**Sachbericht zum Verwendungsnachweis – Teil I: Kurzbericht**

| | |
|---|---|
| ZE:<br>SSV Software Systems GmbH | Förderkennzeichen:<br>16KIS1576 |
| Vorhabenbezeichnung:<br>SASVI Sicherheit auf allen Systemschichten durch Vertrauensketten und Isolierung | |
| Laufzeit des Vorhabens:<br>01.07.2022 – 30.09.2025 | |

## 1. Aufgabenstellung

Das Vorhaben SASVI verfolgt das Ziel, Grundlagen für vertrauenswürdige IT- und OT-Systeme für industrielle Anwendungen zu entwickeln, die auch unter den Bedingungen zunehmender Vernetzung, wachsender Angriffsflächen und offener Hard- und Softwareschnittstellen ein hohes Sicherheitsniveau gewährleisten.

Im Mittelpunkt des Teilvorhabens des Projektpartner *SSV Software Systems GmbH* steht dabei der durchgängige kryptografische Schutz sämtlicher ausgetauschter Daten und Informationen in IT- und OT-Systemen. Erreicht werden soll dies durch End-to-End-Security, bei der Daten direkt durch den Sender geschützt und vom Empfänger eindeutig auf Integrität und Urheberschaft geprüft werden können, sowie durch die sichere Verteilung von Vertrauensankern und Vertrauensketten über das gesamte System.

Die Arbeiten umfassen sowohl konzeptionelle und technische Lösungen als auch Referenzimplementierungen für eine dezentrale, interoperable IIoT-Plattform mit integrierter Sicherheit.

## 2. Stand der Wissenschaft und Technik

Vor Projektbeginn entsprach der Stand der Technik im Bereich vernetzter IT- und OT-Systeme nur eingeschränkt den Anforderungen an eine durchgängig vertrauenswürdige Kommunikation.

In IT-nahen IIoT-Anwendungen dominieren cloud-basierte Plattformen und MQTT-basierte Architekturen, bei denen Nachrichten über zentrale Broker vermittelt werden. Zwar lassen sich Transportwege punktuell, etwa durch TLS, absichern, jedoch wird damit weder die durchgängige Sicherstellung der Integrität noch die eindeutige Nachweisbarkeit der Urheberschaft einzelner Nachrichten gewährleistet. Insbesondere vermittelnde Instanzen wie Cloud-Dienste oder Broker bleiben grundsätzlich in der Lage, Daten zu verändern, ohne dass dies auf Empfängerseite zwingend erkennbar ist.

In klassischen OT-Systemen überwiegen zudem Sicherheitskonzepte nach dem Defense-in-Depth-Prinzip, bei denen die Absicherung vor allem über Netzsegmentierung und Perimeterschutz erfolgt. Diese Ansätze sind mit hohem Integrationsaufwand verbunden und bieten nur begrenzten Schutz gegenüber internen Angriffen oder Manipulationen innerhalb des Kommunikationspfads. Forschungsarbeiten zeigen zwar bereits einzelne Ansätze für Vertrauensketten, Public-Key-Infrastrukturen und signaturbasierte Absicherung, diese liegen jedoch überwiegend als Insellösungen vor und stehen noch nicht als durchgängige, interoperable und industrietaugliche Gesamtkonzepte zur Verfügung.

## 3. Ablauf des Vorhabens

Der Ablauf des Vorhabens gliedert sich in mehrere aufeinander aufbauende Schritte. Zu Beginn des Projekts wurden die fachlichen und technischen Grundlagen gemeinsam mit dem gesamten Projektkonsortium erarbeitet. Hierzu fanden mehrere Workshops statt, in denen unter Einsatz von Methoden wie der STRIDE-Analyse typische Risiken in IIoT-Systemen identifiziert und bewertet wurden. Darüber hinaus wurden Anforderungen und Schutzziele aus der IEC 62443-4-2 berücksichtigt und in die Systemarchitektur einbezogen.

Auf dieser Grundlage wurden Konzepte und Anforderungen für das SSV-Kernthema End-to-End Security sowie für die Verteilung von Vertrauensankern und Vertrauensketten abgeleitet. Darauf aufbauend erfolgte die Ausarbeitung eines Onboarding-Prozesses zum Aufbau der erforderlichen Vertrauensketten sowie die Auswahl geeigneter Technologien für die Umsetzung der End-to-End Security. In der anschließenden Umsetzungsphase wurden Programmbibliotheken zur Realisierung der End-to-End Security entwickelt.

Nach Abschluss dieser Entwicklungsarbeiten wurden die entstandenen Programmbibliotheken in die Demonstratoren des Verbundprojekts integriert. Abschließend wurde die End-to-End Security praktisch am Demonstrator des Verbundprojekts nachgewiesen und veranschaulicht.

## 4. Wesentliche Ergebnisse und Einordnung im Projektkontext

Ein wesentliches Ergebnis des Vorhabens ist die Entwicklung eines Messaging-Protokolls für die End-to-End Security, das zentrale Sicherheitsanforderungen für die Kommunikation in vernetzten IT- und OT-Systemen erfüllt.

Das Protokoll stellt sicher, dass jede Nachricht eindeutig einem Absender sowie einem oder mehreren Empfängern zugeordnet ist. Darüber hinaus enthält jede Nachricht einen definierten Gültigkeitszeitraum und einen klar spezifizierten Nachrichtentyp, etwa zur Übermittlung von Istwerten einer Maschine, zur Vorgabe von Sollwerten oder zur Auslösung eines Firmware-Updates.

Sämtliche in der Nachricht enthaltenen Informationen werden unter Verwendung der Kryptografie auf Basis der Kurve ed25519 geschützt. Dadurch kann der Empfänger jede eingehende Nachricht auf Authentizität und Integrität prüfen. Manipulationen während der Übertragung werden zuverlässig erkannt, sodass veränderte oder ungültige Nachrichten konsequent verworfen werden.

Das Messaging-Protokoll bildet eine zentrale Komponente des Demonstrators und erforderte daher eine enge Zusammenarbeit mit allen Projektpartnern. Die KSB SE & Co. KGaA stellte den Anwendungsfall für den Demonstrator bereit: Eine Pumpe sollte über das SASVI-System sowohl überwacht als auch konfiguriert werden. Hierfür wurde von KSB eine Pumpe zur Verfügung gestellt, die über ein serielles Service-Interface an den Demonstrator angebunden wurde. SSV entwickelte für diese Anbindung eine Gateway-Applikation, die zwischen dem entwickelten Messaging-Protokoll und dem pumpenspezifischen seriellen Protokoll übersetzt.

Die Partner SYSGO GmbH und NXP Semiconductors Germany GmbH trugen das Betriebssystem sowie den Hypervisor für den Demonstrator bei. SSV entwickelte die Anbindung für Over-the-Air-Updates an das Betriebssystem und integrierte diese gemeinsam mit beiden Partnern in den Demonstrator.

Das FZI Forschungszentrum Informatik entwickelte eine Anomalieerkennung für den Demonstrator, die auf aktuelle Zustandsdaten des Systems angewiesen ist. Hierfür stellte SSV eine Python-Anbindung an das Messaging-Protokoll bereit, sodass Istwerte verarbeitet und weiterverwendet werden können.

Darüber hinaus entwickelten die Universität zu Lübeck und die NXP Semiconductors Germany GmbH eine Trusted Execution Environment (TEE) sowie eine Hardwareimplementierung für die Kurve ed25519. SSV nutzt einen bereitgestellten Treiber, der die Anbindung an der Hardwareimplementierung im Demonstrator aus der TEE heraus ermöglicht, um Signaturen für die im Demonstrator erzeugten Nachrichten zu erstellen.

Damit leistet das Messaging-Protokoll nicht nur einen wesentlichen Beitrag zur sicheren Kommunikation, sondern fungiert zugleich als verbindendes Element zwischen den unterschiedlichen technischen Beiträgen der Projektpartner.

*JFI / 2026-03-26*