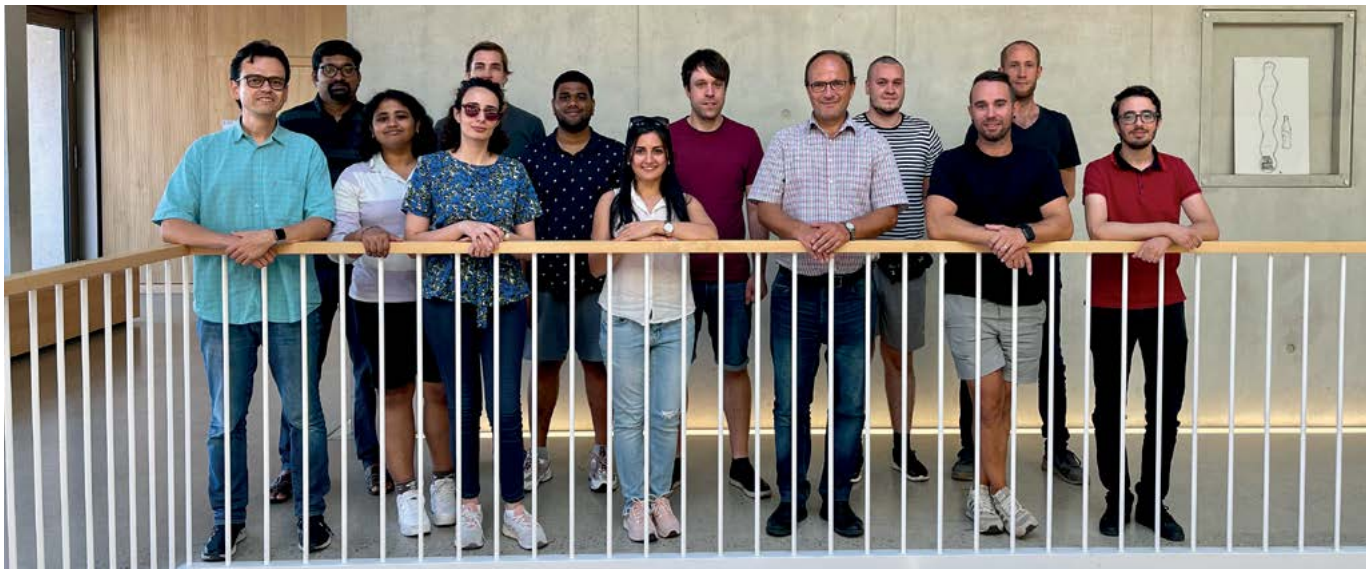
forschung im fokus

Hochschule Offenburg
offenburg.university

2023

INSTITUT FÜR VERLÄSSLICHE EMBEDDED SYSTEMS UND KOMMUNIKATIONSELEKTRONIK [ivESK]



Prof. Dr. Sikora umringt von seinem internationalen ivESK-Team.

Das „Internet der Dinge“ (Internet of Things, IoT) durchdringt industrielle und persönliche Anwendungen zunehmend. Hierzu zählen auch Smart-Metering und Smart-Grid, Industrie- und Prozessautomation, Car-to-Car, beziehungsweise Car-toX-Kommunikation, Heim- und Gebäudeautomation, Telehealth- und Telecare-Anwendungen, drahtgebundene und drahtlose Vernetzung von Embedded Systemen. Ihre Anbindung als sogenannte cyberphysische Systems (CPS) spielen hierbei eine immer wichtigere Rolle. Da auch immer mehr Systeme funktionskritische Aufgaben autonom übernehmen, gewinnen Zuverlässigkeit und Sicherheit mehr an Bedeutung. Entsprechend müssen die Aspekte der Datensicherheit (Security) und der Privatsphäre (Privacy) von Anfang berücksichtigt werden. Besondere Themenschwerpunkte sind zellulare Mobilfunknetze (5G/5.xG/6G) und echtzeitfähige Kommunikationstechnologien insbesondere unter Nutzung der Ansätze des Time Sensitive Networking (TSN), die neben der eigentlichen Entwicklung auch systematischen Tests und Analysen unterzogen werden müssen, wie der Bericht von Fabian Sowieja zeigt (Seite 107). Zudem sind die folgendend vorgestellten Themenkreise der Protokollabsicherung insbesondere von industriellen Netzwerken (Seite 103) oder im Bereich des Smart Meterings (Seite 98) von hoher Bedeutung.

Das Institut ivESK wurde im Herbst 2015 von Prof. Dr. Axel Sikora und Prof. Dr. Dirk Westhoff gegründet und hat sich seither außerordentlich positiv entwickelt. Seit Herbst 2020 ist Prof. Dr. Andreas Schaad Teil des Teams. Es werden pro Jahr etwa 20 FuE-Projekte oft in enger Kooperation mit Unternehmen und anderen Forschungseinrichtungen bearbeitet, um das Internet der Dinge effizienter, zuverlässiger und verlässlicher zu machen.

Am Institut arbeiten gegenwärtig 15 Vollzeitmitarbeitende sowie etwa ebenso viele Studierende in einem sehr internationalen, hoch motivierten und lebendigen Team. Regelmäßig sind Gastwissenschaftler aus der ganzen Welt vor Ort, um neue Themen zu erschließen. Aufgrund der weiterhin sehr positiven Projektlage sind fast immer einige Projekt- und Promotionsstellen verfügbar. Kandidaten für Tutorentätigkeiten und Abschlussarbeiten sind ebenso gern gesehen. Promotionen können über die Assoziierung von Prof. Dr. Axel Sikora an der Technische Fakultät der Universität Freiburg unmittelbar betreut werden.

Institutsleitung
Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing. Axel Sikora

„Smart Meter Inclusif"

Sicherheit für intelligente Zähler

Die europäische Energievision 2030 strebt ein sicheres, nachhaltiges und wettbewerbsfähiges Energiesystem durch den Einsatz von Smart-Grid-Technologien an, um die Effizienz zu verbessern, erneuerbare Energien zu integrieren und die Widerstandsfähigkeit zu erhöhen. Verteilte Smart Grids erfordern robuste Sicherheit zum Schutz vor Cyberangriffen, unbefugtem Zugriff und Datenschutzverletzungen, um die Privatsphäre und kritische Infrastrukturen zu wahren. Um diese Aspekte des Interreg-Projekts „Smart Meter Inclusif" (SMI) abzudecken, beschäftigte sich das ivESK im Arbeitspaket „Sicherheitskonzepte für verteilte Smart Grids" mit einer vergleichenden Sicherheitsanalyse und mit Penetrationstests für intelligente Zähler.

The 2030 European energy vision seeks a secure, sustainable, and competitive energy system through the deployment of smart grid technologies to improve efficiency, integrate renewables, and enhance resilience. Distributed smart grids require robust security to protect against cyber-attacks, unauthorized access, and data breaches, preserving privacy and critical infrastructure.To cover these aspects of the Interreg project „Smart Meter Inclusif" (SMI), the ivESK team executed the work package „Security concepts for distributed Smart Grids" and performed a comparative security analysis and Smart Meters penetration testing.

Axel Sikora
Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing.

Fakultät EMI, Wissenschaftliche Leitung ivESK Kommunikationsnetze, Bussysteme und Schnittstellen, eingebettete / industrielle Netzwerke, Intelligente Energienetzwerke

Ivan Rigoev
M.Sc.

Institut ivESK
Akademischer Mitarbeiter

Andreas Walz
Dipl.-Phys.

Institut ivESK
Akademischer Mitarbeiter

Das SMI-Projekt

Die Literatur im Umfeld der Sicherheit intelligenter Messungsinfrastrukturen [1]–[3] zeigt klar, dass im Moment nicht alle Sicherheitsbedrohungen abgedeckt werden. Um die Situation im Bereich des Smart-Metering als Teil des Interreg-Projekts SMI „Smart Meter Inclusif" [6] besser zu verstehen, implementierte ivESK das Arbeitspaket „Sicherheitskonzepte für verteilte Smart Grids", das eine vergleichende Sicherheitsanalyse und Penetrationstests umfasst.

Vergleichende Sicherheitsanalyse

In den letzten Jahren wurden immer mehr Smart-Metering-Systeme installiert. Vor diesem Hintergrund ist es von entscheidender Bedeutung, ihre Funktionen in Bezug auf Vertraulichkeit und Sicherheit der Benutzerdaten zu bewerten.

Um den aktuellen Stand der französischen, deutschen und schweizerischen Smart-Metering-Systeme besser zu verstehen, wird in dem SM-Projekt eine vergleichende Sicherheitsanalyse durchgeführt. In Frankreich ist der Datenschutz seit 1978 gesetzlich genau definiert, aber die technischen Anforderungen an intelligente Messsysteme sind im Vergleich zu denen in Deutschland und der Schweiz deutlich allgemeiner beschrieben. Allerdings ist der französische Markt mit einer dominanten Rolle von Enedis deutlich homogener, sodass dies in der Praxis kein großes Problem darstellt. Enedis hat ein umfassendes System mit vielen nützlichen Smart-Metering-Funktionen geschaffen. Entsprechend wurde hier das Linky-System als einzige französische Lösung betrachtet. Der Enedis-Dokumentation fehlen jedoch technische Informationen, da die meisten Funktionen nur in Marketingmaterialien beschrieben werden und nur begrenzte Informationen von Enedis-Sprechern bei Projekttreffen erhalten werden konnten. Die Sicherheitsmechanismen im Linky-System, wie Authentifizierung und Verschlüsselung, basieren auf dem DLMS/COSEM-Protokoll für die „Device Language Message Specification and Companion Specification for Energy Metering", wie es in den „Colored books" beschrieben ist [5].

Im Gegensatz dazu verfügt Deutschland über ein vom BSI geschaffenes transparentes und umfassendes Dokumentationssystem, das die Architektur, Protokolle, Zugriffsrechte und weitere Anforderungen an die Smart-Metering-Infrastruktur vollständig beschreibt. Alle Unterlagen sind auf der Website des BSI verfügbar. Deutschland hat jedoch einen langen Prozess zur Entwicklung dieser Anforderungen und Dokumentationen.

Swiss hat geringe aufsichtsrechtliche Restriktionen in Bezug auf Architektur und verwendete Protokolle, was zu einer erhöhten Wahrscheinlichkeit von Schwachstellen führen kann. Die Verwendung mehrerer Protokolle und Gerätevarianten bedeutet jedoch auch, dass eine in einem System wie Landis+Gyr gefundene Schwachstelle nicht unbedingt bedeutet, dass andere Systeme die gleichen Probleme haben. Um konkreter zu werden, betrachtete man in diesem Zusammenhang bei der Recherche Landis+Gyr E450 Smart Meter mit DC450 Datenkonzentrator und Siemens IM150 Smart Meter mit SGW1050 als Schweizer Referenzsysteme.

Die Architektur von French Linky und die Schweizer Lösungen von Landis+Gyr und Siemens sind aus Sicht der Smart-Metering-Architektur ähnlich. Beide verwenden den DLMS/COSEM-Protokollstapel und üblicherweise Power Line Communication (PLC) auf der physischen Schicht. Ein Datenkonzentrator ergänzt ihre Architektur.

Das DLMS/COSEM-Protokoll basiert auf einer Client-Server-Architektur, um Verbrauchsdaten von intelligenten Zählern abzurufen und an das Meter Data Management System eines Energieversorgers zu übertragen. Es weist Schwachstellen wie optionale Authentifizierung, Informationslecks, schwache Authentifizierungsmethoden, Offline-Wörterbuchangriffe und Sicherheitsherabstufung auf. DLMS/COSEM-Implementierungen können auch Probleme aufweisen, wie beispielsweise schlechter Schutz vor Wiederholungsangriffen, vorhersagbare Authentifizierung, identische Systemtitel, nicht authentifizierte verschlüsselte Nachrichten und unsichere Authentifizierung.

IDIS ist eine „Interoperable Device Interface Specification", die definiert, wie DLMS/COSEM-Standards implementiert werden sollten, um die Interoperabilität zwischen intelligenten Zählern verschiedener Anbieter zu ermöglichen. Die IDIS-Sicherheitsspezifikation erfordert HLS für die Authentifizierung, AES-Verschlüsselung mit einem 128-Bit-Schlüssel und eine 4-stufige Client-Server-Authentifizierung mit GMAC, was bedeutet, dass alle oben beschriebenen Schwachstellen abgedeckt sein sollten, falls IDIS implementiert wird. Das IDIS White Paper [4] weist darauf hin, dass die betrachteten Schweizer Systeme und der französische Linky die IDIS-Spezifikationen erfüllen.

Im Unterschied zu den in dieser Arbeit betrachteten französischen und schweizerischen Systemen basiert das deutsche BSI-System auf dem TLS1.2-Protokoll. Im Fall von DLMS/COSEM-basierten Systemen implementiert der intelligente Zähler üblicherweise die Server-Rolle und das Head-End-System implementiert die Client-Rolle. Im Fall des deutschen SMGW-Systems ist diese Kommunikation viel komplizierter. Das zentrale Element des durch BSI-TR-03109 definierten deutschen Smart-Metering-Systems ist das SMGW (Smart Meter Gateway), das Verbindungen zwischen drei verschiedenen Netzwerken verwaltet: dem LMN (Local Metrological Network), wo SMGW Verbrauchsdaten von Strom-, Gas-, Wasser- und Wärmezählern gespeichert und verarbeitet werden, dem HAN (Home Area Network), in dem über das SMGW mit steuerbaren lokalen Systemen (Appliances) kommuniziert wird und dem WAN (Wide Area Network), das verwendet wird, um Daten für externe Marktteilnehmer bereitzustellen.

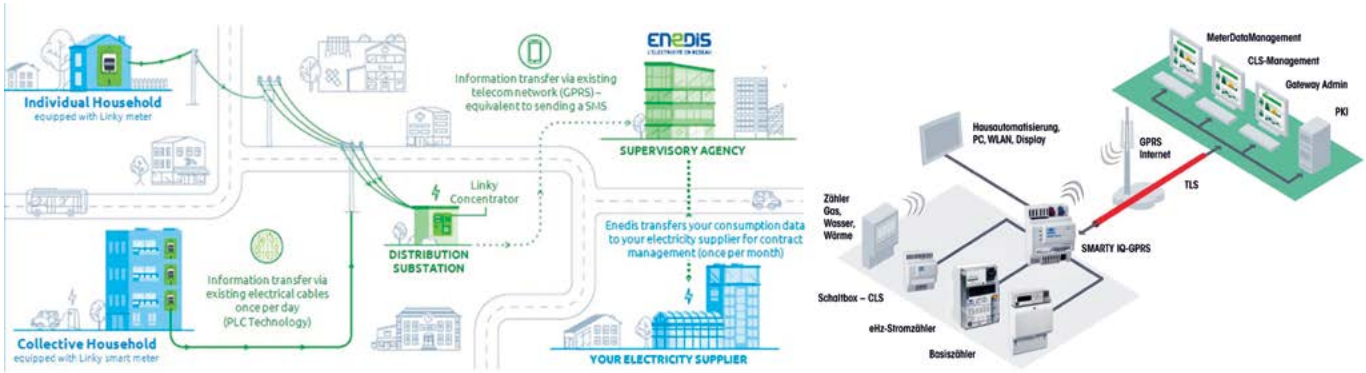


Abb. 1:
Enedis DSO und dt. SMGW SMARTY IQ-LTE-Architekturvergleich

Der SMGW-Administrator ist der Hauptakteur im deutschen SMGW-System und verantwortlich für die Geräte- und Clientverwaltung, die Profil-, Schlüssel- und Zertifikatsverwaltung, die Überwachung und Steuerung des SMGW und die Konfiguration des Weckdienstes. SMGW-Administratoren haben exklusiven Zugriff, um Zugangskontrollprofile zu installieren und zu ändern, die bestimmen, welche Daten an welche externen Marktteilnehmer gesendet werden sollen. Das wichtigste Sicherheitsmerkmal von SMGW ist der Weckdienst. SMGW sollte nicht auf eingehende Verbindungen reagieren, mit Ausnahme des speziellen Aktivierungspakets, und für die gesamte WAN-Kommunikation die Rolle des TLS-Clients implementieren.

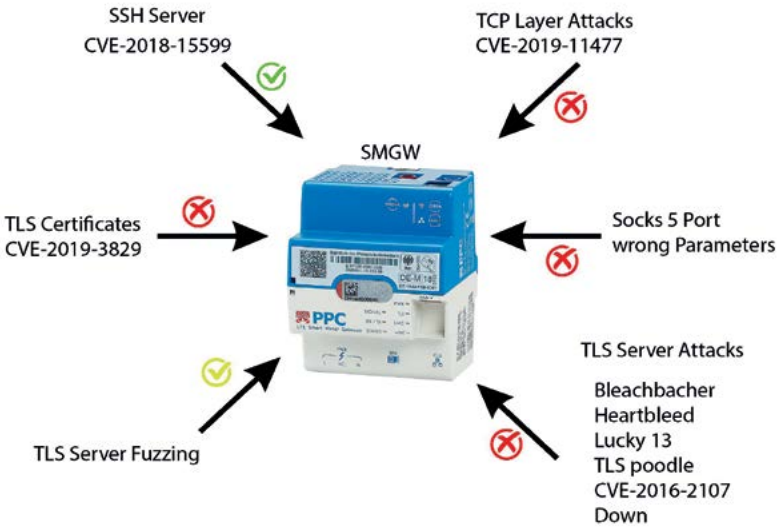


Abb. 2: getestete Angriffsrichtungen

DLMS/COSEM und TLS (mit BSI-Anforderungen) sind in Bezug auf Sicherheitsniveaus, PKI, moderne Sicherheitsprimitive und Cipher Suites vergleichbar. Der Unterschied zwischen ihnen besteht darin, dass TLS komplexer und flexibler ist und ein einfaches Hinzufügen oder Entfernen von Sicherheitsfunktionen ermöglicht. TLS ist weit verbreitet und es wurden mehr Untersuchungen und Tests durchgeführt, was zu mehr bekannten Schwachstellen führte, die bereits abgedeckt sind. Andererseits ist DLMS/COSEM weniger komplex, was eine Implementierung auf eingebettete Systeme leichter macht. Das BSI fordert vom SMGW die Verwendung von TLS mit einer staatlich kontrollierten Root-CA und spezifischen Mechanismen zur Generierung von Zufallszahlen. Alle Schlüssel und Zertifikate werden in einem BSI-CC-zertifizierten Hardware-Sicherheitsmodul gespeichert. Die DLMS/COSEM-Spezifikation erfordert nur die Verwendung eines „starken Zufallszahlengenerators".

Smart-Meter-Penetrationstest

Während der Implementierung des Smart-Meter-Penetrationstest-Projektteils wurden mehrere Geräte getestet, aber der größte Aufwand konzentrierte sich auf die Tests des deutschen SMGW. Um ein echtes SMGW-Gerät zu erwerben, ist eine Registrierung als Anlagenbetreiber auf der Website der BNetzA erforderlich. Danach erhält man vom E-Werk Mittelbaden die Genehmigung, zwei SMGW-Geräte CONEXA 3.0 und Smart Meter Gateway PPC LTE zu testen. Zu den Testbeschränkungen gehört, dass die SMGW-Admin- und EMP-Infrastruktur nicht getestet wird und die Geräte nicht physisch beschädigt werden. Zudem erhält man Benutzeranmeldeinformationen für die Verbrauchswebseite. Der Test wurde aufgrund des fehlenden Zugriffs auf die Geräte-Shell oder Firmware als „Black Box" durchgeführt.

Die Tests konzentrierten sich aufgrund der bequemeren Kommunikation über Ethernet hauptsächlich auf HAN-Angriffe. Es wird vermutet, dass die Implementierung von TLS in allen drei SMGW-Netzwerken ähnlich ist. Ebenso wird erwartet, dass TCP-Layer-Angriffe aufgrund der gemeinsamen Implementierung des TCP-Stacks auf Kernel-Ebene ähnliche Auswirkungen haben. Der Nmap-Scanner zeigt nur zwei offene Ports auf dem Conexa SMGW HAN: TLS-Server auf Port und Port 1080 (socks) für HKS3. Im Fall von PPC fand SMGW den TLS-Server, den Nmap als Lighttpd identifiziert, Dropbear sshd 2017.75.

Die Priorität bestand darin, den SSH-Server zu testen, der auf dem PPC SMGW gefunden wurde, da der Zugriff auch im Nicht-Root-Modus das Testen viel effektiver macht. Die Passwortauthentifizierung wurde aktiviert, aber das Projekt hat keinen Benutzer, für den der Datenverkehr abgefangen werden kann. Die einzige Möglichkeit, eine SSH-Shell zu erhalten, ist Brute Force. Die Dropbear SSH Version 2017.75 ist anfällig für CVE-2018-15599 wegen der Schwachstelle bei der Benutzeraufzählung, die die Brute-Force-Geschwindigkeit durch Abrufen der Benutzernamenliste erhöht. Zum Testen einer SSH-Schwachstelle wurde das Metasploit-Modul ssh_enumusers mit der Option „Malformed Packet Attack" verwendet, das erfolgreich Benutzer auf einem Raspberry Pi-Prüfstand und einem PPC-SMGW aufzählte. Leider stellt die resultierende Benutzerliste keine Informationen über das verwendete Betriebssystem zur Ver-

fügung. Der nächste Schritt beim Brute-Forcing ist das Finden von Passwörtern für gefundene Benutzernamen. Es wurde noch kein Passwort gefunden, wahrscheinlich weil das Passwort nicht im Wörterbuch steht oder die Brute-Force-Geschwindigkeit zu gering ist. Es gibt bekannte Schwachstellen in Dropbear 2017.75, aber keine davon umgeht die Authentifizierung oder führt zur Remote-Code-Ausführung.

Die effektivste Methode zum Testen von SMGW sind TCP-Layer-Angriffe, da der TCP/IP-Stack im Kernel des Linux-basierten Systems integriert ist. Beispiele für Angriffe auf TCP-Schicht sind die TCP/IP-Implementierung von CVE-2019-11815 Remote Code Execution in der Linux-Kernel-Implementierung und die Remote-DoS-in-TCP/IP-Implementierung im Linux-Kernel (CVE-2019-11477, CVE-2019-11478, und CVE-2019-11479). Wenn die HAN-Schnittstelle für einen TCP-Layer-Angriff anfällig ist, sind LMN und WAN aufgrund der Kernel-Integration wahrscheinlich ebenfalls anfällig. Obwohl es keine öffentlich verfügbaren Exploits für die CVEs gibt, ist es aus Sicherheitssicht gut, dass nur ein Exploit für CVE-2019-11477 gefunden wurde und auf den getesteten Systemen nicht richtig funktionierte.

Eine weitere Möglichkeit, das Conexa SMGW zu beeinflussen, besteht darin, seinen Socks5-Port zu öffnen, der für HKS3 erforderlich ist - ein transparenter Kommunikationskanal, der von CLS initiiert wird. Die Verbindung muss vor SOCKSv5 eine TLS-Verbindung mit der Authentifizierungsmethode 0x86 herstellen, wie dies im Entwurf RFC1928 Secure Sockets Layer für SOCKS Version 5 beschrieben ist. Der Socks5-Server von Conexa SMGW akzeptiert nur diese Methode und mehrere Verbindungsversuche führen nicht zu einem Denial-of-Service.

Bei den Geräten prüfte der TLS-Server zunächst die TLS-Parameter wie TLS-Version, Cipher Suites oder vom SMGW unterstützte Erweiterungen. Als nächstes wurden häufige TLS-Protokoll-Schwachstellen wie Bleichenbacher-Angriff, Heartbleed, lucky13, tls poodle, CVE-2016-2107, Drown und z geprüft. Alle Tests wurden von beiden SMGW erfolgreich bestanden.

Eine weitere Testmethode ist das TLS-Server-Fuzzing – eine Technik zur automatisierten Erkennung von Codefehlern. Der Fuzzer generiert Modifikationen an Variablen und analysiert das Laufzeitverhalten der TLS-Software. Beispielsweise kann der ursprüngliche ganzzahlige Wert mit zufälligen Bits XOR-verknüpft, nach links oder rechts verschoben und um einen zufälligen Wert erhöht oder verringert werden. Üblicherweise verwendet Fuzzing-Software wie TLS-Angreifer Address Sanitizer-Software, um einige Pufferüberläufe oder anderes falsches Verhalten zu finden, aber da auf dem Quellcode oder die Firmware der SMGW-Software nicht zugegriffen werden kann, wurde eine „Black-Box"-Testmethode verwendet. In diesem Fall verwendet TLS-Attacker bekannte TLS-Protokollflüsse und vergleicht sie mit der Testimplementierung.

Während eines Scans mit TLS-Angreifer auf Conexa SMGW wurde ein ungewöhnliches Verhalten beobachtet, das dazu führte, dass das SMGW selbst bei legitimen Verbindungsversuchen nicht mehr reagierte. Nach einem zweiten Durchlauf eines intensiven Nmap-Scans reagierte der SMGW HAN TLS-Server nicht mehr und erholte sich auch nach 48 Stunden ohne Neustart des Geräts nicht. Nmap zeigte, dass der TLS-Serverport offen war und normal funktionierte, kennzeichnete ihn jedoch als tcpwrapped. Die tcpwrapped-Antwort gibt an, dass der Netzwerkdienst verfügbar ist, der Client sich jedoch nicht auf der Liste zulässiger Hosts befindet. Um Parameter zu finden, die den Conexa SMGW TLS-Server veranlassen, in den TCP-Wrapping-Zustand zu wechseln, wurde ein Python-Skript erstellt. Die Ergebnisse zeigen, dass nur die Anzahl der Anfragen zählt, nicht die Verzögerung zwischen ihnen. Wenn der vollständige TLS-Verbindungsnachrichtenzyklus befolgt wird, antwortet der SMGW-TLS-Server auch nach 600 Zyklen mit einer fünf Sekunden Verzögerung nicht. Wenn die ClientHello-Nachricht jedoch Parameter enthält, die nicht zu den Servereinstellungen passen, oder wenn der TLS-Verbindungsworkflow nicht vollständig ist, wird der SMGW-TLS-Server nach 25 falschen Verbindungsversuchen blockiert. Das Mischen richtiger und falscher Parameter ist also nicht hilfreich. Auch das Ändern der Client-IP/MAC-Adresse umgeht den Schutz nicht. Das PPC SMGW verfügt über einen ähnlichen Schutz, erforderte jedoch anstelle eines Neustarts eine Zeitüberschreitung von 300 Sekunden.

Aufgrund des TCP-Wrapper-Schutzproblems des SMGW für Conexa SMGW und der geringen Anzahl von Referenz-Workflows in der TLS-Fuzzer-Software wurde entschieden, eine eigene SMGW-Fuzzing-Software auf der

Grundlage des TLS Response-Guided Differential Fuzzing-Ansatzes zu erstellen, der in [6] veröffentlicht wurde.

Um differenzielles Fuzzing einzusetzen, müssen mehrere Implementierungen der Software eingerichtet werden. Dann generiert ein Fuzzing-Tool Eingaben, sendet sie an jede Implementierung und vergleicht die Antworten. Wenn die Antworten nicht identisch sind, könnte dies auf eine Schwachstelle in der TLS-Implementierung zurückzuführen sein. Dieser Ansatz bietet im Vergleich zu TLS-Angreifern oder NEZHA eine bessere Test- und Quellcodeabdeckung. Um den Neustartprozess von SMGW während des Fuzzings zu automatisieren, wurde auch ein Smart Plug hinzugefügt.

Um Fehler während des Fuzzings ohne Zugriff auf die Geräte-Shell zu überwachen, wurde die Nichtantwort des Geräte-Webservers, Unterschiede im Verhalten des Geräte-TLS-Servers im Vergleich zu anderen TLS-Servern, Nichtantwort des Geräte-TLS-Servers und die Antwort der Geräte-TCP-Schicht überprüft. Auch wurde in diesem Rahmen beispielsweise ein Python-OpenCV-Skript verwendet, um die LED-Blinkanalyse zu automatisieren. Es erstellt ein Bild des Geräts, wendet Filter an, identifiziert LED-Positionen und gibt dann eine Liste der LED-Zustände zurück. Als Ergebnis der durchgeführten Fuzzing-Softwaretests gegen SMGW in der aktuellen Phase konnte ein unterschiedliches Verhalten der HAN-TLS-Server von SMGW im Vergleich zu Referenz-TLS-Implementierungen beobachtet werden, man fand aber keine Möglichkeit, es zu nutzen, um Schaden anzurichten.

Auch wurden Schwachstellen in TLS-Zertifikaten wie CVE-2019-3829 getestet, die eine Speicherbeschädigung während der Zertifikatsüberprüfung ermöglichen. Jede Client- oder Serveranwendung, die X.509-Zertifikate mit GnuTLS 3.5.8 oder höher überprüft, ist hiervon vermutlich betroffen. Es gibt mehrere öffentlich verfügbare Exploits für solche Schwachstellen. Aber diese Tests sind ohne weitere Kenntnis der Versionen und Implementierung des TLS-Servers aufgrund einer großen Anzahl von Variationen aufwendig.

Ausblick

Aus diesem Grund wird sich die zukünftige Arbeit auf die Entwicklung eines TLS-Fingerprinting konzentrieren, die auf dem gleichen „Response-Guided Differential Fuzzing"-Ansatz basiert. Wenn dann die Implementierung und die Version des TLS-Servers bekannt sind, können Tests auf einem lokalen PC ausgeführt werden, um die Testgeschwindigkeit zu erhöhen und eine Adressbereinigung verwenden zu können.

Danksagung

Das Projekt Smart Meter Inclusif (SMI) [6] wird von der Europäischen Union über den Europäischen Fonds für regionale Entwicklung (EFRE) im Programm Oberrhein Interreg V-A sowie von der Schweizerischen Eidgenossenschaft und den Kantonen Basel-Stadt, Basel-Landschaft und Aargau kofinanziert. Wir danken dem E-Werk Mittelbaden für die Bereitstellung von Testgeräten.

Referenzen/References:

[1] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," Future Generation Computer Systems, vol. 136, pp. 358–377, Nov. 2022, doi: 10.1016/J.FUTURE.2022.06.013.
[2] M. Nouman Nafees, N. Saxena, A. Cardenas, S. Grijalva, P. Burnap, and P. Burnap, "Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review," ACM Comput Surv, vol. 55, no. 10, Feb. 2023, doi: 10.1145/3565570.
[3] D. J. S. Raja, R. Sriranjani, A. Parvathy, and N. Hemavathi, "A Review on Distributed Denial of Service Attack in Smart Grid," 7th International Conference on Communication and Electronics Systems, ICCES 2022 - Proceedings, pp. 812–819, 2022, doi: 10.1109/ICCES54183.2022.9835859.
[4] Landis+Gyr, "White Paper. IDIS (Interoperable Device Interface Specification)", Accessed: Dec. 05, 2022. [Online]. Available: https://www.landisgyr.com/webfoo/wp-content/uploads/2012/11/IDIS_WhitePaper.pdf
[5] https://www.dlms.com/dlms-cosem/overview
[6] https://www.smi.uha.fr/de/smi-smart-meter-inclusif/

Zertifikatsverwaltung für Geräte auf der Feldebene

Mit der zunehmenden Umsetzung von Industrie 4.0 wird eine kryptografische Absicherung der Kommunikation auf der Feldebene von industriellen Automatisierungssystemen zunehmend unvermeidlich. Daraus ergibt sich als neue Herausforderung nicht zuletzt auch die Notwendigkeit, Zertifikate aus einer Public-Key-Infrastruktur (PKI) effektiv und effizient auf Feldgeräten zu verwalten. Im Folgenden werden aktuelle Ergebnisse aus dem Forschungsvorhaben „FieldPKI" vorgestellt, das sich genau dieser Herausforderung annimmt.

With the ongoing implementation of Industry 4.0, there is an increasing need for cryptographic protection of communication on the field level of industrial automation systems. This trend calls for an effective and efficient management of public-key certificates on field devices. In the following, recent research results from the research project "FieldPKI" are presented that addresses that very challenge.

Axel Sikora
Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing.

Fakultät EMI, Wissenschaftliche Leitung ivESK
Kommunikationsnetze, Bussysteme und Schnittstellen, eingebettete / industrielle Netzwerke, Intelligente Energienetzwerke

Julian Göppert M.Sc.

Institut ivESK
Akademischer Mitarbeiter

Andreas Walz
Dipl.-Phys.

Institut ivESK
Akademischer Mitarbeiter

Automatisierungssysteme waren lange von isolierten Netzwerken geprägt. Die Abschottung dieser sogenannten Operational Technology (OT) von der Domäne der Information Technology (IT) bot ein gewisses Maß an Schutz vor Cyber-Angriffen [1]. Nicht zuletzt durch die Vision von Industrie 4.0 und ganzheitlich und weltweit vernetzten Anlagen fällt diese schützende Trennung jedoch zunehmend und ganz bewusst weg [2]. Damit ergeben sich jedoch ganz neue Anforderungen an die Sicherheit in Automatisierungssystemen [3]. Diese zeigen sich auch auf rechtlicher Ebene, beispielsweise durch einschlägige Normen wie die IEC 62443 oder den EU Cybersecurity Act [4].

Entsprechend befasste sich das im Jahr 2019 am ivESK abgeschlossenen Projekt „SecureField" mit der Integration sicherer Ende-zu-Ende-Kommunikation durch Transport Layer Security (TLS) beziehugnsweise Datagram TLS (DTLS) Protokolls in die Feldebene von Automatisierungssystemen. Damit wird eine starke kryptografische Absicherung der Kommunikation mit Feldgeräten möglich, wie sie üblicherweise für eine sichere Bereitstellung von Web-Inhalten im Internet verwendet wird [5,6].

Die kryptografische Absicherung von Kommunikation erfordert jedoch grundsätzlich das Vorhandensein sowie die Verwaltung entsprechender Credentials, also von Passwörtern, Schlüsseln und Zertifikaten bei den beteiligten Kommunikationspartnern. Für den Web-Anwendungsfall hat sich in den vergangenen 25 Jahren beisoielsweise etabliert, dass sich Web-Server mit Public-Key Zertifikaten und menschliche Nutzer mit Benutzername und Passwort authentisieren. Solche Ansätze aus dem IT-Bereich lassen sich aber in aller Regel nicht eins-zu-eins für Automatisierungssysteme übernehmen, da die Gegebenheiten und Anforderungen dort grundlegend anders gelagert sind.

So sind auch Kommunikationspartner in Automatisierungsanlagen äußerst selten menschliche Nutzer. In den allermeisten Fällen kommunizieren zwei autarke Automatisierungskomponenten miteinander, wie ein Sensor und eine Steuerung. Die Zertifikate, die Web-Server verwenden, stammen fast immer von einer der wenigen großen Zertifizierungsstellen (engl. Certificate Authorities, CAs). Ein Server-Betreiber muss sich dabei darum kümmern, dass er von einer weithin akzeptierten CA ein Zertifikat für seinen Server erhält. Im Automatisierungsbereich ist dieser Ansatz kaum vorstellbar: die wenigsten Anlagenbetreiber werden bereit sein, sich beim Betrieb ihrer Automatisierungsanlage derart unmittelbar von externen Zertifizierungsstellen abhängig zu machen. Des Weiteren sind die von großen CAs ausgestellten Zertifikate darauf ausgelegt, im größtmöglichen Umfang (idealerweise im gesamten Internet) akzeptiert zu werden. Im Automatisierungsbereich wird – trotz aller Öffnungstendenzen – eher ein kleiner und kontrollierbarer Kreis angestrebt.

Im Projekt „FieldPKI“ (2021 - 2023) hat das ivESK daher zusammen mit dem Fraunhofer Institut für integrierte Schaltungen (IIS) in Nürnberg ein system- und technologieübergreifendes Konzept zur sicheren Schlüssel- und Zertifikatsverwaltung in industriellen Feldbuskomponenten erarbeitet, das den gesamten Lebenszyklus solcher Komponenten sowie die besonderen Anforderungen von Systemen der industriellen Automatisierung berücksichtigt.

Im FieldPKI-Projekt wurde viel Wert daraufgelegt, dass die entwickelten Konzepte und Ansätze auch praxistauglich sind und keine rein akademischen Überlegungen bleiben. Im Rahmen der Arbeiten an FieldPKI hat das ivESK daher unter anderem sehr aktiv im Security-Arbeitskreis der PROFIBUS & PROFINET International (PI) mitgewirkt. PI entwickelt und pflegt die Spezifikation von PROFINET, eines der führenden Systeme für die industrielle Automatisierung. Bei PI wurde nahezu zeitgleich eine entsprechende Fragestellung bearbeitet: Wie kann eine Zertifikatsverwaltung für PROFINET-Anlagen erreicht werden? Die Mitwirkung des ivESK führte dabei zu einem fruchtbaren Austausch in beide Richtungen: Für FieldPKI konnte so ein kontinuierlicher Abgleich mit Anforderungen aus der Praxis erreicht werden und parallel konnten auch die Spezifikationsarbeiten bei PI von einer wissenschaftlichen Begleitung profitieren.

Zertifikatsverwaltung, was ist damit gemeint

Wenn (Public-Key) Zertifikate zur Authentifizierung verwendet werden sollen, muss mit mehreren Objekten hantiert werden.

- Das Zertifikat selbst ist ein digitales, durch eine CA signiertes Dokument, das einen öffentlichen Schlüssel an die Identität des Zertifikatshalters bindet. Im Fall von FieldPKI ist der Zertifikatshalter, wie oben beschrieben, in aller Regel ein Feldgerät.
- Das Feldgerät hält den passenden privaten Schlüssel und kann sich damit als Zertifikatshalter ausweisen. Jede Authentisierung muss nicht nur eine Prüfung des Zertifikats umfassen, sondern auch eine „Besitzprüfung“ des privaten Schlüssels, ohne dass dieser dabei bekannt gemacht wird.
- Die Prüfung eines Zertifikats erfordert auf der Seite des Prüfenden einen oder mehrere Vertrauensanker. Diese bestimmen, von welchen CAs Zertifikate grundsätzlich akzeptiert werden. Das Festlegen von Vertrauensankern für Feldgeräte ist eine kritische Operation, deren Bedeutung häufig übersehen oder mindestens unterschätzt wird.

Damit die drei genannten Objekte genutzt und dabei alle Phasen des Lebenszyklus von Feldgeräten berücksichtigt werden können, müssen Zertifikate, Schlüssel und Vertrauensanker:

- in die Feldgeräte eingebracht,
- auf den Feldgeräten erneuert,
- von den Feldgeräten gelöscht und
- in ihrem Geltungsbereich für ungültig erklärt werden können.

Der Begriff „Zertifikatsverwaltung“ soll im Folgenden so verstanden werden, dass er diese vier Operationen auf den drei genannten Objekten umfasst.

Das Basismodell von FieldPKI

Mit FieldPKI wurde ein abstraktes Basismodell entwickelt, das die Zertifikatsverwaltung auf Feldgeräten im oben beschriebenen Sinne abdeckt. Dabei kommt dem jeweiligen Betreiber von Feldgeräten eine besondere Bedeutung zu: Die Verwaltung der Zertifikate, Schlüssel und Vertrauensanker, die für die Absicherung der operativen Kommunikation mit dem Feldgerät verwendet werden, soll seiner Kontrolle unterliegen.

Die folgenden Aspekte stellen die Säulen des Basismodells von FieldPKI dar:

- Der unmittelbare Interaktionspartner eines Feldgerätes bei der Zertifikatsverwaltung ist eine neue logische Vermittlerrolle, die „Credentialing Entity“ (CE). Das Kommunikationsprotokoll ist nicht festgelegt. Die physische Ausprägung der Credentialing Entity ist ebenfalls variabel.
- Zwischen einem Feldgerät und einer Credentialing Entity findet eine beidseitige Authentifikation statt, die dedizierte Zertifikate, Schlüssel und Vertrauensanker verwendet. Diese beschreiben die Bindung eines Feldgerätes an einen Betreiber, dem damit die Kontrolle über die Zertifikatsverwaltung auf dem Feldgerät zukommt.
- Beim initialen Aufbau einer Bindung eines Feldgerätes an einen Betreiber kann dieser ein vom Gerätehersteller eingebrachtes sogenanntes Herstellerzertifikat verwenden, um das Feldgerät zu authentifizieren. Das Feldgerät selbst akzeptiert eine Bindung, solange keine konkurrierende Bindung bereits existiert.

Die Credentialing Entity wurde eingeführt, um mehrere Anforderungen zu adressieren:

- Die CA-Funktionalität muss, je nach Anlagendesign und Betreiberwünschen, eventuell außerhalb der Feldebene (in der IT-Domäne) verortet sein. Mit der Credentialing Entity existiert eine Einheit, die zwischen IT- und OT-Welt vermitteln kann. Alternativ kann die Credentialing Entity die CA-Funktionalität selbst bereitstellen.
- Die Interaktion zur Zertifikatsverwaltung zwischen Feldgerät und Credentialing Entity sollte in das bestehende Feldbus-Kommunikationsmodell integriert werden können. Bei PROFINET sind die Feldgeräte (soweit sie keine Steuerungsaufgaben übernehmen) zum Beispiel stets reaktiv und dürfen selbstständig keine Anfragen stellen. Eine CA ist ebenfalls rein reaktiv. Mit der Credentialing Entity besteht eine Einheit, die die Zertifikatsverwaltungsprozesse proaktiv initiieren kann.

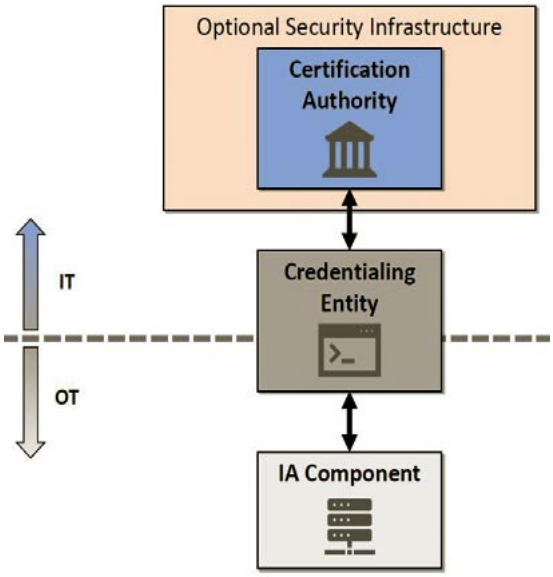


Abb. 1:
Die logische Mediatorrolle der Credentialing Entity kann als Bindeglied zwischen der IT- und OT-Umgebung vermitteln und proaktiv Zertifikatsverwaltungsprozesse auf industriellen Automatisierungskomponenten (IA Component) initiieren

Technologieabbildungen

Das FieldPKI Basismodell erhebt den Anspruch, für viele im Automatisierungsumfeld (und sogar darüber hinaus) übliche Technologien, anwendbar zu sein. Damit wurden im Basismodell ganz bewusst keine konkreten Kommunikationsprotokolle oder Ausprägungsformen der Credentialing Entity festgelegt. Dies geschieht erst über sogenannte Technologieabbildungen, die das Basismodell mit Blick auf eine bestimmte Technologie (wie bei PROFINET) konkretisieren.

Eine Technologieabbildung kann damit eine Technologie, für die bisher noch keine Zertifikatsverwaltung beschrieben wurde, einigermaßen niederschwellig für eine Zertifikatsverwaltung zugänglich machen. Das Basismodell stellt dabei das generische Lösungsmuster dar. Alternativ kann eine Technologieabbildung beschreiben, wie bereits existierende Ansätze zur Zertifikatsverwaltung mit FieldPKI korrelieren. Damit können Lösungsansätze nicht nur „exportiert", sondern auch „importiert" und auf andere Technologien übertragen werden.

Erarbeitet wurden bisher Technologieabbildungen für PROFINET, CANopen, MQTT und IEC 60802, dem TSN-Profil für die industrielle Automatisierung.

Demonstratoren

Zur Validierung des abstrakten Basismodells werden in FieldPKI für ausgewählte Technologieabbildungen Demonstratoren entwickelt. Diese sollen als Beispielausprägungen des Basismodells dessen praktische Umsetzung zeigen.

Als Vertreter einer Technologieabbildung, die das generische Lösungsmuster von FieldPKI auf ein System ohne bereits existierende Ansätze zur Zertifikatsverwaltung überträgt, wird CANopenFD – als nicht Ethernet-basiertes Feldbussystem – gewählt. Dies stellt aufgrund der im Vergleich zu Ethernet-basierten Systemen limitierten Datenrate und typischerweise ressourcenbeschränkten Geräten besondere Herausforderungen dar.

Das ursprünglich zur Vernetzung von Steuergeräten in Kraftfahrzeugen eingesetzte Bussystem CAN FD bildet die Grundlage des Datenaustauschs zwischen den industriellen Automatisierungskomponenten des Demonstrators. CANopenFD erweitert diese Basis um eine Applikationsschicht mit Kommunikationsmechanismen zum Austausch zyklischer Prozessdaten, Notfalldaten sowie azyklischer Servicedaten und kommt auch in industriellen Maschinensteuerungen, Medizintechnikgeräten oder zur Gebäudeautomation zum Einsatz. Über den Austausch azyklischer Servicedaten wird mittels TLS ein beidseitig authentifizierter und autorisierter Kanal zwischen einer CE und einer industriellen Automatisierungskomponente aufgebaut. Dieser Kanal wird genutzt, um im Request-Response-Verfahren die Operationen zur Zertifikatsverwaltung umzuset-

zen. Neben der Implementierung der Protokollerweiterungen werden mit Vertretern der Industrie intensiv diskutierte Beispielszenarien – wie der Inbesitznahme einer neuen oder dem Austausch einer defekten Komponente – an einem realen Hardwareaufbau (siehe Abbildung 2) mit mehreren beispielhaft auf Evaluierungsboards umgesetzten Feldbusgeräten getestet.

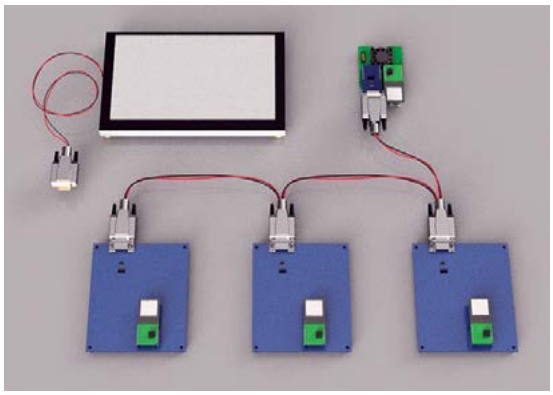


Abb. 2:
Beispiel für einen Problemraum. Knoten sind Zustände, Kanten entsprechen den Operatoren

Der aktuelle Entwurf von IEC 60802 definiert als herstellerübergreifender und vereinheitlichender Standard ein Profil sogenannter Time-Sensitive Networks (TSN) zur industriellen Automatisierung. Neben der Auswahl von Konfigurationen, Protokollen und Features werden auch Ansätze zur Zertifikatsverwaltung festgelegt. Diese stehen in Korrelation zu Ansätzen des Projekts und lassen sich als Technologieabbildung von FieldPKI „importieren". Die IEC 60802 bedient sich der Nutzung des aus dem Umfeld der Konfiguration von Netzwerk-Geräten entstandenen NETCONF (NETwork CONFiguration) Protokolls. Dieses – ebenfalls durch TLS gesicherte – Protokoll bietet basierend auf Remote Procedure Calls Mechanismen zum Einbringen, Ändern und Löschen von Konfigurationsdaten auf Endgeräten. Die IEC 60802 nutzt diese Mechanismen zur Verwaltung von Zertifikaten, Vertrauensankern und privaten Schlüsseln. Im Rahmen der Entwicklung des IEC 60802 Demonstrators werden diese Erweiterungen aufbauend auf bestehenden Umsetzungen implementiert und validiert. Neben der Implementierung der Protokollerweiterungen werden diese – wie beim CANopenFD Demonstrator – in einer Testumgebung mit beispielhafter Hardware und PKI-Hierarchie getestet.

Fazit

Mit FieldPKI wurde mit dem Basismodell ein konzeptioneller Knotenpunkt für Lösungsansätze zur Zertifikatsverwaltung in Automatisierungsanlagen geschaffen. Das FieldPKI Basismodell liefert eine generische Problem- und Lösungsbeschreibung für den Umgang mit Zertifikaten, Schlüsseln und Vertrauensankern in Feldgeräten. Das Basismodell wurde unter Berücksichtigung verschiedenster Anforderungen und Technologien und im regen Austausch mit einer Vielzahl von Industrievertretern entwickelt. Mit Technologieabbildungen lässt sich das Lösungsmuster auf verschiedenste Systeme übertragen. Soweit neue Lösungsansätze für bestimmte Technologien aufkommen, können diese mit großer Wahrscheinlichkeit in das Basismodell integriert werden und so auf weitere Technologien übertragen werden.

Danksagung

Das Projekt (Vorhaben Nr. 21752 N) wurde mit Unterstützung der Forschungsvereinigung Mikroelektronik über das Forschungskuratorium Maschinenbau e.V. (FKM) eingereicht. Es wird über die Arbeitsgemeinschaft industrieller Forschungsvereinigungen „Otto von Guericke" e.V. (AiF) im Rahmen des Programms zur Förderung der Industriellen Gemeinschaftsforschung und -entwicklung (IGF) durch das Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages finanziell gefördert.

Referenzen/References:
[1] W. Qin, S. Chen, M. Peng, "Recent advances in Industrial Internet: insights and challenges", Digital Communications and Networks, DOI: https://doi.org/10.1016/j.dcan.2019.07.001.s
[2] H. Arnarson, F.S. Kanafi, T. Kaarlela, U. Seldeslachts, R. Pieters, "Evaluation of cyber security in agile manufacturing: Maturity of Technologies and Applications", in Proceedings of the 2022 IEEE/SICE International Symposium on System Integration (SII), 2022, ISSN: 2474-2325, DOI: https://doi.org/10.1109/SII52469.2022.9708888
[3] A. Sikora, A. Walz, L. Zimmermann, „Research Aspects for Secure Communication in the Industrial Internet of Things", 11th International IEEE Conference Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18, 2020, https://ieeexplore.ieee.org/document/9125002, DOI: 10.1109/DESSERT50317.2020.9125002
[4] „The EU Cybersecurity Act". Online verfügbar unter https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, zuletzt geprüft am 28.12.2022
[5] M. Friesen, G. Karthikeyan, S. Heiss, L. Wisniewski, H. Trsek, „A Comparative Evaluation of Security Mechanisms in DDS, TLS and DTLS", Kommunikation in der Automation – KommA, Lemgo, 2018, DOI: 10.1007/978-3-662-59895-5_15
[6] M. Barenkamp, „IoT Security Best Practices", HMD Praxis der Wirtschaftsinformatik 58, 400-424, 2021, DOI: https://doi.org/10.1365/s40702-020-00637-4.

Testkomm4.0

Testumgebung für LPWAN- und 5G-Technologien

Axel Sikora
Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing.

Fakultät EMI, Wissenschaftliche Leitung ivESK
Kommunikationsnetze, Bussysteme und Schnittstellen, eingebettete / industrielle Netzwerke, Intelligente Energienetzwerke

Fabian Sowieja
M.Sc.

Institut ivESK
Wissenschaftlicher Mitarbeiter

Mit den neuen schmalbandigen drahtlosen Kommunikationslösungen ergeben sich zahlreiche vielversprechende neue Anwendungsmöglichkeiten für das Internet der Dinge (IoT), aber auch zusätzliche Fragestellungen in der Entwicklung und Anwendung. Im Testkommr.0-Projekt wurde daher in Zusammenarbeit mit dem Hahn-Schickard-Institut eine Testumgebung für drahtlose Kommunikationstechnologien aufgebaut, um systematische Vergleiche unterschiedlicher Low Power WiderArea (LPWA) Netzwerke, zellulärer IoT- (cIoT) und 5G-Netzwerke durchzuführen. Die Testumgebung ermöglicht es, verschiedene LPWAN- und cIoT-Technologien in einer einheitlichen und reproduzierbaren Umgebung für industrielle Anwendungsfälle zu testen.

The new narrowband wireless communication solutions create manifold novel opportunities, but also challenges for developers and users of applications in the Internet of Things. In collaboration with the Hahn-Schickard Institute in the Testkomm project, a test environment for wireless communication technologies is being set up to execute systematic comparisons of different Low Power Wider Area (LPWA) networks, cellular IoT (cIoT) and 5G networks. The test environment allows to flexibly perform uniform and reproducible test with LPWAN and cIoT technologies for industrial use cases.

Drahtlose Kommunikationslösungen

Seit mehreren Jahren setzt sich der Trend der zunehmenden Vernetzung im Rahmen des Internet of Things (IoT) in praktisch allen Anwendungsfeldern der Automatisierungstechnik fort [1]. Als Treiber dieses Trends sind vor allem eine gesteigerte Energieeffizienz, Kosteneinsparungen und hohe Skalierbarkeit zu nennen. Mit diesen Technologien können neue Geschäfts- und Anwendungsfelder ermöglicht werden.

In den letzten Jahren hat sich eine neue Kategorie drahtloser Netze herausgebildet, die sogenannten LPWA-Netze (Low Power Wide Area Networks). Diese können bei einer geringen Sendeleistung im unteren Milliwatt-Bereich Reichweiten im Kilometerbereich – auch unter realen Bedingungen – abdecken. Möglich wird dies durch extreme Empfängerempfindlichkeiten, die im Wesentlichen durch schmalbandige Übertragung, innovative Codierungsverfahren oder niedrige Nettodatenraten erreicht werden. Weiterhin zeichnen sich diese Netze durch eine hohe Skalierbarkeit und einen geringen Energiebedarf der Endgeräte aus [2].

In den Markt der LPWA-Technologien treten seit einiger Zeit nun auch schmalbandige zellulare Mobilfunklösungen (cellular IoT, cIoT) ein. Diese versprechen vor allem eine robustere Übertragung aufgrund des lizenzierten Spektrums. Im Gegensatz zum Spektrum der LPWAN-Lösungen, das mit jeder neuen Technologie etwas voller und damit auch störanfälliger wird, obliegt die Mobilfunknetzplanung den Netzwerkprovidern, die ein möglichst Interferenzfreies Spektrum bereitstellen möchten. Mit der Einführung von 5G ist zudem ein dedizierter Frequenzbereich nur für sogenannte Campusnetzwerke bestimmt, mit dem private und interferenzfreie Mobilfunknetzwerke aufgebaut und betrieben werden können. Solch ein Netzwerk wurde im Rahmen des Testkomm-Projekts auch am ivESK eingerichtet [3].

Für drahtlose Kommunikationstechnologien ergeben sich zahlreiche neue Anwendungsgebiete wie der Einsatz von fahrerlosen Transport-Systemen (FTS) in einer flexiblen Industrie, der Zustandsüberwachung unter-

schiedlichster Systeme, vom Wald bis zum Industriepark und bis zur intelligenten Verkehrsteuerung [4].

Die Anwendungsbereiche für schmalbandige Übertragungsvarianten ergeben sich durch die Verbindung einfacher Geräte zu meist großen sternförmigen Netzwerken mit räumlicher Ausdehnung. Neben Überwachungsanwendungen, wie beispielsweise der Zustandsüberwachung in großen technischen Anlagen, spielen auch einfachere Steueranwendungen eine Rolle. Für die breitbandigeren Mobilfunkvarianten kommen zudem auch zunehmend Regelungs- und Echtzeitanwendungen in den Bereich des Möglichen.

Testautomatisierung

Das Aufkommen vieler neuer Technologien führt unter anderem zu einer schwer durchschaubaren Landschaft an möglichen Funkprotokollen mit unterschiedlichen Eigenschaften. Für einen Anwender stellt sich die Frage, welche Technologie sich nun am besten im Hinblick auf seine Anwendungen eignet und welche Optimierungsmöglichkeiten möglich sind, beispielsweise hinsichtlich erlaubter Latenz, Durchsatz, Zuverlässigkeit oder Energiebedarf.

Sind konkrete Anforderungen einer Anwendung bekannt, können Feldtests in der entsprechenden Funkumgebung durchgeführt und so für einen konkreten Fall validiert werden. Dies bedeutet oftmals aber einen sehr hohen Aufwand, da Geräte transportiert und aufgebaut, Testpunkte manuell angefahren und die Testumgebung während der Testzeit oftmals in einen bestimmten Zustand sein muss. Außerdem sind moderne industrielle Anforderungen meist von einer gewissen Dynamik geprägt, die es erfordert, dass Tests unter unterschiedlichen Bedingungen reproduzierbar durchgeführt werden. Dies ist auf der Feldebene nur mit viel Aufwand realisierbar, was insbesondere für KMUs eine große Hürde darstellt.

Es ist daher von einer hohen Relevanz, dass Tests systematisch und reproduzierbar für unterschiedliche Technologien, Geräte, Umgebungen und Parametrierungen mit nur geringem Aufwand durchgeführt werden können. Es werden bereits einige Tetsbeds im Breich drahtloser Sensornetzwerke eingesetzt [5], um drahtlose Technologien im Labor systematisch untersuchen zu können. Diese sind allerdings noch nicht auf die Anforderungen der LPWA-Technologien ausgelegt.

Im Testkomm-Projekt werden zur Beantwortung solcher Fragestellungen Testumgebungen aufgebaut und systematisch Tests für unterschiedliche Funktechnologien durchgeführt. Hierbei wird der Fokus im Speziellen auf industrielle Anwendungen gelegt. Als Ziel soll eine funktionsfähige Testumgebung für unterschiedliche LPWA und cIoT Lösungen erstellt und über verschiedene Testkampagnen sollen optimierte Parametersätze und die darausfolgenden Leistungsdaten ermittelt werden.

Beschreibung der Testumgebungen

Um unabhängiger von der Ausführungsumgebung (wie Feldtests) zu sein, wurden im Testsystem drei Abstraktionsebenen definiert, die direkt mit dem Entwicklungszyklus gekoppelt sind. Die Grundidee ist hierbei in Abbildung 1 dargestellt. Statt nur in einer konkreten anwendungsfallspezifischen Umgebung testen zu müssen, werden gewisse Eigenschaften der Umgebung und der Geräte abstrahiert, um schon frühzeitig und reproduzierbar Tests durchführen zu können, beispielsweise in einer Ersatz-Feldtestumgebung, einer Laborumgebung oder einer Simulationsumgebung.

Zu Beginn der Entwicklung, wenn keine Hardware vorhanden ist, oder wenn Szenarien getestet werden sollen, die sich mit konkreter Hardware nur schwer realisieren lassen (tausende Geräte an unterschiedlichen Orten),

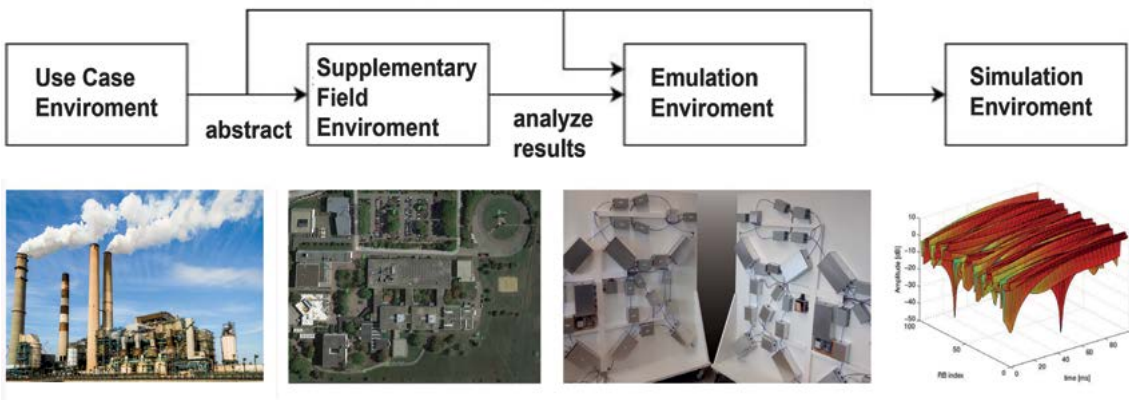


Abb. 1: Unterschiedliche Testumgebungen zur Verifizierung von konkreten Anwendungen

können Simulationen durchgeführt werden. Diese Ebene abstrahiert die physischen Eigenschaften auf mathematische Modelle, eignet sich aber, um prinzipielle Kommunikationsabläufe oder Szenarien zu verifizieren. Für die Simulation wird auf den Open-Source Netzwerksimulator ns-3 zurückgegriffen [8]. Für diesen existieren bereits Modelle für die projektrelevanten Simulationsmodelle, die um projektspezifische Eigenschaften in diesem Projekt erweitert wurden. Die Architektur der Simulation ermöglicht eine unabhängige Nutzung der Simulation via REST-API und einer dafür entwickelten Webseite zur Ausführung und Visualisierung der Ergebnisse.

Auf der zweiten Ebenen können einfache Kanalemulationen in einer eigens entwickelten Funkumgebung (APTB; Automated physical testbed) durchgeführt werden und iln der Funkumgebung können grundsätzliche Kanaleigenschaften und Netzwerktopologien automatisiert eingestellt werden. Zudem können über eine entwickelte Webseite die Netzwerke dynamisch aufgebaut werden. Verbundene Komponenten werden in einer Datenbank abgespeichert und können über eine REST-API automatisiert programmiert werden. Dadurch ist es möglich, einfach zwischen bestimmten Konfigurationen zu wechseln oder dynamische Anpassungen des Funkkanals durchzuführen. Diese Ebene abstrahiert die Funkübertragung auf einige grundsätzliche Kanaleigenschaften wie Dämpfung und Mehrwegekomponenten. Sie eignet sich weitestgehend als Ersatz der Feldtestumgebung. Zur Verifizierung von konkreten Anwendungsfällen sind Tests allerdings nach wie vor im Feld durchzuführen.

Das hier entwickelte Testsystem soll ein einheitliches Interface zum Testen unterschiedlicher Technologien anbieten, parallele Testausführung ermöglichen, mehrere Testumgebungen unterstützen und soll Daten strukturiert speichern und visualisieren können. Die Architektur ist in vereinfachter Form in Abbildung 2 dargestellt. Das zentrale Testsystem basiert auf einem TTCN3 basierten Framework [6]. Die Tests werden in der domänenspezifischen Testsprache TTCN3 [7] geschrieben und durch eine Konfigurationsdatei parametriert. Zur Interaktion mit externen Systemen, wie Test- oder Messgeräte, wurden Schnittstellen entwickelt, sodass Tests auch technologieübergreifend beschreibbar sind. Bei der Ausführung der Tests werden Daten geloggt, die es ermöglichen, die Performanz anhand der beschriebenen KPIs zu messen. Über eine API und ein Webinterface wird zu-

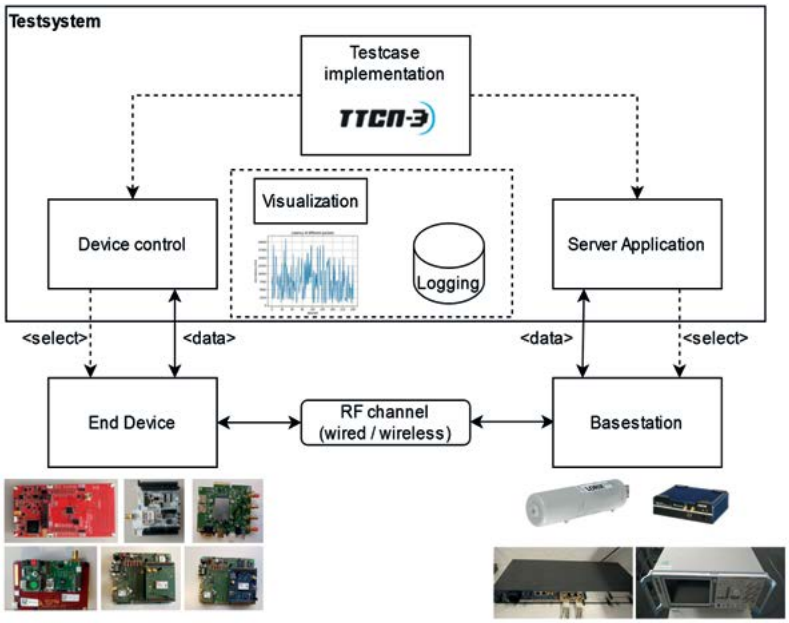


Abb. 2:
Architektur des Test-Komm4.0 Testsystems

dem die wesentliche Funktionalität bereitgestellt, wodurch der Nutzer Tests unabhängig von den konkreten Abhängigkeiten innerhalb des Testsystems durchführen kann. Die entwickelte Architektur ermöglicht hierbei die zentrale Testausführung auf allen Ebenen. Die Ausführungsebenen können allerdings auch unabhängig vom TTCN3-basierten Testsystem genutzt werden. Als Testgeräte wurden zahlreiche Netzwerkgeräte von projektbeteiligten Firmen bereitgestellt sowie auch eigene Hardware eingesetzt. Zum Testen der zellulären Funklösungen konnte zudem mit dem an der Hochschule vorhandenen Kommunikationstester CMW500 tiefere Einblicke in den Kommunikationsablauf gewonnen werden.

Performanzmessung / Verifizierung

Das Testsystem wird in Form von Messkampagnen benutzt, um Technologien in den unterschiedlichen Testumgebungen anhand ausgewählter KPIs (RSSI, SNR, Paketverlust, Latenz, Durchsatz, Energiebedarf) zu vergleichen. Als Resultat stehen visualisierbare Daten zur Verfügung. Für die hier beispielhaft gezeigte Messkampagne wurden 100 Pakete in einem zeitlichen Abstand von 10s im Uplink (vom Endgerät zu einem Server) gesendet.

In Abbildung 3 (links) ist das Ergebnis der Ende-zu-Ende Latenzmessung an verschiedenen Positionen innerhalb des Steinbeis-Gebäudes dargestellt. In der Grafik werden anhand der mittleren Latenz klare Klassenunterschiede zwischen den hier untersuchten Technologien (LoRaWAN, Mioty,

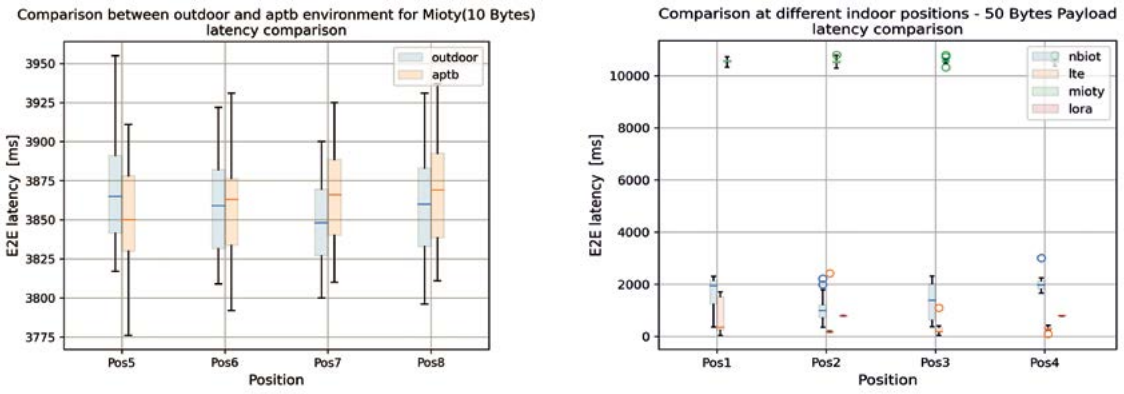


Abb. 3:
Vergleich der Ende-zu-Ende Latenz an unterschiedlichen Positionen und Testumgebungen

NB-IoT und LTE) deutlich. In diesem Aufbau fällt zudem eine hohe Varianz bei den Mobilfunklösungen auf.

Zum Vergleich der Ergebnisse in unterschiedlichen Testumgebungen wurden Tests in der Emulationsumgebung so durchgeführt, dass die Empfangssignalstärke derer im Feldtest entsprach. In Abbildung 3 (rechts) ist die Latenz für die Mioty Technologie an unterschiedlichen Punkten dargestellt. Die Ergebnisse sind dabei nahezu identisch (Latenz +/- 1 Prozent) zur Feldtestmessung.

Fazit / Ausblick

Das Testsystem ermöglicht die systematische und reproduzierbare Durchführung von Testkampagnen in unterschiedlichen Testumgebungen. So können systematische Technologievergleiche durchgeführt werden, aber auch technologische Eigenheiten herausgearbeitet und im Detail analysiert werden. Es wird außerdem deutlich, dass plausible Ergebnisse auch in der entwickelten automatisierten Emulationsumgebung erzeugt werden können. Der Testprozess vereinfacht sich dadurch deutlich und Umgebungsbedingungen lassen sich besser reproduzieren.

Als nächsten Schritte werden umfangreiche Parameterstudien bei unterschiedlichen Kanalbedingungen in der Emulationsumgebung durchgeführt, um Optimierungspotenziale zu untersuchen. Weiterhin werden Last- und Skalierbarkeitstests auf Simulationsebene durchgeführt, um auch Szenarien mit anderen Anforderungen zu untersuchen und zu verifizieren. Von besonderem Interesse sind hierbei mMTC (massive Machine Type Communication) und URLLC (Ultra-Reliable Low-Latence Communication).

Danksagung

Das Projekt (Vorhaben Nr. 21639 N) wurde mit Unterstützung der Forschungsvereinigung Elektrotechnik beim ZVEI e.V. über das Forschungskuratorium Maschinenbau e.V. (FKM) eingereicht. Es wird über die Arbeitsgemeinschaft industrieller Forschungsvereinigungen „Otto von Guericke“ e.V. (AiF) im Rahmen des Programms zur Förderung der Industriellen Gemeinschaftsforschung und -entwicklung (IGF) durch das Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages finanziell gefördert.

Referenzen/References

[1] „World of IoT Sector Map“, Beecham Research. https://www.beechamresearch.com/download-details/world-of-iot-sector-map/ (zugegriffen 2. Januar 2023)
[2] U. Raza, P. Kulkarni, M. Sooriyabandara, und M. Sooriyabandara, „Low Power Wide Area Networks: An Overview“, IEEE Commun. Surv. Tutor., Bd. 19, Nr. 2, S. 855–873, Jan. 2017, doi: 10.1109/comst.2017.2652320
[3] „Funklizenz für 5G Campusnetzwerk erhalten“. https://ivesk.hs-offenburg.de/news-detail/article/funklizenz-fuer-5g-campusnetzwerk-erhalten (zugegriffen 8. Januar 2023)
[4] A. Graf, A. Olveira-Lenz, und P. Hilsenbek, „IHK Mobilfunkatlas“, IHK Schwarzwald-Baar-Heuberg. https://www.ihk.de/sbh/ihk-mobilfunkatlas-5283342 (zugegriffen 2. Januar 2023)
[5] H. Hellbrück, M. Pagel, A. Kröller, D. Bimschas, D. Pfisterer, und S. Fischer, „Using and operating wireless sensor network testbeds with WISEBED“, IFIP Annu. Mediterr. Ad Hoc Netw. Workshop, S. 171–178, Juni 2011, doi: 10.1109/med-hoc-net.2011.5970485
[6] E. Web, „Eclipse TitanTM“, projects.eclipse.org, 27. August 2014. https://projects.eclipse.org/projects/tools.titan (zugegriffen 2. Januar 2023)
[7] ETSI, „Testing and Test Control Notation Version 3 (TTCN-3)“, TTCN-3. http://www.ttcn-3.org/ (zugegriffen 3. Januar 2023)
[8] nsnam, „ns-3“, ns-3. https://www.nsnam.org/ (zugegriffen 2. Januar 2023)

Kontakt

Hochschule Offenburg

Campus Offenburg
Badstr. 24
77652 Offenburg
Telefon: +49 781 205-0
E-Mail: info@hs-offenburg.de

Campus Gengenbach
Klosterstr. 14
77723 Gengenbach
Telefon: +49 7803 9698-0
E-Mail: info@hs-offenburg.de

Campus Research & Transfer [CRT]

Dr. oec. troph. Ira Pawlowski

Leitung
E-Mail: ira.pawlowski@hs-offenburg.de

Telefon: +49 781 205-4618
https://www.hs-offenburg.de/forschung-und-transfer

Unter dem Dach der Hochschule Offenburg wird in neun fachübergreifenden Forschungsinstituten und einer Forschungsgruppe geforscht, entwickelt und Wissen transferiert:
Die Campus Research & Transfer (CRT) ist Ansprechpartner für interessierte Unternehmen, öffentliche Institutionen und andere Hochschulen und Forschungseinrichtungen. Sie agiert zudem als Serviceeinrichtung für alle Forschenden an der Hochschule und unterstützt die Anbahnung, Konzeption und Umsetzung von F&E-Projekten.

Institute

Institut für verlässliche Embedded Systems und Kommunikationselektronik [ivESK]

Prof. Dr.-Ing. Axel Sikora

Institutsleitung
E-Mail: axel.sikora@hs-offenburg.de

Prof. Dr. phil. Andreas Schaad
Mitglied
E-Mail: andreas.schaad@hs-offenburg.de

Telefon: +49 781 205-4691
https://ivesk.hs-offenburg.de

Institut für nachhaltige Energiesysteme [INES]

Prof. Dr. rer. nat. habil. Wolfgang Bessler

Institutsleitung
E-Mail: wolfgang.bessler@hs-offenburg.de

Prof. Dr. rer. nat. Michael Schmidt
Stellvertretende Institutsleitung
E-Mail: schmidt@hs-offenburg.de

Telefon: +49 781 205-4779
https://www.ines.hs-offenburg.de