Sachbericht zum Verwendungsnachweis
Teil I
2024

Verbundvorhaben

RealSec5G

Uniting Realtime Safety and Security in 5G

Gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Konsortialführung: **aconnic system Germany GmbH**	Förderkennzeichen: **01M023022A**
Laufzeit des Vorhabens: von: **01.06.2023** bis: **30.11.2024**	
Berichtszeitraum: von**: 01.06.2023** bis: **30.11.2024**	Datum: **30.06.2025**

Projektpartner:

1. aconnic system Germany GmbH
2. Fraunhofer IPMS

1. Aufgabenstellung und Stand der Technik

Während der aktuelle Stand der 5G-Technologie durch den voranschreitenden Netzausbau und den verstärkten Aufbau lokaler und regionaler 5G-Campusnetze deutlich an Sichtbarkeit gewinnt und zunehmend Einzug in private und industrielle Anwendungsbereiche hält, diskutieren Forscher weltweit sowohl die nächsten Standardisierungsschritte innerhalb zukünftiger 5G-Releases als auch bereits mögliche 6G-Evolutionsschritte, die weit über die aktuellen 5G-Pläne hinausgehen. Vor diesem Hintergrund gilt es, anwendungsgetriebene Safety-Aspekte von Anfang an mitzudenken. In Zukunft wird die 5G/6G-Infrastruktur in Feldern Anwendung finden, welche vorher noch nicht vernetzt waren. Damit kommen neue Anforderungen in Bezug auf Security, Safety und Echtzeitfähigkeiten hinzu, die bislang eher getrennt betrachtet wurden.

Das Projekt “RealSec5G” hat daher erstmals im Rahmen einer Durchführungsstudie erprobt, inwieweit es heute schon möglich ist, die beiden Anforderungen security und safety in Kommunikationsgeräten für 5G/6G-Infrastrukturen umzusetzen. In Folge können neue, zukunftsträchtige Anwendungsfelder durch die beteiligten Projektpartner erschlossen werden.
Die Firmen aconnic (früher albis-elcon) und die Fraunhofer IPMS hatten sich zum Ziel gesetzt, die Anforderungen der funktionalen Sicherheit (safety), in Form von Echtzeitfähigkeit, Redundanz und Übertragungsgarantien sowie der Datensicherheit (security) in Form von Linespeed-Verschlüsselung gleichzeitig in einem kostengünstigen und einfach zu integrierenden System zu kombinieren. Im Projekt wurde dafür durch das Fraunhofer IPMS ein TSN-MACsec Funktionsblock erstmals konzipiert und im Rahmen eines Demonstrators erprobt.

Nach dem Abgleich mit dem Stand der Technik fokussierte sich die aconnic im Projekt auf die Umsetzung des von Fraunhofer konzipierten und entwickelten TSN-MACsec Funktionsblocks in bei aconnic entwickelten Hardware-Demonstratoren für unterschiedliche Datenraten. Die vollständige Integration und Erprobung konnte aufgrund anfänglicher Herausforderungen und mangelnder Zeit am Ende der Projektlaufzeit nicht abgeschlossen werden.

2. Ablauf des Vorhabens

Zur Herstellung einer gemeinsamen Basis zur Erörterung der technischen Fragestellungen im Projekt wurden im Konsortium und mit weiteren Inputgebern zuerst Angriffsszenarien definiert, denen das Gesamtsystem standhalten soll. Dieses Angreifer-Modell wurde einer eingehenden Analyse bezüglich notwendiger sicherheitsrelevanter Eigenschaften unterzogen. Der aktuelle Stand der Technik und die relevanten Standards wurde in dieser Analyse berücksichtigt. Eine Schwachstellenanalyse wurde durchgeführt. Im Anschluss wurden dann funktionale, nicht-funktionale, sowie die Sicherheit betreffende Anforderungen analytisch abgeleitet.

Um zu einer Architektur des Gesamtsystems zu gelangen, wurden zuerst separate Entwürfe für die jeweilige Integration der IP-Cores untereinander und der Integration von IP-Cores (größere Funktionsblöcke und Subsysteme) allgemein auf das Basissystem erstellt. Im Anschluss wurden beide Entwürfe zu einem gemeinsamen Systementwurf integriert.
Zusätzlich wurden Vorschläge erarbeitet, den Softwarelebenszyklus insbesondere im Bereich Sicherheit und Performance an aktuelle Anforderungen u.a. ISO 27001 anzupassen. Dabei stand Automatisierung im Zusammenhang mit der Softwareerstellung und permanenter Code- und Schwachstellenanalyse für verschiedene Systeme (embedded Linux, FPGA) im Mittelpunkt.

Auf Basis des Architekturmodells wurden die bestehenden Funktionsblöcke einzeln betrachtet, neue Konzepte bzgl. funktionale Sicherheit und Datensicherheit umgesetzt und integriert. Die Funktionsblöcke wurden zu einem neuen TSN-MACsec Funktionsblock zusammengeführt. Zusätzlich wurden funktionale Erweiterungen des MACsec für Datenraten bis 100Gbit/s betrachtet und in der Projektlaufzeit bis 10Gbit/s entwickelt. Dann erfolgte bei aconnic die

Evaluierung und Definition der möglichen Hardware bzw. Architektur für die geplante Implementierung des IP-Cores in die spätere Demonstratorplattform. Auch die Aspekte beim Zusammenwirken von TSN und MACsec wurden analysiert und die potenzielle Umsetzung theoretisch erarbeitet bzw. für die spätere Implementierung spezifiziert.

Auf Basis des erarbeiteten Anforderungskatalogs an das Gesamtsystem wurden danach Anforderungen an die zu nutzende Hardwareplattform abgeleitet. Dies umfasst Eval-Board, FPGA-Plattform, sowie die Schnittstelle zwischen beiden. Danach wurde eine Marktanalyse bzgl. in Frage kommender und verfügbarer Eval-Boards und FPGA-Plattformen durchgeführt und eine Auswahl getroffen. Nach der Inbetriebnahme beider Komponenten wurde die FPGA-Plattform in den Datenpfad des Eval-Boards integriert, um den hohen Durchsatz des FPGAs nutzbar zu machen. Schließlich wurde der integrierte IP-Core auf dem Eval-Board nach dem festgelegten Architekturmodel integriert.

aconnic hat daraufhin die Vorarbeiten für die geplante Integration des Fraunhofer IPMS IP-Cores auf die ausgewählten Hardwareplattformen durchgeführt. So wurden entsprechende Hardware/ Architekturen für die Integration evaluiert, bewertet und ausgewählt sowie ein Abgleich der vorhandenen Plattformen bzw. deren Möglichkeiten (u.a. Typ und Größe der FPGA-Plattform) mit den Anforderungen der IP-Cores durchgeführt.
Auch wurden die theoretischen Ansätze bzw. Optionen zur Integration in Bezug auf die effizientesten Datenpfade und die Steuerung des IP-Cores durch den übergeordneten Controller (CPU) bzw. dessen Unterstützung durch Treiber oder Softwarepakete erarbeitet und dokumentiert. Ebenso erfolgte die Betrachtung der Zusammenarbeit von TSN und MACsec, um bei der geplanten Integration die bestmögliche Performance erzielen zu können.

Danach wurde die Testumgebung zur Evaluation der Gesamtlösung bereitgestellt und Testszenarien sowie zu testende Qualitätsparameter festgelegt und entsprechende Testwerkzeuge gewählt. Darauffolgend wurde der Teststand aufgebaut. Dabei wurde insbesondere eine erstellte Firmware, die auf den FPGA-Boards zusätzlich implementierten Prozessoren lief, verwendet und die umfangreiche Testgestaltung und Protokollierung zulässt.

Anhand des Testbeds konnten Evaluierungen zum Zusammenwirken der Security- und TSN-Komponenten durchgeführt und die Performance bewertet werden.

3. Wesentliche Ergebnisse

Es wurden unterschiedliche Konzepte zur Realisierung der gestellten Aufgabe untersucht und dann durch diverse Optimierungen der bislang vorhandenen und ins Projekt eingebrachten IP-Core ein überarbeitetes System geschaffen, das den neuen IP-Core auch für höhere Geschwindigkeiten bis 10 Gbit/s nutzbar macht und die Aspekte für TSN wie Echtzeitfähigkeit berücksichtigt. Das wurde dann auch in der Folge mit dem Testbed durch Messungen entsprechend nachgewiesen. Es wurden Ansätze für Geschwindigkeiten bis 100 Gbit/s erarbeitet.

Im Rahmen der Erstellung des Demonstrators wurden mehrere potenzielle Hardware-Plattformen für 1 Gbit/s, 10 Gbit/s und 100 Gbit/s für die Nutzung der entwickelten IP-Cores untersucht und notwendige zukünftige Erweiterungen bzw. Optimierungen dokumentiert. Es konnte jedoch keine vollständige Integration der IP-Cores durchgeführt werden.

Der Nachweis der Funktion der IP-Cores konnte im Rahmen des Testbeds mit FPGA-Boards erbracht werden. Die im Projekt angestrebte Realisierung eines kombinierten MACsec-TSN-Cores konnte erfolgreich umgesetzt und im Testbed evaluiert werden.

Sachbericht zum Verwendungsnachweis
Teil II
2024

Verbundvorhaben

RealSec5G

Uniting Realtime Safety and Security in 5G

Gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Konsortialführung: **aconnic system Germany GmbH**	Förderkennzeichen: **01M023022A**
Laufzeit des Vorhabens: von: **01.06.2023** bis: **30.11.2024**	
Berichtszeitraum: von: **01.06.2023** bis: **30.11.2024**	Datum: **30.06.2025**

Projektpartner:

1. aconnic system Germany GmbH
2. Fraunhofer IPMS

Abschluss-Sachbericht Teil II

RealSec5G – Uniting Realtime Safety and Security in 5G

Autoren:	Ronny Priemer / René Glaß / Marco Dietrich / Jörg Hopfe Dr. Andreas Heinig / Dr. Alexander Noack
Projekt Manager:	Ronny Priemer/ Dr. Alexander Noack
Firmen:	aconnic system Germany GmbH Fraunhofer IPMS

Berichtszeitraum:	01.06.2023 – 30.11.2024
Version:	A
Datum:	30.06.2025
FKZ:	01M023022A

Inhaltsverzeichnis

Abbildungsverzeichnis

Projektablauf

Aufgabenstellung

Während der aktuelle Stand der 5G-Technologie durch den voranschreitenden Netzausbau und den verstärkten Aufbau lokaler und regionaler 5G-Campusnetze deutlich an Sichtbarkeit gewinnt und zunehmend Einzug in private und industrielle Anwendungsbereiche hält, diskutieren Forscher weltweit sowohl die nächsten Standardisierungsschritte innerhalb zukünftiger 5G-Releases als auch bereits mögliche 6G-Evolutionsschritte, die weit über die aktuellen 5G-Pläne hinausgehen. Vor diesem Hintergrund gilt es, anwendungsgetriebene Safety-Aspekte von Anfang an mitzudenken. In Zukunft wird 5G/6G-Infrastruktur in Feldern Anwendung finden, welche vorher noch nicht vernetzt waren. Damit einhergehend werden neue Anforderungen an die Kommunikationsnetze gestellt. Besonders bei Cyber-Physischen Systemen (CPS), in denen mechanische Komponenten über Netzwerke und moderne Informationstechnik miteinander verbunden sind, wird der Aspekt der funktionalen Sicherheit (safety) von großer Bedeutung sein. CPS können autonom agieren und die für den Betrieb benötigten Daten miteinander austauschen. Derartige Systeme, welche direkten Einfluss auf die physische Welt haben, müssen jederzeit fehlerfrei arbeiten, da sonst Menschen oder Güter und Anlagen zu Schaden kommen können. Der Safety-Aspekt lässt sich dabei direkt in die Anforderung an das Kommunikationsnetz übersetzen, indem Datenpakete deterministisch, d. h. zu exakt definierten Zeitpunkten, und mit garantierten Bandbreiten übertragen werden. Diese Eigenschaft ist für Spezialfälle, vor allem in sogenannten Closed-Loop-Anwendungen, bereits erfüllt. Für offene Architekturen wie 5G/6G-Netze, gilt dies im Allgemeinen jedoch noch nicht, obwohl jene Datensicherheit (security) garantieren müssen, d. h. sowohl Nutz- als auch Verkehrsdaten innerhalb eines Netzes nur sicher verschlüsselt und integritätsgeschützt übertragen werden dürfen. Beide Eigenschaften wurden in der Vergangenheit getrennt voneinander betrachtet. Zukünftige 5G/6G-Architekturen für bestimmte kritische Anwendungsgebiete müssen jedoch zwingend beide Aspekte gemeinsam und gleichzeitig erfüllen. Beispiele für neue safety- und gleichzeitig security-kritische Anwendungsgebiete sind die Überwachung und Steuerung von Bahn- und Energienetzen, Fabrikanlagen und der vernetzte Einsatz von autonomen Fahrzeugen, Robotern und Cobots.

Das Projekt “RealSec5G” möchte erstmals im Rahmen einer Durchführungsstudie erproben, inwieweit es heute schon möglich ist, die beiden Anforderungen security und safety in Kommunikationsgeräten für 5G/6G-Infrastrukturen umzusetzen. In Folge können neue, zukunftsträchtige Anwendungsfelder durch die beteiligten Projektpartner erschlossen werden.

Die Firmen aconnic (früher albis-elcon) und die Fraunhofer IPMS haben sich zum Ziel gesetzt, die Anforderungen der funktionalen Sicherheit (safety), in Form von Echtzeitfähigkeit, Redundanz und Übertragungsgarantien sowie der Datensicherheit (security) in Form von Linespeed-Verschlüsselung gleichzeitig in einem kostengünstigen und einfach zu integrierenden System zu kombinieren. Aktuell werden diese Anforderungen nur getrennt betrachtet. Im Projekt sollte dafür durch das Fraunhofer IPMS ein TSN-MACsec Funktionsblock erstmals konzipiert und im Rahmen eines Demonstrators getestet werden.

Das Systemkonzept des Vorhabens basiert auf der Kombination echtzeitfähiger, deterministischer TSN-Baugruppen (funktionale Sicherheit) des Fraunhofer IPMS mit einer effizienten, die Bandbreite ausreizenden Verschlüsselung (Datensicherheit) auf Basis von MACsec (TSN-MACsec Funktionsblock). MACsec ist ein standardisiertes Protokoll, dass auf OSI-Layer 2 arbeitet und transparent verschlüsselt. Es schützt darüber hinaus die Integrität eines gesamten Ethernet-Frames, unabhängig von darüberliegenden Protokollen. Diese hoch performante Behandlung von Echtzeitkommunikation ist nur mit Hilfe von Spezialhardware möglich. Dabei handelt es sich um FPGA-Plattformen oder FPGA-Erweiterungskarten, welche integrierte Schaltkreise nutzen, deren interne Schaltungsstruktur im Gegensatz zur festverdrahteten Logik bei ASICs flexibel ist und auch mehrfach verändert („programmiert“) werden kann.

Die benötigte Funktionalität wird dann nicht langsam in Software ausgeführt, sondern direkt in Hardware umgesetzt und ist damit sehr schnell und energieeffizient. Die wiederverwendbare Zusammenstellung bestimmter Funktionalitäten mit definierten Eingangs- und Ausgangsschnittstellen werden IP-Cores genannt und stellen eigenständige Module dar, die am Fraunhofer IPMS entwickelt werden.

Die aconnic fokussierte sich im Projekt auf die Umsetzung des von Fraunhofer konzipierten und entwickelten gehärteten TSN-MACsec Funktionsblocks in bei aconnic entwickelten Hardware-Demonstratoren für 1 Gbit/s und 10 Gbit/s Datenraten und den Abgleich mit dem Stand der Technik. Zusätzlich unterstützte aconnic bei der Definition von Use-Cases und der Spezifikation von Systemblöcken und übernahm im Weiteren die Integration des IP Cores in den Demonstrator von aconnic und plante das Zusammenspiel mit dem Demonstrator des Fraunhofer Instituts.

Um die Basis für gesicherte und schwer angreifbare Netzwerkverbindungen schaffen zu können, deren Basis ein stabiles und sicheres Betriebssystem und eine Entwicklungs-Tool-Chain mit wenig bis gar keinen Schwachstellen ist, wurde im Rahmen des Projekts auch eine Analyse der aktuellen Softwareentwicklungsumgebung und Entwicklungsprozesse und deren Optimierung in Richtung einer hoch-verfügbaren und sicheren Umgebung angegangen.

In seiner Rolle als Konsortialführer übernahm aconnic auch die Koordination und Berichterstattung nach Innen und Außen im Projekt.

Voraussetzungen

Ziel des Projekts “RealSec5G” war es, die Anforderungen der funktionalen Sicherheit (safety), in Form von Echtzeitfähigkeit, Redundanz und Übertragungsgarantien sowie der Datensicherheit (security) in Form der Linespeed-Verschlüsselung gleichzeitig in einem kostengünstigen und einfach zu integrierenden System zu erfüllen. Aktuell werden diese Anforderungen nur getrennt betrachtet.

Ergänzend zu den oben beschriebenen Forschungsaktivtäten um den TSN-MACsec Funktionsblock werden im Projekt “RealSec5G” Konzepte erforscht, funktional sichere Aspekte bei gleichzeitiger Verfügbarkeit von Datensicherheit (Verschlüsselung und Integrität) und Performance umzusetzen und so einen gehärteten TSN-MACsec Funktionsblock zu entwickeln. Hierbei liegt der Fokus auf der Berücksichtigung bzw. Einfluss von Safety Artefakten und deren Behandlung. Basieren werden diese Arbeiten auf einem Hardware/Software Co-Design Ansatz. Zieldatenraten für den funktional sicheren TSN-MACsec Funktionsblock sind 1 Gbit/s und 10 Gbit/s.

Zusätzlich sollen Konzepte und Umsetzungslösungen bzgl. funktionaler und Datensicherheit für MACsec mit Datenraten bis zu 100 GBit/s erforscht und ausgewählte Varianten in einem FPGA Demonstratoraufbau umgesetzt und evaluiert werden.

Am Fraunhofer IPMS existieren bereits prototypische IP-Cores für einzelne TSN-Funktionalitäten und auch für MACsec , das bisher jedoch keinerlei Echtzeit-Eigenschaften erfüllt. Ziel dieses Projekts soll es nun sein, erstmals die beiden IP-Cores für TSN und MACsec zu kombinieren und echtzeitfähig zu machen, hohe Datenraten bis 100 Gbit/s zu unterstützen sowie neue Konzepte für funktionale Sicherheit zu entwickeln und auf einer praxistauglichen, vergleichsweise kostengünstigen FPGA-Plattform (Off-The-Shelf-Baugruppe) in einer realistischen Testumgebung zu erproben und zu evaluieren.

Das technologische Gesamtkonzept besteht darin, die oben genannten IP-Cores des Fraunhofer IPMS so anzupassen und miteinander zu integrieren, dass die kombinierten Anforderungen (Funktionale Sicherheit und Datensicherheit) immer erfüllt werden können. In einem nächsten Schritt sollte das Resultat von aconnic auf einer konkreten, praxistauglichen und für zukünftige Anwendungsfälle geeigneten Hardwareplattform integriert und im Testfeld in Betrieb genommen werden. Die hierbei notwendige

Betriebssystemintegration soll sicherstellen, dass z. B. alle notwendigen Hardwareschnittstellen angesprochen werden können und insbesondere die hoch performante Behandlung von Datenpaketen sichergestellt wird. Dazu sollte ein praxisnahes Testbed im Labor aufgebaut (TRL 4) werden.

Das Testbed wird aus mehreren Versuchsaufbauten bestehen. Einerseits werden zwei identische 100 Gbit/s-Geräte miteinander verbunden, um Anwendungsfälle im Backbone-Bereich zu testen, und andererseits werden mehrere (mind. 3) 10 Gbit/s-Geräte in einem Netz verschalten, um Anwendungsfälle in offenen Netzen zu untersuchen. Alle Geräte werden jeweils mit FPGA-Beschleunigern ausgestattet und führen die integrierten IP-Cores aus.

Zusätzlich soll erreicht werden, dass die funktionale Sicherheit über den Lebenszyklus der Software gewährleistet bleibt.

Planung und Ablauf

Für das Projekt war eine Laufzeit von 18 Monaten gemäß nachfolgender Übersicht vorgesehen.

AP		Leiter	Beteiligte		Projektmonat																
			AE	IPMS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Projektmanagement und Dissemination**																					
1.1	Organisation/Betrieb von Meetings und digitalen Kollaborationswerkzeugen	AE	x																			
1.2	Berichte, Veröffentlichungen, Beiträge in Fachmagazinen und bei Konferenzen	AE	x																			
2	**Anforderungsdefinition**																					
2.1	Definition zu betrachtender Angriffsszenarien, Angreifermodellierung und Sicherheitsanalyse	AE	x	x																		
2.2	Anforderungsanalyse auf Basis der definierten Angriffsszenarien und der Ergebnisse aus Angriffsmodellierung als auch Sicherheitsanalyse	AE	x	x																		
3	**Entwurf Systemkonzept**																					
3.1	Entwicklung eines Konzeptes zur Kombination aus TSN und MACsec IP-Cores zu einem Funktionsblock	AE	x	x																		
3.2	Konzeptionierung von Umsetzungsvarianten für zusätzliche integrierte Funktionen zur Unterstützung der funktionalen Sicherheit als auch der Datensicherheit	AE	x	x																		
3.3	Analyse einzelner Umsetzungsvarianten und Auswahl geeigneter Lösungsansätze unter Berücksichtigung der Anforderungen/Lastenheft und Entwicklung eines abgestimmten Architekturmodells	AE	x	x																		
4	**TSN/MACsec**																					
4.1	Integration des MACsec IP Cores in die einzelnen TSN IP Cores für Endpunkt, Switched Endpunkt und Switch.	IPMS		x																		
4.2	Anpassungsentwicklung der MACsec Integration in einen Multiport TSN Switch unter Berücksichtigung der verfügbaren Datenraten pro Port und des Ressourcenbedarfs im FPGA. TSN-MACsec Funktionsblock	IPMS	x	x																		
4.3	Analyse des Einflusses von Safety Artefakten im MACsec IP Core und Behandlung dieser durch Entwicklung von Zusatzfunktionen	IPMS		x																		
4.4	Analyse des Einflusses von Safety Artefakten in den TSN IP Cores und Behandlung dieser durch Entwicklung von Zusatzfunktionen, die einen funktional sicheren Betrieb ermöglichen sollen	IPMS		x																		
4.5	Abstimmung der Safety Funktionen für den Einsatz im TSN-MACsec Funktionsblock und Integration in das entwickelte Design	IPMS	x	x																		
4.6	Entwicklung von Konzepten für MACsec mit Datenraten von bis zu 100Gbit/s und Integration in einem FPGA	IPMS	x	x																		
5	**Integration IP-Cores**																					
5.1	Ableitung Anforderungen an Eval-Board und FPGA-Plattform aus Ergebnissen von AP2	AE	x	x																		
5.2	Marktanalyse und Auswahl verfügbarer Eval-Boards und FPGA-Plattformen	AE	x																			
5.3	Enablement FPGA-Plattform und ausgewähltes Eval-Board	AE	x																			
5.4	Integration FPGA-Plattform in Datenpfad auf Eval-Board	AE	x	x																		
5.5	Integration der IP-Cores auf FPGA-Plattform auf Eval-Board	AE	x	x																		
6	**Aufbau Testbed**																					
6.1	Bereitstellung der Testumgebung, Auswahl Testwerkzeuge, Testszenarien	AE	x	x																		
6.2	Aufbau, Vernetzung der Komponenten	AE	x	x																		
7	**Evaluation**																					
7.1	Quantitative Betrachtungen: Erreichte Latenz/Bandbreite (zu Kosten) evaluieren	IPMS	x	x																		
7.2	Qualitative Betrachtungen: Benutzbarkeit, Integrierbarkeit in eigene SW-Prozesse, Flexibilität	IPMS	x	x																		
7.3	Evaluation erreichbarer Sicherheitsniveaus	IPMS	x	x																		
7.4	Betrachtung neuer Use Cases	IPMS	x																			

Abbildung 1: RealSec 5G Gantt-Chart

Die Umsetzung des Projektes erfolgte gemäß Projektplan. Aufgrund von aufgetretenen Verzögerungen auf Seiten aconnic konnten unter Beibehaltung der ursprünglichen Projektlaufzeit einige Tätigkeiten nicht durchgeführt bzw. nicht abgeschlossen werden. Dazu gehörte u.a. die vollständige Integration des IP-Cores in die Demonstratorumgebung.

Folgende Meilensteine wurden erreicht:

Meilen-stein	Monat	Beschreibung	Erreicht (ja/nein/ teilweise)	Erreichter Stand
M1	6	**Systemkonzept auf Basis Anforderungs-katalog vorhanden.**	**ja**	**Anforderungen dokumen-tiert und Systemkonzept er-stellt**
M2	12	Prototypische Implemen-tationen vorhanden, so dass getestet werden kann.	teilweise	Prototypische Implementierung auf der FPGA-Plattform
M3	15	Prototypische Implemen-tation in Testbed über-führt, Evaluation kann beginnen.	teilweise	Prototypische Implementierung in das Testbed überführt.

Wissenschaftlicher und technischer Stand zu Beginn

Um im Projekt “RealSec5G” den Anforderungen der funktionalen Sicherheit gerecht zu werden, wird das Konzept Time Sensitive Networking (TSN) eingesetzt. TSN ist eine standardisierte und offene Erweiterung der etablierten Ethernet-Technik. Diese wird durch TSN um Mechanismen für Zeitsynchronisation, deterministische Übertragung von Datenpaketen, Quality-of-Service-Garantien (QoS) und resiliente Datenpfade erweitert. TSN macht es möglich, auf derselben physischen Infrastruktur sowohl klassische Best-Effort-Kommunikation als auch deterministische Echtzeitkommunikation durchzuführen und ist folglich wesentlich leistungsfähiger, zuverlässiger und resilienter als bisherige Lösungen. TSN hat damit das Potential den Wildwuchs heutiger proprietären Kommunikationsstandards abzulösen. Bisher findet TSN jedoch vor allem in echtzeitkritischen geschlossenen Systemen wie Motor- und Getriebesteuerungen, Anlagensteuerungen oder Industrierobotern erste Anwendung. So wird zum Beispiel das Zusammenspiel von Industrienetzwerken in der Feldebene (OT) und Büronetzwerken (IT) vom Sensor bis in die Cloud ermöglicht. Besonders innerhalb solcher hyperlokalen Netze gibt es keine zu separierenden unterschiedlichen Sicherheitsdomänen. Eine Verschlüsselung der Verkehrsdaten ist daher klassischerweise nicht notwendig, sodass das Thema Datensicherheit in der Vergangenheit bei TSN-Anwendungen nur proprietär adressiert wurde.

Gleichzeitig existieren bereits leistungsfähige Verschlüsselungslösungen, die es vermögen, selbst Multigigabit-Verbindungen vollständig zu verschlüsseln. Diese finden vor allem im Backbone oder Backhaul-Bereich in Weitverkehrsnetzen, wie z. B. 5G-Infrastrukturen Anwendung. Die Lösungen sind auf den Parameter der maximal erreichbaren Bandbreite optimiert, d. h. sie versuchen den Datendurchsatz über die verschlüsselte Verbindung möglichst nah an die physisch über die jeweilige Verbindung mögliche Bandbreite (linespeed) heranzubringen. Der Parameter Latenz (Sendezeit für ein Datenpaket) spielt dabei eine untergeordnete Rolle. Genaugenommen werden keine Zusagen zur Zustellzeit einzelner Pakete gemacht. Dies nennt man den Best-Effort-Ansatz. Dementsprechend können im worst case exponentiell höhere Übertragungszeiten entstehen als im Durchschnitt erwartet. Solche Linespeed-Verschlüsselungslösungen sind derzeit teure und proprietäre Spezialanwendungen bestimmter Anbieter und für die adressierten Anwendungen in der Regel nicht geeignet. Stattdessen bilden Insellösungen typischerweise eine Einheit aus vom Anbieter bereitgestellter Hardware und Software. Dies erschwert es für Systemintegratoren, wie die aconnic system Germany GmbH, sie in ihre Systeme zu integrieren.

Time Sensitive Networking ist ein wichtiger Baustein für die Umsetzung moderner industrieller Konzepte wie dem Internet of Things (IoT) und wird auch als das „Rückgrat der Industrie 4.0“ betitelt. Als ein Set von Ethernet Sub-Standards von der IEEE 802.1 TSN Task Group entwickelt, schmilzt TSN durch die stetige Adaption und Optimierung der bestehenden Ethernet-Standards die Grenzen zwischen Informationstechnologien (IT) und operativen Technologien (OT). Dabei ermöglicht TSN unterschiedlichen Protokollen die Nutzung einer gemeinsamen Infrastruktur über das gesamte Netzwerk, indem kritischer Echtzeitdatenverkehr und unkritischer Datenverkehr so optimiert werden, dass Echtzeit-Charakteristik und optimale Performance der Datenübertragung gleichzeitig möglich werden.

Grundsätzlich eignet sich der Einsatz von TSN überall dort, wo ein vorhersagbares, deterministisches zeitliches Systemverhalten gefordert ist. Daher rücken insbesondere industrielle Anwendungen, Steuerungen, Messwerterfassungen, Embedded Systems, Sicherheitssysteme, Audio- und Videoverarbeitung und Telekommunikationsanwendungen in den Vordergrund. Diese vielfältigen Anwendungsszenarien setzen jedoch sehr heterogene Echtzeitansprüche voraus und erfordern flexible Lösungsansätze. Um diverse Anforderungen an Latenz, Jitter und Zuverlässigkeit parallel zu gewährleisten, sind unter dem gemeinsamen Namen TSN eine Vielzahl von Standards definiert, die präzise Zeitsynchronisation, garantierte niedrige Latenz, Hochverfügbarkeit bzw. API und Ressourcenverwaltung adressieren. Die folgenden Standards können hierbei als Basisstandards gesehen werden:

- Zeitsynchronisation (IEEE 802.1 AS, 802.1AS 2020)
- Traffic-Shaping (IEEE 802.1 Qav und Qbv)
- Frame Preemption (IEEE 802.3br und IEEE 802.1Qbu)

Durch die Nutzung der TSN-Standards ist die echtzeitfähige Kommunikation in einem einheitlichen Netzwerk auch mit dem Einsatz von Infrastrukturkomponenten wie Endpunkten mit Switch-Funktionalität (2-Ports) möglich, ohne zusätzliche spezialisierte Hardware, etwa proprietäre Feldbussysteme und die entsprechenden Gateways, zu benötigen. In Folge können Herstellerabhängigkeiten vermieden werden. TSN erlaubt den zeitgleichen Transport verschiedener Datenströme (Streams) in einem gemeinsamen Netzwerk. Dabei können diese Streams unterschiedliche Echtzeitanforderungen haben. Werden für Anwendungen beispielsweise extrem niedrige Latenzen und minimaler Jitter benötigt, stellen sich spezielle Anforderungen an die Netzwerkteilnehmer.

Aufgrund des breiten Spektrums an TSN-Funktionen lässt sich die Integration am besten auf der Basis eines Field Programmable Gate Array (FPGA) realisieren. Im Vergleich zu integrierten Schaltkreisen (ICs), bei denen viele Funktionalitäten vorgegeben sind, kann FPGA flexibel programmiert werden. Das Logikgatter (Gate Array) kann so konfiguriert werden, dass es komplexe digitale Funktionen erzeugt. Zu den Vorteilen von FPGAs gegenüber ICs gehören:

- deutlich geringere Entwicklungskosten
- Kürzere Implementierungszeiten
- Flexibel erweiterbar und umprogrammierbar

Zusammenarbeit mit anderen Stellen

Die Rolle des Konsortialführers wurde von der aconnic system Germany GmbH übernommen. Gemeinsam mit Fraunhofer IPMS hat die aconnic zu Beginn des Projekts einen Kooperationsvertrag unterzeichnet, der insbesondere die Nutzungsrechte und die Verwertung der Ergebnisse regelt. Die Zusammenarbeit erfolgt gemäß einer klaren Aufteilung der Verantwortlichkeiten, die auf den jeweiligen Kompetenzen der Projektpartner basiert.

Im Rahmen des ersten Arbeitspakets wurde das Konzept erfolgreich erarbeitet, die Verantwortlichkeiten festgelegt sowie Schnittstellen und Austauschformate definiert. Regelmäßige Abstimmungstreffen wurden durchgeführt, um den Austausch untereinander zu fördern. Zwischen den beteiligten Industriepartnern und dem Fraunhofer IPMS wurden im Verlauf der Projektbearbeitung neue Kooperationsnetzwerke etabliert und die Ergebnisse im Rahmen von diversen Messen und Veranstaltungen präsentiert, um auch über die Projektlaufzeit hinaus die erzielten Ergebnisse verwerten zu können.

Der von Fraunhofer IPMS assoziierte Partner Teleconnect GmbH (TCD) hat das Konsortium mit seiner Expertise und industriellen Fachkenntnis aus Anwendersicht begleitet. Dies geschah insbesondere zu Beginn des Projekts bei der Anforderungsdefinition und am Ende bei der Evaluation. Das Unternehmen hat das Vorhaben aus eigenem Interesse auf freiwilliger Basis und ohne jegliche Verpflichtung unterstützt.

aconnic hat im Projekt die Firma 256bytes.net UG zur Beratung bei der Anpassung der Softwareprozesse, speziell im Bereich des automatisierten Testens unterschiedlicher Eigenschaften von embedded Systemen, sowie bei der Umsetzung bestimmter den gesamten Softwarelebenszyklus betreffender Paradigmen (embedded DevOps) in den Arbeitspaketen 3 und 6, beauftragt.

Die bei der Firma Kernkonzept GmbH ursprünglich geplanten beratenden Aufgaben im Zusammenhang mit dem Enablement von Hardwareplattformen sowie der Performance von Embedded-Linux-Systemen und Implementierungsleistungen wurden aufgrund der bereits berichteten Anfangsschwierigkeiten im Projekt in Abstimmung mit dem Projektträger nicht durchgeführt und stattdessen auf eine Realisierung im klassischen Stil fokussiert, um möglichst viele der inhaltlichen Kernthemen des Projekts umsetzen zu können.

In Abstimmung mit dem Projektträger wurde stattdessen die aus dem Fraunhofer IPMS in 2024 ausgegründete Firma KiviCore beauftragt, um die aconnic mit Ihrer spezifischen Expertise im Bereich von MACsec und TSN insbesondere bei der Beschreibung der späteren Umsetzung des MACsec-TSN-IP-Cores beratend zu unterstützen.

Durchgeführte Arbeiten und Ergebnisse
Arbeitsergebnisse

Erzielte Ergebnisse von aconnic

Anforderungsdefinition :

Bei der Anforderungsdefinition hat aconnic das Fraunhofer IPMS mit Einschätzungen und Erfahrungen aus der industriellen Praxis als Anwender bzw. zukünftiger Anbieter von Übertragungsgeräten mit inkludierter Verschlüsselung unterstützt und sich in das Thema theoretisch und analytisch eingearbeitet, um insbesondere für die weitere Projektbearbeitung spezifisches Know-How im Bereich der Verschlüsselungstechnologien im Zusammenhang mit TSN aufzubauen.

Es wurden u.a. folgende Standards betrachtet and analysiert:

- IEEE 802.1AE: MACsec
- IEEE 802.1X: MACsec key agreement / Extensible authentication protocol
- IEEE 802.1AR secure device identity
- RFC 3748 Extensible authentication protocol
- RFC 5216 EAP-TLS
- IEEE 802.1AS
- IEEE 1588

Es wurde die in diesem Zusammenhang relevante Terminologie erarbeitet und dokumentiert sowie verschiedene use-case nochmal betrachtet und analysiert. Dabei wurden folgende potenziellen use cases als später praxisrelevant herausgearbeitet:

- MACsec als verschlüsselte Transportnetz-Verbindung über synchrone L2-Netzwerke (WAN)
- MACsec als verschlüsselte P2P Verbindung zwischen zwei LAN-Endpunkten in z.B. TSN Netzen im industriellen Umfeld (Echtzeitanwendung) z.B. in 5G Campus Netzen.

Auf dieser Basis wurde dann der prinzipielle Aufbau der MACsec Verschlüsselung (secure connections) sowie deren Zusammenwirken mit den einzelnen Instanzen der verschlüsselten Verbindung und deren Zusammenwirken mit äußeren Systemen wie z.B. dem Authentication Server erarbeitet und entsprechend dokumentiert.

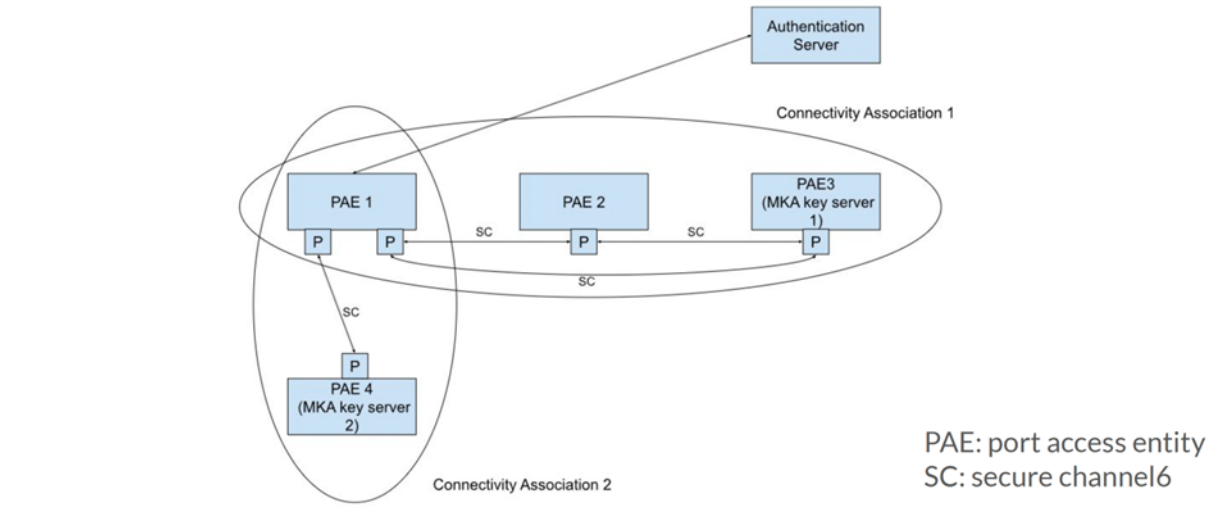

Abbildung 2: secure connections

Ebenso wurde das Zusammenwirken der einzelnen Key-Elemente, die für den Aufbau und die permanente Sicherstellung von verschlüsselten Verbindungen essentiell notwendig sind, arbeitet und deren Abhängigkeiten wie folgt dokumentiert.

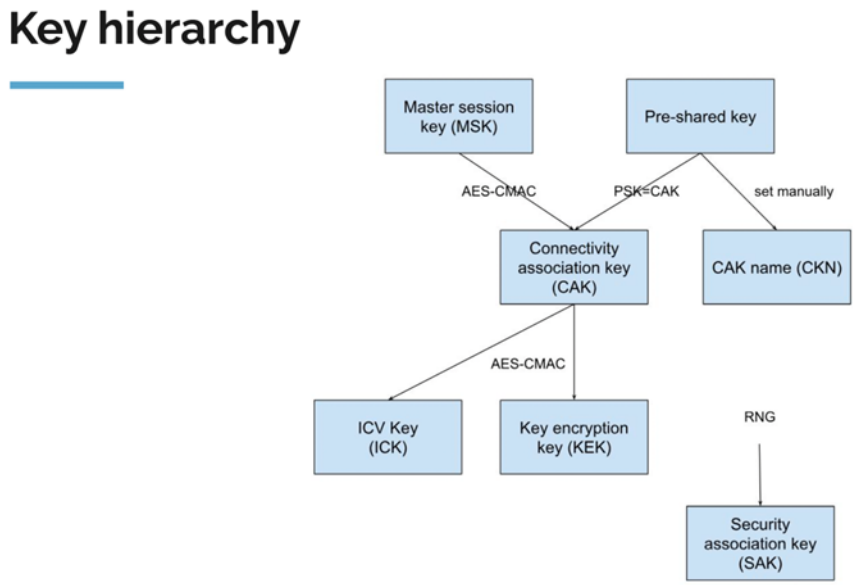

Abbildung 3: key hierarchy

Auf Basis dieses Grundverständnisses konnten dann zwei konkrete Gerätekonzepte (Plattformen) bezüglich deren Eignung für MACsec Verbindungen in Verbindung mit TSN sowie die angestrebte Integration der IP-Cores untersucht und bewertet werden, wie in den nachfolgenden Kapiteln dargestellt wird.

Entwurf Systemkonzept

Erstes Gerätekonzept (untersuchte Plattform #1)

Für die spätere Übernahme des IP-Cores in die Hardwareplattform der Demonstratorplattform wurde als erstes ein potenzielles Gerätekonzept auf Basis einer Marvell Architektur herausgesucht und analysiert. Dafür wurde eine 1 Gigabit Plattform für L2 Metro-Netze verwendet, in der wie im folgenden Bild dargestellt ein FPGA zur potenziellen Aufnahme des IP-Cores integriert ist. Die Analyse ergab, dass dieser FPGA sich nicht direkt im Datenpfad befindet und er bereits für andere Aufgaben verwendet wird. Da der FPGA aber mit 1 Gbit/s an den Hauptprozessor angebunden ist, wird aber eine Erweiterung trotz der genannten Einschränkungen als möglich angesehen. Weiterhin ergab die Analyse, dass diese Plattform aufgrund der Integration von SyncE und PTP auch prinzipiell für einen Einsatz in TSN-Netzen geeignet erscheint.

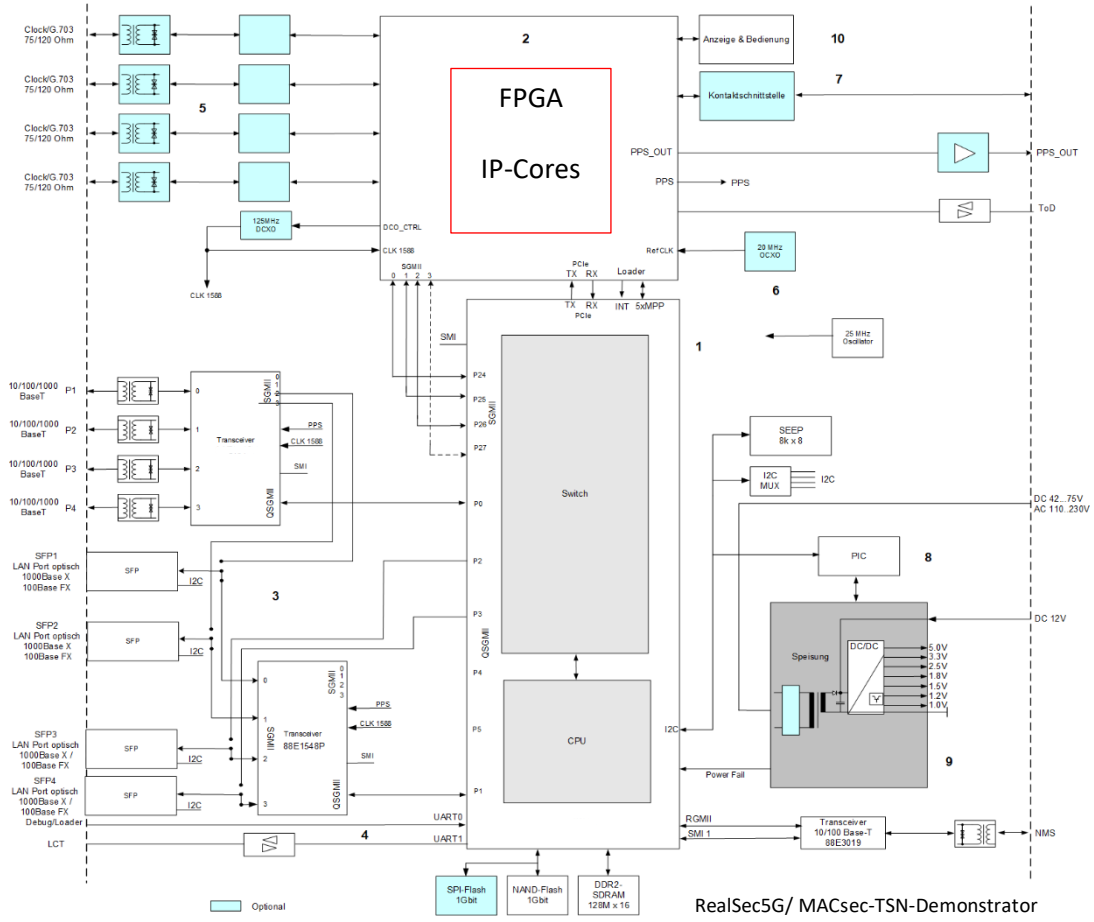

Abbildung 4: Untersuchte Plattform #1

Zweites Gerätekonzept (untersuchte Plattform #2)

Als alternatives Gerätekonzept wurde ein System untersucht, welches auf einer 10G Router/Switch-Plattform MACsec mit TSN potenziell auch ohne FPGA realisieren könnte. Bei der Analyse wurde herausgearbeitet, dass der in der nachfolgenden Abbildung dargestellte FPGA nicht performant an den Hauptprozessor (Network Processor) angebunden ist, um damit 1 Gbit/s oder 10 Gbit/s verschlüsselte Verbindungen zu realisieren. Allerdings verfügt diese Plattform bzw. der Network Prozessor über eine frei programmierbare Hardwarebeschleunigung (date plane), die prinzipiell für die Aufnahme modifizierter IP-Cores geeignet erscheint. Auf der betrachteten Plattform wäre daher eine Portierung des IPMS IP-Cores in die programmierbare Data-Plane denkbar. Dies konnte aber im Rahmen des Projektes nicht

im Detail untersucht werden. Auf dieser Idee aufbauend wurden weitere mögliche use-cases abgeleitet und Ideen zur softwareseitigen (Kernel-Treiber, API, IPC-Mechanismen, Open Source Module, 3rd Party-Module) Systemeinbindung abgeleitet.

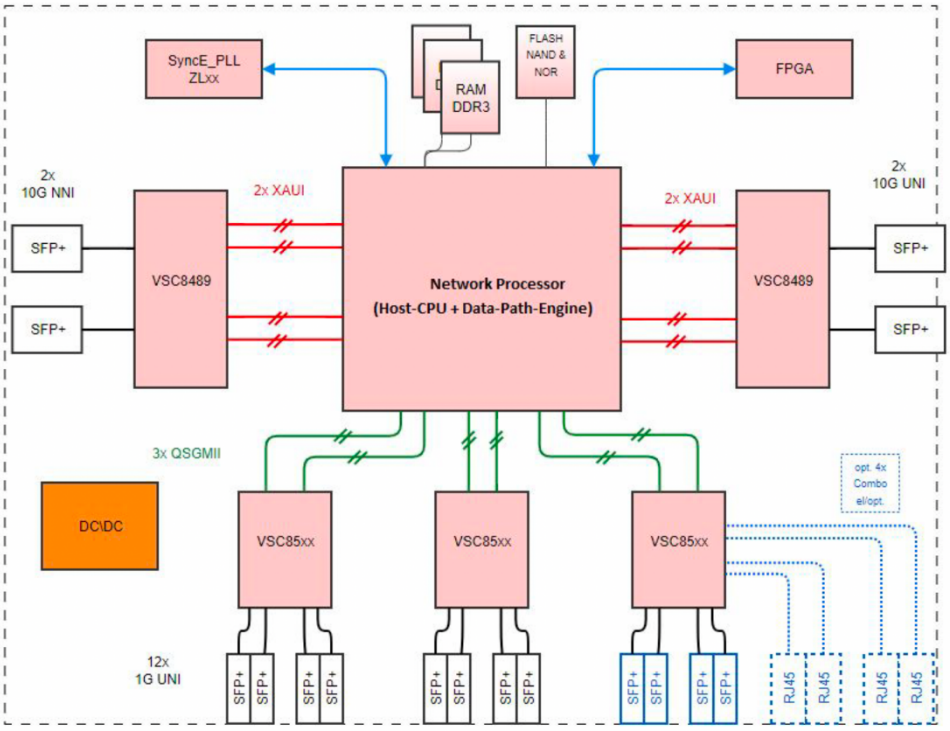

Abbildung 5: Untersuchte Plattform #2

TSN & MACsec

Bezüglich der Echtzeitfähigkeit von MACsec Verbindungen wurden Untersuchungen bzgl. der Herausforderungen von PTP-Übertragungen als einen wesentlichen Bestandteil von TSN-Netzen über MACsec-Verbindungen durchgeführt.

Zur Einführung in die Thematik erfolgten am Anfang zunächst Untersuchungen zu den relevanten Standards für die Zeitsynchronisation mittels PTP.

PTP Overview

IEEE1588-2002 (PTPv1) https://ieeexplore.ieee.org/document/1048550
IEEE1588-2008 (PTPv2) https://ieeexplore.ieee.org/document/4579760
IEEE1588-2019 (PTPv2.1) https://ieeexplore.ieee.org/document/9120376

Version	Release Time	Change	Compatibility
1588v1 (IEEE 1588-2002)	2002	-	-
1588v2 (IEEE 1588-2008)	2008	1588v2 has the following changes over 1588v1: • Provides higher precision. Hardware timestamping is defined to achieve sub-microsecond-level precision. • Implements faster Sync packet transmission. • Introduces the transparent clock (TC) model. • Uses shorter PTP packets and supports new packets such as unicast negotiation packets and P2P delay packets. • Uses type-length-value (TLV) extension to enhance protocol features and functions.	Incompatible with 1588v1
1588v2.1 (IEEE 1588-2019)	2019	1588v2.1 has the following changes over 1588v2: • Provides wider compatibility, allowing a network to provide different time for different applications. • Provides higher security. • Provides the performance monitoring function.	Compatible with 1588v2, but incompatible with 1588v1

Abbildung 6: Übersicht über die zu betrachtenden PTP-Standards
Danach erfolgte die Erarbeitung und Dokumentation potenzieller Einflussfaktoren auf die Echtzeitfähigkeit von PTP in MACsec verschlüsselten Verbindungen.

PTP on MACsec links

- Integrity / Authenticity
  - Timestamp frames not manipulated
  - Authentic link partner
  - Replay protection
- Confidentiality
  - Encrypted payloads
- Implications:
  - PTP Payload (including timestamp) has to be encrypted/decrypted!
  - Adding headers and trailers

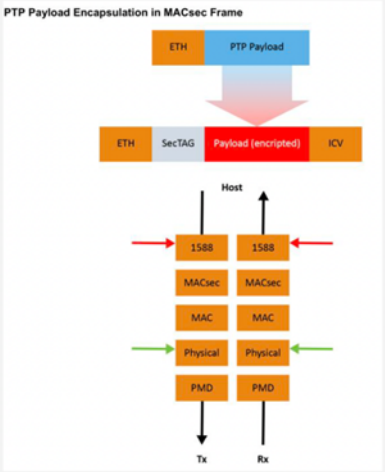

Abbildung 7: PTP und MACsec
Als besonders kritisch wurden dabei die Parameter wie packet delay und packet delay variation herausgearbeitet und der Schwerpunkt der anschließenden Analyse darauf gelegt.

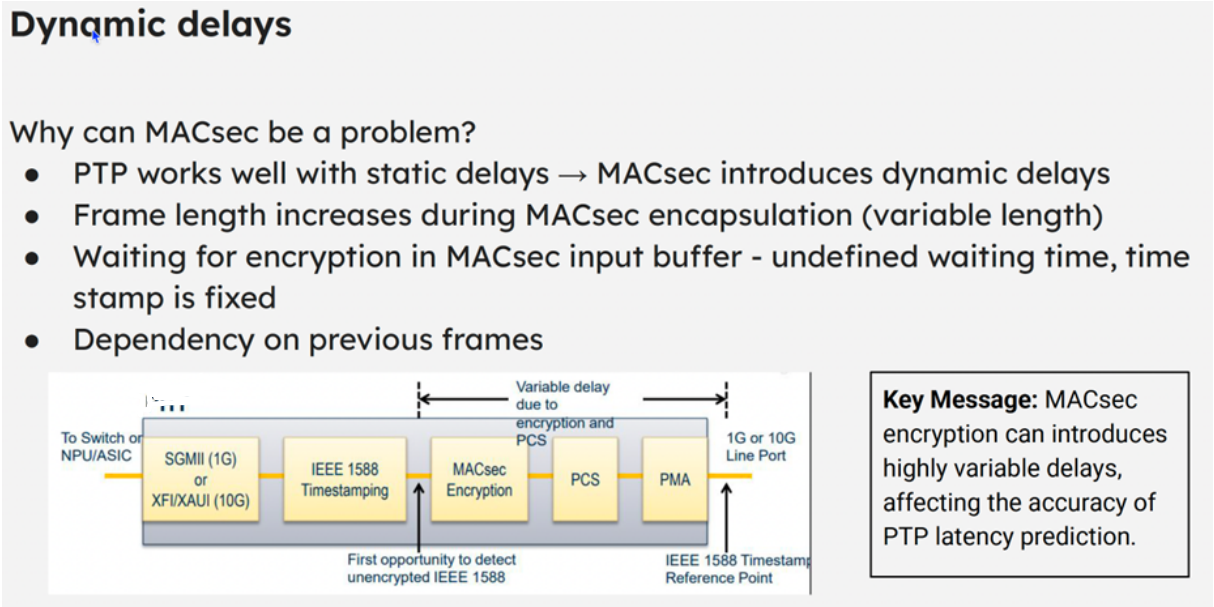

Abbildung 8: Herausforderungen von dynamischem Delay für PTP

Ebenso wurde die der Einfluss des dynamischen Delays von MACsec auf z.B. die Zeitsynchronisierung gemäß IEEE 802.1AS als ein Profil von PTP in besonders zeitkritischen TSN-Netzen angeschaut und bewertet und versucht, entsprechende Maßnahmen zur Schaffung einer Vereinbarkeit von MACec und TSN zu erarbeiten.

Dabei stellte sich ein möglicher Lösungsansatz mittels Delay Kompensation in den time stamps als potenziell wirksam heraus und wurde entsprechend für sie spätere Implementierung dokumentiert.

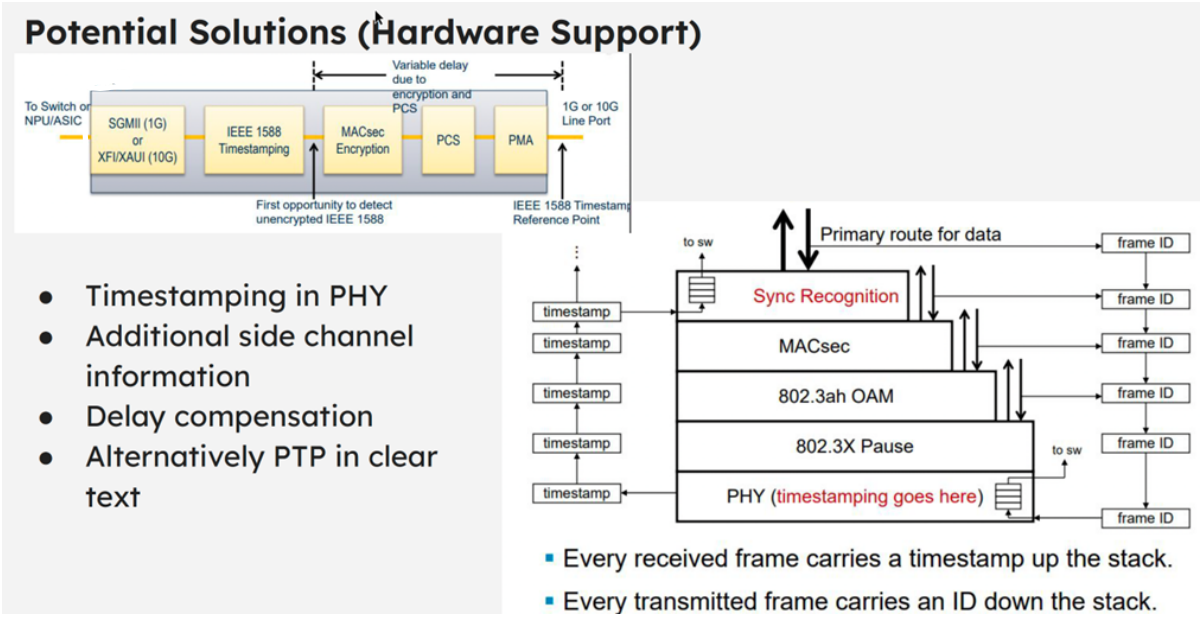

Abbildung 9: Potenzieller Lösungsansatz zur Delay Kompensation

Integration von IP-Cores

Daraufhin wurden beide untersuchten Plattformen auch nochmal hinsichtlich Ihrer Eignung für die Integration der IP-Cores sowie der Vereinbarkeit von MACsec und TSN bewertet und Lösungsansätze zur potenziellen Integration erarbeitet.

Erstes Gerätekonzept (untersuchte Plattform #1)

Die erste (1 Gbit/s Switch) Plattform bietet für die Integration von 1 Gbit/s MACsec in Verbindung mit TSN beste Voraussetzungen, da sie über eine performante 1 Gbit/s Verbindung von der CPU zu FPGA verfügt und auch TSN relevante Komponenten wie SyncE und PTP besitzt.

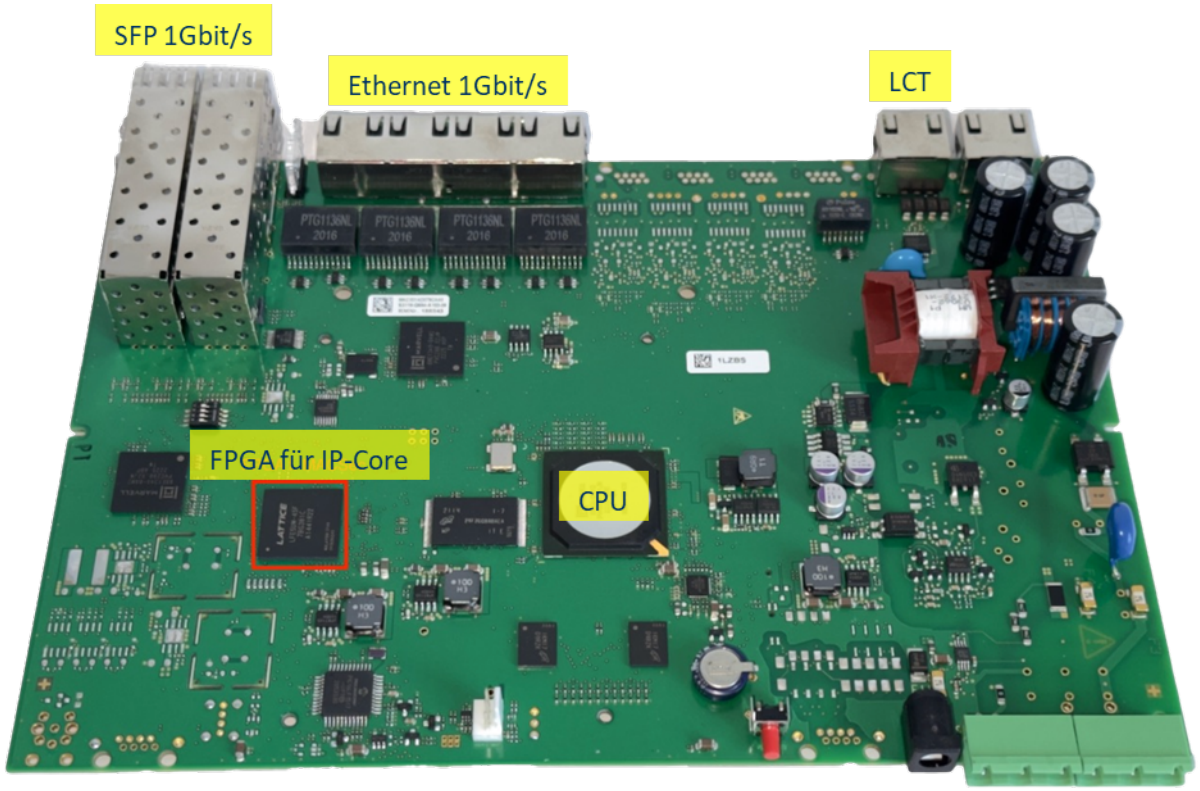

Abbildung 10: Untersuchte Plattform #1

Es wurde herausgearbeitet, dass für das Speichern von sensitiven Informationen wie Keys oder Zertifikaten wesentliche Hardwarekomponenten wie ein TPM2.0 Chip nicht auf dem aktuellen Design verfügbar sind und dieser bei geplanter Nachnutzung zu ergänzen sind.

Ebenso wurden weitere auf dieser Architektur basierender 10 Gbit/s und 100 Gbit/s Plattformen betrachtet und die notwendigen Anpassungen wie die Integration performanter Datenleitungen zwischen CPU und FPGA und die Integration der Sicherheitsfunktion mittels TPM2.0 dokumentiert.

Zweites Gerätekonzept (untersuchte Plattform #2)

Auch bei der zweiten (10 Gbit/s Router) Plattform erfolgte die Analyse und Bewertung.

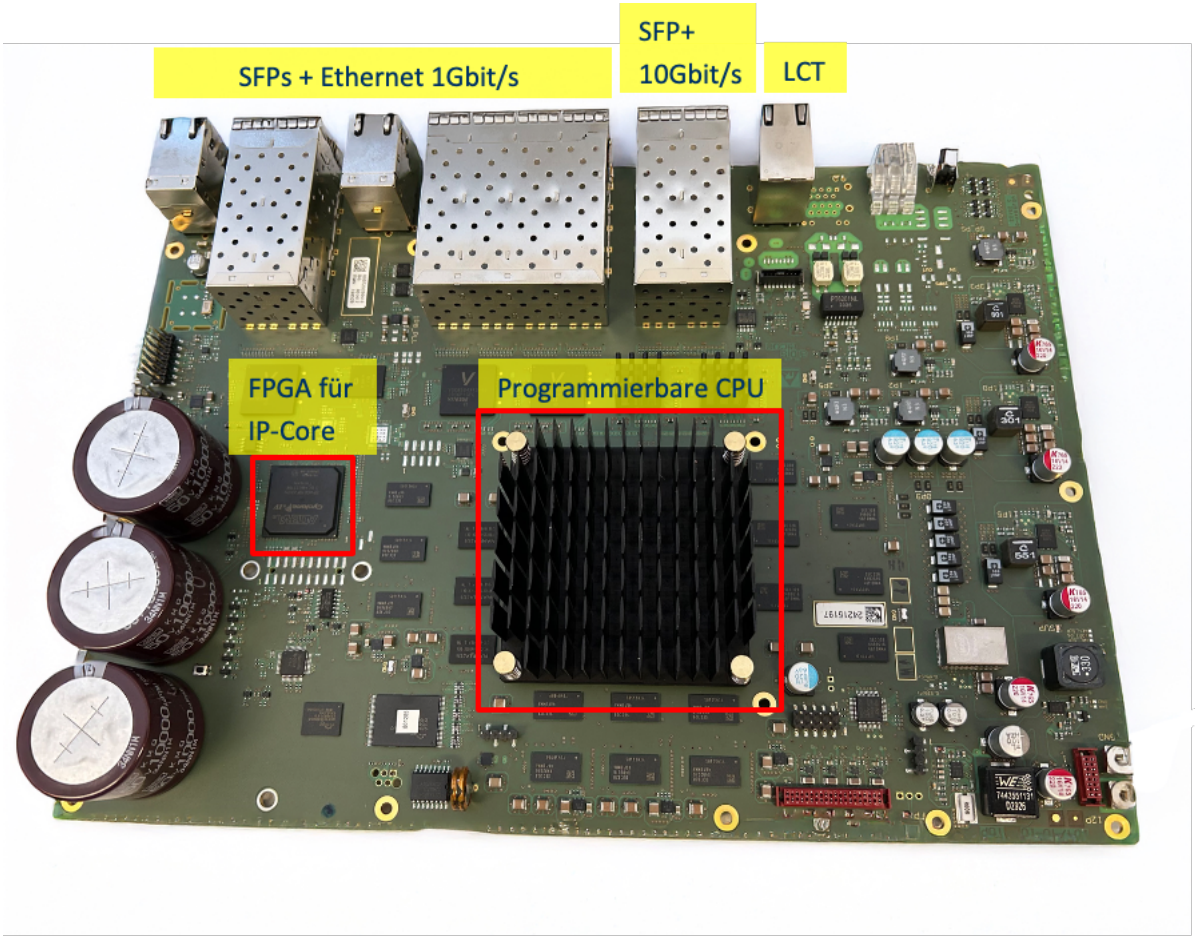

Abbildung 11: Untersuchte Plattform #2

Bezüglich dieser Plattform wurde herausgearbeitet, dass diese grundsätzlich für 10 Gbit/s MACsec Verschlüsselung und durch Hardwarekomponenten für SyncE und PTP in Verbindung mit TSN nutzbar ist. Der aktuell hier eingesetzte FPGA ist momentan mit einer zu geringen Datenleitung an die CPU angebunden und auch von der Größe und Leistungsfähigkeit nicht ausreichend genug, um die Anforderungen an Datendurchsatz und Eignung für den MACsec-TSN-IP Core zu erfüllen.

Es wurde eine weitere theoretische Möglichkeit untersucht, um die in der CPU befindlichen programmierbaren Hardware-Kerne (48 Stück) für die Integration von IP-Cores nutzbar zu machen. Diese theoretische Möglichkeit konnte jedoch im Rahmen des Projektes nicht mehr umgesetzt werden.

Softwareentwicklungsprozess und sichere Entwicklungsumgebung

Unter der Annahme, dass eine ausreichende funktionale Sicherheit in kritischen Systemen zukünftig nicht ausschließlich durch die zugrunde liegenden Techniken und Implementierungen erreicht werden kann, muss zu jeder Zeit ein höchstmöglicher Stand an funktionaler Sicherheit über den gesamten Lebenszyklus einer Software oder eines Systems gewährleistet werden. Dies muss durch Tests und permanente Ermittlung von Parametern fortlaufend verifiziert werden und kann nur durch klar definierte und nachvollziehbare Prozesse entlang des Softwarelebenszyklus und durch Automatisierung erreicht werden.

Diese Prozesse müssen für jegliche Software verfügbar sein. Das gilt zum einem für Embedded-Linux-Systeme aber auch für FPGAs.

Es muss somit eine Entwicklungsumgebung vorhanden sein, welche diese Prozesse unterstützt und höchstmögliche Datensicherheit bietet.

Diesem generischen Prozess müssen alle produkt-spezifischen Prozesse zugrunde liegen. Ziel war es, einen sicheren, transparenten und performanten Prozess für die verschiedenen Systeme zu entwerfen.

Folgende Randbedingungen wurden für den Prozess festgelegt:

- Möglichst viele Prozessschritte automatisieren
- Einzel-Prozessschritte müssen im Lebenszyklus der SW wiederholt ausführbar sein
- Fehler müssen möglichst frühzeitig erkannt werden
- Automatisierte Dokumentation inkl. Dashboards muss vorhanden sein
- Anwendbar für embedded-Linux Systeme und FPGA

Es wurde nachfolgender Prozess für den Softwarelebenszyklus erarbeitet:

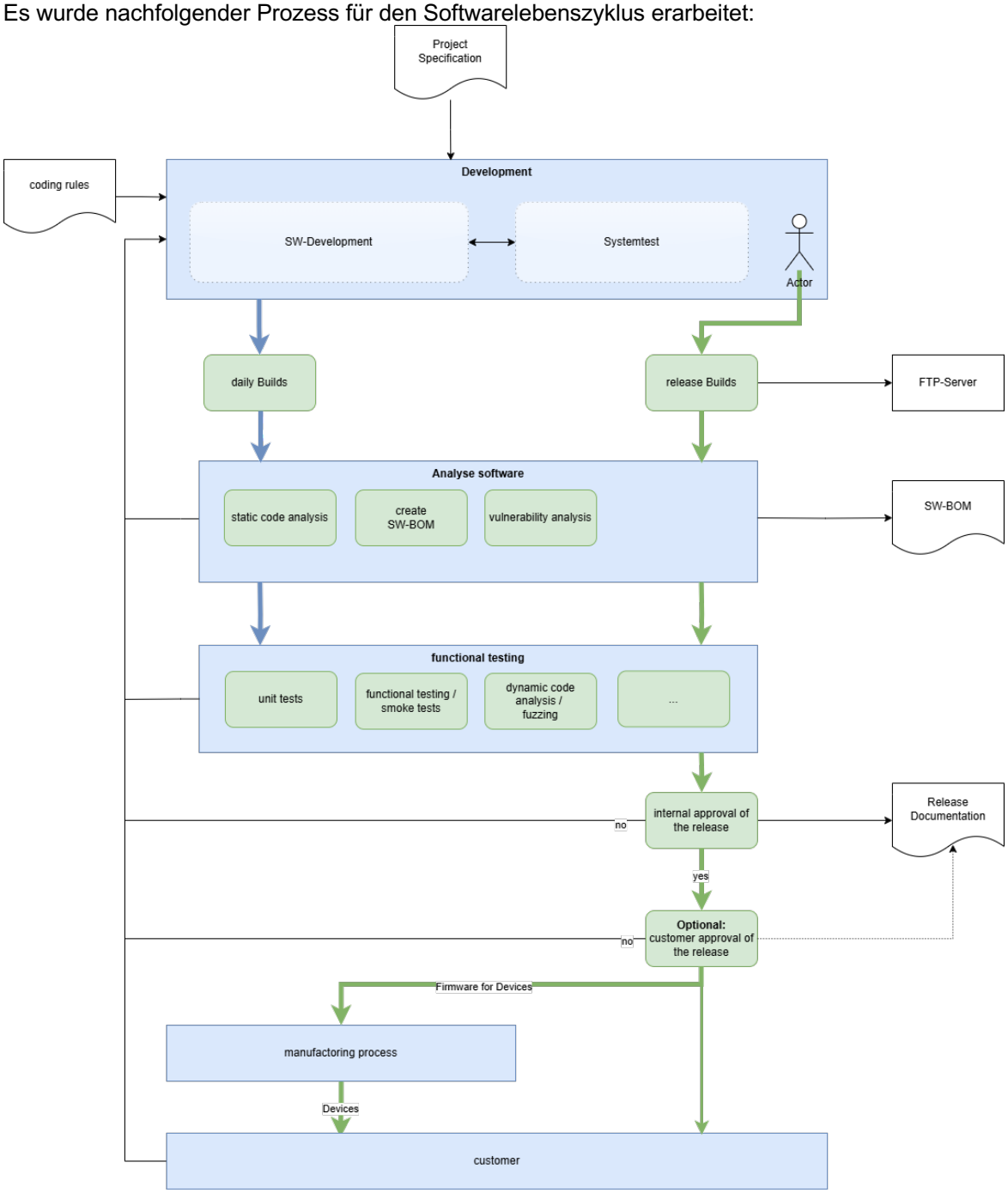

Abbildung 12: Prozess Softwarelebenszyklus

Der Schwerpunkt wurde auf die Software-Analyse bereits während der Entwicklungsphase gelegt. Statische Code-Analysen müssen über verschiedene Tools ausgeführt werden. Eine Schwachstellen -Analyse für bekannte Open-Source Module und auch für eigene Module muss Bestandteil sein. Die ISO 27001 fordert letztendlich eine SW-BOM, welche regelmäßig erzeugt werden muss.

Zusätzlich sind kontinuierliche funktionale Tests zu berücksichtigen.

Neben den eigentlichen Prozessen ist es weiterhin notwendig, die Umgebung, auf der die prozessunterstützenden Tools ausgeführt werden, abzusichern. Hierfür wurde ein Systemkonzept erstellt, welches die gesamte Entwicklungsumgebung zum einen nach außen komplett absichert und trotzdem gute Wartungs- und Erweiterungsmöglichkeiten bietet. Kern ist eine leistungsstarke Firewall inkl. der notwendigen Konfiguration. Alle Prozesskomponenten laufen virtualisiert auf Proxmox-Servern. Das deployment

aller Funktionen erfolgt zentralisiert. Ein Monitoring der automatisierten Prozesse rundet das Konzept ab.

Erzielte Ergebnisse von IPMS

TSN-SE

Time-Sensitive Networking (TSN) ist ein standardisiertes Protokoll, das die deterministische Übertragung von Daten in Ethernet-Netzwerken ermöglicht. Es spielt eine entscheidende Rolle in Anwendungen mit hohen Anforderungen an geringe Latenz und hohe Zuverlässigkeit, wie beispielsweise in der Automatisierungstechnik, der Fahrzeugkommunikation sowie in der Audio- und Videoübertragung.

TSN integriert verschiedene Mechanismen, darunter Zeitstempelung, Bandbreitenreservierung und Priorisierung von Datenströmen, um sicherzustellen, dass kritische Daten rechtzeitig und ohne Unterbrechungen übertragen werden. Diese Techniken fördern die Interoperabilität und Effizienz in komplexen Netzwerkinfrastrukturen und unterstützen die Realisierung von Industrie 4.0-Anwendungen.

Das Protokoll funktioniert durch die Kombination mehrerer Technologien, die darauf abzielen, eine vorhersehbare und zuverlässige Netzwerkkommunikation zu gewährleisten. Zunächst erfolgt eine zeitliche Synchronisation aller Geräte im Netzwerk, häufig unter Verwendung des Precision Time Protocol (PTP).

Darüber hinaus werden Datenströme priorisiert, sodass zeitkritische Informationen vorrangig behandelt werden. TSN implementiert Mechanismen zur Bandbreitenreservierung, um sicherzustellen, dass ausreichend Netzwerkressourcen für die Übertragung dieser wichtigen Daten zur Verfügung stehen.

Ein weiteres wichtiges Element ist die Nutzung von Zeitschlitzen, die es ermöglichen, Daten in definierten Zeitfenstern zu senden. Dies reduziert Kollisionen und Verzögerungen und gewährleistet eine deterministische Übertragung, die insbesondere für Echtzeitanwendungen in der Automatisierungstechnik und Fahrzeugkommunikation unerlässlich ist.

Der vom Fraunhofer IPMS entwickelte TSN-SE IP Core ist ein Modul, das Time-Sensitive Networking für die vollduplexe Punkt-zu-Punkt-Ethernet-Kommunikation unterstützt.

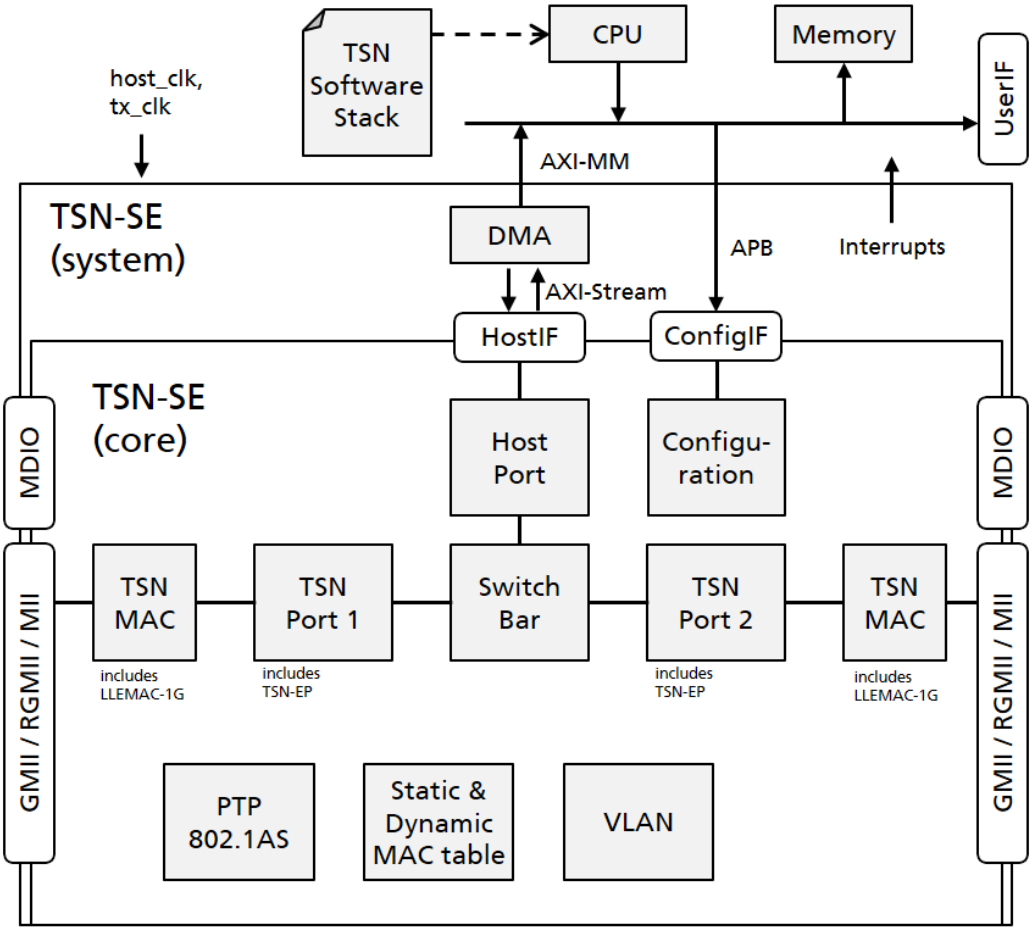

Abbildung 13: IPMS TSN-SE Baugruppe

Der IP-Core umfasst die TSN-Ports, den Content Addressable Memory (CAM) und die Media Access Control (MAC). Er bietet umfassende Hardware-Unterstützung für Ethernet-Bridging gemäß dem Standard IEEE 802.1Q-2018. Für eine präzise Zeitsynchronisation, die den Anforderungen des Standards IEEE 802.1AS entspricht, ist eine Interaktion mit der Software erforderlich. Der IP-Core integriert zudem zwei Instanzen des TSN-EP IP sowie des LLEMAC-1G IP, die ebenfalls vom Fraunhofer IPMS entwickelt und gepflegt werden.

Time Sensitive Networking (TSN) stellt eine Reihe von Standards dar, die für die deterministische Kommunikation über Ethernet-Netzwerke konzipiert sind. Der TSN Switched Endpoint unterstützt die folgenden Standards:

- Bridged und Bridged Networks (IEEE 802.1Q)

Zusätzlich deckt der integrierte Sub-IP-Core TSN-EP folgende Standards ab:

Zeitsynchronisierung (IEEE 802.1AS)

- Traffic Shaping/Scheduling (IEEE 802.1Qav, IEEE 802.1Qbv)
- Frame Preemption (IEEE 802.3br, IEEE 802.1Qbu)
- Ethernet-Kommunikation auf MAC-Ebene (IEEE 802.3)

TSN-EP Unterbaugruppe

Der IP-Core setzt sich aus mehreren Untermodulen zusammen, die für die Zeitsynchronisation, den Datentransfer und die Ethernet-Kommunikation verantwortlich sind. Er bietet umfassende Hardwareunterstützung für die Zeitsynchronisation gemäß dem Standard IEEE 802.1AS. Für eine präzise Zeitsynchronisation ist eine Interaktion mit der Software erforderlich. Der IP-Core unterstützt sowohl TX- als auch RX-Zeitstempel. Zudem besteht die Möglichkeit, eine Echtzeituhr (RTC) zu integrieren, oder externe Zeitstempel zu nutzen, was den Aufbau eines Mehrportsystems mit einer gemeinsamen lokalen Zeit ermöglicht.

Der IP-Core unterstützt eine konfigurierbare Anzahl von Warteschlangen für den Datentransfer, die zwischen 2 und 8 liegen kann. Bei Aktivierung erfolgt der Datentransfer basierend auf Priorität, Guthaben oder in Echtzeit. Der auf Guthaben basierende Shaper-Algorithmus wurde durch den Standard IEEE 802.1Qav (jetzt Teil von IEEE 802.1Q-2014) eingeführt, während der zeitplanende Shaper durch den Standard IEEE 802.1Qbv definiert wurde. Diese Implementierungen sind darauf ausgelegt, eine hohe Präzision und geringe Latenz bei der Planung gemäß diesen Standards zu gewährleisten.

Darüber hinaus implementiert der IP-Core Frame-Preemption gemäß dem Standard IEEE 802.3br, der eine Unterschicht definiert, die das Mischen von Express-Datentransfer mit unterbrechbarem Verkehr unterstützt. Er erfüllt auch die Anforderungen des Standards IEEE 802.1Qbu, der Frame-Preemption für Brücken und überbrückte Netzwerke spezifiziert. Dies umfasst die Zuordnung von Datentransfersklassen zu einem Frame-Preemption-Status (Express oder unterbrechbar) sowie das Verhalten der Datenverkehrsleittechniken im Zusammenhang mit unterbrechbarem Datentransfer.

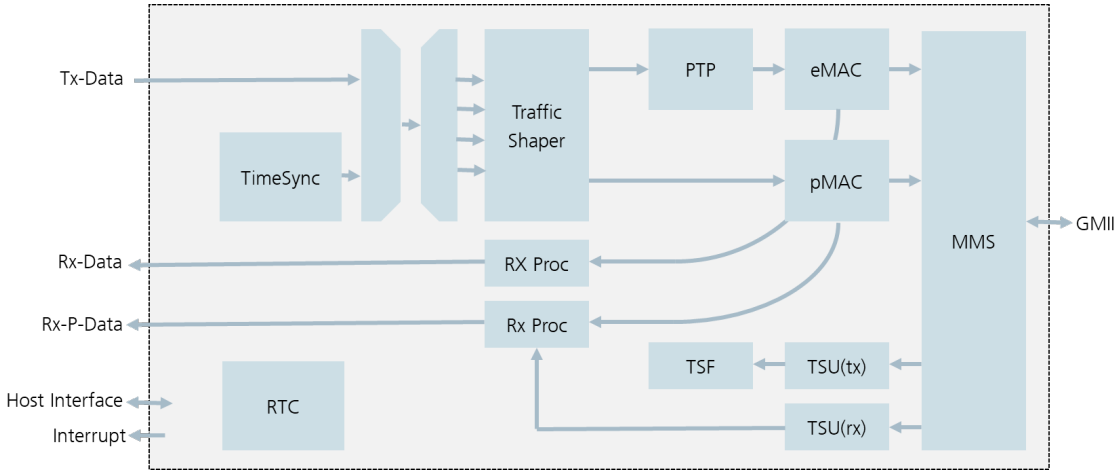

Abbildung 14: IPMS TSN-EP Baugruppe

LLEMAC-1G/ LLEMAC-10G

Die Media Access Control (MAC)-Baugruppe operiert auf der OSI-Schicht 2, auch bekannt als Sicherungsschicht. Eine Ethernet-MAC ist über eine medienunabhängige Schnittstelle, wie beispielsweise GMII, mit einem Ethernet-PHY verbunden. Die MAC fügt einem zu übertragenden Frame die Präambel, den Start Frame Delimiter (SFD) und die Frame Check Sequence (FCS) hinzu und entfernt diese Elemente von empfangenen Frames.

Jeder Ethernet-Frame muss mindestens 64 Oktetts von der Destination Address (DST) bis zur FCS enthalten. Die Präambel und der SFD zählen dabei nicht mit. Sollte ein Host-Controller einen Frame übertragen wollen, der kürzer als die erforderliche Mindestgröße ist, fügt die MAC Füllbytes (0x00) hinzu, um die erforderliche Länge zu erreichen.

Die maximale Größe eines Ethernet-Frames ist abhängig von der Art des Frames, wie Basis-, Q-Tag- oder Envelope-Frames. Zusätzlich zur Standardobergrenze gemäß IEEE 802.3 existieren auch nicht standardisierte Jumbo-Frames, die eine maximale Größe von 9000 Nutzlastoktetten aufweisen können.

Jeder Ethernet-Frame enthält zwei Oktette, die als Länge/Typ bezeichnet werden. In der ersten Version von Ethernet beinhalteten diese Oktette die Länge der Nutzdaten. In der heutigen Version (Ethernet Version 2) dienen sie als Kennung für den Frame-Typ; beispielsweise steht 0x0800 für IPv4. Ein Wert von 1500 (0x05dc) oder weniger deutet auf eine Länge hin, während ein höherer Wert als Typ interpretiert wird. Bei Ethernet Version 1-Frames kann die MAC eine Längenprüfung durchführen. Stimmt der Längenwert nicht mit den Oktetten im Stream überein, kann die MAC ein Fehlersignal generieren.

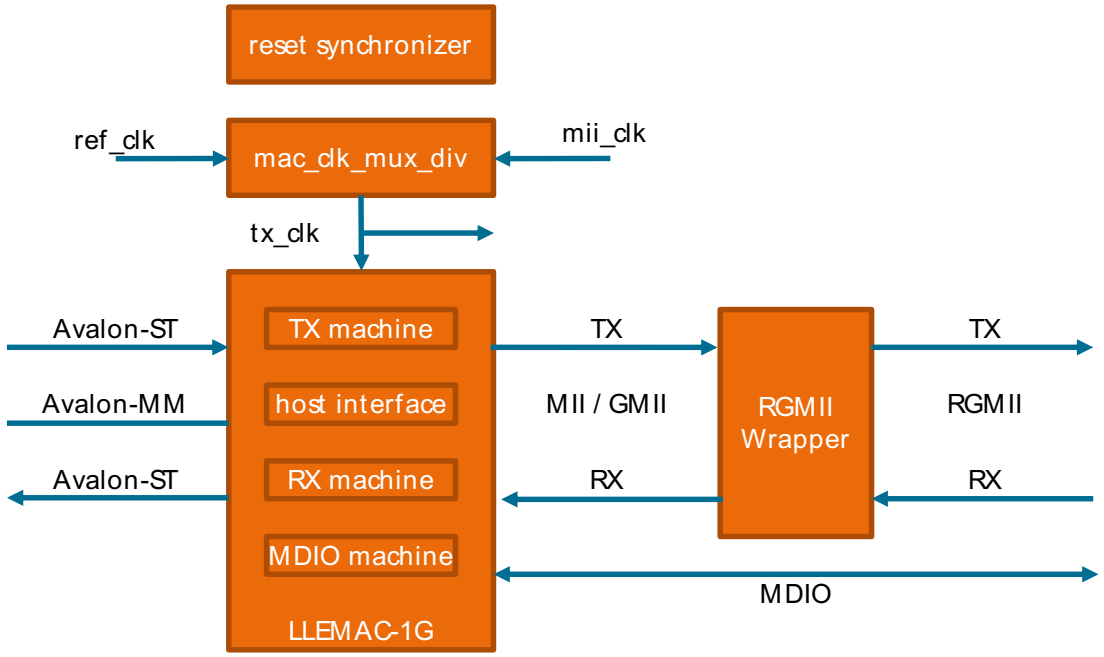

Abbildung : IPMS LLEMAC Baugruppe

Viele **Media Access Control (MAC)**-Implementierungen von Drittanbietern sind mit **Stream-FIFOs** (First-in-First-Out-Speichern) ausgestattet. Allerdings können solche FIFOs, wenn hochpräzise Hardware-Zeitstempel für die Zeitsynchronisation in Netzwerken erforderlich sind, die Ausgangs- und Eingangslatenzen erheblich erhöhen. Dies führt zu variablen Latenzen, die die Präzision der Zeitsynchronisation beeinträchtigen.

Aus diesem Grund empfiehlt der Standard **IEEE 802.1AS**, FIFOs in der MAC-Ausführung zu vermeiden, wenn es um Zeitstempelung und Zeitsynchronisation geht. Dennoch wird ein Host-Controller wahrscheinlich mit einer anderen Geschwindigkeit als Ethernet betrieben, was bedeutet, dass ein Eingangspuffer die Anforderungen an die Echtzeitreaktion deutlich reduzieren kann.

Daher sind FIFOs in bestimmten Anwendungen notwendig, sollten jedoch in die Datenströme in der Nähe des Host-Controllers integriert werden, um die Latenzproblematik zu minimieren und die Synchronisationseffizienz zu maximieren.

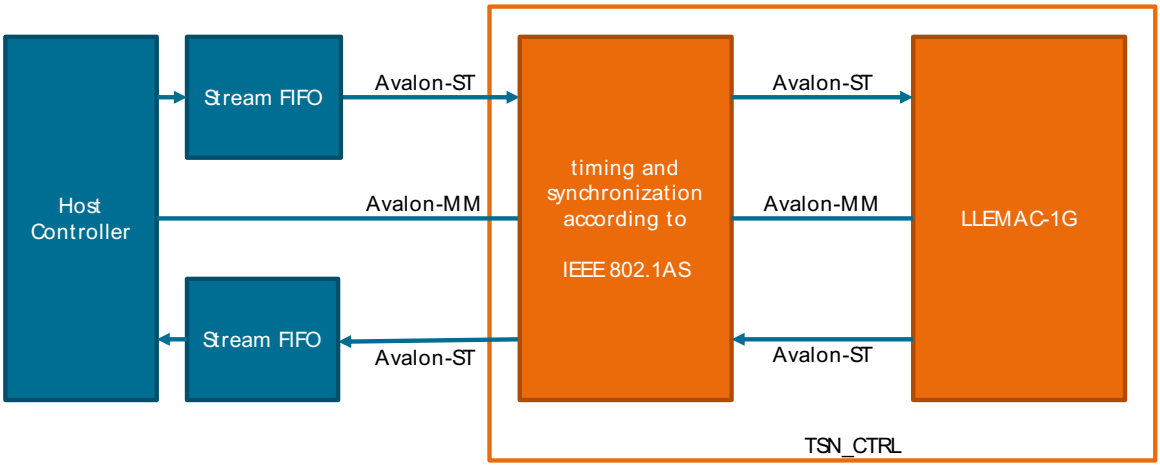

Abbildung 15: Gemeinsamer Einsatz von TSN und LLEMAC Baugruppe im Projekt
Optimierung für höhere Geschwindigkeiten:

Im Rahmen des Projektes wurde im Wesentlichen der Stand des LLEMAC-1G aufgearbeitet und für höhere Geschwindigkeiten zum LLEMAC-10G weiterentwickelt.

MAC-SEC

MACsec , auch bekannt als Media Access Control Security, ist ein Sicherheitsstandard, der speziell zur Sicherung von Ethernet-Netzwerken entwickelt wurde. Er operiert auf der Datenlink-Schicht (Layer 2) und gewährleistet die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten. MACsec implementiert fortschrittliche Verschlüsselungstechniken, um Datenpakete zu schützen und unbefugten Zugriff sowie Manipulationen zu verhindern. Der Standard unterstützt sowohl Punkt-zu-Punkt- als auch Multipoint-Verbindungen und ist in verschiedenen Netzwerkumgebungen einsetzbar, einschließlich Rechenzentren und Unternehmensnetzwerken.

Durch die Einführung von MACsec können Organisationen ihre Netzwerksicherheit erheblich verbessern und das Risiko von Datenmissbrauch oder Datenverlust signifikant reduzieren. Datenpakete, die über das Netzwerk gesendet werden, sind mit MACsec -Headern ausgestattet, die Informationen zur Authentifizierung und Verschlüsselung enthalten. Die eigentlichen Daten werden mithilfe eines symmetrischen Verschlüsselungsverfahrens, wie dem Advanced Encryption Standard (AES), verschlüsselt, was die Vertraulichkeit während der Übertragung sichert.

Zusätzlich implementiert MACsec Mechanismen zur Integritätsprüfung, um sicherzustellen, dass die empfangenen Daten unverändert bleiben. Jedes Paket erhält einen Integrity Check Value (ICV), der auf der Empfangsseite zur Überprüfung der Datenintegrität verwendet wird. Somit stellt MACsec eine robuste Sicherheitslösung für Ethernet-Netzwerke dar und schützt vor verschiedenen Bedrohungen, wie etwa Abhörversuchen oder Datenmanipulation.

Der MACsec IP-Core ermöglicht autorisierten Systemen, die in lokalen Netzwerken (LANs) verbunden sind, die Vertraulichkeit übertragener Daten zu gewährleisten und Maßnahmen gegen Frames zu ergreifen, die von nicht autorisierten Geräten gesendet oder verändert werden. Die Frames entsprechen den Vorgaben der folgenden Standards:

- IEEE-Standard für lokale und globale Netzwerke, Media Access Control (MAC) Security (IEEE Std 802.1AE-2018)
- Media Access Control (MAC) Security, Erweiterte Pakete (IEEE Std 802.1AEbw)

Der IEEE Std 802.1AE-Standard legt die Rahmenbedingungen für die Bereitstellung von verbindungsloser Benutzerdatenvertraulichkeit, Frame-Datenintegrität und Authentizität fest, wobei medienzugriffsunabhängige Protokolle und Entitäten zum Einsatz kommen. Der MACsec IP-Core bietet eine Hardwarelösung für alle datenbezogenen Vorgänge, die gemäß diesem Standard erforderlich sind. Steuerungsoperationen, wie Konfiguration und Schlüsselverwaltung, die im IEEE Std 802.1X beschrieben sind, stehen nicht im Fokus dieses MACsec IP-Cores und müssen in den Schichten über dem Core in der Anwendung implementiert werden.

Im Sendebetrieb wird der eingehende Stream für einen MAC-Frame in einem internen Speicher gepuffert. Der MACsec IP-Core führt die notwendigen kryptografischen Operationen durch, erweitert den MAC-Frame um sicherheitsrelevante Informationen und leitet den resultierenden MACsec -Frame an den ausgehenden Stream weiter. In der im Projekt bearbeiteten Erweiterung wurde der Core dahingehend optimiert, dass der Frame direkt verarbeitet werden kann, wodurch eine vollständige Zwischenspeicherung des Frames nicht mehr erforderlich ist und die Latenzzeiten minimiert werden.

Im Empfangsfall wird der eingehende Stream ebenfalls für einen MACsec -Frame in einem internen Speicher gepuffert. Im Projekt wurde besonders darauf geachtet, dass mit der Bearbeitung und Weiterleitung des Frames sofort nach Empfang des Frames begonnen werden kann. Dies reduziert die Latenzzeiten, die durch den MACsec IP-Core entstehen, erheblich. Der MACsec IP-Core führt die kryptografischen Operationen aus und entfernt den sicherheitsrelevanten Zusatzinhalt aus dem Frame. Nach erfolgreicher Authentifizierung und Integritätsüberprüfung wird der ursprüngliche MAC-Frame als ausgehender Datenstrom weitergeleitet.

Zur Authentifizierung der MAC-Frames bietet der MACsec IP-Core den Galois Counter Mode (GCM), der sowohl für reine Authentifizierung als auch für die Kombination von Authentifizierung und Verschlüsselung verwendet werden kann. Beide Modi basieren auf dem Advanced Encryption Standard (AES), der im MACsec IP-Core mit Schlüsselbreiten von 128 und 256 Bit sowie einer 128-Bit-breiten Galois Field Multiplikation implementiert ist. Optional steht für beide Modi und alle Schlüssellängen der GCM-AES-XPN-Cipher-Modus zur Verfügung, um die Lebensdauer der Schlüsselzuweisungen durch den verwendeten Paketzähler zu verlängern. Diese Sicherheitskomponenten werden im IEEE Std 802.1AE empfohlen und erfüllen die Anforderungen des US National Institute of Standards and Technology (NIST).

- Advanced Encryption Standard (AES) (FIPS PUB 197)
- Galois Counter Mode (GCM) (RFC 5647)
- Das Galois/Counter Mode (GCM) und GMAC Validation System mit der Ergänzung von XPN Validation Testing (GCMVS)

Der MACsec IP-Core bietet Advanced eXtensible Interface (AXI)-Stream-Schnittstellen für den Ein- und Ausgang von Ethernet MAC-Frames. Die Sende- und Empfangsdatenpfade arbeiten dabei vollständig unabhängig voneinander.

Neben den Stream-Schnittstellen ist der MACsec IP-Core im Speicheradressraum eines Mikrocontrollers für Konfigurations- und Schlüsselverwaltungsoperationen verfügbar. Während der MACsec IP-Core eine Operation ausführt, hat der Host-Controller keinen Zugriff auf die Konfigurationsregister.

Im MACsec IP-Core können Konfigurationsinformationen für mehrere sichere Kanäle gespeichert werden. Diese Kanäle werden automatisch jedem Frame zugeordnet, entweder über die MAC-Adresse oder einen Secure Channel Identifier (SCI).

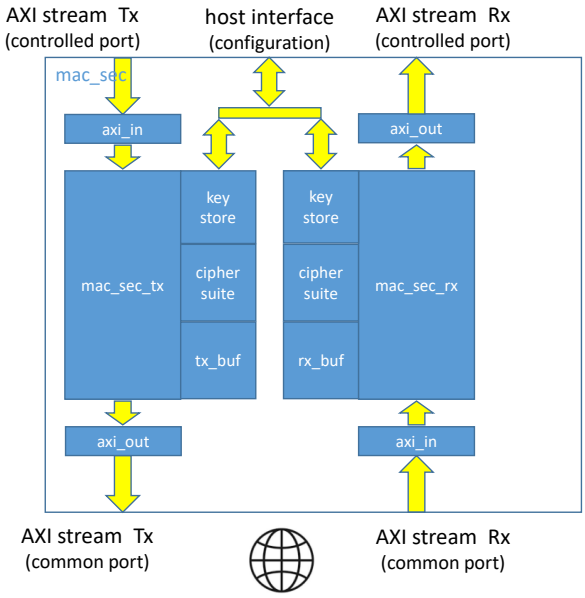

Abbildung 16: IPMS MACsec IP-Core

MACsec erweitert den Standard-MAC-Frame um zusätzliche Sicherheitsfunktionen. Der MACsec IP-Core ist im OSI-7-Schichtenmodell über der Schicht 2 positioniert. Die Initialisierungswerte, wie sichere Schlüssel, Betriebsmodi und die initiale Paketnummer, müssen von der jeweiligen Anwendung bereitgestellt werden.

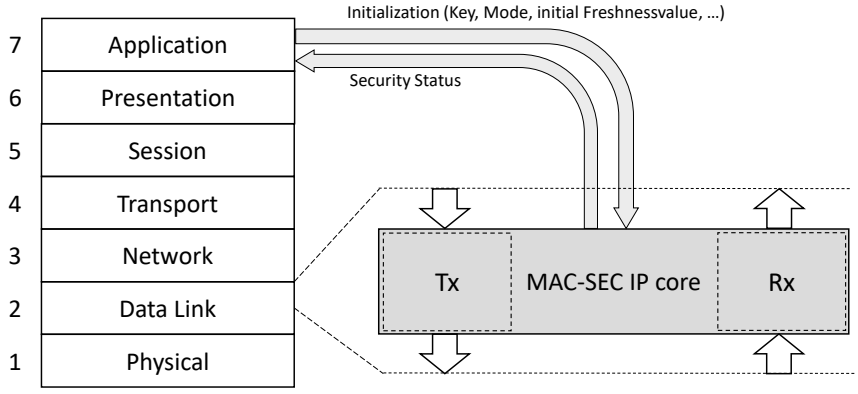

Abbildung 17: MACsec im OSI Schichtenmodell

Der für das Projekt verwendete und deutlich überarbeitete IP-Core hat folgende Eigenschaften:

- Unterstützt die MACsec -Spezifikationen
  - IEEE Std 802.1AE-2018 (IEEE Std 802.1AE-2018) Media Access Control (MAC) Security
  - GCM-AES-128 (IEEE Std 802.1AE-2018)
  - GCM-AES-192
  - GCM-AES-256 (IEEE Std 802.1AE-2018)
  - GCM-AES-XPN-128 (IEEE Std 802.1AE-2018)
  - GCM-AES-XPN-192
  - GCM-AES-XPN-256 (IEEE Std 802.1AE-2018)
- Unterstützt NIST-Verschlüsselungsstandards
  - Advanced Encryption Standard (AES) (FIPS PUB 197)
  - Galois Counter Mode (GCM) (RFC 5647)
- VLAN-in-clear-Funktionalität
- Konfigurierbare Anzahl unterstützter Secure Channels (bis zu 2^16)
  - Secure Channel wird automatisch durch Secure Channel Identifier oder MAC-Adresse verwendet
- Detaillierte Fehlerberichterstattung
  - Frame-Zähler für verschiedene Operationsergebnisse
- AXI-Stream-Schnittstelle für MAC-Daten
  - Separate Sende- und Empfangsstrukturen – vollduplexfähig
- Verschiedene Host-Controller-Schnittstellen für die Konfiguration
  - 32-Bit synchrone Host-Controller-Schnittstelle; Wrapper für 8-Bit-Hosts
  - 32-Bit AMBA APB-Protokollspezifikation v2.0
  - 32-Bit AMBA 3 AHB-Lite-Protokoll v1.0
  - 32-Bit Avalon-MM Version 2018.09.26, einfache Schnittstelle (kein Pipelining)
  - 32-Bit Wishbone
  - Optionale anwendungsspezifische Schnittstelle zum Host-Controller auf Anfrage
- Zusätzliche benutzerspezifische Seitenbandinformationen können konfiguriert werden
- Zusätzliche benutzerspezifische Präfixdaten können konfiguriert werden, z. B. für Zeitstempel von zeitsynchronisierten Netzwerken (TSN)
- Vollständig synchrones und synthetisierbares HDL-Design (System Verilog)
- Nur steigende Taktflanken werden verwendet, keine Tri-States

Optimierung für höhere Geschwindigkeiten:

Im Rahmen des Projekts wurde der MACsec IP-Core umfassend für höhere Geschwindigkeiten überarbeitet. Dies umfasst im Wesentlichen die folgenden grundlegenden strukturellen Änderungen:

- Die Verarbeitungsbreite des Datenstreams wurde von 32 auf 128 Bit erhöht. Diese Anpassung ist notwendig, um eine Übertragungsrate von 10 Gbit/s zu erreichen. Größere Bitbreiten sind aufgrund der festgelegten Verarbeitungsbreite der kryptographischen Algorithmen sinnvoll.
- Datenpakete werden nun nicht mehr zur Bearbeitung zwischengespeichert. Stattdessen erfolgt die Verarbeitung Wort für Wort in Echtzeit, und die Daten werden sofort weitergeleitet. Um interne Datenabhängigkeiten zu berücksichtigen, bleibt ein 64-Byte-Cachespeicher erhalten. Dadurch werden die Latenzzeiten minimiert, was auch den Anforderungen der Time-Sensitive Networking (TSN)-Anwendungen zugutekommt.
- Für die kryptographischen Algorithmen wurde ein Pipelining-Ansatz implementiert, sodass nach Füllung der Pipeline mit jedem Takt ein 128-Bit-Ergebnis verfügbar ist.
- Das Schlüsselmanagement, welches die entsprechenden Schlüsselinformationen für jeden zu verarbeitenden Datenframe bereitstellt, wurde umfassend überarbeitet, um eine schnellere Bereitstellung der Informationen zu gewährleisten.

TSN-SE mit MAC-SEC

Die Kombination von Time-Sensitive Networking (TSN) und Media Access Control Security (MACsec) stellt eine leistungsstarke Lösung für die Herausforderungen in modernen, zeitkritischen und sicherheitsrelevanten Netzwerkumgebungen dar. Während TSN darauf abzielt, eine deterministische und vorhersehbare Datenübertragung mit geringer Latenz zu gewährleisten, sorgt MACsec für die Sicherheit der übertragenen Daten durch Verschlüsselung und Integritätsprüfungen.

Die Integration von MACsec in TSN-Umgebungen ermöglicht es Unternehmen, kritische Datenströme nicht nur zeitgerecht zu übermitteln, sondern auch vor unbefugtem Zugriff und Manipulation zu schützen.

Konzept 1

Im ersten untersuchten Konzept wurde der MACsec IP-Core in der Nähe der Schnittstellen implementiert. Dies kommt Anwendern entgegen, die keine Eingriffe in bestehende MAC/TSN-Lösungen vornehmen möchten oder können und die den MACsec am besten an der GMII/RGMII/MII-Schnittstelle integrieren würden. Allerdings zeigen sich in der Praxis einige Nachteile. Der IP-Core wird an einer für das Protokoll ungünstigen Stelle platziert, was bedeutet, dass Protokollschichten zunächst rückgängig gemacht werden müssen, bevor sie nach dem MACsec -Core wiederhergestellt werden können. Dies führt zu einem erhöhten Aufwand.

Da der Ressourcenbedarf für den MACsec relativ hoch ist, ist der zusätzliche Ressourcenbedarf bedeutend. Außerdem müssen besondere Vorkehrungen hinsichtlich des verwendeten Taktes getroffen werden, da dieser für den MACsec höher sein sollte als der aktuell verwendete Takt. Zudem sind in den Datenframes die Zeitinformationen des TSN enthalten, und die Bearbeitungszeit des MACsec führt zusätzlich zu Latenzzeiten bei der Übertragung.

Da vollen Zugriff auf alle IP-Cores besteht, ist es ratsam, eine günstigere Positionierung für die Implementierung des MACsec zu wählen.

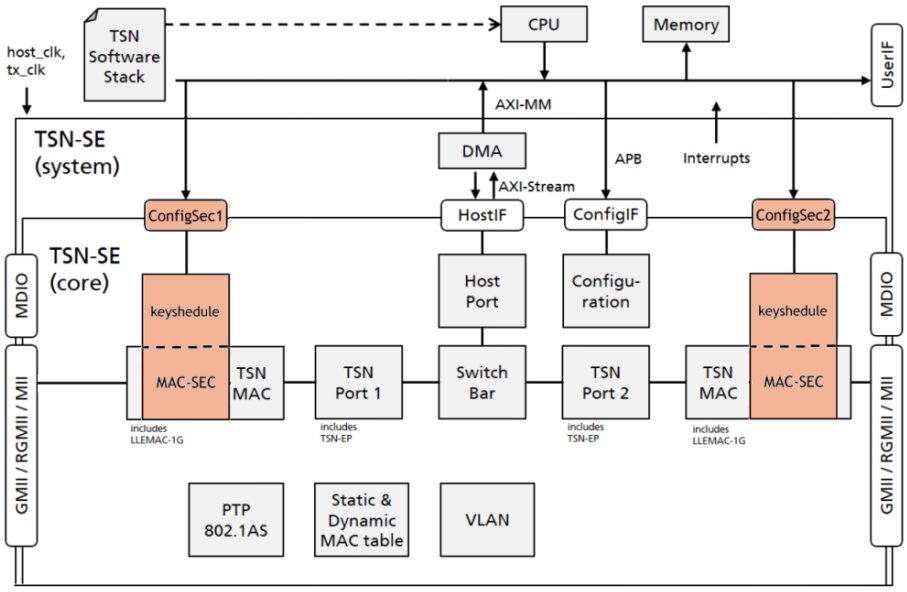

Abbildung 18: TSN-SE+MAC-SEC Konzept 1

Konzept 2:

Im verbesserten Konzept ist der MACsec optimal in den TSN-SE integriert. Dies setzt voraus, dass ein vollständiger Design-Zugriff vorhanden ist, was in diesem Fall gegeben ist. Der MACsec ist an einer Position im OSI-Schichtenmodell angeordnet, die seiner Funktion entspricht, wodurch zusätzliche Aufwände vermieden werden. Die Zeitstempel des TSN werden erst nach der Verarbeitung durch den MACsec hinzugefügt, was bedeutet, dass die Latenzzeit des MACsec keinen Einfluss auf die Zeitstempel hat.

Die Takt-Domäne an dieser Stelle bietet eine ausreichend hohe Taktfrequenz für den Betrieb des MACsec . Diese Konfiguration wurde auch für den Versuchsaufbau im Rahmen des Projekts verwendet.

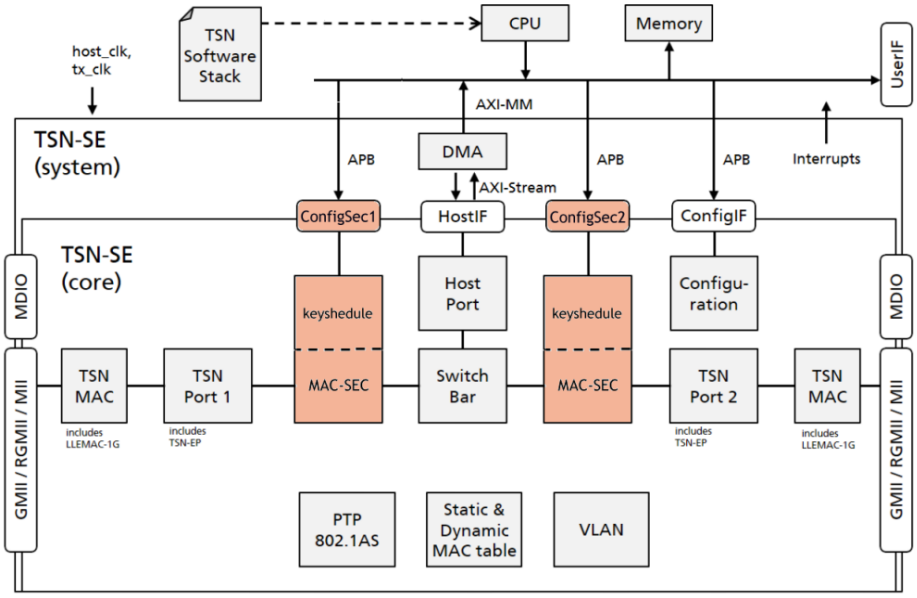

Abbildung 19: TSN-SE+MAC-SEC Konzept 2

Versuchsaufbau

Für den Versuchsaufbau werden zwei Systeme gemäß dem Konzept 2 unter Einsatz der leistungsstarken FPGA-Boards ZCU102 realisiert. Jedes dieser Boards ist mit zwei externen Ethernet-Ports ausgestattet, die eine flexible Anbindung an externe Geräte ermöglichen, sowie einem internen Ethernet-Port, über den eine im FPGA integrierte CPU kommuniziert.

Im Rahmen des Projekts können jeweils ein Computer an jeden dieser Switches angeschlossen werden, was eine einfache und effiziente Testumgebung schafft. Die beiden Switches sind über die jeweils anderen Ports miteinander verbunden, wodurch eine direkte Kommunikationslinie zwischen den beiden Computern entsteht.

Auf dieser Verbindungsleitung wird die Kommunikation der beiden Computer durch MACsec gesichert, was eine robuste Verschlüsselung und Integrität der Daten gewährleistet. Gleichzeitig erfolgt eine Synchronisation mittels Time-Sensitive Networking (TSN), die sicherstellt, dass die Datenübertragung nicht nur zuverlässig, sondern auch zeitkritisch erfolgt.

Diese innovative Konfiguration ermöglicht es, das Verhalten der Kombination aus TSN und MACsec eingehend zu untersuchen und wertvolle Erkenntnisse über die Leistungsfähigkeit und Effizienz dieser Technologien in modernen Netzwerkumgebungen zu gewinnen. Der Versuchsaufbau bietet somit eine ausgezeichnete Plattform, um die Vorteile und Herausforderungen der Integration von TSN und MACsec in zeitkritischen Anwendungen zu analysieren.

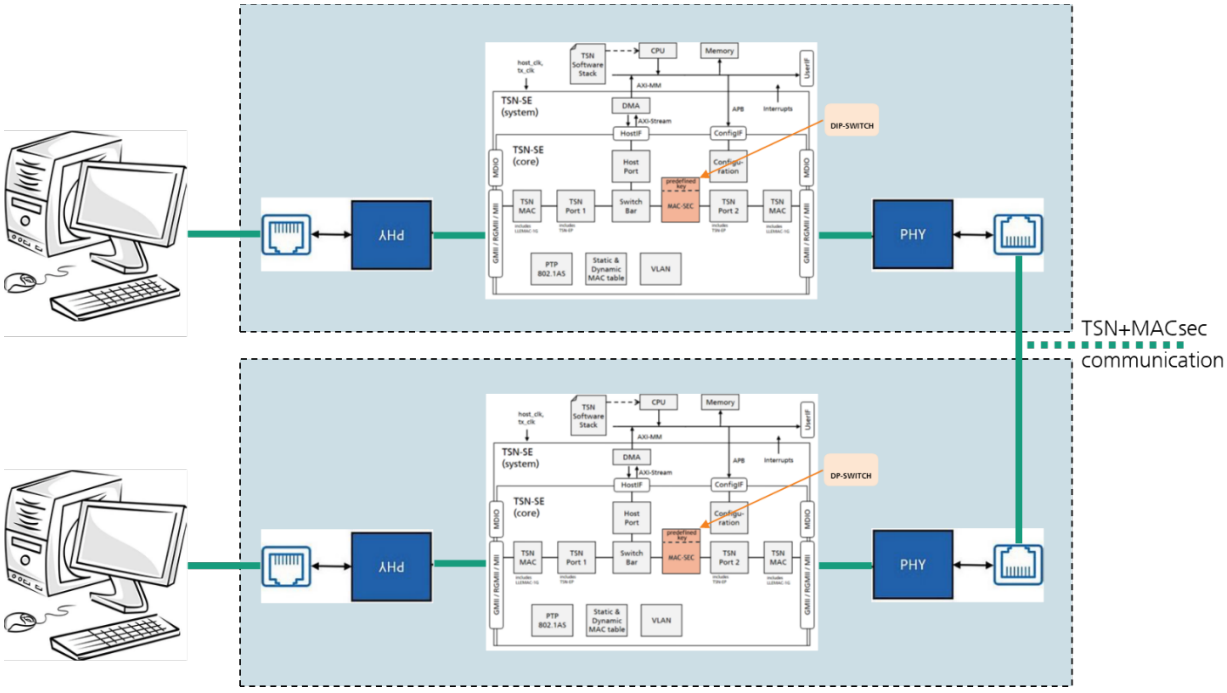

Abbildung 20: Überblick zwei TSN-SE+MAC-SEC im Versuch

Das System bietet zudem die Möglichkeit, mithilfe einer speziell für die CPUs der Boards implementierten Firmware über die CPU-Ports Testdaten zu generieren, zu senden und zu empfangen. Diese Funktionalität ermöglicht eine umfassende Erprobung der Systeme und unterstützt die Validierung der Implementierungen unter realistischen Bedingungen.

Darüber hinaus können über diese CPU wichtige Register ausgelesen werden, die es ermöglichen, Einstellungen, Fehlerzähler und Statusmeldungen der TSN- und MACsec IP-Core zu überwachen und gegebenenfalls anzupassen. Diese umfassenden Auswertungsmöglichkeiten tragen entscheidend dazu bei, die Leistungsfähigkeit und Zuverlässigkeit der Systeme zu optimieren.

Durch diese Vorgehensweise konnten eingehende Untersuchungen zur Wechselwirkung von TSN und MACsec durchgeführt werden. Die Ergebnisse zeigten, dass die im Projekt gewählte Konfiguration eine störungsfreie Interaktion zwischen den beiden Systemen gewährleistet. Beide Systeme erfüllen weiterhin die Anforderungen ihrer jeweiligen Spezifikationen, was die Effektivität der Integration von TSN und MACsec in zeitkritische Anwendungen unterstreicht.

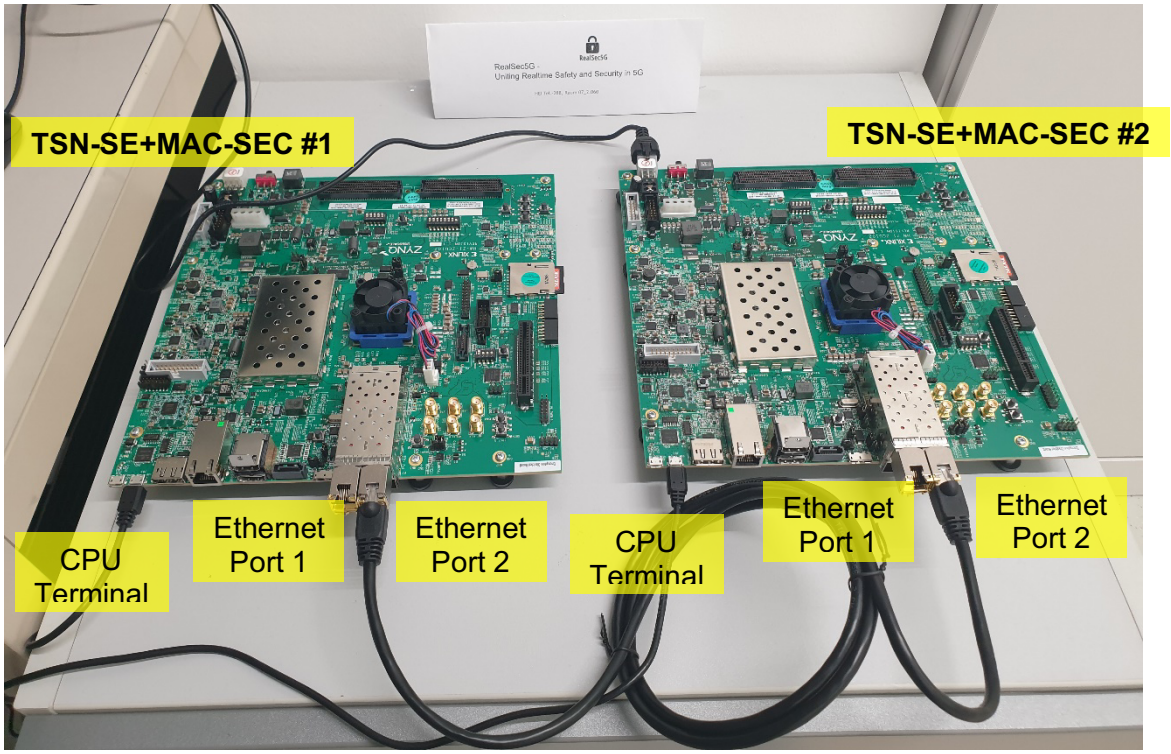

Abbildung 21: Versuchsaufbau

Neben der Verarbeitung von Frames, die über den ersten Port empfangen werden, ermöglicht die Testplattform auch die Übertragung und den Empfang von Frames über den dritten Port, der als CPU-Port konfiguriert ist. Dieser Port dient dazu, Testdaten zu senden und zu empfangen, was eine flexible und umfassende Analyse der Systemleistung ermöglicht.

Durch die implementierte Firmware können eine Vielzahl von Statistiken, Fehlerzählern und anderen relevanten Informationen zur Übertragung ermittelt werden. Diese Daten ermöglichen es, die Effizienz und Zuverlässigkeit der Netzwerkkommunikation zu überwachen und zu bewerten. Die detaillierten Einblicke in den Übertragungsprozess unterstützen die Identifikation potenzieller Probleme und tragen zur

kontinuierlichen Verbesserung der Systemleistung bei.

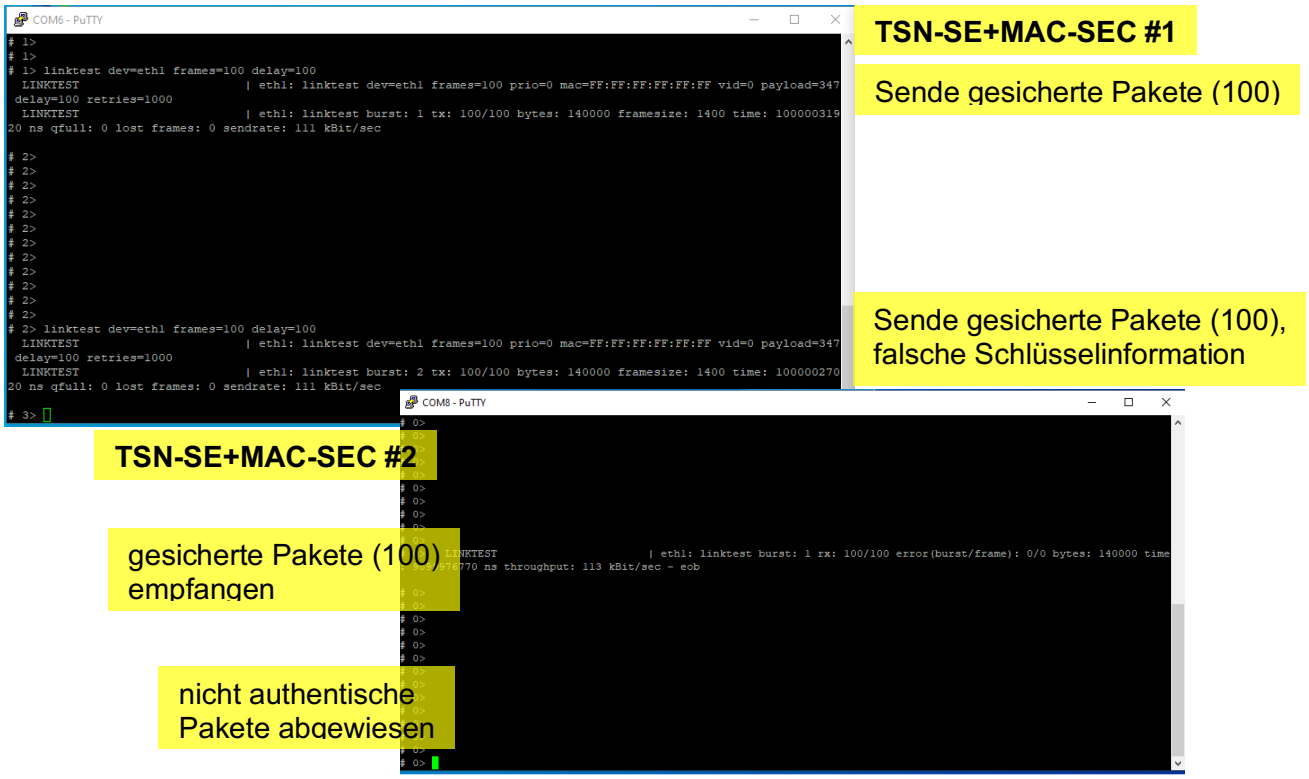

Abbildung 22: Testdurchführung

Arbeitspakete

Arbeitspaket 1: Projektmanagement und Dissemination

Im Arbeitspaket 1 hat aconnic die Projektleitung und Koordinierung aller Aktivitäten als auch die Öffentlichkeitsarbeit in Form von Teilnahmen an Messen und Veranstaltung im Konsortium durchgeführt. Es wurden regelmäßige Projektmeetings zur Koordination des Arbeitstandes und der partnerübergreifenden Arbeiten durchgeführt.
Weiterhin wurden die Ergebnisse des Konsortiums auf nachfolgenden Messen und Veranstaltungen präsentiert:

- Teilnahme am BSI-Fachworkshop zu den Themenschwerpunkten 1 und 4 am 19.03.2024
- Teilnahme am BSI-Fachworkshop III am 13.05.2024 in Dresden im Rahmen der IEEE6G-Konferenz
- Ausstellung auf der Hannovermesse vom 22.-26.04.2024
- Ausstellung auf der IEEE6G in Dresden vom 13.-14.05.2024
- Ausstellung auf der ANGACOM in Köln vom 14.-16.05.2024
- Teilnahme am BSI-5G/ 6G-Forum: Cybersicherheit und digitale Souveränität mit einem Pitch-Vortrag zum RealSec5G Projekt am 26.10.2024
- Besuch der ITSA IT Security Messe in Nürnberg vom 22.-24.10.2024

Die Erstellung von Arbeitsberichten (Quartalsreports, Jahresreport, Abschlussbericht) und Koordination mit den Projektpartnern erfolgte hier ebenso.

Arbeitspaket 2: Anforderungsdefinition

Um eine gemeinsame Basis zur Erörterung der technischen Fragestellungen im Projekt zu schaffen, wurden im Konsortium und weiteren Inputgebern zuerst Angriffsszenarien definiert, denen das Gesamtsystem standhalten soll. Dieses Angreifer-Modell wurde einer eingehenden Analyse bezüglich notwendiger sicherheitsrelevanter Eigenschaften unterzogen. Der aktuelle Stand der Technik und die relevanten Standards wurde in dieser Analyse berücksichtigt. Eine Schwachstellenanalyse wurde durchgeführt. Im Anschluss wurden dann funktionale, nicht-funktionale, sowie die Sicherheit betreffende Anforderungen analytisch abgeleitet.

Arbeitspaket 3: Entwurf Systemkonzeption

Um zu einer Architektur des Gesamtsystems zu gelangen, wurden zuerst separate Entwürfe für die jeweilige Integration der IP-Cores untereinander und der Integration von IP-Cores (größere Funktionsblöcke und Subsysteme) allgemein auf das Basissystem erstellt. Im Anschluss wurden beide Entwürfe zu einem gemeinsamen Systementwurf integriert.

Zusätzlich wurden bei aconnic Vorschläge erarbeitet, den Softwarelebenszyklus insbesondere im Bereich Sicherheit und Performance an aktuelle Anforderungen u.a. ISO 27001 anzupassen. Dabei stand Automatisierung im Zusammenhang mit build und permanenter Code- und Schwachstellenanalyse für verschiedene Systeme (embedded Linux, FPGA) im Mittelpunkt.

Arbeitspaket 4: TSN / MAC-SEC

Auf Basis des Architekturmodells wurden die bestehenden Funktionsblöcke einzeln betrachtet, neue Konzepte bzgl. funktionale Sicherheit und Datensicherheit umgesetzt und integriert als auch die Funktionsblöcke zu einem neuen TSN-MACsec Funktionsblock zusammengeführt. Zusätzlich wurden funktionale Erweiterungen des MACsec für Datenraten bis 10/100 Gbit/s entwickelt. Die strukturellen Erweiterungen erlauben 10G Übertragungsraten bei einer Taktfrequenz von 125 MHz. Weitere Optimierungen im Ablauf sind aus jetziger Sicht in Folge von Datenabhängigkeiten in den Krypto-Algorithmen nicht möglich. Höhere Datenraten sind dann durch höhere Taktraten bei der Zieltechnologie und/oder durch parallele Anwendung mehrerer Cores möglich.

aconnic hat hierbei Unterstützung bei der Entwicklung der anforderungsspezifischen Performance-Erweiterung für die Zusammenführung von TSN und MACsec mit anwenderspezifischem Know-How gegeben. Auch erfolgte in diesem Arbeitspaket die Evaluierung und Definition der möglichen Hardware bzw. Architektur für die geplante Implementierung des MACsec-TSN-IP-Cores in die spätere Demonstratorplattform. Auch die Aspekte beim Zusammenwirken von TSN und MACsec wurden analysiert und die potenzielle Umsetzung theoretisch erarbeitet bzw. für die spätere Implementierung spezifiziert.

Arbeitspaket 5: Integration IP-Cores

Auf Basis des erarbeiteten Anforderungskatalogs an das Gesamtsystem wurden zuerst Anforderungen an die zu nutzende Hardwareplattform abgeleitet. Dies umfasst Eval-Board, FPGA-Plattform, sowie die Schnittstelle zwischen beiden. Danach wurde eine Marktanalyse bzgl. in Frage kommender und verfügbarer Eval-Boards und FPGA-Plattformen durchgeführt und eine Auswahl getroffen. Anschließend wurde das Enablement beider Komponenten durchgeführt. Danach wurde die FPGA-Plattform in den Datenpfad des Eval-Boards integriert, um den hohen Durchsatz des FPGAs nutzbar zu machen. Schließlich wurde der integrierte IP-Core auf dem Eval-Board nach dem festgelegten Architekturmodel integriert.

aconnic hat im Rahmen dieses Arbeitspaketes die Vorarbeiten für die geplante Integration des Fraunhofer IPMS IP-Cores auf die von aconnic ausgewählte Hardwareplattform durchgeführt. So wurde eine entsprechende Hardware/ Architektur für die Integration evaluiert, bewertet und ausgewählt sowie ein Abgleich der vorhandenen Plattform bzw. dessen Möglichkeiten (u.a. Typ und Größe der FPGA-Plattform) mit den Anforderungen von Fraunhofer IPMS bzw. deren IP-Core durchgeführt.

Auch wurden die theoretischen Ansätze bzw. Optionen zur Integration in Bezug auf die effizientesten Datenpfade und die Steuerung des IP-Cores durch den übergeordneten Controller (CPU) bzw. dessen Unterstützung durch Treiber oder Softwarepakete erarbeitet und dokumentiert. Ebenso erfolgte die Betrachtung der Zusammenarbeit von TSN und MACsec, um bei der geplanten Integration die bestmögliche Performance erzielen zu können.

Eine Implementierung konnte jedoch nicht mehr im Rahmen des Projektzeitplans erfolgen.

Arbeitspaket 6: Testbed

In diesem AP wurde die Testumgebung zur Evaluation der Gesamtlösung bereitgestellt. Dazu wurden zuerst Testszenarien definiert, zu testende Qualitätsparameter festgelegt und entsprechende Testwerkzeuge gewählt. Danach wurde der Teststand aufgebaut. Dabei wurde insbesondere eine erstellte Firmware, die auf in den FPGA-Boards zusätzlich implementierten Prozessoren lief verwendet, die umfangreiche Testgestaltung und Protokollierung zulässt.

Im Projekt war nach erfolgreicher Erstellung und Test im Rahmen des Testbeds die Integration in den Demonstrator sowie weiterführende Tests in Bezug auf Performance und die Interaktion zwischen Systemen unterschiedlicher Hardwarebasis (FPGAs) geplant.

Aufgrund der im Projekt aufgetretenen Verzögerungen und der nicht möglichen Verlängerung, konnte dieser Nachweis nicht vollständig durchgeführt werden.

Arbeitspaket 7: Evaluation

In diesem Arbeitspaket (AP) wurde umfassend untersucht, inwieweit die erarbeiteten Lösungen den zu Beginn des Projekts festgelegten Anforderungen gerecht werden. Hierzu wurden sowohl quantitative Aspekte wie die erreichte Latenz und Bandbreite, als auch qualitative Merkmale, wie die Benutzbarkeit, Flexibilität und die Integrierbarkeit in bestehende Softwareprozesse, eingehend evaluiert.

Zusätzlich wurde analysiert, welche potenziellen Schutzniveaus die entwickelte Systemarchitektur sowie die konkrete prototypische Implementierung erreichen können. Die Ergebnisse dieser Evaluierung sind entscheidend für das Verständnis der Leistungsfähigkeit und Sicherheit des Systems. Die Funktionalität des Systems, wie in Abschnitt 2.1.3 beschrieben, wurde erfolgreich nachgewiesen. Es wurde festgestellt, dass die Daten mithilfe des MACsec IP-Core verschlüsselt werden können, ohne dass die Zeitsynchronisation negativ beeinflusst wird. Darüber hinaus konnten vergleichbare Werte für die Genauigkeit gemessen werden, die mit denen eines Vergleichsmodells ohne MACsec übereinstimmen. Diese Erkenntnisse belegen die Effektivität der implementierten Lösungen und deren Eignung für den Einsatz in zeitkritischen Anwendungen.

Positionen des zahlenmäßigen Nachweises

Zu den Hauptpositionen für den zahlenmäßigen Nachweis zählen die Personalkosten und die im Projekt getätigten Investitionen.

Notwendigkeit der geleisteten Arbeit

Alle im Rahmen des Projekts durchgeführten Arbeiten trugen maßgeblich zur Erreichung der gesetzten Projektziele bei. Ziel war es, die TSN-SE- und MACsec -Komponenten weiterzuentwickeln und in einem einheitlichen MACsec-TSN-IP-Core zu integrieren. Dies ermöglichte die Realisierung von TSN-Funktionalitäten unter hohen Sicherheitsanforderungen. Es ist festzustellen, dass jede durchgeführte Maßnahme zu konkreten Ergebnissen führte.

Auch wenn bei aconnic nicht alle Ziele des Projektes durch extern bedingte Verzögerungen erreicht werden konnten, wurde jedoch weitreichendes Know-How für die Umsetzung von High-Security Lösungen in Verbindung mit echtzeitkritischen Anwendungen erzielt und eine technologisch fundierte Basis für die weitere Nutzung und anschließende Verwertung geschaffen.

Verwertbarkeit der Ergebnisse

Es ist geplant, die hier im Projekt erzielten Ergebnisse in zukünftige Produkte für sicherheitsrelevante Anwendungen im Mobilfunk- als auch im Geschäftskundenbereich sowie in weiteren KRITIS-Bereichen wie beispielsweise in industriellen Netzen einfließen zu lassen.

Daher wird die prototypische Integration der FPGA-Plattform in eine von aconnic bereits genutzte Hardwareplattform für Netzwerkgeräte auch nach Projektende fortgesetzt und soll eine Überführung dieser Technologie in die Produktpipeline innerhalb von 2 Jahren nach Projektende ermöglichen.

Mit den erreichten Ergebnissen ist aconnic in der Lage, neue Anwendungsfelder bzw. Use Cases, besonders im Bereich 5G-Campusnetze zu erarbeiten. Es ist geplant, dieses innerhalb eines Jahres nach Projektende durchzuführen. Daran anschließend sollen Umsetzungsprojekte oder Produktentwicklungen in den identifizierten Anwendungsfeldern durchgeführt werden. Diese Tätigkeiten werden innerhalb von 2 Jahren nach Projektende durchgeführt.

Damit kommt aconnic dem Ziel näher, sich als Anbieter von sicheren 5G/6G-Infrastrukturkomponenten, entwickelt und hergestellt in Deutschland am Weltmarkt zu positionieren. Dies stärkt direkt auch die digitale Souveränität Deutschlands.

Das Fraunhofer IPMS entwickelt seit mehr als 15 Jahren industrielle und automobile Kommunikationscontroller (CAN, LIN, CAN-FD, CAN XL) als IP-Cores für ASIC- und FPGA-Systeme. Die neuste Entwicklung ist eine Familie von Kommunikationscontrollern für Ethernet-TSN-Netzwerke, die für Kommunikationsgeschwindigkeiten bis 1 Gbit/s nach den TSN Standards IEEE802.1AS, IEEE 802.1Q und 802.3br ausgelegt sind. Mehr als 150 Kunden weltweit setzen seit über 10 Jahren auf die Qualität der Fraunhofer IPMS IP Core Lösungen und den umfassenden technischen Support. Das Fraunhofer IPMS bietet TSN IP-Cores Module in den Varianten TSN-EP (IP Core für Time Sensitive Networking Endpunkte), TSN-SE (IP Core für Time Sensitive Networking Switched Endpunkte) und TSN-SW (IP Core für Time Sensitive Networking Multiport Switches) an, die jeweils aus Hardwarebeschreibungen, Software und notwendigen Treibern für die Implementierung in unterschiedliche Zielsysteme bestehen. Zusätzlich werden diverse kundenspezifische Anpassungen, Unterstützung bei der Implementierung und Charakterisierung durchgeführt.

Das Fraunhofer IPMS hat in der Vergangenheit viele Projekte mit Bezug zu TSN IP-Cores erfolgreich umgesetzt. Der Fokus lag dabei stets auf Industrieprojekten. Seit vielen Jahren arbeitet das Institut mit Partnern aus der Wirtschaft erfolgreich am Transfer von Forschungsergebnissen in die industrielle Anwendung.

Wissenschaftlicher und technischer Fortschritt Dritter

Während der Projektlaufzeit wurden keine signifikanten neuen Veröffentlichungen von neueren Ergebnissen Dritter zur Kombination von Time-Sensitive Networking (TSN) und MACsec festgestellt. Die US-amerikanische Firma Rambus, ein renommierter Anbieter von IP-Cores, bewirbt aktiv den Einsatz ihres MACsec -Cores in Verbindung mit TSN. Aus den verfügbaren Informationen geht hervor, dass deren MACsec an der GMII-Schnittstelle zwischen den PHYs integriert wird.

Rambus hebt besonders die geringe Latenzzeit ihres MACsec hervor, was angeblich zu einer minimalen Beeinflussung der TSN-Funktionalität führt. Im Gegensatz dazu zeigt der im Rahmen dieses Projekts verfolgte Ansatz, dass die Latenz des MACsec keinen Einfluss auf die Genauigkeit von TSN hat, da der MACsec in einer anderen Position im System angeordnet ist. Diese strategische Platzierung ermöglicht eine optimale Leistungsfähigkeit und eine zuverlässige Synchronisation der Datenübertragung.

Veröffentlichungen

Während der Laufzeit des Projekts wurden keine spezifischen Veröffentlichungen zu den erarbeiteten Themen durchgeführt. Nach dem erfolgreichen Abschluss des Projekts wird jedoch weiter aktiv nach Möglichkeiten gesucht, die erzielten Ergebnisse auf Fachkonferenzen und in wissenschaftlichen Publikationen zu präsentieren.

Die Absicht, die gewonnenen Erkenntnisse einem breiten Publikum zugänglich zu machen, stellt ein Teil der Verwertungsplanung dar und unterstreicht das Engagement des Teams, den Wissensaustausch zu fördern sowie die Relevanz der entwickelten Technologien in der wissenschaftlichen Gemeinschaft und in der Industrie zu betonen. Durch diese Maßnahmen wird angestrebt, die Ergebnisse nicht nur zu disseminieren, sondern auch wertvolles Feedback von Experten und Praktikern zu erhalten, um die Innovationen auf diesem Gebiet weiter voranzutreiben.