Hochschule Karlsruhe – Technik und Wirtschaft
Fakultät für Elektro- und Informationstechnik

Sicherer Verbindungsaufbau für nicht netzwerkfähige Feldgeräte auf Basis von Zertifikaten

Masterthesis (M. Sc.)

von
Kilian Nikolaus Rupp

Hochschule Karlsruhe – Technik und Wirtschaft
Fakultät für Elektro- und Informationstechnik

Sicherer Verbindungsaufbau für nicht netzwerkfähige Feldgeräte auf Basis von Zertifikaten

Masterthesis (M. Sc.)

von
Kilian Nikolaus Rupp
geb. am 06.01.1998
in Saarlouis
Matr.-Nr.: 67723

Betreuer der Firma Hager Group
M. Sc. Nils Schlegelmilch

Betreuer der Hochschule Karlsruhe
Prof. Dr.-Ing. Philipp Nenninger
Prof. Dr.-Ing. Reiner Kriesten

Karlsruhe, 01.10.2025 bis 31.03.2026

Erklärung

Ich versichere hiermit wahrheitsgemäß, die Abschlussarbeit selbstständig angefertigt, alle benutzten Hilfsmittel vollständig und genau angegeben und alles einzeln kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde.

Karlsruhe, den 2. Februar 2026

Unterschrift:

Sicherer Verbindungsaufbau für nicht netzwerkfähige Feldgeräte auf Basis von Zertifikaten

Die steigende Komplexität der Gebäudeautomatisierung und die Integration von Smart-Home-Systemen haben die Anforderungen an Schalteinrichtungen für die Hausinstallationstechnik deutlich erhöht. Diese Arbeit bietet eine umfassende Analyse und Vergleich der von der Firma Berker GmbH & Co. KG speziell für die Unterputzmontage entwickelten elektronischen Schaltertypen. Hierbei werden Schaltungen mit bistabilen Relais, MOSFETs und Triacs betrachtet.

Nach einer einführenden Darstellung der Problemstellung definiert die Arbeit die Anforderungen an 230 V Schalteinrichtungen, die sowohl schaltungstechnische als auch wirtschaftliche Aspekte umfassen. Diese Anforderungen werden durch Berechnungen, Simulationen und Messungen vergleichend untersucht. Darüber hinaus wird ein detaillierter Einblick in die Funktionsweise der Schaltungen gegeben, um den Lesern ein umfassendes Verständnis des Themas zu vermitteln.

Die Ergebnisse zeigen, dass das bistabile Relais die besten schalttechnischen Eigenschaften bietet, jedoch gleichzeitig wirtschaftlich weniger effizient ist. Die Triac-Schaltung ist zwar kostengünstig und einfach, weist jedoch die schlechtesten elektrischen Eigenschaften auf. Im Gegensatz dazu bietet die MOSFET-Schaltung einen ausgewogenen Kompromiss zwischen wirtschaftlichen und technischen Aspekten.

Insgesamt beleuchtet diese Arbeit die komplexen Dynamiken der elektronischen Schalttypen für die Unterputzmontage und liefert wertvolle Einblicke für Endverbraucher, Installateure und Entwickler im Bereich der Hausinstallationstechnik. Durch ihre sorgfältige Analyse und den Vergleich trägt die Arbeit dazu bei, das Verständnis für die Leistungsfähigkeit und Eignung verschiedener Schalttypen in unterschiedlichen Anwendungskontexten zu vertiefen.

Secure Conncetion Establishment for Non-Network-Enabled Field Devices Based on Certitificates

The increasing complexity of building automation and the integration of smart home systems have significantly raised the demands for switchgear in home installation technology. This paper provides a comprehensive analysis and comparison of electronic switch types specifically developed for wall-mounting by Berker GmbH & Co. KG. These include circuits with bistable relays, MOSFETs, and Triacs.

After an introductory overview of the problem statement, the paper defines the requirements for 230 V switching devices, encompassing both circuitry and economic aspects. These requirements are comparatively examined through calculations, simulations, and measurements. Furthermore, a detailed insight into the functioning of the circuits is provided to offer readers a comprehensive understanding of the subject.

The results indicate that bistable relays offer the best switching characteristics but are less economically efficient. While the Triac circuit is cost-effective and straightforward, it exhibits the poorest electrical properties. In contrast, the MOSFET circuit presents a balanced compromise between economic and technical aspects.

Overall, this study sheds light on the complex dynamics of electronic switching types for wall-mounted installations and provides valuable insights for end users, installers, and developers in the field of home installation technology. Through its careful analysis and comparison, the study contributes to deepening the understanding of the performance and suitability of various switching types in different application contexts.

Inhaltsverzeichnis

1 Einleitung

Die kontinuierliche Weiterentwicklung der Gebäudeautomatisierung und die zunehmende Integration von Smart-Home-Systemen haben die Nachfrage nach effizienten und vielseitigen Schalteinrichtungen für die Hausinstallationstechnik erheblich gesteigert. Elektronische Schalter spielen dabei eine Schlüsselrolle, da sie nicht nur die Fernsteuerung elektrischer Lasten ermöglichen, sondern auch dazu beitragen, den Energieverbrauch zu optimieren und die Umweltbelastung zu reduzieren. Vor diesem Hintergrund ist es von entscheidender Bedeutung, die verschiedenen Ansätze zur Schaltung von 230 V-Lasten in Hausinstallationssystemen eingehend zu untersuchen.

Der Bedarf an einer solchen Untersuchung wird durch zwei Hauptfaktoren unterstrichen:

1. Die wachsende Nachfrage nach automatisierten Haustechniklösungen, die eine präzise und energieeffiziente Verwaltung elektrischer Lasten ermöglichen.

2. Die wachsende Bedeutung von Energieeffizienz und Nachhaltigkeit, die den Einsatz effizienter Schaltlösungen unerlässlich macht.

Diese Bachelorarbeit widmet sich daher einer umfassenden Analyse und dem Vergleich von von elektronischen Schaltertypen, die speziell für die Unterputzmontage in der Hausinstallationstechnik entwickelt wurden. Die betrachteten Schalter umfassen bistabile Relais, MOSFET und Triac. Dabei wird ein besonderes Augenmerk auf die spezifischen Eigenschaften und Leistungsparameter gelegt, die für die Unterputzmontage von Relevanz sind. Die leitungsgebundenen Störungen, die bei der Verwendung dieser Schalteinrichtungen auftreten können, werden ebenfalls untersucht, um ein umfassendes Verständnis für die praktische Anwendung und die damit verbundenen Herausforderungen zu schaffen. Zudem werden die verwendeten Schaltungen auf ihre Funktionsweise und verwendeten Schutzmaßnahmen untersucht.

Das Ziel dieser Arbeit ist es, eine fundierte Entscheidungsgrundlage für Planer, Entwickler und Endverbraucher zu schaffen, die vor der Wahl der passenden Schalteinrichtung für ihre spezifischen Bedürfnisse stehen. Abschließend werden die gewonnenen Erkenntnisse im Fazit zusammengefasst und ein Ausblick auf zukünftige Entwicklungen und Forschungsfelder im Bereich der Schalteinrichtungen für Unterputzmontage gegeben.

Die Funktionsweise und Bedienung eines Systems mit elektronischen Schaltern wird in ►Bild **??** veranschaulicht. In dieser Darstellung sind die elektronischen Schalteinrichtungen als Elektronik-Einsätze gekennzeichnet, die für das Schalten der angeschlossenen Lasten zuständig sind. Die Aufsätze auf dem Steckermodul der elektronischen Schalter übertragen die Befehle zum Schalten der angeschlossenen Lasten. Diese Aufsätze können mit KNX-Funktionalität ausgestattet sein, einem intelligenten Bussystem für die

Gebäudesteuerung. Dadurch wird es möglich, Lasten auch dezentral zu steuern und zu schalten, was die Flexibilität und Vielseitigkeit des Systems deutlich erhöht.

2 Grundlagen

2.1 Stand der Technik bei nicht netzwerkfähigen Feldgeräten

Die Hauptpriorität der Sicherheit von OT wird oftmals in der Verfügbarkeit und Zuverlässigkeit der Systeme gesehen. Aspekte der Vertraulichkeit und Integrität werden unter Umständen nachrangig berücksichtigt. Bspw. wird häufig auf eine Verschlüsselung der Daten oder Transportwege verzichtet. Hieraus entsteht die Gefahr das Daten von Angreifern abgefangen sogar manipuliert werden können. In einem solchen Fall ist die Integrität und die Vertraulichkeit der Daten nicht mehr sichergestellt. Ein Angreifer mit physischem Zugriff auf das OT-Netz kann diese Werte somit auslesen, verändern oder neue einspielen (z. B. zur Steuerung einer Maschine oder zur Fälschung von Sensordaten [1].

Als Schutzmaßnahme gegen Cyberangriffe wurden speziell ältere Anlagen eine Zeit lang physikalisch von anderen Netzen getrennt. Dies gilt insbesondere für solche, in denen Systeme mit bekannten Schwachstellen enthalten sind oder eine unzureichende Zugangskontrolle bieten. Diese so genannten „Air-Gaps“ bieten jedoch selten das angestrebte Schutzniveau gegen Cyberangriffe. Denn in vielen Fällen ist weiterhin ein Datenaustausch notwendig oder erwünscht. Die hierfür eingesetzten Daten können von Angreifern genutzt werden, um die Trennung zu überwinden.

Feldgeräte werden oft im geschützten Bereich eingesetzt, dass bedeutet, dass keine unbefugten Personen Zutritt zum Feldgerät haben. Zum Beispiel durch eine Pforte. Angenommen, diese Maßnahme würde tatsächlich den Zutritt von unbefugten Personen wirksam unterbinden, schützt das nicht gegen Angreifer von Innen, sprich Personen die Zutritt haben.

Zudem gibt es auch Anwendungsszenarien, in dem ein geschützter Bereich nicht möglich ist, und Feldgeräte für jeden frei zugänglich sind. Als Beispiel sein hier Stauseen genannt.

Bei vielen Feldgeräten spielt der Energieverbrauch eine sehr große Rolle. Es gibt einen maximalen Wert der nicht überschritten werden kann. Bei Berechnungen von Kryptooperationen ohne spezielle Kryptographische Prozessoren sind rechenintensiv. Dadruch, dass harte Grenzen beim Energieverbrauch gelten, und der Takt vom Mikrocontroller generell gedrosselt ist, können solche Operationen zu langen Rechenzeiten führen, die nicht mehr akzeptabel sind. (Hier irgendwie auf einen Test oder so verweisen). Aufgrund

dessen wird häufig auf Kryptographische Operationen verzichtet, bzw. sind auch aufgrund der vorgegebenen Anforderungen an Energieverbrauch schlichtweg nichtmöglich.

Durch den Trend, auch Feldgeräte ßmartmmiteinander zu vernetzen, steigt auch der Wunsch und Nachfrage auch in ressourcenbeschränkten Geräten Kryptooperationen durchzuführen. Somit gibt es viele Mikrocontroller die kryptographische Berechnungen in einem dafür gemachten HW-Bereich durchführen. Damit können kryptographische Operationen schneller und energieeffizienter durchfügehrt werden. Dadurch kann der eigentliche Chip immernoch langsam, bzw. Energieeffizient sein, aber gleichzeitig die Anferderung nach schnellen Kryptographischen Operationen erfüllen. Somit werden

Feldgeräte werden über längere Zeiträume mit gleicher Hardware betrieben. Die Lebensdauer beträgt zwischen 10 und 15 Jahren. Daher sind noch viele Feldgeräte im Einsatz, die noch ältere Leistungs- und Effizienzschwächere Hardware verwenden. Dadurch dauert es eine lange Zeit, bis sich neuere Trends z.B. die Verwendung von Krypto HW durchsetzt.

Bei vielen industriellen Feldgeräten, insbesondere Feldgeräte mit 2-Draht-Technik ist der verfügbare Energiehaushalt sehr stark begrenzt. Der Strom für die gesamte Elektronik (Sensor, A/D-Wandlung, Signalverarbeitung, Kommunikation) muss typischerweise aus wenigen Milliampere der Stromschleife bereitgestellt werden. Designrichtlinien wie [2] nennen Budgets von 3 - 3,5 mA für die interne Elektronik, die nicht überschritten werden dürfen, damit der Messbereich von 4 - 20 mA eingehalten wird.

Kryptographische Verfahren, die rein in Software auf einem Mikrocontroller, ohne spezielle Krypto-Peripherien, durchgeführt werden, sind im Vergleich zu klassischer Signalverarbeitung sehr rechen- und energieintensiv. Während die meisten Feldgeräte wenig Energie-/ Leistungsreserven besitzen, müssen die Krypto-Operationen auch noch in die Reserven passen.

Ein möglicher Ansatz, um diesen Konflikt zu umgehen, ist der Einsatz von Crypto-Peripherie. Diese lagert die Berechung in dedizierte HW aus, die speziell dafür konstruiert wurde und die Ausführungszeit, sowie auch den Energieverbauch pro Operation deutlich reduzieren.

Ein weiterer Vorteil ist auch die erhöhte Sicherheit, da weitere Security Mechanismen wie sichere Erzeugung von privaten Schlüsseln, Zertifizierte Entropie, Anti-Tampering-Maßnahmen und weitere Features bietet.

Werden eigene Messungen auf dem (auch hier in der Arbeit verwendeten Mikrocontroller) zeigen, dass

Ein weiterer Aspekt ist die lange Einsatzdauer industrieller Feldgeräte. Komponenten der Betriebstechnik (OT) werden in industriellen Steuerungssystemen typischerweise über Zeiträume von 10 bis 15 Jahren oder länger betrieben, deutlich länger als klassische IT-Hardware (Zitat). Das bedeutet, dass heute noch eine große installierte Basis von Feldgeräten mit älterer, nicht kryptofähiger Hardware im Feld ist. Die Modernisierung

hin zu Geräten mit integrierter Krypto-Hardware und damit die breite Umsetzung kryptografisch gesicherter Verbindungen bis hinunter zum Feldgerät erfolgt daher nur schrittweise im Rahmen von Migrations- und Retrofit-Projekten und wird durch Lebensdauer, Zertifizierungen (z. B. ATEX/IECEx) und die hohen Kosten von Gerätewechseln zusätzlich verlangsamt.

3 Bedrohungsmodell

Hallo ich bin Bedrohungsmodell.

Und Hier kann ich Sachen hinzufügen.

Test nach Tabelle. Hallo, ich schreibe jetzt in VScode.

Das ist ein doppeltes Enter. Das ist ein Enter mit zwei leerzeichen nach dem Punkt.

Literaturverzeichnis

[1] BSI - Bundesamt für Sicherheit in der Informationstechnik. *ICS Security Kompendium V2.0*. 23. Apr. 2024. (Online - zuletzt aufgerufen am 30. 01. 2026) (siehe S. 3).

[2] Johnson, T. ; Brychta, M. *Power Limitations of Loop- Powered Smart Transmitters, MS-2475*. Technical Article MS-2475. Analog Devices, Inc., 2013. (Online - zuletzt aufgerufen am 02. 02. 2026) (siehe S. 4).

Abbildungsverzeichnis