Systemarchitektur eines Sicherheitsmoduls im Energiesektor

Frauenschläger, Tobias; Dentgen, Manuel; Mottok, Jürgen
Ostbayerische Technische Hochschule Regensburg

Kurzfassung

Aufgrund der immer weiter anwachsenden Vernetzung der Stromnetze wird die Kommunikation zwischen der Leitstelle des Energieversorgers und den Infrastrukturkomponenten innerhalb eines Umspannwerks immer bedeutsamer. Dabei werden sowohl Steuerbefehle als auch Daten für Überwachungsfunktionen übertragen. In den aktuellen Netzwerkarchitekturen findet diese Kommunikation ohne eine kryptografische Absicherung statt, was einen Angriffspunkt für gezielte Attacken und damit eine potenzielle Gefährdung der Energieversorgung darstellt. Um solchen Angriffen in Zukunft entgegenzuwirken, wird das ES³M-Sicherheitsmodul entwickelt. Dieses soll in das Netzwerk zwischen den beiden Kommunikationspartnern eingesetzt werden und so den Datenverkehr absichern. Mithilfe einer Bedrohungsanalyse wurden Anforderungen abgeleitet, die neben kryptografischen Maßnahmen auch Themen wie funktionale Sicherheit und Langlebigkeit umfassen. Um diese zu erfüllen, wurde eine spezielle Systemarchitektur auf Basis einer Aufgabenteilung entworfen. Diese Architektur und korrespondierende Designentscheidungen werden im Folgenden präsentiert.

1. Einführung

Aufgrund des Klimawandels werden erneuerbare Energien immer wichtiger. Im Jahr 2018 lag deren Anteil am Bruttostromverbrauch in Deutschland bei 37,8 % [1], wobei die Tendenz weiterhin steigend ist. Die Volatilität dieser Art der Energieerzeugung macht es jedoch erforderlich, dass Stromnetze intelligent werden, was bedeutet, dass die einzelnen Komponenten miteinander vernetzt sind und kommunizieren können. Diese intelligenten Netze werden auch als Smart Grids bezeichnet. Mit dem Ziel einer stabilen und dauerhaft sichergestellten Energieversorgung erfolgt eine Überwachung und Steuerung sämtlicher Komponenten des Netzes. Innerhalb der Verteilernetze existieren hierzu private Netzwerke der Energieversorger, welche diese Kommunikation isoliert vom frei zugänglichen Internet ermöglichen. Die Datenleitungen dieser Netze sind in der Regel Teil der Stromnetze für Hoch- und Mittelspannung. Obwohl die Netzwerke vom öffentlichen Internet isoliert sind, können gezielte Cyberattacken jedoch nicht ausgeschlossen werden. Dies wird an großflächigen Stromausfällen in der Ukraine 2016 deutlich [2]: Eine Gruppe von Hackern hatte sich Zugriff zum privaten

Netzwerk des lokalen Energieversorgers verschafft und Steuerbefehle derart manipuliert, dass die Stromversorgung für mehrere tausend Menschen zusammengebrochen ist. Dieser Vorfall beweist, dass umfangreiche kryptografische Mechanismen in die Netzwerke integriert werden müssen, um die Kommunikation der Komponenten mit der zentralen Steuereinheit abzusichern und so die Energieversorgung zu gewährleisten.

Um dies umzusetzen, wird aktuell das ES³M-Sicherheitsmodul entwickelt, welches eine kryptographische Absicherung der Steuer- und Überwachungsfunktionen im Energieverteilernetz ermöglicht. Konkret wird die Kommunikation zwischen einem Umspannwerk und der Leitstelle des Energieversorgers betrachtet. Hierbei wird untersucht, wie der Datenverkehr gesichert werden kann, ohne die Anforderungen kritischer Infrastrukturen zu verletzen. Diese Anforderungen betreffen neben der erforderlichen Kryptographie auch die Themen funktionale Sicherheit, Performance und Langlebigkeit des Systems. Um diesen vielfältigen Zielen gerecht zu werden, muss das Systemdesign des Moduls schon zu Beginn für die unterschiedlichen Anforderungen ausgelegt werden.

Im Folgenden wird die Systemarchitektur des Moduls vorgestellt. Hierzu erfolgt vorbereitend in Kapitel 2 eine Analyse der Ausgangssituation und in Kapitel 3 eine Definition der Systemanforderungen. Kapitel 4 beschreibt darauf aufbauend die resultierende Systemarchitektur des ES^{3}M. Ein Fazit in Kapitel 5 schließt den Beitrag ab.

2. Ausgangssituation

2.1. Netzwerkstruktur

Um Komponenten im Energieverteilernetz von einer zentralen Stelle aus steuern und überwachen zu können, ist ein Datenaustausch erforderlich. Die beiden Endpunkte dieser Verbindung sind die zentrale Steuereinheit des Energieversorgers, auch Leitstelle genannt, und das Umspannwerk, in dem die Komponenten platziert sind. Sämtliche Geräte innerhalb eines Umspannwerks besitzen eine Schnittstelle, über welche sie gesteuert und Überwachungsdaten abgerufen werden können. Um für die Leitstelle ein einheitliches Interface bereitzustellen, wird ein Gateway im Umspannwerk verbaut, welches den lokalen Datenverkehr bündelt. Dieses Gateway bildet demnach den Endpunkt der Verbindung mit der Leitstelle. Die Netzwerkstruktur ist in Abb. 1 zu sehen.

Auf Basis des TCP/IP-Protokolls wird eine Punkt-zu-Punkt-Verbindung aufgebaut, wobei das Gateway auf eingehende Verbindungen wartet (TCP Listener) und der initiale Verbindungsaufbau durch die Leitstelle erfolgt (TCP Client). Darauf aufsetzend wird das normierte Protokoll IEC 60870-5-104 [3] eingesetzt (im weiteren Verlauf mit „IEC 104“ abgekürzt), um Steuerbefehle und Überwachungsdaten zu übertragen.

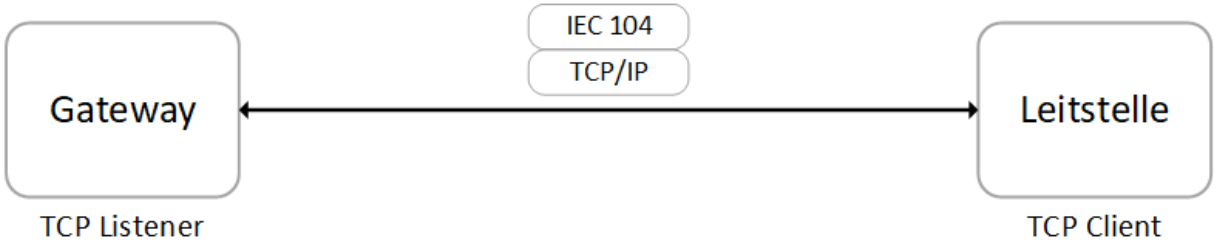

Abb. 1: Aktuelle Netzwerkverbindung

Das lokale Netzwerk innerhalb des Umspannwerks und die Verbindung zur Leitstelle werden als „Produktiv-Netz“ bezeichnet, da hierüber nur Steuer- und Überwachungsfunktionen realisiert sind, die für den Produktivbetrieb des Umspannwerks notwendig sind.

Über ein zweites, nicht in Abb. 1 dargestelltes Diagnosenetzwerk werden Konfigurationen und Firmware-Aktualisierungen der einzelnen Komponenten im Umspannwerk durchgeführt. Dieses ist vollständig vom Produktivnetzwerk isoliert und wird vom Betriebs-Management-Center (BMC) des Energieversorgers administrativ verwaltet. Analog zum Produktiv-Netz ist im Diagnose-Netz das BMC Initiator von Verbindungen. Demnach benötigt jedes Gerät zwei Netzwerkschnittstellen und muss in beiden Netzwerken auf eingehende Verbindungen warten.

2.2. Angriffsszenarien

Auf Basis der in Kapitel 2.1 gezeigten Netzwerkstruktur wird in diesem Kapitel beschrieben, welche Möglichkeiten ein Angreifer hat, eine Cyberattacke durchzuführen und welche Auswirkungen dies auf das Energieverteilernetz und demnach auf die Energieversorgung haben kann.

Grundsätzlich können zwei Arten von potentiellen Angreifern auf das Energieverteilernetz unterschieden werden: Außentäter und Innentäter. Im Folgenden werden diese beiden Arten jeweils genauer betrachtet.

Außentäter

Das Ziel eines Außentäters ist der Kommunikationspfad zwischen dem Gateway im Umspannwerk und der Leitstelle des Energieversorgers, welcher mit einer sogenannten „Man-in-the-Middle-Attacke“ angegriffen werden kann (siehe Abb. 2). Sobald ein Angreifer Zugang zu den Datenleitungen der privaten Netzwerke besitzt, besteht Zugriff auf den gesamten Datenverkehr. Da die Kommunikation lediglich auf TCP/IP basiert, ist ein Abhören technisch leicht umsetzbar. Einem Angreifer wäre es zudem möglich, Steuerbefehle zu verändern oder komplett zu unterdrücken. Somit könnten die Komponenten innerhalb des Umspannwerks nicht mehr korrekt gesteuert werden, was die Energieversorgung massiv beeinträchtigt.

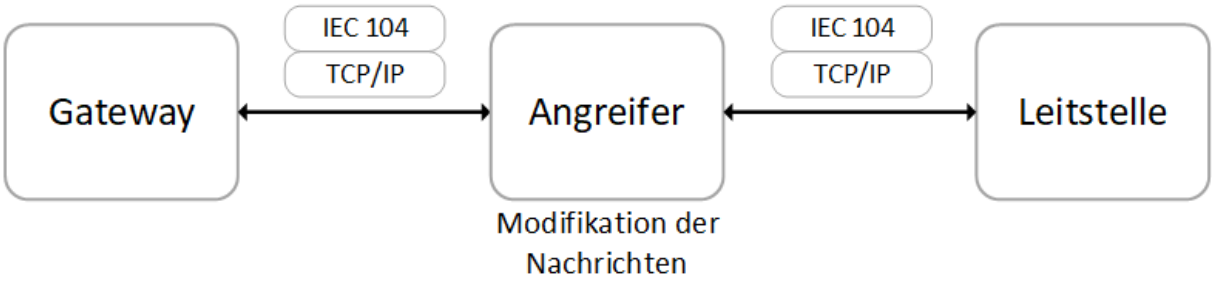

Abb. 2: Man-in-the-Middle-Angriff

Neben dem Umspannwerk kann ein Angriff auch der Leitstelle des Energieversorgers gelten. Durch Modifikation von Überwachungsnachrichten kann bei der Leitstelle ein falsches Bild über den Zustand des Umspannwerks entstehen, was zu weitaus umfangreicheren Problemen führen kann. Zudem kann eine Cyberattacke durchgeführt werden, die ein komplettes temporäres Lahmlegen der informationstechnischen Infrastruktur innerhalb der Leitstelle verursacht, was auch als Denial-of-Service (DoS) bezeichnet wird. Infolgedessen kann die Steuerung sämtlicher dieser Leitstelle unterliegenden Umspannwerke beeinträchtigt werden.

Innentäter

Neben den Außentätern kann noch die Gruppe der Innentäter definiert werden. Hierbei handelt es sich um Angreifer, die bereits einen logischen Zugang zum Umspannwerk besitzen. Dies trifft auf technische Mitarbeiter des Netzbetreibers im Umspannwerk oder auch auf Systemadministratoren in der Leitstelle zu. In diesem Fall ist eine Attacke auf das Umspannwerk aus Sicht der Informationssicherheit nicht relevant. Es besteht jedoch die Möglichkeit, dass ein Innentäter analog zum Vorgehen eines Außentäters falsche Überwachungsdaten an die Leitstelle sendet oder eine Cyberattacke in Richtung Leitstelle durchführt. Dadurch können identisch zu den Außentätern DoS-Attacken oder Falschinformationen über das Umspannwerk resultieren. Da in dieser Umgebung umfangreiche Sicherheitsvorkehrungen getroffen werden, ist diese Bedrohung weitaus geringer als die von Außentätern ausgehende Gefahr.

Aus den beschriebenen Bedrohungen folgt, dass das Abhören von Nachrichten nicht die primäre Gefahr ist. Eine Modifikation und Manipulation der Daten kann hingegen massive Auswirkungen auf die Energieversorgung haben. So könnte neben einer Manipulation der Steuer- und Überwachungsfunktionen u.a. eine nicht authentifizierte Firmware auf Komponenten des Umspannwerks eingespielt oder eine Störung der Leitstelle verursacht werden. Aus diesem Grund werden für die Entwicklung des ES³M die beiden Schutzziele Integrität und Verfügbarkeit stärker gewichtet als die Vertraulichkeit der Kommunikation. Zudem ergeben sich zwei Schutzziele: Einerseits muss der Kommunikationspfad zwischen dem Gateway und der Leitstelle aktiv abgesichert werden, andererseits darf über das ES³M keine Angriffsmöglichkeit in Richtung der Leitstelle entstehen.

3. Anforderungsanalyse

Die Angriffsszenarien aus Kapitel 2.2 zeigen, welche Schutzziele in welchem Maße für das ES³M relevant sind. Auf Basis dieser Ziele sowie der in Kapitel 2.1 beschriebenen Netzwerkstruktur und allgemein dem Einsatz in kritischen Infrastrukturen können Anforderungen definiert werden, die vom ES³M-Sicherheitsmodul erfüllt werden müssen. Diese können in vier Kategorien eingeteilt werden.

Kryptografie

Die Anforderungen hinsichtlich der kryptografischen Absicherung der Kommunikation innerhalb des Energieverteilernetzes werden in der Norm *IEC 62351-3* definiert [4]. Dort wird die Verwendung des in der Netzwerktechnik etablierten Transmission Layer Security Protokolls (TLS) für die Kommunikation zwischen Umspannwerk und Leitstelle vorgeschrieben. Durch die zum Einsatz kommenden Verschlüsselungs- und Signaturverfahren werden die Nachrichten hinsichtlich Vertraulichkeit und Integrität abgesichert. Mithilfe von Zertifikaten werden beim Verbindungsaufbau zudem beide Teilnehmer authentifiziert. Des Weiteren beträgt die maximal zulässige Verbindungsdauer 24 Stunden. Insgesamt wird so ein umfangreicher Schutz gegen Außentäter geschaffen. Um die Verfügbarkeit so hoch wie möglich zu halten und auch gegen Innentäter Schutz zu bieten, ist zudem eine Filterung des Netzwerkverkehrs erforderlich, die nicht passende Nachrichten aussortiert. Somit können unter anderem DoS-Angriffe vermieden werden.

Performance- und Echtzeitanforderungen

Bei der Integration von TLS in den Kommunikationspfad zwischen Umspannwerk und Leitstelle gilt es weitere Anforderungen zu beachten. In Teil 5 der Norm IEC 61850 [5] wird eine maximale Übertragungszeit von einer Sekunde für Nachrichten im Energieverteilernetz definiert. Die zusätzliche Latenz aufgrund der Verarbeitungszeiten der TLS-Nachrichten darf zu keiner Überschreitung dieser Grenze führen.

Langlebigkeit

Komponenten des Energieverteilernetzes müssen in der Regel eine Lebensdauer von circa 15 Jahren erfüllen. Die bei TLS verwendeten kryptografischen Mechanismen werden dieser Anforderung jedoch nicht gerecht. Laut aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [6] kann durch entsprechende Auswahl der eingesetzten Verfahren die Lebensdauer der Kryptografie bis mindestens 2025 garantiert werden, der Zeitraum danach ist jedoch ungewiss. Auch die Thematik des Quantencomputers und der Post-Quantum-Sicherheit wird hierbei relevant, da ein skalierbarer und performanter Quantencomputer alle derzeitig etablierten Mechanismen drastisch schwächen oder sogar ganz brechen könnte [7]. Daraus folgt die Anforderung, dass die zum Einsatz kommende Kryptografie austauschbar sein muss, ohne das gesamte Gerät ersetzen zu müssen.

Funktionale Sicherheit

Das Energieverteilernetz gehört zur kritischen Infrastruktur und muss folglich besondere Anforderungen hinsichtlich funktionaler Sicherheit erfüllen. Auf Basis der in der Norm IEC 61508 [8] definierten Safety Integrity Level (SIL) wurde das ES³M in SIL 3 highdemand eingestuft. Daraus folgt, dass die Verfügbarkeit des Geräts ≥ 99,99999 % und die Fehlerwahrscheinlichkeit ≤ 10^{-7} sein muss. Um dies zu erreichen, sind umfangreiche Verfahren zu integrieren, die neben einem Selbsttest der Prozessoren auch eine Überwachung durch eine unabhängige Instanz fordern.

4. Resultierende Systemarchitektur

4.1. Integration in das bestehende Netzwerk

In Kapitel 2.1 wurde die Netzwerkstruktur des Energieverteilernetzes beschrieben, in die das ES³M integriert und so die Kommunikation zwischen Leitstelle und Umspannwerk abgesichert wird. Dabei wird das Modul neben dem Gateway innerhalb des Umspannwerks platziert und in den Kommunikationspfad zur Leitstelle integriert. Die resultierende Struktur ist in Abb. 3 zu sehen.

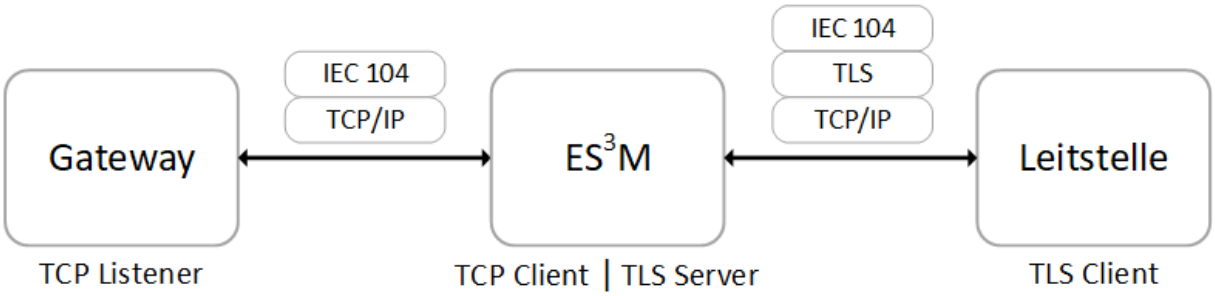

Abb. 3: Netzwerkstruktur mit ES³M

Das Modul besitzt zwei Netzwerkverbindungen in Richtung des Gateways und der Leitstelle. Das Gateway agiert wie zuvor als TCP Listener und wartet auf eingehende Verbindungen, welche in der neuen Struktur durch das ES³M aufgebaut wird (TCP Client). Parallel dazu stellt das ES³M einen TLS-Server dar, der auf eine Verbindung von der Leitstelle als TLS Client wartet. Nach dem Herstellen der Verbindung werden sämtliche Nachrichten des IEC 104-Protokolls über den sicheren Kanal geschickt. Der ungesicherte Kanal zum Gateway besteht somit nur innerhalb des Umspannwerks und ist demnach nicht mehr für Außentäter zugänglich. Im Rahmen des Forschungsprojekts wird lediglich die Realisierung auf Seiten des Umspannwerks betrachtet und daher davon ausgegangen, dass die Leitstelle in der Lage ist, als TLS Client zu arbeiten. Neben dem Produktiv-Netz muss das ES³M zudem in das Diagnose-Netz des BMCs integriert werden, wozu eine weitere Netzwerkschnittstelle am Gerät vorhanden ist.

Hierüber ist das Modul konfigurierbar, die Firmware aktualisierbar und Zustandsinformationen wie beispielsweise Log-Nachrichten abrufbar.

Insgesamt besitzt das ES³M folglich drei Netzwerkschnittstellen: zwei für die Absicherung des Produktiv-Netzes und eine für die Integration in das Diagnose-Netzwerk. Auf dieser Grundlage wurde die interne Architektur des Geräts entworfen.

4.2. Interne Systemarchitektur

Wie Kapitel 4.1 gezeigt hat, benötigt das ES³M drei Netzwerkschnittstellen. Zudem müssen alle in Kapitel 3 definierten Anforderungen erfüllt werden, was ein umfangreiches Systemdesign erfordert. Um die kryptografisch sensiblen Daten im Gerät (Schlüssel, Zertifikate etc.) zu schützen und die Problematik der begrenzten Lebensdauer der Kryptografieverfahren zu lösen, wurde eine Aufgabenteilung (Separation of Concerns) beschlossen: Drei Mikrocontroller verwalten die Netzwerkschnittstellen nach außen, während ein zentraler Controller sämtliche kryptografischen Aufgaben erledigt. Nur dieser eine Controller hat Zugriff auf die sensiblen Daten, wodurch die Sicherheit deutlich erhöht wird. Innerhalb der Kommunikationscontroller erfolgt die bereits angesprochene Netzwerkfilterung, was eine Entlastung des zentralen Kryptocontrollers zur Folge hat. Aus der Aufgabenteilung resultiert zudem eine geringere notwendige Rechenleistung der einzelnen Komponenten. Daher können anstatt Hochleistungsmikroprozessoren Mikrocontroller verwendet werden, welche sämtliche Zusatzkomponenten wie Arbeitsspeicher oder Flash innerhalb eines Gehäuses integriert haben. Dies steigert die Ausfallsicherheit durch die geringere Anzahl an diskreter Komponenten und senkt zusätzlich die Entwicklungszeit und -kosten. Durch ein modulares Design des Kryptocontrollers auf einer Steckplatine kann zukünftig dieser Teil des ES³M ausgetauscht werden, wodurch neue Kryptografiemechanismen hardwareseitig integriert werden können, ohne das gesamte Gerät tauschen zu müssen. Das Ergebnis des Architekturdesigns ist ein System aus vier Mikrocontrollern, was in Abb. 4 konzeptionell zu sehen ist.

Die drei Kommunikationscontroller verwalten jeweils eine Netzwerkschnittstelle. „CommRed“ (unverschlüsselte Seite) und „CommBlack“ (verschlüsselte Seite) sind somit Teil des Produktiv-Netzes, während die Verbindung zum Diagnose-Netz durch „CommDiag“ realisiert wird. CommBlack und CommDiag agieren jeweils als TCP Listener und warten auf eingehende Verbindungen durch die Leitstelle beziehungsweise das BMC. CommRed hingegen baut die Verbindung zum Gateway auf und ist daher ein TCP Client. Der zentrale Kryptocontroller wird als Crypto bezeichnet und stellt die Funktionalität des TLS Servers bereit. Er besitzt eine Verbindung zu allen drei Kommunikationscontrollern für den Datenaustausch und ist allgemein der Hauptcontroller des Systems. Um die Performance zu optimieren und die Sicherheit weiter zu erhöhen, bietet Crypto zudem eine Hardwarebeschleunigung für symmetrische Kryptografieverfahren.

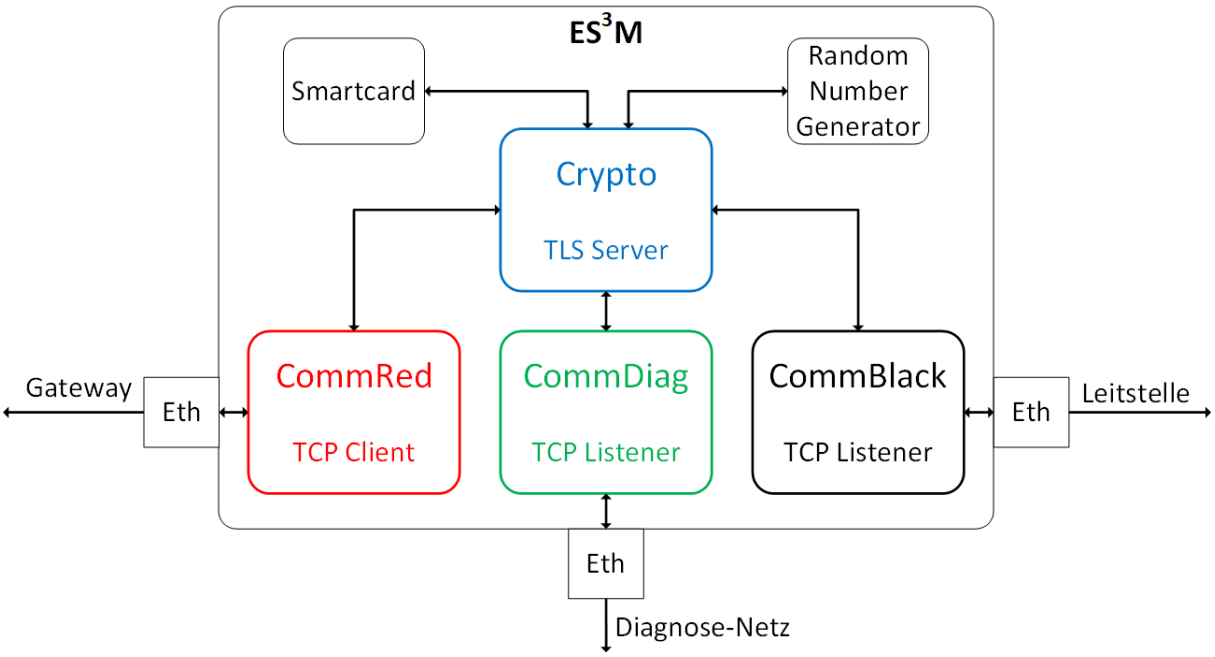

Abb. 4: Interne Systemarchitektur des ES³M mit vier Mikrocontrollern

In Abb. 4 sind zudem bereits zwei Zusatzkomponenten für Crypto zu sehen: eine Smartcard und ein Hardware-Zufallszahlengenerator (Random Number Generator - RNG). Mithilfe des RNG werden Zufallszahlen erzeugt, die eine weitaus bessere Entropie aufweisen, als diejenigen des im Kryptocontroller integrierten RNGs. Die Smartcard wird verwendet, um eine Hardwarebeschleunigung für asymmetrische Kryptografieverfahren bereitzustellen. Die Smartcard an sich ist zudem ebenfalls steckbar. Demnach kann bei einer Hardware-Aktualisierung neben dem gesamten Crypto-Modul auch nur die Smartcard allein getauscht werden.

An der Absicherung des Produktiv-Netzes ist CommDiag nicht direkt beteiligt, weshalb ein Ausfall seinerseits das System nicht sofort zum Stillstand bringt. Bei Problemen der anderen Controller hat dieser zudem über das Diagnose-Netz die Möglichkeit, das BMC zu benachrichtigen. Aus diesen Gründen bildet CommDiag die unabhängige Instanz für die Überwachung der Primärfunktion hinsichtlich der funktionalen Sicherheit (siehe Kapitel 3 – funktionale Sicherheit). Insgesamt ermöglicht diese geteilte Systemarchitektur das Erfüllen aller definierter Anforderungen.

5. Fazit

Die beschriebene Systemarchitektur des ES³M folgt dem Prinzip der Aufgabenteilung. Damit kann die Komplexität der einzelnen Komponenten reduziert werden, wodurch sowohl die kryptografische als auch die funktionale Sicherheit profitieren. Durch entsprechende Auswahl an eingesetzten Controllern und Zusatzbauteilen wird die Performance des Systems optimiert, was hinsichtlich der Echtzeitanforderungen notwendig

ist. Um die Langlebigkeit des Geräts sicherzustellen, vor allem in Hinblick auf die Alterung der eingesetzten Kryptografie, wird das zentrale Crypto-Modul modular ausgelegt, wodurch ein Hardwaretausch ermöglicht wird. Über das Diagnose-Netz sind zudem Aktualisierungen der Software möglich.

Anmerkung

Das Forschungsprojekt ES³M wird durch den Projektträger Jülich (PtJ) bzw. das Bundesministerium für Wirtschaft und Energie (BMWi) gefördert und läuft unter dem Förderkennzeichen 0350042A.

Literatur

[1] Umweltbundesamt: Erneuerbare Energien in Deutschland - Daten zur Entwicklung im Jahr 2018. März 2019. Online, Zugriff am 2. Januar 2020 https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/uba_hgp_eeinzahlen_2019_bf.pdf.

[2] Greenberg, Andy: How an Entire Nation Became Russia's Test Lab for Cyberwar. Online, Zugriff am 2. Januar 2020 https://www.wired.com/story/russian-hackers-attack-ukraine/.

[3] IEC 60870-5-104:2000: Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles, 2000.

[4] IEC 62351-3:2014: Power systems management and associated information exchange – Data and communications security; Part 3: Communication network and system security – Profiles including TCP/IP, 2014.

[5] IEC 61850-5:2014: Kommunikationsnetze und -systeme für die Automatisierung in der elektrischen Energieversorgung; Teil 5: Kommunikationsanforderungen für Funktionen und Gerätemodelle. Kapitel 11.2.3 Type 3 - Low speed messages, 2014.

[6] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 - Verwendung von Transport Layer Security (TLS). Januar 2019. Online, Zugriff am 2. Januar 2020 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=7.

[7] Ziegler, Lynn.: Online security, cryptography, and quantum computing. Forum Lectures, 119, 2015. Online, Zugriff am: 2. Januar 2020 https://digitalcommons.csbsju.edu/forum_lectures/119.

[8] IEC 61508:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

Kontakt

Tobias Frauenschläger, B. Eng.
Ostbayerische Technische Hochschule Regensburg
Laboratory for Safe and Secure Systems LaS³
Seybothstraße 2
93053 Regensburg
E-Mail: tobias.frauenschlaeger@oth-regensburg.de