Prof. Dr.-Ing. Hans-Peter Schmidt
Prof. Dr. Jürgen Mottok
Sebastian Renner, M.Sc.

Neue Entwicklungen, leichtgewichtige Kryptographie und Innovationen in der Industriellen Kommunikationstechnik

Zusammenfassung

Im Cluster Industrial Laboratory for Safe and Secure Systems (ILaS3) arbeiten beide Forschungsgruppen AUT und LaS3 der OTH Amberg-Weiden und Regensburg auf dem Gebiet Safety und Security in der Automatisierungstechnik zusammen. Der Schwerpunkt des LaS³-Teams in Regensburg liegt auf IT-sicheren und funktional sicheren software-intensiven Systemen, während die Arbeitsgruppe in Amberg auf dem Gebiet der industriellen Kommunikationstechnik F&E Projekte durchführt. Im Cluster wird gemeinsam untersucht, wie sich aktuelle Trends der Sicherheitstechnik und Security im industriellen Umfeld und Smart Home einsetzen lassen.

Mit dem Voranschreiten der Digitalisierung und der Vernetzung in verschiedenen Lebensbereichen ergeben sich neue Anforderungen an den Schutz der übertragenen Daten. Da in den Bereichen Smart Home und Industrie 4.0 sensible Daten über öffentliche Netze übertragen werden, müssen Maßnahmen zur Absicherung dieser Kommunikation getroffen werden. In solchen Internet of Things (IoT)- und Industrial IoT (IIoT)-Netzwerken kommen oft ressourcenschwache Geräte zum Einsatz, welche übliche Methoden und Algorithmen zur Verschlüsselung nicht ausreichend unterstützen. Dieser Artikel soll einen Überblick über alternative, besonders effiziente Algorithmen geben und den aktuellen Stand der Forschung zu dem Thema Leichtgewichtige Kryptographie darlegen. Daneben werden die aktuellen Trends in der industriellen Kommunikation im Industrie 4.0 Umfeld vorgestellt und Anknüpfungspunkte aufgezeigt.

Weiterhin wird ein am LaS³ der OTH Regensburg laufendes Forschungsprojekt vorgestellt, das sich mit der Evaluierung effizienter kryptographischer Primitive befasst. Die kostengünstige Anbindung industrieller Steuerungstechnik an IT Netze demonstriert eine Anwendung der Arbeitsgruppe AUT in Amberg, die als Basis für anlagenbezogene Test und Untersuchungen im Cluster eingesetzt werden kann.

Abstract

The research groups AUT and LaS³ from the OTH Amberg-Weiden and Regensburg work together on the topics IT security, safety and automation engineering within the cluster Industrial Laboratory for Safe and Secure Systems (ILaS3). The main focus of the LaS³ team lays on developing secure and safe software-intensive systems, while the researchers at AUT follow projects in the domain of industrial communications. The ILaS³ cluster pools resources and knowledge to investigate recent trends in the field of security research and engineering in smart home und industrial environments.

The ongoing digitalization and networking in different areas results in new requirements regarding the protection of the sent data. Smart home and connected industrial facilities are examples for fields in which sensitive data is communicated over public networks. In these IoT networks, one can often only use very resource-limited devices that are not supporting conventional methods and algorithms for encrypting data. This article wants to present an overview over alternative and especially efficient algorithms and show the current state of research in the area of Lightweight Cryptography. Moreover, a current research project which aims at evaluating efficient cryptographic ciphers is introduced and a cost-effictive application of industrial control systems within corporate IT networks is demonstrated.

1 Einleitung

Durch die Anbindung von immer mehr Geräten an öffentliche Netze ergibt sich ein steigender Bedarf an Methoden zur sicheren Kommunikation. Sowohl im privaten Bereich als auch in der Industrie ist die Vernetzung unterschiedlicher Geräte ein wichtiger Bestandteil der Digitalisierung.

Während in Haushalten vorwiegend Consumer-Komponenten mit dem Internet verbunden werden, spielt im industriellen Umfeld auch die Verbindung von Teilen der Produktion mit weiteren Netzwerken eine große Rolle.

Im industriellen Bereich ergeben sich gerade durch die Industrie 4.0 Paradigmen die Anforderungen, die reine Steuerungstechnik (engl. Operational Technology) mit der IT-Welt zu koppeln. In der Operational Technology (OT) liegt der Fokus auf einem abgeschlossenen System, und Security-Belange werden in der Regel an den Schnittstellen der OT-Domäne zur IT-Welt betrachtet. Durch die nahtlose vertikale Integration – also die durchgängige Kommunikation vom Sensor und Aktor bis in die Cloud – die von Industrie 4.0 Anwendungen gefordert wird – resultiert inhärent in einer Vermischung der IT- und OT-Welt.

In beiden Sparten steigt durch diese Entwicklung die Menge der übertragenen und besonders schützenswerten Daten. Je nach Einsatzzweck kann der Verlust der Integrität oder Vertraulichkeit sensibler Kommunikation schwerwiegende persönliche und wirtschaftliche Folgen haben. Besonders kritisch ist die Verletzung dieser Schutzziele in Bereichen, in denen durch Probleme der IT-Sicherheit auch Anforderungen an die funktionale Sicherheit nicht mehr erfüllt werden können. Die Erfüllung der Schutzziele der IT-Sicherheit wird durch die richtige Implementierung und Anwendung kryptographischer Methoden sichergestellt.

2 Aktuelle Trends in der industriellen Kommunikation

Sowohl bei physikalischen Aspekten der Übertragung als auch in höheren Protokollschichten gibt es umfangreiche Bestrebungen durch Standardisierung neue Technologien nun auch breit nutzbar zu machen.

2.1 Single Pair Ethernet und Advanced Physical Layer

In der industriellen Anwendung soll kostengünstige und bestehende Zwei-Draht-Verkabelung den Anschluss von einfachen Aktoren und Sensoren an die IT-Welt ermöglichen. Hierfür wurde nach mehrjähriger Standardisierungsarbeit von der Arbeitsgruppe 802.3cg bei der IEEE auch eine Variante für den industriellen Einsatz definiert: „10BASE-T1L“ [1]. Er sieht eine Datenrate von 10 Mb/s bei einer Länge der Zwei-Draht-Verkabelung von bis zu 1 km vor. Mit diesem Ethernet-Anschluss wird die Voraussetzung für eine nahtlose Integration von einfachen Sensoren und Aktoren in das IIoT geschaffen. Speziell für die Prozessautomatisierung wurde darüber hinaus der sogenannte Advanced Physical Layer definiert, bei dem die Energieversorgung des Sensors und Aktors für den Explosionsschutzbereich mit enthalten ist. Entwicklungen sind aktuell in der Umsetzung und Industrial Ethernet Standards wie PROFINET werden zurzeit so erweitert, dass diese neuen PHYs herstellerunabhängig in der Industrie eingesetzt werden können.

2.2 Time Sensitive Networks TSN

Ein weiterer wichtiger Meilenstein für die Industrie 4.0 Kommunikationsarchitektur ist die Einführung von TSN [8]. TSN ermöglicht Echtzeitverhalten im Standard Ethernet. Die umfangreichen Standardisierungs-Bestrebungen sind zum großen Teil abgeschlossen. Mit TSN fähigen Komponenten wird die bisherige Restriktion der Echtzeitfähigkeit auf Sensor- und Aktor-Ebene aufgehoben. Im Prinzip lassen sich vorhersagbare Zykluszeiten im gesamten Netz realisieren. Für PROFINET stehen den Mitgliedern bei der Nutzerorganisation bereits erste Tests für die Zertifizierung von PROFINEToverTSN-Geräten kostenfrei zur Verfügung [7]. Diese Tests werden maßgeblich von der Arbeitsgruppe AUT mit entwickelt.

Mit TSN ergeben sich auch neue Möglichkeiten für die Konvergenz von unterschiedlichen Netzwerkprotokollen. Diese werden im Rahmen des gemeinsamen Projekts der IEC und IEEE “IEC/IEEE 60802 TSN Profile for Industrial Automation” adressiert und legen den Grundstein für eine nahtlose Integration unterschiedlichster Dienste im Industrial Ethernet [3].

2.3 Open Platform Communications – Unified Architecture (OPC UA)

OPC UA hat sich zwischenzeitlich als Standard für die Kommunikation von Steuerung zu Steuerung etabliert. Auch die Anbindung von IT Services erfolgt zum Teil bereits über OPC UA. Security-Belange werden in dieser plattformunabhängigen Architektur von Anfang an mitberücksichtigt. In der Regel basieren die Anwendungen zurzeit auf dem Client-Server-Modell. Aktuell wird die Unterstützung des Pub-Sub-Modells sukzessive umgesetzt. Da bei OPC UA die Daten nicht nur übertragen werden, sondern auch semantisch in einem Informationsmodell beschreibbar sind, ist hier die Anknüpfung an eine übergeordnete Cloud und IT-Verarbeitung von vornherein gegeben. Eine Herausforderung stellt dabei jedoch die Modellierung der Anwendung und Abbildung in einem Informationsmodell dar. Während mit OPC UA die grundlegenden Dienste und die Infrastruktur definiert werden, ist das eigentliche Informationsmodell für eine Anwendung im “Companion Standard” hinterlegt.

Unterschiedlichste Sichtweisen auf ein und dieselbe physikalische Gegebenheit müssen hier für die Interoperabilität zusammengeführt sein. Besonders deutlich zeigt sich dies, wenn diese "Companion Standards" zum Teil branchen- oder anwendungsspezifisch erarbeitet wurden bzw. werden. Interoperabilität hängt hier vom gewählten "Companion Standard" und der tatsächlichen Implementierung ab.

Eine relativ neue Initiative ist OPC UA "Field Level Communication", bei der OPC UA bis auf das Sensor- und Aktoren-Niveau heruntergebrochen werden soll. Damit wird auch bei OPC UA die Datensicherheit für einfache Sensoren und Aktoren immer mehr zu einem entscheidenden Gesichtspunkt. Die OPC UA Spezifikation enthält dazu in Teil 2 der OPC-10000 eine ausführliche Modellierung einer Sicherheitsarchitektur [6]. Diese beschreibt detailliert mögliche Bedrohungen sowie nötige Schutzziele und deren Realisierung in unterschiedlichen Anwendungsfällen. Explizite Richtlinien zur Implementierung und Verwendung von bewährten kryptographischen Primitiven werden im Rahmen von OPC UA auch in dem Standard OPC-10000-7 diskutiert. Hier werden Profile für unterschiedliche Geräte-und Funktionsklassen definiert, die je nach Einsatzzweck bestimmte Anforderungen an die Datensicherheit erfüllen können müssen. Es wird genau festgelegt, welcher Algorithmus unter Berücksichtigung welcher Parameter verwendet werden soll.

3 Stand der Forschung & Standardisierung für Secure Systems

Die auch in OPC UA verwendeten Primitive sind über Jahrzehnte erprobte und standardisierte Algorithmen, welche bei richtiger Verwendung ein definiertes Sicherheitslevel erreichen. Ein Beispiel ist der Advanced Encryption Standard (AES), der im Jahr 2000 vom National Institute of Standards and Technology (NIST) der USA als Standard eingeführt wurde und bis heute verwendet wird. AES wurde weit vor den technischen Fortschritten im (I) IoT-Bereich und für damalig aktuelle Desktop-Systeme entwickelt. Mit der Internetanbindung diverser ressourcenschwacher Geräte ergeben sich neue Anforderungen an die verwendeten kryptographischen Algorithmen. Die zum Beispiel in Sensornetzwerken oder industriellen Steuerungsanlagen eingesetzte Hardware ist oft nicht geeignet für den Desktop-Bereich standardisierte Algorithmen ausreichend schnell auszuführen, dennoch ist eine Absicherung der von diesen Geräten ausgehenden Kommunikation notwendig.

Da durch die voranschreitende Vernetzung stetig mehr (ressourcenschwache) Geräte sensible Daten erfassen und kommunizieren müssen, sind neue effiziente Algorithmen nötig, die einerseits entsprechend geeignet für leistungsschwächere Hardware sind und dennoch ein definiertes Sicherheitsniveau erreichen.

Das NIST hat sich nach einer Evaluierungsphase der aktuellen Situation dazu entschieden, effiziente Algorithmen zur Verschlüsselung von Daten zu standardisieren, welche für den Einsatz in den zuvor genannten Anwendungsfällen besonders geeignet sind. Das NIST-Projekt zur Selektion leichtgewichtiger kryptographischer Algorithmen (NIST LWC) wurde 2018 gestartet [4]. Das NIST hat dazu einen "Call for Algorithms" veröffentlicht, in dem zur Einreichung von Algorithmen aufgerufen wird. Vorab wurden verschiedene Kriterien definiert, die ein optimaler Kandidat erfüllen sollte. Es wurden insgesamt 57 Primitive von unterschiedlichen Forscherteams aus der Wissenschaft und der Industrie eingereicht, von denen 56 von dem NIST zur 1. Runde des Evaluierungsprozesses zugelassen wurden. Jeder Kandidat wird in einem von den Entwicklern verfassten Dokument detailliert beschrieben, außerdem war die Abgabe mindestens einer Software-Referenzimplementierung verpflichtend. Verschiedene Experten aus dem akademischen und industriellen Bereich beteiligen sich an der Untersuchung der Algorithmen. Das verantwortliche NIST-Team forscht zudem parallel und kann so seine Entscheidungen auf viele unterschiedliche Arbeitsergebnisse stützen. Aktuell befindet sich das LWC-Projekt in der 2. Runde. Von den 56 ursprünglichen Kandidaten wurden seitens NIST 32 als Zweitrundenkandidaten ausgewählt. Planmäßig wird der Pool an Algorithmen im Dezember 2020 weiter auf ca. acht Primitive reduziert. Diese Finalisten sollen dann wieder für ein weiteres Jahr evaluiert werden, bevor voraussichtlich nur ein Kandidat ausgewählt und anschließend in einem Federal Information Processing Standard (FIPS) standardisiert werden soll.

4 Beispiel Implementierungen im Cluster ILAS3

4.1 Untersuchungen an realitätsnahen Anlagen „OPC UA als universelle Schnittstelle zur IT-Welt"

Für Untersuchungen an realitätsnahen Anlagen wurde ein Industrie 4.0 Demonstrator in der Arbeitsgruppe AUT aufgebaut, der auch für Security Tests eingesetzt werden kann [2]. Er besteht aus zehn Zellen, die mit unterschiedlicher Funktionalität bestückt werden können und durch zwei kooperative Roboterzellen ergänzt werden. Jede Zelle beinhaltet als Kern industrielle Steuerungstechnik (Siemens S7 1500., IO-Link, etc.), die durch verschiedene Module erweitert werden kann.

Hier wird zur einheitlichen Kommunikation jede Zelle zusätzlich mit einem OPC UA-fähigen EDGE Gateway ausgestattet. Als Gateway wurde der frei programmierbare Einplatinencomputer "Raspberry Pi" gewählt. Auf diesem "Raspberry Pi" wurde OPC UA mithilfe des Open Source Stacks "open62541" neben verschiedenen anderen Anwendungen integriert. Der "Raspberry Pi" wurde gewählt, da sowohl Stacks für OPC UA als auch für PROFINET zur

Verfügung stehen und somit eine nahtlose frei programmierbare Kopplung zwischen Industrial Ethernet und OPC UA möglich ist [5]. Mit solchen OPC UA-fähigen Raspberry Pis werden auch industrielle Bildverarbeitung und andere Sensorik realisiert.

Über das EDGE Gateway wird ein digitaler Zwilling mit der tatsächlichen Anlage verknüpft und ermöglicht das Bedienen und Beobachten sowie den auszugsweisen Austausch der Prozessdaten. Dieses Modell der Anlage dient der Nachbildung des Datenaustausches zwischen OT- und IT-Welt. Hervorzuheben ist, dass der digitale Zwilling sowohl PC-basiert ist als auch unter Android als App eingesetzt werden kann. Zusätzlich kann mit der OPC UA-fähigen Sensorik auf Raspberry Pi Basis die Verknüpfung der IT-Welt mit dem einzelnen Sensor untersucht und somit auch die Implementierung des Sicherheitsmodells (siehe Abschnitt 2.3) zukünftig getestet und verifiziert werden.

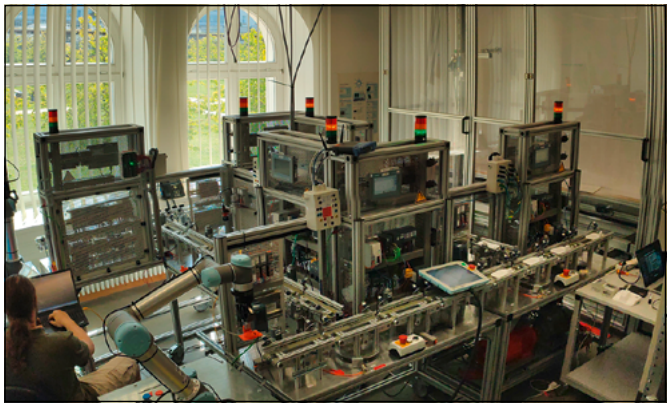

Abbildung 1: a) Demonstrator und digitaler Zwilling

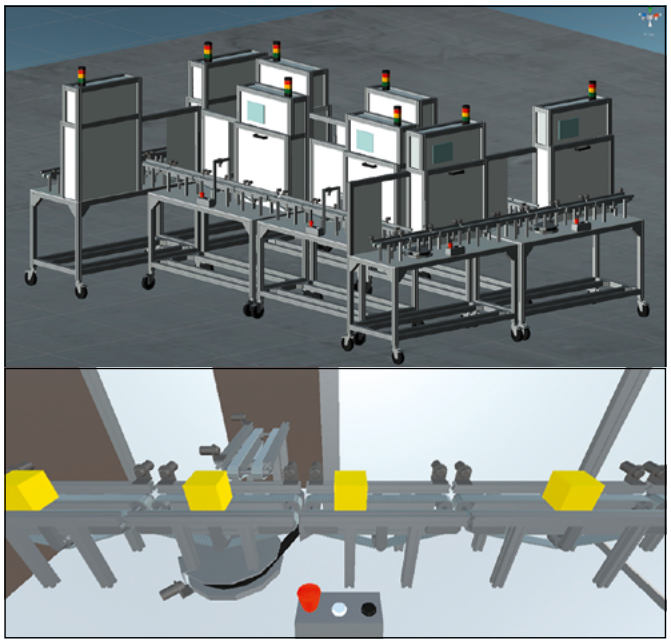

Abbildung 1: b) Digitaler Zwilling, Gesamtansicht und Detail

An dieser Testanlage wurde in einem ersten Schritt die Handhabung von OPC UA-Securitymechanismen betrachtet. Hier wurde sich auf die Implementierung im EDGE Gateway konzentriert. Auf der industriellen Steuerung (Siemens S7 1500) wurden der zur Verfügung stehende OPC UA Server des TIA-Portals eingesetzt. Eine eigene Betrachtung der Security-Handhabung erfolgte bei dieser kommerziellen Lösung noch nicht.

Bereits die Inbetriebnahme des Open Source Stacks – ohne jegliche Security Aspekte – erforderte detailliertes Know-how und ein solides OPC UA-Verständnis. Im Rahmen dieser ersten Betrachtungen konnten die OPC UA unterstützten Security-Maßnahmen noch nicht erfolgreich eingesetzt werden. Dies wird im weiteren Verlauf des Einsatzes von OPC UA weiterverfolgt.

4.2 Evaluierung Leichtgewichtiger Kryptographischer Algorithmen

Die Performanz der im Sicherheitsmodell definierten Primitive ist neben anderen Kriterien eine Metrik, die im Selektionsprozess eine wichtige Rolle spielt. Dabei werden Hard- und Software-Implementierungen in unterschiedlichen Anwendungsfällen betrachtet. Am LaS³ der OTH Regensburg wurde ein Benchmarking Framework mit dem Ziel entwickelt, die Performanz der NIST LWC Software-Implementierungen auf verschiedenen Microcontroller-Plattformen zu messen. Dazu wurde ein modularer Hardware-in-the-Loop (HIL)-Ansatz verfolgt, bei dem gleiche Testroutinen auf verschiedener Hardware ablaufen können. Mithilfe des Frameworks lassen sich wichtige Metriken zur Beurteilung der Software-Performanz messen, außerdem wird sichergestellt, dass die getesteten Implementierungen ordnungsgemäß und wie spezifiziert funktionieren.

Im Moment werden drei verschiedene Testfälle unterstützt. In der ersten Variante werden die vom NIST definierten Testvektoren als Input/Output-Test an die mit der Software-Implementierung bestückten Testhardware gesendet, das Framework misst dabei die Dauer jedes Entschlüsselungs- bzw. Verschlüsselungsvorgangs.
Die Daten zum Hostcomputer werden über eine serielle Schnittstelle übertragen. Die Verarbeitungszeit der Algorithmen wird über hardwaregesteuerte Signale direkt auf dem Testobjekt gemessen, somit werden Messungenauigkeiten aufgrund von Latenzen auf der seriellen Leitung ausgeschlossen. Anhand der gesammelten Daten kann am Ende des Testfalls eine Aussage über die durchschnittliche Geschwindigkeit des Algorithmus getroffen werden. Weitere getestete Metriken sind die Größe der (kompilierten) Implementierung (ROM-Nutzung) und der Speicherverbrauch (RAM-Nutzung). Die Tests finden in einer hochautomatisierten Umgebung statt, womit der manuelle Arbeitsaufwand und die Menge potenzieller Messfehler durch gesteuerte Falscheingaben minimiert wird. Die Experimente werden mittels Logdateien dokumentiert, zudem werden alle getesteten Implemen-

tierungen in einem öffentlich zugänglichen Repository zur Verfügung gestellt. Weiterhin wird im Rahmen des Projekts eine Webseite betrieben, die alle im Laufe des NIST LWC Projekts gewonnenen Erkenntnisse sowie alle Testergebnisse widerspiegelt. Zum aktuellen Zeitpunkt wurden bereits mehr als 300 verschiedene Varianten der LWC-Kandidaten der 2. Runde getestet und die korrespondierenden Ergebnisse online zur Verfügung gestellt.

5 Zusammenfassung und Zukünftige Arbeiten

Mit der Evaluierung der Software-Implementierungen der NIST LWC-Kandidaten liefert das LaS³ für den allgemeinen Selektionsprozess relevante Testergebnisse. Dadurch, dass alle Testdaten öffentlich verfügbar sind und während der gesamten Dauer des Wettbewerbs aktuell gehalten werden, wird versucht, eine größtmögliche Transparenz zu schaffen. Abgesehen von dem Ausbau der unterstützten Testfälle und -plattformen soll das Framework in Zukunft so erweitert werden, dass die Erstellung und Aufnahme von Stromverbrauchsprofilen der jeweiligen Kandidaten möglich wird. Insbesondere für sogenannte Seitenkanalangriffe und zum Überprüfen von bestimmten Härtungsmaßnahmen sind diese Daten hilfreich. Weiterhin soll in diesem Zusammenhang das Spannungsfeld zwischen maximaler Performanz und maximalem Schutz gegenüber Angriffen auf die Implementierung erforscht werden.

Mit dem Industrie 4.0 Demonstrator der OTH Amberg-Weiden stehen zudem im Cluster auch realitätsnahe Testmöglichkeiten zur Verfügung, bei denen nicht nur das einzelne Gerät, sondern die gesamte Automatisierungsanlage als Untersuchungsobjekt eingesetzt werden kann. Hier können abhängig von der vorgegebenen Automatisierungsaufgabe die Handhabung und Wirksamkeit von Security-Implementierungen auf Anlagenebene betrachtet werden.

Im Cluster sollen nun im nächsten Schritt, parallel zu den Handling Tests, auch Security-Szenarien für OPC UA anhand der Anlage untersucht werden. Dazu muss zunächst eine Implementierung und Inbetriebnahme der im OPC-10000-2/7 definierten Security-Komponenten erfolgen. Weiterhin ist es denkbar, die empfohlenen kryptographischen Algorithmen des Sicherheitsmodells gegen geeignete leichtgewichtige Primitive zu ersetzen. Anschließend könnte die konventionelle mit der neuen Implementierung verglichen werden, um Aussagen über die Performanz und die Resistenz gegenüber einfachen Angriffen zu treffen.

Referenzen:

[1] IEEE: IEEE 802.3cg-2019 – IEEE Standard for Ethernet – Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors. Online verfügbar: https://standards.ieee.org/standard/802_3cg-2019.html [Zugegriffen am 26.10.2020]

[2] Demonstrator der Arbeitsgruppe AUT (Automation) OTH Amberg-Weiden. Online verfügbar: www.aut-oth.de [Zugegriffen am 26.10.2020]

[3] IEC/IEEE: IEC/IEEE 60802 TSN Profile for Industrial Automation. Online verfügbar: https://1.ieee802.org/tsn/iec-ieee-60802/ [Zugegriffen am 26.10.2020]

[4] National Institute for Standards and Technology: Lightweight Cryptography Project. Online verfügbar: https://csrc.nist.gov/Projects/lightweight-cryptography [Zugegriffen am 26.10.2020]

[5] Open Source C Implementation of OPC UA. Online verfügbar: https://open62541.org/ [Zugegriffen am 26.10.2020]

[6] OPC Foundation: Open Platform Communications - Unified Architecture. Online verfügbar: https://opcfoundation.org/ [Zugegriffen am 26.10.2020]

[7] PROFIBUS Nutzerorganisation: PROFINET over TSN. Online verfügbar: https://de.profibus.com/downloads/profinettsn-trial-test-bundle/ [Zugegriffen am 26.10.2020]

[8] IEEE: Time-Sensitive Networking (TSN) Task Group. Online verfügbar: https://1.ieee802.org/tsn/ [Zugegriffen am 26.10.2020]

Prof. Dr.-Ing. Hans-Peter Schmidt

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik,
Medien und Informatik
Kaiser-Wilhelm-Ring 23
92224 Amberg

hp.schmidt@oth-aw.de

Prof. Dr. Jürgen Mottok

Ostbayerische Technische
Hochschule (OTH) Regensburg
Fakultät Elektro- und
Informationstechnik
Seybothstraße 2
93053 Regensburg

juergen.mottok@othr.de

Sebastian Renner, M.Sc.

Ostbayerische Technische
Hochschule (OTH) Regensburg
Fakultät Elektro- und
Informationstechnik
Seybothstraße 2
93053 Regensburg

sebastian1.renner@othr.de