

Sachbericht

Teil I – Kurzbericht

Sanctuary2

Eine flexible und praktikable Sicherheitsarchitektur für Arm-basierte Systeme

Zuwendungsempfänger: SANCTUARY Systems GmbH

Förderkennzeichen: 16KIS1863

Förderzeitraum: 01.03.2023 – 31.05.2024

Autoren: Dr.-Ing. Emmanuel Stapf, Dr.-Ing. Ferdinand
Brasser, Dr.-Ing. Patrick Jauernig

1 Einleitung

Der Schutz sensibler Daten ist in Computersystemen von zentraler Bedeutung, insbesondere bei eingebetteten Systemen, deren Komplexität in den letzten Jahren erheblich gestiegen sind. Diese Systeme werden in zahlreichen Branchen wie der Automobilindustrie, Raumfahrt, Verteidigung und industriellen Produktion für Steuerungsfunktionen eingesetzt. Gleichzeitig stehen eingebettete Systeme vor vielfältigen Herausforderungen, darunter komplexe Software-Lieferketten, hoher Kostendruck und kurze Markteinführungszeiten, was die Hersteller zunehmend zur Nutzung von Open-Source- und Drittanbieter-Software zwingt. Diese Abhängigkeit birgt erhebliche Sicherheitsrisiken, da Drittanbieter-Komponenten oft blind vertraut wird, wie prominente Angriffe auf Lieferketten (z.B. log4j oder der SolarWinds-Hack) gezeigt haben. Die überwiegende Mehrheit eingebetteter Systeme basiert auf ARM-Prozessoren, die mit der TrustZone-Sicherheitstechnologie ausgestattet sind. Obwohl TrustZone eine Isolation kritischer Funktionalität vom Betriebssystem ermöglicht, fehlt ihr die Fähigkeit, Software-Komponenten unterschiedlicher Anbieter individuell und stark voneinander zu isolieren. Das vorangegangene Projekt „Sanctuary“ entwickelte daher einer flexiblen Sicherheitsarchitektur für ARM-basierte Systeme, die eine Isolation von Software-Komponenten durch sogenannte Enklaven ermöglicht. Diese unabhängigen und stark isolierten Ausführungsumgebungen bieten höchste Anforderungen an Vertraulichkeit und Integrität. Sanctuary überwindet die zahlenmäßige Begrenzung der Enklaven durch ein skalierbares Design, das ARM TrustZone mit einem eigens entwickelten Hypervisor kombiniert. Während im Projekt „Sanctuary“ ein branchenunabhängiger Prototyp entwickelt wurde, fokussierte sich „Sanctuary2“ auf die Anpassung an die Automobilbranche, insbesondere auf den Einsatz als Sicherheitsarchitektur für zentrale Steuergeräte in Fahrzeugen.

2 Ziele des Vorhabens

Das Projekt Sanctuary2 hatte das Ziel, die im Rahmen von Sanctuary entwickelte Sicherheitslösung für ARM-basierte Computersysteme weiterzuentwickeln und gezielt auf spezifische Anwendungsbereiche, insbesondere im Automotive-Sektor, auszurichten. Dabei lag der Fokus auf der sicheren Konsolidierung von Anwendungen und Diensten unterschiedlicher Anbieter auf einer einzigen Hardware-Plattform, um die Systemkomplexität und den Hardware-Aufwand zu reduzieren. Dies sollte nicht nur Kosten senken, sondern auch die Ressourcennutzung verbessern. Die flexible Architektur des Projekts strebte durch strenge Isolationsmechanismen an, Vertraulichkeit und Integrität zu gewährleisten, während branchenspezifische Anforderungen berücksichtigt wurden. Im Automotive-Sektor umfasste dies die Integration sicherheitsrelevanter Funktionen wie die sichere Anbindung von CAN-Bus-Geräten und die Nutzung von Remote-Attestierungsmechanismen zur Überprüfung der Systemintegrität über Netzwerkverbindungen. Zudem wurde die Portierung der Lösung von einer Software-emulierten Umgebung auf eine branchenspezifische Hardware-Plattform vorangetrieben, um den praktischen Einsatz zu demonstrieren. Mit der Entwicklung eines anwendungsspezifischen Demonstrators sollte die Marktreife der Sicherheitslösung auf Technology Readiness Level 6 angehoben und zugleich die Grundlage für zukünftige Anwendungen geschaffen werden.

3 Wissenschaftlicher und Technischer Stand

Aktuelle Ansätze zu Sicherheitsarchitekturen zielen oft auf alternative Prozessorarchitekturen wie RISC-V oder openMSP430 ab, können jedoch nicht direkt auf ARM-Prozessoren portiert

werden, da sie meist invasive Hardware-Modifikationen erfordern und somit den Einsatz auf Standard-ARM-Prozessoren unmöglich machen. ARM TrustZone, eine weit verbreitete Sicherheitslösung, bietet lediglich zwei isolierte Enklaven, wodurch sensible Dienste zentralisiert werden, und die Angriffsfläche vergrößert wird. Ansätze auf Basis von Virtualisierungstechnologien isolieren Software-Komponenten in virtuellen Maschinen, doch ein kompromittierter Hypervisor kann die gesamte Plattform gefährden. Sanctuary2 überwindet diese Einschränkungen durch die Einführung beliebig vieler strikt isolierter Enklaven, die für jede Software-Komponente bereitgestellt werden können. Dies minimiert Risiken, da die Kompromittierung einer Enklave keine Auswirkungen auf andere Teile des Systems hat. Die Plattform ist hardware-unabhängig und auf bestehenden ARM-Systemen ohne Modifikationen implementierbar, was sie besonders geeignet für industrielle Anwendungen wie im Automotive-Sektor macht, wo lange Produktzyklen und hohe Kosten dominieren. Technologisch kombiniert Sanctuary2 ARM TrustZone zur Sicherung kritischer Dienste mit Virtualisierungstechnologien, die eine flexible und skalierbare Isolation der Software-Komponenten gewährleisten.

4 Ablauf des Vorhabens

Das Projekt Sanctuary2 umfasste sieben Arbeitspakete zur Weiterentwicklung, Prüfung und Verbreitung der Sanctuary-Plattform. Ein Fokus lag auf der Anpassung an Industriestandards, um die Integration in bestehende Entwicklungsumgebungen und die Unterstützung moderner Software-Workloads wie Container-Technologien und Echtzeitbetriebssysteme zu ermöglichen. Erweiterte Sicherheitsfunktionen wurden implementiert und speziell für die Automobilbranche optimiert. Ein automatisiertes Test- und Integrationsframework stellte die Qualität der Plattform sicher, während ein praxisnaher Demonstrator für den Automotive-Bereich mit branchenspezifischen Funktionen und Hardware-Integration erstellt wurde. Die Sicherheitsüberprüfung analysierte Schwachstellen, insbesondere in Schnittstellen und kryptographischen Komponenten, um höchste Sicherheitsstandards zu gewährleisten. Projektergebnisse wurden über Publikationen, Messen und eine Projektwebseite verbreitet, einschließlich der Veröffentlichung des Hypervisors „Peregrine“. Abschließend wurden Marktstrategien entwickelt, die Marktanalysen und Industriefeedback nutzten, um die langfristige Adaption der Plattform zu fördern.

5 Ergebnisse des Vorhabens

Das Projekt Sanctuary2 führte zu einer entscheidenden Weiterentwicklung der Plattform, die nun als flexible Sicherheitsarchitektur eine Isolation vielfältiger Software-Komponenten ermöglicht. Wichtige Sicherheitsfunktionen wie Secure Boot und Remote Attestation wurden integriert, einschließlich der notwendigen kryptographischen Infrastruktur. Die Plattform wurde erfolgreich auf Automotive-spezifische Hardware portiert und durch einen branchenspezifischen Demonstrator ergänzt. Um die Qualität und Sicherheit zu gewährleisten, wurden umfassende Tests auf Komponenten- und Systemebene sowie ein Security Review durchgeführt, das die Zuverlässigkeit der Lösung signifikant steigerte. Die Ergebnisse wurden auf Fachveranstaltungen präsentiert und in Gesprächen mit Automobilherstellern sowie Zulieferern diskutiert. Parallel dazu wurden die Märkte Raumfahrt und Verteidigung als relevante Anwendungsfelder identifiziert, wobei seit dem Abschluss des Projektes bereits Sanctuary-Komponenten in Raumfahrtprojekten eingesetzt wurden und ein Verteidigungsprojekt vorbereitet wird, was die zukünftige Verwertbarkeit der Plattform unterstreicht.

Sachbericht

Teil II – Eingehende Darstellung

Sanctuary2

**Eine flexible und praktikable Sicherheitsarchitektur
für Arm-basierte Systeme**

Zuwendungsempfänger:	SANCTUARY Systems GmbH
Förderkennzeichen:	16KIS1863
Förderzeitraum:	01.03.2023 – 31.05.2024
Autoren:	Dr.-Ing. Emmanuel Stapf, Dr.-Ing. Ferdinand Brasser, Dr.-Ing. Patrick Jauernig

Inhalt

1	EINLEITUNG	3
2	ZIELE DES VORHABENS	4
3	WISSENSCHAFTLICHER UND TECHNISCHER STAND	5
4	ABLAUF DES VORHABENS	6
4.1	ARBEITSPAKET 1: ADAPTION ZU INDUSTRIESTANDARDS	6
4.2	ARBEITSPAKET 2: SICHERHEITSFUNKTIONEN UND -DIENSTE	6
4.3	ARBEITSPAKET 3: CONTINUOUS INTEGRATION UND TESTING	6
4.4	ARBEITSPAKET 4: AUFBAU DEMONSTRATOREN	7
4.5	ARBEITSPAKET 5: SECURITY REVIEW	7
4.6	ARBEITSPAKET 6: KOMMUNIKATION UND WISSENSTRANSFER	7
4.7	ARBEITSPAKET 7: TRANSFERKONZEPTION	7
5	ERGEBNISSE DES VORHABENS UND DEREN VERWERTBARKEIT	8
6	VERÖFFENTLICHUNG DER ERGEBNISSE	9
7	ZAHLENMÄßIGER NACHWEIS	11

1 Einleitung

Sensible Daten bestmöglich zu schützen ist auf nahezu allen heutigen Computersystemen von größter Bedeutung. Für eine Klasse von Computersystemen, eingebettete Systeme, gilt dies jedoch besonders, da die Anforderungen an diese und damit deren Komplexität in den letzten Jahren stetig angestiegen sind. Eingebettete Systeme werden heute in einer Vielzahl von Branchen für Steuerungsfunktionen eingesetzt, z.B. im Automobilbereich, der Raumfahrt, dem Verteidigungssektor oder der industriellen Produktion. Moderne eingebettete Systeme stehen dabei aus Cybersecurity-Sicht vor einer Reihe von Herausforderungen, angefangen bei einer komplexen Software-Lieferkette, aber auch Kostendruck und kurze Markteinführungszeiten sind Probleme, welche die Hersteller zwingen sich weitgehend auf Open-Source- und Drittanbieter-Software zu verlassen. Die Sicherheit der eingebetteten Systeme hängt jedoch von der Sicherheit der einzelnen Software-Komponenten von Drittanbietern ab. Viel zu oft muss diesen Komponenten blind vertraut werden, gerade bei Open-Source-Projekten ohne haftenden Anbieter. Dieses Problem hat bereits zu folgenschweren Angriffen auf die Lieferkette geführt, z. B. log4j oder dem SolarWinds-Hack, die beide enorme finanzielle Verluste und Datenschutzverletzungen zur Folge hatten.

Heutzutage werden auf der überwiegenden Mehrheit der Milliarden von eingebetteten Systemen sogenannte ARM-Prozessoren eingesetzt. ARM-Prozessoren sind in der Regel mit der Sicherheitstechnologie „TrustZone“ ausgestattet, die es erlaubt extrem kritische Funktionalität vom komplexen Betriebssystem zu isolieren. Diese bietet jedoch nicht die Möglichkeit, mehrere Software-Komponenten unterschiedlicher Drittanbieter individuell zu schützen und stark voneinander (also gegenseitig) zu isolieren. Daher kann TrustZone die Sicherheitsherausforderungen moderner eingebetteter Systeme nicht lösen. Es werden daher neue Cybersecurity-Lösungen benötigt, die den aktuellen und auch zukünftigen Anforderungen gewachsen ist.

Das Projekt Sanctuary verfolgte die Entwicklung einer flexiblen und zukunftsweisenden Sicherheitsarchitektur für ARM-basierte eingebettete Systeme. Die neu entwickelte Architektur von Sanctuary ermöglicht eine Isolierung von Software-Komponenten auf einem System durch die Schaffung von unabhängigen, stark isolierten Ausführungsumgebungen, auch Enklaven genannt, die höchste Anforderungen an Vertraulichkeit und Integrität erfüllen. Im Gegensatz zu bestehenden Ansätzen wie ARM TrustZone überwindet Sanctuary die zahlenmäßige Limitierung der Enklaven durch ein flexibles und skalierbares Design. In seinem Kern baut die entwickelte Lösung dabei auf der ARM TrustZone Technologie auf, erweitert diese jedoch geschickt mit einer eigens für dieses Projekt entwickelten Virtualisierungssoftware, auch Hypervisor genannt. Nur durch die Kombination beider Technologien ist es möglich, eine beliebige Anzahl von Enklaven auf einem System bereitzustellen, welche auf starken Sicherheitsgarantien aufbauen und dennoch flexibel und praktikabel in deren Verwendung sind.

In der ersten Phase der StartUpSecure-Förderung (Sanctuary) wurde das grundlegende Konzept der Sanctuary Sicherheitslösung ausgearbeitet und eine prototypische Entwicklung durchgeführt, welche noch unabhängig vom Anwendungsfall in einer konkreten Branche war.

In der zweiten Phase der StartUpSecure-Förderung (Sanctuary2) wurde der Prototype um zusätzliche Sicherheitsfunktionalitäten erweitert und zudem auf einen konkreten Anwendungsfall in der Automobilbranche angepasst, nämlich auf die Verwendung von Sanctuary als Sicherheitsarchitektur für das zentrale Steuergerät in einem Fahrzeug. Im folgenden Sachbericht werden die Ziele, Ergebnisse und der Ablauf des Förderprojekts Sanctuary 2 näher erläutert.

2 Ziele des Vorhabens

Das Projektvorhaben Sanctuary2 verfolgte das Ziel, die im Rahmen von Sanctuary entwickelte innovative Sicherheitslösung für ARM-basierte Computersysteme weiterzuentwickeln und auf spezifische Anwendungsbereiche auszurichten, insbesondere im Automotive-Sektor. Sanctuary2 strebte die sichere Konsolidierung von Anwendungen und Diensten unterschiedlicher Anbieter auf einer einzigen Hardware-Plattform an, um eine Reduktion der Systemkomplexität und des Hardware-Aufwands zu erreichen. Dies trägt zur Kostenreduktion, einer verbesserten Ressourcennutzung und gesteigerter Nachhaltigkeit bei. Die flexible Sicherheitsarchitektur des Projekts sollte es ermöglichen, die verschiedenen Software-Komponenten getrennt durch strenge Isolationsmechanismen parallel auszuführen, wodurch Vertraulichkeit und Integrität gewahrt werden würde.

Ein Schwerpunkt des Projekts lag auf der Anpassung der Sanctuary-Plattform an branchenspezifische Anforderungen des Automobilsektors. Hierzu gehörte die Integration zusätzlicher Sicherheitsfunktionen wie die sichere Anbindung von CAN-Bus-Geräten und die Nutzung von Remote-Attestierungsfunktionen zur Überprüfung der Systemintegrität über Netzwerkverbindungen. Diese Erweiterungen sollten sicherstellen, dass die Plattform auch in hochkritischen Szenarien zuverlässig und sicher eingesetzt werden kann. Darüber hinaus wurde die Portierung der Architektur von einer Software-emulierten Umgebung auf eine branchenspezifische Hardware-Plattform vorangetrieben, um eine praxisnahe Demonstration der Technologie zu ermöglichen.

Sanctuary2 zielte darauf ab, die Marktreife der Sicherheitsarchitektur auf ein Technology Readiness Level (TRL) von 6 zu heben, indem ein anwendungsspezifischer Demonstrator entwickelt werden sollte. Dieser sollte nicht nur die Machbarkeit und Leistungsfähigkeit der Plattform aufzeigen, sondern auch als Grundlage für zukünftige Anwendungen dienen. Gleichzeitig sollte das Projekt die europäische digitale Souveränität unterstützen, indem es eine Sicherheitslösung bereitstellt, die unabhängig von spezifischen Hardware-Herstellern ist und sich flexibel in unterschiedliche industrielle Umgebungen integrieren lässt.

Durch die Weiterentwicklung der Plattform sollte eine wesentliche Grundlage geschaffen werden, um die wachsende Komplexität und die Sicherheitsanforderungen moderner eingebetteter Systeme effektiv zu adressieren. Sanctuary2 hatte damit das Ziel den Grundstein für eine innovative Sicherheitslösungen im Automotive-Bereich und darüber hinaus zu schaffen, womit ein wichtiger Beitrag zur Resilienz gegenüber Cyberangriffen und globalen Lieferkettenrisiken geleistet werden würde.

3 Wissenschaftlicher und Technischer Stand

Die im Projektvorhaben weiterentwickelte Sanctuary Plattform zielt darauf ab eine Sicherheitsarchitektur für eingebettete Systeme zu schaffen welches es erlaubt, eine beliebige Anzahl von Ausführungsumgebungen (Enklaven) bereitzustellen, um Software-Komponenten von Drittanbietern oder Open-Source-Software von sicherheitskritischen Komponenten stark zu isolieren. Das Projektvorhaben zielte dabei explizit auf Systeme mit ARM-Prozessoren ab, da diese die aktuell dominierende Prozessarchitektur im Bereich der eingebetteten Systeme darstellt.

In der Forschung wurden bereits verschiedenste Sicherheitsarchitekturen vorgeschlagen, um eine Vielzahl von Enklaven auf einem System zu ermöglichen. Viele dieser Lösungen ziele jedoch auf alternative Prozessorarchitekturen wie RISC-V oder openMSP430 ab und erfordern meist invasive Änderungen an der Prozessorarchitektur. Auf bestehende ARM-Prozessoren können diese Designs auf Grund der zahlreichen Hardware-Unterschiede nicht direkt portiert werden, zudem würde dies die Verwendung von Standard-ARM-Prozessoren unmöglich machen. Ziel der Sanctuary Plattform war es jedoch möglichst unabhängig von der zugrundeliegenden Hardware zu sein.

Die im Projektvorhaben weiterentwickelte Sanctuary Plattform baut auf der ARM TrustZone-Technologie auf. TrustZone ermöglicht die Trennung eines Systems in zwei Bereiche: einen sicheren und einen unsicheren. In diesem Zug kommt dann ein zentrales Trusted Operating System (TOS) zum Einsatz welches die sensiblen Dienste beheimatet. Diese binäre Trennung hat jedoch erhebliche Nachteile, da alle sensiblen Dienste im sicheren Bereich unterhalb des TOS zentralisiert werden müssen, womit eine Erhöhung der Angriffsfläche für die gesamte TrustZone einhergeht. Zudem erfordert TrustZone eine komplexe und teure Sicherheitsprüfung für jeden zusätzlichen Dienst, welcher in den sicheren Bereich eingebracht werden soll. In Realität bietet TrustZone damit auf dem System nur zwei isolierte Enklaven an – zu wenig für ein komplexes eingebettetes System mit den heute üblichen komplexen Software-Stacks.

Ein weiterer alternativer Ansatz ist die Verwendung von Virtualisierungstechnologien, wie sie auch auf ARM-Prozessoren zur Verfügung stehen. Verschiedene Forschungsarbeiten schlagen vor, Virtualisierung zu nutzen um Software-Komponenten in virtuellen Maschinen (VMs) zu isolieren. Hauptproblem dieser Lösungen ist, dass sicherheitskritische Funktionen und Dienste der Plattform mit in die Virtualisierungssoftware, auch Hypervisor genannt, inkludiert werden müssen. Wird der Hypervisor kompromittiert, so ist die Sicherheit der gesamten Plattform gebrochen.

Sanctuary bietet im Vergleich zu den alternativen Lösungen eine erhebliche Verbesserung des Sicherheitsniveaus durch die Einführung isolierter Enklaven, die individuell für jede Software-Komponente bereitgestellt werden können. Diese Enklaven sind voneinander und vom Rest des Systems strikt isoliert. Durch diese Trennung wird das Risiko minimiert, dass die Kompromittierung einer Enklave andere Teile des Systems beeinträchtigt. Zudem hebt sich Sanctuary durch seine Hardware-Unabhängigkeit und breite Anwendbarkeit ab. Sanctuary kann direkt auf bestehenden ARM-basierten eingebetteten Systemen ohne Hardware-Modifikationen implementiert werden. Dies erhöht die Praktikabilität, insbesondere in industriellen Umgebungen wie der

Automobilbranche, wo lange Produktzyklen und hohe Kosten für Hardware-Anpassungen vorherrschen. Die Sanctuary Plattform erreicht dies durch eine neuartige Kombination der ARM TrustZone Technologie mit Virtualisierungstechnologien; dabei sorgt die Virtualisierung für die Isolation der Software-Komponenten, und TrustZone für den Schutz der sicherheitskritischen Dienste der Plattform.

4 Ablauf des Vorhabens

Das Projektvorhaben Sanctuary2 wurde vom 01.03.2023 bis zum 31.05.2024 durchgeführt, dabei wurden 7 Arbeitspakete bearbeitet, welche im Folgenden näher beschrieben werden. Alle im Projektvorhaben geleisteten Projektarbeiten dienten ausschließlich der Weiterentwicklung der Sanctuary Plattform, dem Testen der Plattform, sowie der Bekanntmachung der Projektergebnisse. Alle Arbeitspakete wurden in der Projektlaufzeit ordnungsgemäß durchgeführt und abgeschlossen.

4.1 Arbeitspaket 1: Adaption zu Industriestandards

Dieses Arbeitspaket konzentrierte sich auf die Anpassung und Weiterentwicklung der Sanctuary-Plattform, um sie für industrielle Anwendungen und Standards fit zu machen. Dazu gehörte die Integration der Plattform in bestehende Entwicklungs- und Verwaltungsumgebungen. Ziel war es, die Konfigurations- und Nutzungsmöglichkeiten der Plattform durch Tools wie Plug-ins für gängige Entwicklungsumgebungen wie Eclipse zu verbessern. Gleichzeitig wurde die Plattform so erweitert, dass sie marktrelevante Technologien wie Software-Container unterstützt, was eine nahtlose Integration in bestehende Systeme ermöglicht. Insgesamt unterstützt die Sanctuary Plattform nun eine Vielzahl von unterschiedlichen Software-Workloads, diese beinhaltet, „Bare-metal“ Applikationen, Unikernels, echtzeitfähige Betriebssysteme (Real-Time Operating Systems), Software Container (z.B., Docker) sowie Linux-basierte Betriebssystem (z.B., Android).

4.2 Arbeitspaket 2: Sicherheitsfunktionen und -dienste

Dieses Arbeitspaket fokussierte sich auf die Erweiterung und Anpassung der Sicherheitsfunktionen der Sanctuary-Plattform. Im Mittelpunkt standen dabei fortschrittliche Sicherheitsdienste wie Secure Boot und Remote Attestation, die so integriert wurden, dass sie von allen Anwendungen auf der Plattform sicher und unabhängig genutzt werden können. Dies erforderte die Entwicklung von Schnittstellen, die die parallele Nutzung dieser Dienste ermöglichen, sowie die Implementierung einer kryptographischen Infrastruktur, die eine sichere Verwaltung von Schlüsseln und Signaturen erlaubt. Ziel war es, die Plattform speziell für den Automotive-Bereich anzupassen.

4.3 Arbeitspaket 3: Continuous Integration und Testing

Um die Qualität und Zuverlässigkeit der Sanctuary-Plattform sicherzustellen, wurde in diesem Arbeitspaket ein automatisiertes Test- und Integrationsframework entwickelt. Dies umfasste die kontinuierliche Prüfung aller Komponenten während der Entwicklung sowie die regelmäßige

Validierung des Zusammenspiels der Plattformmodule. Zudem wurden die Schnittstellen und Dienste der Plattform umfassend dokumentiert, um eine langfristige Weiterentwicklung und mögliche Zertifizierungen zu erleichtern.

4.4 Arbeitspaket 4: Aufbau Demonstratoren

Der Fokus dieses Arbeitspakets lag auf der Entwicklung eines branchenspezifischen Demonstrators, der die Funktionalitäten der Sanctuary-Plattform in einem praxisnahen Szenario zeigt. Dazu wurde die Plattform auf einen in der Automobilbranche eingesetzten Chipsatz portiert und so angepasst, dass spezifische Anforderungen aus dem Automotive-Bereich erfüllt werden. Konkret wurde ein Demonstrator geschaffen, der die Konsolidierung von mehreren Steuergeräten im Fahrzeug zu einem zentralen Steuergerät aufzeigt. Die wichtigsten Änderungen betrafen hier die Unterstützung von der CAN-Bus Schnittstelle, sowie die Portierung von Android Automotive auf die Plattform. Zusätzlich zur Software-Entwicklung erfolgte im Arbeitspaket 4 auch die Hardware-seitige Entwicklung des Demonstrators bestehend aus einem Fahrgestell, Sensoren, Aktuatoren, etc. Des Weiteren wurde auch ein Infotainmentsystem in Form eines Tablets in den Automotive Demonstrator integriert, um die Funktionsweise des portierten Android Automotive Betriebssystems aufzuzeigen.

4.5 Arbeitspaket 5: Security Review

Dieses Arbeitspaket befasste sich mit der gründlichen Sicherheitsüberprüfung der Sanctuary Plattform. Dabei wurden alle Komponenten, von der Hardware-Integration bis zu den Sicherheitsdiensten, intensiv auf Schwachstellen untersucht. Ein besonderes Augenmerk lag auf den Schnittstellen zwischen den Anwendungen und der Plattform sowie auf der Sicherheit der kryptographischen Funktionen. Das Ziel war es, die Plattform so zu optimieren, dass sie den höchsten Sicherheitsanforderungen gerecht wird.

4.6 Arbeitspaket 6: Kommunikation und Wissenstransfer

In diesem Arbeitspaket wurden Strategien entwickelt und durchgeführt, um die Ergebnisse des Projekts effektiv zu kommunizieren und Wissen über die Plattform zu verbreiten. Dies umfasste die Erstellung von technischen Publikationen, die Vorstellung der Ergebnisse auf Fachmessen und weiteren Events mit Fachpublikum. Zudem wurde eine Projektwebseite erstellt und gepflegt, die die Konzepte und Vorteile der Sanctuary-Plattform erläutert. Ziel dieses Arbeitspakets war es, die Plattform bekannt zu machen und potenzielle Anwender und Kooperationspartner anzusprechen. Ebenfalls wurde der entwickelte Hypervisor, Peregrine, auf [GitHub](#) veröffentlicht.

4.7 Arbeitspaket 7: Transferkonzeption

Das Ziel dieses Arbeitspakets war es, Verwertungsstrategien für die Sanctuary Plattform zu entwickeln. Dazu wurden potenzielle Anwendungsfelder und Zielmärkte analysiert, finanzielle Vorteile für potenzielle Nutzer berechnet und Kooperationen mit Industriepartnern angestrebt. Darüber hinaus wurden alternative Nutzungsstrategien untersucht, um die Adaption und Integration

der Plattform in verschiedenen Industriezweigen zu fördern und die wirtschaftliche Verwertung sicherzustellen.

5 Ergebnisse des Vorhabens und deren Verwertbarkeit

Im Rahmen des Projektvorhabens konnte die Sanctuary-Plattform entscheidend weiterentwickelt werden, um als flexible Sicherheitsarchitektur für ARM-basierte eingebettete Systeme einsetzbar zu sein. Zu den zentralen Errungenschaften gehört die Entwicklung einer robusten Sicherheitslösung, die eine Vielzahl Software-Komponenten unterschiedlicher Hersteller auf einer einzigen Plattform isolieren kann und damit sowohl Sicherheits- als auch Leistungsanforderungen erfüllt. Zudem wurde die Sanctuary Plattform um die wichtigen Sicherheitsfunktionalitäten Secure Boot und Remote Attestation erweitert und die hierfür notwendige Infrastruktur aufgebaut. Ein weiteres Ergebnis des Projektvorhabens ist die erfolgreiche Portierung der Plattform auf eine Automotive-spezifische Hardware, sowie die Entwicklung eines kompletten Automotive Demonstrators. Auch die Anpassung des Toolings, welche rund um die Konfiguration und das Deployment der Sanctuary Plattform geschaffen wurde, wurde auf den Automotive Anwendungsfall angepasst. Als weitere Ergebnisse des Projektvorhabens sind umfassende Tests der Sanctuary Plattform durchgeführt worden, sowohl in Bezug auf einzelne Komponenten als auch auf deren Integration zu einem Gesamtsystem. Zudem konnte mit dem durchgeführten Security Review der entwickelten Lösung die Qualität und Zuverlässigkeit der Sanctuary Plattform im Projektvorhaben erheblich gesteigert werden. Parallel wurden (Teil-)Ergebnisse auf Messen und Konferenzen vorgestellt, um Industriefeedback einzuholen.

Nach Abschluss des Projektvorhabens Sanctuary2 liegt der Fokus nun auf der wirtschaftlichen Verwertung der Ergebnisse. Bereits im vorherigen Projektvorhaben Sanctuary wurden daher umfassende Analysen verschiedener Märkte eingebetteter Systeme durchgeführt. Für den Automotive-Markt wurde zu dem damaligen Zeitpunkt die größte Relevanz der Sanctuary Plattform ermittelt, weshalb sich das Projektteam in Sanctuary2 zuerst primär auf die Kommunikation mit potenziellen Anwendern in der Automobilebranche fokussierte. Im Laufe des Projekts wurden dann eine Vielzahl von Gesprächen mit Automobilherstellern und Tier-1 Lieferanten aus der Automobilbranche geführt. In den allermeisten Fällen war das Feedback der Konzerne zur Zielsetzung und Umsetzung der Sanctuary Plattform sehr positiv. In zwei konkreten Fällen wurden Anforderungen und Szenarien zum Einsatz der Sanctuary Plattform auf Automotive Steuergeräten diskutiert und eine nachprojektliche Verwertung angestrebt. Leider konnte im Anschluss an das Projektvorhaben kein Vertragsabschluss verzeichnet werden. Als Hauptgrund kann hier die Risikoaversion der Konzerne genannt werden, die es ihnen nicht erlaubte, eine innovative Basis-Software von einem noch sehr jungen Unternehmen zu beziehen und sich damit in gewisser Weise von diesem abhängig zu machen.

Neben der Fokussierung auf den Automotive-Markt wurden im Projektvorhaben jedoch auch alternative Märkte und Anwendungsfelder der Sanctuary Plattform evaluiert. Dabei konnten vor allem die Branchen Raumfahrt und Verteidigung also potenzielle Absatzmärkte für die Sanctuary Plattform identifiziert werden. Begründet werden kann dies vor allem im Raumfahrtbereich mit

dem aktuell neuentstehenden „New Space“ Markt, bei welchem die Kommerzialisierung der Raumfahrt durch privatwirtschaftliche Unternehmen vorangetrieben wird und damit eine zunehmende Verzahnung mit der klassischen Wirtschaft erfolgt. Im New Space Markt entstehen dabei viele neue Geschäftsmodelle, welche neue Cybersecurity-Herausforderungen nach sich ziehen. Im Geschäftsmodell Satellite-as-a-Service beispielsweise werden Satelliten von mehreren Akteuren geteilt, um Kosten zu sparen. Als Folge ergeben sich auf diesen Satelliten durch die Kombination von Software-Komponenten unterschiedlichster Anbieter auf einer Plattform große Vertrauensprobleme, für welche die Sanctuary Plattform mit ihrer Isolationstechnik eine adäquate Lösung bietet. Im Projektvorhaben wurde zudem bereits untersucht, wie auch Teilkomponenten der Sanctuary Plattform individuell genutzt werden können, um das Sicherheitsniveau eines eingebetteten Systems zu erhöhen. Gerade diese Ergebnisse des Projektvorhabens haben bereits Früchte getragen. Nachprojektlich wurden bereits Teile der Sanctuary Plattform in mehreren Raumfahrtprojekten eingesetzt, um innovative Sicherheitslösungen für Satelliten zu entwickeln. In den nächsten Jahren sind hier von Seiten der Europäischen Weltraumagentur ESA mehrere Aktivitäten zum Einsatz von Hypervisoren und Trusted Execution Environments wie sie auch bei der Sanctuary Plattform zum Einsatz kommen geplant. Viele dieser Projekte haben ebenfalls einen starken wissenschaftlichen Anteil, da dort zunächst Security-Designs entwickelt werden sollen (entsprechend einem Technical Readiness Level kleiner vier). Ebenfalls besteht das Ziel, im Rahmen von EU-Forschungskollaborationen (sowohl aus dem universitären als auch dem industriellen Umfeld) innerhalb der nächsten drei Jahre Teile der Sanctuary Plattform weiterzuentwickeln. Hier sind begleitend weitere Veröffentlichungen geplant. Neben der Verwendung in Raumfahrtprojekten ist im nächsten Jahr auch das erste Projekt im Verteidigungssektor geplant, welches direkt auf den Ergebnissen des Projektvorhabens Sanctuary2 aufbaut.

Insgesamt ergeben sich für die Bereiche Raumfahrt und Verteidigung in der Zukunft sehr gute Verwertungsmöglichkeiten für die Sanctuary Plattform. Zum einen wegen der bereits geplanten und in der Ausführung befindlichen Großprojekten in diesen Bereichen, welche alle einen großen Bedarf an Sicherheitslösungen für eingebettete Systeme haben. Zum anderen, weil die geopolitische Lage in Europa, insbesondere nach Beginn des russischen Angriffskriegs auf die Ukraine, auch in Zukunft weitere Investitionen in die Raumfahrt und Verteidigungsindustrie in Europa und die Sicherheit der eingesetzten Systeme zwingend nötig macht.

6 Veröffentlichung der Ergebnisse

Die Ergebnisse des Projekts wurden auf unterschiedliche Weise öffentlich kommuniziert und verfügbar gemacht. Zum einen wurde Öffentlichkeitsarbeit über die Projekt-Webseite geleistet. Auf dieser wurde die Sicherheitsarchitektur und ihre Eigenschaften erklärt und einer breiten Öffentlichkeit zugänglich gemacht. Zudem wurden, teilweise bereits in Phase 1, Blogbeiträge zu einzelnen Detailspekten verfasst und auf der Website veröffentlicht. Zusätzlich wurde eine Video-Präsentation über die Website bereitgestellt, die die Nutzung von Enclaved Computing im Kontext von eingebetteten Systemen erklärt.

Zusätzlich wurde Flyern und Broschüren entworfen, die ähnlich der Projektwebsite, die Lösung und ihre zentralen Eigenschaften und Alleinstellungsmerkmale präsentierten. Diese Flyer und

Broschüren wurden in gedruckter Form bei unterschiedlichen Veranstaltungen an interessierte Personen verteilt bzw. per E-Mail in digitaler Form an Interessierte geschickt.

Weiterhin wurde die entwickelte Lösung auf verschiedenen öffentlichen Veranstaltungen präsentiert, etwa bei Messen oder Vortragsveranstaltungen. Zur Vorstellung der entwickelten Lösung wurde an den folgenden Messen als Aussteller teilgenommen:

- Die Messe it-sa in Nürnberg („Home of IT Security“) ist die größte IT-Security Messe in Europa. Die Kontakte auf der Messe waren zum einen Personen, die selbst im Bereich Cybersecurity tätig sind und an neuen Entwicklungen in dem Bereich interessiert sind. Zum anderen entstanden Kontakte mit Personen, die auf der Suche nach Cybersicherheitslösungen für ihr Unternehmen bzw. Produkt sind.
- Die Messe „Embedded World“ ist eine internationale Messe mit Schwerpunkt eingebettete Systeme. Auf dieser Messe konnte die entwickelte Lösung Fachbesuchern präsentiert werden, wobei der Hauptteil der Kontakte selbst eingebettete Systeme entwickelt und vertreibt oder aber Dienstleistungen rund um die Entwicklung eingebetteter Systeme anbieten.
- Die SPS (Smart Production Solutions) ist eine der wichtigsten Messe im Bereich Industriesteuerung und -automatisierung. Auf der Messe sind viele Hersteller und Anbieter von Industriesteuerungslösungen vertreten, etwa Speicherprogrammierbaren Steuerungen (SPS) oder Edge Gateways. Auf der Messe wurde die entwickelte Lösung mit dem Einsatzzweck in eben diesen Geräten präsentiert.
- Die Space Tech Expo ist die größte B2B-Veranstaltung im Raumfahrtbereich in Europa. Hier wurde die entwickelte Sicherheitsarchitektur als Lösung für Raumfahrzeuge (z.B. Satelliten) präsentiert.

Neben Fachmessen wurde weitere Veranstaltungen genutzt, z.B. Veranstaltungen von Industrieverbänden, um die Lösung einem breiten Publikum bekannt zu machen und Möglichkeiten für die weitergehenden Verwertung zu validieren. Unter anderem wurde bei einer Veranstaltung mit dem Namen „STARTUPS X HESSENMETALL“ die entwickelte Lösung teilnehmenden Unternehmensvertretern aus dem Verband Hessenmetall präsentiert. Weiterhin wurde die Lösung im Rahmen des Accelerators „SpeedUpSecure“, ausgerichtet von ATHENE Startup Hub sowie der drei Partner-Inkubatoren für Cybersicherheit, präsentiert. Dabei gewann der die Präsentation der Sicherheitsarchitektur den ersten Platz.

Weitere Messen und Veranstaltungen wurden als Teilnehmer besucht, wobei diese Besuche genutzt wurden, um Kontakte zu potenziellen Anwendern zu etablieren und weitere Informationen über Marktanforderungen zu gewinnen.

Weiterhin diente die im Projekt erarbeitete Sicherheitsarchitektur als Grundlage für die Durchführung einer Masterarbeit. In der Masterarbeit mit dem Titel „A software architecture enabling secure, reliable on-orbit firmware updates for modern CubeSats“ wurde die Sicherheitslösung von Sanctuary2 mit einem Update-Mechanismus für den Anwendungsfall Satelliten erweitert, wobei die besonderen Bedingungen und Anforderungen hinsichtlich der Datenübertragung bei Raumfahrzeugen in der Konzeptionierung und Implementierung betrachtet wurden. Eine weitere Masterarbeit mit dem Titel „Dynamic Virtual Machine management in mixed criticality

systems on ARM-based embedded platforms“, die ebenfalls auf den Projektergebnissen aufbaut, wurde im Berichtszeitraum begonnen, jedoch erst nach Ende des Projekts abgeschlossen.

Als finaler Baustein bei der Verbreitung der Projektergebnisse wurde die Plattform GitHub genutzt, um einen zentralen Teil der Projektlösung (den Hypervisor Peregrine) Open Source zur Verfügung zu stellen: <https://github.com/SANCTUARY-Systems/Peregrine-Hypervisor>. Die Bereitstellung erlaubt es Anwendern Teile der Technology zu testen und zu nutzen, sowie Forschenden auf den Ergebnissen aufzubauen.

7 Zahlenmäßiger Nachweis

Im Folgenden werden die wichtigsten Position des zahlenmäßigen Nachweises diskutiert. Die Höhe des gesamten verwendeten Budgets für Sanctuary2 betrug 619.032,01 €. Die Mittel für Personal stellen hier mit 87 % den mit Abstand größten Kostenblock dar. Der zweitgrößte Kostenblock umfasst alle für das Projekt angeschafften Arbeitsgeräte, Entwicklungs-Boards, Software-Lizenzen und Demonstratoren und macht 6 % der Gesamtkosten aus. Alle angeschafften Geräte werden im Unternehmen weiterhin für die Weiterentwicklung der Sanctuary Plattform und weitere Forschungsprojekte genutzt. Der dritte Kostenblock, welcher für 4 % der Gesamtkosten verantwortlich ist, umfasst hauptsächlich die Kosten der angemieteten Büroflächen für die Dauer des Projekts. Insgesamt wurde nur ein kleiner Teil der Gesamtfördersumme für die Vergabe von Aufträgen (1,6 %) und Dienstreisen (1,4 %) ausgegeben. Die Dienstreisen erhielten hier hauptsächlich den Besuch und die Ausstellung auf Fachmessen, um die Projektergebnisse potenziellen Anwendern vorzustellen.

Position Bezeichnung	Anteil an Gesamtausgaben	Position Kosten
Vollzeitmitarbeiter	74 %	458.591,56 €
Studentische Hilfskräfte	13%	78.056,87 €
Gegenstände und Verwaltungsausgaben	6 %	38.614,40 €
Mieten und Rechnerkosten	4 %	24.970,50 €
Vergabe von Aufträgen	1,6 %	9.600,00 €
Dienstreisen	1,4 %	9.198,68 €
		619.032,01 €