem Mitlesen (Vertraulichkeit) und Manipulation (Authentizität und Integrität) geschützt werden. Nach einer ausführlichen Konzeptions- und Architekturphase erfolgt eine beispielhafte Umsetzung. Dabei werden nicht nur die technischen Aspekte, sondern auch organisatorische Prozesse über den gesamten Lebenszyklus von Automatisierungskomponenten betrachtet.

Als Ergebnis dieses Forschungsprojekts werden eine Referenzarchitektur zum Schutz vor Angriffen auf die Feldbusebene, sowie Schlüsselkomponenten der optimierten PKI implementiert und quelloffen bereitstehen. Die Erkenntnisse werden auch in die aktuell laufenden Standardisierungsaktivitäten, z.B. bei PNO und CiA einfließen.

Nutzen:

Mit den Projektergebnissen werden die Hürden für eine Umsetzung und Vermarktung entsprechender Sicherheitsmechanismen in Produkten und Anlagen von KMU signifikant verringert. Die entstehenden Forschungsergebnisse können von Unternehmen der industriellen Automation verwertet werden, indem die entstandenen Ergebnisse direkt in ihrer Produktentwicklung oder als Vorlage für eine Eigenentwicklung genutzt werden