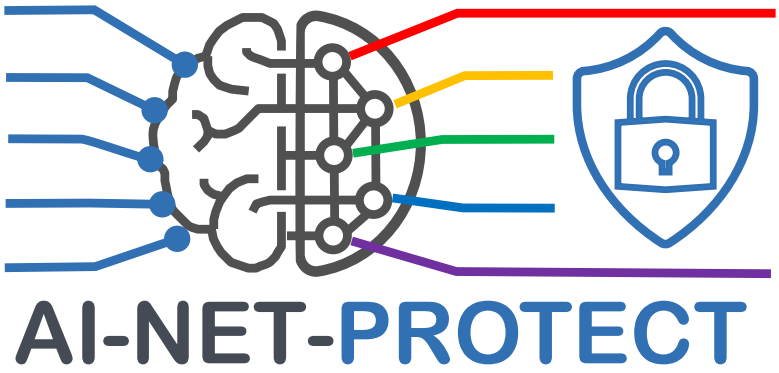


Bereitstellung automatisierter Resilienz und sicherer Netze auf vertrauenswürdigen Geräten für kritische Infrastrukturen und Unternehmen

Sachbericht zum Verwendungsnachweis

Verbundprojekt:	Bereitstellung automatisierter Resilienz und sicherer Netze auf vertrauenswürdigen Geräten für kritische Infrastrukturen und Unternehmen (AI-NET-PROTECT)
Teilvorhaben:	Telemetrie, Netzwerkplanung, Künstliche Intelligenz (Infosim)
Zuwendungsempfänger:	Infosim GmbH & Co. KG
Laufzeit des Projekts:	01.02.2021 bis 30.06.2024
Autoren:	David Hock Stefan Kremling Fabian Lipp Simon Schardt

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS1290 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Inhaltsverzeichnis

Abkürzungen

gNMI	gRPC Network Management Interface
gRPC	google Remote Procedure Call
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
KI	künstliche Intelligenz
MDF	Main Distribution Frame
ML	maschinelles Lernen
NMS	Netzwerkmanagementsystem
ONF	Open Networking Foundation
OTN	optisches Transportnetz
PoC	Proof-of-Concept
SNMP	Simple Network Management Protocol
TAPI	Transport Application Programmable Interface
YANG	Yet Another Next Generation

1 Kurzdarstellung

Ursprüngliche Aufgabenstellung Der Wohlstand und die Wettbewerbsfähigkeit Europas hängen stark davon ab, wie erfolgreich die digitale Transformation gemeistert wird. Digitale Technologien sind unverzichtbar für die Lösung globaler Herausforderungen und die aktive Gestaltung des Wandels in Bereichen wie Gesundheit, Industrie und Mobilität. Eine zukunftsfähige Kommunikationsinfrastruktur, die überall und jederzeit verfügbar, skalierbar und sicher ist, bildet die Grundlage für die Digitalisierung von Wirtschaft und Gesellschaft. Sie soll eine Vielzahl neuer digitaler Dienste und Anwendungen ermöglichen, von denen wir uns viele heute noch gar nicht vorstellen können.

Die intelligente Automatisierung von Kommunikationsnetzen ist zentral, um die steigende technische Komplexität moderner Netze zu bewältigen und gleichzeitig Sicherheit, Skalierbarkeit und Effizienz zu gewährleisten. AI-NET vereint mehr als 70 führende europäische Partner, um neue Ansätze für Netzautomatisierung zu entwickeln und zur Anwendungsreife zu bringen.

Heutige Kommunikationsnetze zeichnen sich für Nutzer und Betreiber oft durch eine hohe technische Komplexität aus. Heterogene Netzarchitekturen, Edge Computing und Network Slicing, sowie stetig steigende Anforderungen an Dienstgüte, Agilität und Flexibilität verursachen ungekannte betriebliche Herausforderungen. Unzureichend bekannte Stellgrößen, Parameterschwankungen und Degradationseffekte erfordern hohe Sicherheitsreserven in der Netzplanung und verursachen einen erhöhten Energieverbrauch. Konfigurationsfehler können nicht nur die Ausfallsicherheit der Netze, sondern auch die Informationssicherheit von Betriebs- und Nutzerdaten gefährden. Fehlfunktionen sind häufig schwer zu lokalisieren und nur mit erheblichem Zeitaufwand zu beheben. Eine intelligente Ende-zu-Ende-Automatisierung auf der Netz- und Dienstebene soll manuelle Prozessschritte weitestgehend vermeiden und in Zukunft einen vollständig autonomen Netzbetrieb ermöglichen.

Ziel von AI-NET-PROTECT Der Schwerpunkt des Teilprojekts PROTECT war die Bereitstellung automatisierter Resilienz und sicherer Netze auf vertrauenswürdigen Geräten für kritische Infrastrukturen und Unternehmen. AI-NET-PROTECT soll für den Schutz kritischer Daten, hohe Performanz in Bezug auf wesentliche Leistungsparameter (wie Latenz, Durchsatz und Verfügbarkeit) und hohe Robustheit der Netzinfrastruktur (Schutz gegen Manipulationen und Angriffe) sorgen. Um diese Ziele zu erreichen, wurde in PROTECT eine skalierbare Netz- und Knotenarchitektur entwickelt, um die verschiedenen kritischen Leistungsparameter durch eine Mischung aus offener und spezialisierter Hardware und Software zu adressieren. Streaming Network Telemetry und Intent-based Software-Defined Network Management and Control bieten Zero-Touch-Bereitstellung

und unterstützen die Automatisierung von Ende-zu-Ende-Diensten mit Hilfe von künstlicher Intelligenz (KI). Die wichtigsten Anwendungsfälle für KI sind Leistungsoptimierung, proaktive Fehler- und Anomalieerkennung, Penetrations- und Schwachstellentests, sowie das Management von Sicherheitsangriffen.

Ablauf des Vorhabens Das Forschungsprojekt gliederte sich in drei Hauptphasen: a) Anforderungen und Architektur, b) Umsetzung und c) Demonstration und externe Kommunikation. In der ersten Phase wurden die Grundlagen gelegt, was die Definition von Anforderungen, die Entwicklung der Software- und Netzarchitektur, die technoökonomischen Analyse, sowie die Festlegung von Leistungskennzahlen (KPIs) mit einschließt. Die zweite Phase konzentrierte sich auf die Umsetzung innovativer Technologien, darunter Streaming Network Telemetry, Datenanalyse und Verfahren des maschinelles Lernens. Zudem werden Multi-Domain- und Multi-Technologie-Steuerung, sowie Ende-zu-Ende-Dienstautomatisierung betrachtet. In der abschließenden Phase wurden Anwendungsszenarien definiert und in einer partnerübergreifenden Testumgebung demonstriert, Netzperformanz-KPIs analysiert und die Ergebnisse in verschiedenen Veranstaltungen nach außen getragen.

Das hier dargestellte Projekt war ein Teilvorhaben des Projekts AI-NET-PROTECT, welches wiederum eine der sogenannten „Säulen“ von AI-NET darstellt. AI-NET wurde im Rahmen des EUREKA-Clusters CELTIC-NEXT durchgeführt. Dieser Cluster beschäftigt sich mit der nächsten Generation von Telekommunikationstechnologien für die digitale Gesellschaft. Die Säulen von AI-NET wurden in verschiedenen europäischen Ländern (Deutschland, Finnland, Frankreich, Niederlande, Polen, Schweden, Vereinigtes Königreich) öffentlich gefördert. Insgesamt nahmen 96 Partner an AI-NET teil. Das Konsortium von AI-NET-PROTECT setzte sich aus 3 Industriepartnern, 3 Telekommunikationsanbietern, 12 KMUs, 10 Universitäten und 11 Forschungsinstituten in Deutschland, Niederlande, Polen und Schweden zusammen.

Wesentliche Ergebnisse Infosim hat im Rahmen des Projekts wesentliche Ergebnisse in mehreren Schlüsselbereichen erzielt. Im Bereich KI und maschinelles Lernen (ML) wurden innovative Ansätze zur Analyse von Zeitreihen-Daten entwickelt und evaluiert. Die Nutzung moderner Streaming Network Telemetry als Alternative zu klassischen Protokollen wie Simple Network Management Protocol (SNMP) wurde eingehend untersucht, insbesondere hinsichtlich der Effizienz und Skalierbarkeit. Für die Serviceorchestrierung wurde eine beispielhafte, komplexe Service-Struktur aufgebaut und darauf unterschiedliche Überwachungs- und Visualisierungsansätze implementiert. Zudem wurden Methoden für die Kapazitätsplanung entwickelt, beispielsweise zur Vorhersage von zukünftigem Netzwerkverkehr und zur Visualisierung relevanter Metriken. Die Demonstrationen im Rahmen einer gemeinsamen Testumgebung konzentrierten sich auf die Umsetzung eines zentralen Managements, insbesondere für optische Transportnetze (OTNs), die Integration mit Schnittstellen von Projektpartnern, die Service-Überwachung und den Vergleich zwischen Telemetrie und SNMP.

2 Eingehende Darstellung

2.1 Verwendung der Zuwendung und erzielte Ergebnisse im Einzelnen

In diesem Abschnitt geben wir einen Überblick über die im Projekt durchgeführten Arbeiten, sowie die damit erzielten Ergebnisse. Die Gliederung des Abschnitts orientiert sich dabei an den bereits zuvor genannten drei Hauptphasen: Anforderungen und Architektur, Umsetzung sowie Demonstration und externe Kommunikation. In den verschiedenen Unterabschnitten werden nacheinander ausgewählte Ergebnisse dieser drei Phasen in mehr Detail vorgestellt.

2.1.1 Architektur, Anwendungen, Anwendungsfälle

In der ersten Hauptphase des Projektes lag der Fokus auf Fragestellungen zu Anforderungen und Architektur. Dies schloss auch die Betrachtung einer techno-ökonomischen Analyse und die Auswahl, Erhebung und Visualisierung passender KPIs mit ein.

2.1.1.1 AI-NET-PROTECT Gesamtarchitektur

Gemeinsam mit den Konsortialpartnern wurde eine Gesamtarchitektur entwickelt, um die Anforderungen moderner Telekommunikationsnetze zu erfüllen und die verschiedenen, von den Partnern betrachteten, Schwerpunkte mit zu berücksichtigen. Die definierte Referenzarchitektur, die in Abbildung 1 dargestellt ist, umfasst daher eine Vielzahl unterschiedlicher Aspekte, die im Rahmen des Projekts von den verschiedenen beteiligten Partnern untersucht wurden. Dies reicht von den zugrundeliegenden physikalischen und virtuellen Komponenten des Kommunikationsnetzes selbst bis hin zu verschiedenen logischen Komponenten auf unterschiedlichen Ebenen (Management, Steuerung, Anwendung, etc.).

Das in der Architektur mit eingearbeitete Streaming Telemetry Framework ist darauf ausgelegt, in Access-, Metro- und Kernnetzwerken zu operieren und Technologien verschiedener Anbieter zu unterstützen. Es erlaubt die Nutzung unterschiedlicher Protokolle, Datenmodelle und Abonnementmodi für Streaming Network Telemetry und bietet außerdem autonome Konfigurationsmöglichkeiten zur effizienten Datenerfassung.

Zentrale Komponenten der Architektur sind ein Modul im Controller, das die Aktivierung und Rekonfiguration von Telemetrie-Funktionen und Abonnements übernimmt, sowie ein Modul zur Datenerfassung und -verarbeitung. Dieses Modul speichert die Telemetriedaten im zentralen Data Lake und ermöglicht optional eine Vorverarbeitung durch spezialisierte Anwendungen. Ein besonderes Merkmal der Architektur ist die Möglichkeit

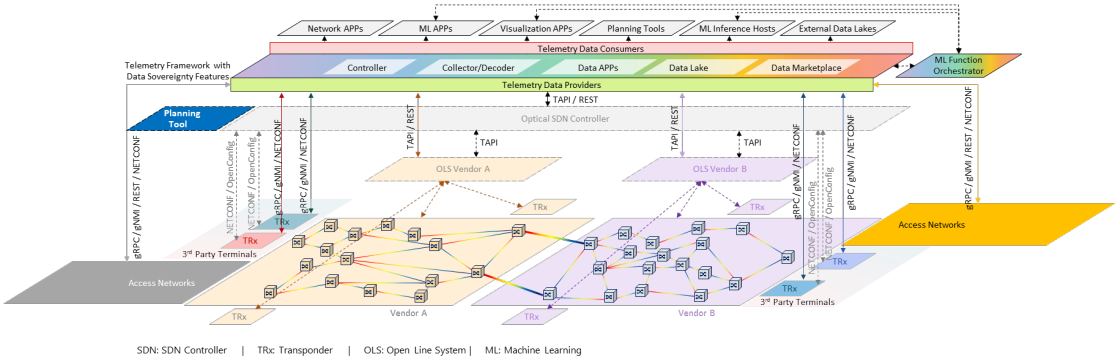


Abbildung 1: Vom AI-NET-PROTECT Konsortium gemeinsam definitierte Architektur – Open and Disaggregated Ecosystem

die gesammelten Telemetriedaten über verschiedene APIs bereitzustellen. Diese APIs erlauben den Zugriff auf Daten in verschiedenen Verarbeitungsstufen, von Rohdaten bis hin zu abstrahierten oder anonymisierten Datensätzen. Damit unterstützt die Architektur eine Vielzahl von Anwendungen wie Leistungsoptimierung, proaktive Fehlererkennung und flexible Dienstkonfiguration, um die Effizienz und Sicherheit moderner Kommunikationsnetze zu steigern.

Infosim kommt in der Gesamtarchitektur aufgrund der vorhandenen Expertise und der Bereitstellung ihrer Softwarelösung für das Netzwerkmanagement in der Demonstrationsinfrastruktur eine zentrale Rolle bei der Integration der vielen unterschiedlichen Komponenten und Systeme zu. Ein Schwerpunkt war hier die Berücksichtigung von Push- und Pull-basierten Monitoring-Ansätzen, auf die in Abschnitt 2.1.2 noch genauer eingegangen wird. Auch die Einbindung passender künstliche Intelligenz (KI)-basierter Ansätze an unterschiedlichen Stellen des Managements gehörte zu den Schwerpunkten von Infosim.

Ein besonderer Erfolg der im Projekt erarbeiteten Architektur lag darin, dass diese in der Abschlussdemo mit mehreren integrierten Demonstratoren erfolgreich angewendet und verifiziert wurde, siehe Abschnitt 2.1.6. Während der gesamten Projektlaufzeit wurde eine enge Zusammenarbeit mit den anderen Hauptphasen des Projekts (Umsetzung und Demo) aufrechterhalten, um sicherzustellen, dass die neuesten Entwicklungen als Aktualisierungen in die Architektur mit einfließen.

2.1.1.2 Techno-ökonomische Analyse

Bei einer techno-ökonomischen Analyse eines Netzwerkes müssen auch solche Aspekte berücksichtigt werden, die speziell das Netzwerkmanagement betreffen. Zu diesem Zweck hat Infosim die Datenerfassung mit Streaming Network Telemetry auf der Grundlage eines künstlichen Internet Service Provider (ISP)-Netzes untersucht. Die Bewertung eines Netzwerkes hängt von einer effizienten Verwaltung der Datenspeicherung ab, da die Datenmengen aufgrund von Faktoren wie den Messintervallen und der Menge der Interface-Messungen stark schwanken. Um dieser Komplexität zu begegnen, wurde ein künstliches

Tabelle 1: Anzahl der Geräte im künstlichen deutschen ISP-Netz

Funktion	Anzahl der Geräte
Peer	138
Border	12
Core	10
Distribution	48
Point of presence (POP)	299
MDF	8307

deutsches ISP-Netz konzipert und aufgebaut (Abbildung 2), welches die Erkenntnisse aus der Zusammenarbeit mit weiteren Industriepartnern einbezieht. Dieses Referenznetz ist auch in verschiedenen anderen Teilen des Projektes, insbesondere im Bereich der Kapazitätsplanung, siehe Abschnitt 2.1.5, zum Einsatz gekommen. Die Netzarchitektur umfasst alle Geräteebenen, von den Peer-Verbindungen, bis zu den Hauptverteilern, auch Main Distribution Frames (MDFs) genannt. Die vollständige Liste der in diesem Modell enthaltenen Geräte findet sich in Tabelle 1.

Insgesamt resultiert daraus ein Netzwerk aus 8.814 Geräten (Knoten) und 9.222 Verbindungen (Kanten) zwischen diesen Geräten. Jede Verbindung wird mit zwei Interface-Messungen (Quell- und Zielgerät) ausgewertet. Die meisten Messungen werden jedoch an dem Interface vom MDF zum Endnutzer vorgenommen. Unter der Annahme, dass ein MDF-Switch mit 48 Anschlüssen verwendet wird, ergibt dies ein Maximum von 398.736 Verbindungen bzw. Interface-Messungen. Für eine typische Interface-Messung wird eine realistische Schätzung von 1 kB pro Zeitpunkt verwendet. Die Zuwachsrate für die Gesamtdatenmenge wird dann als Produkt aus Daten pro Messung und Anzahl der Messungen berechnet. Eine stochastische Variation in der Anzahl der Ports der verwendeten MDF-Geräte wird dabei zusätzlich berücksichtigt. Als Annahme werden ca. 60 % der Ports verwendet, d. h. ungefähr 29 Ports pro MDF. Zusätzlich wird eine großzügige Standardabweichung von 50 % der zuvor genannten Portnutzung implementiert. Die Entwicklung der Datenmengen folgt dementsprechend der folgenden stochastischen Evolutionsgleichung:

$$
\begin{aligned}
dV &= r_{\text{data}} \cdot (n_{\text{isp}} + n_{\text{end}})\, dt + r_{\text{data}} \cdot n_{\text{end}} \sigma\, dW_t \\
r_{\text{data}} &= \text{Daten pro Messung} \\
n_{\text{isp}} &= \text{Anzahl der Interfaces (Endnutzer nicht miteinbezogen)} \\
n_{\text{end}} &= \text{Anzahl der Interfaces von MDF zu Endnutzer} \\
\sigma &= \text{Standardabweichung für den Prozentsatz der genutzten Endnutzer-Ports}
\end{aligned}
$$

Nach dieser Berechnung ergibt sich, dass nach einem Jahr der Messungen im Sekundentakt die gesammelten Daten in etwa 1400 TB betragen. Diese Daten werden mit Hilfe von Aggregationstechniken signifikant reduziert:

- Nach 14 Tagen Wechsel zu minutengenauen Daten: Reduktionsfaktor = 60

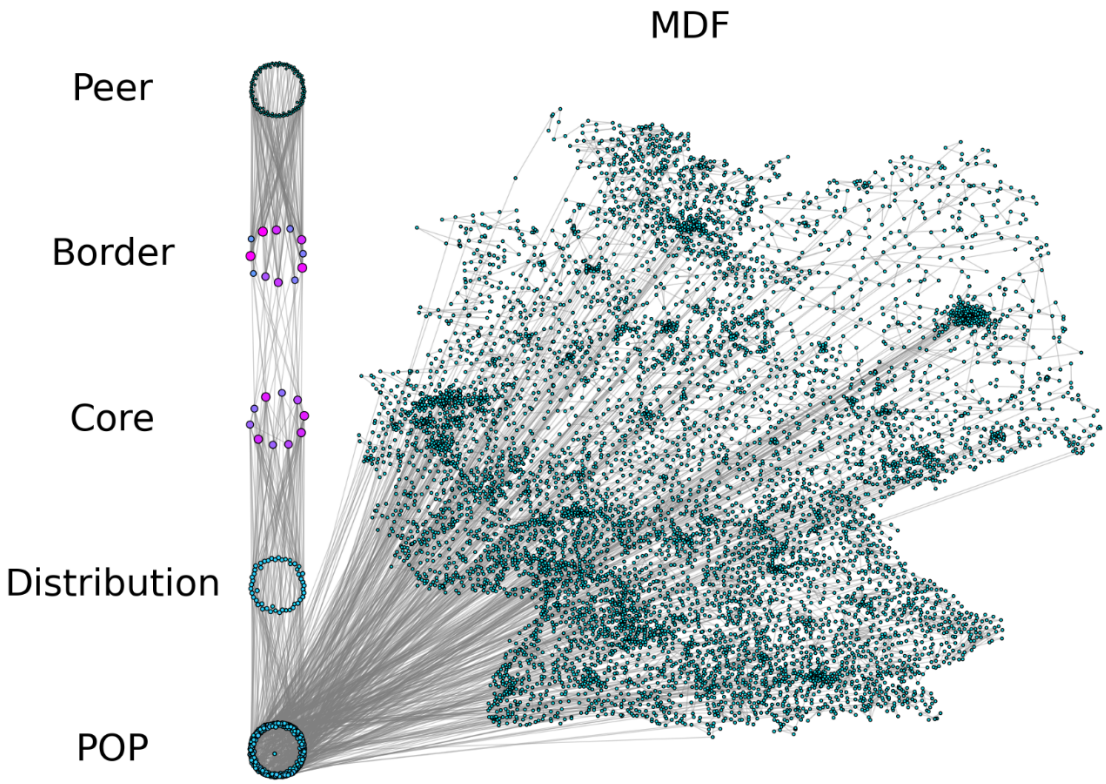


Abbildung 2: Visualisierung des künstlichen ISP-Netzes, das für die techno-ökonomische Analyse der Datenspeicherung verwendet wird: Jeder Knoten stellt eines der verschiedenen Geräte dar. Größe und Farbe der Knoten variieren mit ihrem Knotengrad, d. h. der Anzahl der Verbindungen zu und von diesem Knoten. Für diese Visualisierung wurden nur MDF-Geräte geografisch verteilt. Graue Linien zeigen die Verbindung zwischen zwei Geräten an.

- Nach 60 Tagen Wechsel auf stündliche Daten: Reduktionsfaktor = 60
- Nach 120 Tagen Wechsel zu achtstündigen Daten: Reduktionsfaktor = 8

In unserem Beispiel führt dies zu einer Gesamtmenge an Daten im Bereich von 60 TB, was die Notwendigkeit einer sinnvollen Datenaggregation demonstriert (Abbildung 3).

Zusammenfassend lässt sich feststellen, dass Aspekte, die sich auf das Management eines Kommunikationsnetzes und insbesondere auch auf die feingranulare Überwachung der verschiedenen Systeme im Netz beziehen, durchaus auch eine wichtige Rolle für die techno-ökonomische Gesamtanalyse spielen.

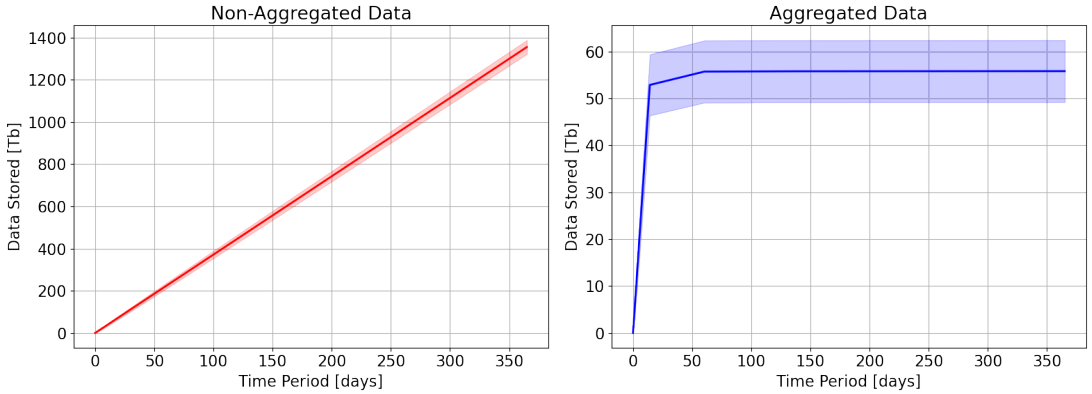


Abbildung 3: Vergleich der Gesamtdaten, die ohne (links) und mit (rechts) der Datenaggregation über ein Jahr hinweg gesammelt wurden: In dem künstlichen ISP-Netz wurden Interface-Messungen im Sekundentakt angenommen.

2.1.1.3 KPIs

Eine weitere Aufgabe im Projekt war die Definition von relevanten KPIs zur Leistungsbewertung, welche den implementierten Konzepten, Technologien und Lösungen zugeordnet sind und schließlich in den entwickelten Demonstratoren gemessen werden können. Infosims Schwerpunkt lag hierbei vor allem auf solchen KPIs, die sich im Bereich Netzwerk- und Servicemanagement ergeben, vom Endgerät bis hin zum zentralen Management.

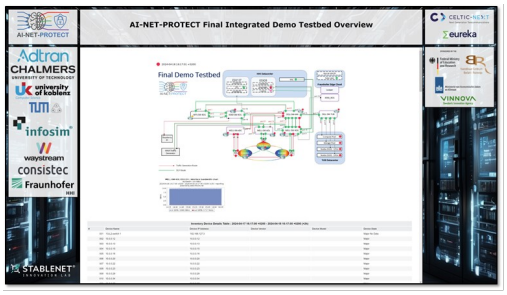
KPIs geben nicht nur Auskunft über den generellen operativen Status eines Netzwerks, sondern gleichzeitig auch Einblicke in die übergreifende Leistungsfähigkeit und mögliches Optimierungspotential. Hier spielen Themen wie Leistungsfähigkeit (Performance), u. a. in Form von Bandbreitennutzung, Latenz oder Paketverlustrate, Zuverlässigkeit (Reliability), u. a. in Form von Betriebszeit/Stillstandzeit, Mittlere Zeit zwischen Fehlern (MTBF), Mittlere Reparaturzeit (MTTR) und Effizienz (Efficiency), u. a. in Form von Ressourcennutzung, Betriebskosten und Netzdurchsatz gleichermaßen eine Rolle.

Gemeinsam mit den Partnern aus dem Konsortium wurden in einem iterativen Prozess relevante KPIs erarbeitet und mit den Aktivitäten und Demonstratoren des Projekts in Verbindung gebracht. Da andere Partner beispielsweise einen Schwerpunkt auf den Bereich Deep Packet Inspection (DPI) gelegt hatten und KPIs in diesem Bereich bereits sehr gut abdeckten, ergänzte Infosim aus dem Blick des Netzwerkmanagements vor allem solche KPIs, welche geräte- oder servicebasiert erfasst werden können.

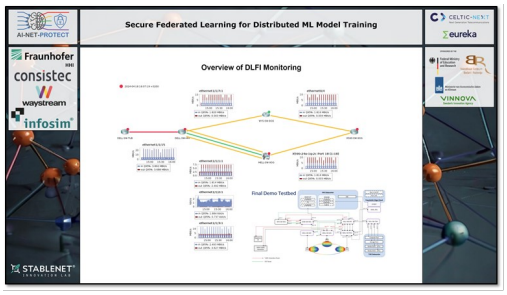
Als konkretes Ergebnis aus diesen Akivitäten wurden insbesondere in den verschiedenen Demonstratoren, die auf der endgültigen Demo-Architektur von AI-NET-PROTECT laufen, für die einzelnen Anwendungsfälle jeweils eine Anzahl von geeigneten KPIs identifiziert. Für jeden dieser KPIs wurde die geeignete Art der Überwachung (telemetriebasiert, Simple Network Management Protocol (SNMP)-basiert, basierend auf aktivem Probing oder Skriptmessungen) identifiziert und als Proof-of-Concept (PoC) implemen-

tiert. Die Ergebnisse für die verschiedenen Demonstratoren wurden auf spezifischen Dashboards für die verschiedenen Demos dargestellt.

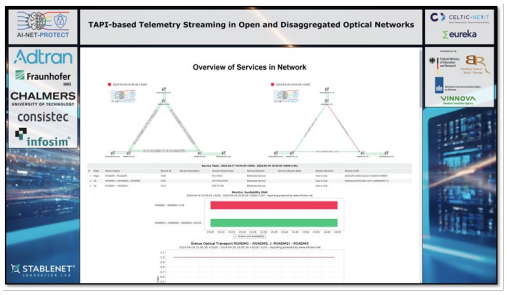
Abbildung 4 gibt einen Überblick über ausgewählte Dashboards, die für die gemeinsamen Demonstratoren in der Demo-Umgebung des HHI erstellt wurden. Details zu den Demonstratoren folgen im Abschnitt 2.1.6. Die KPIs reichen von einfachen Ping-Messungen und Interface-Statistiken über hostbasierte CPU- und Speichermessungen und Ähnliches bis hin zu spezifischen Service-Verfügbarkeits-KPIs, die eine komplexere Logik über verschiedene individuelle Services hinweg beinhalten. Messintervalle können dabei je nach Use Case individuell angepasst und die Darstellung der Daten nach passenden Zeiträumen aggregiert werden (Min, Max, Avg, Quantile).



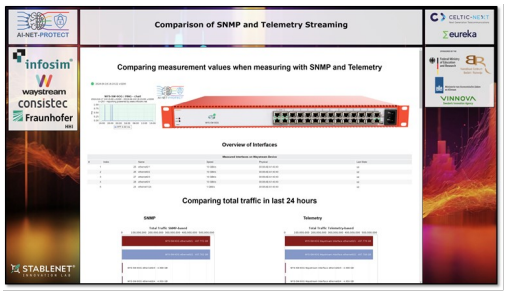
(a) Generelles Architektur Dashboard



(b) Dashboard zur DLFI Demo



(c) Dashboard zur TAPI Demo



(d) Dashboard zur SNMP/Telemetry Demo

Abbildung 4: Überblick über verschiedene Dashboards mit KPIs

2.1.2 Streaming Network Telemetry

Im Gegensatz zur traditionellen Netzwerküberwachung mit SNMP, bei der Informationen und Daten von Netzwerkgeräten aktiv in Intervallen vom Netzwerkmanagementsystem (NMS) abgefragt werden (Polling), ermöglicht Streaming Network Telemetry eine kontinuierliche Übertragung ohne, dass explizite Anfragen erforderlich sind. Daraus ergeben sich einige Vorteile: Kontinuierliches Streaming ermöglicht sehr kurze Messintervalle, so dass eine Überwachung nahezu in Echtzeit möglich ist. Die höhere Auflösung liefert detailliertere Informationen, so dass auch kurzzeitige Extremereignisse erfasst werden, die sonst bei längeren Messintervallen gemittelt würden, wie in Abbildung 5 dargestellt.

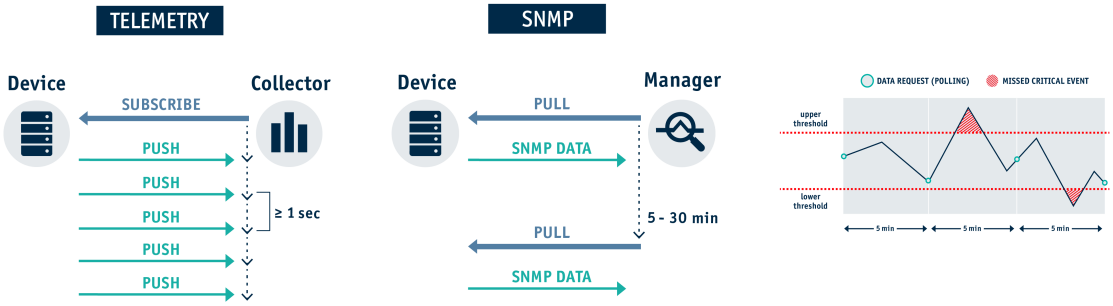


Abbildung 5: Vergleich der grundlegenden Prinzipien bei Telemetrie und SNMP: Bei großen Messintervallen (typisch bei SNMP) werden kritische Events gemittelt und somit nicht erfasst.

Auf der anderen Seite werden aber wesentlich mehr Daten über das Netz übertragen (Traffic), die effizient verarbeitet und analysiert werden müssen.

Modularer Controller

Die grundlegende Architektur von StableNet, dem NMS von Infosim, basiert auf einer Agenten-Server-Struktur. Dabei führt der Agent die Messungen durch, während der Server die Daten zusammenführt, für eine persistente Datenhaltung verantwortlich ist und die Visualisierung der Daten ermöglicht. In großen Netzwerken können mehrere Agenten logisch oder örtlich verteilt werden, um auch eine große Anzahl an Geräten und Messungen handhaben zu können. Die Integration von Streaming Network Telemetry erfordert jedoch eine grundlegende Anpassung der bisherigen Agenten-Architektur. Dafür wurde ein modulares Framework entwickelt, um verschiedene Funktionalitäten in separaten Modulen zu kapseln, die ähnlich einer Microservice-Architektur miteinander interagieren können, wie in Abbildung 6 dargestellt.

Grundlegend basiert Streaming Network Telemetry auf YANG-Datenmodellen. Für das Netzwerkmanagement gibt es einerseits offene und standardisierte Modelle, die unabhängig von allen Herstellern genutzt werden können (z. B. OpenConfig oder von der IETF). Andererseits setzen einige Hersteller auf proprietäre Modelle, welche sie selbst definieren und somit bestmöglich an ihre Anforderungen und Geräte anpassen können. Konkret wurde in diesem Projekt an Schnittstellen für zukünftige Module gearbeitet, um Telemetriedaten verschiedener Hersteller über individuelle Adapter in StableNet integrieren zu können.

2.1.3 Service-Monitoring/-Orchestrierung

Im Forschungsvorhaben SENDATE[1], welches dem Projekt PROTECT vorausging, lag ein Schwerpunkt in der Definition und Umsetzung eines servicebasierten Ansatzes für ein ganzheitliches Netzwerkmanagement. In diesem Kontext werden beispielsweise funktionale Einheiten als Service bezeichnet, die von einem Netzwerk bereitgestellt werden, um

[1]FKZ 16KIS0466, Laufzeit 04/2016 bis 03/2019, `https://doi.org/10.2314/KXP:1683532597`

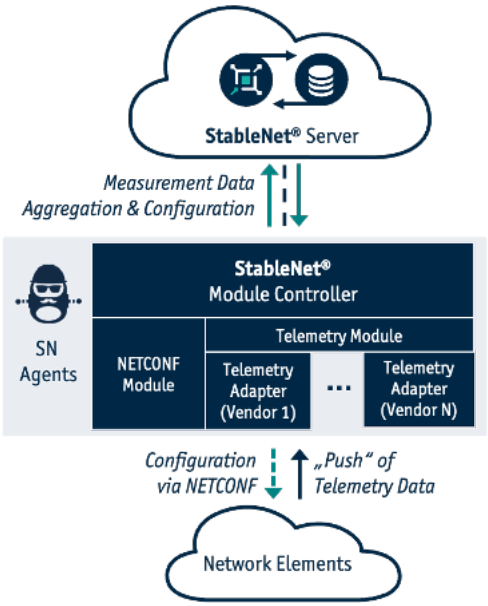


Abbildung 6: Architektur eines modularen NMS-Agenten

bestimmte Anforderungen zu erfüllen. Das kann sowohl physische, virtuelle oder logische Aspekte eines Netzwerkes betreffen. Für die Gestaltung, Überwachung und Optimierung von Netzwerken spielen Services eine zentrale Rolle.

Im vorliegenden Projekt haben wir das generische Service-Modell aufgegriffen und auf verschiedene Anwendungen adaptiert. Ein Anwendungsfall basiert beispielsweise auf dem optischen Transport über die von der Open Networking Foundation (ONF) entwickelten Programmierschnittstelle (API) für Transportnetzwerke (TAPI). Details zu dieser Demo sind in Abschnitt 2.1.6.4 dargestellt.

Services können in dem Modell mithilfe von Attributen beschrieben werden. Auf der oberen Ebene, der *Service Domäne*, unterscheiden wir im vorliegenden Fall zwischen *Optischen Services* und *IP Services*, wobei letzterer für die Demo nicht weiter Beachtung findet. In der Ebene darunter werden die Services in verschiedene Schichten (*Layer*) gruppiert, konkret in *Fasern* und *Wellenlängen*. Das Attribut *Typ* unterteilt Services in Kategorien und legt damit einige grundlegende Eigenschaften fest, beispielsweise Messungen zur Überwachung. In unserem Beispiel unterschieden wir hier die Typen *Physikalische Verbindung*, *E2E Service* und *Optischer Transport*.

Zusätzlich wurde das Service-Modell auch für die Umsetzung des TM Forum Catalyst genutzt und auf die darin betrachtete Anwendung adaptiert (vgl. Abschnitt 2.1.6.6). Zu den bereits oben genannten Service-Schichten wurde hier eine Visualisierung basierend auf geografischen Informationen integriert. Aufgrund der Anzahl an Services in diesem PoC und den damit einhergehenden Verlust an Übersichtlichkeit, wurden zudem neue Darstellungsoptionen integriert, z. B. eine 3D-Darstellung. Dies ermöglichte außerdem die Integration von VR-Technologien und die Darstellung in einem virtuellen Raum.

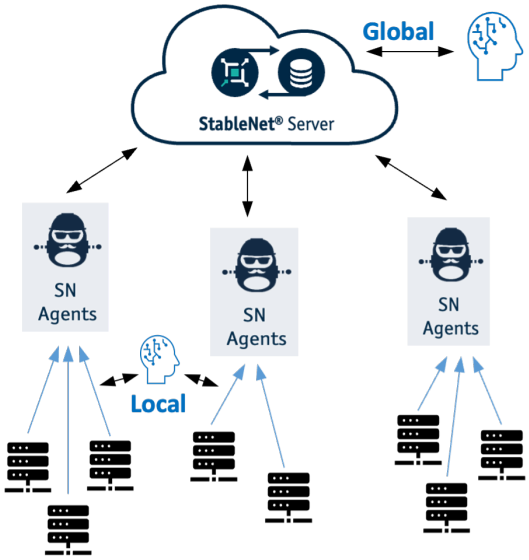


Abbildung 7: Konzept von lokalen und globalen ML-Ansätzen und deren Integration im Umfeld der StableNet-Architektur

2.1.4 KI-unterstützte Netzoperationen

Heutige Kommunikationsnetze sind durch hohe technische Komplexität gekennzeichnet. Heterogene Architekturen, Edge Computing und Network Slicing, sowie steigende Anforderungen an Dienstqualität, Agilität und Flexibilität stellen die Betreiber vor Herausforderungen. Bei großen, verteilten Netzen mit begrenzter Dynamik lassen sich durch den Einsatz fortschrittlicher Technologien (z. B. durch Anwendung von KI) signifikant Ressourcen einsparen, da keine neuen Messpunkte zur Überwachung eingerichtet werden müssen. Innerhalb dieses Projektes war die Erforschung und Erprobung von (verteilten) ML-Algorithmen und den damit einhergehenden Analysen im Kontext des Netzwerkmanagements eine zentrale Aufgabe. Speziell wurde hier zwischen lokaler und globaler Anwendung von ML-Algorithmen und deren möglicher Implementierung innerhalb der Architektur eines NMS unterschieden, konkret am Beispiel von StableNet (siehe Abbildung 7).

Die Server-Agenten-Architektur von StableNet ermöglicht es, mehrere Agenten innerhalb eines Netzwerkes zu verteilen. Jeder Agent überwacht einen lokal abgegrenzten Bereich und befindet sich in Nähe zu den Geräten, der Server bündelt die Messungen der einzelnen Agenten. Diese Architektur ermöglicht auf Agentenebene lokale und unabhängige Analysen einzelner Messreihen, beispielsweise Zeitreihen einzelner Metriken von einzelnen Geräten. Auf Server-Ebene werden Analysen über das gesamte Netzwerk hinweg möglich. Allerdings sind diese globalen Analysen aufgrund der Datenübertragung zwischen Agenten und Server nur mit einem zeitlichen Versatz möglich.

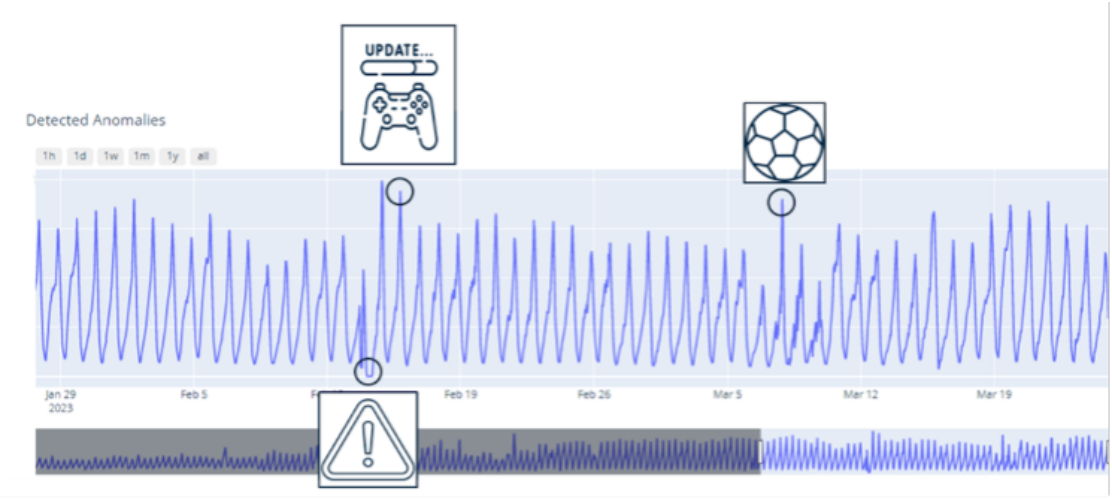


Abbildung 8: Event-basierte Vorhersage und Erkennung von Anomalien in Zeitreihen

2.1.4.1 Anomalieerkennung

Ein wesentlicher Schwerpunkt war die Erkennung von Anomalien, d. h. die automatische Unterscheidung zwischen normalem und anormalem Verhalten. Im Falle einer erkannten Anomalie, kann dann eine Alarmierung der Betreiber/Administratoren ausgelöst werden. Die erste Herausforderung lag bereits in der Definition einer Anomalie in Bezug auf die Art der Daten, d. h. beispielsweise Zeitreihen oder Log-Dateien. Häufig wurden einzelne Ausreißer oder Spitzen als Anomalie betrachtet und mit Hilfe einer relativ einfachen Schwellwerterkennung leicht erkannt. Sobald jedoch die Basislinie nicht mehr konstant war (z. B. Tag-Nacht-Zyklus oder Wochentag vs. Wochenendtag), gestaltete sich dies nicht mehr als trivial. Darüber hinaus gab es auch Anomalien, die eine erklärbare und unkritische Ursache hatten und für die der Algorithmus keinen Alarm auslösen sollte. Beispiele hierfür sind Verkehrsspitzen aufgrund konkreter Ereignisse, wie z. B. ein Fußballspiel, das nur über Streaming-Dienste übertragen wird und der damit verbundene Anstieg des Datenverkehrs in diesem Zeitraum. Unser Ansatz verwendet ein Ereignisgedächtnis, in dem entsprechendes Vorwissen gespeichert und bei der Anomalieerkennung berücksichtigt wird. Die Anomalieerkennung basiert auf einer Vorhersage, der historische Daten zugrunde liegen und die Informationen über bevorstehende Ereignisse einbezieht, die einen Einfluss auf die Daten haben werden. Die Abweichung zwischen Vorhersage und tatsächlichem Wert definiert hierbei die Anomalie (vgl. Abbildung 8). Die Anomalieerkennung ist nicht nur für den Netzbetrieb, sondern auch für die Kapazitätsplanung von besonderer Bedeutung. Der implementierte Algorithmus für die Anomalieerkennung ermöglicht bereits eine Prognose basierend auf der Hisorie der Datenreihe. Durch die Kombination mit einer Ereignis-Datenbank können frühzeitige mögliche Kapazitätsengpässe erkannt und entsprechende Gegenmaßnahmen eingeleitet bzw. die Netznachfrage genauer prognostiziert und die Ressourcenzuweisung optimiert werden. Dies gewährleistet eine effiziente Nutzung der vorhandenen Infrastruktur und wird in Abschnitt 2.1.5

weiter beschrieben. Darüber hinaus haben wir Visualisierungs- und Analysewerkzeuge weiterentwickelt, die zusätzliche Einblicke in das Netzverhalten geben und eine datenbasierte Entscheidungsfindung zur Optimierung des Netzbetriebs ermöglichen.

2.1.4.2 Lokale und globale Vorhersagen

Im Bereich der lokalen Vorhersage und Analyse wurden dezentralisierte Ansätze untersucht, d. h. man trainierte die Modelle zunächst auf globaler Ebene, setzte sie aber anschließend verteilt ein, um die Skalierbarkeit zu verbessern. Zu den hier betrachteten Anwendungsfällen gehören verschiedene Arten und Implementierungen der Erkennung von Anomalien und der Vorhersage von Wertkurven für einzelne Zeitreihendaten. Diese Fälle wurden unter dem Aspekt betrachtet, wie unterschiedliche Daten in ein Modell einfließen können, um mögliche Zusammenhänge abzubilden und damit die Qualität der Vorhersagen zu erhöhen. Das zentrale NMS kann fehlende Messpunkte kompensieren, indem sie Modelle zur Vorhersage des aktuellen Zustands verwendet. Ausgehend von dieser Beobachtung wurden die ausgewählten Anwendungsfälle gezielt daraufhin analysiert, wie Vorhersagemodelle einerseits von einer Messstation zur Beurteilung der Relevanz der gesammelten Daten, und andererseits von der zentralen Anwendung zur Vorhersage von Zuständen mit ausreichender Genauigkeit genutzt werden können. Im Bereich der globalen Vorhersage- und Analysemodelle wurden zentralisierte Ansätze, die zwar rechenintensiver, aber auch vielseitiger als dezentralisierte lokale Ansätze sein können, näher untersucht. Als Beispiele für Anwendungsfälle wurden die Erkennung von Anomalien und die Vorhersage von Wertetrends über verschiedene Zeitreihen und verteilte Systeme hinweg, sowie die Korrelation verschiedener Daten zur Erkennung ähnlichen Verhaltens betrachtet. Darüber hinaus waren die Integration lokaler und globaler Störungen, Schnittstellenanpassung und -abstimmung, Feinabstimmung, Untersuchung von Wechselwirkungen und die Optimierung auf der Basis von Wechselwirkungen relevante Themen dieser Aufgabe. Die Untersuchungen, die in lokal und global unterschieden werden, wurden in einem Gesamtsystem kombiniert. Dazu wurden lokale Verfahren auf der Datenebene, z. B. mittels eines protokollunabhängigen Paketprozessors (P4), möglichst nahe an der Messstelle implementiert. Schließlich können die global verfügbaren Informationen genutzt werden, um die Kombination verschiedener Messfunktionen auf der Datenebene zu optimieren.

Lokale Datenanalysen

Auf lokaler Ebene wurde zunächst eine Datenpipeline eingerichtet, in der ML-Modelle zur Vorverarbeitung des Datenstroms von Netzwerkgeräten angewendet werden, bevor diese in das globale NMS integriert werden, wie in Abbildung 9 dargestellt. Ein Datenkollektor nimmt die vom Gerät gesendeten Telemetriedaten auf und leitet diese an eine Kafka-basierte Streaming-Plattform weiter. Kafka ermöglicht nahezu in Echtzeit die Verarbeitung eines Datenstroms, bevor dieser von einem StableNet-Agenten abgeholt wird. In der Kafka-Streaming-Plattform wurden verschiedene lokale Modelle für die Vorverarbeitung implementiert und getestet. Ziel war es, Anomalien mit geeigneten Modellen möglichst in Echtzeit zu erfassen und damit die Aggregation der Daten bei der

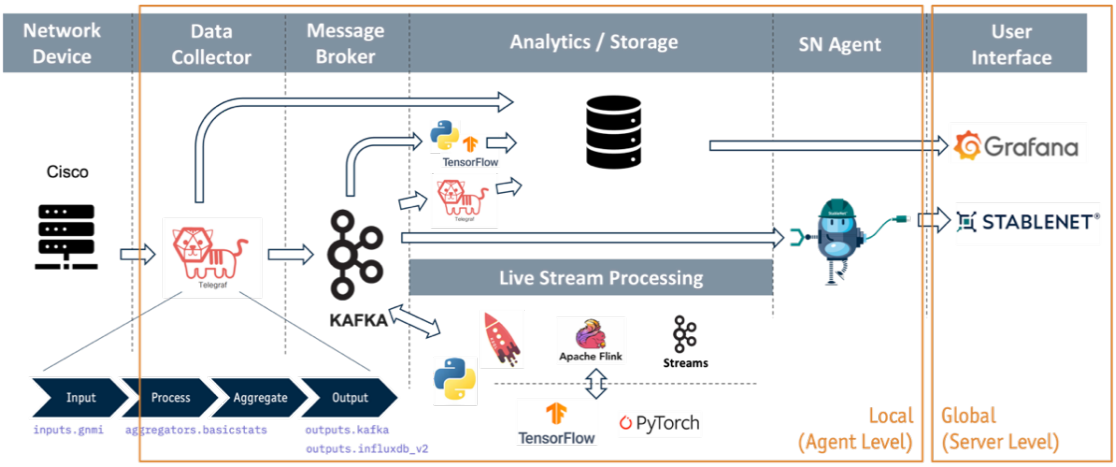


Abbildung 9: Datenverarbeitung auf lokaler (Agenten-) Ebene

Integration in das NMS zu steuern. Dies ermöglicht zum einen eine Datensparsamkeit für unauffällige Daten und zum anderen eine gute Möglichkeit zur Nachbearbeitung und Kombination mit anderen hochauflösenden Datenströmen.

Zu Demonstrationszwecken wurden während der Projektdurchführung verschiedene PoCs umgesetzt. In einem ersten PoC wurden die von Netzwerkgeräten gestreamten Daten zunächst über einen Kollektor mit einem gNMI-Plug-In abonniert und an eine Kafka Event-Streaming-Pipeline übergeben. gNMI ist eine von Google entwickelte gRPC-Netzwerkverwaltungsschnittstelle und ermöglicht die Bearbeitung der Konfiguration von Netzwerkgeräten, sowie das Anzeigen von Betriebsdaten. Der über gNMI bereitgestellte Inhalt wird mit YANG-Datenmodellen strukturiert. Die nun geordneten Daten können mithilfe von Stream-Processing in nahezu Echtzeit weiterverarbeitet werden, bevor diese entweder über ein Dashboard visualisiert, oder in ein NMS überführt werden. Exemplarisch wurden hier zwei Verarbeitungsschritte demonstriert: Zum einen konnten Anomalien mithilfe verschiedener Algorithmen gefunden werden. Die detektierten Anomalie-Events wurden in einen eigenen Kafka-Stream überführt und können so auch separat in das NMS eingelesen werden. Daneben wurde eine ML-Applikation entwickelt, die basierend auf der Historie einer Metrik des Streams (z. B. ein- und ausgehenden Pakete eines Interfaces) einen Vorhersage ermöglicht. Abbildung 10 zeigt die für diesen PoC umgesetzte Datenpipeline und ein dafür erstelltes Dashboard zur Visualisierung der Ergebnisse.

Es wurden verschiedene Frameworks zur Anomaliedetektion getestet: Facebook Prophet, TensorFlow und das Anomaly Detektion Toolkit (ADTK). Als Datenkollektor wurde Telegraf mit gNMI Input und einem Kafka Output Plugin genutzt. Die im Kafkastream vorgehaltenen Daten können in nahezu Echtzeit als Stream direkt prozessiert werden. Hierfür gibt es u. a. Tools wie Apache Flink oder Kafka Streams. Da viele ML-Frameworks in Python verfügbar sind und die Frequenz der Telemetrie-Daten geräteseitig auf 10 Sekunden limitiert war, wurde ein anderer Ansatz genutzt, indem die Daten

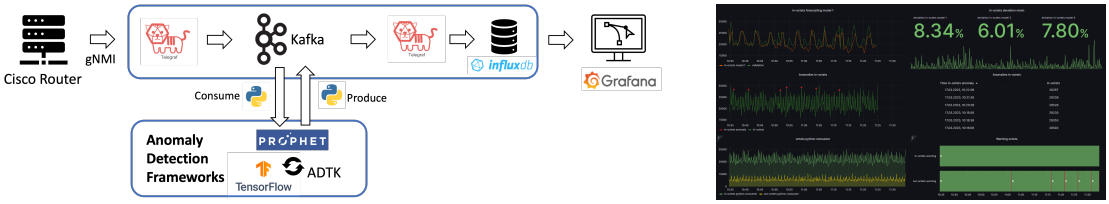


Abbildung 10: Datenpipeline und Dashboard zur Detektion von Anomalien in Streaming Network Telemetry Daten

zunächst in Python ausgelesen, mit den verschiedenen ML-Methoden verarbeitet und wieder zurück nach Kafka gestreamt wurden. Generell konnte mit allen getesteten ML-Algorithmen Anomalien erkannt werden. Jedoch zeigten sich Unterschiede in der Nutzerfreundlichkeit und der Möglichkeit, Randbedingungen zu berücksichtigen. Beispielsweise erlaubt der Facebook Prophet Algorithmus saisonale Einflüsse auf verschiedenen Skalen mit zu berücksichtigen (Tag/Nacht, Wochentag/Wochenende, etc.). Da dies bei Netzwerkdaten auch relevant ist, wurden dieser Algorithmus für viele weitere Arbeiten genutzt.

Ein weiterer PoC, welcher zusammen mit den Partnern Waystream und Fraunhofer HHI umgesetzt wurde, ist in Abschnitt 2.1.6.3 beschrieben. Darin wurden SNMP und Telemetrie hinsichtlich verschiedener Messintervalle und deren Auswirkungen untersucht.

Globale Datenanalysen

Hier wurde z. B. an einem Anomaliescore weitergearbeitet, der die Auswirkung der Anomalie innerhalb einer gesamten Netztopologie berücksichtigt und bewertet (vgl. Abbildung 11)

Auf globaler, netzweiter Ebene besteht die Möglichkeit, dieses Thema durch den Vergleich verschiedener Zeitreihen anzugehen und den „Sonderling“ zu erkennen. Um diesen Ansatz zu verfolgen, werden die verschiedenen Zeitreihendaten zunächst nach ähnlichem zeitlichen Verhalten geclustert, siehe Abbildung 12. Dies ist komparabel dazu, wie Bilder von einer Bilderkennungssoftware behandelt werden, die ähnliche Gesichter mit Zuordnungsmerkmalen clustert.

Auf dieser Grundlage wird es einfacher, die Bilder/Zeitreihen zu finden, die außerhalb der bestehenden Cluster zu liegen scheinen, und festzustellen, ob es sich tatsächlich um echte „Ausreißer“ mit Anomalien handelt, oder nur um leicht abweichende Bilder, die daher nicht automatisch als Teil eines Clusters erkannt werden. Im nächsten Schritt wird ein aktiver Lernansatz angewandt, bei dem der Benutzer aufgefordert wird, entweder zu entscheiden, ob das „abweichende“ Bild in eines der vorhandenen Cluster passt, oder ob das es tatsächlich ein anormales Verhalten aufweist und separat behandelt werden sollte.

2.1.5 Kapazitätsplanung

Einen weiteren Schwerpunkt im Projekt bildeten die Arbeiten zur Kapazitätsplanung, Topologieanalyse und Visualisierung.

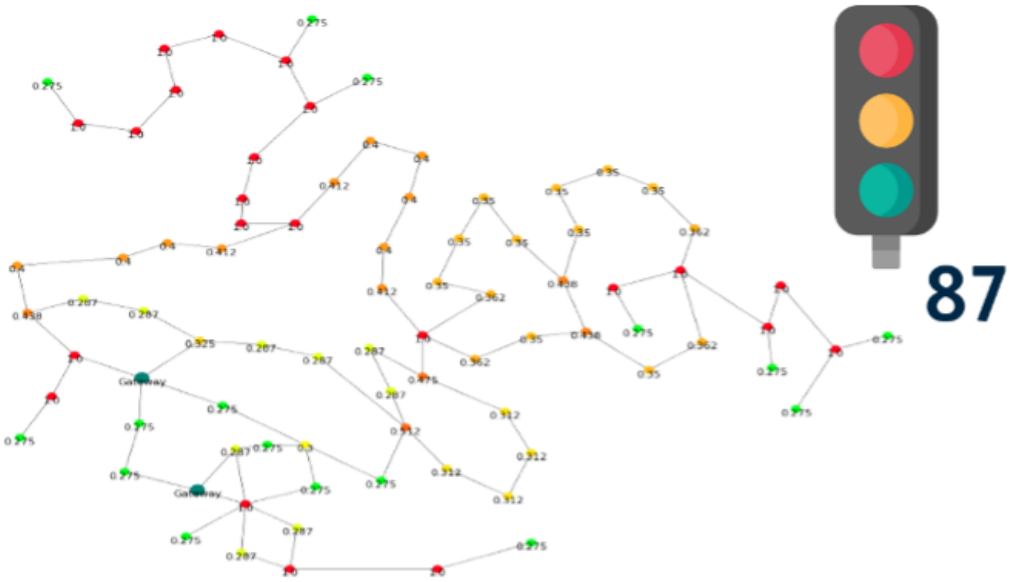


Abbildung 11: Darstellung des Anomaliescores innerhalb einer Netzwerk-Topologie

Konkret wurden im Bereich der Kapazitätsplanung verschiedenartige Möglichkeiten erarbeitet, um Zeitreihen genauer analysieren und ihre Entwicklung vorhersagen zu können. Wo immer möglich, wurde dabei der Austausch mit bestehenden Kunden und Partnern gesucht, um darüber Feedback von weiteren Seiten zu erhalten, welche Ansätze auch in der Praxis besonders relevant sein könnten. Ein konkreter Ansatzpunkt, der im Projekt sehr stark weiterverfolgt und ausgearbeitet wurde, ist die Analyse des Einflusses von Ereignissen/Events auf Zeitreihen und wie diese auch für Prognosen berücksichtigt werden können. Beispiele hierfür sind u. a. die Veränderung des Verkehrsaufkommens bei bestimmten Ereignissen wie der Online-Übertragung von Sport-Events oder dem automatischen Einspielen von Updates auf zehntausenden Endgeräten wie Spielekonsolen. Andere Arten von Events können auch Störfälle im Netzwerk oder Unwetter sein.

Im Bereich der Topologieanalyse wurden Ansätze erarbeitet, um unterschiedlichste Metriken zur Bewertung von Netzwerken und den darin enthaltenen Services betrachten zu können. Diese Erkenntnisse unterstützen beispielsweise auch dabei, Engpässe im Netz noch schneller/besser identifizieren zu können oder Erweiterungsmöglichkeiten des Netzes zu finden.

Im Bereich der Visualisierung wurde eine 3D-Darstellung der Analyseergebnisse erarbeitet und stetig erweitert, um eine bessere interaktive Analyse der Topologien zu ermöglichen. Abbildung 13 zeigt Beispiele für eine solche Darstellung und Analyse einer Netztopologie inkl. der Farbmarkierungen, die eine der verfügbaren Metriken darstellen.

In dem umgesetzten webbasierten PoC zur metrikbasierten Analyse von Netzwerkgraphen wählen Nutzer eine Weather Map, einen Nachbarschaftsgraphen zwischen Geräten oder einem Netzwerkservice, aus dem NMS aus. Zusätzlich kann man eine Graphme-

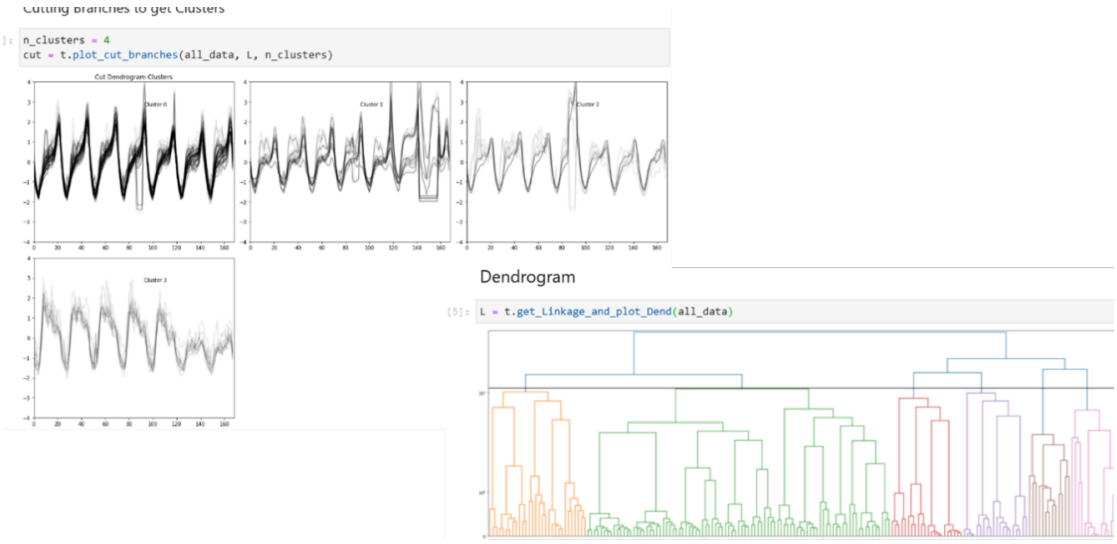


Abbildung 12: Datenverarbeitung auf globaler (Server) Ebene: Einzelne Zeitreihen der gleichen Metrik von verschiedenen Geräten können geclustert werden.

(a) Graph und Knoteneinstellungen

(b) Graph und Linkeinstellungen

Abbildung 13: Kapazitätsplanung: erweiterte Topologieanalyse

trik selektieren, nach der der Graph eingefärbt werden soll. In einem Edit-Modus ist es darüber hinaus möglich, den Einfluss verschiedener topologischer Veränderungen am Netz zu untersuchen. Die Arbeiten an der Kapazitätsplanung waren auch eng mit der techno-ökonomischen Analyse und insbesondere der in diesem Kontext erarbeiteten Referenztopologie, welche bereits unter Abschnitt 2.1.1.2 genauer erklärt wurde, verzahnt.

2.1.6 Demonstrationen/PoCs

Einer der sehr zentralen Punkte für einen Großteil aller Aktivitäten im Projektverlauf war es, stets die praktische Umsetzbarkeit fokussiert im Blick zu behalten und, wo immer möglich, auch als PoC demonstrieren zu können. Daher wurde sowohl seitens Infosim individuell, aber auch in Zusammenarbeit mit verschiedensten Konsortialpartnern stets Wert darauf gelegt, bestmögliche Testbeds und Demos zur praktischen Vorführung von

Projektergebnissen zu erarbeiten. Es gab dabei insgesamt eine Vielzahl verschiedener Aktivitäten und Kooperationen, welche nicht alle in diesem Bericht aufgezählt werden können, weshalb entschieden wurde, sich auf die Darstellung einer Hauptauswahl zu fokussieren. In den folgenden Abschnitten wird zuerst die generelle Demo-Architektur der „Final Project Demo“, welche im Projekt vom Gesamtkonsortium erarbeitet wurde, kurz dargelegt und danach Hauptaktivitäten mit großer Beteiligung seitens Infosim weiter im Detail erläutert.

2.1.6.1 Demo-Architektur

Wie in Abschnitt 2.1.1 bereits eingangs gezeigt, war es eine gemeinsame Errungenschaft des ganzen Projektkonsortiums, dass eine Gesamtarchitektur für ein offenes und disaggregiertes Ökosystem erarbeitet werden konnte, welche die verschiedenen Teilaspekte und Komponenten von den jeweiligen Partnern mitberücksichtigt und in den richtigen Zusammenhang bringt.

Im Rahmen der Demoaktivitäten wurde beim Projektpartner Fraunhofer HHI ein Gesamtdemo-Setup aufgebaut, welches viele Teile der Architektur auch praktisch als PoC abbildete. Dieses ist in Abbildung 14 dargestellt. Es enthält Hardware- und Software-Komponenten verschiedener Partner und konnte als Setup-Referenz verwendet werden. Abbildung 15 zeigt eine Weather Map der Demo in StableNet. Die Punkte (rot/grün) sind Statusindikatoren, entweder für Interfaces, oder das Gerät selbst. Neben den optischen Komponenten des Core-Rings wurden diverse IP-Komponenten mit integriert.

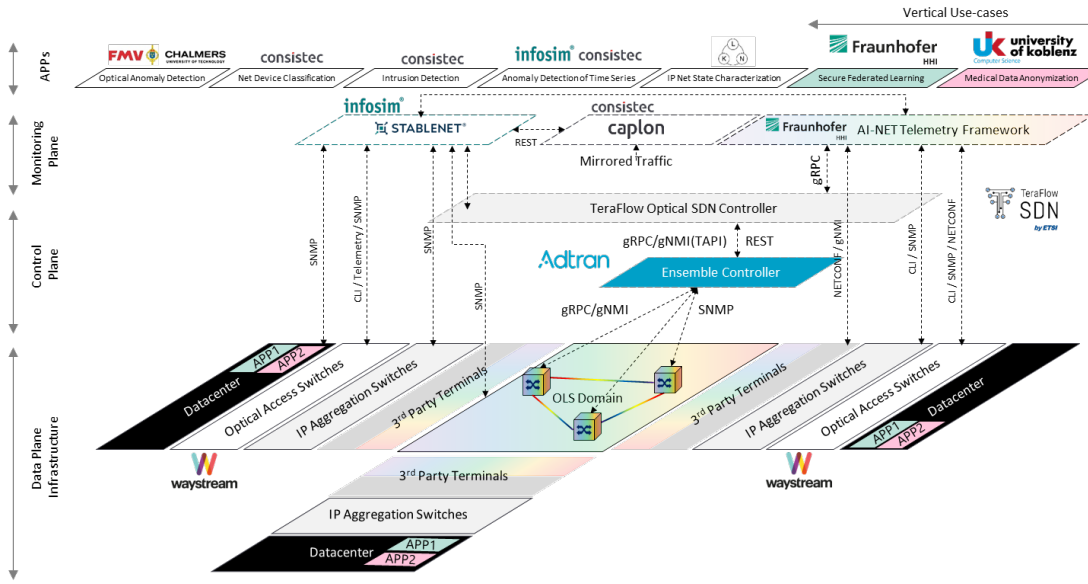


Abbildung 14: Finale AI-NET-PROTECT Demo-Architektur, wie sie zum Projektende beim Partner Fraunhofer HHI aktiv ist

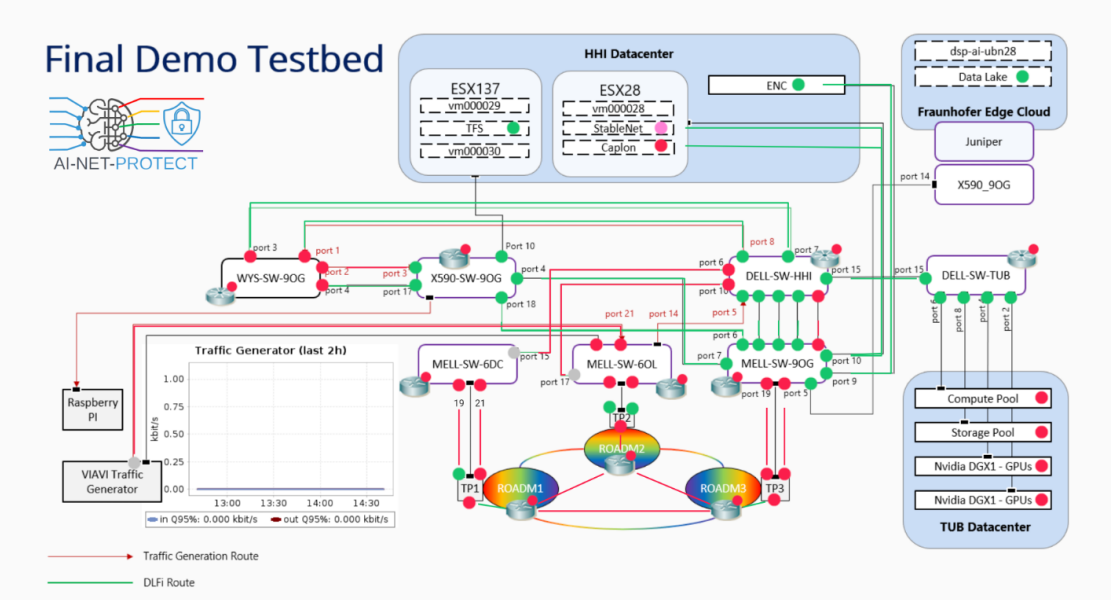


Abbildung 15: StableNet Weather Map für die AI-NET-PROTECT Demo-Infrastruktur beim Partner Fraunhofer HHI

2.1.6.2 AI-basiertes Netzwerkmanagement eines Lehrstuhl-Netzwerkes

Dieser PoC wurde gemeinsam mit den Partnern TUM-LKN und consistec durchgeführt. Der Lehrstuhl für Kommunikationsnetze betreibt ein heterogenes Netzwerk, bestehend aus verschiedenen Rechnern (z. B. Mitarbeiterarbeitsplätze, Studentenlabor), spezieller forschungsbezogener Hardware (Testbeds) und einer Infrastruktur, die verschiedene Dienste im Netzwerk bereitstellt. Durch die Integration der Technologien von Infosim und consistec und die Zusammenführung mit dem Know-how der Forscher am LKN demonstrierten wir eine integrierte Monitoring-Lösung für ein solches Netzwerk. Basierend auf diesen Daten, führten wir eine vertiefte Analyse des Netzzustandes durch. Diese beinhaltet die Erkennung von nicht-normalen Zuständen durch die Anwendung von NOracle, das zuvor am LKN in Zusammenarbeit mit Infosim entwickelt wurde. Der Ansatz verwendet Flussdaten und so genannte stochastische Blockmodelle (SBMs), um Netzwerk-Hosts in Gruppen aufzuteilen und potenziell übergeordnete Beziehungen zwischen diesen Gruppen aufzudecken. Anschließend können die trainierten SBMs verwendet werden, um abnormales Netzwerkverhalten zu identifizieren. Der Aufbau des Netzwerks und die Architektur des PoCs ist in Abbildung 16 dargestellt.

Überwacht wurde in erster Linie der Hauptserverraum des Lehrstuhls. Hier liefen auf mehreren Servern eine Vielzahl von VMs für produktive Dienste, sowie Lehr- und Forschungsaufgaben. Im Kern verbanden zwei Core-Switches die Server und Speichersysteme lokal miteinander. Außerdem stellten sie die Verbindung zu den anderen Teilen des Lehrstuhlnetzes her. Mit dem NMS StableNet konnten Geräte im gesamten Netzwerk erkannt, sowie SNMP-basierte Überwachungsdaten und eine Layer-2-Topologieübersicht

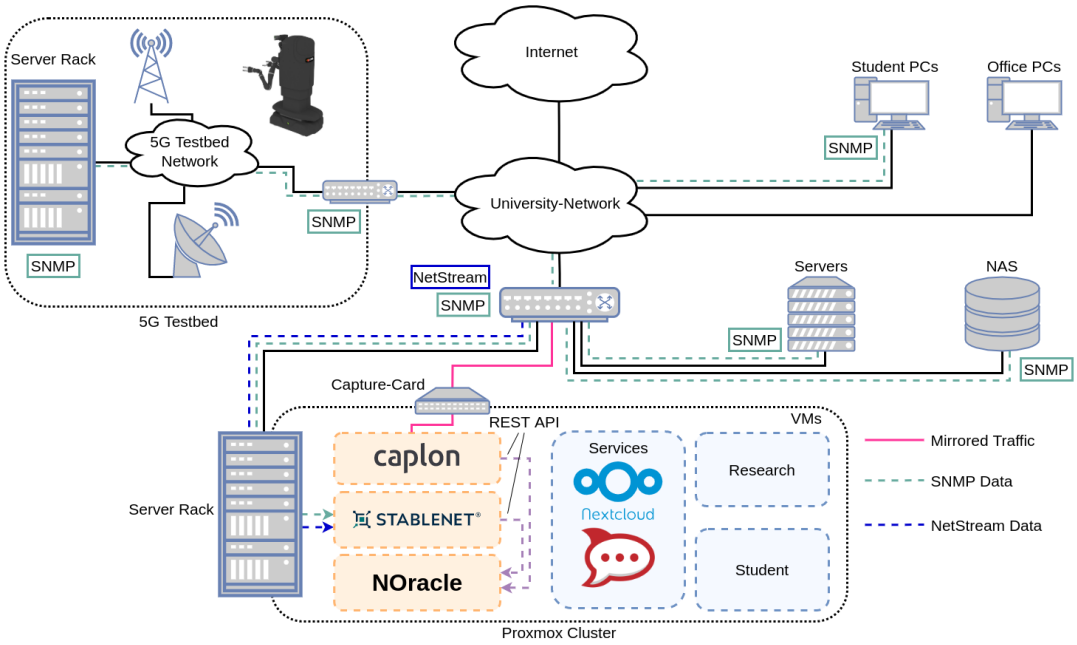


Abbildung 16: Architektur zum AI-basierten Management eines Lehrstuhl-Netzwerkes (siehe Abschnitt 2.1.6.2)

bereitgestellt werden. Darüber hinaus sammelte StableNet über NetStream Flussdaten von beiden Core-Switches und stellte sie NOracle zur Verfügung. Begrenzt durch die Möglichkeiten der Switches stellten diese Flussdaten nur eine Stichprobe der Pakete dar (sampling). caplon, die Softwarelösung von consistec, verarbeitete den von beiden Core-Switches gespiegelten Rohverkehr mit einer speziellen Capture-Hardware. Dadurch konnte der Netzverkehr vollständig erfasst und analysiert werden (ohne sampling).Diese Daten wurden ebenfalls NOracle zur Verfügung gestellt.

In der Demonstration zeigten wir unterschiedliche Aspekte des Gesamtsystems. Zunächst konnte man mit den Funktionen der grafischen Benutzeroberflächen von caplon und StableNet, sowie der gegenseitigen Integrationen der beiden Partner einen Gesamtüberblick über das System und einzelne Messwerte erhalten. In NOracle konnte man den „normalen“ Zustand des Netzwerks betrachten und einzelne Verbindungen im Nutzerinterface hervorheben. In der Demonstration wurde ein künstlicher „Vorfall“ im Netzwerk ausgelöst, beispielsweise ein Port Scan, der von einem Endgerät ausgeht. Dieser war in NOracle sofort sichtbar. Die abschließende Integration verwendete Daten von StableNet und caplon, sowie die entsprechenden NOracle-Ausgaben, um die Verkehrsänderungen während des Vorfalls zu beschreiben und festzustellen, welche Maschinen beteiligt waren. Mit diesen Erkenntnissen konnte das System automatisch auf den Vorfall reagieren und entsprechende Maßnahmen einleiten. In diesem Beispiel wurde der entsprechende Port am Switch deaktiviert und das Endgerät, das den Vorfall ausgelöst hat, damit vom Netzwerk isoliert.

2.1.6.3 Vergleich von SNMP und Streaming Network Telemetry

In diesem PoC wurden unterschiedliche Technologien zum Monitoring von Netzwerkgeräten miteinander verglichen. Konkret ging es darum, die Vor- und Nachteile von SNMP und Streaming Network Telemetry einander gegenüberzustellen. Streaming Network Telemetry ist ein aktueller Ansatz, um klassische Protokolle für die Netzwerküberwachung zu ersetzen. SNMP wird seit Jahrzehnten zur Netzwerküberwachung verwendet. Einige Grundlagen zu diesen beiden Ansätzen sind auch in Abschnitt 2.1.2 dargestellt. Im PoC wurde ein Ansatz gezeigt, um einen Vergleich dieser Techniken auf echten Geräten durchzuführen.

Beispielhaft wurde ein Switch des Projektpartners Waystream eingesetzt, der in der Testumgebung am Fraunhofer HHI eingebaut war. Dieser kann so konfiguriert werden, dass er regelmäßig Messdaten an ein NMS sendet, lässt sich jedoch alternativ auch per SNMP abfragen. Das NMS wird daneben auch verwendet, um den Switch zu rekonfigurieren und damit unterschiedliche Messszenarien darzustellen (z. B. unterschiedliche Intervalle für die Telemetrie-Übermittlung). Neben den Messdaten direkt vom Waystream-Switch, werden die durch das Monitoring übertragenen Datenmengen mit Hilfe von caplon erfasst (aufgeteilt in Telemetry und SNMP) und als Messgröße ins NMS integriert. Zusätzlich ist ein Traffic Generator im Testbed aufgebaut, um realistische Auslastungen auf den Netzwerk-Interfaces des Switches zu erzeugen, die dann gemessen werden. Die Architektur des PoCs ist in Abbildung 17 dargestellt.

Im Folgenden stellen wir beispielhaft einige Auswertungen der erfassten Daten vor. Tabelle 2 zeigt, dass die Messungen mit den verschiedenen Ansätzen konsistent sind, auch wenn geringere Messintervalle natürlich genauere Aussagen zulassen. Abbildung 18a stellt die für Monitoring-Daten genutzte Bandbreite in Abhängigkeit der konfigurierten Messintervalle dar. In der gewählten Konfiguration verursacht insbesondere Telemetry mit einer hohen Messfrequenz eine vergleichsweise hohe Bandbreite. Die dargestellten Werte verändern sich ggf. mit der Auswahl der abgefragten Metriken und weiteren Konfigurationsoptionen und können deshalb nicht verallgemeinert werden. Abbildung 18b stellt analog dazu eine Gegenüberstellung zur CPU-Auslastung auf dem Switch dar. Auch hier kann man einen Zusammenhang zwischen Messintervall und CPU-Auslastung erkennen. Durch eine andere Konfiguration der Abfolgen der unterschiedlichen Messfrequenzen könnte man noch besser analysieren, wie sehr die unterschiedlichen Technologien die CPU belasten. Genauso kann man auch weitere Metriken, wie beispielsweise die Speicherauslastung, überwachen und analysieren. Solche Analyse-Ergebnisse können Anhaltspunkte zur Dimensionierung, Skalierung und Konfiguration eines Systems geben (vgl. auch Abschnitt 2.1.1.2).

2.1.6.4 Streaming Network Telemetry in optischen Netzwerken unter Anwendung der TAPI-Schnittstelle

Zusammen mit den Partnern Adtran und Fraunhofer HHI wurde eine Demo zur ONF Transport API (TAPI) umgesetzt. Mit StableNet wurde das Monitoring für eine Service-Rekonfiguration implementiert. In Abbildung 19 ist der relevante Teil aus der Architektur

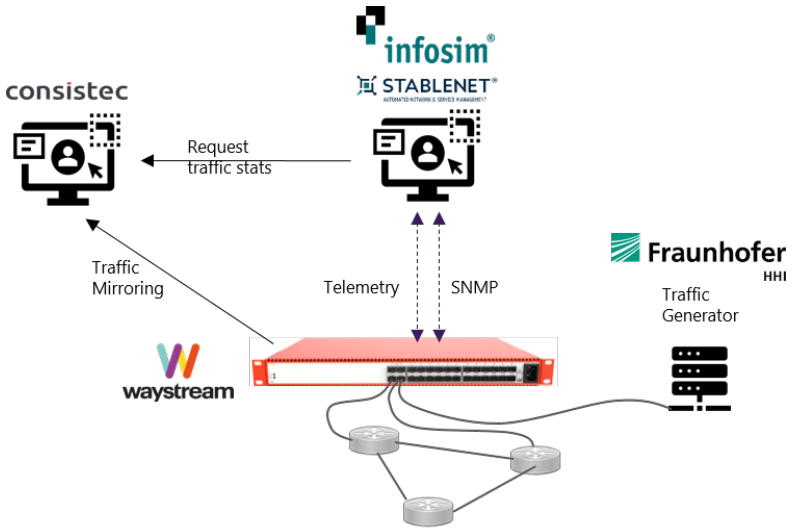


Abbildung 17: Testaufbau zum Vergleich der Messmethoden SNMP und Telemetry (siehe Abschnitt 2.1.6.3): Das getestete Gerät (in diesem PoC ein Switch von Waystream) ist in der Mitte dargestellt.

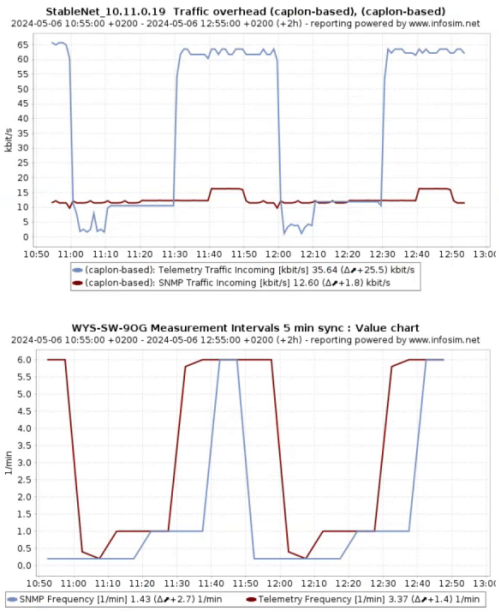
Tabelle 2: Die Tabelle vergleicht Messungen desselben Interfaces mittels SNMP und Telemetry über einen Zeitraum von zwei Stunden mit unterschiedlichen Messintervallen. Die Zahlen zeigen, dass Summe und Durchschnitt fast identisch sind, aber Minimal- und Maximalwerte zwischen den beiden Techniken aufgrund des feineren Messintervalls der Telemetriemessungen abweichen können.

ethernet0/4: 05-06 10:42 to 12:42
Messung per SNMP

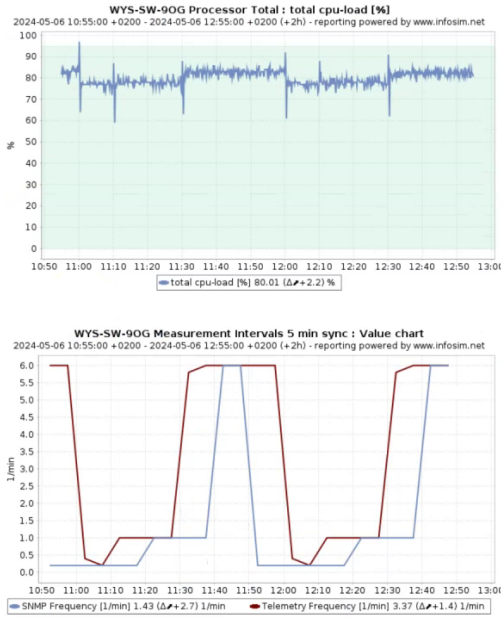
Param.	**in-octets**	**out-octets**
Count	171 #	171 #
Sum	844.008 kB	1.546 MB
Avg	0.939 kbit/s	1.761 kbit/s
Min	0.490 kbit/s	1.302 kbit/s
Max	2.315 kbit/s	2.408 kbit/s

ethernet0/4: 05-06 10:42 to 12:42
Messung per Telemetry

Param.	**in-octets**	**out-octets**
Count	402 #	402 #
Sum	843.568 kB	1.545 MB
Avg	0.939 kbit/s	1.761 kbit/s
Min	0.488 kbit/s	0.985 kbit/s
Max	1.990 kbit/s	3.405 kbit/s



(a) Gegenüberstellung von Messfrequenz und durch die Messung verursachten Durchsatz für SNMP (rot) bzw. Telemetry (blau)



(b) Gegenüberstellung von Messfrequenz und CPU-Auslastung auf dem Switch

Abbildung 18: Zusammenhang verschiedener Metriken mit Technologie und Messintervall der Netzwerküberwachung: Die beiden übereinander liegenden Diagramme sind jeweils zeitlich synchron. Unten ist die Messfrequenz der SNMP-Messung (blau) und der Telemetry-Messung (rot) dargestellt.

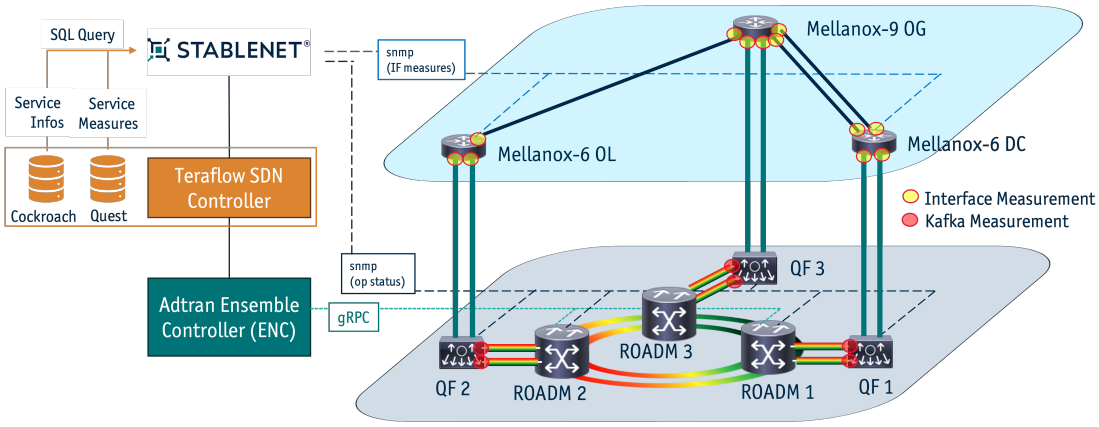


Abbildung 19: Architektur des TAPI-UseCases (siehe Abschnitt 2.1.6.4)

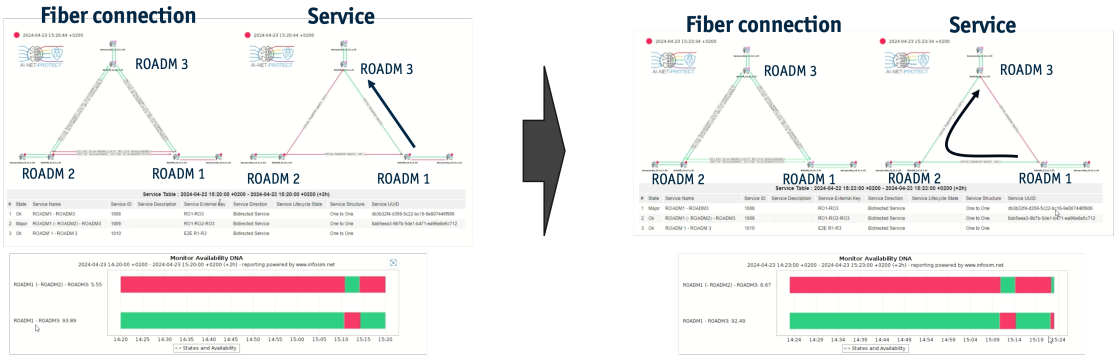


Abbildung 20: Monitoring der Service-Rekonfiguration zwischen ROADM 1 und ROADM 3

dargestellt und mit weiteren Details ergänzt. Neben StableNet wurde in dem PoC auch der TeraFlow SDN Controller sowie der Ensemble Controller (ENC) angewendet.

Zentrales Element war der SDN Controller, worin die E2E Services spezifiziert wurden (Endpunkte, Kapazität, ...). Der SDN Controller hat die Informationen an den ENC übergeben, welcher die Geräte entsprechend konfiguriert hat. Die Konfiguration wurde über die Datenbank des SDN-Controller an StableNet übergeben und auf das Service-Modell übertragen, sodass entsprechende Messungen angelegt werden konnten. Für die Demo wurde zwei Services zwischen den Endpunkten an ROADM 1 und ROADM 3 definiert, eine direkte Verbindung (Abbildung 20, links) und eine Verbindung via ROADM 2 (Abbildung 20, rechts). Wie im Service-Modell in Abschnitt 2.1.3 beschrieben wurden sowohl die physikalischen Verbindungen als auch die E2E-Services umgesetzt.

Darüber hinaus wurden zusätzlich Performance Parameter der optischen Transponder überwacht, wie in Abbildung 21 dargestellt. Transponder übernehmen die zentrale Aufgabe der Signalumwandlung und -übertragung und bilden die Schnittstelle zwischen elektrischen Datenströmen von Netzwerkgeräten und der optischen Übertragungsschicht, wie

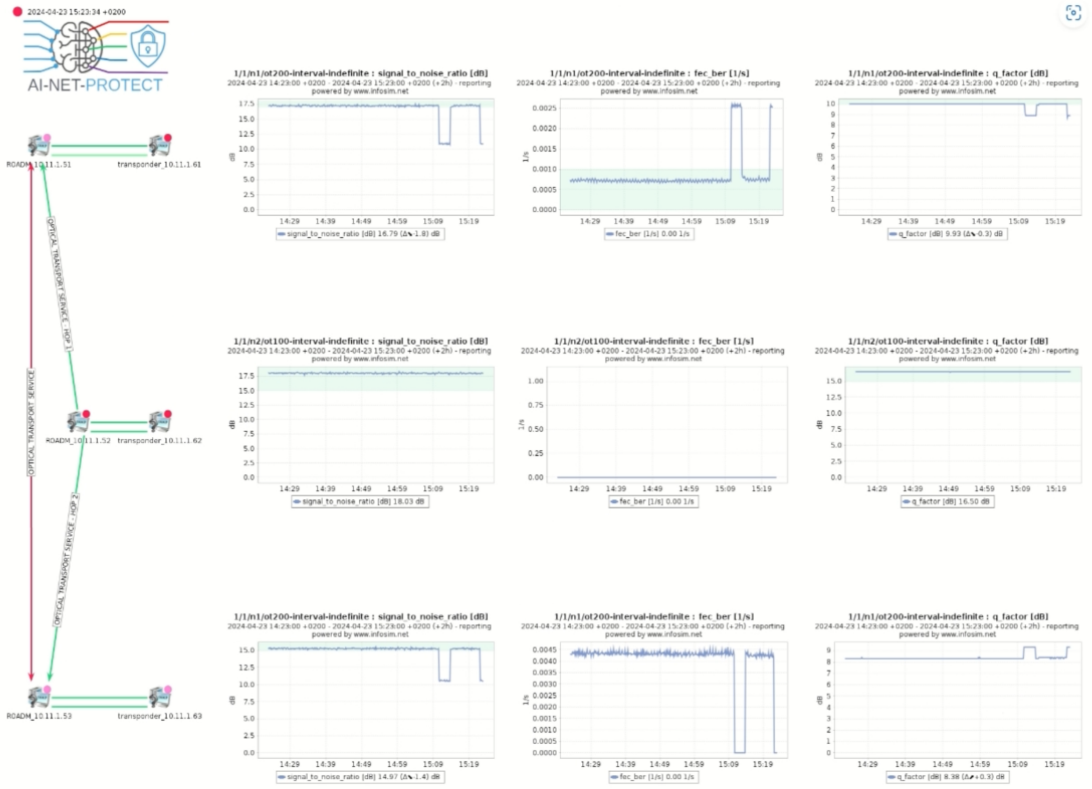


Abbildung 21: Monitoring der optischen Transponder via Kafka in StableNet

in Abbildung 19 dargestellt. Die Transponder verfügen über keine SNMP-Schnittstelle, können jedoch Daten über eine Streaming-Schnittstelle abgegriffen werden. Hier wurden verschiedene Datenmodelle (OpenConfig, ONF-TAPI) und Protokolle (z. B. gNMI, NETCONF) genutzt. Die Daten wurden zunächst an eine Kafka-Datenpipeline des Fraunhofer HHI gestreamt und anschließend über einen im Projekt entwickelten Kafka-StableNet-Deamon in entsprechende Messungen in StableNet integriert. Die Service-Rekonfiguration kann auch direkt in den Transponderdaten beobachtet werden.

2.1.6.5 Verhaltensbasierte Klassifikation von Netzwerkgeräten

Dieser PoC wurde gemeinsam mit dem Partner consistec durchgeführt und ist Teil der Demo-Umgebung, die im Labor am HHI aufgebaut wurde. Einen Überblick über den PoC, der im Folgenden beschrieben wird, gibt Abbildung 22.

Moderne Netzwerke umfassen viele verschiedene Gerätetypen, die in einer Analyse des Netzwerkverkehrs nur als Paare von IP-Adressen und Portnummern erscheinen. Weitere Informationen zu ihrem Typ sind daraus nicht direkt zu erkennen. Vielfach gibt es Inventarsysteme bzw. Komponentenmanagementsysteme (CMDB), in denen diese Informationen abgelegt werden sollen. Diese manuell geführten Systeme sind allerdings

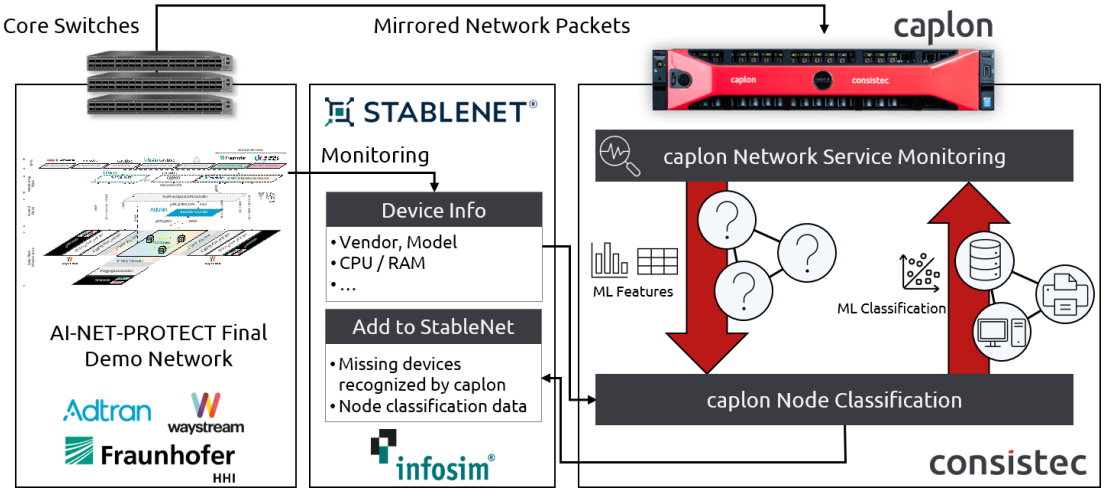


Abbildung 22: Architektur des PoC aus Abschnitt 2.1.6.5

Device Table : 2024-12-22 13:43:00 +0100 - 2024-12-23 13:43:00 +0100 (+1h)

#	Device Name	Device IP Address	Device Vendor	Device Model	Node Type	DNS Server	Domain Controller	File Server	other	Server	Web Server
01	DELL-SW-HHI	10.11.0.6		Unknown					1.0	0.999	
02	Caplon_10.11.0.20	10.11.0.20		Caplon	Domain Controller,File Server,Web Server		0.1394	0.435	0.2957	0.8695	0.2215
03	WYS-SW-9OG	10.11.0.12	Waystream	ASR8024E-DC	File Server			0.2439	0.8561	0.8043	
04	ENC_10.11.0.4	10.11.0.4		ENC	DNS Server	0.6185			0.4699	0.592	
05	ROADM_10.11.1.52	10.11.1.52	Adva Optical	ROADM					1.0	0.8636	
06	MELL-SW-9OG	10.11.0.10		Mellanox3	File Server			0.3324	0.7645	0.7202	
07	ROADM_10.11.1.51	10.11.1.51	Adva Optical	ROADM					1.0	0.878	
08	MELL-SW-6DC	10.11.0.9		Mellanox1	Domain Controller,File Server		0.2171	0.3661	0.5168	0.9993	
09	transponder_10.11.1.62	10.11.1.62		QuadFlex	Domain Controller		0.2062		0.8014	0.9958	
10	transponder_10.11.1.63	10.11.1.63		QuadFlex	Domain Controller,Web Server		0.2199		0.5916	0.6169	0.2882

Abbildung 23: Ergebnisse der Geräte-Klassifikation in einem StableNet-Report

fehleranfällig, veralten schnell und erfordern hohen Aufwand, wenn sie neu erstellt werden. In diesem PoC werden Geräte automatisiert im Hinblick auf bekannte Gerätetypen analysiert und klassifiziert. Basis dafür ist das Verhalten der Geräte und die von ihnen ausgehende Netzwerkkommunikation. Diese Erkenntnisse können beispielsweise auch hilfreich sein, um Verhaltensänderungen zu erkennen, die auf Angriffe hindeuten können.

Während des Betriebs werden zahlreiche Zeitreihen-, Verbindungs- und Telemetriedaten im Netzwerk erfasst. Daraus lassen sich unter Nutzung von ML-Algorithmen Geräte wie Drucker oder Server, sowie bestimmte Dienste klassifizieren. In bestehenden Netzwerken, in denen die Geräte bereits mit entsprechenden Informationen versehen sind, kann die Klassifizierung zur Validierung dieser Informationen genutzt werden, während sie in neuen Umgebungen einen Ausgangspunkt für eine Geräteübersicht bietet.

Im Testaufbau ist der ML-Algorithmus tief mit den unterschiedlichen genutzten Tools integriert. Die Monitoring-Lösung caplon von consistec wird eingesetzt, um die IP-Kommunikation zu erfassen und zu analysieren. Basierend auf daraus generierten Zeitreihen-Daten, werden die Geräte mittels ML-Algorithmen in vordefinierte Klassen (z. B.

Drucker, Datei-Server) eingeteilt. Daneben erhebt StableNet statische Informationen von den Geräten (z. B. über SNMP), die ebenfalls einbezogen werden. Ein Dashboard zeigt die Entscheidungsgrundlagen und Ergebnisse des Modells und kann Details zu einzelnen Geräten im Netzwerk darstellen. Die ermittelten Informationen werden außerdem in StableNet zurückgespiegelt. Dort werden neu erkannte Geräte im System ergänzt und die Ergebnisse der Geräte-Klassifizierung hinterlegt. Als Beispiel, wie diese Geräte-Klassifizierung in StableNet abgefragt werden kann, zeigt Abbildung 23 einen Ausschnitt aus einem Report, der die Ergebnisse der Klassifikation darstellt.

2.1.6.6 TM Forum Catalyst 2023

Neben den direkten Demonstratoren mit verschiedenen Projektpartnern aus dem Konsortium, war es Infosim ein Anliegen, die im Projekt erarbeiteten Ansätze auch außerhalb des direkten Projektkontextes bereits als PoC einzusetzen, um sie einerseits zu testen und andererseits bestmöglichen Input für die weitere Umsetzung zu erhalten. In diesem Zusammenhang nahm Infosim insbesondere das TM Forum in den Blick. Infosim hatte bereits in der Vergangenheit sehr positive Erfahrungen mit den TM Forum Catalyst-Projekten gesammelt und dabei auch mehrere Auszeichnungen erhalten. Diese erfolgten in den Jahren 2016, 2017 und 2018, was sicher auch dank der aus den Forschungsprojekten eingeflossenen Zwischenergebnisse erreicht werden konnte. Nach einer pandemiebedingten Pause entschied sich Infosim daher im Rahmen des AI-NET-PROTECT-Projekts, 2023 erneut an den Catalyst-Initiativen teilzunehmen. Das TM Forum selbst bezeichnet Catalysts als „rapid-fire PoC“ Projekte, in denen mehrere Firmen ihre kommerziellen Produkte mit neuen innovativen Ansätzen und TM Forum Digital Open APIs zusammenbringen.

Dieses Engagement ermöglichte es, wie erhofft, die im Projekt entwickelten PoC-Ansätze in einem größeren Umfeld zu testen und, wo immer möglich, mit anderen Partnern unter Verwendung standardisierter APIs zu integrieren. Die 2023 erarbeiteten Konzepte fanden auch im Catalyst 2024 eine Fortsetzung, obwohl dieser nicht mehr explizit im Projektkontext von AI-NET-PROTECT durchgeführt wurde. Insbesondere konnten viele der Arbeiten im Bereich Service-Modellierung, -Monitoring und -Visualisierung eingebracht werden.

Der Catalyst 2023 mit dem Titel „Autonomous Networks Hyperloops – Phase IV“[2] konzentrierte sich auf die Entwicklung autonomer Netzwerke zur Unterstützung kritischer Operationen, einschließlich der Nutzung des Metaverse für nahtlose, qualitativ hochwertige, vernetzte Erfahrungen in verschiedenen Sektoren. Zu den beteiligten Partnern gehörten unter anderem Orange, NTT, Chunghwa Telecom, Verizon und TIM. Infosim trug durch seine Expertise in Netzwerkmanagement und -automatisierung, ergänzt um die neuen PoCs aus dem AI-NET-PROTECT Projekt, wesentlich zum Erfolg dieses Catalysts bei. Abbildung 24 zeigt in einer schematischen Darstellung die wesentliche Rolle von Infosim als Teil des gesamten Catalyst-Teams, indem die unterstützten Bereiche der Catalyst Architektur farblich markiert und mit Beispiel-Screenshots von

[2] `https://www.tmforum.org/catalysts/projects/M23.0.586`

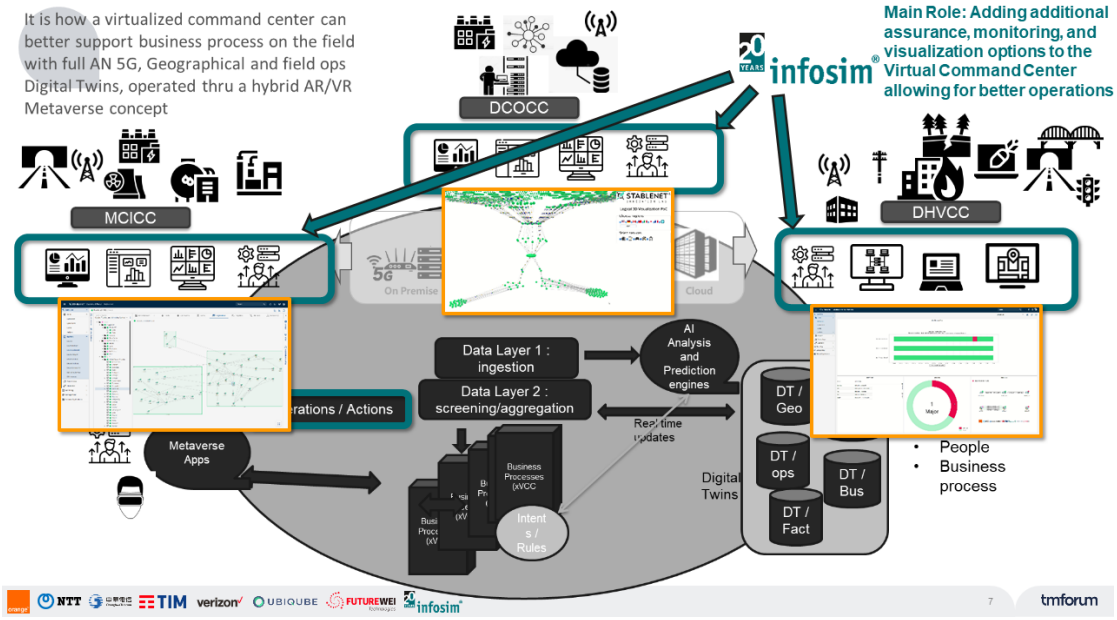


Abbildung 24: Schematische Darstellung der Rolle von Infosim im Rahmen des Catalyst inkl. Beispiel-Screenshots

Infosim illustriert sind.

Im Jahr 2024 wurde das Projekt in „Autonomous Networks Hyperloops – Phase V“[3] weitergeführt, wobei der Fokus auf der Entwicklung digitaler Plattformen zur Verbesserung des Krisenmanagements durch autonome Netzwerke, künstliche Intelligenz und digitale Zwillinge lag. Dieses Projekt wurde mit dem TM Forum Catalyst Award in der Kategorie „Outstanding Catalyst – Beyond Telco“ ausgezeichnet.

Durch die Teilnahme an den Catalyst-Projekten konnte Infosim die im AI-NET-PROTECT-Projekt entwickelten Ansätze in realen Anwendungsfällen erproben und weiterentwickeln, was zu einer verbesserten Netzwerkautomatisierung und -sicherheit in kritischen Infrastrukturen beitrug. Außerdem wurden Veranstaltungen des TM Forums dazu genutzt, die jeweils aktuellen Teile des Projektes vorzustellen und direktes Feedback aus der Industrie einzuholen.

2.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die wichtigsten Positionen des zahlenmäßigen Nachweises bestehen aus Personalkosten, Reisekosten, Abschreibungen auf vorhabenspezifische Anlagen, sowie sonstigen unmittelbaren Vorhabenkosten. Diese wurden in regelmäßigen Abständen an das BMBF gemeldet. Die Kosten lagen im Wesentlichen im Plan.

[3] https://www.tmforum.org/catalysts/projects/C24.0.651

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Der Verlauf der Arbeit im Projekt folgte im Wesentlichen dem Projektantrag. Auf neue Erkenntnisse wurde im Projektverlauf reagiert und die Arbeitspakete und Meilensteine den geänderten Anforderungen entsprechend angepasst.

2.4 Voraussichtlicher Nutzen

Infosim hat sich im Projekt mit Technologien wie KI, Streaming Network Telemetry, Service-Orchestrierung und Kapazitätsplanung beschäftigt. Diese Technologien haben in den vergangenen Jahren zunehmende Relevanz am Markt erhalten und werden mehr und mehr von Kunden nachgefragt. Insbesondere bei den im Projekt erarbeiteten Konzepten und Demonstratoren zur Integration von Telemetry-Ansätzen zeigt sich ein großes Interesse bei möglichen Nutzern. Nach Ende des geförderten Projekts wird hier schon mit ersten Kunden eine kommerzielle Umsetzung diskutiert.

Zusätzlich ist Infosim bereits während des Projekts auf mögliche Zielkunden und Partner zugegangen, um die erstellten PoCs, sowie die darin berücksichtigten Anforderungen einerseits zu validieren und andererseits für die Zukunft möglichst nah an eine marktreife Lösung anzugleichen. Durch den Erwerb von Know-how im Projekt und die Durchführung von Demonstrationen im Forschungsprojekt, sollte die Wettbewerbsfähigkeit von Infosim generell und die des Produktes StableNet gezielt gesteigert werden. Die Mitarbeit in dem Forschungsprojekt hat schon jetzt dazu geführt, dass Infosim noch besser in der Lage ist, zukünftigen Anforderungen in den Bereichen KI, Service-Orchestrierung und Kapazitätsplanung gerecht zu werden.

Weiterhin führen die durch das Projekt erworbenen Kompetenzen, gerade auch in den Bereichen KI und maschinelles Lernen (ML), dazu, dass Infosim generell seine Innovationskraft weiter steigern konnte, was auch eventuellen Folgeprojekten oder anderen wissenschaftlichen und wirtschaftlichen Anknüpfungspunkten sehr zugute kommt.

Speziell zum Bereich KI und ML soll zudem noch kurz erwähnt werden, dass auch zum Zeitpunkt der Erstellung dieses Berichts gerade diese Themen immer noch stark kontrovers zwischen Hype und konkret messbarem Mehrwert schwanken. In manchen Bereichen sind diese Technologien mittlerweile längst angekommen, in anderen Bereichen ist hingegen immer noch kein ganz eindeutiger Nutzen oder eine Verbesserung gegenüber klassischeren, statistischen Ansätzen greifbar. Das Forschungsprojekt PROTECT hat definitiv dabei geholfen, besser herauszuarbeiten, welche konkreten Zeit- und Kostenersparnisse sich wirklich aus der Nutzung von KI und ML ergeben können. Dies legt somit eine gute Grundlage für weitere Arbeiten in diesem Themenfeld, sowohl in anschließenden Forschungsprojekten, als auch bei einer möglichen Umsetzung ausgewählter PoC-Ergebnisse in Richtung Schaffung eines kommerziellen Produktes.

2.5 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen während seiner Durchführung

Im Laufe des Projektes wurde darauf geachtet, ob die im Projekt betrachteten Fragestellungen an anderer Stelle untersucht werden. Der Fortschritt bei anderen Stellen wurde konsequent durch Teilnahme an Konferenzen, Diskussionen mit Projektpartnern, sowie Universitäten und Forschungsinstitutionen verfolgt. Ergänzend dazu beobachtet Infosim aktuelle Standardisierungsaktivitäten im industriellen Umfeld (beispielsweise TM Forum). Der Fokus lag hierbei insbesondere auf den Bereichen KI und Service-Orchestrierung. Gewonnene Erkenntnisse wurden fortwährend berücksichtigt und in die eigene Arbeit aufgenommen.

2.6 Erfolgte oder geplante Veröffentlichungen

Projektbegleitend wurde Wert auf eine entsprechende Dissemination gelegt, um die Forschungsergebnisse zu verbreiten und Diskussionen, sowie den fachlichen Austausch anzuregen. Die dabei gewonnenen Ergebnisse dienten wiederum als sehr hilfreicher Input für weitere Aktivitäten. Im Folgenden wird eine stichpunktartige Aufzählung von Veröffentlichungen und Disseminationsaktivitäten gegeben.

- Präsentation des Projektes auf einer eigenen Projektwebsite[4], sowie auf der Seite von Infosim[5]
- Präsentation von Projektergebnissen bei verschiedenen ESF-geförderten Projekten, wie u. A. ESF-ZDEX oder KI-Hub Nordbayern inkl. Austausch zu projektrelevanten Themen mit verschiedenen Fachleuten
- Erwähnung von Projektergebnissen im Rahmen von Vorträgen auf der 9th/10th Swiss Service & Infrastructure Management User Conference im Oktober 2021 und November 2022
- David Hock, „AI-based Network Management – a deeper look into selected use cases“, AI-NET Workshop (collocated with EuCNC 2023) – Enabling 6G and Sustainable Digital Transformation by Intelligent Network Automation, Göteborg, 06.06.2023, Vortrag
- Stefan Köhler, David Hock, „Current and upcoming challenges of automated network management in practice“, ITC 35th – Networked Systems and Services[6], Turin, 03.10.2023, Keynote

[4] `https://protect.ai-net.tech/`
[5] `https://www.infosim.net/ai-net-protect/`
[6] `https://itc35.itc-conference.org/`

- Christian Burk, David Hock, Johan Sandell, Behnam Shariati, „Towards automated and proactive anomaly detection in fiber access networks“, DENOG15[7], Berlin, 20.11.2023, Präsentation
- Karoly Makonyi, Henrik Abrahamsson, Daniel Henriksson, David Hock, Stefan Kremling, Fabian Lipp, Jonathan Salisbury and Johan Sandell, „On the use of streaming telemetry data for network health monitoring and anomaly detection“[8], Swedish National Computer Networking and Cloud Computing Workshop[9], Linköping, Sweden, 11.06.2024
- David Hock, *AI-NET-PROTECT Final Demo Use Case – Comparing SNMP and Telemetry*, Video, 2024, `https://youtu.be/mx4A6AIrMJM`, beschreibt den PoC aus Abschnitt 2.1.6.3
- Darüber hinaus: zahlreiche Erwähnungen des Projektes bei Veranstaltungen von Infosim und im Austausch mit Kunden und Partnern
- TM Forum Catalyst 2023, sowie die damit verbundenen Events TM Forum Accelerate 2023 und DTW 2023, siehe auch Abschnitt 2.1.6.6
- Teilnahme an verschiedenen Treffen der AI-NET Working Groups zum Austausch mit Partnern in den anderen Teilprojekten
- Teilnahme und Beiträge zu den jährlichen Public Events von AI-NET

[7] `https://www.denog.de/de/meetings/denog15/index.html`, Link zum Video des Vortrags: `https://media.ccc.de/v/denog15-36953-towards-automated-and-proactive-anomaly-detection-in-fiber-access-networks`

[8] `https://www.waystream.com/wp-content/uploads/SNCNW2024-On-the-use-of-streaming-telemetry-data-for-network-health-monitoring-and-anomaly-detection.pdf`

[9] `https://www.sncnw.se/2024/`

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht

3. Titel

Telemetrie, Netzwerkplanung, Künstliche Intelligenz

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 30.06.2024
Hock, David Lipp, Fabian Kremling, Stefan Schardt, Simon	6. Veröffentlichungsdatum
	7. Form der Publikation Schlussbericht
8. Durchführende Institution(en) (Name, Adresse) Infosim GmbH & Co. KG Landsteinerstraße 4 97074 Würzburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 16KIS1290
	11. Seitenzahl 34
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 0
	14. Tabellen 2
	15. Abbildungen 24

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

Der Schwerpunkt des Teilprojekts PROTECT war die Bereitstellung automatisierter Resilienz und sicherer Netze auf vertrauenswürdigen Geräten für kritische Infrastrukturen und Unternehmen. AI-NET-PROTECT soll für den Schutz kritischer Daten, hohe Performanz in Bezug auf wesentliche Leistungsparameter (wie Latenz, Durchsatz und Verfügbarkeit) und hohe Robustheit der Netzinfrastruktur (Schutz gegen Manipulationen und Angriffe) sorgen. Um diese Ziele zu erreichen, wurde in PROTECT eine skalierbare Netz- und Knotenarchitektur entwickelt, um die verschiedenen kritischen Leistungsparameter durch eine Mischung aus offener und spezialisierter Hardware und Software zu adressieren. Streaming Network Telemetry und Intent-based Software-Defined Network Management and Control bieten Zero-Touch-Bereitstellung und unterstützen die Automatisierung von Ende-zu-Ende-Diensten mit Hilfe von künstlicher Intelligenz (KI). Die wichtigsten Anwendungsfälle für KI sind Leistungsoptimierung, proaktive Fehler- und Anomalieerkennung, Penetrations- und Schwachstellentests, sowie das Management von Sicherheitsangriffen.

19. Schlagwörter

KI, ML, Netzwerk

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) Final report

3. title

Telemetrie, Netzwerkplanung, Künstliche Intelligenz

4. author(s) (family name, first name(s))	5. end of project 30.06.2024
Hock, David Lipp, Fabian Kremling, Stefan Schardt, Simon	6. publication date
	7. form of publication Final report
8. performing organization(s) (name, address) Infosim GmbH & Co. KG Landsteinerstraße 4 97074 Würzburg	9. originator's report no.
	10. reference no. 16KIS1290
	11. no. of pages 34
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 0
	14. no. of tables 2
	15. no. of figures 24

16. supplementary notes

17. presented at (title, place, date)

18. abstract

The focus of the PROTECT sub-project was to provide automated resilience and secure networks on trusted devices for critical infrastructures and companies. AI-NET-PROTECT is designed to ensure the protection of critical data, high performance in terms of key performance parameters (such as latency, throughput and availability) and high robustness of the network infrastructure (protection against manipulation and attacks). To achieve these goals, a scalable network and node architecture was developed in PROTECT to address the various critical performance parameters through a mixture of open and specialised hardware and software. Streaming Network Telemetry and Intent-based Software-Defined Network Management and Control provide zero-touch provisioning and support the automation of end-to-end services using artificial intelligence (AI). The most important use cases for AI are performance optimisation, proactive fault and anomaly detection, penetration and vulnerability testing, as well as the management of security attacks.

19. keywords
AI, ML, Network

20. publisher	21. price