OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

ZENTRUM DIGITALISIERUNG. BAYERN

Laboratory for Safe and Secure Systems
a discipline of software engineering

ES³M – Energy Safe&Secure System Module
IT-Sichere Energienetze

Forschungsförderung
im 6. Energieforschungsprogramm
„**Forschung für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung**“
- Förderinitiative **Stromnetze**

Prof. Dr. Jürgen Mottok

ZD.B-Forschungs-Professur
für „Sichere und zuverlässige dezentrale Systeme”
Faculty of Electrical Engineering and Information Technology
Laboratory for Safe and Secure Systems, LaS³
- a software engineering discipline (www.las3.de)
Zentrum Digitalisierung Bayern (ZD.B)

OTH Regensburg
Ostbayerische Technische Hochschule Regensburg
Seybothstrasse 2
93053 Regensburg

Phone +49 (0)941/943-1120
Mobile +49 0160 966 569 62
E-Mail: juergen.mottok@oth-regensburg.de
LaS³: www.las3.de
OTH: www.oth-regensburg.de

Adressen und Ansprechpartner der Verbundpartner

Nr.	Projekt-Partner	
1	--- Projektleitung --- Prof. Dr. Jürgen Mottok juergen.mottok@oth-regensburg.de Prof. Dr. Rudi Hackenberg rudolf.hackenberg@oth-regens-burg.de **Laboratory for Safe and Secure Systems (LaS³) – ZD.B** **OTH Regensburg** Seybothstrasse 2 93053 Regensburg	OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG LaS³ Laboratory for Safe and Secure Systems a discipline of software engineering ZD.B ZENTRUM DIGITALISIERUNG. BAYERN
2	Thilo Böhm T.Boehm@reinhausen.com Gudrun Diepold g.diepold@reinhausen.com **Maschinenfabrik Reinhausen GmbH** Falkensteinstr. 8 93059 Regensburg	MR
3	Dr. Joachim Jost jojo@j-jost.de **DV-Systemberatung** Wolsteiner Weg 5 12559 Berlin	**Dr. Joachim Jost** **DV-Systemberatung**
4	Frank Bergmann info@ibbergmann.org **IBB - Ingenieurbüro Bergmann** Sonnenweg 3 15537 Grünheide	**IBB - Ingenieurbüro Bergmann**
5	Frank Breitschaft f.breitschaft@gai-netconsult.de **GAI NetConsult GmbH** Am Borsigturm 58 13507 Berlin	GAI NetConsult
6	--- ***Assoziierter Partner*** --- Peter Rümenapp peter.ruemenapp@amprion.net **Amprion GmbH** Rheinlanddamm 24 44139 Dortmund	amprion

1 Kurzfassung und Ziele

„Etablierung eines Safe and Secure Modul für sichere Kommunikation bei der Energieübertragung zwischen Infrastruktur und Leitstelle gemäß IEC 62351 mit Features der Krypto-Wartung.“

1.1 Gesellschaftliche Aspekte der IT-Security und der Kontext der Energieversorger-Infrastruktur

Die Energienetze in Deutschland zählen zu den kritischen Infrastrukturen. Der vorliegende Förderantrag ES³M verfolgt das Ziel, intelligente sichere Kommunikation der Energienetze zu etablieren. Dabei stellt die sichere Kommunikation der Infrastruktur-Komponenten (controlled stations) mit den Leitstellen (controlling stations) eine gesellschaftliche, politische und technologische Herausforderung dar (kritische Infrastrukturen, IT-Sicherheitsgesetz, …).

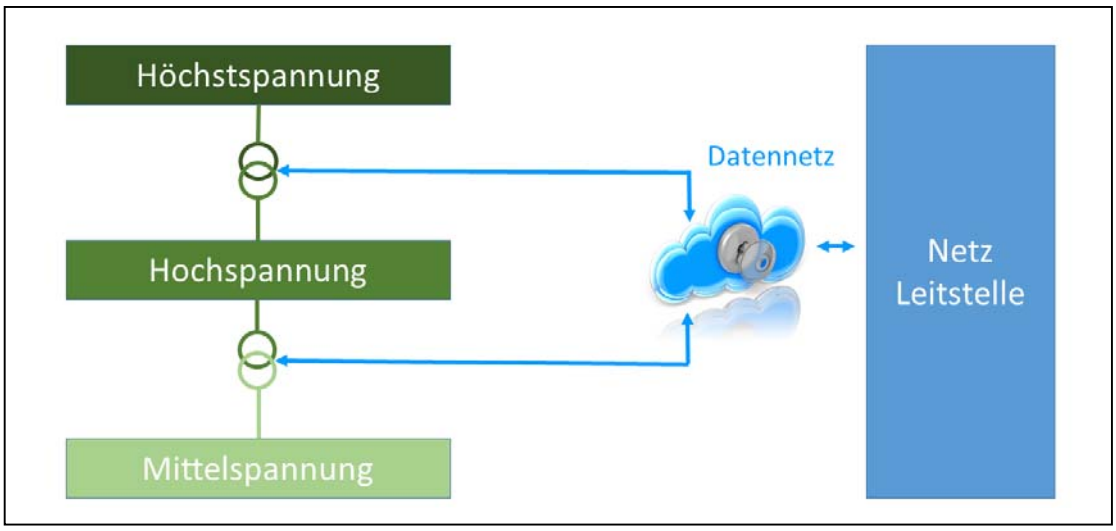
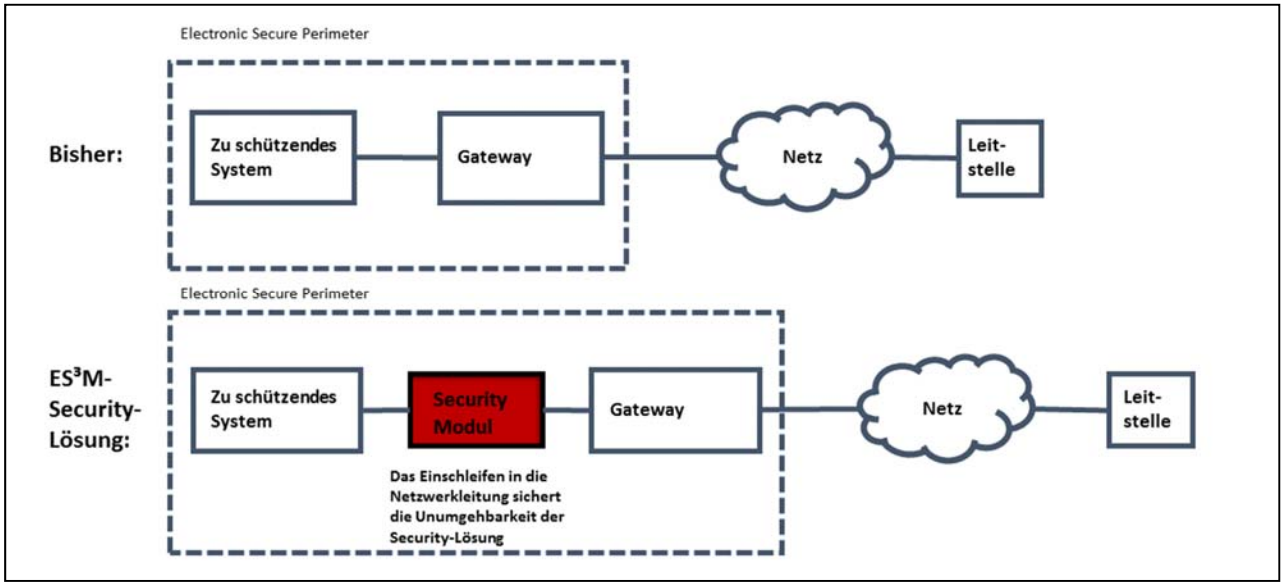


Abbildung 1: Notwendigkeit einer sicheren Datenübertragung zwischen Netzinfrastruktur und Leitstellen

Ziel des Vorhabens ist die **Entwicklung eines „Energie Safey and Secure Modul“ (ES³M) als Lösungselement in Form eines Prototyps**, welcher den Einsatz von modernster Kryptographie sowohl garantierte als auch geringe Latenzzeiten in Einklang bringt. Hierdurch soll die Etablierung einer sicheren und abgesicherten Kommunikationslandschaft im Bereich der Energieerzeugung und –übertragung ermöglicht werden. Als Teil der kritischen Infrastruktur spielt die Versorgung mit elektrischer Energie eine Schüsselkomponente in einer modernen Gesellschaft. Durch die zunehmende Volatilität von Einspeiser und Verbraucher in das Energienetz steigt der Bedarf an vernetzten Kommunikations- und Betriebsmittel überproportional. Daraus wiederum resultieren eine erhöhte Systemkomplexität und damit verbundene mögliche Angriffspunkte für eine gezielte Störung von außen. Das Gerät soll daher die Grundlage einer homogenen kryptographischen Lösung auf allen Ebenen der Leittechnik realisieren.

In Abbildung 2 ist die angestrebte ES³M-Security-Lösung grob dargestellt; Die Feindarstellung erfolgt in Kapitel 3 „Ausführlicher Arbeitsplan“.



Abildung 2: Das Safe&Secure System Modul zwischen Leitstelle und zu schützendem System

1.2 Bezug zu förderpolitischen Zielen

Die Auschreibung „Forschung für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung“ stellt Gegenstände der Förderung dar. In tabellarischer Übersicht erfolgt eine Zuordnung der Gegenstände der Förderung zu den acht ES³M-Zielen.

Tabelle 1: Zuordnung der Gegenstände der Förderung zu den acht ES³M-Zielen

Prio	***Förder-Gegenstände des Calls „Forschung für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung“***	**Energy Safe and Secure Module (ES³M)** **Infrastruktur ⇔ Netzbetreiber**
1	*Stromnetze (3.9.2)* ***Intelligente Netzbetriebsführung: – Systemsicherheit sowie Kommunikations- und Datensicherheit in intelligenten Netzen***	**Technisch** **Ziel 1 - Sichere Leittechnikanbindung** **Ziel 2 - Sicherstellung der funktionalen Sicherheit** **Ziel 3 - Einsatz geeigneter Prüfverfahren und Tools** **Wissenschaftlich** **Ziel 4 - Normative Konformität** **Ziel 5 - Beherrschung der Alterung von Krypto-Algorithmen** **Ziel 6 - Zufallszahlen-Generator mit hoher Entropie** **Ziel 7 - Robustheit** **Ziel 8 - Geprüfte Sicherheit als „Markenzeichen“**
2	Stromnetze (3.9.2) Verbesserte Zustandserkennung der Netze und Entwicklung notwendiger Messtechnik	Ziel 1 - Sichere Leittechnikanbindung Ziel 2 - Sicherstellung der Gültigkeit übermittelter Daten
2	Stromnetze (3.9.2) Die Ertüchtigung der Stromnetzinfrastruktur und deren Ausrichtung auf die Einspeisung hoher Anteile erneuerbarer Energien durch neue Technologien und Konzepte voranzutreiben.	
2	Stromnetze (3.9.2) Anpassung der Leitwarten an flexible Stromeinspeisung und -nachfrage	
3	Übergreifende Fragestellungen (3.4.4) Die Entwicklung von Wartungskonzepten für einen effizienten, kostengünstigen Anlagenbetrieb	**Ziel 1 - Sichere Leittechnikanbindung** **Ziel 2 - Sicherstellung der Gültigkeit übermittelter Daten**

1.3 Drei Technische Arbeitsziele

Generelles ES³M-Projektziel: Es soll ein preiswertes universell verwendbares hochintegriertes Hard- und Software basiertes Sicherheitsmodul in Form einer kleinen Platine mit einem oder

mehreren dedizierten Kryptochips geschaffen werden, welches in verschiedene Longterm Missioncritical Powerdistribution-Systeme auf Seiten der Controlling Stations und der Controlled Stations integriert werden kann.

Innerhalb des ES³M-Projektes werden über die Analyse der Anforderungen, Konzeptionen und Umsetzung der Hard- und Softwaremodule alle Voraussetzungen dafür geschaffen werden, um die Kommunikation von Steuerungs- und Überwachungssysteme intelligenter Transformatoren untereinander und zu den übergeordneten Leitstellen so zu härten, dass sie eine sichere Kommunikationsbasis ermöglichen. Eine Zertifizierung des für eine sichere Kommunikation notwendigen Prototyps soll entsprechend ISO27019 bzw. BDEW-Whitepaper und nachfolgend CC EAL4 vorbereitet werden.

Ziel 1 - Sichere Leittechnikanbindung und Sicherstellung der Gültigkeit übermittelter Daten von Steuer- und Regelsystemen über normenkonforme Leittechnikprotokolle und Absicherung des Datenverkehrs: Hier konzentriert sich die Forschungsarbeit auf die Einhaltung der Schutzziele Integrität, Authentizität des Datentransfers zwischen den kommunizierenden Systemen und Geräten ohne Einbußen an die Verfügbarkeit oder Echtzeitanforderungen der zu übertragenden Daten. Ein modularer Ansatz ermöglicht hierbei jedoch die Implementierung erweiterter Sicherheitsstrukturen für einen nachträglich flexibleren Einsatz verschiedener Technologien (Schaffung von Routinen für Update). Die Daten-Kommunikationen unterscheidet **Sensordaten mit Reaktionsanforderung**, **Sensor-Messdaten** vom Trafo selbst, **Befehle** und die **Parametrierung der Steuerung**.

Ziel 2 - Sicherstellung der funktionalen Sicherheit der Kommunikationsfähigkeit von Betriebsmitteln untereinander oder zur Leitstelle.

Ziel 3 - Einsatz geeigneter Prüfverfahren und Tools zur Härtung der Systeme.

1.4 Fünf wissenschaftliche Arbeitsziele Kryptographie - Security by Design

Folgende Ziele der IT-Security sollen im ES³M-Projekt erreicht werden:

Ziel 4 - Normative Konformität:

Konformität zum Standard IEC/TS 62351 “Power Systems management and associated information exchange – Data and communication security”

Ziel 5 - Beherrschung der Alterung von Krypto-Algorithmen:

Ständige Anpassung des Sicherheitsniveaus an aktuelle Empfehlungen zu Algorithmen, Schlüssellängen und Protokollen von BSI, ENISA, NIST, NSA. Durch einfache Updatemöglichkeiten von Software und Hardware soll das Sicherheitsniveau über die gesamte Lebensdauer des Systems immer gleichbleibend hochgehalten werden können.

Ziel 6 - Zufallszahlen-Generator mit hoher Entropie: Einsatz eines kryptografisch hoch qualitativen physikalischen Zufallszahlengenerators, der den Empfehlungen des BSI und ENISA für die höchsten Einsatzklassen genügt (z.B. BSI AIS31 PTG.3).

Ziel 7 - Robustheit: Robustes Verhalten gegenüber Angriffen aus dem Netzwerk.

Ziel 8 - Geprüfte Sicherheit als „Markenzeichen“ für sichere Energienetze: Vorbereitung der Zertifizierung nach BDEW sowie nach CC EAL4 durch das BSI oder einer vom BSI akkreditierten Prüfstelle. Dem Kunden wird geprüfte Sicherheit angeboten.

2 Aktueller Stand von Wissenschaft und Technik

Die Diskussion zielt zum sowohl auf den gegenwärtigen Stand der Kommunikationskomponenten am Markt, als auch auf die Problemfelder der Kryptographie in technischen Systemen ab.

2.1 Gegenwärtiger Stand der Kommunikations-Komponenten

Die gegenwärtigen Technologien am Markt haben gewisse Defizite, die im Folgenden erläutert werden. Es existieren Hersteller, die sich auf eine sichere Kommunikation spezialisiert haben. Die Produkte dieser sind zertifiziert nach höchsten Sicherheitsmaßstäben (VS-NfD, NATO-restricted) und verfügen alle über einen PTRNG, der zum Teil zertifiziert ist. Im Folgenden werden Hersteller und deren relevante Produkte aufgezählt, sowie deren Charakteristiken hervorgehoben:

- **Rohde & Schwarz/SITLine ETH50:** Dabei handelt es sich um einen OSI-Layer 2 basierte Ethernetverschlüsseler. Dieser unterstützt die hohen Anforderungen an Sicherheit, EMV und Umwelt, ebenso wird ein breites Spektrum an Betriebstemperatur erlaubt.
- **Secunet/SINA Box L3 R S:** In diesem Fall ein auf OSI-Layer 3 IP-basierte Verschlüsseler. Alternativ existieren Ausführungen zu OSI-Layer 2 Verschlüssler mit geänderter Bauform. Dieser unterstützt die hohen Anforderungen an Sicherheit, EMV und Umwelt, ebenso wird ein breites Spektrum an Betriebstemperatur erlaubt.
- **Atmedia 100M Ethernet Verschlüssler:** Der 100M Ethernetverschlüssler basiert auf einer OSI-Layer 2 Ethernetverschlüsselung und erlaubt nur ein eingeschränktes Spektrum der Betriebstemperatur. Der Umgang mit den durch den PTRNG erzeugten Zufallszahlen ist an FIPS-140-2-L3 angelehnt.

In der Regel setzen viele Hersteller auf eine Verschlüsselung auf einer möglichst niedrigen OSI-Schicht, dies birgt ein erhöhtes Maß an Sicherheit. Die aufgezählten IT-Security-Komponenten decken nicht die Normen der IT-Security der Energiedomäne (IEC 62351) ab. Der hier verfolgte Ansatz will genau dieser Security-Norm umsetzen, dabei die Umweltanforderungen in einer Umspannstation (Temperatur, EMV) abdecken und kostengünstig in einem attraktiven Preissegment verfügbar werden.

2.2 Problemfelder der Kryptographie

Alterung von Kryptoalgorithmen als Problem: Kryptoalgorithmen unterliegen einer Alterung. Die beabsichtigte Schutzwirkung von Kryptoalgorithmen lässt im Laufe der Jahre nach durch wissenschaftliche und technische Fortschritte auf dem Gebiet der Kryptoanalyse und die enorme Steigerung der Leistungsfähigkeit moderner Computer. NSA – Veröffentlichung zu elliptischen Kurven und Quantencomputer. Es erwächst daraus die Notwendigkeit, auf die neu-

esten Entwicklungen der Kryptoanalyse zeitnah zu reagieren und bei Notwendigkeit Algorithmen, Schlüssellängen oder Protokolle gegen modernere Versionen im Feld auszutauschen. Sicherheitsbehörden geben dazu periodisch Empfehlungen heraus, z.B. BSI, ENISA, NIST, NSA. Der Voraussage-Horizont bewegt sich gegenwärtig bei etwa 10 Jahren für symmetrische Algorithmen und bei etwa 6 Jahren für asymmetrische Algorithmen. Marktbedarf: Wenn die zu erwartende Lebensdauer eines Systems länger ist, als der Voraussage-Horizont der Sicherheitsbehörden, müssen Krypto-Algorithmen (**auch Post-Quantum**), Schlüssellängen oder Protokolle leicht austauschbar sein, um das angestrebte Sicherheitsniveau aufrechtzuerhalten.

Qualität der Zufallszahlen: Mängel bei der Erzeugung kryptografisch hoch qualitativer Zufallszahlen führen dazu, dass die Nichtvorhersagbarkeit leidet und unter Umständen aus der Kenntnis einer Folge von erzeugten Zufallszahlen Vorgänger oder Nachfolger bestimmt werden können. Schlüsselaustauschverfahren sind damit angreifbar. Selbst Algorithmen mit großen Schlüssellängen wie AES256 sind wirkungslos, wenn die verwendeten Schlüssel leicht erraten werden können.

Security by Obscurity: Einige Hersteller verraten nicht, welche Sicherheitsmaßnahmen eingesetzt werden, behaupten aber ihrer Systeme seien sicher und hoffen darauf, dass keine Schwachstellen entdeckt werden. Deshalb sollten Sicherheitsmaßnahmen von einer unabhängigen Zertifizierungsstelle nach anerkannten Methoden, z.B. Common Criteria o.ä. zertifiziert werden.

2.3 Qualifikation- und Kompetenz

LaS³ - OTH Regensburg: Das LaS³ ist ein gemeinsames Forschungscluster der OTH. Das LaS³ sieht sich als Mediator zwischen Wissenschaft und Anwendung. Das LaS³ hat derzeit 15 Doktoranden und 10 Studierende des Masterstudiengangs „Master of Applied Research“. Damit zeigen Prof. Dr. Rudolf Hackenberg und Prof. Dr. Jürgen Mottok die Kompetenz, eine Forschergruppe nachhaltig zu führen und als **Innovator für „Safe and Secure Systems”** zu wirken.

ZD.B[1]-Forschungs-Professor Dr. Jürgen Mottok (juergen.mottok@oth-regensburg.de), Projektleiter, lehrt Informatik an der OTH Regensburg. Seine Lehrgebiete sind Software Engineering, Programmiersprachen, Echtzeitsysteme, Functional Safety und IT-Security. Er leitet wissenschaftlich das Laboratory for Safe and Secure Systems (LaS³, http://www.las3.de) in Regensburg und ist in zahleichen Safety- und Security-Gremien vertreten sowie Träger des „**Preises für besondere Leistungen bei der Zusammenarbeit zwischen Wirtschaft und Wissenschaft**“.

Professor Dr. Rudolf G. Hackenberg hat die Lehrgebiete Computer Architektur und die Informationssicherheit sowie Datenverarbeitungssysteme und deren Hardware Grundlagen. Er leitet die Penetrationtest-Arbeitsgruppe des Laboratory for Safe and Secure Systems.

[1] Das Zentrum Digitalisierung,Bayern (ZD.B) ist eine Forschungs-, Kooperations- und Gründungsplattform mit Geschäftsstelle in Garching.

Maschinenfabrik Reinhausen GmbH: Die MR ist auf dem Gebiet der Entwicklung, Herstellung, Vermarktung und des Vertriebes hochwertiger Stufenschalter zur Spannungsregelung (VACUTAP®, OILTAP®), Umsteller (DEETAP®) sowie von Transformatoren-Zubehör weltweit tätig. Ca. 90 Prozent der Wertschöpfung von MR finden innerhalb Deutschlands statt, gruppenweit wird mit etwa 3.350 Mitarbeitern ein Umsatz von rund 750 M€ erzielt.

Amprion GmbH: Die Amprion GmbH ist Deutschlands größter Übertragungsnetzbetreiber (ÜNB) nach dem Energiewirtschaftsgesetz (EnWG) für den Strombereich. Das Unternehmen, welches als Teil des RWE-Konzerns entstand, beschäftigt etwa 1250 Mitarbeiter, sein Hauptsitz befindet sich in Dortmund.

DV-Systemberatung Dr. Joachim Jost: Design und Implementierung von Kryptosystemen für Bahntechnik, Gesundheitswesen und staatliche Bedarfsträger.

IBB - Ingenieurbüro Bergmann: Das Ingenieurbüro Bergmann entwickelt einen AIS31 PTG.3 Zufallszahlengenerator.

GAI NetConsult GmbH: Beratung zur Informationssicherheit in der Energie Domäne.

2.4 Darstellung bisheriger Vorarbeiten zum Projekt

Das **LaS³** leitet den Forschungsverbund FORMUS³IC u.a. Entwicklung von **IT-Sicherheit** und das CarSec Projekt des LaS³ prüft vernetzte Fahrzeuge auf **Sicherheits-Schwachstellen**.

MR wirkt aktiv an den Normierungsgremien für sichere Energieversorgung auf nationaler und internationaler Ebene mit. Hierbei wurde sich stark an den BDEW-(Bund Deutsche Energie- und Wasserwirtschaft) white papers orientiert.

Joachim Josts Know How in angewandter Kryptographie in diversen Branchen kann für die sichere Energieversorgung genutzt werden.

IBB Bergmann hat schon verschiedene physikalische Zufallszahlengeneratoren appliziert und patentiert mit einem vom BSI erstellten stochastischem Modell.

Die **Sondierungsgespräche** von Prof. Dr. Jürgen Mottok und Dr. Joachim Jost in den Jahren 2016/2017 mit den Projektpartnern MR, Amprion, IBB und GAINet Consult führten zu einer passgenauen Fokussierung des ES³M-Förderantrages.

2.5 Existierende entgegenstehende Schutzrechte

Die kryptographischen Algorithmen werden im Regelfall patenfrei offengelegt. Der Projektpartner IBB Bergmann wird seinen eigenen patentierten HW-basierten Zufallszahlengenerator in das Fördervorhaben einbringen. Entgegenstehende Schutzrechte sind für das ES³M-Fördervorhaben nicht bekannt.