# PKI-basierte Sicherheitsarchitekturen – SecureField

**Vorhaben Nr. 19384 N**

## Durchgängige Integration von PKI-basierten Sicherheitsarchitekturen in die Feldebene von Industrie 4.0-Anwendungen

**Abschlussbericht**


**Kurzfassung:**

Die industrielle Kommunikation war früher von relativ eingeschränkten, geschlossenen Feldbussystemen geprägt. Mit der zunehmenden Öffnung von Automatisierungsnetzen durch die horizontale und vertikale Integration in Produktionsanlagen entstehen gefährliche Angriffsflächen, die zum Diebstahl von Produktionsgeheimnissen, der Manipulation oder dem kompletten Lahmlegen der Produktionsprozesse führen können. Hieraus ergeben sich grundlegend neue Anforderung an die Datensicherheit, denen mit innovativen Lösungsansätzen begegnet werden muss.

Ziel des Forschungsvorhabens „SecureField“ war es, die Umsetzbarkeit und Anwendbarkeit des Ansatzes *„(D)TLS-over-Anything“* zu untersuchen und nachzuweisen, sowie einen Werkzeugkasten zur Definition und Implementierung entsprechender Sicherheitslösungen vorzubereiten. Als langjährig etablierter Standard im IT-Umfeld stellte sich das (Datagram) Transport Layer Security ((D)TLS) Protokoll in Kombination mit einer industrie- bzw. automatisierungskompatiblen Public-Key-Infrastruktur (PKI) als äußerst vielversprechende Möglichkeit dar, Datensicherheit auch im OT-Umfeld zu erzielen. Hierbei sollten insbesondere KMU adressiert werden, für welche eigene Entwicklungsarbeiten in diesem Umfeld häufig zu aufwändig und technisch sowie wirtschaftlich zu riskant sind.

Mit „SecureField“ konnten Ergebnisse auf mehreren Ebenen erzielt werden. Zunächst konnte im Projektverlauf ein umfassendes und generisches Konzept zur Ende-zu-Ende-Absicherung von Kommunikationspfaden und -protokollen im industriellen Umfeld erarbeitet werden. Dieses Konzept besteht aus einem generischen Kommunikationsmodell sowie aus einem generischen Authentifikationsmodell.

- **Kommunikationsmodell:** Das Kommunikationsmodell ist die Basis des Ansatzes „*(D)TLS-over-Anything*“ und befasst sich mit der Abbildung einer (D)TLS-basierten Protokollschicht auf einen nahezu beliebigen Transportkanal. Zentrales Element hierbei ist eine parametrierbare Adaptionsschicht, die die Eigenschaften des Transportkanals, welche nicht im Einklang mit den Anforderungen von (D)TLS stehen, ausgleicht. Hierzu wird ein universelles Charakterisierungsmodell für den Transportkanal entwickelt und die jeweiligen Auswirkungen der Kanaleigenschaften auf die Adaptionsschicht beschrieben.
- **Authentifikationsmodell**: Das Authentifikationsmodell befasst sich mit der Authentifikation von Feldgeräten mithilfe einer Public-Key-Infrastruktur (PKI) aus einer Protokoll-, aber auch aus einer Prozesssicht. Es basiert auf zwei Identitätsebenen: die optionale, vom Gerätehersteller eingebrachte und kontrollierte Ebene der Herstellerzertifikate, sowie die vom Anlagenbetreiber eingebrachte und verwaltete Ebene der Betreiberzertifikate. Letztere wird als zwingend vorhanden angenommen, da diese der Absicherung der operativen Kommunikation dient. Das Authentifikationsmodell stellt die Ausgangsbasis für feldbusspezifische Spezifikationen und Implementierungen dar.

Weiterhin wurde im Rahmen der Arbeiten an „SecureField“ intensiv in den Standardisierungsgruppen verschiedener Feldbussysteme, insbesondere in der Security-Arbeitsgruppe (CB/PG10) der PROFIBUS Nutzerorganisation e. V. (PNO), mitgearbeitet. Hierbei fand ein

wertvoller Austausch in beide Richtungen statt: die Arbeiten an „SecureField“ konnten unmittelbar mit praxisnahen Anforderungen und Entwicklungen synchronisiert werden und die Forschungsstelle konnte wissenschaftlich-technische Erkenntnisse aus „SecureField“ unmittelbar in die Standardisierungsvorgänge einbringen. Neben PROFINET waren SafetyNET p und CANopen (FD) Gegenstand detaillierterer Betrachtungen.

Im Projektverlauf ist zudem eine Reihe von Softwareartefakten sowie Prototypen- und Demonstratoraufbauten entstanden, die eine Umsetzung des Ansatzes von „SecureField“ für SafetyNET p und CANopen FD leisten und eine gute Ausgangsbasis für weitere Entwicklungsarbeiten darstellen können.

Das Ziel des Forschungsvorhabens ist erreicht worden.

---


| | |
|---|---|
| Berichtsumfang: | 72 S., 34 Abb., 2 Tab., 36 Lit. |
| Laufzeit: | 01.03.2017 - 31.12.2019 |
| Zuschussgeber: | BMWi/IGF-Nr. 19384 N |
| Forschungsstelle(n): | Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK), Hochschule Offenburg<br>Leiter: Prof. Dr.-Ing. Axel Sikora |
| Bearbeiter und Verfasser: | Prof. Dr.-Ing. Axel Sikora (ivESK)<br>Artem Yushev. M.Sc. (ivESK)<br>Phuong Nguyen, M.Sc. (ivESK)<br>M.Tech Joseena Memadathil Jose (ivESK)<br>M.Tech Jubin Elayanithottathil (ivESK)<br>Laurent Hirth, M.Sc. (ivESK)<br>Dipl.-Phys. Andreas Walz (ivESK) |
| Vorsitzende(r) projektbegleitender Ausschuss: | Wolfgang Straßer (@-yet GmbH) |
| Vorsitzender Beirat: | Thomas Pilz (Pilz GmbH & Co. KG) |
| Weitere Berichte zum Forschungsvorhaben: | - |