

FieldPKI

Vorhaben Nr. 21752 N

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

Abschlussbericht

Kurzfassung:

Durch die zunehmende Vernetzung der industriellen Automatisierungstechnik sowohl bei Anlagensteuerungen als auch mit Produktionsplanungssystemen und externen Kommunikationspartnern sind ähnliche Schutzmaßnahmen gegen Angriffe auf die Automatisierungsnetze erforderlich, wie bei gängigen Internetanwendungen. Das Vorhandensein von kryptographischen Schlüsseln und Zertifikaten ist eine wichtige Voraussetzung zur Umsetzung von kryptographisch gesicherter Kommunikation auf der Feldebene. Eine zentrale Rolle zur Erstellung und Verwaltung von Zertifikaten spielt dabei eine Public Key Infrastructure (PKI). Mittels einer optimierten PKI und der Umsetzung der Zertifikatsbewirtschaftung auf den Feldbussen lassen sich z.B. mit dem Transport Layer Security (TLS) Protokolls auch auf Feldbussen sichere Ende-zu-Ende-Tunnel aufbauen, die durch kryptographische Methoden vor unberechtigtem Mitlesen (Vertraulichkeit) und Manipulation (Authentizität und Integrität) geschützt werden. Im Projekt wurden Kommunikationsarchitekturen unter Nutzung einer PKI und von Software- und Hardwaremodulen erarbeitet, die für die Entwicklung und den Betrieb industrieller Automatisierungs- und Kommunikationslösungen benötigt werden.

Nach einer ausführlichen Konzeptions- und Architekturphase erfolgte eine beispielhafte Umsetzung im Rahmen zweier Demonstratoren (CANopen und TSN). Dabei wurden nicht nur die technischen Aspekte, sondern auch organisatorische Prozesse über den gesamten Lebenszyklus von Automatisierungskomponenten betrachtet. Als Ergebnis dieses Forschungsprojekts wurde eine Referenzarchitektur zur Umsetzung eines Zertifikatsmanagements und dem Schutz vor Angriffen auf der Feldebene, sowie Schlüsselkomponenten der optimierten PKI implementiert und quelloffen bereitstehen. Die Erkenntnisse wurden auch im Rahmen der aktuell laufenden Standardisierungsaktivitäten, z.B. bei PNO und CiA vorgestellt.

Das Ziel des Vorhabens ist erreicht worden.

Laufzeit: 01.04.2021 – 31.03.2023

Fördergeber: Bundesministerium für Wirtschaft und Klimaschutz / Arbeitsgemeinschaft industrieller Forschungsvereinigungen e. V. (BMWK/AiF)

Fördernummer(n): IGF 21752 N

Forschungsstelle(n): Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK), Hochschule Offenburg (HSO)
Leiter: Prof. Dr.-Ing. Axel Sikora

Fraunhofer Gesellschaft e.V. Fraunhofer Institut für Integrierte Schaltungen (IIS)
Leiter: Prof. Dr.-Ing. Albert Heuberger

Bearbeiter und Verfasser: Prof. Dr.-Ing. Axel Sikora (ivESK)
Dipl.-Ing. Karlheinz Ronge (IIS)
Dipl.Phys. Andreas Walz (ivESK)
M.Sc. Julian Göppert (ivESK)
Dipl.-Ing. (FH) Andreas Oeder (IIS)
M.Sc. Anja Meldau (IIS)

Projektkoordination/projektbegleitender Ausschuss: Dipl.-Kfm. Wolfgang Straßer (@-yet GmbH) (Vorsitzender)

Vorsitzender wiss. Beirat: Dipl.-Kfm. Thomas Pilz (Pilz GmbH & Co. KG)

Danksagung

Dieser Bericht ist das wissenschaftliche Ergebnis einer Forschungsaufgabe, die von der Deutschen Forschungsgesellschaft für Automatisierung und Mikroelektronik (DFAM) e. V. gestellt und am Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) der Hochschule Offenburg (Instituts- und Projektleitung Prof. Dr. Ing. Axel Sikora und am Fraunhofer Institut für Integrierte Schaltungen IIS (Institutsleitung Prof. Dr.-Ing. Albert Heuberger, Projektleitung Dipl.-Ing. Karlheinz Ronge)bearbeitet wurde. Die DFAM dankt den Projektleitern und den wissenschaftlichen Bearbeitern Dipl.Phys. Andreas Walz (ivESK), M.Sc. Julian Göppert (ivESK), Dipl.-Ing. (FH) Andreas Oeder (IIS) M.Sc. Anja Meldau (IIS) für die Durchführung des Vorhabens sowie der Arbeitsgemeinschaft industrieller Forschungsvereinigungen (AiF) e. V. für die finanzielle Förderung. Das Vorhaben wurde von einem Arbeitskreis der DFAM unter der Leitung von Titel Wolfgang Straßer (@-yet GmbH) begleitet. Diesem projektbegleitenden Ausschuss gebührt unser Dank für die große Unterstützung. Insbesondere danken wir der Das Forschungsvorhaben wurde im Rahmen des Programms zur Förderung der industriellen Gemeinschaftsforschung (IGF-Nr. IGF 21752 N) vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) über die Arbeitsgemeinschaft industrieller Forschungsvereinigungen (AiF) e. V. aufgrund eines Beschlusses des Deutschen Bundestages gefördert.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

