Architekturkonzept deterministischer Kommunikationsnetzwerke für die IT/OT-Konvergenz

Dissertation

zur Erlangung des akademischen Grades

Doktoringenieur

(Dr.-Ing.)

von **M. Sc. Thomas Kampa**

geb. am 06.09.1994 in Seligenstadt

genehmigt durch die Fakultät für Elektrotechnik und Informationstechnik
der Otto-von-Guericke-Universität Magdeburg

Gutachter:

Prof. Dr.-Ing. Ulrich Jumar

Prof. Dr.-Ing. Mike Barth

Prof. Dr.-Ing. Daniel Großmann

Promotionskolloquium am 30. März 2025

Zusammenfassung

Die industrielle Fertigung steht vor der Herausforderung, immer komplexere und vernetzte Systeme zu betreiben, welche zur selben Zeit hohe Anforderungen an Zuverlässigkeit und Sicherheit erfüllen müssen. Traditionelle Ansätze stoßen dabei zunehmend an ihre Grenzen. Hier bietet die Einführung von Virtualisierungstechnologie eine vielversprechende Lösung, wodurch jedoch zusätzliche Anforderungen an die Kommunikationsnetzwerke gestellt werden.

Diese Arbeit entwickelt auf Basis dieser identifizierten Anforderungen spezifische Architekturbausteine für ein IT/OT-konvergiertes Kommunikationsnetzwerk. Fokus liegt dabei auf der Erreichung von Determinismus, damit eine zuverlässige und echtzeitfähige Kommunikation erreicht wird. Durch die Kombination von Mechanismen wie Paketduplizierung und Quality of Service wird die Virtualisierung und Konsolidierung von Automatisierungsapplikationen ermöglicht, was die Betreibbarkeit aufgrund der flexiblen und skalierbaren Infrastruktur vereinfacht.

Das Ergebnis ist ein umfassendes Architekturkonzept, das die breite Nutzung von IT-Technologien in der Automatisierungsdomäne ermöglicht. Repräsentative Versuchsaufbauten und der Vergleich mit den definierten Anforderungen bestätigen die Validität des entwickelten Konzepts.

Abstract

Industrial production is facing the challenge of operating increasingly complex and networked systems, which at the same time have to meet high reliability and safety requirements. Traditional approaches are increasingly reaching their limits. Here, the introduction of virtualization technology offers a promising solution, which, however, places additional demands on the communication networks.

Based on these identified requirements, architecture modules are developed for an IT/OT-converged communication network. One focus is on achieving determinism in order to achieve reliable and real-time capable communication. The combination of mechanisms such as packet duplication and quality of service enables the virtualization and consolidation of automation applications, which simplifies operability due to the flexible and scalable infrastructure.

The result is a comprehensive architecture concept that enables the broad use of IT technologies in the automation domain. Representative test setups and the comparison with the defined requirements confirm the validity of the developed concept.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACL Access Control List

ASIC Anwendungsspezifischen integrierten Schaltung

Avg Durchschnitt

BFD Bidirectional Forwarding Detection

BGP Border Gateway Protocol

BSI Deutsches Bundesamt für Sicherheit in der Informationstechnik

CA Certificate Authority

CERT Computer Emergency Response Team

CI/CD Continuous Integration/Continuous Deployment

CKC Cyber Kill Chain

COTS Commercial off-the-Shelf

CQF Cyclic Queuing and Forwarding

CRC Cyclic Redundancy Check

CT Zykluszeit

DAN Dual-attached Node

DCP Discovery Protokoll

DetNet Deterministic Networking

DiD Defense in Depth

DoS Denial of Service

DDoS Distributed Denial of Service

DSCP Differentiated Services Code Point

DPI Deep Packet Inspection

E/A Eingang/Ausgang

ECMP Equal-cost Multi-path

eBPF Extended Berkeley Packet Filters

EDP Enhanced Data Path

ERP Enterprise Resource Planning

EVPN Ethernet Virtual Private Network

FIB Forwarding Information Base

FMEA Fehlermöglichkeits- und Einflussanalyse

FPGA Field Programmable Gate Array

FR Foundational Requirements

FRER Frame Replication and Elimination

GBP Group-based Policy

GRE Generic Routing Encapsulation

HMI Human Machine Interface

HSR High-availability Seamless Redundancy

HSRP Hot Standby Redundancy Protocol

IB Infiniband

IDS Intrusion Detection System

IE Industrial Ethernet

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

IIoT Industrial Internet of Things

IoT Internet of Things

IP Internet Protocol

IPC Industrieller Personal Computer

IPS Intrusion Prevention System

IPsec Internet Protocol Security

ISO International Organization for Standardization

IS-IS Intermediate System to Intermediate System Protocol

IT Informationstechnik

IvS Industrial virtual Switch

KI künstliche Intelligenz

LACP Link Aggregation Control Protocol

LISP Locator Identity Separation Protocol

LLDP Link Layer Device Protocol

MAC Media Access Control

MACsec Media Access Control Security

Max Maximum

MES Manufacturing Execution System

Min Minimum

MPLS Multiprotocol Label Switching

MPLS-TP Multiprotocol Label Switching Transport-Profile

MRP Media Redundancy Protocol

MTU Maximum Transmission Unit

NAC Netzwerkzugangskontrolle, engl. network access control

NTP Network Time Protocol

NTS Network Time Security

OPC UA Open Platform Communications Unified Architecture

OSI Open Systems Interconnection

OSPF Open Shortest Path First

OT Operative Technologie

PCI Protocol Control Information

PDU Protocol Data Unit

pEth Physische Ethernet-Schnittstellen

PhySec Physical Security

PLR Paketverlustrate

PLS Prozessleitsystems

PRP Parallel Redundancy Protocol

PTP Precision Time Protocol

QoS Quality of Service

RDMA Remote Direct Memory Access

RE Requirement Enhancements

RedBox Reduction Box

RFC Request for Comments

RoCE RDMA over Converged Ethernet

SAN Single-attached Node

SCADA Supervisory Control and Data Acquisition

SD Standardabweichung

SDN Software-defined Networking

SDU Service Data Unit

SG Sicherheitsgruppe

SL Security Level

SPOF Single Point of Failure

SPS Speicherprogrammierbare Steuerung

SR System Requirement

SR-IOV Single-Root Input/Output-Virtualisierung

SPI Stateful Packet Inspection

TCP Transmission Control Protocol

TSN Time Sensitive Networking

TT Übertragungszeit

TWAMP Two-Way Active Measurement Protocol

UDP User Datagram Protocol

UT Aktualisierungszeit

VDAN Virtual Dual-attached Node

VDI Virtual Desktop Infrastructure

vEth Virtuelle Ethernet-Schnittstelle

VID VLAN Identifier

VLAN Virtual Local Area Network

VM Virtuelle Maschine

VNI Virtual Network Identifier

VRF Virtual Routing Function

VRRP Virtual Router Redundancy Protocol

vSPS Virtuellen speicherprogrammierbaren Steuerung

VTEP VXLAN-Tunnel-Endpunkt

VXLAN Virtual extensible Local Area Network

WAF Web Application Firewall

WAN Weitverkehrsnetzwerke

WDT Watchdog-Timer

WRED Weighted Random Early Detection

XDP eXpress Data Path

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

In diesem Kapitel wird ein Überblick über das Thema gegeben, die Motivation für die vorliegende Arbeit erläutert sowie das Gesamtziel und die Struktur vorgestellt.

1.1 Motivation

Die vergangenen Jahrzehnte haben unser tägliches Verhalten durch die Verbreitung des Internets grundlegend verändert. Wir können uns ein Leben ohne Internetkonnektivität kaum noch vorstellen – sei es für Videokonferenzen, Navigation, Websuchen oder Streaming. Die jüngste Ergänzung durch das Cloud-Computing hat diese Entwicklung weiter beschleunigt, indem flexibel Ressourcen bereitgestellt und neue Applikationen Nachfrage-basiert skaliert werden können. Die Grundlage für all diese Fortschritte bilden Netzwerk- und Virtualisierungstechnologien, die Nutzer und Server miteinander verbinden und die verfügbaren Ressourcen effizient und flexibel bereitstellen.

Im industriellen Umfeld erfordert die Umsetzung von Industrie 4.0 Konzepten die immer stärkere Vernetzung von Komponenten und Systemen der Automatisierungstechnik mit IT-Systemen. Ein häufig genanntes, fehlendes Puzzlestück ist die Konvergenz von Informationstechnik (IT) und der Operative Technologie (OT), welche auch als Betriebstechnologie bezeichnet wird. Die IT/OT-Konvergenz sieht einen Einsatz von IT-Technologien wie Virtualisierung und moderner Kommunikationstechnik in der industriellen Automatisierung vor, indem Infrastruktur und Applikationen der IT- und OT-Domänen miteinander verschmelzen. Dies führt zu einer verbesserten Interoperabilität und Flexibilität und ermöglicht in der Automatisierungstechnik eine effizientere Nutzung von Ressourcen, vereinfachte Datenverarbeitung, sowie eine erhöhte Anpassungsfähigkeit an sich schnell ändernde Anforderungen.

Applikationen innerhalb der Automatisierungswelt werden auch heute noch bevorzugt als Hardware-Box vertrieben und tragen zum Wachstum der Komplexität innerhalb des Shopfloors bei. Dies wird verstärkt durch neuartige Anwendungen wie künstliche Intelligenz (KI) für Qualitätssicherung und prädiktive Wartung, welche mit hohen Anforderungen an Ressourcen und Handhabung einhergehen. Dieser Entwicklung entgegenwirkend gewinnen zunehmend Software-basierte Produkte an Relevanz, die allerdings die passende Infrastruktur und Prozesse benötigen, um eingesetzt werden zu können. Als jüngstes Beispiel für die Virtualisierung von zuvor Hardware-gebundenen Applikationen ist die Speicherprogrammierbare Steuerung (SPS) zu nennen, wodurch die Flexibilität, Skalierbarkeit und Wartbarkeit erhöht werden kann [Gol+15].

Nach der Konsolidierung von Applikationen auf Public Cloud-Infrastrukturen kann nun auch der inverse Trend hin zu Edge Cloud und privaten Cloud-Instanzen beobachtet

werden [Mah+18]. Diese Entwicklung ermöglicht die Steigerung der Ressourceneffizienz durch Virtualisierung, die Kapselung von sensitiven Daten unter Nutzung einer kontrollierten Umgebung, sowie die Reduktion von Latenzzeiten. Hierbei können Applikationen auf einem echtzeitfähigen Hypervisor virtualisiert werden, die eine Nutzung für Applikationen mit Determinismus-Anforderungen ermöglichen. Das Edge Cloud-Paradigma, welches verteilte Systeme in Proximität des Nutzers vorsieht, reduziert die beobachtete Komplexität in der Automatisierungsdomäne und stellt eine Plattform für deren Applikationen dar. Der Trend hin zur holistischen Vernetzung und Digitalisierung der Fertigung wird häufig unter dem Begriff Industrie 4.0 zusammengefasst [Sch17].

Allerdings erfordert die Nutzung von verteilten Systemen in der Automatisierung eine Vernetzung von Feldgeräten, beispielsweise Sensorik und Aktorik, mit dem verteilten System und damit der Erfüllung der spezifischen Anforderungen von OT-Systemen. Prozesse innerhalb der Automatisierung werden vor allem vor dem Hintergrund der Verfügbarkeit, Robustheit und Langlebigkeit optimiert [FRK19]. Sofern Applikationen mit enormen Verfügbarkeits- und Determinismusanforderungen und hoher Kritikalität für Prozesse auf einer Edge Cloud betrieben werden sollen, erhöht sich auch der Stellenwert des Netzwerkes, welches die Applikation mit dem jeweiligen Kommunikationspartner verbindet. Ein Beispiel für eine zeitkritische Kommunikation im Automatisierungsumfeld ist die Kommunikation der Virtuellen speicherprogrammierbaren Steuerung (vSPS), welche die Steuerung von Aktorik und Sensorik der physikalischen Prozesse übernimmt. Verschiedene Bestrebungen aus Wissenschaft und Industrie haben die Vision einer vollständig virtualisierten Form der Steuerung ermöglicht und zur Produktreife gebracht [Mue+24].

Allerdings ergeben sich Herausforderungen für Unternehmen, die die wünschenswerte Evolution in Richtung Industrie 4.0 und Virtualisierung durchführen möchten. Barrieren bei der Adoption umfassen neben fehlendem Personal mit der notwendigen Expertise eine unzureichende IT-Infrastruktur, die vor allem auf einer zuverlässigen Cloud-Infrastruktur und einem Kommunikationsnetzwerk besteht [KAV17; SHF24]. Hierbei ist für das Erreichen der Vernetzung von zentraler Bedeutung, dass das jeweilige Kommunikationsnetzwerk die Anwendungen von IT und OT über ein gemeinsames Netzwerk unterstützt. Das in dieser Arbeit vorgestellte Konzept vereint die Stärken und Trends beider Welten und ermöglicht gleichzeitig eine Integration mit bestehenden Systemen, eine sogenannte Brownfield-Integration. Dies ist vor allem aufgrund der milliardenschweren Vermögenswerte in OT-Hardware und der Nutzung vorhandener Fähigkeiten der Mitarbeiter von hoher Wichtigkeit für eine Adoption eines Architekturkonzeptes. Es werden maßgeblich IT-Technologien genutzt, um die verschiedenen Anforderungen des Automatisierungsbereichs zu erfüllen. Während OT-Applikationen auf ausgewählter IT-Hardware und von IT-Mechanismen unterstützt werden können, ist das Umgekehrte aufgrund fehlender Eigenschaften und Standards nicht der Fall.

1.2 Ziel der Arbeit

Ziel dieser Arbeit ist es daher, ein Architekturkonzept für IT/OT-konvergierte Kommunikationsnetzwerke zu entwickeln, welches die Fortschritte der IT in die Domäne der Automatisierungstechnik überträgt und nutzbar macht. Hierbei sollen zunächst die Anforderungen an die Kommunikationsnetzwerke und Steuerungstechnik identifiziert und anschließend Lösungen konzipiert werden. Die vorgestellten Bestandteile des Architekturkonzepts werden prototypisch implementiert und validiert.

Eine grundlegende Zielstellung während der Entwicklung des Konzeptes ist die mögliche Anwendung in Brownfield-Szenarien. Die Automatisierungswelt ist vor allem an langjährige Investitionen von Anlagen und Gebäuden gebunden, die das Bauen auf einer grünen Wiese als Seltenheit erscheinen lässt. Weiterhin ist das Fachwissen der Arbeitskräfte langjährig entwickelt worden, sodass möglichst auf Gegebenem aufgebaut werden sollte. Aus diesem Grund muss eine Migration hin zu neuen Prozessen und Systemen gewährleistet werden.

1.3 Struktur der Arbeit

Die vorliegende Arbeit besteht aus sechs Kapiteln. Nach der vorangegangenen Motivation und Beschreibung der Zielstellung erfolgt ein grundlegender Überblick über Kommunikationsnetzwerke in der Automatisierungsdomäne und die Darstellung des Wandels der industriellen Steuerungstechnik in Kapitel 2. Auf dessen Basis werden die Forschungsfragen formuliert.

Kapitel 3 stellt den Stand der Wissenschaft der IT/OT-Konvergenz dar. Hierbei werden Konzepte der Bereiche Echtzeitfähigkeit, Determinismus, und Hochverfügbarkeit von Kommunikationsnetzwerken, Hochverfügbarkeit von vSPSn, und IT/OT-Sicherheit betrachtet. Diese werden abschließend im Kontext eines IT/OT-konvergierten Kommunikationsnetzwerkes bewertet.

Die Entwicklung eines Architekturkonzepts für ein IT/OT-konvergiertes Kommunikationsnetzwerk erfolgt in Kapitel 4. Hierzu werden Anforderungen definiert und ein Überblick über das Gesamtkonzept gegeben. Anschließend erfolgt die Darstellung von entwickelten Architekturbausteinen auf Basis der zuvor definierten Anforderungen an eine Architektur.

In Kapitel 5 folgt die Validierung der jeweiligen Mechanismen und Teilkonzepte mittels einer Vielzahl von Versuchsaufbauten sowie anhand von theoretischen Bewertungen. Hierbei werden die Ergebnisse kritisch diskutiert und anlehnende Themen, wie die Konvergenz von kabelgebundener und kabelloser Kommunikation, betrachtet.

Abschließend werden in Kapitel 6 die Ergebnisse der Arbeit zusammengefasst und diskutiert.

2 Kommunikationsnetzwerke in der Automatisierungsdomäne

Das Kapitel 2 stellt die wissenschaftliche Relevanz der Arbeit dar. Hierzu wird die Evolution der industriellen Kommunikation und Steuerungstechnik, der aktuelle Aufbau von Automatisierungssystemen nach der Automatisierungspyramide, als auch die Modelle der Industrie 4.0 vorgestellt. Die Definition der Forschungsfragen dieser Arbeit schließt das Kapitel ab.

2.1 Die industrielle Produktion im Wandel

Industrielle Produktionssysteme stehen in einem kontinuierlichen Wandel. Technologien, Prozesse, Produkte, und Gesellschaft nehmen Einfluss auf die industrielle Fertigung, wodurch über die vergangenen Jahrhunderte verschiedene Entwicklungen stattgefunden haben. Ein Blick in die Vergangenheit ermöglicht die Identifikation von drei industriellen Revolutionen, die jeweils einen grundlegenden, raschen Umbruch der Produktion widerspiegeln. Nach [Bar+17] müssen für eine industrielle Revolution drei wesentliche Kriterien erfüllt sein:

1. Technologischer Wandel als Auslöser/Voraussetzung
2. Veränderungen in den Bereichen Arbeits- und Sozialordnung, Energieversorgung, Verkehr, Kommunikation und/oder Politik
3. Gesellschafts- und Strukturwandel führt zu einer schnellen Entwicklung

Die erste industrielle Revolution im 18. Jahrhundert wurde durch die Verbreitung der Dampfmaschine ermöglicht und durch weitere Innovationen in Bereichen wie der Herstellung von Stoffen und der Eisengewinnung begünstigt [Ste21]. Die damit verbundene Industrialisierung transformierte große Teile der Bevölkerung von Bauern zu Fabrikarbeitern und führte zu erheblichen Produktivitätssteigerungen. Zudem kam es zur Bildung von Gewerkschaften und Arbeiterparteien [SK11].

Durch die zunehmende Nutzung mechanischer und elektromechanischer Systeme innerhalb der Industrie wurde um das Jahr 1870 die Massenproduktion von Produkten ermöglicht. In einem ähnlichen Zeitraum erfolgte die Einführung von Arbeitsteilung und der wissenschaftlichen Betriebsführung, welche zur Steigerung der Effizienz von Prozessen führten [Ste21]. Dies erhöhte erneut die Produktivität und ging mit Preissenkungen für Produkte und Lohnerhöhungen für Fabrikarbeiter einher.

Die Einführung von Elektronik und Informations- und Kommunikationstechnologie in der industriellen Produktion und der damit verbundenen Etablierung der Robotik markiert um 1960 die dritte industrielle Revolution und führte zur Automatisierung der Fertigung [Ste21]. Mit der im Jahr 1969 vorgestellten SPS wurde die Steuerung von Prozessen und

Maschinen durch gehärtete, austauschbare Controller verbreitet und vereinfacht [ST12]. Parallel erfolgte auch der Beginn der Digitalisierung von Administration und Verwaltung von Betrieben.

Seit einigen Jahren wird der Beginn einer vierten industriellen Revolution beschrieben, die auch unter dem Namen Industrie 4.0 bekannt ist [Sch17]. Hierbei werden integrale Themenbereiche wie eine datenzentrierte Produktion, Nutzung von Cloud-Infrastrukturen, erhöhter Bedarf an IT-Security, als auch eine robuste und zuverlässige Vernetzung von Maschinen und Applikationen hervorgehoben [Bau+14]. Dies schließt auch die Vernetzung mit externen Partnern und Infrastrukturen ein, wodurch vorherrschende Barrieren gegenüber Kommunikationskanälen der Automatisierungsdomäne in das Internet zunehmend aufgelöst werden. Durch die nahtlose Integration von Maschinen und Systemen werden Effizienz- und Qualitätssteigerungen unter der Nutzung von Cyber-physischen Systemen erwartet [Vog+21]. Des Weiteren wird eine flexiblere, anpassungsfähigere Fertigung ermöglicht, die die Erweiterung der Produktvielfalt aufgrund Global-, Regional-, und Personalisierung ermöglicht [Bau17].

Allerdings verläuft die Adoption der Industrie 4.0-Technologien durch Unternehmen langsam. Verschiedene Barrieren wurden hierfür in der Literatur identifiziert. Unzureichende Kenntnisse und fehlende Akzeptanz des Personals führen zu einer fehlenden Grundlage für Transformationen [KAV17]. Auch wird die zentrale Rolle einer IT-Infrastruktur, die Visionen der Industrie 4.0 ermöglicht, identifiziert und hervorgehoben, die innerhalb der Automatisierungsdomäne nicht adäquat ausgefüllt wird [Aut+18]. Als grundlegende Technologien der Infrastruktur werden sowohl das Cloud-Computing als auch die Konnektivität zwischen Applikationen und Geräten innerhalb der Industrie hervorgehoben, die Applikationen basierend auf Datenanalysen, Virtualisierung, und KI ermöglichen [SHF24].

Zusätzliche Adoptionshürden entstehen weiterhin durch die für Industrie 4.0 notwendige Konvergenz von IT- und OT-Systemen. Sie unterscheiden sich grundlegend in deren Anforderungen an Performance, Verfügbarkeit, Systemressourcen und der Beurteilung von Risiken [DSV15].

IT-Systeme zeichnen sich vor allem durch Flexibilität und Skalierbarkeit sowie einer Toleranz gegenüber Lastspitzen aus. OT-Systeme hingegen erfordern vor allem Determinismus und Zuverlässigkeit der Prozesse sowie die Kompatibilität mit einer Reihe an OT-spezifischen Standards. Diese werden unter anderem in dem nächsten Abschnitt näher behandelt.

2.1.1 Industrielle Kommunikationstechnik

Neben den benannten industriellen Revolutionen war die industrielle Automatisierung kontinuierlicher Evolution ausgesetzt.

Abbildung 2.1 stellt die klassische Automatisierungspyramide dar. Sie beschreibt eine hierarchische Struktur von Automatisierungssystemen und wurde durch die Standardisierung verschiedener Ebenen entwickelt. Jede Ebene beherbergt diverse Funktionen, Applikationen, und Verantwortlichkeiten. Durch das Zusammenspiel aller Komponenten und der Datenübertragung untereinander werden Automatisierungsprozesse gesteuert und überwacht.

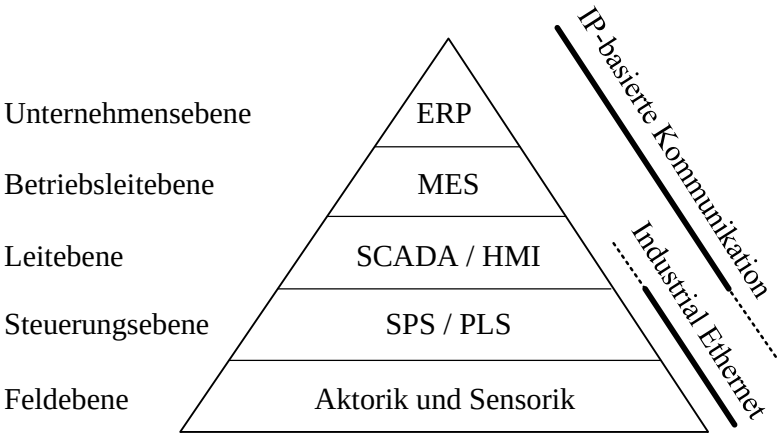


Abbildung 2.1: Die klassische Automatisierungspyramide nach [Sau10]

Die Feldebene stellt die physikalische Interaktion mit Produktionsprozessen dar. Sie enthält Sensorik und Aktorik, die von Komponenten der Steuerungsebene gesteuert werden. Hierzu zählen Steuerungssysteme wie SPS und Prozessleitsystems (PLS), die auf Basis von Datenpunkten der Feldebene Ausgaben berechnen und Steuerbefehle senden. Darüber befinden sich Leitsysteme zur Überwachung und Parametrierung der Steuerungssysteme. Die Leitebene enthält neben einem Supervisory Control and Data Acquisition (SCADA)-System ein Human Machine Interface (HMI) für die Interaktion von Personal mit den Prozessen. Ein Manufacturing Execution System (MES) ist für die Produktionsplanung und -steuerung zuständig und erhält umfassende Informationen von übergelagerten Management-Systemen. Das Enterprise Resource Planning (ERP) innerhalb der Unternehmensebene wird für die Produktionsplanung und Bestellabwicklung verwendet [And17; Hau16].

Um die Anforderungen der Feldebene an Echtzeit und Robustheit zu erfüllen, entwickelten sich im Laufe der Jahre Feldbusstandards. Industrielle Feldbustechnologie ermöglichte einen standardisierten, deterministischen Informationsaustausch innerhalb und zwischen Produktionssystemen [Her+18]. Hierdurch wurden außerdem die andernfalls notwendige Punkt-zu-Punkt Verbindung zwischen der Steuerung und allen Geräten aufgelöst. Steuerungshersteller entwickelten teils konkurrierende Echtzeitprotokolle, die eine deterministische Übertragung von Informationen zwischen den Feldgeräten ermöglichten. Hierbei ist erwähnenswert, dass Feldgeräte innerhalb der Feldebene einige Anforderungen an deren elektrische und mechanische Ausführung erfüllen müssen, sobald sie sich außerhalb von geschützten Schaltschränken befinden [Her+18]:

- Einfache Montage
- Beständigkeit gegen Öl, Spritzwasser und Kühlmittel
- Robuste Steckverbinder
- Widerstandsfähig gegen Temperatur, Schwingungen und Stöße

Einige Zeit wurde das klassische Ethernet, vor allem der kabelgebundene Standard nach IEEE 802.3, als nicht ausreichend deterministisch klassifiziert, wodurch eine Adoption noch Jahrzehnte dauern sollte [Dec09]. Um die Jahrtausendwende veränderten sich zunehmend auch die Anforderungen an industrielle Kommunikationsnetzwerke, da sie neben dem Steuerungs-Datenverkehr auch weitere Informationen mit höheren Bandbreitenanforderungen wie Bilder, Sprache und Video übertragen mussten [Dec09]. Gleichzeitig wurden Ethernet-basierte Kommunikationsnetzwerke robuster und lieferten höhere Bandbreiten und demnach auch die notwendige Performance für industrielle Anwendungen. Dies führte letztlich zur Adoption Ethernet im industriellen Umfeld und stellt einen wichtigen Meilenstein zur IT/OT-Konvergenz dar.

Industrial Ethernet (IE) beschreibt eine Gruppe mehrerer industrieller Standards, die einige Mechanismen von Ethernet adoptiert haben. Hierunter fallen aktuell der Verbreitung nach absteigend PROFINET, EtherNet/IP, EtherCAT, und Modbus TCP [HMS24]. Eine Übersicht über die jeweiligen Standards bietet die Literatur [Fel05]. Die Ausprägungen der IE-Standards unterscheiden sich in ihrer Kompatibilität mit Ethernet sowie der Nutzung IP-basierter Kommunikation. Aufgrund der Notwendigkeit von Personensicherheit der jeweiligen Prozesse werden IE-Protokolle durch Safety-Standards nach International Electrotechnical Commission (IEC) 61508 erweitert [Int11].

Die Kette an Verantwortlichkeiten und Kommunikationsbeziehungen der einzelnen Ebenen wird zunehmend in Frage gestellt und die Auflösung der klassischen Automatisierungspyramide erwartet [BH14; VDB13]. Dies wird auch anhand der Betrachtung eines Beispiels innerhalb der diskreten Produktion im Folgenden deutlich.

2.1.2 Aktuelle Kommunikationsarchitektur

Abbildung 2.2 stellt eine generische Kommunikationsarchitektur nach der klassischen Automatisierungspyramide dar [KMG22]. Sie ermöglicht die Analyse der wichtigsten Kommunikationsbeziehungen und der daraus entstehenden Anforderungen in Folge der Migration zur Industrie 4.0-Technologien. Es kann zwischen drei Bereichen unterschieden werden, die jeweils für gewöhnlich durch Firewalls getrennt sind.

- Automatisierungstechnik: Dieser Bereich enthält die Sensorik und Aktorik sowie die hierzu notwendige Steuerungstechnik. Vor allem werden hier IE-Protokolle genutzt, um zeitkritische und zuverlässige Kommunikation zu ermöglichen.

- IP-basiertes Netzwerk: Die einzelnen Teilbereiche der Automatisierungstechnik werden untereinander und mit übergelagerten Systemen durch ein IP-basiertes Netzwerk verbunden. Diese Ebene befindet sich für gewöhnlich in einem anderen Verantwortungsbereich und nutzt Standards und Technologien aus der IT-Domäne.

- Private/Public Cloud: Übergelagerte Systeme werden zentralisiert auf verteilten Systemen betrieben. Darunter fallen unter anderem MES und ERP zur übergreifenden Steuerung von Prozessen.

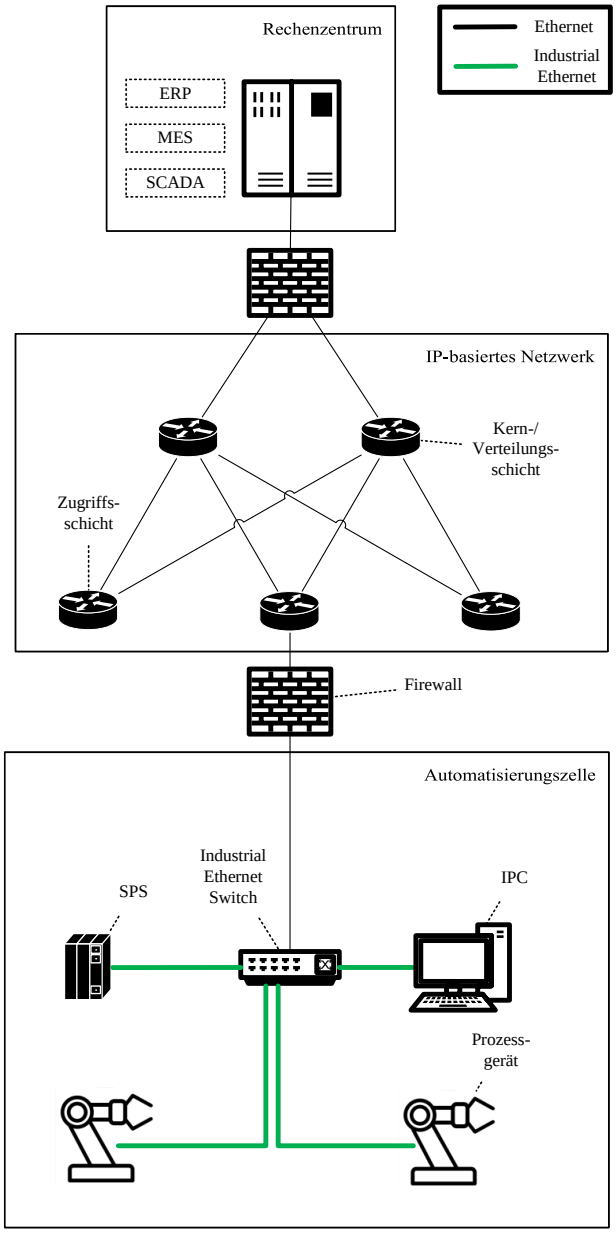


Abbildung 2.2: Generische Kommunikationsarchitektur der Automatisierungdomäne nach [KMG22]

Die Automatisierungszelle enthält eine SPS, die als Steuerung der IE-Geräte wie Roboter, Sensorik und Ventilinseln fungiert. Es wird hier der Fabrikautomatisierung entnommene Begriff der Automatisierungszelle genutzt, um ein IE-Netzwerk abzugrenzen. Jeglicher IE-Datenverkehr wird innerhalb der Zelle durch IE-Switches oder der Weiterleitung durch andere Prozessgeräte in Reihe übertragen. Hierbei gelangt der Steuerungs-Datenverkehr nicht in das übergelagerte IP-basierte Netzwerk. Aus Sicht der IT-Security ist dies auch ratsam, nachdem innerhalb dieses Bereiches keine Authentifizierungsmechanismen auf Netzwerkebene vorhanden sind. Neue Anwendungen werden häufig durch das Hinzufügen weiterer Hardware realisiert [KMG22]. Diese Entwicklung kann beispielsweise auch bei den ersten

Evaluierungen von vSPS beobachtet werden [Fu+24]. Dadurch gestaltet sich die Einführung neuer Anwendungen innerhalb der Automatisierungstechnik durch die Hardware-Bindung als komplex und erhöht den Wartungsaufwand. Außerdem begünstigt die aktuelle Architektur neue Single Point of Failure (SPOF) innerhalb der Prozesskette.

Zur selben Zeit ist eine Kommunikation aus der Zelle notwendig, um beispielsweise Auftragsdaten des Manufacturing Execution System (MES) zu erhalten oder Störungen und Statusmeldungen an ein SCADA zu senden. Diese sogenannte *Nord/Süd-Kommunikation*, oder vertikale Vernetzung, wird zunehmend aufgrund neuer Anwendungen erhöht, beispielsweise der Nutzung von datengetriebener Entscheidungsfindung oder der Optimierung von Prozessen [BH14]. Allerdings beruht das vorherrschende IT/OT-Security-Konzept auf der Nutzung von Firewalls und der Abschottung von Automatisierungsprozessen, sodass sich vor allem dynamisch ändernde Anforderungen an Kommunikationsbeziehungen, beispielsweise ausgelöst durch Mobilitätsszenarien oder der dynamischen Allokierung von neuen Kommunikationspartnern, schwer abbilden lassen. Das übergelagerte IP-basierte Netzwerk gewinnt hierbei an Bedeutung, nachdem dessen Zuverlässigkeit direkten Einfluss auf die untergelagerten Automatisierungsprozesse nimmt. Eine Kompatibilität der verwendeten Standards zwischen der IT- und OT-Domäne ist häufig nicht gewährleistet.

Somit lassen sich einige Defizite klassischer Architekturen bei der Adoption von Industrie 4.0-Konzepten herausstellen [Gil16]:

- Die strikte Separierung erschwert die Adoption von IT-Technologien in der Automatisierungsdomäne und die Findung von Betriebsschnitten und Verantwortlichkeiten.
- Die Einführung von neuen Technologien im Automatisierungsumfeld ist aufgrund von Rahmenbedingungen durch aktuelle Infrastrukturen nicht möglich oder profitabel.
- Kooperation mit internen und externen Partnern ist durch fehlende skalierbare Segmentierungsmöglichkeiten herausfordernd.
- Verwendung von proprietären oder inkompatiblen Standards und Schnittstellen erschwert die Interoperabilität und führt zu starren Systemen.
- Monolithische Software-Designs von Produktions-Applikationen wie MES verbreitet, was häufig zur erschwerten Integration mit anderen Systemen und einem Lock-in-Effekt führt [Man+22]

Neben der Kommunikation bilden die Applikationen einen weiteren zentralen Betrachtungsgegenstand. Die Auflösung der steigenden Komplexität durch das Hinzufügen weiterer Applikationen innerhalb der Automatisierungsdomäne könnte durch die Anwendung des Cloud-Computings gelöst werden.

2.1.3 Cloud-Computing in der Automatisierung

Innerhalb der Literatur existieren verschiedene Definitionen von Cloud-Computing [MPR15; RPZ10]. Hervorgehoben wird zum einen die Bereitstellung von Applikationen auf IT-

Infrastrukturen, die sich physisch nicht am Anwendungsort der Applikation befindet. Diese Separierung in der Bereitstellung des jeweiligen Dienstes führt zur Schlüsselrolle des Kommunikationsnetzwerkes, welches den Anwendungsort mit der Cloud-Infrastruktur verbindet. Zum anderen ermöglicht die Virtualisierung eine flexible und effiziente Nutzung der Ressourcen. Abschließend wird auf IT-Dienstleistungen verwiesen, welche die Handhabung und Interaktion mit Systemen auf der Cloud-Infrastruktur vereinfachen sollen.

Im Vergleich zum klassischen Cloud-Computing befindet sich nach dem Edge-Computing-Ansatz die IT-Infrastruktur näher am jeweiligen Anwendungsort. Gleichzeitig werden die weiteren Eigenschaften von Cloud-Infrastrukturen wie Fehlertoleranz und Virtualisierung von Applikationen beibehalten, was nun auch eine weitflächige Anwendung innerhalb der Automatisierungsdomäne ermöglicht [Sta+20].

Eine Migration der IT-Infrastruktur aus Rechenzentren in eine fertigungsnahe Lokalität ist jedoch nicht ausreichend, um eine vollständige Virtualisierung von Applikationen der Automatisierung zu ermöglichen. Aufgrund der unterschiedlichen Eigenschaften von IT und OT entstehen Zielkonflikte. Durch die Konvergenz von IT und OT entstehen daher neue Anforderungen an die Steuerungs- und Kommunikationstechnik. Dadurch wird eine Validierung auf Basis des Abgleichs von Anforderungen mit Ergebnissen ermöglicht, die zur Fehlervermeidung und der Sicherung von Qualität beiträgt [VDI21]. Die Anforderungen werden im Folgenden näher beleuchtet.

2.2 Anforderungen an die Steuerungstechnik

Steuerungen bilden ein zentrales Organ innerhalb der industriellen Automatisierung. Neben der Kontrolle von Prozessen stellen sie weiterhin einen integralen Kommunikationspartner zu weiteren Systemen wie dem SCADA oder MES. In Zukunft erfordern Steuerungen eine flexible Anpassung ihrer Ressourcen um beispielsweise Konnektivität in Form eines Open Platform Communications Unified Architecture (OPC UA)-Servers oder zusätzlicher Monitoring-Funktionen erweitert werden können, ohne die Performance der notwendigen Berechnungen zu reduzieren.

Um die Vorteile der Virtualisierung nutzen zu können, bedarf es einer Lauffähigkeit von echtzeitkritischen Applikationen auf verteilten Systemen. Dies erfordert eine Hardware-agnostische Funktionalität der Applikationen, die zuvor häufig nur mit dedizierter Hardware erbracht werden konnte. Mittlerweile gibt es von ausgewählten Herstellern die ersten Implementierungen von vSPS sowie die Aussicht auf SIL3-konformen Safety-vSPS auf virtuellen Umgebungen auf Basis des arithmetischen Kodierens [Mue+24]. Hierdurch können während der Laufzeit transiente, permanente und systematische zufällige Fehler aufgedeckt werden [BM13].

Jedoch sind aus infrastruktureller Sicht einige Notwendigkeiten innerhalb der Automatisierungsdomäne für einen klassischen Lift&Shift-Ansatz unzureichend erfüllt. Erste experimentelle Validierungen von vSPS sind bereits in der Literatur vorhanden, doch wird hier weiterhin Industrieller Personal Computer (IPC) verwendet [Fu+24]. Um wirklich alle

Vorteile einer Edge Cloud nutzen zu können, ist neben der erfolgreichen Virtualisierung der Applikation die Konsolidierung von OT-Systemen notwendig. Diese führt zur Verbesserung der Ressourcennutzung sowie der Skalierbarkeit und Betreibbarkeit.

Zur selben Zeit führt die Konsolidierung zu einem erhöhten Risiko für einen Stillstand mehrerer Prozesse, sodass die Notwendigkeit für eine Hochverfügbarkeitslösung erhöht wird. Im Falle eines Ausfalls müssen Prozesse in kurzer Zeit wiederhergestellt und gestartet werden. Trotz der schon lange bekannten Vorteile der Virtualisierung von SPS könnte dies eine der Gründe für die fehlende Umsetzung innerhalb der Automatisierungsindustrie in der Breite sein [CSM16; Gol+15].

Auf Basis der identifizierten Barrieren der Adoption von Industrie 4.0-Technologien ist auch die Akzeptanz und Befähigung des Personals für eine Realisierung neuer Konzepte von integraler Bedeutung [KAV17]. Somit gilt hier, die Änderungen für das Personal zu minimieren, um einen weitreichenden notwendigen Wissensaufbau zu vermeiden und stattdessen inkrementelle Veränderungen durchzuführen. Anwender von einer rein virtuellen Steuerung als Ersatz für die zuvor Hardware-basierten Lösungen zu überzeugen, ist ein notwendiges Kriterium für die Adoption von Virtualisierung in der Automatisierungsdomäne. Auch bei der Einführung der SPS benötigte es einige Zeit, die Anwender davon zu überzeugen, dass eine kleine Box mit Software ganze Schränke von Logikgattern und Kabeln ersetzen könnte [ST12]. Damit die Adoption begünstigt wird, erfordert der Umbruch trotz revolutionärem Charakter einen kontinuierliche Anpassung von Prozessen.

Auch müssen im Rahmen der Konvergenz von IT und OT mit neuen Bedrohungen für die Applikationen gerechnet werden. Fehlende Segmentierungsmöglichkeiten innerhalb der Automatisierungsdomäne gekoppelt mit der zunehmenden Konvergenz von IT und OT erhöhen die Wahrscheinlichkeit für Angriffe auf industrielle Prozesse. Zudem werden aufgrund von vermehrten Schwachstellen, beispielsweise innerhalb des Linux-Kernels mit einer Verdopplung der Anzahl von 2021 zu 2024, häufige Aktualisierungen der Applikationen und Infrastruktur notwendig [Bre24]. Diese müssen kontrolliert, skalierbar, und ohne Einbußen der Verfügbarkeit der Prozesse erfolgen.

2.3 Anforderungen an die Kommunikationstechnik

Der Wandel der industriellen Produktion wirkt sich auch auf die Kommunikationstechnik aus. Nachdem die Vernetzung von Maschinen und Applikationen als Wegbereiter diverser Industrie 4.0-Konzepte gilt, erhöht sich der Stellenwert von Kommunikationsnetzwerken. Vor allem der Bedarf an Nord/Süd-Kommunikation wird durch Fernbedienungsszenarien, der Nutzung von (Edge) Cloud-Technologie oder dem Wunsch nach datengestützter Fertigung erhöht. Dies führt jedoch neue Anforderungen an das IP-basierte Kommunikationsnetzwerk ein.

Eine mögliche Auslagerung und Konsolidierung von zuvor auf der Feldebene vorhandenen Applikationen in eine Edge Cloud führt zur Erweiterung der Determinismusanforderungen auf das IP-basierte Kommunikationsnetzwerk. Insbesondere die Nutzung von vSPS

erfordert die Möglichkeit, IE-Telegramme über das überlagerte IP-basierte Netzwerk zu übertragen. Hierbei gilt es vor allem auf die Kompatibilität der jeweiligen IE-Protokolle mit Ethernet und IP zu achten und Safety-Implementierungen aufgrund ihrer Verbreitung zu unterstützen. Essentiell für eine Nutzung von IT-Infrastruktur im OT-Bereich ist weiterhin das Black Channel-Prinzip, nachdem einige der nach IEC 61508 definierten Safety-Protokolle agieren [Int11]. Dadurch müssen keine IT-Infrastrukturkomponenten zwischen den Safety-relevanten Geräten und Applikationen zertifiziert werden, was die Konvergenz von IT und OT vereinfacht.

Die Einführung von verteilten Systemen und Fokus auf datengetriebene Entscheidungsfindung in der Automatisierungsdomäne erhöht außerdem den Stellenwert eines zuverlässigen Netzwerkes. Kommunikationsunterbrechungen, die bereits unter einer Sekunde dauern, führen vor allem in Safety-Anwendungen zu einem Stillstand des Prozesses. Hier werden demnach Konzepte und Mechanismen benötigt, die die notwendige Resilienz gegen Störungen erbringen und die Verfügbarkeit der Prozesse steigern.

Das beschriebene Verschwinden von klaren Grenzen zwischen den einzelnen Schichten der Automatisierungspyramide durch die Konvergenz von IT und OT erzeugt neue Anforderungen an Kommunikationsnetzwerke innerhalb der Automatisierung. Der Schwerpunkt der IT-Security verlagert sich aufgrund der nach Industrie 4.0 angestrebten Vernetzung von der Host- und Kommunikationsebenen [And17]. Aktuelle Zonierungskonzepte, basierend auf der hierarchischen Trennung der Ebenen, stoßen nun an ihre Grenzen, da die erforderliche Dynamik und Flexibilität von Kommunikationsbeziehungen nicht mit der statischen Natur von klassischen Automatisierungsaufbauten in Einklang gebracht werden kann. Die Nutzung von klassischen IT-Security Mechanismen ist in der Automatisierungsdomäne nur eingeschränkt möglich. Während jegliche Multimedia-Geräte über den Standard IEEE 802.1x an einem Netzwerk authentifiziert werden können, fehlt aktuellen Automatisierungsgeräten häufig diese Fähigkeit. Dies ist neben Kostengründen auf die Notwendigkeit zurückzuführen, Funktionen auf Robustheit, Einfachheit, und Wartbarkeit zu optimieren und somit Komplexität zu reduzieren. Auch bei der Entwicklung von IE-Protokollen wurde selten auf Security-Mechanismen geachtet, sodass jegliche IE-Kommunikation für gewöhnlich im Klartext erfolgt. Zur selben Zeit ist es notwendig, die Determinismus- und Verfügbarkeitsanforderungen der Applikationen zu erfüllen. Hierzu gilt es demnach, neue Konzepte zu entwickeln, die eine Anwendung auf beide Domänen erlauben.

Eine kürzlich erfolgte Zusammenfassung erfolgreicher Cyberangriffe auf industrielle Steuerungen kommt zu dem Schluss, dass die meisten Angriffe durch veraltete Software mit bekannten Schwachstellen, passwortbasierte Authentifizierung ohne starke Regeln oder Zwei-Faktor-Authentifizierung, unüberprüfte Datenübertragungen oder USB-Sticks sowie die mangelnde Isolation von Steuerungen in IT/OT-Netzwerken ermöglicht werden [ACZ20]. Somit gibt es eine Reihe an Angriffsvektoren, die durch Schutzmechanismen abgewehrt werden sollen.

2.4 Formulierung des Forschungsgegenstandes

Traditionelle IT-Kommunikationsnetzwerke und -Umgebungen wurden bisher hauptsächlich auf Skalierbarkeit und Effizienz optimiert und basierten auf etablierten Standards. Mit der fortschreitenden Konvergenz von IT und OT ergeben sich neue Anforderungen, insbesondere im Bereich Determinismus, Echtzeitfähigkeit, Zuverlässigkeit und Personensicherheit. Hierbei steht nun nicht mehr die Effizienz und Standardisierung im Vordergrund, sondern die zuverlässige Erfüllung aller Anforderungen für eine unterbrechungsfreie Automatisierung. Diese Anforderungen sind vielfältig.

Die Virtualisierung und Konsolidierung von zuvor im Shopfloor befindlichen Steuerungen erfordert die deterministische Übertragung von Steuerungs-Datenverkehr über ein IP-basiertes Netzwerk zwischen Shopfloor und (Edge) Cloud-Umgebung. Gleichzeitig müssen über dieselben physikalischen Medien niederpriorisierte Datenströme übertragen werden, ohne die deterministische Übertragung der echtzeitkritischen Telegramme zu beeinträchtigen.

Die Zuverlässigkeit des Kommunikationsnetzwerkes ist nun wichtiger denn je, da hohe Bandbreiten dazu führen, dass Datenströme auf wenige physikalische Verbindungen verteilt werden. Ein Ausfall einer Netzwerkstrecke oder -komponente kann daher mehrere Teile der Automatisierung beeinträchtigen. Der erhöhte hierdurch beeinträchtigte Bereich gilt auch für die auf Servern konsolidierten Applikationen. Ein einzelner Serverausfall kann bereits mehrere darauf befindliche Steuerungen und damit große Teile der Fertigung zum Stillstand bringen.

Darüber hinaus eröffnet die Aufweichung der vorhandenen starren Trennung zwischen den einzelnen Ebenen der Automatisierungspyramide und die Verschiebung von Applikationen in Cloud-Umgebungen der Cyberkriminalität neue Angriffsflächen. Folglich nimmt aufgrund der fortschreitenden Verteilung von Funktionen innerhalb des Kommunikationsnetzwerkes auch der Stellenwert eines IT/OT-Security-Konzepts zu. Hierbei müssen einerseits Geräte und Applikationen vor neuen Angriffsvektoren geschützt werden und gleichzeitig eine Beeinträchtigung von Prozessen durch neue Maßnahmen verhindert werden.

Zusammenfassend erfordert die Konvergenz von IT und OT neue Ansätze zur Sicherstellung von Determinismus, Zuverlässigkeit, und IT/OT-Security. Daraus ergeben sich folgende Forschungsfragen:

- Forschungsfrage 1: Welche Mechanismen ermöglichen eine deterministische Kommunikation auf IP-Ebene für echtzeitkritische Applikationen?
- Forschungsfrage 2: Welche Hochverfügbarkeitskonzepte können zur Erreichung der notwendigen Zuverlässigkeit der Automatisierungsdomäne genutzt werden?
- Forschungsfrage 3: Wie kann ein IT/OT-konvergiertes Netzwerk die steigenden Cybersicherheits-Anforderungen erfüllen?

3 Stand der Wissenschaft

Das folgende Kapitel fasst den aktuellen Stand der Wissenschaft in Bezug auf die zu behandelnden Forschungsfragen zusammen. Hierzu werden grundlegende Konzepte der Bereiche Kommunikationsnetzwerke, Steuerungstechnik, und IT-Sicherheit eingeführt. Eine Bewertung der Erkenntnisse schließt dieses Kapitel ab.

3.1 ISO/OSI-Schichtenmodell

Zunächst wird hier das ISO/OSI-Schichtenmodell beschrieben, welches zwar allgemein bekannt ist, aber gleichzeitig die Basis für jegliche relevanten Kommunikationsstandards darstellt. Seit 1979 wird von der International Organization for Standardization (ISO) nach dem Open Systems Interconnection (OSI) das ISO/OSI-Schichtenmodell standardisiert. Die Zielstellung des Standards ist ein Referenzmodell, welches die Interoperabilität verschiedener Netzwerkhersteller miteinander in einem Kommunikationsnetzwerk ermöglicht. Des Weiteren gewährleistet das Modell die Modularität der einzelnen Teilfunktionen durch eine strenge Hierarchie der einzelnen Schichten [LG20].

Das Schichtenmodell gliedert sich in sieben Schichten. Abbildung 3.1 stellt das Versenden von Daten zwischen Quelle und Empfänger dar. Hierfür werden die einzelnen Schichten beim Versenden von oben nach unten verlaufen, in welcher jede Schicht das gegebene Datenpaket kapseln kann. Dies erfolgt beispielsweise durch das Anhängen eines Headers oder Trailers. Das gekapselte Objekt wird anschließend an die nächste Schicht weitergegeben. Im Rahmen der Entkapselung erfolgen die Schritte in umgekehrter Reihenfolge. Vermittlungssysteme zwischen den Endsystemen kapseln und entkapseln die Telegramme sofern notwendig [LG20].

Der hinzugefügte Header in der jeweiligen Schicht wird als Protocol Control Information (PCI) bezeichnet. Wird der Inhalt der nächsthöheren Schicht, der Service Data Unit (SDU), hinzugenommen, ergibt sich die Protocol Data Unit (PDU), welche sich je nach Schicht in ihrer Bezeichnung unterscheidet. Diesen Sachverhalt lässt sich in Abhängigkeit einer Schicht N mit folgender Formel abbilden:

$$PDU(N) = PCI(N) + SDU(N) + Trailer(N) \tag{3.1}$$

$$= SDU(N-1) \tag{3.2}$$

Weiterhin lässt sich beobachten, dass folgender Zusammenhang gilt:

$$PDU(N+1) = SDU(N) \tag{3.3}$$

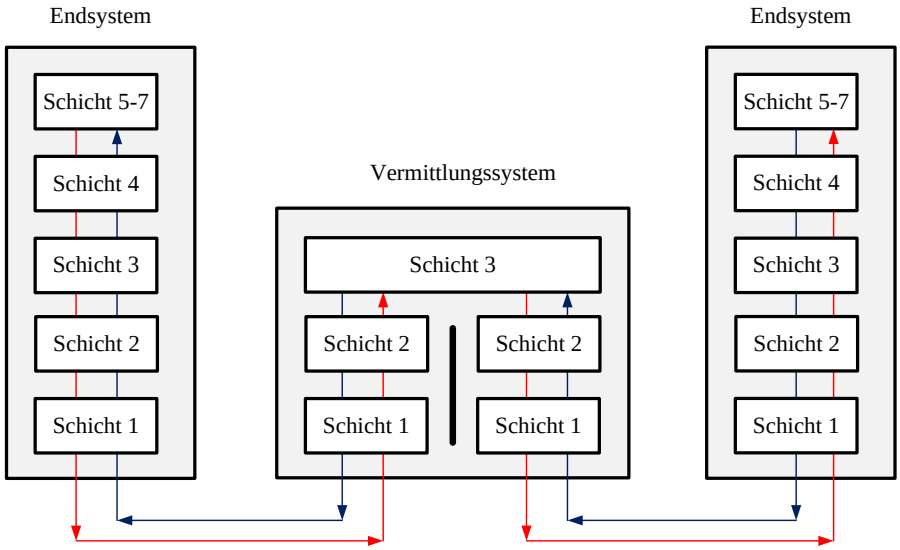


Abbildung 3.1: ISO/OSI-Referenzmodell nach [LG20]

Abbildung 3.2 stellt die Bezeichnungen der PDU der jeweiligen Schichten und die Funktionsweise des Hinzufügens der PCI dar.

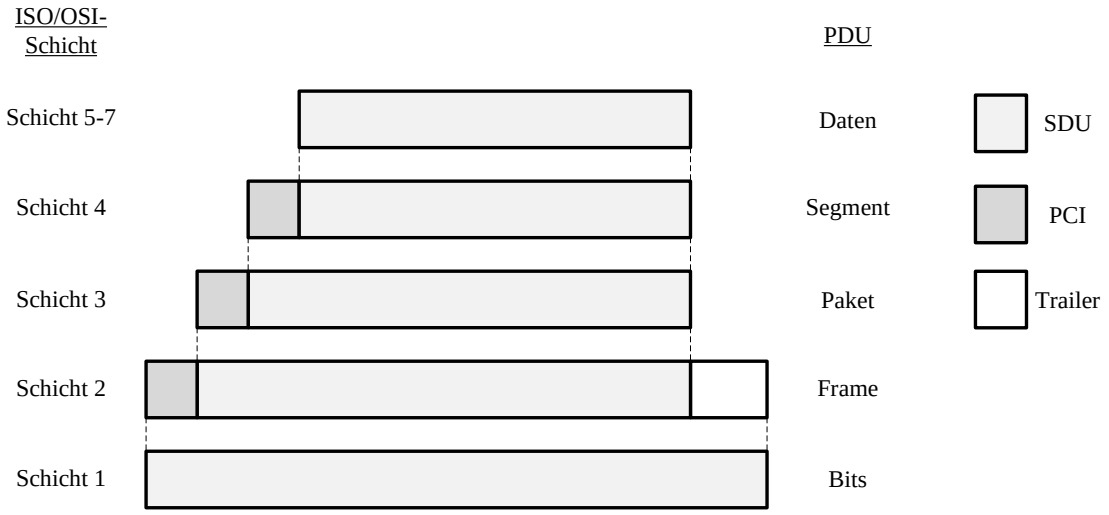


Abbildung 3.2: PDU Bezeichnungen: SDU, PCI und Trailer

Während das ISO/OSI-Referenzmodell eine Gruppierung von Protokollen ermöglicht, ist anzumerken, dass es sich lediglich um ein Referenzmodell handelt und gewisse Protokolle sich nicht einheitlich in die vorgegebene Struktur einsortieren lassen. Dennoch bilden die Schichten im Allgemeinen die Basis für jegliche Kommunikationsnetzwerke und werden daher im Folgenden detaillierter beschrieben.

3.1.1 Bitübertragungsschicht (Schicht 1)

Die Bitübertragungsschicht beschreibt die Übertragung von Daten in Form von Bits über ein physikalisches Medium. Protokolle dieser Schicht definieren unter anderem die Geschwindigkeit der Übertragung, die Bitrate, sowie ob eine Kommunikation in beide Richtungen gleichzeitig erfolgen kann. Nachdem es bei jeglicher Form der Kommunikation, kabelgebunden als auch kabellos, zu Verlust und Verfälschung der übertragenen Daten kommen kann, werden häufig redundante Informationen zur Überprüfung und Wiederherstellung des Bitstroms hinzugefügt [TW12].

3.1.2 Sicherungsschicht (Schicht 2)

Die zweite Schicht wird als Sicherungsschicht bezeichnet. Neben der Behandlung von Übertragungsfehlern mittels Prüfsummen und der Bereitstellung einer gemeinsamen Schnittstelle für Schicht 3-Kommunikation erfolgt hier eine Regulierung des Datenverkehrs [TW12]. Diese Schicht wird nur oberflächlich beschrieben und für weitere Details auf Literatur verwiesen [LG20; Mey14].

Telegramme erhalten Media Access Control (MAC)-Adressen der Quell- und Zieladresse, sodass eine Adressierung auf dieser Schicht ermöglicht wird. Das bevorzugt eingesetzte Netzwerkgerät dieser Schicht ist ein Switch. Eintreffende Frames werden auf Basis einer MAC-Adresstabelle innerhalb des Switches an den jeweiligen Port weitergeleitet, hinter welcher sich die Zieladresse befindet. Sollte die Ziel-Mac-Adresse noch nicht bekannt sein, erfolgt das Aussenden einer Broadcast-Nachricht. Dies führt zur Aussendung auf allen Ports des Switches. Sollte eine Antwort von dem jeweiligen Gerät erfolgen, wird der Eintrag in der MAC-Adresstabelle aufgenommen. Anhand der Ziel-MAC-Adresse können auch direkt alle oder nur eine Teilmenge der Geräte adressiert werden, indem die jeweilige MAC-Adresse einer Broadcast- oder Multicast-Adresse entspricht [Cis21]. Ein Padding sowie ein Cyclic Redundancy Check (CRC) schließen das Frame ab [Mey14].

Weitere Header und Trailer werden gewöhnlicherweise in dieser Schicht hinzugefügt. Der wichtigste zu erwähnende Standard ist IEEE 802.1Q.

3.1.2.1 IEEE 802.1Q

Der Standard IEEE 802.1Q definiert die herstellerübergreifende Signalisierung einer Priorisierung von Datenverkehr als auch die logische Segmentierung von physikalischen Netzwerken. Insgesamt drei Bits des 802.1Q-Headers können zur Definition einer Prioritätsklasse genutzt werden, sodass insgesamt acht Klassen definiert werden können. Die logische Segmentierung erfolgt auf Basis des Konzeptes von Virtual Local Area Network (VLAN), sodass Kommunikationsteilnehmer verschiedener VLAN voneinander getrennt werden können. Zudem erlaubt es die Anwendung von Regeln und Identifizierung von ausgewählten Telegrammen. Der VLAN Identifier (VID) kann 4096 verschiedene Werte erhalten [IEE18].

3.1.3 Vermittlungsschicht (Schicht 3)

Die Netzwerk-/ oder Vermittlungsschicht ermöglicht die Kommunikation zwischen unterschiedlichen Netzwerken. Sie zeichnet sich durch fehlende Annahmen auf Topologien aus, sodass die Wegfindung der Pakete über Routingprotokolle erfolgt [LG20].

Relevante Konzepte, die in dieser Schicht definiert werden, sind Internet Protocol (IP)-Adressen, Subnetzmasken und Gateways. Generell werden IPv4-Adressen genutzt, die auf 32 Bits eine Adresse definieren. Durch die zunehmende Digitalisierung von Geräten wurden bereits IPv6-Adressen eingeführt, die mit 128 Bits auch in Zukunft einzigartige IP-Adressen ermöglichen können. Im Gegensatz zu MAC-Adressen sind IP-Adressen nicht Hardware-gebunden und demnach flexibel zuweisbar. Die Einteilung des IP-Adressbereiches erfolgt durch die Nutzung von Subnetzmasken, welche Teile der Adresse maskieren. Eine Kommunikation zwischen verschiedenen Netzwerken erfolgt über die Angabe des eigenen Gateways. Das Gateway ist für gewöhnlich ein Router oder Schicht 3-Switch, der Kenntnis über Routen in andere Netzwerke besitzt und das jeweilige Paket weiterleitet. Sowohl die Routen als auch die Wege zum Gateway des Zielnetzwerkes werden über Routingprotokolle bekanntgemacht und bestimmt [TW12].

Weiterhin können Differentiated Services Code Point (DSCP)-Werte von 0-63 genutzt werden, um eine Priorisierung von Paketen innerhalb von Routern und Switchen zu ermöglichen. Router und Switche besitzen für gewöhnlich mehrere Hardware-Warteschlangen, die jeweils unterschiedlich parametriert werden können. Die Priorisierung erfolgt auf Basis von Quality of Service (QoS), wodurch Pakete auf Basis ihres DSCP-Wertes in ausgewählte Warteschlangen gelangen, die gegenüber anderen Warteschlangen beispielsweise schneller geleert werden. Priorisierung per Datenstrom ohne eine Gruppierung ist aus Skalierungsgründen für eine höhere Anzahl nicht umsetzbar [Bla+98].

3.1.4 Transportschicht (Schicht 4)

Sobald sich mehrere Applikationen hinter einer IP-Adresse verbergen, erfolgt dessen Adressierung über die Definition von Ports. Diese werden in der vierten Schicht, der Transportschicht, innerhalb eines 16 Bit-Headers definiert. Diese Schnittstelle wird auch als Socket bezeichnet.

Innerhalb dieser Schicht kann vor allem zwischen den beiden Protokollen Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) unterschieden werden. TCP stellt das Standardprotokoll im Internet dar und ermöglicht eine zuverlässige Zustellung von Segmenten durch einen erneuten Versand von Telegrammen in Folge eines Paketverlustes. Die Sicherstellung korrekter Sequenzen und angekommener Segmente ist komplex, weshalb sowohl auf die Literatur als auch Request for Comments (RFC) 4614 verwiesen wird, welche als Leitfaden eine Reihe an Erweiterungen von TCP zusammenfasst [Duk+06; TW12]. Im Gegensatz dazu stellt UDP ein verbindungsloses Transportprotokoll dar, welches IP-Pakete um Quell- und Ziel-Ports erweitert. Aufgrund der Einfachheit und der verbindungslosen Kommunikation wird dieses Protokoll häufig für Echtzeitanwendungen genutzt [TW12].

3.1.5 Anwendungsorientierte Schichten (Schicht 5 bis 7)

Das ISO/OSI-Referenzmodell definiert drei weitere Schichten, wobei sie im Rahmen dieser Arbeit nicht relevant sind. Demnach werden in der Sitzungsschicht das Management von Sessions beschrieben, die eröffnet, überwacht, und beendet werden können. Innerhalb der Darstellungsschicht, Schicht 6, erfolgt eine Syntax- und Formatanpassung. Abschließend stellt die Anwendungsschicht die siebte Schicht des Modells dar, in welche Parameter der Kommunikation spezifiziert und Dienste angeboten werden [Mey14]. Tiefgehende Informationen zu den Schichten finden sich in der Literatur [LG20].

3.2 Software-defined Networking

Dieser Abschnitt handelt von dem Software-defined Networking (SDN)-Ansatz, welcher die Kontrolllogik der Netzwerkgeräte von der Paketweiterleitung separiert. Hierzu werden im Folgenden die Datenebene und Kontrollebene vorgestellt.

3.2.1 Datenebene durch VXLAN

Basierend auf RFC 7348 wird seit 2014 der Virtual extensible Local Area Network (VXLAN)-Standard von der Internet Engineering Task Force (IETF) spezifiziert [Mah+14]. Ursprünglich für Rechenzentren entwickelt ermöglicht VXLAN das Erzeugen von virtuellen Netzwerken auf Schicht 2 durch Tunneln von Telegrammen. Dies wird auch als Overlay bezeichnet, nachdem ein virtuelles Schicht 2-Netzwerk über ein Schicht 3-Netzwerk erzeugt wird. Im Folgenden werden die für die Arbeit relevanten Parameter und Eigenschaften von VXLAN definiert. Für eine vollständige Beschreibung des VXLAN-Protokolls wird auf RFC 7348 verwiesen [Mah+14].

Abbildung 3.3 stellt beispielhaft ein VXLAN-Telegramm dar. Dieses enthält zunächst den Virtual Network Identifier (VNI), welcher nach RFC 7348 ein virtuelles Overlay-Netzwerk beschreibt [Mah+14]. Durch die verfügbaren 2^{24} Kombinationen von VNI ist nun im Vergleich zu den 2^{12} möglichen VID des IEEE 802.1Q-Headers möglich, die Kommunikation feingranular und skalierbar einzuschränken. Skalierbarkeit bezeichnet im Kontext von Kommunikationsnetzwerken die Fähigkeit, eine große Anzahl von Netzwerkkomponenten, Geräten oder Benutzern zu vernetzen, ohne Performance oder Betreibbarkeit des Kommunikationsnetzwerkes einzuschränken.

Weiterhin haben sich innerhalb von Implementierung von VXLAN Group-based Policy (GBP) etabliert. Obwohl es sich lediglich um einen Entwurf eines Standards handelt, stellen GBP den Industriestandard der Mikrosegmentierung dar [SK16]. Es werden 16 Bit des in RFC 7348 definierten reservierten Bereichs genutzt, um eine Sicherheitsgruppe (SG), im De-Facto-Standard als Group Policy ID bezeichnet, zu definieren. Dieser Parameter wird Kommunikationsteilnehmern zugewiesen und ermöglicht Netzwerkkomponenten, definierte Regeln für eine gegebene Kommunikationsbeziehung anzuwenden. Allerdings besitzt die Nutzung von VXLAN auch Implikationen auf die IT-Security. Traditionell können Schicht 2-Netzwerke nur innerhalb ihres Netzwerkes kommunizieren, sodass Angreifer Zugang zu dem

jeweiligen Netzwerk besitzen müssen. Dieser Zugang wird für gewöhnlich über Firewalls reglementiert. Durch das Tunneln von Schicht 2-Netzwerken über ein IP-basiertes Netzwerk können nun vereinfacht Kommunikation zu den zuvor isolierten Netzwerken aufgebaut werden, sodass dies weitere Schutzmechanismen erfordert.

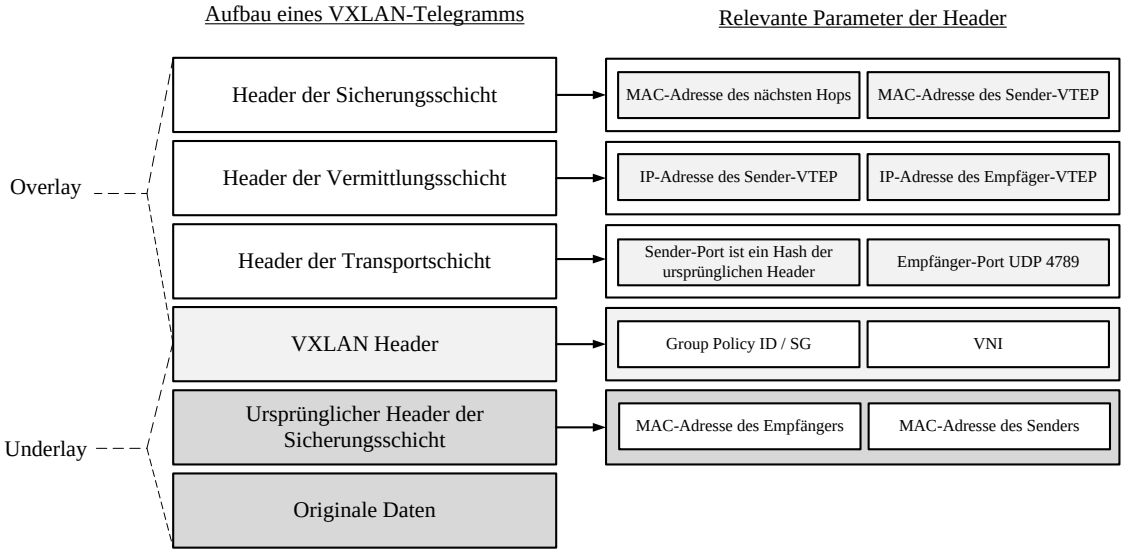


Abbildung 3.3: VXLAN-Header und relevante Parameter

Durch VXLAN wird somit ein virtuelles Schicht 2-Netzwerk über das physikalische Netzwerk erzeugt. Für Geräte der Feldebene, beispielsweise Prozessgeräte und Aktoren als auch virtuelle Kommunikationsteilnehmer wie vSPS, sieht es weitgehend so aus, als wären sie jeweils in einem physikalischen Schicht 2-Netzwerk verbunden. Die Kapselung erfolgt am sogenannten VXLAN-Tunnel-Endpunkt (VTEP) durch hardwarebasierte Funktionen in der Anwendungsspezifischen integrierten Schaltung (ASIC) der Netzwerkkomponente, wobei auch Implementierungen in Software oder Netzwerkkarten existieren.

VXLAN wurde bereits als mögliches Tunnelprotokoll für IE-Steuerungsverkehr benannt, wobei tiefergehende Betrachtungen sowie die Nutzung einer Kontrollebene fehlen [HMS21; Ros+23].

3.2.2 Funktion der Kontrollebene

Damit die Informationen über Geräte und Netzwerke hinter den jeweiligen VTEP ausgetauscht werden können, benötigt es ein weiteres Protokoll nach dem SDN-Ansatz. Hierzu ist es notwendig, den Begriff der Fabric einzuführen.

Eine Fabric beschreibt ein logisches Konstrukt, welches sich über mehrere Netzwerkgeräte erstreckt und eine Entität darstellt. Eine Fabric verbindet jegliche daran verbundene Kommunikationspartner vergleichbar mit einem Mesh-Netzwerk. Ein VTEP ist eine Entität, die Datenverkehr von außerhalb der Fabric mittels VXLAN kapselt und wiederum ausgehenden Datenverkehr entkapselt.

Durch die Nutzung einer Kontrollebene gilt das VXLAN-Protokoll als besonders skalierbar und effizient, da ausschließlich die Switche mit einem VTEP die Informationen über die mit ihnen verbundenen Geräten und deren Kommunikationspartner erhalten müssen. Daraufhin erfolgt die Übertragung innerhalb der Fabric ohne weitere Kapselungen auf Basis klassischer Routing-/ und Switching-Mechanismen. Die Entkapselung erfolgt am Ausgang der Fabric.

Die dafür verwendeten Protokolle sind beispielsweise Ethernet Virtual Private Network (EVPN) oder Locator Identity Separation Protocol (LISP). Während Unterschiede innerhalb der Mechanismen und Methoden vorhanden sind, werden sie ausschließlich für den Austausch der für VXLAN notwendigen Tunnelendpunkt-Informationen verwendet. Hierbei ist vor allem die Konsistenz der Zustände von Relevanz, damit die richtigen Informationen zu den einzelnen Netzwerkkomponenten, die einen VTEP darstellen, übertragen werden. Für eine tiefergehende Betrachtung der einzelnen Standards wird auf die Literatur verwiesen [Far+13; GG21].

3.2.3 Datenübertragung in einer Fabric

Die eigentliche Übertragung der Telegramme innerhalb der Fabric erfolgt auf Basis von klassischen Routing-Mechanismen. Deswegen wird das Underlay durch ein beliebiges Routingprotokoll wie Intermediate System to Intermediate System Protocol (IS-IS), Border Gateway Protocol (BGP) oder Open Shortest Path First (OSPF) bereitgestellt. Somit werden notwendige Informationen über Routen zwischen den einzelnen Netzwerkkomponenten ausgetauscht, sodass eine Datenkommunikation ermöglicht wird. Die jeweiligen Routingprotokolle werden innerhalb der Literatur näher beleuchtet [Sch16].

Besonders ist hierbei, dass lediglich die Informationen der VTEP über diese Protokolle ausgetauscht werden müssen, nachdem VXLAN durch die Kapselung keine Endgeräte als Ziel-Adresse vorsieht. Dies geht erneut mit einer Steigerung der Skalierbarkeit einher, obwohl es die Betreibbarkeit der Lösung aufgrund der Komplexität erhöht. Sollen nach dem Fabric-Ansatz Geräte an beliebige Zugriffschicht-Netzwerkkomponenten verbunden werden können, ist ein Anycast-Gateway notwendig. Hier wird die jeweilige Gateway-IP-Adresse auf die Netzwerkkomponenten konfiguriert, die für das jeweilige Subnetz ein Gateway darstellen sollen. Somit kann die Konfiguration der mit der Zugriffschicht verbundenen Geräte identisch bleiben, obwohl sie mit einem anderen physikalischen Switch kommunizieren. Diese Ermöglichung der Mobilität ist vor dem Hintergrund der kabellosen Kommunikation als auch der Virtualisierung von großem Vorteil.

3.3 Echtzeitfähigkeit und Determinismus von Kommunikationsnetzwerken

Die Definition von Echtzeit ist situativ an das jeweilige Szenario anzupassen und beschreibt im Allgemeinen die Nützlichkeit eines Systems, wenn eine Frist nicht eingehalten wird [But+05].

3.3.1 Quality of Service

Innerhalb der Evolution von QoS für Kommunikationsnetzwerke konnten zwei Pfade beobachtet werden. Bei der Leitungsvermittlung wird die Bandbreite Ende-zu-Ende reserviert und ermöglicht damit eine verlustfreie Übertragung. Ein Beispiel hierfür stellt das klassische Telefonnetz dar. Diese Art der Kommunikation bewirkt, dass Zustandsinformationen über jeden Datenstrom in jeder beteiligten Netzwerkkomponente vorhanden sein müssen. Standardisiert wurden hierzu beispielsweise Mechanismen innerhalb von RFC 1633 und RFC 2211 [Szi+13].

Nachdem dieses System somit nicht die Skalierungsanforderungen von großen, dynamischen Kommunikationsnetzwerken erfüllen konnte, entstand das Differentiated Services Schema. Hier wird der DSCP-Wert eines IP-Pakets verwendet, um die Telegramme in eine gewünschte Warteschlange einzusortieren und somit eine Priorisierung von Paketen zu ermöglichen. Die Priorisierung führt zu niedrigeren Latenzzeiten und geringerem Paketverlust. Unter Einhaltung der Rahmenbedingungen wie Bandbreitenreservierung für ausgewählte Warteschlangen und passende Kommunikationszeitpläne kann dadurch eine echtzeitfähige Kommunikation ermöglicht werden.

An einer Netzwerkkomponente eintreffende Pakete durchlaufen eine Folge an verschiedenen Schritten, bevor sie weitergeleitet werden. Nach der Klassifikation, welche beispielsweise auf Basis des DSCP-Wertes erfolgt, können vor allem Bandbreiten begrenzt und somit Pakete verworfen werden. Dies geschieht auch bei der Stauvermeidung, sodass Pakete bei gefüllten Warteschlangen nach verschiedenen Algorithmen, beispielsweise Weighted Random Early Detection (WRED), frühzeitig verworfen werden und vor allem TCP-basierter Kommunikation signalisieren, die genutzte Bandbreite zu reduzieren [Szi+13].

3.3.2 Time Sensitive Networking

Time Sensitive Networking (TSN) steht als Hypernom für eine Reihe von Erweiterungen des Ethernet-Standards, die eine deterministische Kommunikation auf Schicht 2 ermöglichen. Nach der Modularitätsanforderung des ISO/OSI-Referenzmodells werden darüberliegende Schichten nicht beeinflusst. Einige Substandards werden im Folgenden behandelt. Eine komplette Übersicht über alle veröffentlichten Standards bietet eine Zusammenstellung der Institute of Electrical and Electronics Engineers (IEEE) [IEE24].

Zunächst wird mittels der Standards IEEE 802.1Qbu die Priorisierung von hochpriorem Datenverkehr und Unterbrechung der Kommunikation von niederpriorem Datenverkehr ermöglicht, welches als Preemption bezeichnet wird [Nas+19]. Dies ermöglicht auch die formale Validierung einer maximalen Latenzzeit für die Kommunikation, welche insbesondere auch die hervorragenden Latenz-Eigenschaften von IEEE 802.3 in Kombination mit Preemption hervorhebt [TE16].

Je nach Anforderung an die jeweilige Kommunikation sind weitere Mechanismen anwendbar. Demnach reduziert IEEE 802.1Qbv den Jitter durch die Nutzung eines Kommunikationszeitplans mit Zeitschlitzen auf Basis eines zeitgesteuerten Weiterleitungsmechanismus

[IEE16]. Dies ist vor allem für Bewegungsregelungen von Relevanz, da diese Gruppe der Applikationen sensitiv auf Jitter reagieren. Weiterhin sind erneut Untersuchungen über die maximalen Latenz- und Jitterwerte in der Literatur zu finden [ZPC18]. Mittels IEEE 802.1Qcc können Netzwerkressourcen automatisiert verwaltet werden und IEEE 802.1AS ermöglicht ein gemeinsames Verständnis von Zeit [Nas+19].

Abschließend stellt das Cyclic Queuing and Forwarding (CQF) eine Möglichkeit zur deterministischen Übertragung von zeitkritischem Datenverkehr dar [IEE19]. Dies wird durch das zyklische Übertragen von Datenströmen zu definierten Zeitintervallen erreicht. Der Standard kombiniert unter anderem Mechanismen aus IEEE 802.1Qbv und IEEE 802.1Qci, welche Filterung und damit Entscheidungen auf einer Datenstrom-Basis ermöglichen [IEE19].

3.3.3 Deterministic Networking

Vor allem in größeren Umgebungen wird ein IP-basiertes Netzwerk benötigt, welches zur selben Zeit die Determinismus-Anforderungen ausgelöst durch die IT/OT-Konvergenz erfüllt. Dieses Ziel verfolgt die IETF Deterministic Networking (DetNet)-Gruppe, welche die zuvor auf Schicht 2 begrenzten Mechanismen um die Vermittlungsschicht versucht zu erweitern. Eine Zusammenfassung über die Aktivitäten und veröffentlichten RFC findet sich in der Übersicht der IETF [IET22].

Im Vergleich zu TSN wird der inhärenten IT/OT-Security mehr Beachtung geschenkt, da auch Kommunikation höherer Schichten ermöglicht wird. Zudem erfolgt eine stärkere Fokussierung auf Skalierbarkeit. Diese wird beispielsweise durch eine Erweiterung des CQF durch eine zustandslose Komponente ermöglicht, wodurch mehrere Datenströme zusammengefasst werden können. Dies wiederum folgt dem Design-Ansatz des Internets, wodurch das Kommunikationsnetzwerk sowohl skalierbar als auch robust wird [Sto00].

Kommerziell erhältlich sind bisher keine Netzwerkkomponenten, die die jeweiligen Standards erfüllen. Eine Validierung eines Prototypen erfolgte bereits mit Hilfe einer SPS des Unternehmens CODESYS GmbH, in welcher Steuerungs-Datenverkehr deterministisch über ein IP-basiertes Netzwerk übertragen wurde [Bad+19].

3.4 Hochverfügbarkeit von Kommunikationsnetzwerken

Die Verfügbarkeit und Zuverlässigkeit von Kommunikationsnetzwerken war bereits Gegenstand diverser wissenschaftlicher Arbeiten. Zuverlässigkeit wird häufig als zusammenfassender Ausdruck für verschiedene Begriffe wie Funktionszuverlässigkeit, Sicherheit oder Verfügbarkeit verwendet [Ver07].

Der Begriff der Verfügbarkeit besitzt je nach Zielstellung unterschiedliche Definitionen. Die für die Automatisierung relevante operationale Verfügbarkeit beschreibt die durchschnittliche Verfügbarkeit des Systems gegenüber der Gesamtzeit und schließt Hochfahrzeit und Wartungsfenster mit ein [Kat95]. Tabelle 3.1 stellt verschiedene Systemdefinitionen mit den zugehörigen Verfügbarkeiten dar. Damit die Eigenschaft der Hochverfügbarkeit erreicht werden kann, wird eine Verfügbarkeit von 99,999% oder höher benötigt [GS91]. Dieser Wert

unterscheidet sich jedoch je nach Literaturquelle [Net18].

Tabelle 3.1: Verfügbarkeit von Systemklassen nach [GS91]

Systemtyp	Nichtverfügbarkeit $\frac{min}{y}$	Verfügbarkeit
Unverwaltet	52560	90%
Verwaltet	5256	99%
Gut verwaltet	525,6	99,9%
Fehlertolerant	52,56	99,99%
Hochverfügbar	5,256	99,999%
Sehr hochverfügbar	0,527	99,9999%
Ultra-hochverfügbar	0,053	99,99999%

Verfügbarkeit kann durch verschiedene Maßnahmen erhöht werden, die die Wahrscheinlichkeit eines Systemausfalls reduzieren. Demnach ermöglicht die Nutzung redundanter Systembestandteile, beispielsweise einer aktiven und passiven Komponente, die Reduktion der Stillstandszeit im Fehlerfall [LT09]. Allerdings besitzt auch die Komplexität eines Netzwerkes einen Einfluss auf dessen Verfügbarkeit. Innerhalb der Designphase wird anhand von Erfahrungen von Googles Netzwerkinfrastruktur ein Fokus auf Verfügbarkeit empfohlen, obwohl komplexere Lösungen nicht explizit ausgeschlossen werden [Gov+16].

Nachdem Datenverluste oder Verbindungsabbrüche besonders geschäftskritscher Systeme und Applikationen vermieden werden sollten, haben sich bereits verschiedene Standards und Mechanismen zur Realisierung von Hochverfügbarkeit für Kommunikationsnetzwerke etabliert. Es gilt im Allgemeinen, SPOF zu vermeiden. Im Folgenden werden verschiedene Konzepte und Begriffe eingeführt, die für das spätere Architekturkonzept von Relevanz sind sowie den Stand der Wissenschaft widerspiegeln.

3.4.1 Standards für Schicht 2

Die Sicherungsschicht bietet bereits vielfältige Optionen zur Erreichung der Hochverfügbarkeit von Kommunikationsnetzwerken. Häufig zeichnen sich diese durch die Duplizierung von Telegrammen aus und gehören zur Gruppe der statischen Redundanzprotokolle, deren Mechanismen nicht von äußeren Abhängigkeiten oder Kalkulationen aufgrund von Zustandsübergängen abhängen.

Bei der Anbindung von Servern wird häufig das Link Aggregation Control Protocol (LACP) genutzt, welches durch die Bündelung mehrerer physikalischer Verbindungen zu einer logischen Verbindung eine Lastverteilung ermöglicht [IEE20]. Fehlerhafte Verbindungen werden durch das Versenden von Hello-Paketen erkannt, welche für die Gruppe der dynamischen Redundanzprotokolle einen typischen Mechanismus darstellen.

Innerhalb des Standards IEC 62439-3 werden zwei Duplizierungsmechanismen beschrieben. Das Parallel Redundancy Protocol (PRP) zeichnet sich durch die Duplizierung von Frames aus, bei der wiederum auf der Empfängerseite das schnellere der beiden duplizierten Telegramme weitergeleitet und das Langsamere verworfen wird. Duplikate werden anhand

einer Zyklusnummer, welcher Teil des PRP-Trailers ist, und der Quell-MAC-Adresse erkannt. Mögliche Ausprägungen von Kommunikationsteilnehmern innerhalb von PRP-Netzwerken sind in Abbildung 3.4 dargestellt. Notwendig für das korrekte Verhalten dieses Standards sind zwei separate Netzwerke, LAN A und LAN B, an welche entweder die Reduction Box (RedBox) oder ein Dual-attached Node (DAN) verbunden werden kann. Geräte und Applikationen, die sich hinter einer RedBox befinden, werden als Virtual Dual-attached Node (VDAN) bezeichnet. Gleichzeitig werden auch Single-attached Node (SAN) unterstützt, die nur an einem der beiden Netzwerke verbunden sind. Erreicht wird dies durch die Nutzung eines Trailers, sodass es als Padding ignoriert wird [Int+16].

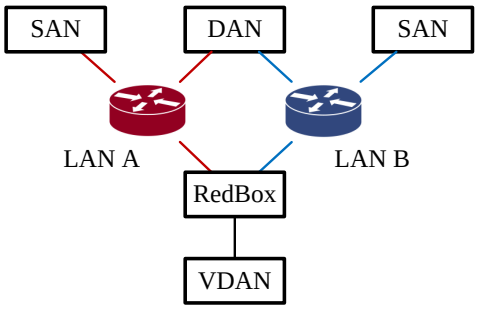


Abbildung 3.4: Übersicht von möglichen PRP-Kommunikationsarten

Als zweiten Standard wird in IEC 62439-3 High-availability Seamless Redundancy (HSR) beschrieben, welches Ring-Topologien voraussetzt. Somit können nur DAN genutzt werden. Allerdings befinden sich hier Informationen wie die Zyklusnummer im Header, sodass eine schnellere Übertragung der Frames, beispielsweise durch Cut-Through Switching, ermöglicht wird [Int+16].

Auch die Gruppe der TSN-Standards bietet eine Lösung zur Duplizierungsmechanismen auf Schicht 2. IEEE 802.1CB definiert Frame Replication and Elimination (FRER), welcher sich durch beliebige Netzwerktopologien und der Kompatibilität mit beiden IEC 62439-3 Standards auszeichnet [IEE17]. Weiterhin kann die Duplikatserkennung auf Basis von IP-Adressen erfolgen.

Es existieren weitere proprietäre Mechanismen, die allerdings nur in ausgewählten Bereichen wie bei der Nutzung des Protokolls PROFINET IRT Anwendung finden. Diese sind jedoch generell nicht auf andere Protokolle anwendbar, sodass die Anwendbarkeit des Architekturkonzeptes eingeschränkt werden würde.

3.4.2 Label Switching

Multiprotocol Label Switching (MPLS), oft als Schicht 2,5-Protokoll beschrieben, ermöglicht ein schnelles Umleiten von Datenverkehr im Fehlerfall unter dem Namen Multiprotocol Label Switching Transport-Profile (MPLS-TP). Ein Backup-Pfad beginnt am Punkt der lokalen Reparatur und verbindet sich mit dem primären Pfad an einem Zusammenführungspunkt. Dieser Mechanismus erfordert jedoch die Erkennung von Fehlerzuständen und

das anschließende Umschalten auf den Backup-Pfad. Deshalb hängt die Dauer der Wiederherstellungszeit vor allem von der Detektion des Fehlerzustandes, der Signalisierungszeit zu den jeweiligen Orten der Entscheidung sowie möglicher Netzwerkkonvergenzzeiten ab. Hierfür wird verbreitet das Bidirectional Forwarding Detection (BFD) genutzt, welches Redundanzprotokoll-agnostisch eine Detektierung von Link-Fehlern ermöglicht. Dies wird durch das zyklische Versenden von Hello-Paketen erreicht, die bei einer hohen Frequenz in wenigen Millisekunden ein Fehler detektieren können [KW10]. Für nähere Informationen zu MPLS wird auf weitere Literatur verwiesen [Hus04].

3.4.3 Standards für Schicht 3/4

Die DetNet-Arbeitsgruppe definierte in IETF „Draft Packet Ordering Function“ das Konzept der Paketduplizierung und -eliminierung, um Hochverfügbarkeit für deterministische IP-basierte Netzwerke zu erreichen. IEEE 802.1CB, wie im vorherigen Abschnitt beschrieben, wird als potenzieller Mechanismus genannt. Es wird innerhalb der Bestrebungen kein weiterer Mechanismus eingeführt. IEEE 802.1CB ermöglicht jedoch die Verwendung von IP-Adressen als Kommunikationsstrom-Identikator, wodurch die Notwendigkeit der MAC-Adressen-basierten Eliminierung von Duplikaten entfällt.

Im Kontext des Routings existieren verschiedene Standards, die durch dynamische Redundanzmechanismen definiert sind. Diese Protokolle schaffen in der Regel Redundanz für einen einzelnen Hop durch die Einrichtung eines Backup-Gateways oder -Pfades. Der IETF-Standard Virtual Router Redundancy Protocol (VRRP) ermöglicht die Konfiguration mehrerer Backup-Router [Nad10]. Weitere proprietäre Standards wie das Hot Standby Redundancy Protocol (HSRP) von Cisco existieren, sind jedoch nicht Gegenstand dieser Arbeit [Li+98]. Dynamische Redundanzprotokolle sind nur für Anwendungen geeignet, die tolerant gegenüber Paketverlusten und Umschaltzeiten von 50 ms und mehr sind. Der Hello-Timer kann nicht unter bestimmte Schwellenwerte gesenkt werden, was eine untere Grenze für Umschaltzeiten darstellt.

Analog zu LACP auf Schicht 2 wird Equal-cost Multi-path (ECMP) für Lastverteilung verwendet und ermöglicht schnelles Umschalten im Falle eines einzelnen Pfadausfalls. Trotz seines Namens wird kein Routing von duplizierten Paketen auf mehreren Pfaden durchgeführt. Stattdessen kann schnelles Umschalten durch das Vordefinieren eines Backup-Pfades erreicht werden. Schließlich benötigt jeder Router neben einer virtuellen IP-Adresse eine feste IP-Adresse in jedem Subnetz, mit dem er verbunden sein soll. Dies kann besonders in Fällen mit einer knappen Anzahl von IP-Adressen und vielen kleineren Subnetzen eine Herausforderung darstellen.

iPRP stellt eine Implementierung von PRP auf Schicht 4 dar, welche das Versenden von Duplikaten über mehrere UDP-Ports realisiert [Pop+16]. Der Hauptvorteil dieser Lösung besteht darin, dass die Erkennung von Duplikaten durch MAC-Adressen entfällt. Stattdessen basiert die Erkennung auf IP-Adressen.

3.4.4 Weitere Redundanzlösungen für Kommunikationsnetzwerke

Nachdem die Verfügbarkeit einen zentralen Stellenwert von Infrastruktur darstellt, gibt es in verschiedenen Anwendungsbereichen weitere Mechanismen und Methoden zur Erreichung von Hochverfügbarkeit.

3.4.4.1 WAN-Kommunikation

Weitverkehrsnetzwerke (WAN) leiden häufig unter Paketverlusten und Unzuverlässigkeit aufgrund der hohen Anzahl an Hops, der zurückgelegten Strecke und dem Durchqueren mehrerer Verwaltungsdomänen verschiedener Entitäten. Um diese Herausforderungen zu bewältigen, unterstützen viele WAN-Router in der Industrie Paketduplizierungsschemata. Hierbei werden mehrere logische Tunnel eingerichtet, die idealerweise unterschiedliche physische Pfade durchqueren, um die Hochverfügbarkeit für fehlerhafte WAN-Verbindungen zu gewährleisten. Ähnlich wie bei den in Abschnitt 3.4.1 vorgestellten Schicht 2-Mechanismen wird eine Zyklusnummer eingefügt, um Duplikate am Zusammenführungspunkt zu identifizieren und zu verwerfen.

3.4.4.2 Software-defined Networking

SDN entkoppelt die Datenebene von der Kontrollebene, was die Flexibilität erhöht und komplexe Routenplanung ermöglicht. Es gibt eine Vielzahl an Implementierungen, die auf Technologien wie P4 und Openflow basieren [McK+08]. P4 wurde eingeführt, um Unabhängigkeit von der zugrunde liegenden Hardware zu ermöglichen [Bos+14]. Diese Lösungen bieten Programmierbarkeit und ermöglichen daher neue Schemata für Resilienz und Energieoptimierung.

Ein bemerkenswertes Beispiel ist die Nutzung von BFD im Openflow-basierten Konzept von van Adrichem et al., das Wiederherstellungszeiten im einstelligen Millisekundenbereich erreicht [vvK14]. Allerdings behandelt diese Arbeit keine Skalierbarkeitsprobleme, die sich aus der Berechnung von Routen in großflächigen Netzwerken ergeben.

3.4.4.3 Kabellose Kommunikation

Rauschende Kommunikationskanäle sind vor allem bei drahtlosen Verbindungen weit verbreitet. Daher wurden in diesem Bereich intensive Forschungsaktivitäten durchgeführt, um Jitter und Paketverluste durch Duplizierungsmechanismen zu reduzieren, insbesondere im OT-Bereich. Eine Vielzahl an Literatur ist im Kontext der Hochverfügbarkeit vorhanden [Aij19]. Hierbei können entweder zwei verschiedene Frequenzbänder oder zwei Funkgeräte verwendet werden, um eine Dual-Path-Kommunikation zu erreichen. Im Kontext von IEEE 802.11 wird Paketduplizierung verwendet, um Duplikate an zwei verschiedene Access Points zu senden [CSV16].

3.4.5 Zwischenfazit der hochverfügbaren Kommunikationsnetzwerke

Zusammenfassend ermöglichen PRP, HSR und IEEE 802.1CB Hochverfügbarkeit ohne Umschaltzeit. Allerdings befinden sich diese Standards auf Schicht 2 und basieren daher auf MAC-Adressen, was für eine IP-basierte Kommunikationsinfrastruktur nicht zielführend ist. Ansätze wie iPRP finden aufgrund mangelnder Aufmerksamkeit von Standardisierungsgremien keine breite Anwendung. Dynamische Redundanzmechanismen sind in der Regel auf höhere Umschaltzeiten beschränkt, wodurch sie für industrielle Applikationen häufig ungeeignet sind. SDN-basierte Mechanismen für großflächige Implementierungen fehlen aufgrund des hohen Rechenaufwands für die Berechnung korrekter Datenpfade.

Lastverteilung über mehrere Pfade wird von einer Reihe von Standards unterstützt, aber keiner der in einer umfassenden Umfrage vorgestellten Standards bietet eine Lastverteilung innerhalb eines Datenflusses [Li+16]. Typischerweise wird der Datenverkehr auf Basis einzelner Flüsse ausgeglichen, da die Kommunikationscharakteristika eine Lastverteilung innerhalb eines Flusses verhindern, beispielsweise die Asymmetrie von Paketen unter TCP/IP-Kommunikation.

3.5 Hochverfügbarkeit von echtzeitkritischen Applikationen

Dieser Abschnitt beschreibt Ansätze, Hochverfügbarkeit von echtzeitkritischen Applikationen auf verteilten Systemen zu erreichen. Neben der detaillierten Beleuchtung eines Standards der Cloudtechnologie stellt dieser Abschnitt verschiedene Konzepte der Literatur dar.

3.5.1 Remote Direct Memory Access

Die Technologie Remote Direct Memory Access (RDMA) ermöglicht einen Informationsaustausch zwischen zwei Kommunikationspartnern ohne Involvieren des Prozessors oder des Betriebssystems [Zha+17]. Hierbei wird der Hauptspeicher eines Hosts mit dem eines anderen synchronisiert. Die Nutzung von RDMA ist innerhalb von Rechenzentren weit verbreitet. Dies gilt allerdings nicht für die OT-Domäne, in welcher keine Anwendungen in der Literatur beschrieben werden. Dabei ermöglicht RDMA eine Datenübertragung deterministischer Weise mit niedrigen Latenzzeiten und gleichzeitig hohen Bandbreiten. Für eine ordnungsgemäßge Funktionsweise ist ein Kommunikationsnetzwerk ohne Datenverlust notwendig. Aus dieser Anforderung heraus entstanden zwei Ausprägungen dieser Technologie.

Infiniband (IB) stellt einen kabelgebundenen Standard dar, welcher nicht auf IEEE 802.3 basiert. Um diesen Standard nutzen zu können, sind spezielle Netzwerkhardware und -karten notwendig. Die jeweiligen Schichten eins bis vier des ISO/OSI-Referenzmodells sind in zwei Standardausführungen beschrieben [Inf21a; Inf21b]. Ein kreditbasiertes Stauvermeidungsmechanismus gewährleistet die verlustfreie Übertragung der Informationen [Rei+06]. Diese Mechanismen sind besonders in Rechenzentren von Bedeutung, in welchen hohe Durchsatzraten und geringe Latenzzeiten erforderlich sind. Eine Verwendung von Kreditpaketen stellt sicher, dass Telegramme ohne Verlust in die entgegengesetzte Richtung fließen können.

Hierdurch können die Netzwerkkonvergenz beschleunigt und die Pufferbelegung verringert werden [CHJ16]

Auf der anderen Seite nutzt RDMA over Converged Ethernet (RoCE) bestehende Ethernet-Netzwerke für die Paketübertragung und führte mit RoCE v2 Routing-Fähigkeiten ein, indem es sich auf UDP als zugrunde liegendes Transportprotokoll stützt. Nachdem dieser Standard mittlerweile ausschließlich verwendet wird, wird RoCE v2 im weiteren Verlauf dieser Arbeit als RoCE bezeichnet.

Werden Pakete im Zuge der RDMA-Kommunikation vertauscht, erfolgt auf Basis der IB Schicht 4-Mechanismen ein Verwerfen und erneute Übertragung der jeweiligen Pakete, was zu einer Reduzierung der Übertragungsleistung führt [Inf21a]. Allerdings existieren bereits Lösungen in ausgewählten Netzwerkkarten, die stattdessen die Pakete zwischenspeichern und somit kein Verwerfen von vertauschten Paketen erfolgt.

Sofern keine RoCE-fähigen Netzwerkkarten vorhanden sind, können die IB Schicht 4-Mechanismen auch in Software ausgeführt werden, welches allerdings im Vergleich zur Ausführung auf Hardware-optimierten Netzwerkkarten zu Performance-Einbußen führt.

In Abbildung 3.5 wird eine Übersicht der verschiedenen Möglichkeiten zur Nutzung von RDMA im Vergleich zum ISO/OSI-Referenzmodell gegeben.

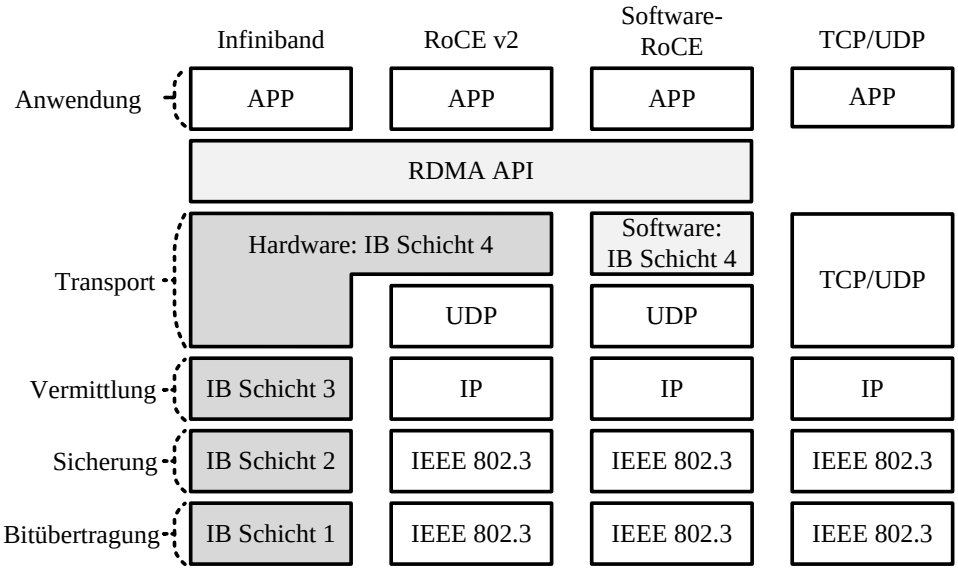


Abbildung 3.5: Infiniband vs. RoCE v2 vs. soft-RoCE vs. TCP/IP in Relation zum ISO/OSI-Schichtenmodell nach [KG23b]

Zur Erfüllung der verlustfreien Übertragung RDMA-basierter Kommunikation stellt IEEE 802.1Qbb eine verbreitete Lösung dar [Mit+18]. Die Nutzung von IEEE 802.1Qbb kann jedoch zu einem Deadlock des gesamten oder Teile des Kommunikationsnetzwerkes führen. Ein möglicher Lösungsweg ist die Nutzung von verbesserten RoCE-Netzwerkkarten, welches den Umgang mit Paketverlust modifiziert [Mit+18]. Weitere entwickelte Systeme zur Verhinderung von Paketverlust durch Überlast, im Englischen als Congestion Control bezeichnet, umfassen DCQCN, TIMELY und IRN [Mit+15; Mit+18; Zhu+15]. Unsicher-

heit in der Vorhersage der Bandbreite ist ursächlich für die erschwerte Optimierung von Überlastvermeidung des Netzwerkes und gleichzeitiger Maximierung des Durchsatzes und deterministischen Latenzzeiten [Zha+21].

3.5.2 Hochverfügbarkeitskonzepte von Applikationen

Klassische Verfügbarkeitskonzepte von Datenbanken sehen entweder eine aktiv-aktiv oder aktiv-passiv Konstellation von Instanzen vor. Diese wurden durch aktive Speicherreplizierung mittels RDMA erweitert [Zam+19].

Hochverfügbarkeit von Virtuelle Maschine (VM) ist Forschungsgegenstand verschiedener Arbeiten. Hierbei wird die Synchronisation in einigen Systemen wie Remus und dem FT Protocol innerhalb von Infrastrukturkomponenten durchgeführt, sodass eine Anpassung der Applikation nicht notwendig ist und die komplette VM mit Betriebssystem und Speichern gesichert wird [Cul+08; SNV10].

Im Kontext von Container-Technologie und Mikroservices werden die Nutzung eines verteilten Speichers und der damit interagierenden Protokollen wie DORADO sowie die von persistenten Speicher durch Speicherkontroller vorgeschlagen [Abd+19; Net+17]. Des Weiteren stellt Shimmy ein Kommunikationsschnittstelle für Mikroservices unter der Nutzung eines verteilten Speichers und RDMA dar [Abr+19].

3.5.3 Redundanzkonzepte heutiger SPS

Während die Notwendigkeit für Redundanzkonzepte vor allem durch die Virtualisierung und Konsolidierung auf Edge Cloud-Umgebungen motiviert wird, sind bereits heute redundante Ausführungen von SPS verfügbar. Diese werden beispielsweise in kritischen Prozessen wie der Kontrolle von Vakuumpumpen oder Dampfturbinen genutzt [Sie22].

Das generelle Konzept der verfügbaren Lösungen, beispielsweise der SPS-Hersteller Siemens, Rockwell Automation und CODESYS, ist in Abbildung 3.6 dargestellt. Zustände werden zwischen einer aktiven und einer Backup-SPS zyklisch synchronisiert. Die Größe des zu synchronisierenden Zustandes wird nicht angegeben. Die Umschaltzeiten bewegen sich im Bereich von 50 ms [Sie22].

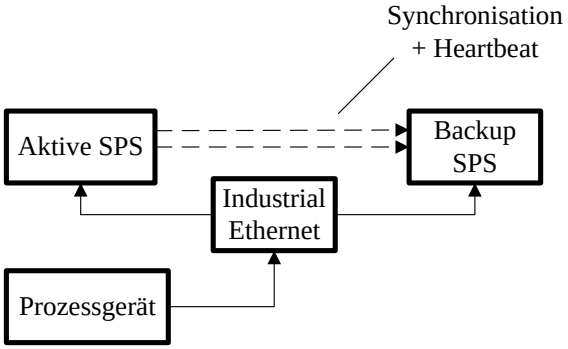


Abbildung 3.6: Verallgemeinertes Konzept von verfügbaren Redundanzlösungen von SPS nach [KG23b]

3.5.4 Zwischenfazit der hochverfügbaren Applikationen

RDMA erlaubt die deterministische Übertragung und Synchronisation von Zuständen zwischen zweier Applikationen. Dies wird erreicht, indem Prozessor und Betriebssystem innerhalb des Prozesses nicht involviert sind. Anwendungen der RDMA-Technologie im OT-Umfeld lassen sich in der Literatur nicht finden.

Die Beschreibung aktueller Hochverfügbarkeitskonzepte für SPS sowie Applikationen auf verteilten Systemen lässt die Frage offen, ob heutige Konzepte die Anforderungen auch auf einer Edge Cloud erfüllen und ob eine direkte Übertragung auf ein verteiltes System möglich ist.

Weiterhin stellt die Überlastkontrolle von RDMA-basierten Netzwerken einen aktiven Forschungszweig dar, da vorhandener Paketverlust die Performance der RDMA-Kommunikation stark einschränkt.

3.6 IT/OT-Security

Aufgrund der steigenden Wichtigkeit von Sicherheit innerhalb der Automatisierung sind die Veröffentlichungen in diesem Bereich zahlreich und vielfältig. Zunächst werden in diesem Abschnitt verschiedene IT-Security Design-Prinzipien eingeführt, die anschließend im Kontext der IT/OT-Security-Konzepten in der Literatur Anwendung finden. Zudem wird ein Überblick über Methoden zur Evaluierung von IT/OT-Security-Konzepten gegeben.

3.6.1 Zero Trust und NAC

Zero Trust ist ein IT-Securitymodell, welches die umfassende Authentifizierung und Autorisierung von Kommunikationsteilnehmern sowie den Ansatz der geringsten Privilegien erfordert. Somit werden ausgewählten Teilnehmern eine Rolle zugeteilt, die für die Ausführung notwendige Rechte besitzt. Bei einer konsequenten Anwendung des Prinzips gilt dies auch für innere Netzwerke hinter Firewalls wie ein mögliches IT/OT-konvergiertes Kommunikationsnetzwerk. Die Rollenvergabe kann auf Basis der Netzwerkzugangskontrolle, engl. network access control (NAC) erfolgen. Hier werden jegliche Teilnehmer zunächst authentifiziert, bevor sie innerhalb des Netzwerkes kommunizieren können [Kin+10]. Beide Konzepte, Zero Trust und NAC, verfolgen eine andere Annahme als Security-Architekturen basierend auf Abschottung. Firewall-basierte Konzepte erwarten, dass innerhalb des geschützten Bereiches ausschließlich Kommunikationsteilnehmer vorhanden sind, denen vertraut werden kann. Trotz verschiedener Annahmen lassen sich die jeweiligen Konzepte miteinander kombinieren, um somit dem Defense in Depth (DiD)-Gedanken zu folgen.

Ward und Beyer erkannten das Problem erfolgreicher Angreifer innerhalb eines Netzwerkes, das nur durch Firewalls nach außen hin geschützt ist. Das hieraus entwickelte System, BeyondCorp, folgt konsequent dem Zero-Trust-Paradigma und eliminiert somit die Notwendigkeit eines Intranets [WB14]. BeyondProd verfolgt den identischen Ansatz und erweitert die Anwendung auf eine Cloud-Umgebung durch die Nutzung eines Mesh-Netzwerks. Hierbei werden eine Vielzahl an Designentscheidungen getroffen, beispielsweise der Anwendung von

Sicherheitsmechanismen auf der Infrastrukturebene anstatt auf Applikationsseite sowie das Konzept von binärer Autorisierung [Bak20]. Die Autoren beider Systeme erkennen jedoch an, dass nicht jeder Dienst und Client ohne Hürden migriert werden kann und bestimmte Anforderungen erfüllt sein müssen, um die vorgeschlagene Methodik anzuwenden.

3.6.2 Defense in Depth

Anstatt auf nur einen Mechanismus für die Abwehr gegen spezifische Bedrohungen zu setzen, sieht der DiD-Ansatz analog zu Redundanzkonzepten absichtlich mehrere Mechanismen des Schutzes vor. Dies erhöht die Wahrscheinlichkeit für die erfolgreiche Identifikation und Abwehr von Angreifern. Aufgrund der fortschreitenden Konvergenz von IT und OT, und der damit einhergehenden Erhöhung an Angriffen in der Vielfalt als auch der Anzahl, bietet dies eine Möglichkeit, dieser Herausforderung zu begegnen. Die jeweiligen Mechanismen greifen hierzu für gewöhnlich unabhängig voneinander. Diese können grob in die Schichten der physikalischen Security, Netzwerk-, Host- und Applikations-Security eingeteilt werden [Nel16].

Firewalls bieten ein effektives Mittel, um ungewünschte Kommunikation einzuschränken. Weiterhin können mehrere Firewalls geschichtet werden, sowohl physikalisch als auch in virtueller Ausführung, um unterschiedliche Regelsätze und Granularitäten abzubilden. Um im Falle eines Angriffs die Angriffsfläche zu minimieren wurden Segmentierungsmechanismen geschaffen.

3.6.3 Segmentierung von Kommunikationsnetzwerken

Um die Kommunikation zwischen Teilnehmern eines physikalischen Netzwerkes einschränken zu können, werden Segmentierungsmechanismen verwendet. Hierbei gibt es eine Vielzahl an möglichen Funktionen, die für gewöhnlich auf unterschiedlichen Ebenen des ISO/OSI-Schichtenmodells agieren.

- VLAN: Unter der Nutzung von VLAN-Tags können Netzwerke auf Schicht 2 logisch voneinander getrennt werden. Ermöglicht wird dies durch die Vergabe unterschiedlicher VID.

- Sicherheitsgruppe: VXLAN-basierte Kommunikation ermöglicht die Nutzung von GBP, die einen 16 Bit-Identifikator im VXLAN-Header darstellen [SK16]. Hierbei werden Kommunikationspartnern einer SG zugewiesen. Diese können in Access Control List (ACL) verwendet werden, um Kommunikationen zwischen SG zu erlauben oder verhindern.

- Virtual Routing Function (VRF): Die Nutzung von VRF erlaubt die Separierung von Routing Tabellen auf Netzwerkgeräten. Somit ist keine Kommunikation zwischen verschiedenen VRF aufgrund fehlender Informationen möglich. In diesem Kontext wird auch der Begriff der Zone verwendet.

- Separierung der Kontrollebene: Im Kontext des SDN-Konstruktes kann die Separierung von Daten- und Kontrollebene genutzt werden, um ausschließlich Informationen zwischen gewünschten beteiligten Netzwerkgeräten auszutauschen. Ein proprietäres Beispiel stellt hierfür der Mechanismus von Fabric-Zones dar [Cis23].

- Air Gap: Sollte jegliche Kommunikation mit anderen Netzwerken unterbunden werden, kann eine physikalische Trennung notwendig sein. Dies wird als Air Gap bezeichnet.

Die verschiedenen Ebenen der Segmentierung erfüllen die Anforderungen des DiD-Ansatz innerhalb der Segmentierung. Zusammengefasst folgen die jeweiligen Segmentierungsmöglichkeiten einem Zonen- und Übergangsmodell, welches sich unter anderem nach IEC 62443 richtet. Hierbei werden Zonenübergänge gesondert gesichert, um eine laterale Ausbreitung von Angreifern innerhalb eines Kommunikationsnetzwerkes zu verhindern. Die Übergänge zwischen Segmenten können auf verschiedene Weisen geprüft werden.

Das Design der Segmentierung von Kommunikationsnetzwerken ist für gewöhnlich ad hoc. Sung et al. bieten einen systematischen VLAN-Designansatz zur Reduzierung des Datenverkehrs und zur systematischen Platzierung von ACL, um die gewünschten Sicherheitsanforderungen zu erfüllen [Sun+08]. Im Kontext der industriellen Kommunikation wurde zuvor eine Mikrosegmentierung mit automatischer Segmentgenerierung basierend auf maschinellem Lernen angewendet, jedoch nicht auf skalierte IT/OT-konvergierte Netzwerke [APP21].

3.6.4 Intrusion Detection System

Eine Möglichkeit, Auffälligkeiten zu identifizieren, ist ein Intrusion Detection System (IDS). Es ist in der Lage, Anomalien auf Basis von Paketinformationen und Logs zu erkennen. Diese werden auf Basis von Signaturen und maschinellem Lernen erkannt. Anschließend erfolgt eine Meldung der identifizierten Aktivität, beispielsweise an ein Computer Emergency Response Team (CERT). Das Kommunikationsnetzwerk wurde bereits als optimale Stelle für die Erkennung von Angriffen auf Prozessgeräte durch IDS identifiziert [TH18]. Hier wurde eine Vielzahl an Erkennungsmechanismen auf Basis maschinellem Lernens für Anwendungsfälle innerhalb der IT/OT-Konvergenz evaluiert. Zolanvari et al. bieten eine Vielzahl an Anwendungsfällen für IDS sowie eine Risikobewertungsmatrix für Schwachstellen für IIoT-Umgebungen [Zol+19].

3.6.5 Firewall

Die Nutzung von Firewalls stellt auch weiterhin einen zentralen Bestandteil von IT-Security-Konzepten dar. Sie wurden in den vergangenen Jahren zunehmend mit neuen Funktionen wie einem Intrusion Prevention System (IPS) erweitert, welches im Kontrast zum IDS verdächtige Aktivitäten unterbinden kann, indem Kommunikationen aktiv geblockt werden. Für gewöhnlich werden auf Basis der Informationen im Header Rückschlüsse über die Validität der Kommunikation gezogen. Durch die Erweiterung mittels Deep Packet Inspection (DPI)

können auch Daten innerhalb der Anwendungsebene analysiert werden, um Bewertungen durchzuführen. Abschließend können Web Application Firewall (WAF) genutzt werden, um Kommunikationsteilnehmer vor einer Vielzahl an Angriffen innerhalb der Anwendungsebene zu schützen.

3.6.6 Verschlüsselung

Die Verschlüsselung von Kommunikation kann verschiedene Gründe haben. Sie schützt die Vertraulichkeit der Informationen und kann die Integrität bewahren. Mechanismen greifen erneut vergleichbar mit den Segmentierungsmöglichkeiten auf verschiedenen ISO/OSI-Schichten:

- Physical Security (PhySec): Maßnahmen auf Basis von Schicht 1 werden innerhalb der Literatur als PhySec bezeichnet. Sie reduzieren den Einfluss von Verschlüsselung auf Latenzzeiten, sind jedoch nicht über mehrere physikalische Medien anwendbar. Zudem existieren noch keine definierten Standards [LAS20; Tia+23].
- Media Access Control Security (MACsec): MACsec beschreibt einen verbreiteten Standard zur Verschlüsselung. Nachdem es sich um einen Schicht 2-Mechanismus handelt, ist die Funktionalität Physik-agnostisch. Dennoch können Hardware-beschleunigter Datenverkehr mit einem geringen Latenzzuwachs ver- und entschlüsselt werden [IEE18].
- Internet Protocol Security (IPsec): Ermöglicht die Verschlüsselung auf IP-Basis. Dies ermöglicht die Nutzung des Standards für Fernzugriffsszenarien.

Die Literatur bietet eine Vielzahl an Verschlüsselungsmethoden. Verschiedene Latenzerhöhungen von Verschlüsselungsmethoden wurden aufgrund der Notwendigkeit einer Kapselung des IE-Verkehrs über IP-basierte Netzwerke verglichen [LKS19]. Nachdem innerhalb des zur Verfügung stehenden Lösungsraumes mehrere Eigenschaften erfüllt werden müssen, bietet dies eine Möglichkeit, Determinismus und die Konsistenz des Steuerungs-Datenverkehrs sicherzustellen.

Verschiedene Konzepte im Bereich der Authentifizierung und sicheren Kommunikation existieren für das Internet of Things (IoT), beispielsweise basierend auf DTLS, oder Datenverschlüsselung mittels JEDI [Kot+13; Kum+19]. Die Konzepte sind jedoch im Allgemeinen nicht auf die IT/OT-Konvergenz anwendbar aufgrund der Brownfield-Anforderung und der damit zusammenhängenden fehlenden Reprogrammierbarkeit von Feldgeräten. Weiterhin ist der Determinismus kein notwendiges Kriterium für Kommunikationsnetzwerke im IoT-Bereich.

3.6.7 Validierung von Security-Konzepten

Es existieren eine Vielzahl an Methoden, um das Security Level (SL) einer Security-Architektur ohne experimentelle Validierung zu ermitteln. Neben der Analyse anhand von bekannten Angriffsvektoren werden zwei Ansätze häufig verwendet, die im Folgenden vorgestellt werden.

3.6.7.1 IEC 62443-3-3

Die Norm IEC 62443-3-3 erlaubt eine methodische Analyse von entwickelten IT/OT-Security-Konzepten auf Basis von einer Reihe von definierten Anforderungen [ID20]. Die Anwendungsdomäne beschränkt sich vor allem auf das OT-Umfeld mit Automatisierungs- und Steuerungsgeräten. Hierbei können bis zu vier verschiedene SL erreicht werden, die jeweils verschiedene Stufen des Schutzes erfüllen müssen. Die Anforderungen sind in einer Baumstruktur organisiert, in der sieben grundlegende Anforderungen, Foundational Requirements (FR), definiert werden, die jeweils verschiedene System Requirement (SR) und Requirement Enhancements (RE) enthalten.

3.6.7.2 Cyber Kill Chain

Die Cyber Kill Chain (CKC) stellt eine praxisnahe Methode dar, um Angriffsszenarien mit einem Fokus auf das Eindringen von Angreifern für ein gegebenes IT-Security-Konzept zu bewerten. Die Methode wurde ursprünglich von Lockheed Martin zur militärischen Abwehr entwickelt [Loc21]. Hierbei werden sequentiell die unterschiedlichen Stadien eines Cyberangriffes analysisert und Gegenmaßnahmen identifiziert, die das jeweilige Konzept vorsieht. Folgend wird die Abfolge eines Angriffes nach der CKC näher beleuchtet [Loc21]:

- Aufklärung: Sammlung von Informationen über ein Ziel
- Bewaffnung: Vorbereitung des Angriffes auf Basis der gewonnen Erkenntnisse
- Lieferung: Übertragung der Schadsoftware oder Vergleichbares
- Ausführung: Durchführung des vorbereiteten Angriffes
- Installation: Installation des Schadsoftware
- Steuerung & Kontrolle: Kommunikationsaufbau mit dem kompromittierten Host
- Aktionen mit Auswirkungen auf das Ziel: Erreichung des gewünschten Ergebnisses

Obwohl die traditionelle CKC weiterhin weitreichende Anwendung erfährt, wurden ähnliche Konzepte entwickelt, um spezifische Schwachpunkte des ursprünglichen Ansatzes zu eliminieren. Häufig wird ein zu starker Fokus der CKC auf Schadsoftware und Firewalls betont. Diese und weitere Limitierungen wurden mit der Entwicklung der Unified CKC aufgehoben [Pv17]. Weiterhin hat bereits eine Adoption speziell für industrielle Steuerungstechnik stattgefunden, wobei weite Teile der ursprünglichen CKC sowie das generelle Konzept identisch sind [AL15]. Generell können Cyberattacken eher unterbrochen werden, wenn die jeweiligen Schutzmaßnahmen schnell aktiv werden [YR15].

Ehrlich et al. stellen relevante Sicherheitsstandards und Bewertungsmethoden für die IT/OT-Konvergenz vor [M E+19]. Insbesondere wird die zukünftige Anpassungsfähigkeit von Fertigungssystemen und der daraus resultierende Bedarf an einem flexiblen Netzwerk hervorgehoben. Flexibilität und Anpassungsfähigkeit des Netzwerks sind Kernmerkmale des

SDN. Dieses findet im Bereich der IT/OT-Security Anwendung, beispielsweise im Schutz gegen Denial of Service (DoS)- und Distributed Denial of Service (DDoS)-Angriffe und der Entfernung von industriellen Firewalls zugunsten von Software-definierten Mechanismen im Netzwerk [Che+17; Fos+21].

Mit Hilfe von ThreatGet ist es möglich, die erfolgreiche Anwendung von Sicherheitsmechanismen auf vernetzte Systeme zu überprüfen [SSM22]. Hierbei wird ein IIoT-System basierend auf IEC 62443 validiert. Allerdings werden keine realistischen skalierten Implementierungen berücksichtigt.

3.6.8 Konzepte und Systeme der Literatur

Verschiedene Systeme und Konzepte wurden entwickelt, um den steigenden Sicherheitsanforderungen zu begegnen. In diesem Abschnitt wird ein verstärkter Fokus auf Konzepte und Architekturen gelegt, die auf ein IT/OT-konvergiertes Kommunikationsnetzwerk anwendbar sind.

Anhand der Virtualisierung und Konsolidierung von SPS wurde ein Security-Konzept für zeitkritische Kommunikationsnetzwerke entwickelt [Kob+18]. Unter genauerer Betrachtung werden jedoch keine Mechanismen zur Abwehr von Angriffen benannt. Stattdessen folgt es dem klassischen Konzept der Abschottung und beschreibt die Nutzung von TSN und DetNet.

Die Nutzung von Redundanzprotokollen wie PRP wurde bereits im Kontext des Edge-Computing diskutiert und bewertet [KW21]. Hierbei wurde die Notwendigkeit für Hochverfügbare Kommunikationsnetzwerke in realen Anwendungen hervorgehoben und mittels TSN die Echtzeitfähigkeit des Netzwerkes bis hinein in eine Edge Cloud garantiert.

Mosteiro-Sanchez et al. geben einen detaillierten Überblick über die Unterschiede von IT- und OT-Systemen sowie das DiD-Prinzip, welches hier Anwendung findet [Mos+20]. Weiterhin werden eine Vielzahl an Systemen zur Erreichung einer Ende-zu-Ende Verschlüsselung beschrieben. Allerdings wurden hier keine Virtualisierungsumgebungen berücksichtigt.

Auf den ersten Blick scheinen Blockchain-basierte Implementierungen aufgrund ihrer sicheren Datenstruktur eine natürliche Wahl für Security-Konzepte zu sein. Die Analyse von Alladi et al. zeigt jedoch einen Mangel an tatsächlich implementierten Anwendungsfällen und mehrere offene Fragen hinsichtlich Skalierbarkeit, Einführung zusätzlicher Bedrohungsvektoren und mangelnder Effizienz in Bezug auf Energie und Kosten [All+19].

Auf Basis einer weitreichenden Literaturanalyse konnte kein Konzept identifiziert werden, welches die Determinismus-Anforderungen mit den Security-Anforderungen eines großen IP-basierten Netzwerkes kombiniert [Tan+20].

Ein vielversprechender Ansatz zur Erfüllung der Brownfield-Anforderung ist der Einsatz von Edge-Gateways. Diese bieten einen zentralen Punkt für die Datenaggregation und -verarbeitung in industriellen Umgebungen. Darüber hinaus können Edge-Gateways die IT/OT-Sicherheitseigenschaften der vorhandenen Implementierungen verbessern, indem sie als Schnittstelle zwischen IT- und OT-Systemen fungieren [Cra+20; LMZ16]. Allerdings führt dieses Konzept für gewöhnlich zur Einführung weiterer SPOF, welche die Verfügbarkeit

der Prozesse reduzieren [FHH23].

3.6.9 Zwischenfazit der IT/OT-Security

Die bereits entwickelten Konzepte der Literatur bieten einen umfangreichen Satz an Methoden und Maßnahmen zur Erreichung und Bewertung von sicheren Kommunikationsnetzwerken. Allerdings werden operationale Gegebenheiten innerhalb der OT-Domäne bei der Umsetzung der vorgestellten Konzepte wenig Beachtung geschenkt. Dies stellt allerdings einen zentralen Bestandteil dar, damit entwickelte Konzepte adoptiert werden.

Des Weiteren werden die Auswirkungen der einzelnen Mechanismen untereinander nicht beleuchtet. Häufig werden ausschließlich einzelne Mechanismen untersucht und für einige wenige Szenarien evaluiert. Zuletzt fehlt auch eine umfassende Betrachtung eines Security-Konzeptes für IT/OT-konvergierte Kommunikationsnetzwerke mit Edge Cloud-Infrastruktur.

3.7 Virtualisierung in der industriellen Automatisierung

Die klassische Automatisierungspyramide stellt eine Herausforderung für die Integration moderner Technologien wie der Virtualisierung dar. Um diese Herausforderungen zu bewältigen und die IT/OT-Konvergenz zu erleichtern, wurden verschiedene Architektur-Konzepte vorgeschlagen.

Ein bedeutendes Beispiel stellt die Namur Open Architecture dar, welche die strikte Trennung der Hierarchien durchbricht, indem sie einen zweiten Kommunikationskanal einführt. Dieser Kanal dient der Übertragung relevanter Daten für Überwachungs- und Optimierungszwecke [Kle+17]. Ein weiteres wichtiges Konzept zur Modularisierung ist das Module Type Package (MTP), das in VDI/VDE/NAMUR 2658 standardisiert ist. MTP bietet Flexibilität für Prozesse durch die Nutzung offener Schnittstellen und herstellerunabhängiger Mechanismen [Koc+23].

Chen et al. betonen in ihrer vorgeschlagenen Architektur die Bedeutung der Datenverarbeitung in der Nähe der Entstehung [Che+18]. Edge Cloud-Infrastrukturen wurden bereits mehrfach vorgeschlagen, um die Effizienz und Flexibilität zu erhöhen [Cha+21; Rai+18; Sch+23]. Erste Versuche in Richtung einer Referenzarchitektur für industrielles Edge-Computing wurden ebenfalls unternommen [WG20]. Trotz dieser Fortschritte bietet keine der bestehenden Architekturen einen ganzheitlichen Blick auf die Netzwerk- und Virtualisierungsinfrastruktur.

Auch die Nutzung von vSPS wurde bereits vorgeschlagen. Hierbei wurden die jeweiligen Vorteile benannt sowie Herausforderungen in bestimmten Anwendungsszenarien beschrieben [ADM16; CSM16].

3.8 Bewertung der Erkenntnisse

Dieses Kapitel hat den Stand der Wissenschaft von deterministischen Kommunikationsnetzwerken für die IT/OT-Konvergenz abgebildet. Hierbei werden ausgehend von einer Einführung in die Kommunikationstechnik, die für die Konvergenz relevanten Bereiche Echtzeitfähigkeit und Determinismus, Hochverfügbarkeit, und IT/OT-Security sequentiell beleuchtet. Zudem wird eine Übersicht über die Nutzung von verteilten Systemen in der industriellen Fertigung gegeben.

Es wird deutlich, dass keines der vorgestellten Architekturkonzepte alle notwendigen Anforderungen an die Steuerungs- und Kommunikationstechnik für die IT/OT-Konvergenz berücksichtigt und erfüllt. Des Weiteren ist die fehlende Skalierbarkeit vieler Konzepte zu nennen, die ausschließlich in kleinen Bebauungen Anwendung finden können.

4 Architekturkonzept zur Erreichung der IT/OT-Konvergenz

Kapitel 4 stellt einen Überblick über die Methodik der Entwicklung sowie das vorgeschlagene Architekturkonzept zur Erreichung der IT/OT-Konvergenz dar. Hierzu werden anforderungsbasiert Lösungsbausteine entwickelt, welche die Zielarchitektur und damit Edge Cloud-basierte Automatisierung ermöglichen.

4.1 Methodik

In den vorherigen Kapiteln wurde die Notwendigkeit für die Entwicklung eines neuartigen Architekturkonzeptes für die IT/OT-Konvergenz festgestellt. Dieser Abschnitt beschreibt die Entwicklungsmethodik, nach der das Konzept entstanden ist. Aufgrund der Heterogenität und Komplexität der Automatisierungstechnik und des vielfältigen Lösungsraumes der IT ist eine Methodik notwendig, damit die Konzepterstellung eine weitreichende Anzahl an Rahmenbedingungen erfüllen kann.

Zunächst wird auf Grundlage der Problembeschreibung ein mögliches Gesamtkonzept entwickelt, welches die in Kapitel 2 beschriebenen Anforderungen erfüllt und den nächsten Schritt im Wandel der Automatisierung darstellen könnte. Das Konzept bedient sich hierbei einigen vergleichbaren Entwicklungen und Fortschritten der IT-Domäne, die teilweise für die Automatisierung adaptiert werden können. Die Entwicklung des Konzeptes zielt hierbei auf die Anwendung in einem industriellen Umfeld mit vorhandenen oder geplanten Produktionssystemen ab.

Daraufhin erfolgt eine Detailbetrachtung der daraus resultierenden Anforderungen an das Kommunikationsnetzwerk. Hierbei ist die Zerlegung des Problems in kleinere Einheiten essenziell, um die Problemstellung verständlich und beherrschbar zu machen. Daraus ergibt sich eine Aufteilung in sechs Anforderungen, welche unter anderem auch die in Abschnitt 2.4 vorgestellten Forschungsfragen einschließen.

Danach werden die einzelnen Lösungsbausteine des Architekturkonzepts entwickelt. Es ist erwähnenswert, dass der Entwicklungsprozess iterativ und inkrementell gestaltet wird, um die notwendige Flexibiltät für eine Reaktion auf zuvor unbekannte Anforderungen zu ermöglichen. Dies wird unter anderem durch eine Bevorzugung softwaregetriebener Lösungsbausteine erreicht, die eine Rekonfiguration und Adaption erlauben. Die Bewertung der verschiedenen Lösungen erfolgt unter Betrachtung der für einen weitflächigen Einsatz der vorgeschlagenen Architektur notwendigen Eigenschaften. Diese enthalten nach Schmied die folgende Gesichtspunkte [Sch23]:

- Verständlichkeit
- Validierung

- Integration von Standards
- Skalierbarkeit
- Modularität
- Technologie-Neutralität
- Adaptivität

Hierbei sind besonders die Validierung mittels der repräsentativen Versuchsaufbauten und die Integration von Standards hervorzuheben, die grundlegend für eine Adoption des entwickelten Architekturkonzeptes sind. Weiterhin wird ein hoher Wert auf Verständlichkeit gelegt, da aufgrund der Anwendungsdomäne die Vermittlung von Anforderungen an neue Produkte sowie die Beherrschbarkeit der operativen Tätigkeit gewährleistet sein muss.

4.2 Konzeptübersicht

Dieser Abschnitt führt in die anvisierte Edge Cloud-basierte Kommunikationsarchitektur ein. Hierbei wird auf Grundlage der Entwicklungen in der Automatisierungstechnik und der Informationstechnik ein IT/OT-konvergiertes Netzwerkkonzept vorgestellt, welches die Virtualisierung von zuvor Hardware-gebundenen Applikationen und damit auch deren Konsolidierung ermöglicht.

Wenn die Entwicklung der IT in den vergangenen Jahrzehnten betrachtet wird, kann eine starke Bewegung hin zur Virtualisierung und Konsolidierung von Applikation in verteilten Systemen beobachtet werden. Sowohl die wissenschaftliche als auch die technische Basis hierfür ist somit gegeben. Dies steht jedoch im Widerspruch zur Entwicklung der industriellen Steuerungstechnik, die wie in Kapitel 2.2 beschrieben seit Jahrzehnten weitestgehend konzeptionell unverändert ist. Bereitstellungen von Applikationen innerhalb der OT-Domäne folgen weiterhin der Funktion auf Box-Prinzip: Sofern der Shopfloor durch neue Applikationen erweitert werden soll, wird parallel auch eine physikalische Box wie ein IPC zur Ressourcenbereitstellung hinzugefügt. Die immer weiter ansteigende Anzahl an Applikationen und damit auch an IPC erschwert die operative Handhabung, die Absicherung hinsichtlich IT-Security und die Verfügbarkeit von Anlagen durch hinzugefügte SPOF.

Aufgrund der notwendigen Steigerung der Flexibilität und Betreibbarkeit dieser Deployments wird deshalb eine weitere Instanz, eine Edge Cloud, innerhalb des anvisierten Architekturkonzeptes vorgesehen. Edge Clouds stellen eine Infrastrukturkomponente dar, auf der die für Applikationen notwendigen Hardwareressourcen nach dem Vorbild der Virtualisierung bereitgestellt werden. Dabei befinden sich Edge Clouds im Gegensatz zu klassischen Cloud-Infrastrukturen näher an den physikalischen Geräten, sodass Daten geringere Wege zurücklegen müssen und diese Komponente somit optimal für kritische und echtzeitrelevante Applikationen geeignet ist. Logisch gesehen ist es empfehlenswert, aufgrund von Determinismus und Verfügbarkeitsbestrebungen keine Firewalls zwischen Edge Clouds und deren

Clients zu platzieren. Stattdessen bietet es sich hier an, das System zu härten und die Aspekte der IT/OT-Security mittels Funktionen innerhalb des Netzwerkes abzubilden.

Das Hinzufügen einer konsolidierten Edge Cloud-Umgebung ist in der aktuellen Kommunikationsarchitektur nicht zielführend, vor allem aufgrund der vorhandenen Nord/Süd-Segmentierung des Netzwerkes durch die hierarchische Strukturierung der Automatisierungsdomäne und die damit verbundene Trennung zwischen IT und OT. Die hier entwickelte Kommunikationsarchitektur denkt Kommunikationsschema neu und führt eine Edge Cloud als neue Ressource ein. Abbildung 4.1 stellt das neuartige Konzept dar und wird im Folgenden näher betrachtet.

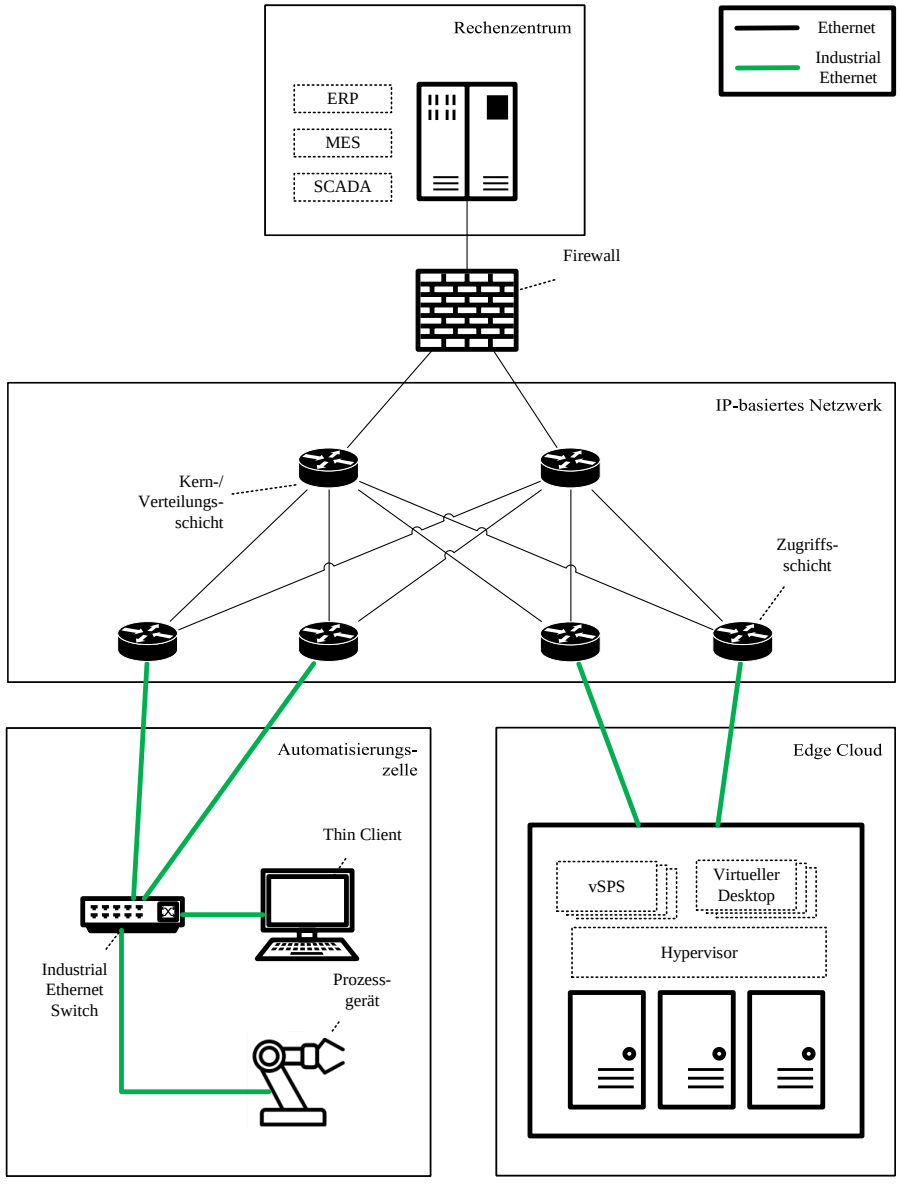


Abbildung 4.1: Edge Cloud-basierte Automatisierung mit Echtzeitapplikation nach [KMG22].

Physikalische Prozessgeräte, die für die automatisierten Prozesse notwendig bleiben, befinden sich weiterhin innerhalb der Automatisierungsebene und sind mit einem IE-Switch

verbunden. Thin Clients stellen in Kombination mit weiteren Peripherie-Geräten wie Tastaturen, Maus oder Scanner, die Möglichkeit zur Administration von Prozessen und Anwendungen sowie der Darstellung von Inhalten im Shopfloor dar. Das zugehörige Gegenstück ist eine Virtuelle Maschine, Virtueller Desktop, Container oder vergleichbare andere Infrastrukturkomponenten auf der Edge Cloud, zu der eine Remote-Verbindung hergestellt oder ein Service wie die Anzeige einer Webseite konsumiert wird. Abschließend sind auch weitere Applikationen wie SPS virtualisiert auf einer Edge Cloud, sodass die Anzahl an Hardwareressourcen im Shopfloor stark reduziert wird.

Die Applikationen befinden sich gebündelt auf einer oder mehreren Edge Cloud Infrastrukturen, welche die neue Entität dieses Architekturkonzeptes darstellt. Auf dieser werden jegliche Applikationen, die sich zuvor noch auf physikalischen Hardware-Boxen und IPC befunden haben, virtualisiert und konsolidiert betrieben. Hierunter fallen vSPS, Virtuelle Desktops, die beispielsweise HMI und Projektierungssoftware enthalten, als auch KI-Inferenzmaschinen. Ein Hypervisor ermöglicht es, mehrere Server zu einem verteilten System zu verbinden und Applikationen über physikalische Grenzen hinweg flexibel zu verteilen und zu skalieren. Durch die Verlagerung von IPC und anderen physikalischen Boxen auf ein verteiltes System entstehen neuartige Anforderungen an das übergelagerte IP-basierte Netzwerk zur Unterstützung der Konsolidierung und Effizienzsteigerungen.

Das IP-basierte Netzwerk verbindet sämtliche Entitäten miteinander und ermöglicht somit die Kommunikation untereinander, wodurch insbesondere auch die Schlüsselrolle des IP-basierten Netzwerks im Zentrum der Architektur deutlich wird. Echtzeitkommunikation, beispielsweise basierend auf IE-Standards wie PROFINET und EtherNet/IP, muss aufgrund der Auslagerung der Applikationen aus Automatisierungszellen über das IP-basierte Netzwerk ermöglicht werden. Zudem gewinnen in dem Vorgang auch die Verfügbarkeit des Netzwerks und die IT/OT-Security an noch höherer Bedeutung. Firewalls zwischen Automatisierungszellen und IP-basierten Netzwerken sowie jegliche weitere Gateways werden entfernt, um die Echtzeitfähigkeit und die Operativität zu verbessern.

Abschließend enthält ein Rechenzentrum, entweder eine private oder publike Instanz, die weiteren produktionsrelevanten Services, welche in diesem Kontext nach der klassischen Automatisierungspyramide die übergelagerten Systeme darstellen. Darunter fallen unter anderem das SCADA und MES wie auch ERP und Datenanalysesysteme. Nachdem Rechenzentren häufig besondere Anforderungen an IT-Security auferlegt werden, steht vereinfacht hierfür eine Firewall für die Segmentierung der Nord/Süd-Kommunikation. Diese kann durch weitere WAN-Strecken, mehrere Routing-Domänen, und verschiedene Firewall-Instanzen entfernt sein. Dies soll unter anderem auch verdeutlichen, dass das Auslagern der zuvor im Shopfloor befindlichen Systeme in eine klassische Rechenzentrumsumgebung typischerweise nicht zielführend ist.

4.3 Anforderungen

Das neuartige Konzept stellt einige Anforderungen an das IT/OT-konvergierte Netzwerk. Diese wurden in verschiedener Literatur erarbeitet und konkretisiert [KG23a; KMG22]. Hauptverantwortlich für die neuen Anforderungen ist die Verlagerung von Applikationen in eine Edge Cloud, sodass Kommunikationsflüsse, die sich zuvor ausschließlich in Automatisierungsnetzwerken befunden haben, nun auch im IP-basierten Netzwerk vorzufinden sind. Die Anforderungen werden im Folgenden vorgestellt.

4.3.1 Industrial Ethernet über IP

Innerhalb der Automatisierungsdomäne werden, wie in Abschnitt 2.3 beschrieben, vor allem IE-Protokolle für echtzeitkritische und Safety-relevante Applikationen verwendet. Den ersten Schritt zur Nutzung dieser Standards in herkömmlichen IT-Netzwerken wurde bereits mit der Einführung von IE getätigt. Nachdem IT-Netzwerke typischerweise IP-basiert sind, muss die Kommunikation für eine skalierbare Architektur Routing-fähig sein. Dies ist jedoch nicht bei allen IE-Standards und unterstützenden Applikationen der Fall. Kommunikation erfolgt teilweise auch notwendigerweise in der zweiten ISO/OSI-Schicht, beispielsweise bei der Zuweisung von Stationsnamen und Echtzeitkommunikation in PROFINET und der Nachbarschaftserkennung bei EtherNet/IP. Hierbei ist es essentiell, dass bei einer Migration zu virtualisierten Applikationen der Rekonfigurationsaufwand gering gehalten wird, um die wichtige Brownfield-Adaption des Konzepts zu ermöglichen. Durch die Verschiebung von Applikationen aus dem IE-basierten Netzwerk, vor allem vSPS und Konfigurations-/ und Parametrierungsprogramme, in eine Edge Cloud hinter einem IP-basierten Netzwerk müssen demnach in skalierter Weise Kommunikationswege innerhalb der zweiten ISO/OSI-Schicht zwischen Geräten im Automatisierungsnetzwerk einerseits und Applikationen im virtuellen Raum der Edge Cloud andererseits ermöglicht werden.

4.3.2 Echtzeitkommunikation und Determinismus

Damit das Architekturkonzept Akzeptanz in Brownfield-Szenarien erhält, muss die Konfiguration von Geräten und Applikationen weitgehend unverändert bleiben. Dies führt zu hohen Anforderungen an die Netzwerkkommunikation zwischen den physikalischen Geräten in der Automatisierungsebene und Instanzen auf der Edge Cloud, inklusive der virtuellen Schichten. Von besonderem Interesse ist durch die Nutzung von IE-Standards hierbei der Determinismus.

Determinismus im Kontext der Kommunikationstechnik liegt dann vor, wenn Telegramme zwischen Sender und Empfänger ausreichend schnell übermittelt werden, damit der ausführende Prozess in seiner festgelegten Geschwindigkeit vorhersagbar ist. Dafür müssen die jeweiligen Metriken Latenz, Jitter und Paketverlust bekannt sein, um für eine gegebene Konfiguration mit einer definierten Ausführungszeit und erwarteten Antwortzeit Aussagen treffen zu können [IEE23].

Hierbei sind die notwendigerweise zu erreichenden Werte abhängig von der Domäne,

der Applikation, dem Protokoll, den beteiligten Geräten und der Konfiguration. Eine grobgliedrige Einteilung und damit einhergehende Anforderungen an Jitter und Latenz liefern verschiedene Literaturquellen und sind exemplarisch nach der Norm IEC 61784-2 in Tabelle 4.1 dargestellt. Die Latenzzeit beschreibt die Zeit vom Aussenden bis zum Empfangen des Telegramms. Der Jitter beschreibt zeitliche Schwankungen der Latenzzeit.

Tabelle 4.1: Latenz-/ und Jitteranforderungen in der Automatisierungstechnik nach IEC 61784-2 [IEC19]

Echtzeitklasse	Anwendungen	Latenz	Jitter
1	Manuelle Prozesssteuerung, Prozessüberwachung, SPS zu SPS Kommunikation	10-100 ms	/
2	Automatische Prozesssteuerung, SPS zu Sensor/Aktor Kommunikation	1-10 ms	$\leq$ 1 ms
3	Bewegungsregelung	$<$ 1 ms	$\leq$ 1 µs

Im Rahmen des vorliegenden Architekturkonzeptes werden die Echtzeitklassen 1 und 2 als mögliche Anwendungsgruppen definiert. Echtzeitklasse 3 benötigt aufgrund des notwendigen sehr geringen Jitters und niedriger Latenzzeiten häufig neben spezieller Hardware und Protokollen auch diverse Mechanismen wie Zeitsynchronisation und einen Kommunikationszeitplan von Datenströmen.

Innerhalb Echtzeitklasse 2 werden vor allem PROFINET und EtherNet/IP eingesetzt, welche eine Zykluszeit von 1 ms oder höher erlauben. Um ein deterministisches Verhalten garantieren zu können, wird der maximal erlaubte Jitter auf 50% der minimalen Zykluszeit und demnach 0,5 ms festgelegt. Zudem wird die Einwegelatenz auf einen maximalen Wert von 0,5 ms festgelegt. Sofern diese Rahmenbedingungen eingehalten werden, kommen die jeweiligen Telegramme beim Empfänger an, bevor ein neues Telegramm vom Sender verschickt wird, sodass ein vorhersagbares Verhalten ermöglicht wird.

Abschließend muss auch die Echtzeitfähigkeit der Virtualisierungsplattform gewährleistet sein, um Applikationen mit Echtzeitanforderungen betreiben zu können. Ein gängiger Ansatz der Literatur ist die Nutzung des Blackbox-Programms cyclictest, welches in regelmäßigen Abständen Software-Interrupts auslöst und die Reaktions- und Abarbeitungszeit misst.

4.3.3 Hochverfügbarkeit von Kommunikationsnetzwerken

Durch die Verlagerung von Automatisierungsapplikationen in eine Edge Cloud werden mehrere echtzeitkritische Kommunikationsbeziehungen über eine gemeinsam genutzte Netzwerkinfrastruktur gebildet. Dies bedeutet auch, dass zu jedem Zeitpunkt Kommunikationsflüsse verschiedener Anwendungen über ein einzelnes Netzwerkgerät verlaufen können. Im Störungsfall können daher bei Nichteinhaltung der Wiederherstellungszeit mehrere Anwendungsbeziehungen unterbrochen werden. Dies gilt für alle Geräte entlang des Kommunikationspfades, der somit aus mehreren SPOF für jeden einzelnen Kommunikationsfluss besteht. Damit wird als weitere Anforderung an das Netzwerk mindestens ein zweiter

Pfad benötigt, welcher im normalen Zustand den anderen Pfad nicht überschneidet. Die Redundanz gilt hierbei sowohl für Geräte als auch andere physikalische Medien wie Kabel.

Der Verlust von Daten wird innerhalb der in dem vorherigen Abschnitt vorgestellten Echtzeitklassen nicht näher spezifiziert. Innerhalb von IE-Protokollen lässt sich jedoch ein Watchdog definieren, welcher aus dem Produkt der Zykluszeit und einer natürlichen Zahl $x \geq 3$ besteht. Sofern in dieser Zeit kein zulässiges IE-Telegramm beim jeweiligen Gerät ankommt, wird die Verbindung zwischen SPS und Prozessgerät terminiert. Nachdem Safety-relevante Applikationen bestätigende Protokolle nutzen, müssen hier Endgeräte den Empfang der letzten Nachricht bestätigen und dies im Telegramm, beispielsweise durch inkrementieren einer laufenden Nummer, kenntlich machen. Dies bedeutet auch, dass der Watchdog in Safety-Prozessen nicht nur die Kommunikationsverzögerung, sondern auch die Verarbeitsungszeit innerhalb der beteiligten Geräte und Applikationen einschließt.

Analog zu der vorherigen Anforderung wird auch hier die strengstmögliche Einstellung von IE-basierter Kommunikation als Anforderung angenommen, damit eine Brownfield-Migration vereinfacht wird. Dies bedeutet, dass in einem Fehlerfall maximal zwei Telegramme in Folge für einen unidirektionalen Kommunikationsfluss verloren gehen dürfen. Bei einer Zykluszeit von 1 ms und vernachlässigbaren Übertragungszeiten ergibt sich somit eine Wiederherstellungszeit nach einer Störung von $t \leq 2\ ms$. Diese wird durch vorhandene Latenzzeiten und Jitter weiter reduziert.

Die Einführung einer Edge Cloud Infrastruktur und der damit verbundenen Konvergenz von IT und OT erhöht demnach die Bedeutung eines hochverfügbaren Netzwerkes. Die grundlegende Anforderung an die logische Verbindung ist vereinfacht in Abbildung 4.2 dargestellt. Damit Applikationen dieser Kritikalität in einer entfernten Plattform betrieben werden können, sind notwendigerweise zwei Pfade durch das Netzwerk zwischen virtualisierter Applikation und den physikalischen Endgeräten notwendig. Protokolle und Mechanismen sind zu den jeweiligen Anforderungen an die Wiederherstellungszeit und weitere Rahmenbedingungen zu wählen. Allerdings gilt es, die Kompatibilität mit den jeweiligen IE-Protokollen sicherzustellen und wo möglich deterministische Redundanzmechanismen zu verwenden.

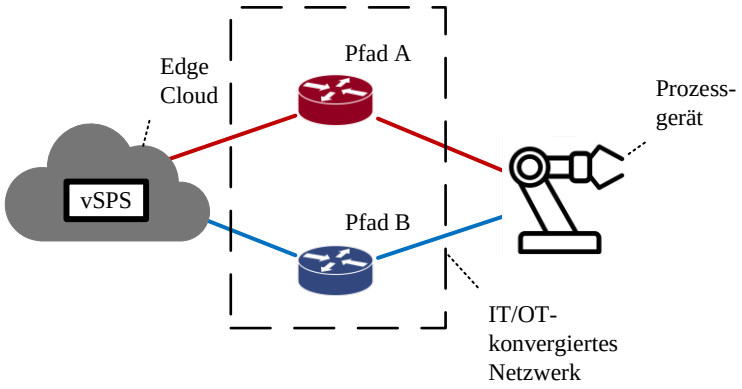


Abbildung 4.2: Redundante Pfade verbinden Applikationen der Edge Cloud mit dem Shopfloor.

4.3.4 Hochverfügbarkeit von vSPS

Ein ähnliches Szenario ist durch die Konsolidierung von zuvor Hardware-gebundenen Applikationen auf einer virtualisierten Plattform vorzufinden. Da leistungsfähige Server innerhalb von Rechenzentren mehrere Applikationen auf einem physikalischen Gerät beherbergen können, ist die Auswirkung eines Ausfalls eines oder sogar mehrerer Server sehr weitreichend. Dies ist ein Risiko für den generellen Wunsch industrielle Automatisierungssysteme für eine lange Zeit ohne nennenswerte Eingriffe zu betreiben und die jeweiligen Systeme hochverfügbar zu halten.

Besondere Aufmerksamkeit erzeugt hierbei die Virtualisierung von SPS, welche als zustandbehaftete Applikationen im Falle eines Ausfalls die Zustandsvariablen innerhalb des Arbeitsspeichers verlieren. Generell muss hier zwischen statischen und dynamischen Daten unterschieden werden. Statische Daten enthalten statische Variablen sowie das Programm, welche ausschließlich durch eine Projektierungssoftware verändert werden und häufig zur Rekompilierung des Codes führen.

Dem gegenübergestellt enthält das dynamische Subset Eingang/Ausgang (E/A)-Daten, sowie interne Zustände und Variablen. Verfügbare Lösungen von Hardware-SPS auf dem Markt erlauben statische Zustandsgrößen von 150 KB bis 9 MB sowie dynamische Zustandsgrößen von 1 MB bis 60 MB [Sie24]. Dabei ist davon auszugehen, dass sich in einem SPS-Zyklus nur ein Teil der Daten ändert. Selbst für größere Anlagen stellte eine vergangene Studie zu erwartetende Zustandsgrößen im einstelligen Prozentbereich fest [Kra07].

Ein Subset der dynamischen Daten wird als Remanenzdaten bezeichnet. Diese enthalten beispielsweise vor allem Informationen über Füllstände, Positionen, und Produktionsstücke. Beim Verlust dieser Daten kommt es zu erhöhten Stillständen, da beispielsweise Werkstücke entfernt oder Roboter neu kalibriert werden müssen.

Ein einzelner Serverausfall kann daher bei einem fehlenden Redundanzkonzept zu einem Ausfall eines größeren Bereichs der Automatisierungstechnik und daher zu einer hohen Wiederherstellungszeit führen. Im Falle eines Ausfalls der klassischen Hardware-SPS, beispielsweise bei Verlust der Spannungsversorgung, werden die Remanenzdaten in einen nicht-flüchtigen Speicher geschrieben. Ermöglicht wird dies durch einen Kondensator, der für einige Sekunden die Spannung aufrecht erhält. Die Wiederherstellung kann dadurch schneller erfolgen. Sollten auch Remanenzdaten von einem Verlust betroffen sein, wäre bei der Hardware-SPS nur ein SPS-Bereich beeinflusst, auch wenn in diesem Fall mit einer längeren Wiederherstellungszeit zu rechnen wäre.

Aufgrund der Konsolidierung von mehreren SPS auf einem Server wären in einem vergleichbaren Szenario direkt mehrere Bereiche betroffen, was die Notwendigkeit für Hochverfügbarkeitslösungen unterstreicht und die Annahme der Grundüberlegung der Vermeidung von SPOF von verteilten Systemen bekräftigt.

Die Erwartungshaltung eines Endnutzers einer vSPS ist somit, dass analog zu heute die zu persistierenden Daten, sogenannte Remanenzdaten, gesichert werden, und dies auch bei einem Serverausfall. Dies muss gleichzeitig mit einer SPS-Programmzeit im Bereich von

einstelligen bis zweistelligen Millisekunden geschehen, ohne den darauf folgenden Zyklus zu lange zu verzögern. Die notwendige Verzögerung zum Starten des nächsten Zyklus kann auf die Notwendigkeit für Datenkonsistenz zurückgeführt werden. Um erneut die Akzeptanz der Lösung zu gewährleisten, sollte die für das Wegspeichern der Daten benötigte Zeit im einstelligen Millisekundenbereich befinden.

Abschließend wäre eine unterbrechungsfreie Hochverfügbarkeitslösung am erstrebenswertesten. Hierbei sind jedoch IE-Protokoll-Spezifika zu beachten, die beispielsweise das Umschalten zwischen Instanzen ohne eine Unterbrechung erschweren oder nicht möglich machen.

4.3.5 IT/OT-Security

Durch die Einführung der Edge Cloud und der damit verbundenen Konvergenz von IT und OT werden vor allem im Bereich IT/OT-Security die Unterschiede zwischen den beiden Domänen deutlich. IE-Protokolle sind vor allem für die Verwendung in abgeschlossenen und kontrollierten Systemen konzipiert. Dies lässt sich unter anderem durch das Fehlen von Authentisierungsmechanismen wie IEEE 802.1x bei Automatsierungsgeräten erkennen. Innerhalb der IT-Domäne hingegen dürfen Endpunkte ohne erfolgreiche Authentifizierung nicht im Netzwerk kommunizieren - ein Konzept, das unter dem Namen NAC bekannt ist. Um OT-Applikationen nun auch in dem selben Netz betreiben zu können, ohne das Level der IT/OT-Security zu reduzieren, wird demnach eine skalierbare Lösung benötigt, welche von OT und IT gleichermaßen angenommen wird.

Des Weiteren wird derzeit das Netzwerk mittels Firewalls in der Nord- und Südrichtung segmentiert. Durch die fortlaufende Steigerung dieser Kommunikationsrichtung durch neue Applikationen wie Data Engineering und die Einführung einer Edge Cloud Infrastruktur gelangt das aktuell genutzte Konzept an Grenzen. Abbildung 4.3 zeigt die aktuelle Infrastruktur ergänzt durch eine Edge Cloud. Ohne weitere Anpassung müsste nun der Steuerungs-Datenverkehr nicht nur das IP-basierte Netzwerk, sondern auch Firewalls durchqueren, welche damit einen weiteren SPOF darstellen als auch unklare Echtzeiteigenschaften und erhöhten Konfigurationsaufwand besitzen. Es gilt ein vergleichbares Level an IT-Security zu ermöglichen, ohne dabei die anderen Anforderungen an Determinismus oder Hochverfügbarkeit einzuschränken.

4.3.6 Betreibbarkeit

Die Adoption von neuartigen Architekturkonzepten ist grundlegend eingeschränkt, wenn sie aufgrund hoher Komplexität, Impraktibilität in der Handhabung oder fehlender klarer Strukturen nicht betreibbar sind. Die Betreibbarkeit der Lösung ist vor allem in der Automatisierungstechnik von höchster Bedeutung, da ein robustes und fehlerloses Verhalten die Verfügbarkeit der Prozesse hoch hält. Hierbei werden vor allem Lösungen von geringer Komplexität, beispielsweise durch Plug-and-Play Mechanismen sowie aussagekräftige Fehlerbeseitigungs-Optionen geschätzt und eingesetzt. Gerade bei der Adoption der Architek-

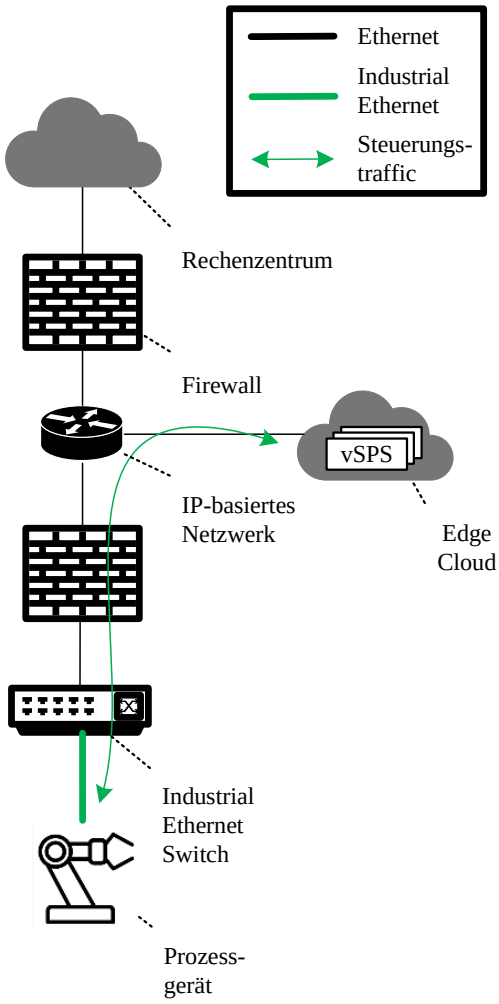


Abbildung 4.3: Eine Edge Cloud als Teil eines klassischen Architekturkonzeptes nach [KMG24].

tur in größeren Umgebungen gilt es auch weiterhin die Komplexität der Lösung beherrschbar und die Kritikalität von Änderungen entlang der Kette gering zu halten.

Abschließend ist die Beobachtbarkeit des Systems von integraler Bedeutung, um auf Störungen schnell reagieren und einen funktionierenden Betrieb zielgerichtet wiederherstellen zu können. Dafür müssen Metriken erfasst und Logs gespeichert werden, um daraufhin passende Alarme zu definieren und Fehler-Ursachen-Analysen zu ermöglichen.

4.4 Industrial Ethernet über IP

Der folgende Abschnitt beschreibt die Realisierung des Transportes von IE-Protokollen über ein IP-basiertes Netzwerk. Die grundlegende Anforderung ist dabei das Spannen von ISO/OSI Schicht 2-Netzwerken, von der Automatisierungsebene bis hinein in die Edge Cloud. Dies folgt auf die Auslagerung von Steuerungs- und Konfigurationsapplikationen in eine Edge Cloud. Weiterhin werden in diesem und allen weiteren Abschnitten die Betreibbarkeit

der Lösung mitbetrachtet, um eine Adoption des Konzeptes zu vereinfachen.

IP-basierte Netzwerke nutzen häufig Transfernetzwerke, VLANs und Routing-Protokolle zwischen den einzelnen Switchen und Routern um Broadcast-Domänen zu beschränken und eine Skalierung des Netzwerks zu ermöglichen. Sofern die Notwendigkeit für eine Schicht 2-Kommunikation besteht, müssen in größeren Netzwerken Pakete typischerweise mit Hilfe eines Tunnelprotokolls gekapselt werden, sofern die jeweiligen Kommunikationspartner an unterschiedlichen Stellen des Netzwerkes verortet sind.

Konzeptionell fällt hierbei die Wahl auf das Kapselungsprotokoll VXLAN. Dies lässt sich folgendermaßen begründen: Das IP-basierte Netzwerk soll IT und OT-Applikationen über eine gemeinsam genutzte Hardware unterstützen. Innerhalb der IT-Domäne, Campus- und Rechenzentrums-Netzwerken, wird zunehmend VXLAN genutzt, um virtuelle Overlay-Netzwerke über ein physikalisches Underlay zu spannen und eine skalierbare Lösung für Schicht 2-Kommunikation zu ermöglichen. Weiterhin werden die auf 2^{12} beschränkten VLANs des IEEE 802.1Q-Headers um VID innerhalb des VXLAN-Headers erweitert, welche 2^{24} Kombinationen ermöglicht und somit feingranular und skalierbar konfigurierbar sind. Zudem erlaubt VXLAN die Einführung von Mikrosegmentierung auf Basis von GBP, welches ein neuartiges Werkzeug für die IT-Security darstellt und in dem Abschnitt 4.3.5 näher beleuchtet wird.

Durch VXLAN wird somit ein virtuelles Schicht 2-Netzwerk über das physikalische Netzwerk erzeugt. Für Endgeräte, beispielsweise Prozessgeräte und Aktoren als auch virtuelle Teilnehmer wie vSPS, sieht es weitgehend so aus, als wären sie jeweils in einem physikalischen Schicht 2-Netzwerk verbunden. Der gesamte Vorgang ist in Abbildung 4.4 dargestellt. Die Kapselung erfolgt am sogenannten Edge des Netzwerks durch hardwarebasierte Funktionen in der ASIC des Switches. Daraufhin erfolgt die Übertragung innerhalb der Fabric ohne weitere Kapselungen auf Basis klassischer Routing-/ und Switching-Mechanismen. Die Entkapselung erfolgt am Ausgang der Fabric.

VXLAN alleine ist jedoch nicht ausreichend um zu einer skalierbaren Lösung zu gelangen. Dem SDN-Ansatz folgend sieht das Konzept vor, ausschließlich die Datenebene mittels VXLAN umzusetzen. Die Modularität von SDN und Standardkonformität von VXLAN ermöglicht die Nutzung verschiedener Mechanismen und Prokotolle für die Kontrollebene. Im Rahmen des Architekturkonzeptes werden die beiden Standards EVPN/BGP und LISP verwendet, welche auch bereits in der Industrie adoptiert werden. Analog zur Virtualisierung von Server-Ressourcen durch einen Hypervisor wird die eigentliche Komplexität der Physik für den Endnutzer abstrahiert, wodurch die Administration des Netzwerkes erleichtert wird. Des Weiteren können Anycast-Gateways am Edge des Netzwerks (in der Zugriffsschicht) verwendet werden, um über physikalische Grenzen hinweg eine Gateway-IP-Adresse für ein Netz bereitzustellen. Abschließend werden Informationen über verbundene Endgeräte mittels effizienten Mechanismen an die jeweiligen an der Kommunikation beteiligten Netzwerkgeräte übertragen.

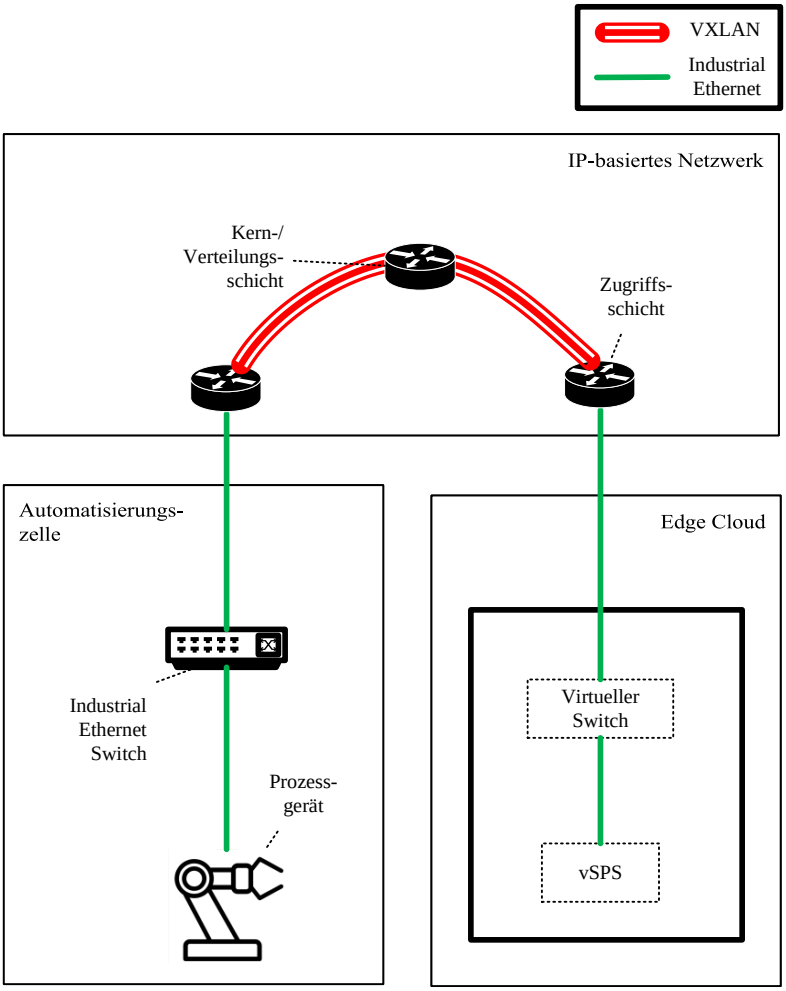


Abbildung 4.4: Kapselung von Datenverkehr zwischen der Automatisierungsebene und Edge Cloud

4.4.1 Nutzung weiterer Standards

Das Architekturkonzept nutzt bewusst VXLAN mit einer passenden Technologie für die Kontrollebene aufgrund der Eignung für IT- und OT-Datenverkehr. Gleichzeitig sind diese Kombinationen in Campus-Netzwerken und bis hinein in das Rechenzentrum in der IT bereits verbreitet, wodurch zudem auch eine Konvergenz von Campus und Rechenzentrum möglich wird. Des Weiteren wird auf die Nutzung von Label-basierte Technologien wie MPLS oder Segment Routing verzichtet, da sie in typischen Campus-Netzwerken und Rechenzentren aufgrund ihrer Komplexität in der Handhabung und dem Preis nicht als realistisches Konzept adoptiert werden können. Stattdessen wird ein klassisches IP-basiertes Netzwerk vorausgesetzt, wodurch auch die notwendige Kompetenz bei der vorhandenen Netzwerkadministration bereits vorhanden ist.

Eine Nutzung von Punkt-zu-Punkt Tunnelprotokollen wie Generic Routing Encapsulation (GRE) ist aufgrund der fehlenden Skalierbarkeit nicht ohne Weiteres empfehlenswert. Entscheidender Faktor ist hierbei die Handhabung der Kontrollebene nach dem SDN-Ansatz

und die Erweiterung durch zusätzliche Funktionen wie die Segmentierung auf Basis von GBP und die feingranulare Aufteilung des Netzwerkes durch VNI.

4.5 Echtzeitfähigkeit und Determinismus

Deterministische Kommunikation ist ein essentieller Bestandteil von Netzwerken, die IE-Traffic transportieren. Diese Eigenschaft muss vom Sender bis zum Empfänger sichergestellt werden, um einen reibungslosen Betrieb zu ermöglichen. Der folgende Abschnitt beschreibt, wie das anvisierte Architekturkonzept die Anforderungen an Echtzeitfähigkeit und Determinismus von Steuerungskommunikation erfüllt.

Zunächst zeichnet sich industrieller Steuerungs-Datenverkehr durch ein deterministisches Kommunikationsverhalten in Bezug auf die Auslastung des Netzwerkes und Aussendung von Telegrammen aus. Hierbei erfolgt ein zyklischer Datenaustausch zwischen Controller und Prozessgerät in einer festgelegten Zykluszeit t in Millisekunden. Die Größe der Nutzdaten wird durch die Eingänge und Ausgänge eines jeden Prozessgerätes vorgegeben, die sich auch innerhalb eines Gerätes unterscheiden können. Somit ergibt sich bei einer gegebenen Anzahl an Bytes für die Nutzdaten und Header folgender Wert für die notwendige Bandbreite des Kommunikationsflusses:

$$flow_{bw} = \frac{1000\frac{ms}{s}}{t} \times (Header + Data) \tag{4.1}$$

Die Summe der Bandbreitenanforderungen aller vorhandenen Kommunikationsflüsse über einen physikalischen Link ergibt die notwendige zu reservierende Bandbreite. Die erhaltene Summe ist demnach nicht innerhalb des gesamten Netzwerks gültig, sondern auf Port-Basis und in größeren Netzwerken mit Millionen Kommunikationsflüssen zu berechnen. Sollen nun zusätzlich die Telegramme in einer strukturierten Art und Weise über das Netzwerk übertragen werden, erfordert das passende Algorithmen und Mechanismen, die von Infrastruktur und Applikation genutzt werden. Dies verdeutlicht in Kürze die Komplexität, die nun mittels standardisierten Mechanismen von IEEE und IETF gelöst werden soll.

4.5.1 Determinismus mittels DetNet

Die erklärten Hauptziele von IETF DetNet sind eine minimale und maximale Ende-zu-Ende-Latenz über das gesamte Netzwerk für ausgewählte Kommunikationsflüsse bereitzustellen, sowie Paketverlust durch Überlastung des Netzwerkes zu vermeiden. Nachdem die Standardisierung noch nicht abgeschlossen ist, können im Rahmen des Konzeptes nur allgemeine Rahmenbedingungen genannt werden und ausgewählte Standards gewählt werden, die aufgrund ihres Nutzens und der Implementierbarkeit vermutlich in Zukunft Anwendung finden.

Einzelnen Kommunikationsflüssen muss den Vorgaben entsprechend Bandbreite reserviert werden, die vor allem vier Parameter enthalten:

- Commited information rate beschreibt die Anzahl an Bytes, die innerhalb eines

Telegramms in einem Zeitslot T übertragen werden können.

- Commited burst size beschreibt die Anzahl an Kommunikationsflüssen, die Pakete innerhalb eines Timeslots verschicken können.
- Peak information rate sowie peak burst size erlauben Steigerungen der beiden anderen Parameter über den normalen Wert hinaus, angegeben in Bytes respektive Anzahl der Kommunikationsflüsse.

Abbildung 4.5 stellt die zyklische Kommunikationszeitplanung von Paketen innerhalb von DetNet dar. Die Besonderheit dieses Verfahrens ist, dass der Jitter mit der Anzahl an Hops nicht zunimmt und somit konstant bleibt. Technologiebedingt ist der Jitter auf das Zweifache der Zykluszeit T begrenzt. Theoretisch ist es sogar möglich, den maximalen Jitter noch weiter zu begrenzen. Werden Kommunikationsflüssen feste Slots innerhalb der Intervalle zugewiesen, kann der Jitter, theoretisch, auf 0 µs reduziert werden. Werden Kommunikationsslots nicht mehr benötigt, können diese für Best-Effort-Kommunikation benutzt werden. Innerhalb des IP-basierten Netzwerkes werden Kommunikationsflüsse aggregiert und über-

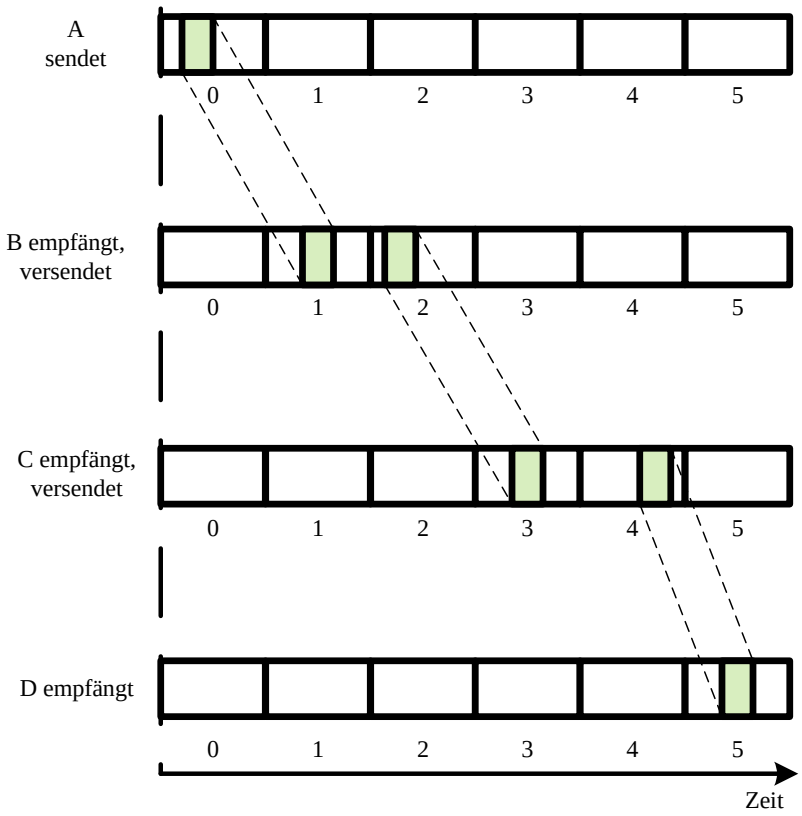


Abbildung 4.5: Determinismus durch einen zyklischen Kommunikationszeitplan in IETF DetNet

tragen. Die fehlende Unterscheidung zwischen den unterschiedlichen Flüssen vereinfacht die Kommunikationszeitplanung und ermöglicht eine bessere Skalierbarkeit. TSN-Substandard IEEE 802.1Qch kann für den zyklischen Kommunikationszeitplan verwendet werden.

4.5.2 Determinismus mittels klassischen QoS-Mechanismen

Innerhalb von Commercial off-the-Shelf (COTS)-Hardware können Telegramme priorisiert in dedizierten Hardware-Warteschlangen behandelt werden, sodass Latenzzeiten und Jitter minimiert werden. Damit die Echtzeitkommunikation die notwendigen Anforderungen erfüllen kann, müssen die Telegramme zu jeder Zeit an jeder einzelnen Stelle erkannt und priorisiert werden. Die Erkennung und das Einordnen in die passende Hardware-Warteschlange ist in Abbildung 4.6 dargestellt. Hierbei durchlaufen die jeweiligen Telegramme die folgenden Schritte am Beispiel von PROFINET Kommunikation und der jeweiligen ISO/OSI-Schicht:

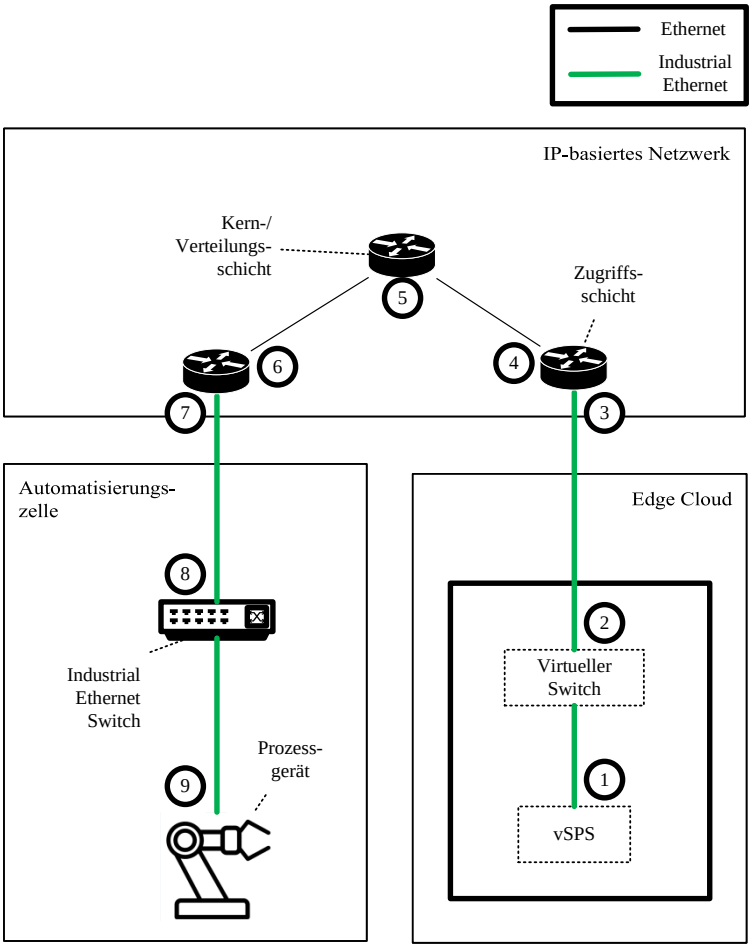


Abbildung 4.6: Ende-zu-Ende QoS durch eine VXLAN Fabric

1. Schicht 2: Versenden des PROFINET-Telegramms, VID = 0 und IEEE 802.1p = 6
2. Schicht 2: Änderung der VID von 0 zu %VLAN_ID
3. Schicht 2: Nutzung des einzigartigen EtherTypes zur Zuordnung eines einzigartigen DSCP-Wertes - alternativ auf Basis von IEEE 802.1p
4. Schicht 3: Nutzung des einzigartigen DSCP-Wertes, Zuweisung einer dedizierten Warteschlange

5. Schicht 3: Keine Änderung, Nutzung des DSCP-Wertes und Sortierung in die richtige Warteschlange
6. Schicht 3: Nutzung des einzigartigen DSCP-Wertes, Zuweisung einer dedizierten Warteschlange
7. Schicht 2: Einzigartiger DSCP-Wert wird Priorität 6 von IEEE 802.1p zugeordnet, VLAN entspricht %VLAN_ID
8. Schicht 2: Änderung der VID von %VLAN_ID zu 0
9. Schicht 2: Empfangen des PROFINET-Telegramms, VID = 0 und IEEE 802.1p = 6

Innerhalb der Fabric ist es weiterhin wichtig, dass die Ende-zu-Ende Regeln bezüglich QoS identisch sind, damit eine Priorisierung der Pakete konsequent durchgeführt und ein deterministisches Verhalten ermöglicht wird. Die zu reservierende Bandbreite auf jedem Port kann mittels Gleichung 4.1 berechnet werden. Aufgrund der im Vergleich zu IT-Applikationen geringen Bandbreite können bereits mit einer geringen Reservierung von beispielsweise 10% der maximalen Bandbreite jeglicher Traffic priorisiert werden. Dies ist auf Bandbreitensteigerungen und Kostensenkungen innerhalb der IT zurückzuführen, da selbst in der Zugriffsschicht in Rechenzentrumsinfrastrukturen bereits Bandbreiten von bis zu 800 Gbit/s genutzt werden. Dem gegenübergestellt ist die notwendige Bandbreite von IE-Applikationen weitestgehend unverändert und kann auch weiterhin mit bis zu 100 Mbit/s pro SPS-Bereich überschlagen werden.

Aufgrund der Zielstellung der IT/OT-Konvergenz und der damit verbundenen Übertragung von Multimediakommunikation muss das Konzept auch klassischen Enterprise-Datenverkehr unterstützen und priorisiert behandeln, wozu unter anderem auch Sprach-, Daten- und Videokommunikation zählt, um die Nutzererfahrung nicht einzuschränken. Hierbei stellt sich die Frage nach notwendigen Bandbreiten zwischen den einzelnen Netzwerkkomponenten sowie dem Anteil der Bandbreiteneservierung für die jeweiligen Services. Dies ist nur in konkreten vorhandenen Szenarien und Geräten zu bestimmen und benötigt daher eine auf die Gegebenheiten abgestimmte Konfiguration.

4.5.3 Determinismus in der Virtualisierung

Nachdem es sich um echtzeitkritische Applikationen auf einem verteilten System handelt, wird im Folgenden kurz auch auf die Echtzeitfähigkeit und Determinismus von Virtualisierungsumgebungen eingegangen. Hier gilt es zwischen dem deterministischen Verhalten von Applikationen sowie Echtzeitfähigkeit von Virtualisierungsschichten zu unterscheiden.

Die Echtzeitfähigkeit der Applikation hängt vor allem mit dem untergelagerten Systemen zusammen. Abbildung 4.7 stellt verschiedene Optionen dar, mit welchen Applikationen eingesetzt werden können. Grundsätzlich wird immer eine Hardware benötigt, die nicht nur rein physikalisch die notwendigen Operationen in der benötigten Zeit ausführen kann, sondern auch für Echtzeitapplikationen optimiert ist. Als Betriebssystem wird im Allgemeinen ein

Linux-Derivat genutzt, welches mittels preempt_RT-Patch niederpriore Tasks zugunsten höherpriorer Tasks pausieren kann. Durch die Reservierung von Prozessorrechenleistung mittels Hypervisor-Technologie oder von ganzen isolierten Prozessorkernen besitzen Applikationen wie eine vSPS auch auf verteilten Systemen ein echtzeitfähiges Verhalten. Eine detaillierte Beschreibung der Erreichung von deterministischen Verhalten von Applikationen auf verteilten Systemen ist in Abschnitt A.3 wiederzufinden. Abschließend empfiehlt es sich, die virtualisierte Netzwerkschicht mittels Polling-Mechanismen kontinuierlich und hochfrequent nach vorhandenen Telegrammen in Warteschlangen abzufragen, um Latenzen und Jittereigenschaften zu verbessern. Dies ist entgegen typischer Mechanismen, welche auf Bandbreitenmaximierung und Effizienz optimiert sind.

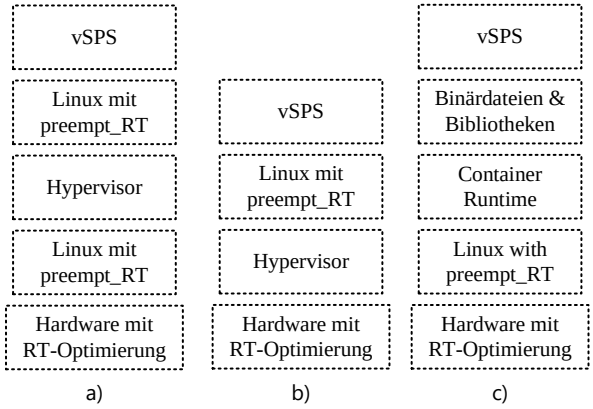


Abbildung 4.7: Mögliche Bereitstellungsmöglichkeiten von echtzeitkritischen Applikationen wie vSPS nach [KMG22]

4.6 Hochverfügbarkeit von Kommunikationsnetzwerken

Die Auswahl eines passenden Redundanzprotokolls ist abhängig von mehreren Faktoren, unter anderem der Wiederherstellungszeit, akzeptablen Paketverlustraten, Komplexität und Determinismus. Verschiedene Mechanismen und Protokolle sind hierbei bereits heute in Benutzung, beispielsweise das Zusammenfassen von mehreren physikalischen Einheiten zu einer logischen Einheit durch VRRP oder die Erkennung von Störungen in Ringtopologien durch Media Redundancy Protocol (MRP). Das grundlegende Designziel ist die Vermeidung von SPOF zur Erhöhung der Verfügbarkeit.

4.6.1 Kommunikationsarten

Das entwickelte Konzept erlaubt drei verschiedene Kommunikationsmuster durch das Netzwerk, welche in Abbildung 4.8 dargestellt sind. Sie sind für jegliche Dual-Path-Netzwerkarchitekturen anwendbar und werden in den folgenden Abschnitten erläutert.

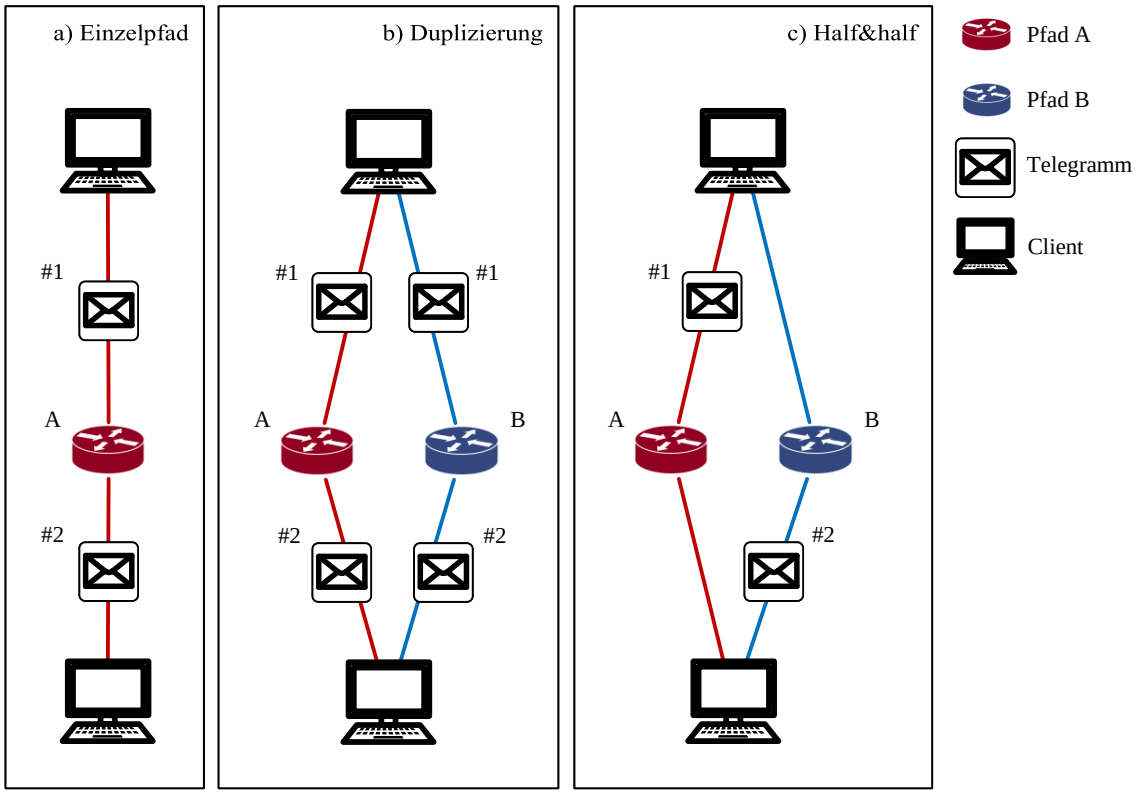


Abbildung 4.8: Drei verschiedene Kommunikationsmuster, um Telegramme zu übertragen: a) Single-Path Kommunikation, b) Paketduplizierung und c) Half&Half nach [KG23b].

4.6.1.1 Single-Path Kommunikation

Die klassische Kommunikation über einen einzelnen Pfad ist auch weiterhin möglich und explizit vorgesehen. Dies ist insbesondere für IT-Anwendungen von Bedeutung, die sich durch eine hohe Bandbreite und keine strengen Verfügbarkeitsanforderungen durch die Nutzung von TCP/IP auszeichnen. Darüber hinaus kann im Falle eines Netzwerkgeräteausfalles auf dynamische Redundanzmechanismen zurückgegriffen werden, um die Kommunikation automatisiert wiederherstellen zu können.

4.6.1.2 Paketduplizierung

Sofern die Anforderungen an eine Übertragung Umschaltzeiten von 50 ms untertreffen und ein Abbau der Kommunikation negative Auswirkungen, beispielsweise finanzielle oder akzeptanzbasierte, mit sich führt, sind statische Redundanzmechanismen wie die Duplizierung von Paketen zu bevorzugen. Diese sind vor allem in der industriellen Kommunikation verbreitet, da selbst eine kurzzeitige Störung eine längere Ausfallzeit mit sich führen kann. Hierbei werden Telegramme an einem Punkt dupliziert und an einer anderen Stelle dedupliziert. Dies birgt auch Vorteile in Bezug auf Latenzreduzierungen, indem Lastspitzen in einem Pfad abgefangen und durch die Übertragung über den anderen Pfad ausgeglättet werden können.

Während die Nutzung verschiedener Duplizierungsstandards möglich wäre, wird im Rahmen des Konzeptes PRP verwendet. Dieses Netzwerkprotokoll genießt eine gute Adoption innerhalb der Automatisierungsindustrie, ermöglicht die gleichzeitige Nutzung von SAN und DAN, und zeichnet sich durch einfaches Setup und Fehlersuche aus. Während das Protokoll bereits breitflächig in industriellen Switchen zur Verfügung steht, findet es in der IT-Domäne bisher keine Verwendung. Dies liegt vor allem an der Tatsache, dass Duplizierungsmechanismen im Allgemeinen nur für Schicht 2-Kommunikation definiert sind, die innerhalb der IT selten notwendig ist.

Mehrere Möglichkeiten existieren, um auf der Edge Cloud die PRP-Funktionalität zu realisieren. Zunächst können Applikationen selbst die Duplizierung übernehmen, wobei dies in Software mit Echtzeiteigenschaften nur durch Priorisierung des Tasks möglich ist. Weiterhin ist Duplizierung auf Field Programmable Gate Array (FPGA)-basierten Karten sowie auf Switchen innerhalb der Zugangsschicht analog zu der Umsetzung in industriellen Switchen möglich.

Abschließend kann der virtuelle Switch der Edge Cloud-Infrastruktur um die PRP-Funktionalität erweitert werden. Diese Lösung bietet maximale Flexibilität und erlaubt gleichzeitig die Konsolidierung mehrerer PRP-Datenströme innerhalb der ohnehin vorhanden virtualisierten Netzwerkschicht. Zudem kann die PRP-Funktionalität vollständig von dem Endnutzer maskiert werden, wodurch sich die Nutzererfahrung nicht ändert.

Für eine optimale Effektivität der Duplizierung von Telegrammen sind zwei Pfade durch das IT/OT-konvergierte Netzwerk notwendig. Diese Thematik wird im späteren Abschnitt 4.6.2.1 innerhalb dieses Kapitels behandelt.

4.6.1.3 Half&Half

Um einen Mittelweg zwischen single-path Kommunikation und Paketduplizierung zu bieten und damit die Eigenschaften des Netzwerkes mit den jeweiligen Anforderungen der Applikationen besser paaren zu können, wurde das neue Kommunikationsmuster Half&Half entwickelt. Telegramme werden hier, wie in Abbildung 4.8 dargestellt, abwechselnd zwischen den Pfaden A und B übertragen. Im Falle eines Pfadausfalles geht jedes zweite Telegramm verloren, bis entweder der Pfad wiederhergestellt oder von Half&Half auf single-path Kommunikation umgestellt wird. Für IE-Protokolle wie PROFINET oder EtherNet/IP ist dies ausreichend, da aufgrund der überfrequenten Kommunikation ein Paketverlust von 50% toleriert werden kann, ohne dass die Applikation beeinträchtigt wird.

Entscheidend ist hierbei der Watchdog Timer $i \times CT$, welcher nur bei einem validen ankommenden Telegramm zurückgesetzt wird und ein Vielfaches der Zykluszeit CT darstellt. Nachdem in dieser Kommunikationsart Telegramme nacheinander über unterschiedliche Pfade verschickt werden, ist auch die Latenzdifferenz der beiden Pfade sowie die maximalen Latenzunterschiede innerhalb eines Pfades, $\Delta_{A/B}$, von Relevanz. Ein neues Telegramm wird im Intervall $2 \times CT$ über den jeweiligen Pfad geschickt, eine deterministische Aussendung der Telegramme durch die jeweilige Applikation vorausgesetzt, wodurch sich zur Worst-Case-Abschätzung Gleichung 4.2 ergibt. Hierbei ist es wichtig zu nennen, dass diese Gleichung für

jeden Kommunikationsfluss und jede Richtung geprüft werden muss, nachdem beispielsweise die Auslastung in eine Richtung höher als in andere Richtungen und deshalb die Latenz größer sein könnte. Dies verdeutlicht auch die Notwendigkeit einer Ein-Wege-Latenzmessung für Monitoring-Systeme.

Abschließend kann für das Worst-Case-Beispiel von $i = 3$ die maximal tolerierbaren Werte von $\Delta_{A/B}$ in Abhängigkeit von der Zykluszeit CT bestimmt werden, was in Gleichung 4.4 dargestellt ist. Dies erlaubt umgekehrt auch die Berechnung einer minimalen Zykluszeit, sofern die Kommunikationseigenschaften des Netzwerks bekannt sind.

$$WDT \geq 2 \times CT + max(\Delta_A, \Delta_B) \tag{4.2}$$

$$i \geq \frac{max(\Delta_A, \Delta_B)}{CT} + 2 \tag{4.3}$$

$$CT \geq max(\Delta_A, \Delta_B) \quad \forall i = 3 \tag{4.4}$$

Ein Vorteil der Nutzung dieser Kommunikationsart ist, wie in Tabelle 4.2 dargestellt, vor allem die Reduktion der notwendigen Bandbreite auf ein vergleichbares Level mit single-path Kommunikation. Weiterhin kann die Komplexität und Hardwareressourcen im Vergleich zur Paketduplizierung an den jeweiligen Zweigpunkten reduziert werden, da der Sender nur den Pfad auswählen und der Empfänger nur das Telegramm weiterleiten muss, ohne eine zustandsabhängige Verarbeitung durchführen zu müssen. Abschließend führen beide Vorteile zu einer Reduktion des notwendigen Energieverbrauchs.

Tabelle 4.2: Notwendige Bandbreite (BW) im normalen Status, Paketverlust FO_{PL} und Wiederherstellungszeit FO_t im Fehlerfall für die drei Kommunikationsarten.

Modus	BW_A	BW_B	FO_{PL}	FO_t
a)	100%	0%	100%	Router Wiederherstellung
b)	100%	100%	0%	0 ms
c)	50%	50%	50%	0 ms / Timeout

4.6.2 Konzept für mehrere Pfade

Aufgrund der in Abschnitt 4.3 beschriebenen strengen Anforderungen an Paketverlustraten für IE-Protokolle muss die Netzwerkarchitektur mindestens zwei getrennte Pfade bereitstellen, um die Resilienzanforderungen zu erfüllen. Im Folgenden werden ausschließlich zwei Pfade dargestellt und erläutert, obwohl das Konzept auch bei mehr als zwei Pfaden anwendbar ist.

Grundlegend sind zwei Konzepte möglich. Die erste Option ist eine logische Trennung der Netzwerke in zwei VXLAN-Fabrics, beispielsweise durch jeweils eine eigene Kontroll- und Managementebene. Diese Lösung führt zu einem hohen hardwareseitigen Aufwand durch die Dopplung jeglicher Netzwerkhardware. Zudem können SAN nicht über beide

Netzwerke kommunizieren, da es sonst zu einer Routing-Schleife kommen könnte. Allerdings schützt diese Art der Redundanz nicht nur vor unvermeidbaren Fehlern durch Hardware- und Softwarestörungen, sondern erlaubt es auch Misskonfigurationen innerhalb einer Fabric abzufangen.

4.6.2.1 Dual-Path-Kommunikation durch eine Fabric

Eine zweite Option ist die Nutzung einer einzigen Fabric nach einem einem Traffic Engineering Ansatz. Traffic Engineering beschreibt die Wahl eines expliziten Weges eines Telegramms durch ein Kommunikationsnetzwerk. Während dies eine einzige Fehlerdomäne auf der Managementebene erzeugt, können hier Hardwareressourcen eingespart und Routing-Schleifen vermieden werden. Die Idee des Traffic Engineerings ist im eigentlichen VXLAN-Kontext nicht vorgesehen, da hier nur Eintritts- und Ausgangsport in die Fabric bekannt sein müssen und dazwischen die Komplexität durch die Trennung von Underlay und Overlay abstrahiert wird. Das Underlay muss demnach auf Basis von VNI eine Pfadauswahl treffen, was wiederum auch mehrere Loopback-Adressen auf einem einzelnen Netzwerkgerät benötigt.

Eine schematische Realisierung dieses Konzeptes wird im Folgenden vorgestellt. Das Netzwerk wird in zwei Farben unterteilt, rot und blau. Die Router werden statisch einer Farbe zugeordnet. Die Anzahl der Uplinks ist auf zwei pro Router begrenzt, um das Konzept verständlicher zu gestalten. Jedoch unterstützt und bevorzugt das vorgestellte Konzept auch mehr als zwei Uplinks, um den Störungsbereich in Fehlerszenarien zu verringern und eine Lastverteilung über mehrere Links zu ermöglichen. Die Verbindungen zwischen den verschiedenen Routern stehen im Mittelpunkt dieses Konzepts.

Die Netzwerkgeräte jeder Farbe, rot und blau, bilden zwei getrennte Pfade, um eine Paketduplizierung ohne SPOF durch das IP-basierte Netzwerk zu realisieren. Allerdings kann im Falle eines Failover-Szenarios ein Paket einer anderen Farbe von dem jeweiligen Netzwerkgerät übertragen werden. Das bedeutet, dass ein Ausfall eines einzelnen Knotens nur vorübergehend einen der beiden Pfade deaktiviert und so je nach Ausbaustufe einen SPOF für die Zeit der Wiederherstellung des Knotens oder der Verbindung erzeugt. Der Mechanismus ist in Abbildung 4.9 dargestellt.

Bei einem Knoten- oder Verbindungsfehler wird eine zustandsbehaftete Umschaltung durchgeführt. In dem in der Abbildung dargestellten Fall wird der Backup-Pfad zwischen A3.1/A1.1 und B2.1 für Telegramme des Pfades A aktiv. Sobald der Pfad wiederhergestellt ist, wird auch der reguläre Zustand wiederhergestellt.

Jedes Telegramm wird mit A oder B gekennzeichnet. Sobald ein Telegramm beim Router eingeht, wird eine Reihe von Prüfungen durchgeführt, und schließlich wird entschieden, ob das Telegramm über den primären oder den Backup-Pfad gesendet wird. Es ist auch möglich, das Telegramm bei der Ankunft zu kennzeichnen, sofern eine Kennzeichnung noch nicht vorhanden ist. Auf diese Weise sind Protokoll-Implementierungen ausschließlich auf Netzwerkgeräte beschränkt.

Abbildung 4.10 zeigt die Trennung in einen roten und einen blauen Pfad über das

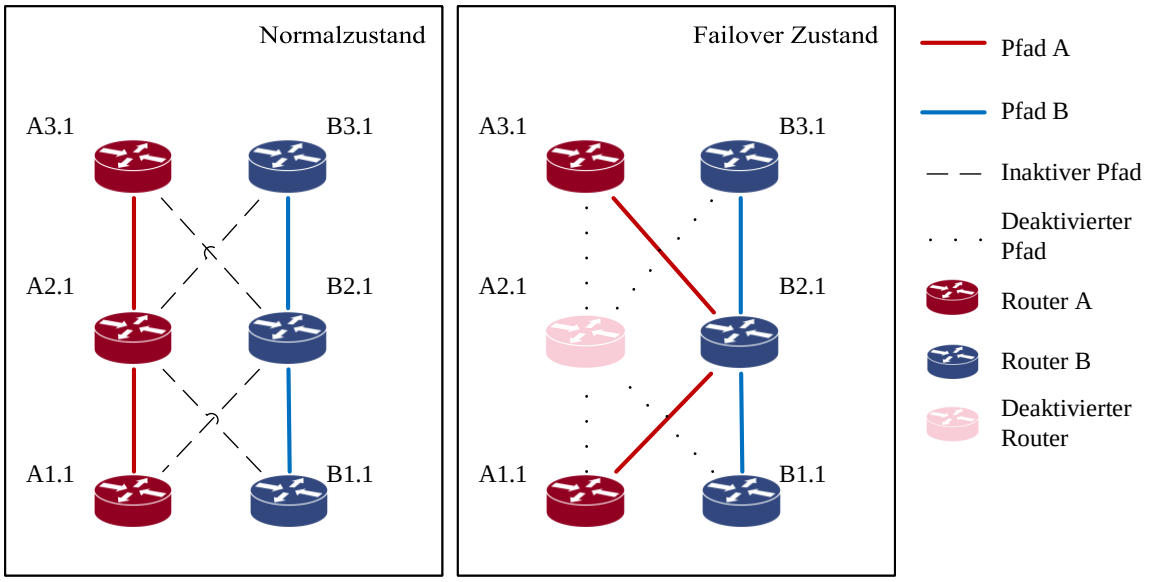


Abbildung 4.9: Duales Rollenkonzept für Dual-Path-Kommunikation in einer VXLAN-Fabric

IP-basierte Netzwerk, welches verschiedene Kommunikationspartner miteinander verbindet. Auffällig sind die vielen gestrichelten Netzwerkverbindungen, die ungenutzt vorhanden und nur im Fehlerfall in einem Dual-Path-Konzept genutzt werden können. Diese können zumindest von neutralem, grünem Datenverkehr genutzt werden, welche keinen Anspruch auf deterministische Pfade besitzen. Bei hohen Bandbreitenanforderungen an deterministische Kommunikation ist dies jedoch keine ausreichend zufriedenstellende Lösung.

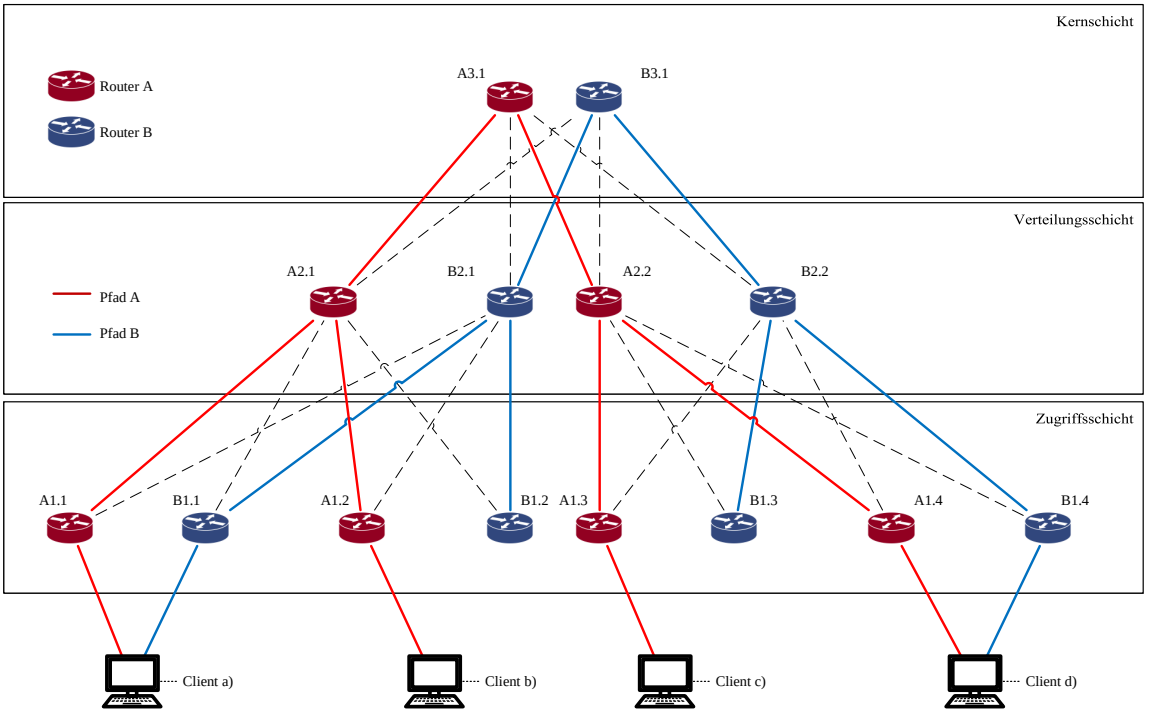


Abbildung 4.10: Multi-path Architektur für ein IP-basiertes Netzwerk

4.6.2.2 Quad-Path Architektur

Ein Blick auf die Abbildung 4.9 zeigt, dass inaktive Backup-Links nur von Kommunikation ohne Pfadanforderungen genutzt wird, während primäre Links insbesondere in Burst-Szenarien bereits unter Überlastung durch hochprioren Datenverkehr stehen können. Diese Beobachtung führt zu einer Erweiterung der vorgeschlagenen Architektur, die als Quad-Path-Routing-Architektur bezeichnet wird. Kommunikationsflüsse werden mit A/C für den roten Pfad und B/D für den blauen Pfad gekennzeichnet, welcher jeweils das erste Netzwerkgerät des Telegramms nach dem Client darstellt.

Jedes Netzwerkgerät besitzt zwei Rollen, die paketbezogene rote/blaue Rolle und die geradlinige/ungeradlinige Rolle, um die Last gleichmäßig zu verteilen. A.i.j bezeichnet den j-ten Router mit der roten Rolle in der Schicht i des Netzwerkes. Pakete werden auf die in Tabelle 4.3 beschriebene Weise weitergeleitet, um eine Lastverteilung zu erreichen und gleichzeitig Paketverlust durch Überlast im Falle eines ausgefallenen Routers zu vermeiden.

Das Umschalten in Failover-Szenarien kann nach der Erkennung einer fehlerhaften Verbindung oder eines fehlerhaften Knotens erfolgen. Der funktionierende Router enthält bereits die Information über den nächsten Hop für das Telegramm mit dem unterbrochenen Pfad im Forwarding Information Base (FIB). Wenn beispielsweise die Verbindung A1.1 -> A2.1 unterbrochen ist, verwendet Telegramm A den Pfad von Telegramm C.

Tabelle 4.3: Lastverteilung für Netzwerkgeräte verschiedener Schichten: Zugriff (1), Verteilung (2) und Kern (3)

Rolle	Schicht i	A zu A	A zu B
A	1,3	50%	50%
A	2	100%	0%
B	1,3	50%	50%
B	2	0%	100%

Abbildung 4.11 zeigt die Verbindungsauslastung für ein Standard- und ein Failover-Szenario. Im Vergleich zum Dual-Path-Konzept ist die Verbindungsauslastung für das Standard-Szenario um die Hälfte reduziert, während die Verbindungsauslastung im Failover-Szenario identisch ist.

4.7 Hochverfügbarkeit von echtzeitfähigen, zustandsbehafteten Applikationen

Nachdem das Netzwerk aufgrund von Redundanzmechanismen hochverfügbar konzipiert wurde, stellt sich nun die Frage nach Hochverfügbarkeit für Applikationen auf der Edge Cloud. Vor allem für die Applikation SPS, die zuvor unabhängig voneinander verteilt innerhalb der Automatisierungsebene verortet waren, führt die Konsolidierung auf einem verteilten System zu einer Vergrößerung der Störungsbereiche im Falle einer Störung. Aufgrund von leistungsstarker Serverhardware ist es möglich, mehrere vSPS auf einem Server zu betreiben. Deshalb ist ein Konzept notwendig, welches die Vorteile eines verteilten Systems nutzen

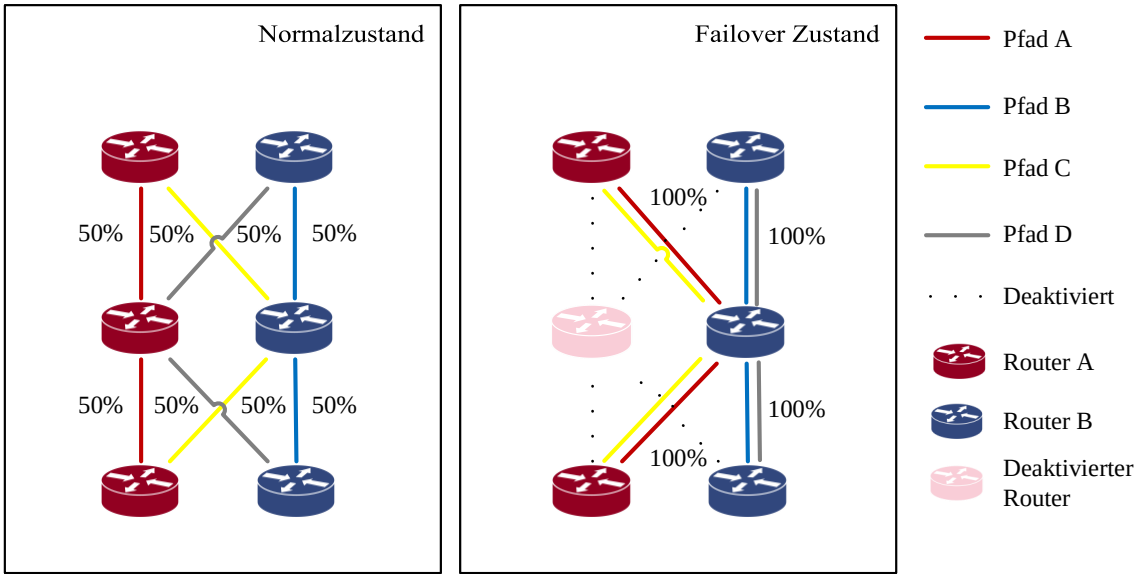


Abbildung 4.11: Quad-path Architektur für ein IP-basiertes Netzwerk

kann und in einem Lift-and-Shift Szenario einsetzbar ist.

Das generelle Konzept ist in Abbildung 4.12 dargestellt. Zwei Instanzen einer vSPS werden mit dem selben Programm auf unterschiedlichen Servern ausgeführt. Zustände der aktiven und Backup-Applikation werden über das IP-basierte Netzwerk synchronisiert. Im Falle eines Ausfalls der aktiven Applikation wird die Backup-Applikation aktiv und übernimmt dadurch die Steuerung der jeweiligen Prozessgeräte. Gleichzeitig wird eine neue Applikation auf einem anderen Server instanziiert, welche die Rolle des Backups einnimmt.

Kernstück des neuartigen Konzepts ist die Nutzung von RDMA im industriellen Umfeld zur Synchronisation der Zustandsvariablen. Dieses Protokoll ermöglicht das Überspringen jeglicher Zwischenschichten des Betriebssystems und greift ohne Nutzung des Prozessors direkt auf die Puffer der Netzwerkkarte zu. Zudem werden hardwarebasierte Funktionen der Netzwerkkarte genutzt um Daten zwischen RDMA-fähigen Geräten auszutauschen. Dies ermöglicht eine direkte Synchronisation ohne Zwischenspeichern der Daten und Hinzufügen von Headern in Software und führt damit zu deterministischem Verhalten bei der Synchronisation von Zuständen. Voraussetzung für die Nutzung des Konzeptes ist die Bereitstellung der RDMA-Funktionalität durch das Durchreichen eines physikalischen Netzwerkports oder die Virtualisierung der Netzwerkfunktionen, beispielsweise mittels Single-Root Input/Output-Virtualisierung (SR-IOV), Freeflow [Kim+19] oder MasQ [He+20].

4.7.1 Rollen-Verwaltung

Das Aktualisieren, Bestimmen und Halten der Rolle der aktuellen SPS-Instanz wird durch einen Rollen-Manager übernommen. Hierbei erfolgt beim Starten der SPS die Übergabe der dafür notwendigen Informationen durch Umgebungsvariablen. Die Übertragung der eigenen Rolle an weitere Instanzen einer SPS erfolgt zyklisch und kontinuierlich über UDP-basierte

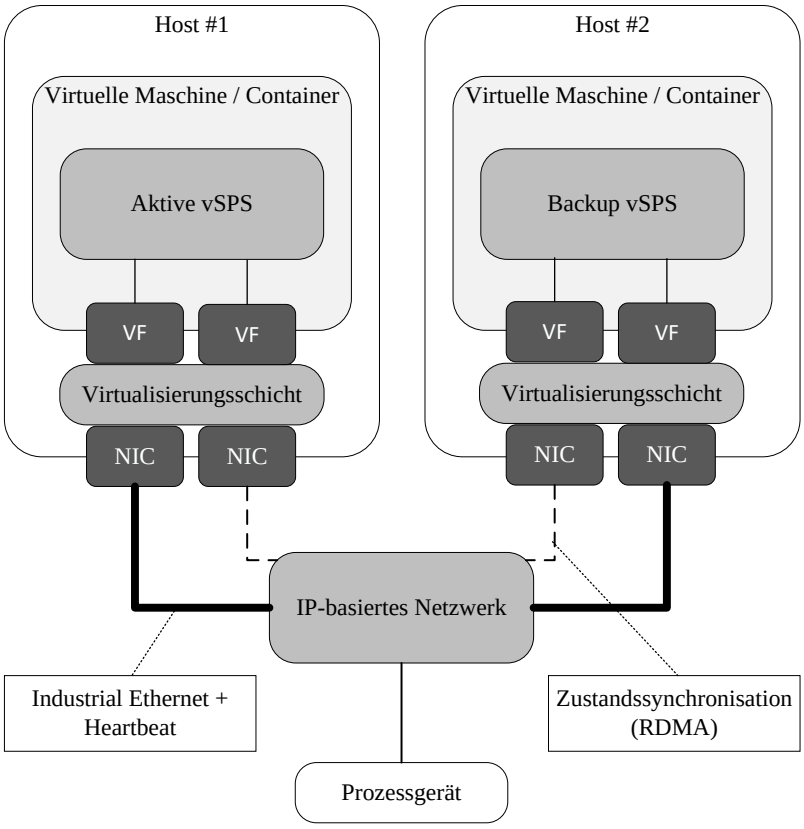


Abbildung 4.12: Detailbetrachtung der Kommunikationsbeziehungen zwischen den vSPS-Instanzen und den Prozessgeräten

Kommunikation durch Eingabe der IP-Adresse und Ports.

4.7.2 Zustands-Verwaltung

Die zu schützenden Ressourcen der Applikation sind die jeweiligen Zustandsvariablen. Diese werden von einem Zustands-Manager übermittelt und verwaltet. Da eine Minimierung des zu übertragenden Zustands die Dauer der Übertragung reduziert, erlaubt das Konzept zwei verschiedene Ansätze, eine vollständige und eine partielle Synchronisation. Abschließend stellt eine Submenge der Zustandsvariablen die Remanenzdaten dar, welche für ein schnelles Hochfahren des Prozesses nach einem unkontrollierten Stopp persistiert werden sollten.

4.7.3 Lösung des Split Brain-Problems

Innerhalb von verteilten Systemen kann vor allem bei der Anwendung von Hochverfügbarkeitskonzepten das Phänomen eines Split Brains auftreten. Sofern die Kommunikation zwischen primärer und Backup Applikation unterbrochen, die Kommunikation zum zu steuernden Prozessgerät jedoch jeweils noch vorhanden ist, geht die Backup-SPS fälschlicherweise in den aktiven Modus und versucht die Prozessgeräte zu steuern.

Hierzu gibt es neben einem Quorum die Möglichkeit, eine Witness oder einen Heartbeat zu nutzen [Le+15; Vog+98]. Ein Quorum erscheint hierbei als ungeeignet, da eine

ungerade Anzahl an Teilnehmern notwendig ist und dies mit erhöhter Komplexität, verlängerter Wartedauer auf einen konsistenten Zustand sowie erhöhte Ressourcennutzung und Lizenzgebühren verbunden ist. Als Witness könnte beispielsweise das zu steuernde Endgerät fungieren, welches sich in gewissen Ausführungen bereits mit mehreren Controllern parallel verbinden kann. Sobald der Watchdog Timer ausläuft, baut das Prozessgerät für gewöhnlich die Verbindung zu dem primären Gerät ab und ermöglicht das Koppeln mit einer neuen vSPS-Instanz. Abschließend ist die Nutzung eines Heartbeats denkbar, welcher auch heute in hardwarebasierten Lösungen genutzt wird. Hierbei müssen die Kommunikation zum jeweiligen Endgerät und der Heartbeat sowohl physikalisches Medium als auch Software-seitige Konfigurationen wie Routing und Subnetz teilen, um ein Split Brain-Szenario vermeiden zu können. Dies ist innerhalb des hier entwickelten Konzeptes die ausgewählte Lösung, welche in Abbildung 4.12 dargestellt ist.

4.7.3.1 Vollständige Synchronisation

Innerhalb eines Zyklus wird bei einer vollständigen Synchronisation der gesamte Zustandsspeicher synchronisiert. Dies geschieht unabhängig davon, ob sich Variablen seit der letzten Synchronisation geändert haben. Nachdem die zu synchronisierende Zustandsgröße einen direkten Einfluss auf die Übertragungsdauer hat, ist diese Art der Synchronisation nur für kleinere Datenmengen empfehlenswert. Bei einer größeren Menge an Daten kann trotz RDMA die Übertragung die gewünschte maximale Synchronisationszeit übertreffen, sodass das Konzept keine Anwendung finden könnte. Während die Anforderung abhängig von der Applikation und demnach nicht allgemein definierbar ist, bewegen sich SPS-Programmzeiten im Bereich von einstelligen bis zweistelligen Millisekunden. Aufgrund des gewünschten Einhaltens der Datenkonsistenz sollten die Berechnungen des nächsten Zyklus erst nach Abschluss der Zustandssynchronisation erfolgen.

4.7.3.2 Partielle Synchronisation

Sofern eine hohe zu synchronisierende Datenmenge vorliegt, ist eine Nutzung eines partiellen Synchronisationsmechanismusses empfehlenswert. Hierbei werden ausschließlich Zustandvariablen von der primären zur Backup-Applikation übertragen, die sich seit der letzten Übertragung geändert haben. Aufgrund der Tatsache, dass die Synchronisationsgeschwindgkeit unabhängig von der zu synchronisierenden Menge an Daten ist, reduziert dieser Mechanismus die Synchronisationszeit proportional zur Anzahl an ungeänderten Zustandsvariablen. Allerdings müssen jegliche Änderungen von Variablen vermerkt werden, was die Komplexität der Lösung erhöht.

4.7.4 RDMA über DetNet

Eine zentralisierte Steuerung der Synchronisierung mehrerer vSPS-Instanzen mit ihren jeweiligen Backup-Applikationen kann erforderlich sein, um Burst-Szenarien und hohe Raten an erneuter Versendung der Pakete zu vermeiden. Eine rein anwendungsgesteuerte

Synchronisierung ist aufgrund des Fehlens einer ganzheitlichen Sicht auf Netzwerk- und Host-Aktivitäten nicht wünschenswert. Ein möglicher Weg wäre hierbei die Nutzung von RDMA über DetNet, welches einen Kommunikationszeitplan über alle Synchronisationen erzeugt.

Aufgrund der Kompatibilität mit Ethernet sollte RoCE ohne Änderungen für jede beliebige Ethernet-basierte DetNet-Implementierung funktionieren, da es auf UDP als Transportprotokoll basiert. Die Priorisierung von RDMA gegenüber Verkehr mit niedrigerer Priorität erfolgt in der Regel durch die Verwendung der Prioritätsbits nach IEEE 802.1p.

4.8 IT/OT-Security

Die Verlagerung von ursprünglich im Anlagennetz verorteten Funktionen hat einen direkten Einfluss auf die Eigenschaften der IT/OT-Security. War es in der Vergangenheit möglich, autark und ohne Nord/Süd-Kommunikation Automatisierungsprozesse ablaufen zu lassen, ist nun aufgrund des neuartigen Konzeptes die Kommunikation in die Edge Cloud essenziell für das Funktionieren der Prozessgeräte. Der folgende Abschnitt führt daher in das neu-entwickelte ineinandergreifende IT/OT-Security-Konzept ein, um sowohl Automatisierungstechnik als auch IT-Applikationen gegen Bedrohungen in einem IT/OT-konvergierten Netzwerk zu schützen [KMG24]. Eine grobe Übersicht der Kommunikationsbeziehungen wird in Abbildung 4.13 gegeben. Hierbei liegt der Fokus des Konzeptes in der Kommunikation 1) zwischen Edge Cloud und Prozessgeräten über das IT/OT-konvergierte Netzwerk.

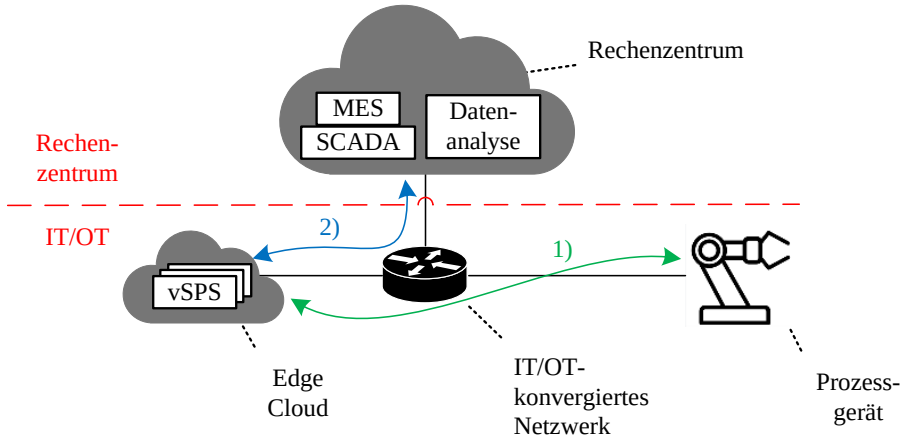


Abbildung 4.13: Kommunikationsbeziehungen in einem Edge Cloud-basierten Konzept mit einem IT/OT-konvergierten Netzwerk nach [KMG24].

Die Einführung einer Edge Cloud erzeugt verschiedene Herausforderungen. Geräte innerhalb der Automatisierungsdomäne werden nach Plug-and-Play Mechanismen in Betrieb genommen, verschlüsseln weder den Kommunikationsaufbau noch Datenaustausch und erwarten daher ein abgeschlossenes, lokales Netzwerk. Durch die Konvergenz von IT und OT sind nun Automatisierungsgeräte und /-kommunikationen klassischen Bedrohungen der IT ausgesetzt. Die OT-Domäne war aufgrund der Fokussierung auf Verfügbarkeit, Stabili-

tät und Einfachheit geprägt durch fehlende Innovationen und Anforderungen im Bereich der IT-Security. Außerdem sind Änderungen innerhalb von Prozessgeräten nur langjährig umsetzbar, da die Haltbarkeit hoch und der Innovationsfaktor gering ist.

Während dies ausschließlich als Nachteil gesehen werden kann, führt die Notwendigkeit der Härtung zu einer Steigerung des Schutzlevels innerhalb der Automatisierungstechnik und erlaubt das Design einer neuen Architektur nach bewährten Verfahren aus der IT kombiniert mit den Besonderheiten der OT. Auch heute schon ist das sogenannte Air Gap von Automatisierungsgeräten nicht mehr vorzufinden, da aufgrund von Kommunikation mit übergelagerten Systemen, 2) in Abbildung 4.13, das Abschirmen von Geräten häufig nicht gänzlich möglich ist. Aufgrund der Notwendigkeit für Brownfield-Integration und der Nutzung von Geräten ohne nennenswerte Härtung wird das Konzept Geräte-neutral ausgelegt.

Konzeptionell wird das DiD-Prinzip angewandt, in dem mehrere Maßnahmen das Schutzlevel multiplikativ erhöhen. Das Ansetzen von Maßnahmen kann an unterschiedlichen Stellen geschehen:

- Applikation
- Host
- Netzwerk
- Physikalisch

Die Netzwerkschicht ist hierbei eine mit dem vermutlich höchstem Potenzial für Maßnahmen im Kontext der IT/OT-Security. Zunächst bestehen IP-basierte Netzwerke aus COTS-Hardware, welche typischerweise alle fünf bis sieben Jahre gewechselt werden müssen, um die Verfügbarkeit hochzuhalten und Hilfsleistungen der Hersteller für die jeweiligen Geräte nutzen zu können. Durch den vergleichsweise kurzen Lebenszyklus, im Vergleich zu langjähriger Automatisierungshardware, gepaart mit dem Hinzufügen von Funktionen und Verbesserungen durch regelmäßige Softwareupdates stellen Netzwerkgeräte einen guten Träger für Innovationen dar. Des Weiteren sind im Rahmen der Adoption eines IT/OT-konvergierten Netzwerkes weitgehende Änderungen notwendig, um beispielsweise die Hochverfügbarkeit, den Determinismus oder die Kommunikation über Schicht 2 zu ermöglichen, sodass zur selben Zeit Anpassungen im Hinblick auf die IT/OT-Security durchgeführt werden können. Zudem bietet die Einführung eines Security-Konzeptes innerhalb des Netzwerkes eine Grundlage für weitere Maßnahmen in anderen Bereichen und erlaubt Endgeräten im ersten Schritt unverändert zu bleiben, sodass eine Brownfield-Integration ermöglicht wird. Das in der Folge weiter detaillierte Konzept soll eine Referenzarchitektur darstellen, die nach den jeweiligen Gegebenheiten angepasst werden kann.

Die einzelnen Elemente des entwickelten Konzeptes für die IT/OT-Security sind in Abbildung 4.14 dargestellt. Das System enthält sechs verschiedene Teilsysteme, Asset Management, daran anknüpfendes NAC, Mikrosegmentierung, Verschlüsselung, Stateful Packet Inspection (SPI) und IDS, sowie ein CERT. Hierbei ist entscheidend, dass die jeweiligen

Bausteine bewusst Abhängigkeiten zueinander besitzen und nicht ohne weiteres entfernt werden können. Zwar widerspricht dies dem Ansatz der Modularität, anderseits ermöglicht es eine einheitliche Architektur für IT- und OT-Security und führt zur Einhaltung der jeweiligen Prozesse. Dies wurde in der Vergangenheit innerhalb der Automatisierungstechnik aufgrund der Vereinfachung des Aufbaus oder Beschleunigung der Störungsbeseitung umgangen, auf Kosten von möglichen Schwachstellen.

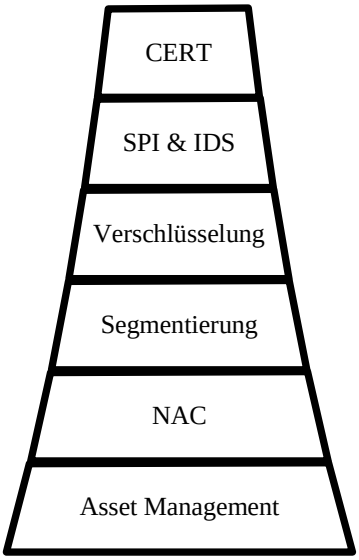


Abbildung 4.14: Elemente der netzwerkbasierten IT/OT-Security nach [KMG24].

4.8.1 Asset Management

Nach den Ausführungen über den Zero Trust-Ansatz in Abschnitt 3.6.1 sind Kenntnisse über jegliche Kommunikationspartner innerhalb des IT/OT-Netzwerks notwendig, um mögliche unerwünschte Kommunikationsteilnehmer innerhalb des Netzwerkes zu identifizieren. Die eindeutige Identifikation kann auf Basis mehrerer Eigenschaften erfolgen. Dazu zählen unter anderem eindeutige Seriennummern, MAC-Adressen, sowie Zertifikate. Neben der Identifikation von Assets sind auch installierte Applikationen und Infrastrukturelemente als auch Versionsnummern von Bedeutung, damit bei Bekanntwerden von Sicherheitslücken die betroffenen System effizient mit Updates versorgt werden können. Abschließend ist die physikalische Lokalisation von Bedeutung, beispielsweise der genutzte Netzwerkport oder das Fach im Ersatzteillager, damit diese Informationen im Falle eines Ausfalls oder Security-Vorfalls zielgerichtet ermittelt werden können.

4.8.2 Network Access Control

NAC beschreibt die Beschränkung von zu Kommunikation zugelassenen Kommunikationspartnern auf authentifizierte Instanzen auf Basis von Zertifikaten oder anderen einzigartigen Merkmalen. Der Industriestandard innerhalb der IT-Domäne erlaubt eine Authentisierung

mittels Zertifikaten basierend auf IEEE 802.1x. Hierbei enthalten Zertifikate Hostnamen, die ausschließlich von einer ausgewählten Certificate Authority (CA) ausgestellt wird. Automatisierungsgeräte hingegen besitzen für gewöhnlich keinen IEEE 802.1x-Client und sind demnach nicht in der Lage, eine zertifikatsbasierte Authentisierung durchzuführen. Daher sollte bei diesen Geräten einzigartige MAC-Adressen genutzt werden, um diese auf Basis der Informationen im Asset Management zu authentisieren.

Durch die Nutzung von NAC innerhalb des IT/OT-konvergierten Netzwerkes ergeben sich eine Vielzahl an Vorteilen:

- Unterbindung von Kommunikation nicht-authorisierter Kommunikationsteilnehmer
- Fehlende oder fehlerbehaftete Dokumentation von Assets innerhalb des Asset Managements wird geprüft, da sonst keine Kommunikation dieser Teilnehmer möglich ist
- Automatisierte Zuweisung von Netzwerken und anderen Eigenschaften wie gewünschten Mikrosegmenten
- Ermöglicht zielgerichtet die Beschränkung der Kommunikationen einzelner Teilnehmer

Die Authentisierung im OT-Bereich basiert hauptsächlich auf einem Benutzernamen und einem Kennwort. In der Praxis werden jedoch in der Regel einfache Benutzername/Kennwort-Kombinationen verwendet, die keine nennenswerte Herausforderung darstellen. Ohne die Durchsetzung strenger Kennwortrichtlinien und weiterer Maßnahmen werden Angreifer durch diese Hürden lediglich kurzzeitig vom Zugriff auf Endgeräte aufgehalten. Obwohl dies Teil der Host- oder Anwendungssicherheit ist, sind aufgrund der Effektivität von Passwortrichtlinien, Zwei-Faktor-Authentifizierung und der Integration von rollenbasierten Benutzerverwaltungen diese Maßnahmen für alle an das Netzwerk angebundenen Clients anzuwenden.

Weiterhin sind standardisierte und effiziente Prozesse für die Instandhaltung von Automatisierungstechnik relevant, damit beispielsweise im Falle von Hardwareänderungen die MAC-Adresse innerhalb des Asset Managements aktualisiert wird. Außerdem empfiehlt es sich, alle nicht identifizierten Geräte in eine Quarantäne-Zone zu bewegen, um daraufhin eine manuelle Administration zu ermöglichen.

4.8.3 Segmentierung

Dem DiD-Paradigma aus Abschnitt 3.6.2 folgend sieht das Konzept ein mehrschichtiges Segmentierungskonzept vor. Eine Makro-Segmentierung kann auf Basis von unterschiedlichen Ansätzen erfolgen. In absteigend feiner-werdenden Reihenfolge ist dies eine Separierung auf Hardware-Ebene, mittels getrennten Netzwerkkontrollebenen, sowie unter der Nutzung von Zonen auf Basis von VRF.

Innerhalb dieser Zonen können wiederum beispielsweise tausende Kommunikationsteilnehmer miteinander kommunizieren, sodass diese Art der Segmentierung nur für eine grobe

Teilung des Netzwerkes verwendbar ist. Die Segmentierung zwischen Broadcast-Domänen erfolgt auf Basis von VLANs. Eine weitere strenge Segmentierung wird durch die Entfernung des Gateways in einem Subnetz ermöglicht, sodass ausschließlich Geräte innerhalb dieses Subnetzes miteinander kommunizieren können. Dies ist gerade für industrielle Kommunikation vorzusehen, an deren Stellen kein Routing notwendig ist.

Eine feingranulare Segmentierung ermöglicht die Reduktion des notwendigen Datenverkehrs über eine Perimeter-Firewall und verringert somit die Anzahl an zu untersuchendem Datenverkehr. Dies wird im Abschnitt 4.8.5 näher erläutert. Firewalls, die zuvor die IT-Domäne von der OT-Umgebung getrennt hatten, werden durch gruppenbasierte ACLs ersetzt. Kommunikationsteilnehmer erhalten GBP, welche innerhalb des VXLAN propagiert werden und es ermöglichen, gruppenbasierte Kommunikationsrichtlinien zu definieren. Jeweilige Teilnehmer, die die selben Regeln teilen, werden innerhalb einer SG zusammengefasst.

Die Implementierung von Reihen- und Ring-Topologien, welche innerhalb der Automatisierungstechnik verbreitet sind, stellt eine zusätzliche Herausforderung für das Segmentierungskonzept dar. Die Anwendung der gruppenbasierten Kommunikationsrichtlinien ist hier wegen eines geteilten Netzwerkports von mehreren Endgeräten nicht trivial. Konzeptionell müssen deshalb bei Anwendung einer Reihen- oder Ring-Topologie Endgeräte zusammengefasst werden, zwischen denen keine Segmentierungsanforderungen bestehen und die der selben SG angehören. Der Punkt, an welchem die Regeln angewandt werden, sollte so nah wie möglich am Endgerät erfolgen, beispielsweise an einem IE-Switch oder der Zugriffsschicht des IP-basierten Netzwerks, um unnötige Last innerhalb des Netzwerkes zu vermeiden.

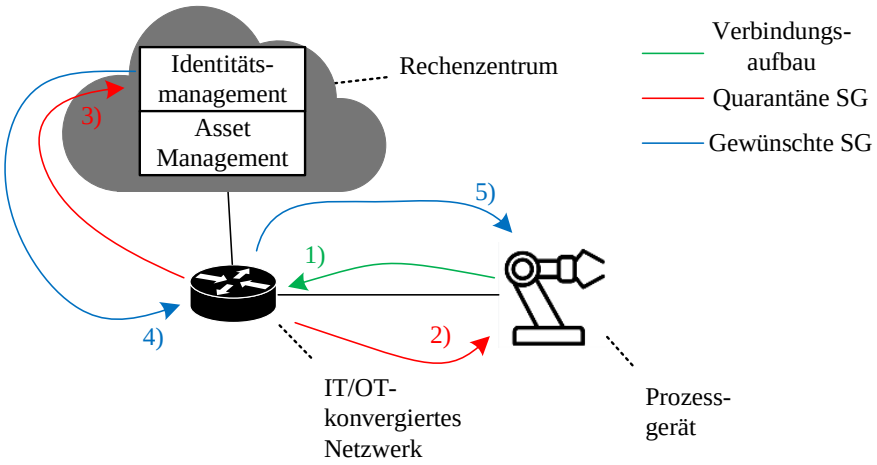


Abbildung 4.15: Ablauf der Authentifizierung und Netzwerkparametrierung für einzelne Clients.

4.8.3.1 Hierarchische gruppenbasierte Mikrosegmentierung

Werden IT-Security-Konzepte nicht ausreichend in Prozesse und Randbedingungen angepasst, werden diese in der Praxis aufgrund der Komplexität oder des erhöhten Verwaltungsaufwandes nicht genutzt und holistisch umgesetzt. Dies gilt vor allem für Bereiche mit einem

Fokus auf Produktivität und Verfügbarkeit. Wie in Abschnitt 3.6.3 dargestellt, sind die verfügbaren gruppenbasierten Segmentierungsschemata flach und eindimensional, was zu einem hohen Verwaltungsaufwand führt.

Daher wurde die hierarchische gruppenbasierte Mikrosegmentierung vorgeschlagen [KMG24]. Dieses Konzept erlaubt die Gruppierung von Gruppen nach einem Vererbungsmechanismus. Innerhalb einer nxn-Kommunikationstabelle, mit n äquivalent zu der Anzahl der verfügbaren SG, kann dadurch die Anzahl der zu beschreibenden Kommunikationsbeziehungen um ein Vielfaches reduziert werden. Beispielhaft stellt dies Abbildung 4.16 dar, in der SG 3.1 und 3.2 die selben erlaubten Kommunikationsbeziehungen zu anderen SG besitzen sollen. Die beiden SG könnten beispielsweise Automatisierungszellen darstellen, die nach außen hin mit den selben übergelagerten Systemen im Rechenzentrum sowie Applikationen auf der Edge Cloud kommunizieren müssen. Innerhalb der Hauptgruppe kann die eigentliche Kommunikation erneut spezifiziert werden. In diesem Beispiel wird der Einfachheit halber nur die Kommunikation innerhalb derselben SG erlaubt. Sofern die Infrastruktur bereits eine flache, gruppenbasierte Segmentierung, beispielsweise durch GBP in VXLAN, besitzt, ist das Hinzufügen der hierfür notwendigen Abstraktionsschicht trivial. Insbesondere in der OT-Domäne wird dadurch die Verwaltung von Regeln stark vereinfacht, da hier häufig mehrere Gruppen ähnliche Kommunikationsflüsse besitzen und dafür die jeweiligen identischen Berechtigungen benötigen.

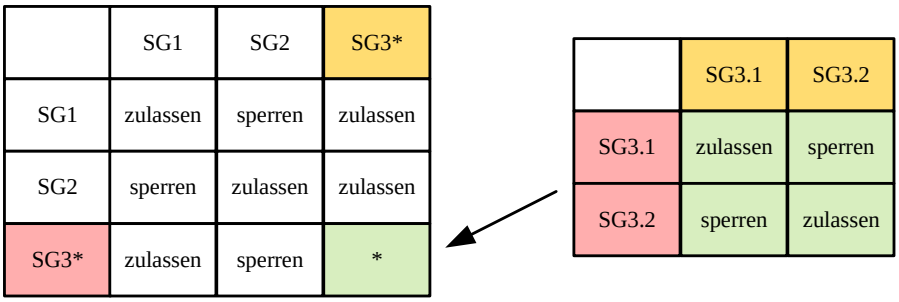


Abbildung 4.16: Vereinfachtes Management von SG durch hierarchische, gruppenbasierte Mikrosegmentierung nach [KMG24].

4.8.4 Verschlüsselung

In Abschnitt 2.3 wurde dargestellt, dass aktuell verfügbare IE-Standards keine Mechanismen für IT/OT-Security mit sich bringen. Dies ist insbesondere kritisch, da Änderungen von Daten direkten Einfluss auf die Physik und demnach beispielsweise die Produktqualität haben können. Hierbei ist nicht die Vertraulichkeit von Daten schützenswert, da sie ausschließlich für die jeweilige Automatisierungsbebauung hilfreich ist. Die Konsistenz von IE-Kommunikation hingegen gilt es sicherzustellen, da sonst Daten zwischen vSPS und Prozessgerät verändert werden könnten. Eine verbreitete Lösung, welche auch innerhalb von Hardware-Berechnungen durchführt und dadurch zu einer geringen Latenzerhöhung führt, ist MACsec, standardisiert in IEEE 802.1AE. Dieser Mechanismus ermöglicht eine effiziente Verschlüsselung und

schützt damit nicht nur die Vertraulichkeit, sondern auch die Konsistenz der Daten. Einen vielversprechenden Ansatz bietet auch PhySec, welcher im Vergleich zu MACsec allerdings nicht medienneutral ist und somit nicht auf kabelgebundene und kabellose Kommunikation gleichermaßen anwendbar ist, da bereits in der ersten Schicht des ISO/OSI-Referenzmodells die Kommunikation ver- und entschlüsselt wird. Auf Basis einer Literaturrecherche in Abschnitt 3.6.6 erscheint PhySec aufgrund der geringeren Latenzerhöhung im Vergleich zu MACsec langfristig zu bevorzugen, wobei eine Standardisierung noch nicht absehbar ist. Abschließend können an selber Stelle andere Mechanismen verwendet werden, beispielsweise die noch in der Standardisierung befindlichen PROFINET Security-Mechanismen, welche in der höchsten Klasse die Konsistenz der Daten sichern.

4.8.5 Zonenübergänge

Sofern Kommunikationspartner innerhalb von unterschiedlichen Zonen verortet sind, sieht das Konzept vor, diese Art der Kommunikation gesondert abzusichern. Inter-Zonenkommunikationen erlaubt die sogenannte Seitwärtsbewegung zwischen Bereichen, die es zwingend einzuschränken gilt, damit mögliche Angreifer ausschließlich in einer abgeschotteten Zone agieren und damit isoliert werden können. Konzeptionell gilt es, möglichst viele Zonen mit möglichst geringer Inter-Zonenkommunikation zu planen. Hierdurch werden sowohl mögliche kompromittierte Bereiche als auch der im besonderen Maße zu untersuchende Datenverkehr minimiert. Dabei ist es erwähnenswert, dass Inter-Mikrosegmentkommunikation innerhalb einer einzelnen Zone explizit nicht der selben Inspektion wie Inter-Zonenkommunikation unterzogen und stattdessen die zustandslose Segmentierung der Mikrosegmentierung genutzt wird.

Innerhalb des Zonenübergängen werden zwei grundlegende Mechanismen vorgesehen. Durch die Nutzung von SPI innerhalb einer Firewall kann nicht nur auf Basis von statischen Ports und IP-Adressen Kommunikationen eingeschränkt werden, wie dies in klassischen Firewalls der Fall ist, sondern auch auf Basis von erwarteten Zuständen und Verbindungsaufbauten. Ein Beispiel wäre hierfür, dass Thin Clients zu der jeweiligen Virtual Desktop Infrastructure (VDI) oder VM die Kommunikation aufbauen. Wird ein Aufbau in umgekehrter Richtung beobachtet, deutet dies auf einen unerwünschten Kommunikationsfluss hin. Die Informationen aus der SPI und weiteren Quellen können weiterhin einem IDS zugeführt werden, um mittels Detektion von Anomalien und verdächtigen Signaturen unerwünschten Datenverkehr zu erkennen. Erneut bewirkt die Minimierung von beobachteten Datenverkehr des IDS zu einer Verbesserung der Effektivität durch die Reduzierung des Grundrauschens von gewünschten Kommunikationsmustern.

Moderne Firewalls erlauben die Nutzung weiterer Mechanismen, beispielsweise die Nutzung eines IPS welches auf Basis eines IDS die Kommunikationenflüsse aktiv unterbricht. Das hier vorgestellte Konzept sieht jedoch die Nutzung eines CERT vor, welches Empfehlungen des IDS erhält und die Kommunikationsflüsse unterbindet. Diese Konzeptentscheidung resultiert aus der Kritikalität und der Neuheit der Kommunikationen innerhalb der Automatisierungstechnik über eine vergleichbare Infrastrukturkomponente. Sofern über einen

längeren Zeitraum die Empfehlungen des IPS keine nennenswerten negativen Auswirkungen gehabt hätten, kann weiterhin auf das automatisierte Blocken der Kommunikation gewechselt werden. Abschließend ist hier noch die WAF zu nennen, die vor allem für Interaktionen mit Geräten innerhalb des Internets einen erweiterten Schutz bietet.

4.8.6 Ineinandergreifende IT/OT-Security

In diesem Abschnitt wird beschrieben, wie sich jeder hinzugefügte Mechanismus positiv auf andere Mechanismen auswirkt und so die ineinandergreifende IT/OT-Security-Architektur ergänzt. Darüber hinaus werden drei verschiedene Kommunikationsmuster dargestellt und anhand den vorherigen Ausführungen diskutiert.

Tabelle 4.4 zeigt die beobachteten positiven Auswirkungen durch das Hinzufügen einzelner Maßnahmen. Aufgrund der Synergien zwischen den verschiedenen eingesetzten Mechanismen zeigt sich, dass das Hinzufügen zusätzlicher Maßnahmen einen multiplikativen Effekt auf das Security-Level hat und demnach einzelne Mechanismen nicht ohne Weiteres entfernt können. Dies widerspricht dem angestrebten Gestaltungsziel der Modularität, verbessert jedoch die Konsistenz der Lösung und vereinfacht die Administration in einem Bereich, der keine Fehler erlaubt.

Tabelle 4.4: Übersicht der ineinandergreifenden Multiplikatoreffekte der vorgeschlagenen Netzwerk-Sicherheitsmaßnahmen (+++ = ermöglicht, ++ = ergänzt und erweitert, + = teilt Gestaltungsziele) nach [KMG24]

	Asset Management	NAC	Mikrosegmentierung	Verschlüsselung	SPI / IDS
Asset Management	/	+++	+++	++	++
NAC	++	/	++	+	++
Mikrosegmentierung	+	++	/	+	+++
Verschlüsselung	++	++	++	/	/
SPI / IDS	++	/	++	/	/

Weiterhin stellt Abbildung 4.17 die Zielarchitektur dar. Teilnehmer des IT/OT-konvergierten Netzwerkes müssen innerhalb des Asset Managements gelistet und durch NAC authentifiziert werden, entweder auf Basis von Zertifikation durch IEEE 802.1x oder die jeweilige MAC-Adresse. Darauf erfolgt die Zuweisung des korrekten Netzwerkes und der SG. Die Kommunikation kann in drei verschiedene Arten unterteilt werden:

- Intra-Zonenkommunikation: Auf Basis eines Regelwerkes, welches erlaubte Kommunikationsbeziehungen zwischen SG innerhalb einer Zone enthält, werden Kommunikationsflüsse erlaubt. Vor allem echtzeitkritische Kommunikation, beispielsweise vSPS zu

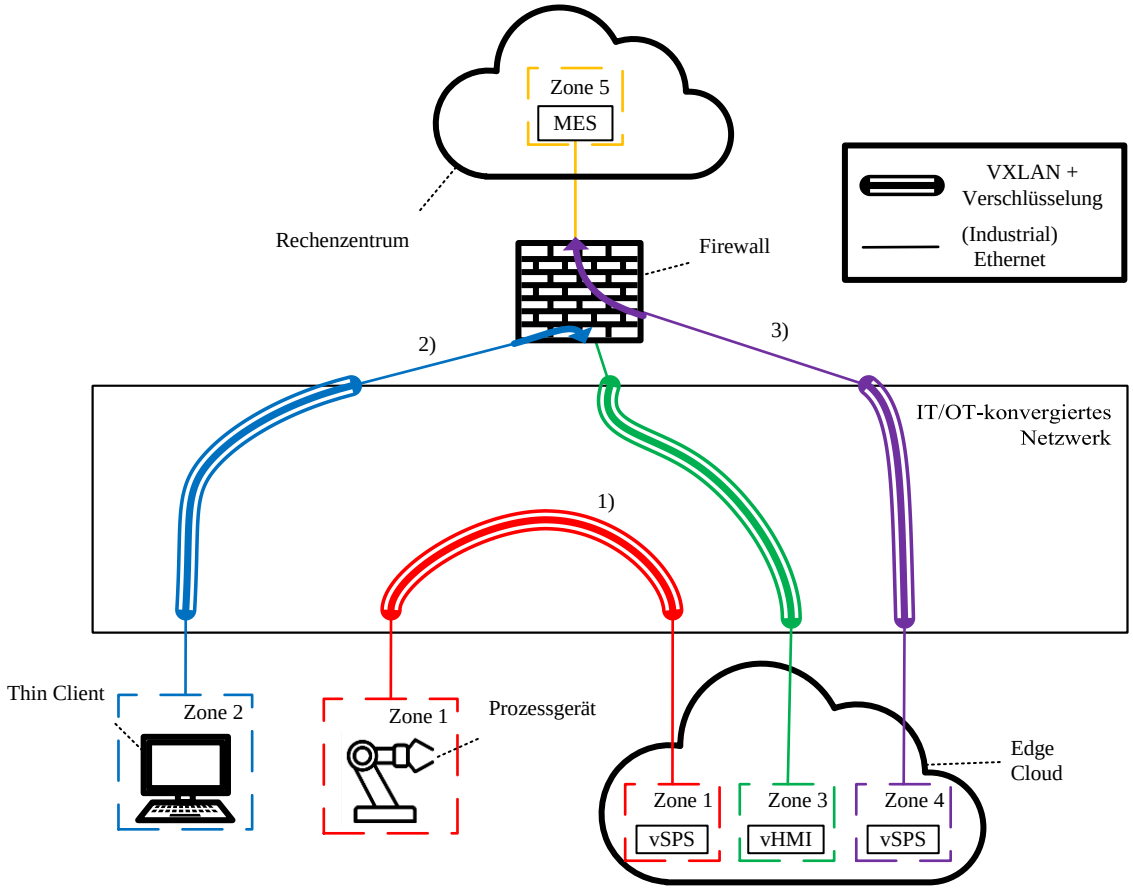


Abbildung 4.17: Das entwickelte IT/OT-Security-Konzept am Beispiel von 1) Intra-Zonenkommunikation, 2) Inter-Zonenkommunikation, 3) Inter-Domänenkommunikation nach [KMG24]

Prozessgerät-Kommunikation, sollte diese Art adoptieren, um den Determinismus der Kommunikation nicht zu verletzen.

- Inter-Zonenkommunikation: Hier wird die Kommunikation über eine Firewall mit SPI-/ und IDS-Funktionalität überprüft. Dadurch wird sichergestellt, dass eine Seitwärtsbewegung über Zonen hinweg detektiert werden kann.

- Inter-Domänenkommunikation: Nachdem auch weiterhin übergeordnete Systeme wie ein MES und SCADA innerhalb eines zentralisierten Rechenzentrums lokalisiert sind, muss die notwendige Nord/Süd-Kommunikation gesondert über Firewalls überwacht werden. Die Kommunikation über das Internet sollte hier vor allem mittels einer WAF abgesichert werden.

4.9 Fazit zum Architekturkonzept

Dieses Kapitel hat ein Architekturkonzept für deterministische Kommunikationsnetzwerke dargestellt, um die IT/OT-Konvergenz zu ermöglichen. Während verschiedene Konzepti-

deen und Teilaspekte bereits in der Literatur vorhanden sind, werden hier insbesondere die Realisierbarkeit der IT/OT-Konvergenz innerhalb der entwickelten Architektur in den Vordergrund gestellt und Abhängigkeiten beider Domänen holistisch betrachtet. Hierbei wurde auf Basis einer Anforderungsanalyse die Nutzung etablierter Standards mit neuartigen Konzepten in der Bereitstellung von Applikationen in der Automatisierungstechnik verbunden. Weiterhin wurden mögliche Nachteile durch die Virtualisierung in Form von neuartigen Hochverfügbarkeitsansätzen in IP-basierten Netzwerken und virtualisierten Applikationen aufgehoben und darüber hinaus Vorteile für eine Transition zu der vorgestellten Architektur geschaffen.

Die Bewertung erfolgt auf Basis der in Abschnitt 4.1 eingeführten Anforderungen an das Architekturkonzept sowie die in Abschnitt 4.3 beschriebenen Anforderungen an die jeweiligen Architekturbausteine.

Die Einführung der Edge Cloud vereinfacht die Aktualisierung von Anwendungen durch skalierbare Virtualisierungsansätze. Dazu können beispielhaft Golden Images für VM erstellt werden und bei Problemen nach Updates auf vorherige Versionen zurückgegriffen werden. Auch wird die Administration der virtuellen Anwendungen durch Cloud-basierte Tools stark vereinfacht und kann durch zentrale, feingranulare Rollen- und Rechtekonzepte besser geregelt werden, was wiederum zur Erhöhung der IT-Security beiträgt. Darüber hinaus basiert das Konzept auf COTS-Netzwerk- und Serverhardware. Dadurch wird die Interoperabilität mit typischen IT-Systemen durch die Plattform gewährleistet und ermöglicht bereits heute eine Adoption des Konzeptes. Der konsolidierte und einheitliche Ansatz der Rechenzentrumsinfrastruktur optimiert die Ressourcennutzung mittels Überprovisionierung von Hardware-Ressourcen. Dies gilt sowohl für die bisher verteilten Anwendungen in der Automatisierung als auch für die Netzwerkinfrastruktur, die für IT- und OT-Kommunikation genutzt wird.

Die systematische Herleitung von Anforderungen und deren korrespondierenden Konzeptansätzen vereinfachen die Verständlichkeit der Architektur. Weiterhin werden mehrere Ansätze für einen ausgewählten Architekturbaustein vorgestellt, was die Modularität des Konzepts verdeutlicht und verschiedene Kombinationen nach vorhandenen Rahmenbedingungen ermöglicht. Die Skalierbarkeit wird durch die Verwendung von etablierten Standards der IT erreicht, welche bereits in großen Umgebungen erfolgreich genutzt werden. Neu ist hierbei die Anwendung auf OT-Applikationen und die konsequente Konvergenz des Netzwerkes durch Adressierung von möglichen Unzulänglichkeiten. Die Validierung der jeweiligen Ansätze erfolgt im folgenden Kapitel 5. Abschließend ermöglicht die Nutzung von Software-basierten Mechanismen und kurzen Anwendungszyklen von IT-Geräten eine erhöhte Adaptivität der Architektur an veränderliche Rahmenbedingungen und Anforderungen. Auch werden hierdurch sowohl Greenfield- als auch Brownfield-Umsetzungen ermöglicht, sodass die Wahrscheinlichkeit einer Adoption und Wirtschaftlichkeit des Konzeptes erhöht wird.

Eine Hochverfügbarkeitslösung für Netzwerktechnik wurde basierend auf statischer Redundanz entwickelt und ermöglicht die notwendige Resilienz gegen unvorhergesehene Ausfälle,

wodurch auch das Vertrauen in das Konzept bei einer Umsetzung gesteigert wird. Erweitert wird diese durch das neuentwicklte Kommunikationsmuster Half&Half, welche eine Alternative zur Duplizierung von Paketen darstellt. Weiterhin wurden aufgrund der Notwendigkeit für redundante Pfade sowohl die Duplizierung der Netzwerkkontrollebene zum Schutz gegen Konfigurationsfehler als auch ein Konzept für die Nutzung einer einzigen VXLAN-basierten Fabric auf Basis eines neuartigen Pfadmechanismus dargestellt.

Des Weiteren wurde ein Konzept für die Realisierung von Hochverfügbarkeit von vSPS dargestellt. Dabei wurden die volle und partielle Synchronisation von Zuständen beschrieben. Weiterhin wurde die Notwendigkeit für RDMA über DetNet motiviert und erstmalig dargestellt, um auch in größeren Umgebungen die Konsistenz der Daten in vorhersagbarer Zeit zu garantieren und Performance-Einbußen von RDMA-basierten Netzwerken in Überlastszenarien zu reduzieren.

In Bezug auf IT/OT-Security wurde ein neuartiges, ineinandergreifendes Konzept dargestellt, um ein IT/OT-konvergiertes Netzwerk zu sichern und Edge Cloud-basierte Automatisierung zu ermöglichen. Hierbei wurden erneut dominanterweise verbreitete Standards der IT genutzt, da diese die Anforderungen beider Domänen erfüllen und als bewährte Mechanismen administrierbar und gehärtet sind. Erweitert wurden bestehende Mechanismen durch neue Konzepte wie ein hierarchisches gruppenbasiertes Segmentierungskonzept.

5 Evaluierung und Diskussion der Architekturbausteine

Kapitel 5 validiert das vorgeschlagene Architekturkonzept anhand von Versuchsaufbauten mit simulierten und realen Automatisierungsgeräten sowie repräsentativen Testszenarien. Dabei kommen auch verschiedene Hardware- und Softwarelösungen unterschiedlicher Hersteller zum Einsatz, die die benötigten Funktionalitäten enthalten.

5.1 Vorgehensweise

Um eine neutrale Bewertung der entwickelten Architekturbausteine zu ermöglichen, werden etablierte Methoden aus der Literatur herangezogen und die ermittelten Werte den Anforderungen aus Abschnitt 4.3 gegenübergestellt.

Auf Basis von VDE/VDI 2185 werden relevante Kenngrößen für die Beurteilung der Eignung des IT/OT-konvergierten Netzwerkes für industriellen Steuerungs-Datenverkehr ermittelt. Hierzu werden spezifische Testszenarien konstruiert, um Eigenschaften wie Latenzzeiten, Paketverlust und Jitter zu messen. Diese Testszenarien spiegeln realistische Betriebsbedingungen des Netzwerkes unter Last wider, wodurch die Eignung der angewandten Mechanismen bewertet werden kann.

Die Hochverfügbarkeit des Systems wird gegenüber Applikations- und Infrastruktureigenschaften untersucht. Hierbei werden in Anlehnung an eine Fehlermöglichkeits- und Einflussanalyse (FMEA) typische Fehlerszenarien beschrieben. Maßnahmen, die durch die Bausteine des Architekturkonzepts ergriffen werden, sollen sicherstellen, dass es zu keinem Ausfall kommt oder zumindest ein schneller Wiederanlauf der Prozesse ermöglicht wird. Diese Maßnahmen umfassen unter anderem die Implementierung redundanter Netzwerkpfade, die Nutzung von Failover-Mechanismen sowie die Sicherung von remanenten Prozessdaten.

Das IT/OT-Sicherheitskonzept wird auf Basis der Norm IEC 62443-3-3 evaluiert, der für industrielle Kommunikationsnetze einen Bewertungskatalog zur Einordnung des erreichten IT-Sicherheitsniveaus bereitstellt. Ergänzt wird dies durch eine Diskussion der wahrscheinlichsten Bedrohungen für industrielle Steuerungssysteme, herausgegeben vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI). Abschließend werden identifizierte Angriffsvektoren, die sich durch die Konvergenz von IT und OT ergeben, anhand des entwickelten Konzepts bewertet.

5.1.1 VDI/VDE 2185

Die VDI/VDE Richtlinie 2185 bietet eine eigentlich für funkgestützte Kommunikation entwickelte Methodik zur Analyse von Kommunikationsnetzwerken [Ver20]. Im Rahmen dieser Arbeit wird eine Teilmenge der in VDI/VDE 2185 eingeführten messbaren Parameter

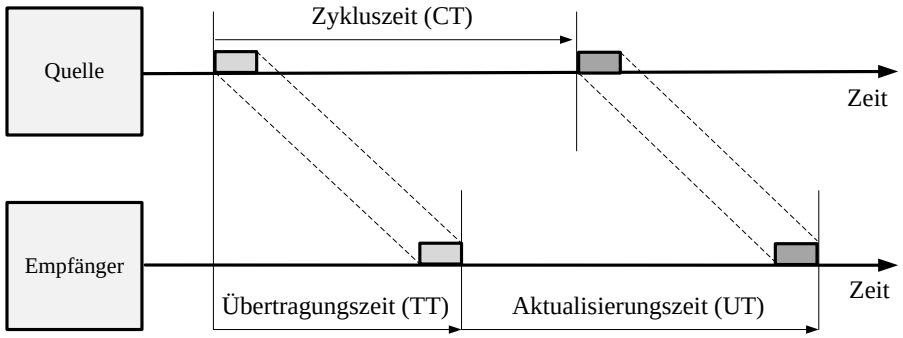


Abbildung 5.1: Darstellung von Netzwerkmetriken nach VDI/VDE 2185 [Ver20]

genutzt, um Aussagen über die Eigenschaften und Qualität von Kommunikationsnetzwerken zu ermöglichen. Die jeweiligen Metriken sind in Abbildung 5.1 dargestellt:

- Übertragungszeit (TT)
- Aktualisierungszeit (UT) für zyklische Anwendungen
- Paketverlustrate (PLR)

Neben diesen Parametern ist abschließend noch die Anzahl an vertauschten Telegrammen nennenswert. Dieser Parameter wird allerdings nebensächlich behandelt, da IE-Protokolle wie PROFINET Erkennungsmechanismen auf Basis einer Sequenznummer enthalten. Weiterhin ist aufgrund der definierten Rahmenbedingungen ein Vertauschen von Telegrammen nicht möglich, da ein neues Telegramm erst losgeschickt werden sollte, wenn das Vorhergehende bereits konsumiert wurde. Dies wird durch die maximale Übertragungszeit unter der Aktualisierungszeit erreicht, ein pünktliches Aussenden durch die Anwendung vorausgesetzt.

5.2 Kommunikation über IP

IE-Protokolle sind vor allem für die Verwendung in lokalen Schicht 2-Netzwerken konzipiert. Durch die Erweiterung der Kommunikation zu einer Edge Cloud-Instanz und der damit verbundenen Kommunikation über Schicht 3-Netzwerkgeräte und -Segmente ist eine Kapselung notwendig, um die jeweiligen IE-Telegramme zu übertragen. Nachdem in Abschnitt 4.4 konzeptionell das Protokoll VXLAN aufgrund der gewünschten IT/OT-Konvergenz und Skalierbarkeit der Architektur gewählt wurde, wird in diesem Abschnitt die Eignung für IE-Protokolle experimentell untersucht.

5.2.1 Versuchsaufbau

Die anschließenden Validierungen erfolgen mittels zwei Versuchsaufbauten von verschiedenen Herstellern von Netzwerkgeräten. Sie stellen jeweils ein repräsentatives dreischichtiges Netzwerk für ein IT/OT-konvergiertes Netzwerk in Bezug auf die verwendeten Bandbreiten und die Anzahl der Netzwerkschichten dar. Bei einem realen Ausbau dieser Infrastruktur

würde eine Skalierung durch das Hinzufügen von weiteren Netzwerkgeräten in der jeweiligen Schicht erfolgen.

Der Testaufbau a) nutzt ausschließlich Campus-Switche des Unternehmens Cisco Systems, Inc. der Catalyst 9000-Serie. Die jeweiligen Automatisierungsgeräte sind mit einem Cisco IE3400 verbunden, welcher einen industriellen Switch darstellt, der unter anderem die Protokolle PRP und PROFINET unterstützt. Jegliche Geräte werden hier in das gewünschte VLAN per Access-Port am IE3400 Switch zugeordnet. Eine VXLAN-Fabric wird mit LISP als Kontrollebenen-Protokoll und IS-IS als Interior Gateway Protocol (IGP) konfiguriert.

Im zweiten Versuchsaufbau werden Netzwerkgeräte des Unternehmens Juniper Networks, Inc. verwendet. Neben einem unterschiedlichen Betriebssystem, Junos OS, werden hier Rechenzentrums-Geräte genutzt, um eine VXLAN-Fabric aufzubauen. Weiterhin wird hier EVPN/BGP als Protokoll der Kontrollebene verwendet, welches sich vor allem durch Interoperabilität zwischen Herstellern und der Nutzung des weitverbreiteten Standards BGP auszeichnet.

5.2.2 Experimentelle Validierung

Die Validierung erfolgt unter der Nutzung der in Abschnitt 5.2.1 definierten Versuchsaufbauten. Obwohl sich das Protokoll der Kontrollebene unterscheidet, ist der Mechanismus der Kapselung identisch. Vereinfacht ist die Kapselung für beide Versuchsaufbauten mit VXLAN in Abbildung 5.2 dargestellt.

Beim Eintritt eines Telegramms in eine VXLAN-Fabric erfolgt am VTEP die Kapselung. Auf Basis der VID des zu kapsulierenden Telegramms wird das entsprechend konfigurierte VNI zugewiesen. Die Übertragung durch die Fabric erfolgt anschließend auf Basis klassischer Routing Mechanismen mittels des gewählten IGP.

Die durchgeführte Evaluierung mittels PROFINET und PROFIsafe ist erfolgreich. Dies schließt auch PROFINET-Discovery Protokoll (DCP)-Telegramme auf Basis von Schicht 2-Multicast ein. Hierdurch ist es somit möglich, die meisten Arten von Telegrammen durch ein IP-basiertes Netzwerk zu tunneln.

Diese Aussage gilt es jedoch zu differenzieren. Ausgewählte Protokolle wie das Link Layer Device Protocol (LLDP), das in IEEE-802.1AB standardisiert ist, werden in der Regel nicht zwischen virtuellen Instanzen in der Edge Cloud und Geräten in der Automatisierungszelle mittels VXLAN übertragen. LLDP-Telegramme und vergleichbare Protokolle werden am nächsten Netzwerk-Hop konsumiert, so dass es in diesem konkreten Beispiel für die Industriegeräte innerhalb der Automatisierungszelle den Anschein hat, dass keine physische Verbindung zu den virtuellen Instanzen vorhanden ist.

Dieses Szenario ist bereits in der Vergangenheit vor der Virtualisierung von Automatisierungsapplikationen aufgetreten, beispielsweise im Falle von PROFINET-Kommunikation über WLAN, was dort zu Änderungen am Standard geführt hat. Aus diesem Grund enthält der evaluierte Testaufbau a) ein Siemens ET200, welches mittels Gerätetausch auf Basis von PROFINET-basierten Mechanismen ersetzt werden soll.

Im Rahmen der Validierung zeigt sich, dass der Tausch des Gerätes mittels PROFINET-

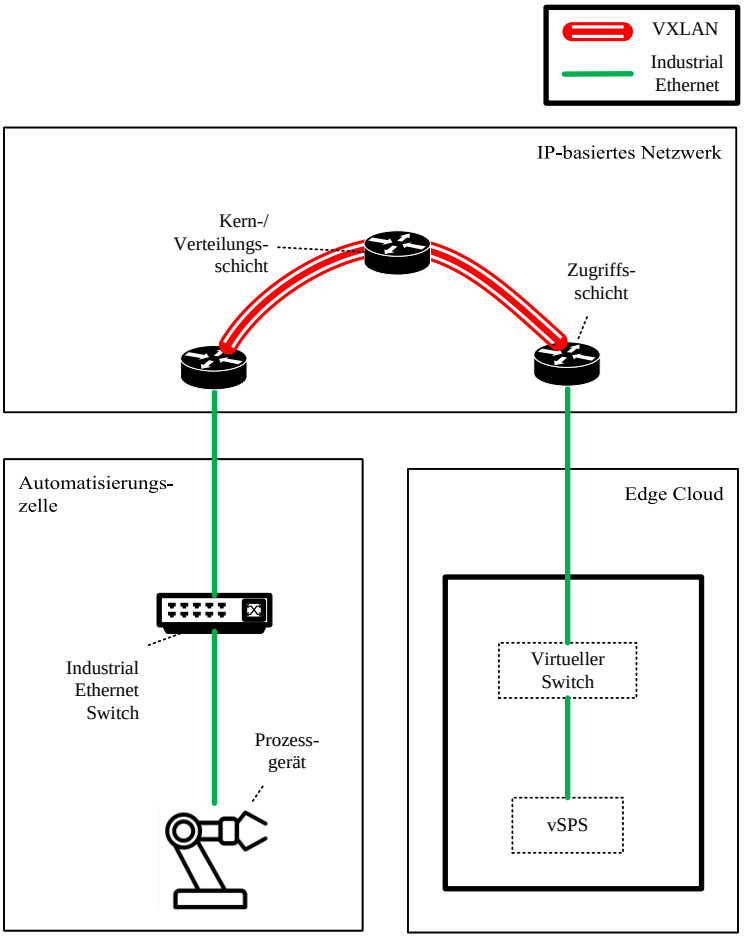


Abbildung 5.2: Schicht 2-Kommunikation über IP mittels VXLAN-Kapselung

Mechanismen auch weiterhin möglich ist, nachdem LLDP-Telegramme innerhalb der Automatisierungszelle weiterhin übertragen werden. Die fehlende LLDP-Kommunikation zwischen vSPS und dem Industrieswitch, an dem die vSPS innerhalb der Topologiesicht verbunden ist, hat demnach keinen Einfluss auf die Funktionalität.

Der zweite Versuchsaufbau mit Juniper-Switchen erlaubt das Tunneln von Schicht 2-Protokollen, die normalerweise am nächsten Netzwerk-Hop konsumiert werden würden [Jun24]. Das Tunneln von LLDP ist hier erfolgreich. Ein Tunneln dieser Art von Protokollen ist jedoch nur möglich, wenn Access-Ports an der Zugangsschicht der VXLAN-Fabric genutzt werden.

5.2.3 Diskussion

Tunnelprotokolle wie VXLAN ermöglichen die Übertragung von Schicht 2-basierten Datenverkehr über IP-basierte Netzwerke. Die Kommunikation zwischen vSPS-Instanzen von Siemens und CODESYS und PROFINET-Geräten über eine VXLAN-Fabric wird ermöglicht durch die Kapselung und Entkapselung sowie die Unterstützung für Schicht 2-Multicast.

Die Validierung verdeutlicht weiterhin, dass auch ohne eine LLDP-Kommunikation zu einer vSPS-Instanz auf einer Edge Cloud LLDP-basierte Mechanismen wie ein Gerätetausch im Fehlerfall weiterhin funktionieren. Somit stellt sich hier die Frage, ob diese Einschränkung auch in weiteren Standards akzeptiert werden sollte, um eine breite Akzeptanz des neuen Konzeptes sicherzustellen. Das Tunneln dieser Protokolle ist zwar auch möglich, wie die Validierung mittels Juniper-Switchen gezeigt hat, allerdings entstehen hierdurch erneut einige Design-Einschränkungen. Die zwingende Nutzung von Access-Ports und damit keine Nutzung von Trunk-Ports bedeutet, dass jede vSPS-Instanz einen dedizierten physikalischen Port auf dem Server für die IE-Kommunikation benötigt. Dies entspricht keiner skalierbaren Lösung und reduziert die Flexibilität, da Konfigurationen der Ports am Switch und Server simultan geändert werden müssen, sollte eine vSPS wegen geplanten oder ungeplanten Situationen zwischen Servern migriert werden.

Weiterhin kann VXLAN auch für klassische Office-Geräte genutzt werden um beispielsweise das Netzwerk dynamisch zu segmentieren. Diese Eigenschaft erlaubt eine Konvergenz zu einem gemeinsamen Netzwerk, in welchem sowohl industrielle als auch Enterprise-Applikationen in einem IP-basierten Netzwerk unterstützt werden.

5.3 Hochverfügbarkeit von Kommunikationsnetzwerken

Die Hochverfügbarkeit des Netzwerkes stellt eine zentrale Anforderung dar, nachdem vor allem Safety-relevante Applikationen auch bei kurzzeitigen Störungen bereits pausiert werden und somit die Verfügbarkeit des Prozesses reduziert wird. Weiterhin erhöht eine stabile Infrastruktur die Akzeptanz des Konzeptes.

Nach der in dem vorherigen Abschnitt 5.1.1 betrachteten VDI/VDE Richtlinie 2185 lässt sich die Verfügbarkeit A folgendermaßen berechnen:

$$A = 1 - \mathrm{PLR} \tag{5.1}$$

Hochverfügbarkeit wird demnach innerhalb des Kommunikationsnetzwerkes mit einer PLR unterhalb 0,00001% erreicht. Dies beschreibt jedoch nicht die Zuverlässigkeit der Applikation, welche beispielsweise im Falle eines PROFINET-basierten Systems bereits bei drei aufeinanderfolgenden verlorenen Telegrammen aufgrund des dadurch ausgelösten Kommunikationsabbaus zum Stillstand kommt. Sofern Safety-Applikationen genutzt werden, ist eine Quittierung der Busfehler durch menschliches Eingreifen und in Abhängigkeit des vorliegenden Szenarios weitere Schritte wie das Entfernen von Produktionsgütern sowie das Zurücksetzen von Robotern und Prozessen notwendig. Im Folgenden werden die einzelnen Teilaspekte evaluiert und Implementierungen detailliert vorgestellt.

5.3.1 Multi-Path Kommunikation durch eine Fabric

Das in Abschnitt 4.6.2.1 beschriebene Konzept mit mehreren Pfaden durch eine Fabric wird derzeit von den jeweiligen Netzwerkherstellern nicht unterstützt. Dies wird unter anderem

auch durch die Trennung des Overlays und Underlays nach dem Netzwerkvirtualisierungsansatz hervorgerufen. Informationen über den Eintritts- und Austrittspunkt eines Telegramms in einer Fabric wird innerhalb der Kontrollebene ausgetauscht. Der Weg zwischen dem Eintritts- und gewünschten Austrittspunkt der Fabric wird jedoch auf Basis des Underlays bestimmt, welches in der Entscheidungsfindung ausschließlich Routingprotokolle nutzt. Diese enthalten keine Kenntnisse über Informationen des Overlays, sodass die Auswahl des Pfades nicht ohne Implementierung innerhalb von Switchen möglich ist. Analog zum Dual-Path-Konzept ist auch das Quad-Path-Konzept nicht umsetzbar, solange nicht der Weg auf Basis der VNI-Zuweisung gewählt werden kann.

Auf einer theoretischen Ebene müssen die folgenden Punkte erfüllt sein, um mehrere Pfade durch eine VXLAN-Fabric zu ermöglichen:

- Erweiterung auf mehrere Underlays, die jeweils unterschiedliche Pfade durch das Netzwerk abbilden. Diese wählen auf Basis von Routingmetriken weiterhin primäre und Backup-Pfade, um im Fehlerfall umzuschalten.
- Die Wahl des Underlays erfolgt auf Basis des VNIs oder einer vergleichbaren für die jeweilige Netzwerkkomponente einzigartigen Eigenschaft der Kommunikationsbeziehung.
- Die identische MAC-Adresse muss an unterschiedlicher Stelle des Netzwerkes in dem selben VLAN simultan möglich sein, wobei die Kommunikation untereinander unterbunden wird.

5.3.2 Dual-Fabric Konzept

Als alternative Lösung werden in dem folgenden Abschnitt zwei VXLAN-Fabrics genutzt, um die Übertragung der beiden Kommunikationsströme zu ermöglichen. Dies erfüllt die Notwendigkeit von getrennten Underlays, ermöglicht die mehrfache Nutzung der selben MAC-Adresse und benötigt keine Auswahl des Underlays, da die jeweilige Netzwerkkomponente nur Teil eines Underlays ist. Bei diesem Konzept gilt es jedoch auch zu beachten, dass die Nord/Süd-Kommunikation für einen ausgewählten Kommunikationsteilnehmer nur in einer Fabric erfolgen darf, da sonst aufgrund der selben Adresse hinter zwei Netzwerkbereichen die Gefahr für Routingschleifen besteht. Die Dopplung der Kontrollebene bietet allerdings auch den Vorteil, Konfigurationsfehler und Softwareprobleme abzufangen.

Abbildung 5.3 stellt einen beispielhaften Versuchsaufbau eines Dual-Fabric Konzeptes dar. Die jeweiligen Server, die einen Bestandteil der Edge Cloud darstellen, sind mit Cisco Catalyst 9500 Switchen verbunden. Diese Switche sind Teil der Fabric und führen die Kapselung von IE-Telegrammen mittels VXLAN durch. Daraufhin erfolgt, unter gleichzeitiger Priorisierung mittels QoS, die Übertragung der Pakete durch die Fabric. Am Austrittspunkt, den Cisco Catalyst 9300 Switchen, erfolgt die Dekapselung und die Übertragung an den Cisco IE3400, an dem die jeweiligen Prozessgeräte hängen. Die Nutzung der beiden Pfade kann über mehrere Protokolle erfolgen, die eine unterbrechungsfreie Kommunikation ermöglichen.

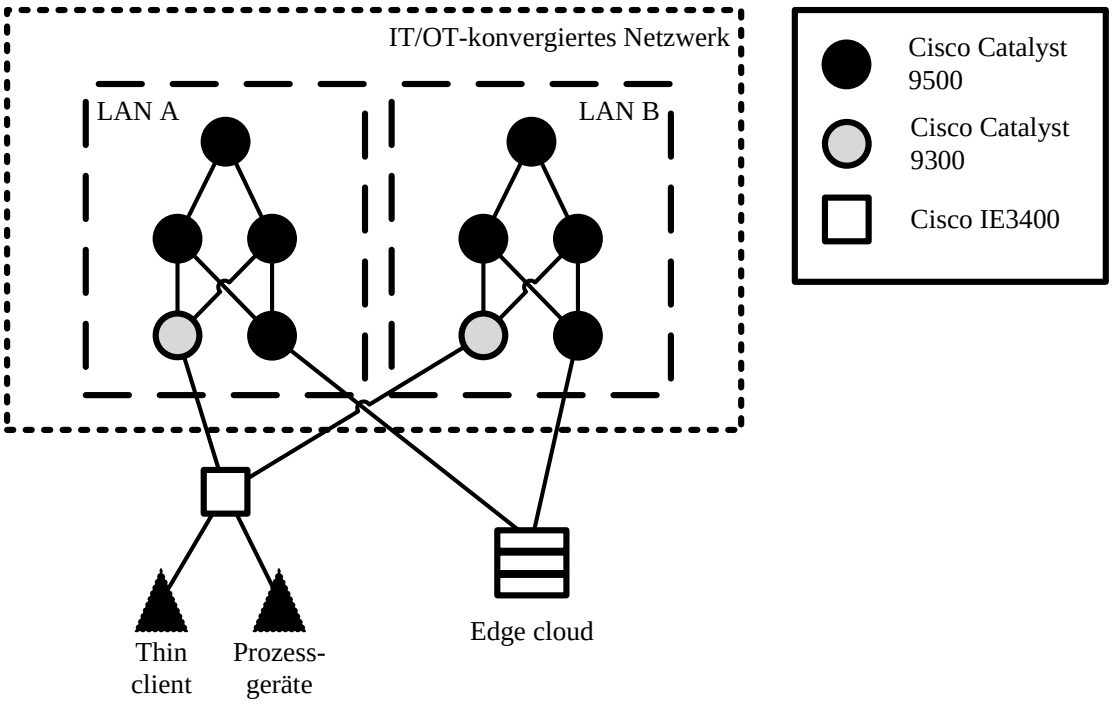


Abbildung 5.3: Validierung des Ende-zu-Ende Konzeptes für Hochverfügbarkeit mittels eines Dual-Fabric Konzeptes nach [KMG22]

5.3.3 Duplizierung mittels PRP

Paketduplizierung stellt einen statischen Mechanismus zur Erreichung von hochverfügbaren Kommunikationsnetzwerken dar. Aufgrund der Verbreitung von PRP im industriellen Umfeld unterstützt auch der Cisco IE3400 in Abbildung 5.3 diesen Standard. Hier werden die von Prozessgeräten versendeten IE-Telegramme dupliziert und mit einem PRP-Trailer versehen.

Nach der Übertragung durch die beiden VXLAN-Fabrics erfolgt der Eintritt in die Edge Cloud und das Erreichen des Industrial virtual Switch (IvS). Dieser wurde im Rahmen der gemeinsamen Entwicklung mit Broadcom Ltd. um die PRP-Funktionalität erweitert, sodass der IvS, unter Einhaltung der notwendigen Determinismusanforderungen, die Telegramme dedupliziert und letztlich an die gewünschte Applikation weiterleitet. Umgekehrt werden in Anlehnung an den Cisco IE3400 Telegramme in ausgehender Richtung dupliziert und mit dem PRP-Trailer markiert.

Kommunikationsbeziehungen, die keine Paketduplizierung benötigen, können auch weiterhin hinter den jeweiligen PRP-Duplizierungsknoten liegen. Die hierfür notwendige SAN-Markierung wird in Tabellen in beiden Knoten hinterlegt. Somit kann beispielsweise eine Kommunikation zwischen dem Thin Client im Shopfloor und einer HMI-Instanz auf der Edge Cloud ohne Duplizierung der Telegramme erfolgen. Dies reduziert die genutzte Bandbreite und benötigten Ressourcen für die PRP-Funktionalität. Gleichzeitig ist ein Wechseln der Netzwerke, beispielsweise bei einem Ausfall einer Fabric, auch für SAN möglich.

5.3.3.1 Validierung

Die Validierung erfolgt auf qualitative Weise, indem vSPS-Instanzen mit einem Watchdog-Timer (WDT) von 3 Millisekunden mit ihren jeweiligen Prozessgeräten auf Basis von PROFINET kommunizieren. Hierzu wird der Dual-Fabric Testaufbau, welcher in Abbildung 5.4 dargestellt ist, verwendet. Dabei wird jeweils nur ein Fehlerfall gleichzeitig erzeugt und beispielhaft werden einige Fehlerszenarien dargestellt. Zur Validierung des Konzeptes für echtzeitkritische Applikationen werden hierzu beispielsweise sequenziell jegliche Verbindungen zwischen Netzwerkkomponenten als auch Stromverbindungen zu Netzwerkkomponenten entfernt. Dies schließt beispielsweise die Verbindung der Edge Cloud mit LAN A in Ausfall #1, oder die Verbindung des IE-Switches mit LAN B im Ausfallszenario #2 ein. Neben Verbindungen zwischen Netzwerkkomponenten werden auch die Stromversorgungen der einzelnen Schichten und Fabric-Rollen in Ausfallenszenarien #3 - #5 entfernt, beispielsweise des Cisco Catalyst 9300 oder der Cisco Catalyst 9500-Komponenten. Abschließend werden auch komplette VXLAN-Fabrics, nach dem PRP-Vokabular mit LAN A und LAN B bezeichnet, sequenziell in Ausfallszenario #6 abgeschaltet.

Im Rahmen aller Ausfallszenarien konnten aufgrund der statischen Redundanz durch PRP keine PROFINET-Alarme in vSPS-Instanzen festgestellt werden.

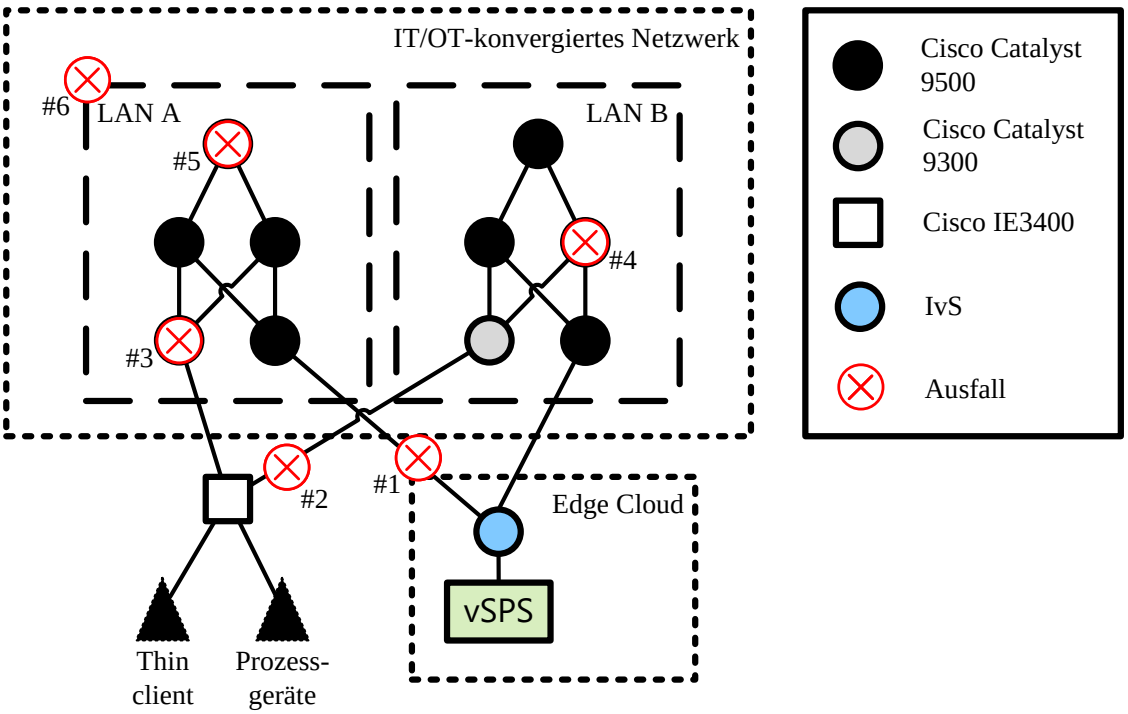


Abbildung 5.4: Validierung des PRP-basierten Redundanzkonzeptes in verschiedenen Ausfallszenarien.

5.3.3.2 Bewertung

Die Nutzung von einer Fabric für zwei oder mehrere Pfade wird lediglich theoretisch beschrieben. Eine Implementierung benötigt Anpassungen an der Software und gegebenenfalls Hardware der jeweiligen Netzwerkgerätehersteller. Dennoch bietet das vorgestellte Konzept eine Implementierungshilfe und Diskussionsgrundlagen für Anpassungen von Netzwerkstandards.

Die Verwendung von zwei Fabrics zur Erreichung mehrere Pfade erfordert eine erhöhte Anzahl an Hardwarekomponenten. Weiterhin wird die Komplexität durch das notwendige synchrone Management zweier getrennter Netzwerkinfrastrukturen erhöht. Gleichzeitig können jedoch Probleme innerhalb einer Fabric kompensiert werden. Nachdem Konfigurationsfehler und Software-Probleme nicht vollständig zu eliminieren sind, bietet diese Lösung erhöhte Resilienz gegenüber einer Vielzahl an Fehlerzuständen, insbesondere Problemen innerhalb der Kontrollebene [Gov+16; Kri+22].

PRP als Redundanzprotokoll erfüllt die Erwartungen und konnte durch die Erweiterung der Funktionalität in dem IvS auch in den virtuellen Raum erweitert werden, sodass selbst Probleme mit Netzwerkkarten durch die Zuweisung verschiedener Netzwerkports auf unterschiedlichen Karten keinen Einfluss auf die Verfügbarkeit des Gesamtsystems besitzen. Allerdings wird durch Paketduplizierung sowohl die Komplexität erhöht als auch die notwendige Bandbreite verdoppelt. Diese ist jedoch im Falle von Steuerungs-Datenverkehr im Vergleich zu IT-Applikationen gering.

Im virtuellen Raum erfüllt der IvS damit die Verfügbarkeitsanforderungen und erlaubt die Skalierung des Systems durch das Betreiben von mehreren vSPS-Instanzen auf einem physikalischen Host als auch die Verschiebung im Fehler- und Wartungsfall.

5.3.4 Half&Half

Als Alternative zur Redundanz mittels Paketduplizierung wird im Folgenden ein neuartiges Konzept zur Erreichung der notwendigen Resilienz im Fehlerfall innerhalb des Netzwerkes validiert.

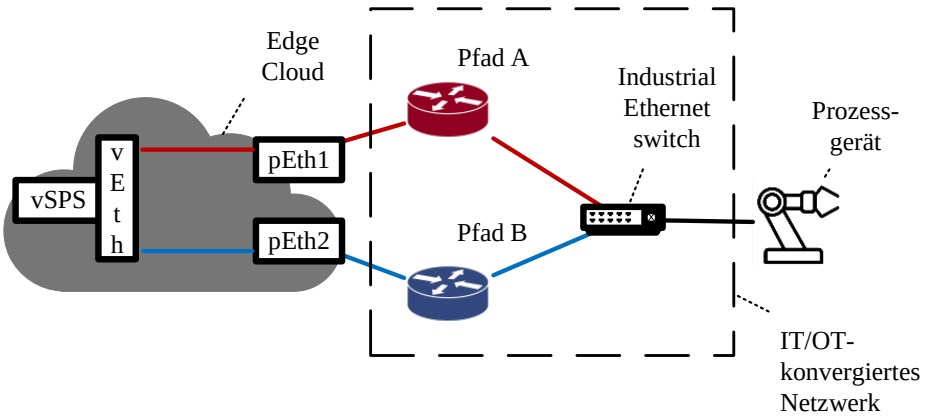


Abbildung 5.5: Geplantes Konzept für die Bereitstellung mit programmierbaren IE-Switchen und Pfadauswahl-Logik in der Edge-Cloud für eine vSPS nach [KG23b].

Ein Implementierungskonzept ist in Abbildung 5.5 dargestellt und betrachtet beispielhaft die Kommunikation zwischen SPS und Prozessgerät. Daten werden von der vSPS an eine Virtuelle Ethernet-Schnittstelle (vEth) gesendet. Beim Ausgang von vEth werden Echtzeitdatenpakete abwechselnd an die Physische Ethernet-Schnittstellen (pEth) pEth1 und pEth2 weitergeleitet. In den Host eintretender für die vSPS bestimmter Datenverkehr wird über die pEth empfangen und an die virtuelle Schnittstelle vEth weitergeleitet.

Eine Echtzeitimplementierung kann durch den Einsatz des Extended Berkeley Packet Filters (eBPF) realisiert werden [Vie+20]. In den vergangenen Jahren stieg die Nutzung von eBPF aufgrund dessen starken Fokus auf Performance, Flexibilität und Sicherheit [Gba+24]. Generell ermöglicht eBPF die dynamische Programmierung des Linux-Kernels. Die Umleitung von Paketen zu anderen Schnittstellen ist durch die Redirect-Funktionalität in eBPF und eXpress Data Path (XDP) möglich. Durch die Erweiterung mittels XDP kann die Performance weiter verbessert werden, indem Funktionalitäten auf Teilen der Netzwerkkarten-Hardware genutzt werden. Alternativ könnten bestehende Standards wie ECMP so angepasst werden, dass Pakete zwischen den Netzwerken A und B alternieren.

Die Funktionalität der Pfadauswahl, die als Client-seitige Implementierung vorgesehen ist, stellt vor dem Hintergrund der Brownfield-Anforderung eine Schwierigkeit dar. Viele Geräte, insbesondere in der Automatisierungstechnik, unterstützen nachträglich eine derartige Anpassung nicht, weshalb eine Implementierung am ersten Netzwerk-Knotenpunkt, also am Zugriffs- oder Industrieswitch, erforderlich wird. Die Programmierbarkeit der Datenebene mittels P4 oder OpenFlow könnte die erforderliche Funktionalität auf deterministische Weise bereitstellen, ohne Anpassungen an dem ASIC vorzunehmen.

5.3.4.1 Validierung

Der folgende Abschnitt validiert die Anwendbarkeit des Half&Half Konzeptes für PROFINET und EtherNet/IP und diskutiert die Ergebnisse.

Das Verhalten von IE-Geräten bei kontinuierlichem 50-prozentigen Paketverlust ist unklar und wird in diesem Abschnitt experimentell überprüft. Theoretisch sollte der WDT von PROFINET- und EtherNet/IP-Geräten nicht ausgelöst werden, wenn jedes zweite Paket verworfen wird, da der WDT mindestens das Dreifache der Zykluszeit (CT) darstellt, was den Verlust von zwei aufeinanderfolgenden Telegrammen erlaubt.

Es werden CODESYS-Laufzeitumgebung als SPS und E/A auf zwei unterschiedlichen Hosts genutzt, die direkt über eine einzelne Netzwerkverbindung miteinander verbunden sind. Um den Ausfall eines einzelnen Netzwerkes, Netzwerk A oder B, zu emulieren, verwirft ein entwickeltes XDP-basiertes Programm abwechselnd die Hälfte der eingehenden IE-Telegramme, wenn die Zieladresse mit der gewünschten MAC-Adresse im Header vorhanden ist. Der Zustand der vorherigen Aktion, Verwerfen oder Weiterleiten, wird in einer eBPF Schlüssel-Werte-Datenbank, BPF-Map, gespeichert. Telegramme werden mit der Funktion XDP_DROP verworfen [Vie+20]. Ausschnitte des implementierten Codes befinden sich in Abschnitt A.5.

Der beobachtete Paketverlust in der durchgeführten Validierung entspricht den erwarteten

50% in einem EtherNet/IP-SPS-Programm mit $WDT = 4 \times CT$. Auf der SPS-Seite wird ein Zähler inkrementiert und der Wert an den Eingang des E/A geschrieben. Da der Wert innerhalb jedes Telegramms um eins erhöht wird, wird ein Paketverlust erkannt, wenn der Wert auf der E/A-Seite um mehr als eins erhöht wird. Die gleiche Methode wird auf der SPS-Seite angewendet. Alternativ kann der Paketverlust innerhalb des XDP-Programms beobachtet werden. Es wurden während der gesamten Testszenarien keine WDT-Alarme ausgelöst.

Eine ähnliche Validierung wird mit PROFINET RT durchgeführt, hier mit $WDT = 3 \times CT$. Erneut wird ein Versuchsaufbau analog zu der Validierung von EtherNet/IP genutzt. Ein inkrementierender Zähler wird verwendet, um den Paketverlust zu messen. Die Aktivierung des XDP-basierten Paketverlust-Programms löst während der gesamten Testszenarien keine WDT-Alarme aus, da nur ein Telegramm in Folge verloren geht.

5.3.4.2 Diskussion und Bewertung

Aufgrund der überfrequenten Kommunikationsschemata der validierten IE-Protokolle PROFINET und EtherNet/IP und ihrer Resilienz gegenüber einem oder sogar zwei verlorenen Telegramme in Folge wird die Funktionalität des Prozesses durch einen kontinuierlichen 50-prozentigen Paketverlust nicht beeinträchtigt, solange nicht drei oder mehr Pakete in Folge verloren gehen. Dies bestätigt die Anwendbarkeit von Half&Half für Anwendungsfälle, die eine Toleranz gegenüber einzelne verlorene Pakete aufweisen. Half&Half kann durch eine Reihe weiterer Konzepte, beispielsweise dynamischen Failover-Mechanismen, ergänzt werden, um die Dauer des 50-prozentigen Paketverlustes zu reduzieren. Der 50-prozentige Verlust an Telegrammen könnte weiterhin durch die Nutzung von mehr als zwei Pfaden reduziert werden, wobei der Paketverlust umgekehrt proportional zur Anzahl der beteiligten Pfade skaliert. Der damit verbundene notwendige Speicher des Zustands in den jeweiligen Geräten, die den Pfad auswählen, bleibt dabei sehr gering. Allerdings könnten die Netzwerkgeräte zwischen den Pfadselektoren größere Weiterleitungstabellen speichern müssen, abhängig von der verwendeten Technologie. Schließlich ist auch eine komplexere Auswahl-Logik möglich. Diese sollte jedoch aus expliziten Gründen gewählt werden, beispielsweise bei Überlastung eines der beteiligten Pfade.

Das vorgeschlagene Konzept vereint die Stärken mehrerer Resilienzkonzepte mit neuartigen Eigenschaften. Half&Half erfüllt die notwendigen Hochverfügbarkeitsanforderungen, während Bandbreiten- und Stromverbrauch sowie die Komplexität auf der Empfängerseite vergleichbar mit dem Single-Path-Routing sind. Im Vergleich zur Paketduplizierung wird die Notwendigkeit entfernt, ankommende Duplikate auf der Empfängerseite zu verfolgen. Weiterhin wird eine deterministisches Intra-Flow Lastverteilung ermöglicht, das insbesondere für industrielle Automatisierungsnetzwerke aufgrund der geringen verfügbaren Bandbreite Anwendung finden könnte. Zwar existieren bereits eine Vielzahl an Standards, die eine Lastverteilung auf mehreren Pfaden erlauben, allerdings keine für einen einzigen Datenstrom [Li+16].

Weiterhin ist nun ein variabler Mechanismus möglich, welcher ein Umschalten zwi-

schen den einzelnen Betriebsmodi auf Basis von beobachteten Netzwerkmetriken ermöglicht, beispielsweise erhöhte Übertragungszeiten, Paketverlust und Jitter. Eine Wahl des Betriebsmodus sollte hierbei auf Basis der Kritikalität der Kommunikation für die jeweilige Anwendung erfolgen. Beispielsweise empfiehlt sich die Verwendung von Single-Path Kommunikation für eine Standard-TCP-Verbindung, Half&Half für die zyklische Kommunikation von IE und Paketduplizierung für sicherheitsrelevante Telegramme oder Alarme.

An dieser Stelle zeigt sich abschließend die Schwierigkeit der Definition von Hochverfügbarkeit nach VDI/VDE 2185. Obwohl im Fehlerfall die Verfügbarkeit auf 50% reduziert wird, bleibt die Verfügbarkeit der IE-Applikation bei 100%. Paketverlustraten von variierenden wenigen Prozentpunkten sind im Allgemeinen bereits mit starken Performance-Einbußen im IT-Bereich verbunden, da in einem solchen Szenario TCP-Mechanismen Eigenschaften wie Fenstergröße reduzieren. Die statische Natur der IE-Kommunikation erlaubt jedoch Konzepte wie Half&Half, ohne die Verfügbarkeit und Performance der Applikation einzuschränken.

Abschließend könnte eine Implementierung von Half&Half innerhalb eines IE-Switches eine weitflächige Anwendung des Konzeptes in der Automatisierungsdomäne ermöglichen.

5.4 Echtzeitfähigkeit und Determinismus

Eine Vielzahl von Applikationen innerhalb der Automatisierungsdomäne erfordert Determinismus und Echtzeitfähigkeit sowohl in der Ausführung als auch in der Kommunikation mit den jeweiligen Kommunikationspartnern. Die Evaluierung der vorliegenden Konzepte erfolgt im Folgenden auf Basis verschiedener Lastszenarien. Dabei werden Hintergrund-Datenverkehr und höherpriorer Datenverkehr gleichzeitig aufgetragen, Messungen mittels spezialisierter Hardware oder Software durchgeführt sowie qualitative Versuchsreihen unter Nutzung der erwarteten Applikationen durchgeführt.

Darüber hinaus ist die Sicherstellung der Echtzeitfähigkeit des verteilten Systems sowie der einzelnen virtuellen Maschinen und Container notwendig. Eine detaillierte Beschreibung der Erreichung eines deterministischen Verhaltens von Applikationen auf verteilten Systemen findet sich in Abschnitt A.3.

5.4.1 Virtualisiertes Netzwerk

Das Konzept sieht vor, echtzeitkritische Applikationen auf verteilten Systemen zu betreiben. Dies schließt nicht nur die Echtzeitfähigkeit der Applikation ein, sondern auch die Übertragung und Konformität von IE-Protokollen bei Nutzung von vSPS.

Im Rahmen eines gemeinsamen Entwicklungsprojektes wurde mit dem Unternehmen VMware by Broadcom Inc. ein neuer virtueller Switch entwickelt, welcher den Namen IvS trägt. Dieser wurde unter anderem auf Basis der in Abschnitt 4.3 definierten Anforderungen konzipiert und entwickelt. Zur Nutzung dieses Switches sind Enhanced Data Path (EDP)-fähige Netzwerkkarten notwendig [Bro24]. Mittels regelmäßigem Polling können geringe Übertragungszeiten erreicht werden. Neben PROFINET-Kompatibilität ermöglicht der IvS weiterhin die Duplizierung von Telegrammen mittels PRP, welches in einem späteren

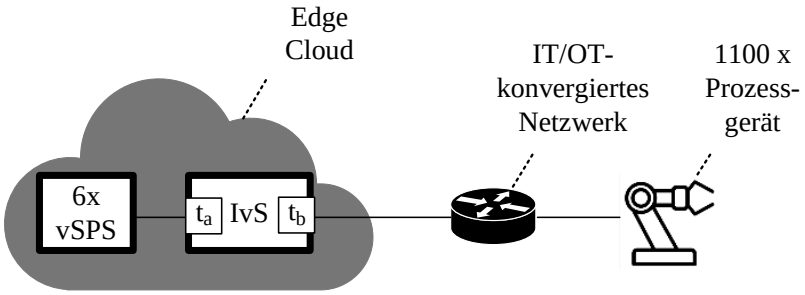


Abbildung 5.6: Validierung des IvS mittels PROFINET-Kommunikation zwischen vSPS-Instanzen und Prozessgeräte

Abschnitt dieses Kapitels evaluiert wird.

5.4.1.1 Validierung

Die Validierung des IvS erfolgt unter Nutzung von realen und simulierten PROFINET-Geräten. Es handelt sich um eine Entwicklungsversion, sodass die hier ermittelten Werte keinen Aufschluss über das letztendliche Produkt liefern. Eine Vereinfachung des experimentellen Versuchsaufbaus ist in Abbildung 5.6 dargestellt. Jedes Telegramm, welches von dem IvS übertragen wird, erhält an t_a und t_b einen Zeitstempel. Die Bildung der Differenz ermöglicht die Ermittlung der Übertragungsdauer.

Sechs Safety-vSPS des Unternehmens Siemens AG, Version 1.18, werden auf einem einzelnen Server betrieben und genutzt, um insgesamt 1100 PROFINET-Geräte zu steuern. Mit einem Durchsatz von 270.000 übertragenen Paketen pro Sekunde über einen Testzeitraum von 60 Stunden konnte eine Vielzahl an Metriken ermittelt werden. Relevante Ergebnisse des Dauertests sind in Tabelle 5.1 dargestellt. Über alle Steuerung-Datenströme aggregiert ist die Übertragungsdauer 99,9999986% der Telegramme $\leq$ 64 µs, und 100% $\leq$ 96 µs. Es wurden in beide Richtungen keine Pakete, beispielsweise aufgrund von Überlast der Puffer, verworfen.

Tabelle 5.1: Experimentell ermittelte Übertragungszeit TT des Industrial virtual Switch

vSPS	Anzahl Pakete	TT: 0-32 µs	TT: 33-64 µs	TT: 65-96 µs	TT: Max
#1	28,902 Millionen	99,9999697%	0,0000303%	0,0000000%	53 µs
#2	28,902 Millionen	99,9999720%	0,0000280%	0,0000000%	64 µs
#3	28,826 Millionen	99,9934844%	0,0065113%	0,0000042%	95 µs
#4	28,900 Millionen	99,9836351%	0,0163579%	0,0000071%	96 µs
#5	0,452 Millionen	99,9999746%	0,0000254%	0,0000000%	48 µs
#6	5,995 Millionen	99,9997343%	0,0002657%	0,0000000%	52 µs
Aggregiert	121,977 Millionen	99,9945559%	0,0054415%	0,0000027%	96 µs

5.4.1.2 Bewertung

Unter der Nutzung des entwickelten IvS ist eine deterministische Übertragung des IE-Datenverkehrs möglich. Auf Basis von sechs vSPS-Instanzen und einer realistischen Belastung des Netzwerkes durch 1100 PROFINET-Geräte konnte eine maximale Übertragungszeit von 96 µs ermittelt werden. Unterschiede innerhalb der verschiedenen vSPS sind auf die Zuordnung der Prozessorkerne zurückzuführen, da Instanzen #3 und #4 einem Kern zugeordnet waren. Die übertragenen Telegramme haben somit auch einen Einfluss auf die maximale Übertragungszeit, wobei sich die ermittelten Werte unter der benötigten Übertragungszeit befinden.

Allerdings gelten die hier betrachteten Metriken ausschließlich für die Kommunikation innerhalb des verteilten Systems, sodass in den folgenden Abschnitten die Echtzeitfähigkeit des IP-basierten, physikalischen Netzwerkes Gegenstand der Betrachtung ist.

5.4.2 Quality of Service

Auf Basis der in Abschnitt 4.5.2 beschriebenen Schritte erfolgt die Konfiguration der einzelnen Netzwerkkomponenten. Der in Abschnitt A.4 abgebildete Code-Ausschnitt ist beispielhaft auf jeder Netzwerkkomponente enthalten, welche PROFINET-Datenverkehr auf Basis des einzigartigen EtherTypes erkennt und im Rahmen der VXLAN-Kapselung den DSCP-Wert des IP-Headers auf den einzigartigen Wert 50 setzt. Dieser ist an weiteren Switchen innerhalb der VXLAN-Fabric Anzeichen für eine notwendige Priorisierung und Einordnung in eine dedizierte Hardware-Warteschlange. Es können hierbei beliebige Werte zugewiesen werden, allerdings empfiehlt es sich, einen ungewöhnlichen DSCP-Wert zu nutzen, damit nicht eine große Menge an Telegrammen von außerhalb der Fabric mit dem gewählten DSCP-Wert vorhanden ist. Diese Telegramme müssen beim Eintritt in die Fabric einem anderen DSCP-Wert zugewiesen werden, um in priorisierten Hardware-Warteschlangen der Netzwerkkomponenten ausschließlich echtzeitfähigen Datenverkehr vorzufinden. Weitere notwendige Konfigurationen sind ebenfalls in Abschnitt A.4 enthalten.

An dieser Stelle ist auch anzumerken, dass die hier beschriebene Konfiguration nicht auf allen evaluierten COTS-Netzwerkkomponenten möglich war. So konnten auf Switches des Unternehmens HPE Aruba die DSCP-Werte der VXLAN-Telegramme auf Basis des EtherTypes oder der in IEEE 802.1p enthaltenen Priorität nicht geändert werden, da beim Eintritt in die Fabric kein DSCP-Wert aufgrund der Schicht 2-basierten Kommunikation vorhanden ist. Dies verdeutlicht die Notwendigkeit für eine regelmäßige Validierung der einzelnen Architekturbausteine mittels gewünschten Hardware- und Softwarekomponenten.

Obwohl die Netzwerkkomponenten in der Regel IP-basierte Kommunikation ermöglichen, erfolgt die Übertragung der Telegramme auf Basis der im Puffer gespeicherten Informationen, was eine schnelle Übertragung im Vergleich zu dem auf Longest Prefix Match-basierten IP-Kommunikation ermöglicht. In den folgenden Abschnitten wird die Eignung der QoS-Mechanismen zur Erreichung des notwendigen Determinismus untersucht.

5.4.3 Qualitative Evaluierung

Um die Eignung des entwickelten Architekturkonzeptes für die Applikation einer Safety-vSPS zu evaluieren, wird der in Abbildung 5.6 dargestellte Versuchsaufbau genutzt. Hierfür werden vSPS-Instanzen von Siemens auf einer verteilten Umgebung betrieben. Jegliche WDT der beteiligten PROFINET- und PROFIsafe Geräte werden auf 3 ms gesetzt, die anspruchsvollste Einstellung. Weiterhin wird niederpiorer Hintergrund-Datenverkehr genutzt, um die jeweiligen Netzwerkkomponenten zu belasten. Innerhalb des betrachteten Zeitraumes von 72 Stunden werden keine Alarme aufgrund von WDT-Verletzungen beobachtet.

5.4.4 Quantitative Evaluierung

Eine Evaluierung auf Basis von quantitativen Messmethoden ermöglicht, Ergebnisse zu vergleichen und erlaubt statistische Analysen, welche die Eignung von Konzepten neutral bewertet. Dieser Abschnitt beschreibt zwei verschiedene Ansätze, um die Echtzeiteigenschaften des entwickelten Konzeptes zu quantifizieren.

5.4.4.1 Datengenerator

Der experimentelle Aufbau wird um Datengeneratoren erweitert, um quantitative Messgrößen zu erhalten. Hierbei wird ein Datengenerator für den Echtzeit- und ein Weiterer für den Hintergrund-Datenverkehr genutzt. Dies ist in Abbildung 5.7 dargestellt. Die physischen Verbindungen sind durch das Einspeisen von niederpriorem Datenverkehr mit Leitungsgeschwindigkeit überlastet, wobei etwa 4% Paketverlust beobachtet werden können. Dies ist in einem solchen Szenario zu erwarten und kann auch mittels Befehlen am Netzwerkgerät überprüft werden, dessen Ausgaben beispielhaft in Abschnitt A.4 dargestellt sind.

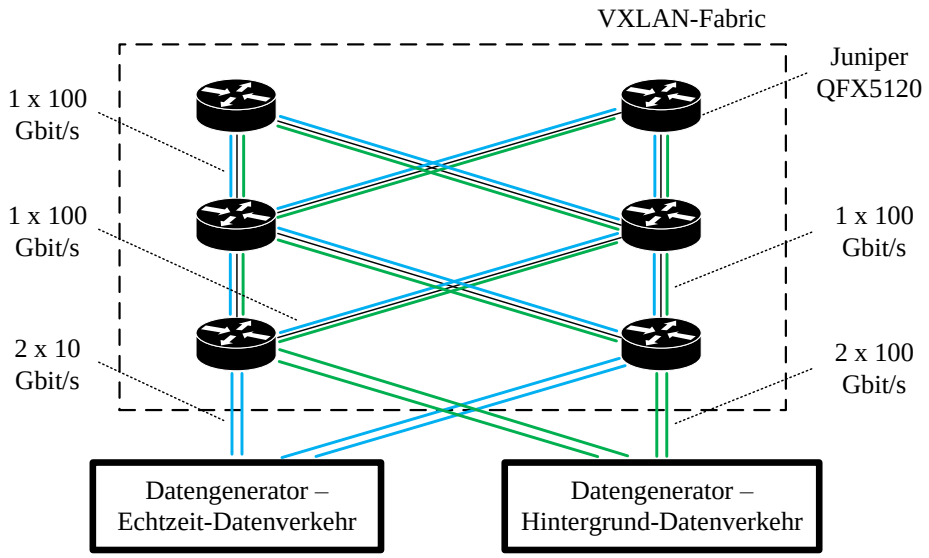


Abbildung 5.7: Validierung der Echtzeitfähigkeit einer VXLAN-Fabric mit hochpriorisierten Datenverkehr (blau) und Hintergrund-Datenverkehr mit niedriger Priorität (grün)

Nachdem das Netzwerk bereits über die verfügbare Kapazität hinaus belastet wird, werden bidirektionale 10 Gbit/s-Datenströme mit variierenden Maximum Transmission Unit (MTU)-Größen und einer dedizierten Warteschlange auf allen beteiligten Netzwerkkomponenten sequentiell angewendet. Durch die Nutzung des einzigartigen EtherTypes bei der Generierung des zu priorisierenden Datenstromes, hier 0x8892 von PROFINET, werden Telegramme im PROFINET-Format in priorisierte Hardware-Warteschlangen einsortiert und übertragen. Nachdem ein Datengenerator als Quelle und Ziel der Telegramme verwendet wird, können quantitative Werte wie die Übertragungszeit in eine Richtung gemessen werden, ohne eine Zeitsynchronisation durchführen zu müssen. Die Ergebnisse für variierende Maximum Transmission Unit (MTU) sind in Tabelle 5.2 dargestellt. Die Werte wurden über jeweils einen Tag ermittelt. Es werden in dieser und weiteren statistischen Analysen das jeweilige Minimum (Min), Maximum (Max), und der Durchschnitt (Avg) angegeben.

Tabelle 5.2: Ein-Wege-Übertragungszeit von hochpriorisiertem Datenverkehr über fünf Hops einer einzelnen VXLAN-Fabric mit Hintergrund-Datenverkehr

MTU (Bytes)	Min TT (µs)	Avg TT (µs)	Max TT (µs)
64	5,22	5,26	5,31
1512	6,53	6,58	6,87
9100	13,48	13,53	13,60

5.4.4.2 TWAMP

Die zuvor durchgeführten Messungen erlauben jeweils Aussagen über Netzwerkmetriken im virtuellen und physikalischen Raum als auch Aussagen über die Verfügbarkeit des Kommunikationsnetzwerkes. Mittels einer Lösung basierend auf Two-Way Active Measurement Protocol (TWAMP) werden im Folgenden die jeweiligen Werte mittels synthetischem Datenverkehr parallel zu Belastungen der Infrastruktur durch IE-Datenverkehr als auch Hintergrund-Datenverkehr durch Datengeneratoren evaluiert.

Die hierzu genutzten Geräte und Applikationen stellen eine Lösung des Unternehmens Accedian Networks Inc. dar. Deren Messmittel werden vorrangig im Netzversorger-Bereich genutzt, um Anomalien und Engpässe in der Versorgung von Endgeräten zu identifizieren. Eine patentierte Form der Zeitsynchronisation ermöglicht die Messung von Ein-Wege-Übertragungszeiten mit Mikrosekundenpräzision [HH12].

Die Platzierung der Sensoren innerhalb der Infrastruktur ist in Abbildung 5.8 dargestellt. Transceiver werden in Switchen und Servern der Edge Cloud verwendet, während eine Container-Applikation innerhalb einer Linux Debian-basierten VM auf dem verteilten System betrieben wird und deren Eigenschaften auf Echtzeit optimiert wurden. Dadurch ist es auch möglich, Ende-zu-Ende Metriken zu erhalten, da Sensoren sowohl innerhalb des verteilten Systems als auch in der Feldebene vorhanden sind. Die Definition von Datenströmen ermöglicht das Erhalten von Informationen für vergleichbare Applikationen, dessen Telegramme innerhalb des Netzwerkes identisch priorisiert behandelt werden.

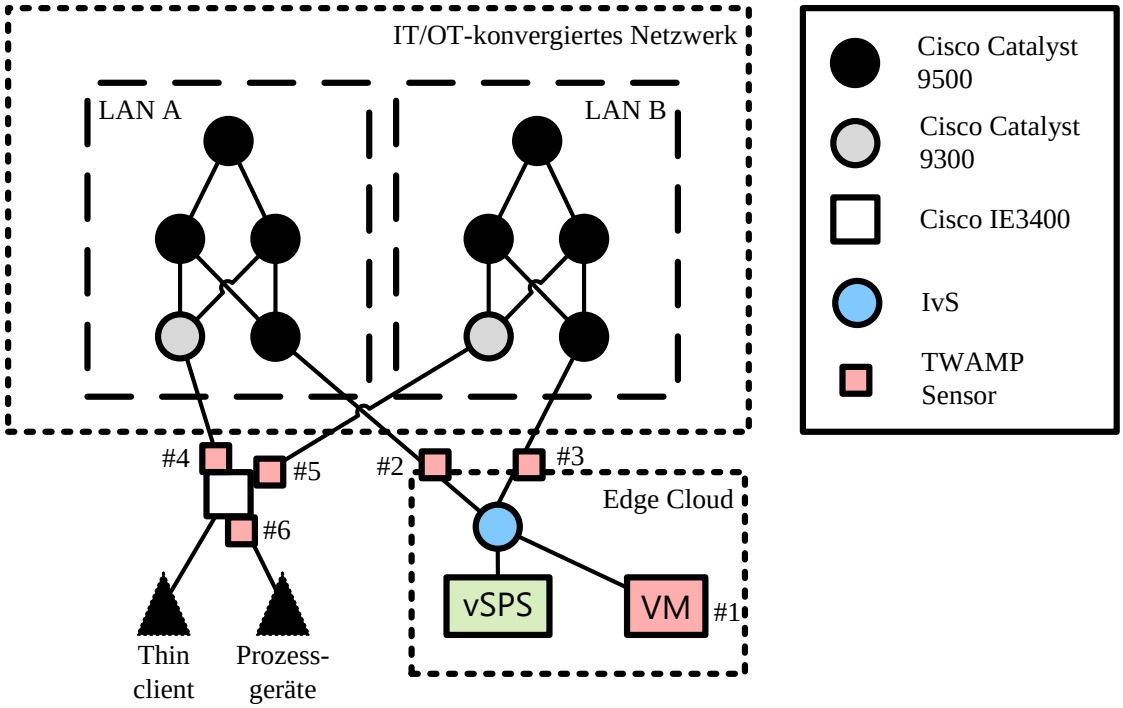


Abbildung 5.8: Generierung von synthetischen Datenverkehr an verschiedenen Messpunkten zur Erfassung von Netzwerkmetriken mittels TWAMP

Innerhalb der VXLAN-Fabric LAN A werden 20 Gbit/s Hintergrund-Datenverkehr und 2x1 Gbit/s zu priorisierenden Datenverkehr verwendet, der in der selben Hardware-Warteschlange wie Steuerungs-Datenverkehr wie PROFINET übertragen wird. LAN B hingegen erhält ausschließlich 2x1 Gbit/s zu priorisierenden Datenverkehr, um das erwartete Datenverkehrsprofil eines realen IT/OT-konvergierten Netzwerkes zu simulieren. Weiterhin werden weitere Daten, beispielsweise die Kommunikation zwischen vSPS-Instanzen und deren PROFINET-Geräte, übertragen. Die TWAMP-Sensoren erzeugen bis zu 1000 Telegramme pro Sekunde für jeden Datenstrom. Die Ergebnisse für einen Testzeitraum von 72 Stunden sind in Tabelle 5.3 dargestellt.

5.4.5 Diskussion

In diesem Abschnitt konnten auf Basis verschiedener Versuchsreihen der notwendige Determinismus für Automatisierungsapplikationen validiert werden.

Die quantitativen Messungen unterstreichen erneut, dass QoS-Mechanismen moderner COTS-Netzwerkhardware und eine kontrollierte Umgebung die IE-Kommunikation über ein gemeinsam genutztes IP-basiertes Kommunikationsnetzwerk ermöglichen. Hierbei ist wichtig anzumerken, dass jegliche Kabellängen in den durchgeführten Validierungen mit Entfernungen unter zehn Metern vernachlässigbar waren. Größere Entfernungen mit Glasfaser fügen etwa fünf Mikrosekunden pro Kilometer an Übertragungszeit hinzu [Pol+13]. Weiterhin ist die vorhandene Bandbreite eine entscheidende Variable, die einen direkten Einfluss auf die Übertragungsdauer besitzt. Dies verdeutlicht auch der Vergleich zwischen den beiden

Tabelle 5.3: Netzwerkmetriken von hochpriorem und niederpriorem Datenverkehr über bis zu vier Hops eines IT/OT-konvergierten Netzwerkes unter realistischen Lastbedingungen.

Datenfluss	Priorität	Max TT	Max Jitter	Max PLR	Beschreibung
#1 -> #2	hoch	16,1 µs	8,23 µs	0,0 %	LAN A - virtuell
#3 -> #5	niedrig	25,6 µs	7,92 µs	0,0 %	LAN B - Physik
#3 -> #5	hoch	25,6 µs	8,96 µs	0,0 %	LAN B - Physik
#3 -> #6	niedrig	36,2 µs	7,05 µs	0,0 %	LAN B - Physik
#3 -> #6	hoch	36,3 µs	7,02 µs	0,0 %	LAN B - Physik
#1 -> #5	niedrig	45,4 µs	23,9 µs	0,0 %	LAN B - komplett
#1 -> #5	hoch	43,8 µs	21,6 µs	0,0 %	LAN B - komplett
#1 -> #6	niedrig	58,9 µs	21,5 µs	0,0 %	PRP - komplett
#1 -> #6	hoch	60,3 µs	22,7 µs	0,0 %	PRP - komplett
#2 -> #4	niedrig	291 µs	271 µs	6,92 %	LAN A - Physik
#2 -> #4	hoch	83,4 µs	31,2 µs	0,0 %	LAN A - Physik
#2 -> #6	niedrig	388 µs	290 µs	6,92 %	LAN A - Physik
#2 -> #6	hoch	65 µs	20,7 µs	0,0 %	LAN A - Physik
#1 -> #4	niedrig	427 µs	180 µs	6,84 %	LAN A - komplett
#1 -> #4	hoch	93,9 µs	40,1 µs	0,0 %	LAN A - komplett

Versuchsaufbauten und den damit einhergehenden Messungen auf Basis von TWAMP und einem Datengenerator. Während im Falle des Testaufbaus mit dem Datengenerator 100 Gbit/s-Links zwischen den einzelnen Netzwerkkomponenten vorhanden waren, werden im Testaufbau mit TWAMP 1, 10, und 25 Gbit/s-Links für jeweils den Cisco IE3400, Catalyst 9300, und Catalyst 9500 verwendet.

Allerdings bestätigen beide Messungen mittels TWAMP und den Datengeneratoren die Eignung von QoS zur Erreichung der notwendigen Echtzeiteigenschaften von Steuerungs-Datenverkehr.

Die ermittelten Netzwerkmetriken entsprechen den Erwartungen. In LAN A des TWAMP-Testaufbaus wurden jegliche Verbindungen an die Überlast gebracht, sodass Telegramme mit fehlender Priorisierung hohe Übertragungszeiten und Paketverluste hinnehmen. Dies kann bei LAN B nicht beobachtet werden, da kein niederpriorer Datenverkehr die Verbindungen belastet. Die Kommunikation über PRP bleibt konstant unter der Anforderung von 500 µs an maximale Übertragungszeit und Jitter, sodass auch unter zu erwartbaren Hochlastsituationen die notwendige Echtzeitfähigkeit bestätigt werden kann.

Weiterhin ermöglichen die Messungen nach TWAMP auch im Betrieb des IT/OT-konvergierten Netzwerkes eine Sicherung und Überwachung der relevanten Parameter. Dies schließt neben den Netzwerkmetriken auch die verwendete Bandbreite mit ein. Durch die Möglichkeit, Datenströmen mittels Transceivern zu analysieren und die Übertragungsleistung nicht einzuschränken, wird der Betrieb und die Fehlersuche erleichtert.

5.4.5.1 COTS-Hardware in der Automatisierungsdomäne

Dieser Abschnitt beschäftigt sich mit der Frage, warum COTS-Hardware aus dem IT-Bereich für OT-Applikationen eingesetzt werden sollte. Entgegen der weit verbreiteten Meinung, dass in diesem Kontext zwingend TSN genutzt werden muss, stellt die vorliegende Arbeit einen alternativen Ansatz zur Erreichung der notwendigen Echtzeitfähigkeit und des Determinismus vor. Dieser Ansatz basiert auf denselben Methoden, die auch im industriellen Ethernet-Umfeld verwendet werden.

Dennoch sind einige Kritikpunkte denkbar:

- Bandbreite nicht voll nutzbar: Auch PROFINET empfiehlt, maximal 50% der Bandbreite zu nutzen, um eine zuverlässige Kommunikation zu gewährleisten. Industrielle Kommunikation ist oft durch sehr geringe Bandbreiten gekennzeichnet, beispielsweise 100 Mbit/s pro Automatisierungszelle. Weiterhin sinken die Preise für höhere Durchsatzraten jährlich, was die Nutzung höherer Bandbreiten wirtschaftlicher macht.

- Fehlender Determinismus und Echtzeitgarantien: Die Nutzung von Mechanismen, die aus industriellen Ethernet-Standards bekannt sind, bieten vergleichbare Echtzeit- und Determinismus-Garantien. Es ist jedoch korrekt, dass nicht das Niveau der Protokolle für Bewegungsregelungen erreicht wird.

- Keine Nutzung von TSN oder DetNet: Die Komplexität zur Erreichung der gewünschten Anforderungen ist hoch. Weiterhin ist die Verfügbarkeit von TSN- und DetNet-Geräten derzeit unzureichend, da es bisher nur prototypische Implementierungen gibt.

5.5 Hochverfügbarkeit von echtzeitfähigen, zustandsbehafteten Applikationen

In diesem Abschnitt wird das entwickelte RDMA-basierte Konzept zur Erreichung von Hochverfügbarkeit für echtzeitfähige, zustandsbehaftete Applikationen evaluiert und bewertet. Diese Validierung umfasst die Erstellung eines Prototypen auf Basis von C++, die Erweiterung von CODESYS SPS mit RDMA-basierter Zustandssynchronisation, sowie die Kombination mit einem deterministischen, IP-basierten Netzwerk, um die Leistungsfähigkeit und Zuverlässigkeit des Systems unter realistischen Bedingungen zu testen. Durch die gleichzeitige Notwendigkeit für Echtzeitfähigkeit und Konsistenz der Zustände ist die Realisierung von Hochverfügbarkeit für diese Art der Systeme herausfordernd.

Da WDT in IE-Protokollen und die Rechenzeit eines IEC-Tasks stark von der jeweiligen Anwendung abhängen, konzentriert sich die Validierung ausschließlich auf die Synchronisation des Zustands zwischen der primären und der Backup-SPS und dem Vergleich mit dem Stand der Technik. Die Zustandsynchronisation kann in ihrer Zustandsgröße variiert werden, um unterschiedliche Szenarien und Bandbreiten zu simulieren.

Durch die Modifikation der Redundanzkomponente einer SPS von CODESYS kann die RDMA-Technologie der Applikation hinzugefügt werden. Die Komponente ist in der Programmiersprache C geschrieben und synchronisiert unter anderem einen Puffer der

primären SPS mit dem Puffer der sekundären SPS. Während die aktuelle Implementierung auf UDP- und TCP-Kommunikation zwischen den beiden Anwendungen basiert, synchronisiert die entwickelte Implementierung den Puffer ausschließlich mittels RDMA.

Das in Abbildung 5.9 dargestellte Ablaufdiagramm stellt die Abfolge der Schritte dar, die für die Synchronisation von zwei zustandsbehafteten vSPS-Instanzen notwendig sind.

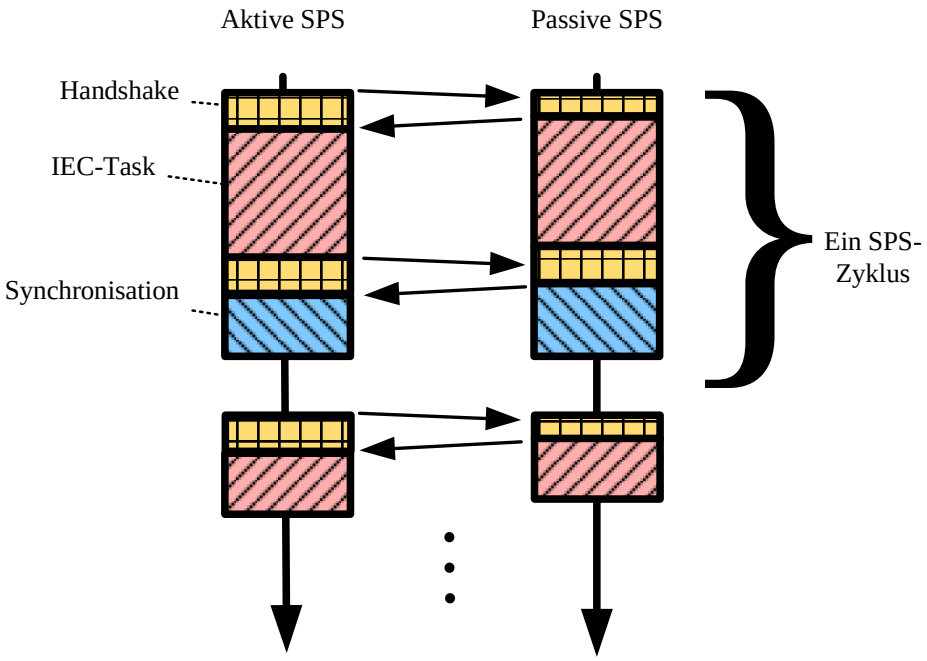


Abbildung 5.9: Ablaufdiagramm von zwei SPS-Instanzen, deren Zustandvariablen zyklisch synchronisiert werden [KG23a]

5.5.1 Experimenteller Versuchsaufbau

Für die Anwendungen werden zwei verschiedene Hosts verwendet, die in Tabelle 5.4 näher beschrieben sind. Es werden PREEMPT_RT-Patches genutzt, um die Unterbrechung von niederprioren Tasks durch Höherpriore zu erlauben. Eine detaillierte Beschreibung der Erreichung von deterministischem Verhalten von Applikationen auf verteilten Systemen als auch auf gewöhnlichen Linux-basierten Systemen gibt Abschnitt A.3.

Eine Mellanox ConnectX-5 Netzwerkkarte wird verwendet, da sie RDMA und das Precision Time Protocol (PTP) unterstützt. Um die Synchronisationszeit zu berechnen, wird jedes Mal, wenn die primäre Anwendung eine Zustandsynchronisation über RDMA initiiert, ein Zeitstempel t_1 gespeichert. In der sekundären Anwendung wird ebenfalls ein Zeitstempel t_2 gespeichert, sobald die Synchronisation abgeschlossen ist. Durch den Vergleich beider Zeitstempel ergibt sich die Synchronisationszeit, weshalb ein gemeinsames Verständnis von Zeit mittels PTP nötig ist. Es ergibt sich folgende Gleichung 5.2 für die Berechnung der Synchronisationszeit:

$$t_{sync} = t_2 - t_1 \tag{5.2}$$

Tabelle 5.4: Hardware-Eigenschaften der Hosts

	Host #1	Host #2
CPU	Intel i9-9900 8x3,1 GHz	Intel Xeon W-2175 14x2,5 GHz
RAM	DDR4 2133 MHz 4x16 GiB	DDR4 2666 MHz 8x16 GiB
Speicher	Samsung SSD 970 EVO 500 GB	SK hynix PC300 SSD 1 TB
Netzwerkkarte	Nvidia MCX512A-ACAT 2x25 Gbit/s	Nvidia MCX512A-ACAT MCX512A-ACAT 2x25 Gbit/s
Betriebssystem	Linux Ubuntu 20.04LTS	Linux Ubuntu 20.04LTS

5.5.2 Validierung mittels modifizierter SPS

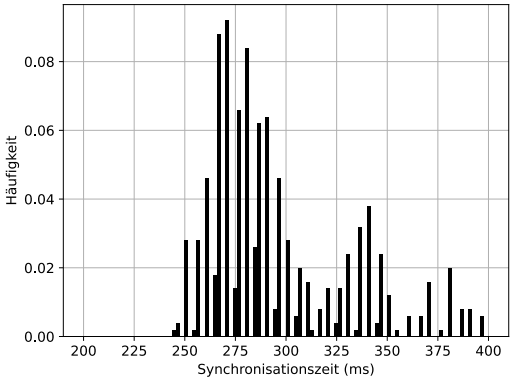
Sechs verschiedene Testfälle werden definiert, in denen sowohl das Kommunikationsprotokoll der Synchronisierung zwischen RoCE und UDP gewechselt als auch die Zustandsgrößen von 100 KB, 1 MB und 10 MB variiert werden. Tabelle 5.5 stellt die minimalen, maximalen, und durchschnittlichen Werte sowie die Standardabweichung (SD) der Synchronisationszeit für die sechs Testszenarien dar, die jeweils 100 Mal für 10 Sekunden ausgeführt werden. Die Messungen erfolgen an spezifischen Ausführungspunkten innerhalb der Applikation mit einer Millisekunden-Genauigkeit. Die Genauigkeit ist begrenzt durch eine interne Implementierung anderer Systembestandteile, sodass keine genauere Messung möglich ist. Die Ergebnisse für Zustandsgrößen von 1 MB und 10 MB werden in Abbildung 5.10 als Wahrscheinlichkeitsverteilung visualisiert.

Tabelle 5.5: Statistische Analyse der Zustandsynchronisationszeiten der CODESYS-SPS basierend auf UDP/TCP und RoCE. Alle Werte sind in Millisekunden angegeben [KEG23].

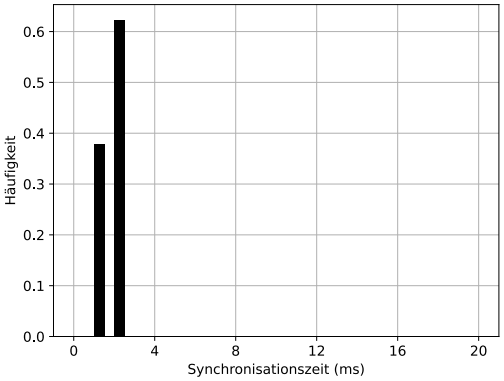
Protokoll	Zustandsgröße	Min	Max	Avg	SD
UDP/TCP	100 KB	25,00	51,00	44,47	8,94
RoCE	100 KB	0,00	2,00	0,20	0,40
UDP/TCP	1 MB	245,00	396,00	295,06	35,00
RoCE	1 MB	1,00	2,00	1,63	0,48
UDP/TCP	10 MB	2467,00	3673,00	2529,36	91,33
RoCE	10 MB	15,00	17,00	15,87	0,37

5.5.3 Validierung partieller Synchronisation

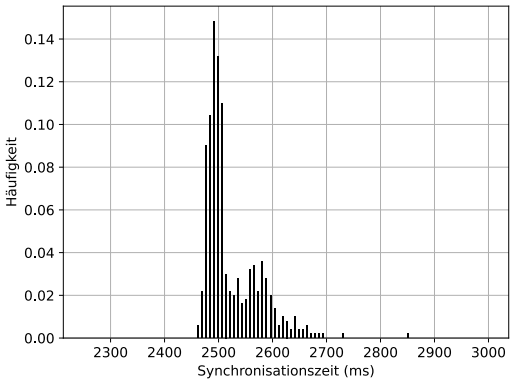
Im Allgemeinen ändern sich in jedem Berechnungszyklus nur Submengen der Zustandsvariablen. Deshalb wird im Folgenden die Performance der vollen und partiellen Synchronisation von Zuständen verglichen. Hierzu wird ein auf C++-basierter Zustandssimulator entwickelt, welcher zyklisch, ähnlich zu einer vSPS, den Zustand mittels RDMA synchronisiert.



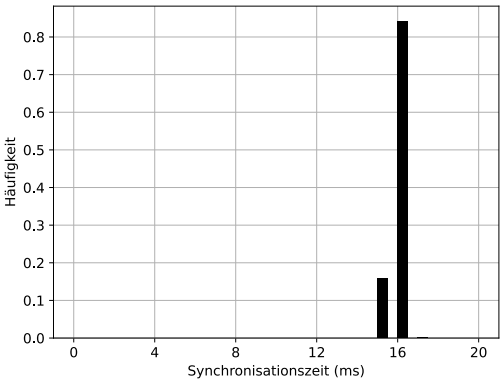
(a) UDP/TCP - 1 MB



(b) RoCE - 1 MB



(c) UDP/TCP - 10 MB



(d) RoCE - 10 MB

Abbildung 5.10: Synchronisationszeiten der CODESYS-SPS unter Nutzung von UDP/TCP und RoCE

Hierbei ist erwähnenswert, dass auch im Falle der partiellen Synchronisation ausschließlich zusammenhängende Bereiche des Speichers genutzt werden.

Die Ergebnisse der Validierung sind in Tabelle 5.6 dargestellt. Es werden sowohl eine volle Synchronisation von 1 MB und 10 MB als auch eine partielle Synchronisation mit einer Zustandsgröße von 10 MB und einer Änderungsrate von 10% durchgeführt und die jeweilige Synchronisationszeit gemessen. Die Versuchsreihen werden jeweils 1000-mal in 10 Sekunden Abschnitten durchgeführt.

Tabelle 5.6: Synchronisationszeiten der RDMA-basierten Zustandsübertragung der vollen und partiellen Synchronisation nach [KEG23]. Falls nicht anders angegeben, sind alle Werte in Millisekunden.

Zustandsgröße	Synchronisationsart	Min	Max	Avg	SD
1 MB	voll	1,70	1,95	1,85	0,05
10 MB	partiell, 10% Änderungsrate	1,68	1,94	1,84	0,40
10 MB	voll	13,34	14,13	13,62	0,07

5.5.4 Erweiterung um ein deterministisches Netzwerk

In den vorangegangenen Validierungen wurde darauf verzichtet, ein Netzwerk zwischen den Hosts zu verwenden, um eine kontrollierte Umgebung für Leistungsmessungen der jeweiligen Konzepte zu schaffen. Netzwerke können durch Überlastung beeinträchtigt werden, was zu Verzögerung der Synchronisation und Paketverlusten führen kann und damit eine präzise Messung der Synchronisationszeiten verhindert. Weiterhin besitzt jede Komponente innerhalb des Netzwerkes eine Gatterlaufzeit, die das Signal benötigt, um die Komponente zu durchqueren. Final sind auch physikalische Laufzeiten zu berücksichtigen, die aufgrund von zusätzlichen Kabeln und SFPs hervorgerufen werden. In den folgenden Abschnitten wird das Konzept nun durch die Integration eines deterministischen IP-basierten Netzwerks erweitert, um die Auswirkungen dieses Aufbaus zu untersuchen. Hierbei ist es nach erfolgter Literaturrecherche die erste Validierung einer RoCE-basierten Kommunikation über ein deterministisches IP-basiertes Netzwerk.

Um in Szenarien mit hoher Netzwerkauslastung lange Übertragungszeiten und eine hohe Rate an erneuten Übertragungen zu vermeiden, könnte insbesondere bei RoCE eine zentrale Verwaltung der Synchronisation mehrerer Anwendungen mit ihren jeweiligen Backups notwendig sein. Eine rein anwendungsgetriebene Synchronisation ist nicht ideal, da sie keine ganzheitliche Sicht auf die Synchronisationen im Netzwerk und damit auf die Auslastung der einzelnen Ressourcen bietet.

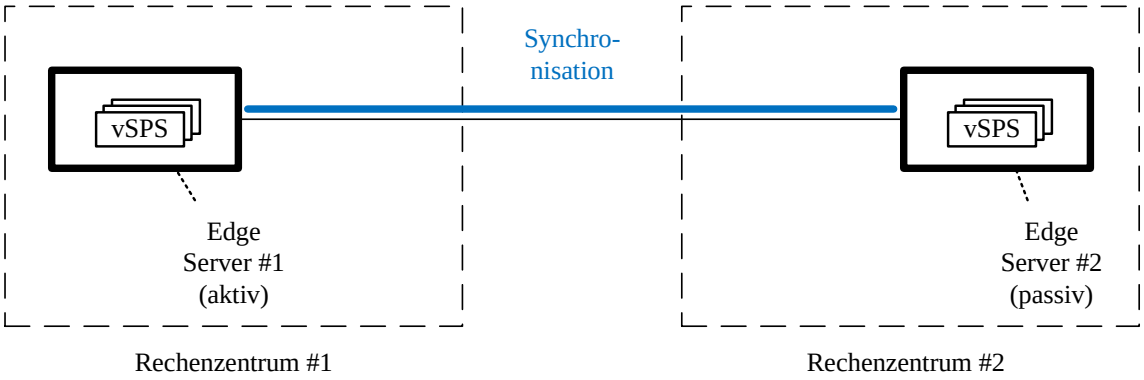
Ein holistischer Kommunikationszeitplan der Netzwerkressourcen wäre daher wünschenswert. Eine vielversprechende Technologie, die derzeit von der IETF standardisiert wird, könnte deterministisches Verhalten und Überlastvermeidung in gerouteten Umgebungen gewährleisten [IET22]. Daher wird in diesem Abschnitt RDMA über diese Technologie, DetNet, als den nächsten Entwicklungsschritt evaluiert, insbesondere im Kontext deterministischer Kommunikation und Dienste. Die Hauptvorteile dieses Ansatzes sind deterministische Kommunikationsgrenzen ohne Paketverlust durch Überlast sowie eine geplante Ressourcenzuweisung in zyklischer Weise.

Aus Sicht der Kompatibilität sollte RoCE ohne Anpassungen für jede Ethernet-basierte DetNet-Implementierung funktionieren, da es UDP als Transportprotokoll verwendet. Die Priorisierung von RDMA gegenüber weniger priorisiertem Datenverkehr erfolgt in der Regel durch die Nutzung der Prioritätsbits im Ethernet/IP-Header, vergleichbar mit dem validierten Ansatz in Abschnitt 5.4.2.

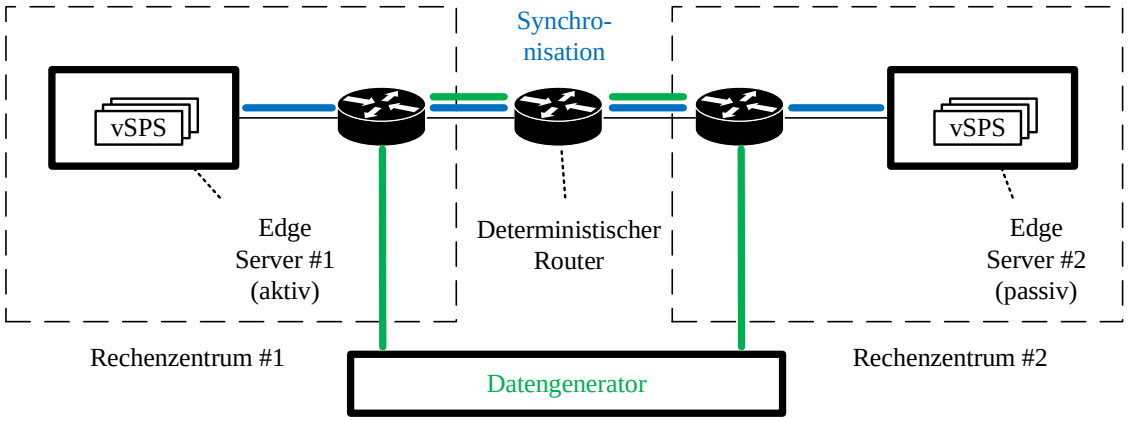
5.5.4.1 Experimentelle Validierung

Dieser Abschnitt beschreibt die einzelnen Testszenarien sowie die Ergebnisse der experimentellen Validierung.

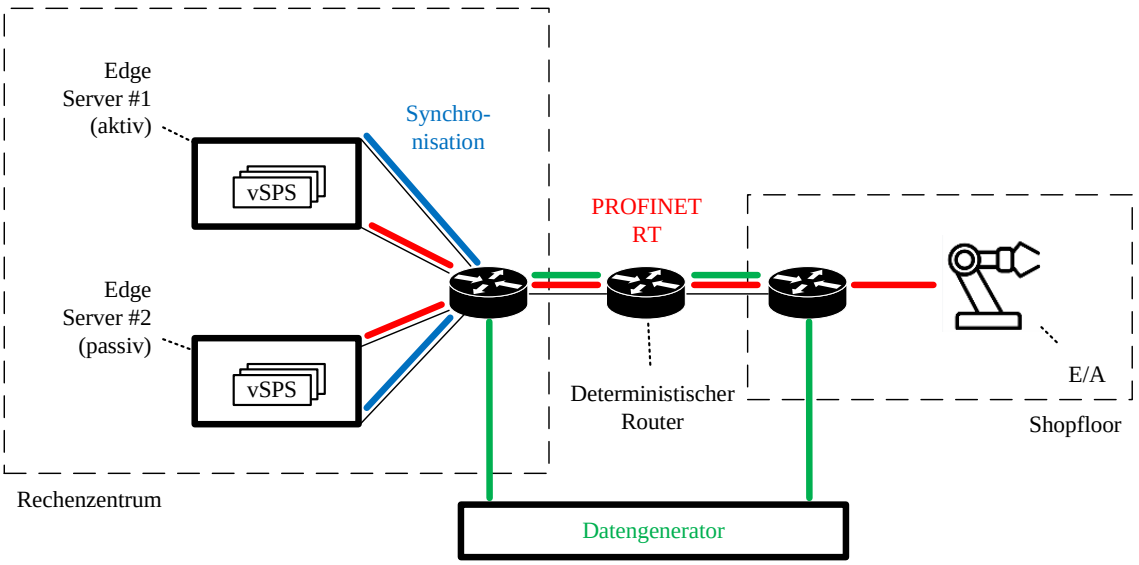
Tabelle 5.7 stellt die RDMA-basierte Synchronisationszeit in Abhängigkeit der zu synchronisierenden Zustandsgröße sowie der Anzahl an Netzwerk-Hops dar. Null Netzwerk-Hops entsprechen hierbei dem Aufbau dargestellt in Abbildung 5.11a), drei Netzwerk-Hops dem Aufbau in Abbildung 5.11b). Das Hinzufügen von mehreren Netzwerkkomponenten zwischen



(a) Testszenario mit zwei vSPS ohne dazwischenliegendes Netzwerk



(b) Testszenario mit zwei vSPS und einem deterministischen, IP-basierten Netzwerk zur Fehlertoleranz über Rechenzentren.



(c) Testszenario mit zwei vSPS und einem deterministischen, IP-basierten Netzwerk mit PROFINET-Geräten.

Abbildung 5.11: Testszenarien mit drei verschiedenen Netzwerktopologien nach [KG23a]

den beiden CODESYS vSPS-Instanzen erhöht die Synchronisationszeit um eine zweistellige

bis niedrige dreistellige Anzahl an Mikrosekunden. Nachdem die Messungen nach der selben Messmethode wie in Abschnitt 5.5.2 beschrieben ablaufen, ist jedoch die Genauigkeit auf Millisekunden begrenzt. Erwähnenswert ist außerdem, dass ausschließlich 1 Gbit/s-Links genutzt werden konnten, wodurch sich die Dauer der Synchronisation trotz RDMA erhöht.

Der nach Abbildung 5.11c) beschriebene Aufbau enthält PROFINET Geräte mit einem WDT von 3 ms und einer PROFINET-Zykluszeit von 1 ms. Keine WDT-Verletzungen können im Rahmen einer Testphase über 10 Stunden verzeichnet werden.

Tabelle 5.7: Statistische Analyse der Zustandsynchronisationszeiten der CODESYS-SPS mit RoCE unter variierender Anzahl an Netzwerk-Hops. Sofern nicht anders beschrieben sind alle Werte in Millisekunden angegeben [KG23a].

Netzwerk-Hops	Zustandsgröße	Min	Max	Avg	SD
0 Hops	100 KB	0,00	2,00	0,957	0,205
3 Hops	100 KB	1,00	3,00	1,019	0,136
0 Hops	1 MB	8,00	10,00	8,978	0,146
3 Hops	1 MB	9,00	10,00	9,056	0,231
0 Hops	10 MB	89,00	90,00	89,224	0,417
3 Hops	10 MB	89,00	90,00	89,274	0,446

5.5.5 Diskussion

Das vorgestellte RDMA-basierte Konzept erreicht in verschiedenen Versuchsreihen Synchronisationszeiten im einstelligen Millisekundenbereich bei Zustandsgrößen von einigen Megabyte. Im Vergleich zu der unmodifizierten, auf UDP-basierten Synchronisation einer verbreiteten Software-SPS konnte eine Reduktion der Synchronisationszeit um durchschnittlich bis zu 99,39% erreicht werden. Des Weiteren wurde die absolute Standardabweichung signifikant verringert, was es Echtzeitanwendungen ermöglicht, ihre Hochverfügbarkeitsanforderungen gemäß Abschnitt 4.3.4 zu erfüllen, ohne die Geschwindigkeit der Prozesse zu reduzieren.

Die Geschwindigkeit der Zustandsübertragung ist eine entscheidende Variable für die Adoption des Konzeptes. Durch die Erhöhung der Bandbreite zwischen den Instanzen kann die Zeit der Synchronisation verringert werden. Eine vollständige Synchronisation, welche die aktuelle Standardmethode für die Synchronisation vorhandener Produkte darstellt, benötigt jedoch viel Bandbreite, um gewünschte Synchronisationszeiten zu erreichen. Dies ist häufig nicht notwendig, da unveränderte Daten zwischen den einzelnen Instanzen übertragen werden. Eine partielle Synchronisation reduziert die Bandbreitennutzung erheblich, erfordert jedoch Anpassungen in weiteren Bereichen der SPS und vergleichbaren Applikationen.

Die erste Validierung von RoCE über DetNet bestätigt das Harmonieren der beiden Technologien aufgrund der übereinstimmenden Liefergegenstände und Kommunikationsprofile. Damit können auch größere Distanzen zwischen den zu synchronisierenden Instanzen überbrückt werden, ohne die Echtzeitfähigkeit der vSPS zu beeinträchtigen, und ermöglichen damit beispielsweise Rechenzentrumsredundanz. Hierbei wäre auch ein holistischer

Kommunikationszeitplan aller Kommunikationen zu präferieren, welcher jedoch außerhalb des Umfangs dieser Arbeit liegt. Dies ist vor allem auf Einschränkungen der Konfiguration deterministischen IP-Router und der Initiierung der Synchronisation zwischen den vSPS-Instanzen zurückzuführen.

Weiterhin übernehmen Cloud-Infrastrukturen zunehmend Mikroservice-Architekturen und setzen Kubernetes als Management-System ein. Im Kontext der vSPS-Anwendung könnte eine Umstrukturierung hin zu einer Mikroservice-basierten Architektur die Skalierbarkeit und Verfügbarkeit weiter verbessern. Das endgültige Ziel könnte die Auflösung der statischen 1:1-Beziehung zwischen einer SPS und einem Prozessgerät im Feld sein, zugunsten einer 1:n-Architektur mit einem Kubernetes-verwalteten Dienst. Eine ähnliche Vision wird derzeit von Standardisierungsorganisationen verfolgt [LB20].

5.5.5.1 Netzwerkauslastung einer vSPS

Die Ausführungsdauer eines SPS-Zykluses kann aufgrund von Koroutinen, fluktuierender Hardwareauslastung und anderen externen Einflüssen variieren. Die Synchronisation des Zustandes erfolgt nach Abschluss eines vollständigen Zyklus, wie in Abbildung 5.9 beschrieben. Variierende Zykluszeiten der SPS-Zyklen beeinflussen jedoch nicht die Netzwerkauslastung durch die SPS-E/A-Kommunikation, wie in Abbildung 5.12 dargestellt. Dies liegt an der statischen Natur der Kommunikation von IE-Protokollen, welche eine zeitgesteuerte Aktualisierungszeit für zyklische Anwendungen vorsehen. Allerdings führt die Konvergenz der Kommunikation zwischen den SPS und ihren jeweiligen Prozessgeräten sowie die Synchronisation der SPS untereinander zu einem bemerkenswerten Muster der Netzwerkauslastung, das im unteren Teil der Abbildung 5.12 dargestellt ist. Diese Darstellung zeigt, dass azyklische Kommunikationsmuster mit zyklischen Kommunikationsmustern koexistieren müssen, wobei Datenströme beider Muster eine deterministische Kommunikation erfordern.

5.5.5.2 Verteilung von vSPS-Instanzen

Vor allem in Fehlerzuständen gilt es, die Lastverteilung auf den jeweiligen Hosts eines verteilten Systems angemessen zu verteilen. Abbildung 5.13 zeigt hierfür eine beispielhafte Anordnung in Kombination mit dem vorgestellten Konzept. vSPSX.1 beschreibt die aktive, vSPSX.2 die Backup SPS. Eine arbiträre Anzahl an Instanzen läuft auf jeden Server, in diesem konkreten Fall 12 primäre und 12 Backup vSPS. Durch einen Serverausfall, beispielsweise ausgelöst durch eine Hardwareproblematik, entsteht ein Failover der Instanzen vSPS 1.1-12.1, in welchem 1.2-12.2 als primäre vSPS-Instanz übernehmen. Die Last auf den verbliebenen Hosts ist ohne eine Migration der jeweiligen Instanzen bereits homogen. Durch die Skalierung auf mehr als drei Hosts wird die Anzahl an zusätzlichen Instanzen je Host weiter verringert.

Weiterhin ist es empfehlenswert, jegliche Instanzen von vSPS auf einem Server zu konsolidieren, welche in einem Safety-Kopplungskreis miteinander verbunden sind. Beim Ausfall einer Instanz kommt aufgrund der Safety-Kopplung, beispielsweise mittels Buskopplern, die

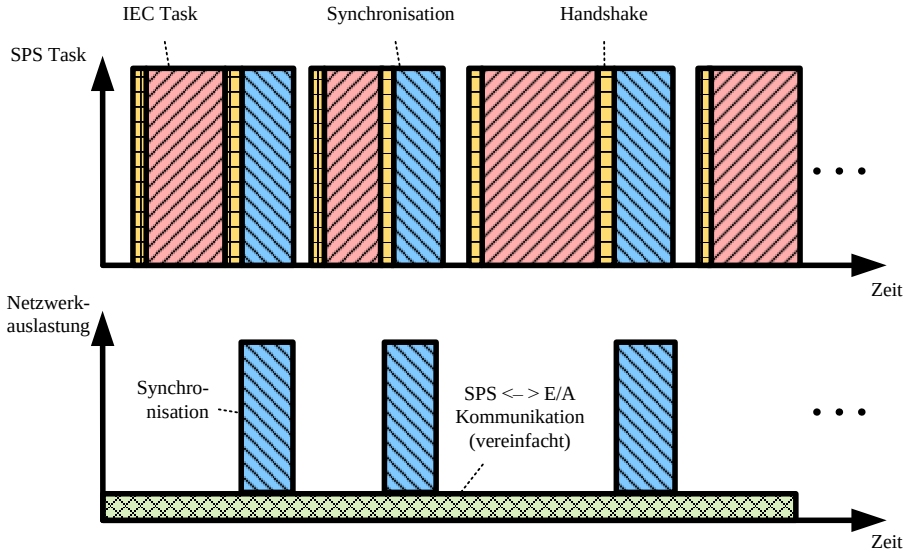


Abbildung 5.12: Der Einfluss variierender Ausführungsdauer eines SPS-Zykluses auf die Synchronisation, wodurch auch bei zyklischen Anwendungen azyklische Kommunikationsmuster entstehen können, nach [KG23a].

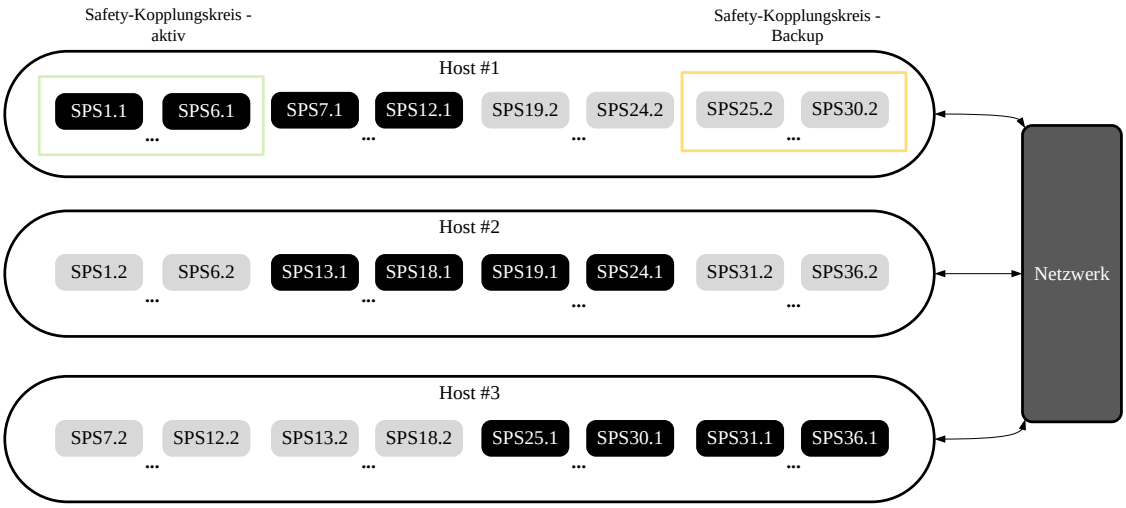


Abbildung 5.13: Anordnung von vSPS-Instanzen zur Reduktion von Fehlerzuständen

jeweiligen gekoppelten Bereiche zum Stehen. Diese Anordnung vereinfacht weiterhin die Möglichkeit eines virtuellen Buskopplers, da Kommunikation zwischen den SPS-Bereichen ausschließlich in dem Server erfolgen kann.

5.5.5.3 Stoßfreie Hochverfügbarkeit

Der abschließende Aspekt des entwickelten Konzeptes ist ein stoßfreier Failover-Mechanismus für geplante und ungeplante Szenarien. Hierfür müssen die Echtzeiteigenschaften des jeweiligen Prozesses erfüllt werden. Failover-Zeiten im Bereich von wenigen Millisekunden erfordern die Erkennung einer ausgefallenen primären vSPS in geringerer Zeit als dem festgelegten WDT. Dies wird durch ein hochfrequentes Heartbeat-Signal erreicht, das beispielsweise jede Millisekunde oder häufiger gesendet wird. Gleichzeitig muss die Backup-Anwendung bereits im laufenden Zustand sein, um das gewünschte stoßfreie Verhalten zu erreichen. Dies wird durch gleichzeitige Berechnungen innerhalb der primären und der Backup-Anwendung erreicht. Im Fall der vSPS wird der jeweilige IEC-Task in beiden Anwendungen ausgeführt und am Ende des Zyklus synchronisiert, bevor die Ausgangswerte geändert werden. Schließlich muss das IE-Protokoll eine stoßfreie Übernahme durch eine zweite SPS-Instanz unterstützen, wie es beispielsweise der PROFINET S2-Standard vorsieht.

5.6 IT/OT-Security

Dieser Abschnitt enthält eine Validierung des entwickelten IT/OT-Security-Konzeptes und vergleicht das Security-Level mit dem in Abschnitt 2.1.2 beschriebenen Segmentierungsansatz auf Basis der Automatisierungspyramide. Hierzu werden drei verschiedene Methoden verwendet: eine formale Bewertung basierend auf IEC 62443-3-3, eine praxisnahe Bewertung auf Basis der Cyber-Kill-Chain sowie den kritischsten Angriffsvektoren für industrielle Steuerungssysteme laut dem Deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI) und ausgelöst durch die Konvergenz von IT und OT. Zunächst erfolgt nun allerdings die Überprüfung der Segmentierung von IE mittels VXLAN.

5.6.1 Mikrosegmentierung von Schicht 2-Kommunikation

Unter der Nutzung von VXLAN als Tunnel-Protokoll können Kommunikationsteilnehmer in SG zusammengefasst werden. Dies wird durch die Definition von GBP innerhalb des VXLAN-Headers erreicht. Im Folgenden wird nun die Verwendung von GBP für die Segmentierung von Kommunikationsteilnehmern eines Netzwerkes auf Schicht 2 betrachtet.

Hierzu wird der in Abbildung 5.14 dargestellte Versuchsaufbau verwendet, zum einen unter Nutzung von Netzwerkkomponenten des Unternehmens Cisco, zum anderen von Juniper. Zwei verschiedene GBP werden den jeweiligen Geräten zugewiesen und die Schicht 2-Kommunikation mittels GBP-basierten Regeln versucht zu unterbinden.

Es zeigt sich, dass sich die Implementierungen der einzelnen Netzwerkherstellern voneinander unterscheiden. Während eine Kommunikation von den Juniper-Geräten unterbunden wird, ist dies bei Cisco nicht der Fall. Dies liegt darin begründet, dass die Implementierung bei

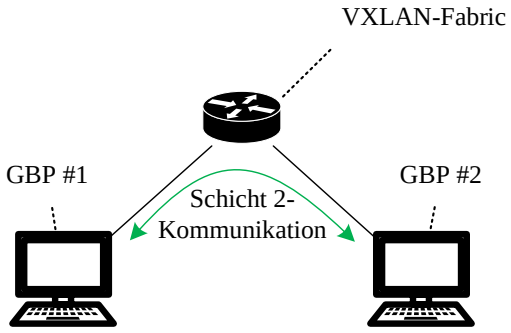


Abbildung 5.14: Evaluierung der Mikrosegmentierung von Schicht 2-Kommunikation

Cisco nur auf IP-Basis erfolgt und somit für Schicht 2-Kommunikation keine Segmentierung möglich ist.

5.6.2 Security-Level Beurteilung nach IEC 62443-3-3

Das methodische Vorgehen nach der Norm IEC 62443-3-3 wurde in Abschnitt 3.6.7.1 vorgestellt und ermöglicht eine systematische Analyse der Security-Anforderungen und -Maßnahmen, um das umgesetzte Security-Level zu bestimmen.

Für die beispielhafte Applikation vSPS werden die jeweiligen SL für die in Abschnitt 2.1.2 vorgestellte Architektur und das in Abschnitt 4.8 beschriebene Konzept erfasst und verglichen. Die komplette Evaluierung benötigt mehrere Seiten Dokumentation, weshalb nur ein relevanter Ausschnitt in Tabelle 5.8 dargestellt wird, in dem das SL durch die angewandten Maßnahmen verändert wurde. Durch die ausschließliche Anwendung von Maßnahmen im Netzwerk war es möglich, in diversen SR zu einem SL3 zu gelangen, welches einen guten Schutz vor Angriffen darstellt. Dies unterstreicht erneut den Stellenwert eines sicheren Netzwerkes innerhalb einer IT/OT-konvergierten Infrastruktur.

Allerdings verbleiben auch einige SL auf einem nicht adäquaten Niveau von SL1 oder darunter, beispielsweise SR 3.2 - Schutz vor Schadcode - aufgrund der fehlenden Antivirus-Software. Auch SR 3.3 - Verifikation der IT Sicherheitsfunktionalität - kann wegen fehlenden Security-Scans nicht erhöht werden. Diese Punkte können allerdings nach dem DiD-Ansatz auf anderen Ebenen aufgegriffen werden, beispielsweise durch Host-, Applikations- und physikalische Security. Im Rahmen des neuen Konzeptes wurden für keine SR oder RE das SL im Vergleich zur früheren Architektur reduziert.

5.6.3 Bewertung mittels Cyber Kill Chain

Die CKC-Methode bietet eine praxisorientierte Methode um Schutzmaßnahmen und Schwachstellen der Abwehr von Cyberangriffen zu identifizieren. Dies erweitert somit den formalen theoretischen Ansatz von IEC 62443-3-3 und ermöglicht eine umfassende Bewertung der IT/OT-Security-Architektur.

Tabelle 5.8: Auszug des Vergleichs gemäß der Systemanforderungen (SR) der IEC 62443-3-3 für das alte und das neu entwickelte Konzept anhand des exemplarischen Anwendungsfalles einer vSPS auf einer Edge Cloud nach [KMG24].

Anforderung	Alt	Neu
SR 2.8 Prüfbare Ereignisse und deren Aufzeichnung	/	SL3
SR 3.1 Kommunikationsintegrität	/	SL3
SR 4.1 Vertraulichkeit von Informationen	/	SL3
SR 5.1 Netzaufteilung	SL1	SL3
SR 5.2 Schutz der Zonengrenze	/	SL3
SR 6.2 Kontinuierliche Überwachung	/	SL3
SR 7.1 Schutz gegen DoS-Ereignisse	/	SL3
SR 7.8 Verzeichnis der Komponenten eines Automatisierungssystems	/	SL3

In einem beispielhaften Szenario wird untersucht, wie die definierten Schutzmaßnahmen Auswirkungen eines mit Malware infizierten USB-Stick einschränken können, welcher mit einem Host im IT/OT-konvergierten Netzwerk verbunden wird. Die Initiierung geschieht durch die Ausführung einer Datei mit Malware auf dem USB-Stick. Tabelle 5.9 enthält die Bewertung nach der CKC. Der zweite Schritt des CKC, die Bewaffnung, wird von Angreifern normalerweise in ihrer eigenen Umgebung durchgeführt und wird daher hier nicht berücksichtigt. Die Aktionen Degradieren, Täuschen und Zerstören werden ebenfalls nicht in der Tabelle aufgeführt, da sie in der aktuellen Architektur nicht berücksichtigt werden. Da die Maßnahmen das Echtzeitverhalten der Kommunikation oder Berechnungen negativ beeinflussen könnten, werden diese nicht verwendet [Roh19].

Tabelle 5.9: Handlungsoptionen-Matrix, um das Szenario infizierter USB-Stick nach der CKC-Methode zu bewerten [KMG24].

Phase	Erkennen	Verhindern	Vermindern
Aufklärung	IDS	ACL	
Lieferung	IDS SPI	IPS WAF	
Ausführung			
Installation			
Steuerung & Kontrolle	IDS SPI	ACL WAF	IPS
Aktionen mit Auswirkungen auf das Ziel	IDS SPI	IPS	

Lediglich auf der Basis von Schutzmaßnahmen innerhalb des Netzwerkes ist es bereits möglich, für die meisten Schritte der CKC Maßnahmen zu benennen, die Aktionen der jeweiligen Phase erkennen oder verhindern. Hierfür ermöglicht das strenge Segmentierungskonzept und die damit einhergehende effiziente Überwachung von Übergängen durch ein IDS und ein IPS auch bereits frühzeitig die Möglichkeit, verdächtige Aktivitäten innerhalb des Netzwerkes zu detektieren und zu unterbinden. Die Effektivität dieses Konzeptes ist

direkt verbunden mit der Korrelation von vorhandenen Daten im Asset Management, erlaubten Kommunikationsbeziehungen zwischen SG, sowie der Reduktion des Grundrauschens innerhalb von Firewall-Instanzen durch Mikrosegmentierung.

Dennoch zeigt sich auch, dass Maßnahmen im Netzwerk allein keinen umfassenden Schutz bieten. Die beiden Schritte Ausführung und Installation können nicht durch netzwerkseitige Maßnahmen verhindert oder erkannt werden, da in den jeweiligen Prozessschritten der CKC für gewöhnlich keine Interaktion mit Netzwerkkomponenten stattfindet. Dies verdeutlicht die Notwendigkeit der Adoption des DiD-Ansatzes, um neben Schutzmaßnahmen im Netzwerk auch Instrumente in Applikation, Host und physikalischen Bereichen zu nutzen.

5.6.4 Angriffsvektoren

Eine abschließende Bewertung findet durch die Betrachtung von Angriffsvektoren statt, die entweder der Literatur entnommen oder aufgrund der Etablierung einer Edge Cloud-Instanz und dem damit verbundenen Netzwerkkonzept entstanden sind.

5.6.4.1 Industrielle Ethernet-Protokolle

IE-Protokolle, wie PROFINET, EtherNet/IP und Modbus TCP, bieten eine große Angriffsfläche. Daten werden in Klartext übertragen, sodass jegliche Kommunikation vor Empfang manipuliert werden kann. Hierbei handelt es sich sowohl um Datenverkehr, der Einfluss auf die Physik der Prozesse nimmt, als auch Daten mit einer Notwendigkeit der Speicherung, beispielsweise bei sicherheitsrelevanten Verschraubungen. Dies betrifft weiterhin auch Addressierungsformen, beispielsweise Stationsnamen in PROFINET, als auch Benutzernamen und Passwörter. Durch die Echtzeitanforderungen und Kostendruck der jeweiligen Geräte der Automatisierungstechnik sind Verschlüsselungen des Datenverkehrs derzeit nur in Ausnahmefällen möglich. Erweiterungen, die die vorhandene IE-Protokolle um Maßnahmen zur Absicherung erweitern, sind jedoch bereits in Arbeit oder veröffentlicht [Wal+23]. Die Anforderung, vorhandene Infrastrukturkomponenten auch weiterhin zu betreiben und abzusichern, erfordert jedoch die Nutzung von Mechanismen außerhalb neuer Funktionen in IE-Protokollen.

Aktuelle Safety-Protokolle wie PROFIsafe bieten ebenfalls keinen ausreichenden Schutz gegen die beschriebenen Angriffe, da die Prüfung der Datenintegrität mittels des Cyclic Redundancy Check-Ansatzes als unsicher gilt [ÅB09]. Hier sollten kryptografische Maßnahmen wie PHYsec oder MACsec eingesetzt werden, um die Datenintegrität der Klartext-Kommunikation zu gewährleisten [IEE18; LAS20; Tia+23]. Safety-Protokolle, die derzeit von den Standardisierungsorganisationen entwickelt oder erweitert werden, könnten bestimmte Probleme mindern, indem sie beispielsweise den Schlüsselaustausch und das Vertrauen zwischen Kommunikationspartnern in der Automatisierungsdomäne verbessern [Wal+23].

5.6.4.2 Zeitsynchronisation

Ein gemeinsames Verständnis von Zeit, relativ oder absolut, ist eine verbreitete Anforderung von Steuerungs-Applikationen und -Netzwerken. Es erleichtert die Fehlersuche durch mit Zeitstempel versehene Aktionen und Logs, die eine zeitliche Korrelation über mehrere physikalische Grenzen hinweg erlauben, was auch innerhalb von verteilten Systemen essenziell ist. Auch ermöglicht dies einen Kommunikationszeitplan für Datenströme zu erzeugen, um mittels reservierten Zeitslots eine deterministische Datenübertragung zu ermöglichen. Final benötigen sicherheitsrelevante Applikationen Gewissheit, dass das vorhandene relative Zeitverständnis korrekt ist. Dies wird beispielsweise in Implementierungen von Safety-SPS durch zwei Oszillatoren ermöglicht, deren Frequenzen regelmäßig verglichen werden, um die Wahrscheinlichkeit für ein zu schnelles oder langsames Agieren der Applikation zu mindern.

Die Zeitsynchronisation ist somit für bestimmte Funktionen innerhalb der OT-Domäne unerlässlich und erfordert daher Implementierungen von PTP, wie IEEE 802.1AS oder IEEE 1588, die die Authentifizierung der Kommunikationspartner und Verschlüsselung beinhalten. Während dies für Network Time Protocol (NTP) unter dem Namen Network Time Security (NTS) standardisiert wurde, befindet sich die PTP-Implementierung noch im Entwurfsstatus [Fra+20; LB22]. Das Fehlen von Sicherheitsfunktionen bei PTP wurde bereits in der Vergangenheit diskutiert und MACsec sowie IPSec als mögliche Mechanismen zur Sicherung der Zeitsynchronisation vorgeschlagen [Miz11].

5.6.4.3 Paketduplizierung

Hochverfügbarkeit und Zuverlässigkeit sind zentrale Eigenschaften industrieller Netzwerke und eines der zentralen Anforderungen an ein IT/OT-konvergiertes Netzwerk. Besonders in großen Installationen mit konsolidierten Applikationen ist die Duplizierung von Paketen ein notwendiger Mechanismus, um die gewünschten Anforderungen zu erfüllen. Eine Vielzahl von Standards bietet unterbrechungsfreie Kommunikation in Failover-Szenarien durch Duplizierung von Telegrammen, beispielsweise PRP und HSR gemäß IEC 62439-3 oder IEEE 802.1CB [IEE17; Int+16].

Der Mechanismus der Paketduplizierung bietet jedoch auch einen neuartigen Angriffsvektor. Die Erkennung von Duplikaten am Endpunkt basiert auf Sequenznummern, die je nach verwendetem Protokoll entweder im Header oder Trailer eingebettet sind. Durch die fehlende Verschlüsselung und Integritätsprüfung ist es möglich, die Sequenznummer zu manipulieren, was dazu führen kann, dass gültige Telegramme aufgrund einer unerwarteten Sequenznummer verworfen werden. Angreifer könnten somit Sequenznummern manipulieren, um die Kommunikation zu stören und die Zuverlässigkeit des Netzwerkes zu beeinträchtigen. Dies unterstreicht die Notwendigkeit zusätzlicher Maßnahmen, um die Integrität und Authentizität der Daten zu gewährleisten.

5.6.4.4 Bewertung der Angriffsvektoren

Dieser Abschnitt enthält eine Diskussion der wahrscheinlichsten Bedrohungen für industrielle Steuerungssysteme, veröffentlicht vom BSI. Die Angriffsvektoren sind innerhalb von Tabelle 5.10 mit den Bezeichnungen AV1) - AV10) versehen. Ebenfalls enthalten sind die in den vorherigen Abschnitten beschriebenen Angriffsvektoren AV11) - AV13) aufgrund der Konvergenz von IT und OT. Verglichen wird der aktuelle Schutz auf Basis von traditionellen Ansätzen, beschrieben in Abschnitt 2.1.2, mit dem vorgestellten IT/OT-Security-Konzept.

Tabelle 5.10: Änderungen des Security-Levels durch Adoption des entwickelten IT/OT-Security-Konzeptes als Reaktion auf die wahrscheinlichsten Angriffsvektoren beschrieben durch das BSI sowie durch neue Angriffsvektoren ausgelöst durch die Konvergenz von IT und OT.

	Angriffsvektor	SL
AV1)	Schadsoftware einschleusen über Datenträger / mobile Systeme	gesteigert
AV2)	Infektion mit Schadsoftware über Internet und Intranet	gesteigert
AV3)	Kompromittierung von Extranet und Cloud-Komponenten	gesteigert
AV4)	Internet-verbundene Steuerungskomponenten	gesteigert
AV5)	Einbruch über Fernwartungszugänge	gesteigert
AV6)	(D)DoS Angriffe	gesteigert
AV7)	Technisches Fehlverhalten und höhere Gewalt	gesteigert
AV8)	Menschliches Fehlverhalten und Sabotage	gleich
AV9)	Social Engineering und Phishing	gleich
AV10)	Soft- und Hardwareschwachstellen in der Lieferkette	gleich
AV11)	Industrielle Ethernet-Protokolle in der IT/OT-Konvergenz	gesteigert
AV12)	Paketduplizierung	gesteigert
AV13)	Zeitsynchronisation	gesteigert

Die Angriffsvektoren AV1), AV2), und AV3) werden durch konsequente Mikrosegmentierung und der Sicherung von Zonenübergängen durch Systeme wie IDS abgeschwächt. Hierdurch kann nach einer Kompromittierung eines Hosts oder Gerätes die Ausbreitung auf eine oder wenige SG beschränkt und die auffälligen Geräte isoliert werden. Dies trifft auch auf AV4) zu, wobei hier zusätzlich Maßnahmen wie DPI Anwendung finden. Durch die Etablierung von dedizierten, temporären Fernwartungszonen mit einer minimalen Anzahl an Rechten sind Zugriffe von außen nach AV5) einschränkbar. Die rigorose Etablierung und Umsetzung von NAC ermöglicht in Kombination mit der Reduktion der Angriffsfläche mittels Mikrosegmentierung eine Verminderung der Auswirkung und Wahrscheinlichkeit von erfolgreichen (D)DoS-Attacken. Weiterhin werden durch die Etablierung von IT-Hardware und -Konzepten die Verfügbarkeit von Applikationen gesteigert, da konzeptionell Redundanzen innerhalb des Netzwerkes und der Edge Cloud-Umgebung vorgesehen werden.

AV8), AV9) und AV10) bleiben auch nach der Anwendung des Konzeptes in ihrem Schutz-Level unverändert. Hier sind vor allem Maßnahmen aus anderen Bereichen des DiD-Ansatzes zu nennen, die eine Verbesserung erwirken können, beispielsweise durch die Notwendigkeit der Erzeugung von Artefakten mittels gesicherten Continuous Integration/Continuous

Deployment (CI/CD)-Pipelines.

AV11) erfordert vor allem die Sicherung der Datenintegrität aufgrund der Klartext-basierten Kommunikation der IE-Protokolle. Hierfür werden technologieneutral mehrere Optionen vorgeschlagen, beispielsweise die Nutzung von Hop-zu-Hop-Verschlüsselung auf Basis von PhySec oder MACsec. Auch für AV12) können die selben Mechanismen das Security-Level erhöhen. Innerhalb von AV13) kann beobachtet werden, dass ein Zero Trust-Netzwerk mit Verschlüsselung keine zusätzlichen Anpassungen der Protokolle benötigt, um den Prozess der Zeitsynchronisation abzusichern. Neben NAC und dedizierten Mikrosegmenten für Zeitquellen ermöglichen erneut Verschlüsselungsprotokolle einen verbesserten Schutz.

5.6.5 Bewertung des IT/OT-Security-Konzeptes

Auf Basis der Evaluierung mittels drei verschiedener Ansätze konnte das Security-Level in verschiedenen Bereichen der IT/OT-konvergierten Infrastruktur signifikant gesteigert werden.

Die Evaluierung der Mikrosegmentierung mittels GBP verdeutlicht fehlendes Standardverhalten, vermutlich ausgelöst durch den fehlenden RFC, wie in Abschnitt 3.2.1 beschrieben. So ist es mit der GBP-Implementierung des Unternehmens Juniper Networks, Inc. möglich, auch Schicht 2-Kommunikation einzuschränken, während dies mit Komponenten des Unternehmens Cisco Systems, Inc. nur auf Schicht 3 möglich ist.

Die systematische Evaluierung nach IEC 62443-3-3 bestätigt wiederum die Eignung des entwickelten IT/OT-Security-Konzeptes für Industrie 4.0 Applikationen wie eine vSPS auf einer verteilten Umgebung. Anhand der CKC wird erneut die Relevanz des DiD-Ansatzes deutlich, stellt allerdings auch die weitreichenden Schutzmöglichkeiten durch Konzepte innerhalb des Kommunikationsnetzwerkes dar.

Hierbei kommen an verschiedenen Stellen unterschiedliche Mechanismen zum Tragen. Dies verdeutlicht auch die Notwendigkeit des ineinandergreifenden IT/OT-Security-Konzeptes, welches durch die Verkettung der Mechanismen die Einhaltung der jeweiligen Bausteine fordert. Für eine Reihe an unterschiedlichen Angriffsvektoren konnte das Schutzlevel gesteigert werden. Dies gilt insbesondere für neue Angriffsflächen, die durch die Konvergenz von IT und OT entstehen.

5.6.5.1 Sichere Software-Lieferkette und Code-Ausführung

Auch die Häufigkeit von Cyberangriffen auf Lieferketten nimmt stetig zu [Bun22]. Eine sichere und automatisierte Software-Lieferkette ist jedoch ein oft übersehener Bestandteil, der zwar in IT-Unternehmen Standard ist, allerdings noch keine Verbreitung innerhalb der Automatisierungsdomäne erfahren hat. Aufgrund der Kritikalität von SPS-Programmen, vor allem für Produktqualität, Produktivität und menschliche Sicherheit, ist an dieser Stelle auf ein fehlendes Sicherheitsniveau in der Lieferkette für Software-Artefakte im OT-Bereich hinzuweisen. Dies wurde auch bereits in der Literatur als schwerwiegende Schwachstelle identifiziert [AL15].

Aktuell werden SPS-Programme lokal in einem Engineering-Programm von OT-Personal modifiziert, kompiliert, und direkt auf die jeweilige (v)SPS geladen. Für zukünftige Implementierungen empfehlen sich allerdings die Anwendung folgender Maßnahmen für eine sichere Software-Lieferkette:

- Der Code muss über eine sichere CI/CD-Pipeline geliefert werden.
- Anwendungen sollten nur signierten Code ausführen können.
- Anwendungen auf Cloud-Infrastrukturen müssen gesichert werden, beispielsweise durch die Vermeidung von Kernel-Leaks nach dem System BeyondProd [Bak20].

5.7 Konvergenz zwischen kabelgebundener und kabelloser Kommunikation

Obwohl kabellose Kommunikation bisher nicht im Fokus dieser Arbeit lag, ergibt sich zum Abschluss dieses Kapitels die Notwendigkeit, dieses Übertragungsmedium auch im industriellen Kontext zu würdigen. Vor allem das Industrial Internet of Things (IIoT) ist getrieben durch eine steigende Adoption von kabelloser Kommunikationstechnologien. Das vor allem in Kapitel 4 vorgestellte Konzept kann im Allgemeinen auch auf dieses Kommunikationsmedium bezogen werden. Während die Anforderungen beispielsweise im IT/OT-Security-Bereich durch neue Angriffsvektoren leicht verändert sind, sind weitere Anforderungen in Bezug auf Echtzeitfähigkeit, Hochverfügbarkeit, und Determinismus identisch.

In einer vorangegangen Veröffentlichung wurde die Interoperabilität zwischen 5G und DetNet und identifizierte Lücken in der Standardisierung beider Technologien beschrieben, um die Integration beider Standards zu erreichen [Amb+22]. Während die Integration zwischen 5G und TSN bereits beschrieben ist, fehlt dies in der notwendigen Ausführlichkeit für 5G und DetNet. Standardisierungsgremien wie die 5G-ACIA haben bereits Ansätze zu den Themen Virtualisierung einerseits und Sicherheitskonzepte und -anforderungen für eine 5G-OT-Integration andererseits veröffentlicht [5A21; 5A23].

Durch die Auslagerung von zuvor in mobilen Robotern befindlichen Steuerungen ergeben sich neue Optionen in der Flexibilität als auch Einsparungen von Ressourcen. Dies ist vergleichbar mit der zuvor beschriebenen Konsolidierung von im Shopfloor befindlichen Hardware-Ressourcen auf einer Edge Cloud. Hierzu ist jedoch ein deterministisches Netzwerk notwendig, welches über physikalische Medien hinweg besteht. Hierzu wurde die Interoperabilität von 5G und DetNet als eine Lücke in konvergierten kabelgebundenen und drahtlosen Netzwerken identifiziert und die Notwendigkeit für Echtzeitfähigkeit und Resilienz auf Schicht 3 des ISO/OSI-Modells für ein ganzheitliches deterministisches Netzwerk aufgezeigt [Amb+22]. Darauf basierend wurde ein Konzept entwickelt, das die Anforderungen zukünftiger industrieller Netzwerke erfüllen soll. Letztlich ist jedoch eine Standardisierung von DetNet in Kombination mit Funkstandards wie 5G notwendig, um ein vollständig integriertes 5G- und DetNet-Netzwerk zu ermöglichen.

5.8 Fazit und Gegenüberstellung mit den Anforderungen

Die in diesem Kapitel vorgestellten Versuchsaufbauten demonstrieren die praktische Umsetzung und erlauben eine Bewertung der für die IT/OT-Konvergenz notwendigen Architekturbausteine. Tabelle 5.11 stellt die zuvor vor allem in Abschnitt 4.3 beschriebenen Anforderungen mit den jeweiligen Architekturbausteinen und den validierten Ergebnissen gegenüber. Es zeigt sich, dass das entwickelte Architekturkonzept jegliche Anforderungen voll oder zumindest im überwiegenden Maß erfüllt.

Kommunikation von zuvor auf dem Shopfloor befindlichen Applikationen mit deren Kommunikationspartnern konnte mittels COTS-Hardware und des Tunnelprotokolls VXLAN erreicht werden. Hierzu wurden umfassende Versuchsaufbauten verwendet um über verschiedene Hersteller hinweg funktionierende Konfigurationen zu ermitteln und validieren. Das Architekturkonzept konnte die Anforderung der Migration zu verteilten Systemen erfüllen und die notwendigen prozessualen Anpassungen für OT-Personal minimieren.

Die erste Forschungsfrage, beschrieben in Abschnitt 2.4, stellt die Frage nach Mechanismen, die den notwendigen Determinismus für echtzeitkritische Applikationen bereitstellen können. Dies wurde vor allem durch Ende-zu-Ende Übertragungszeiten im Mikrosekundenbereich erreicht, welche damit die Anforderungen von Applikationen mit harten Echtzeitanforderungen erfüllen. Klassische Netzwerkmechanismen des QoS konnten hierfür unter betriebsnahen Bedingungen erfolgreich erprobt werden. Die Nutzung des IvS wurde darüber hinaus unter der Nutzung von vSPS validiert und ermöglicht auch in der virtualisierten Umgebung eine deterministische Kommunikation.

Die Erreichung der Zuverlässigkeit für die Automatisierungsdomäne wurde als zweite Forschungsfrage in Abschnitt 2.4 identifiziert. Hierbei nehmen Kommunikationsnetzwerke aufgrund der Verlagerung von Automatisierungsapplikationen in konsolidierte Edge Cloud-Umgebungen eine zentrale Rolle ein. Außerdem erfordert auch die Konsolidierung selbst neue Ansätze, um die Verfügbarkeit der Applikationen und Prozesse zu erhöhen.

Zunächst wurden hierzu zwei Möglichkeiten zur Erreichung von mehreren Pfaden aufgezeigt. Während die Option mit einer VXLAN-Fabric nur konzeptionell und auf einer theoretischen Ebene beschrieben wurde, konnte das Konzept mit einem Dual-Fabric Ansatz erfolgreich validiert werden. Hierzu wurde das statische Redundanzprotokoll PRP genutzt, um die gesamte Strecke innerhalb des IP-basierten Netzwerkes abzusichern. Durch die Erweiterung von Single-Path Kommunikation und Paketduplizierung durch das entwickelte Redundanzkonzept Half&Half ist es möglich, aus drei vordefinierten Betriebsmodi zu wählen und Datenströme an ihre Resilienzanforderungen anzupassen und die Komplexität durch die Eliminierung der Paketduplizierung zu verringern.

Die Hochverfügbarkeitanforderungen für zustandsbehaftete Applikationen mit harten Echtzeitanforderungen wie vSPS konnte mittels des RoCE-basierten Konzeptes erfüllt werden. Hierfür waren vor allem in diesem Abschnitt umfangreiche Softwareentwicklungen notwendig, da aufgrund des frühen Stadiums der IT/OT-Konvergenz IT-Standards wie RDMA bisher keine Verbreitung in der Automatisierungsdomäne finden. Die Validierung erfolgte sowohl

durch die Modifikation einer vSPS als auch die Ergänzung durch ein deterministisches IP-basiertes Netzwerk, welche die Erweiterung auf ein geo-redundantes Konzept eröffnet. Weiterhin wird somit die direkte Übertragung von Applikationen auf verteilte Systeme ermöglicht, wodurch zuvor Hardware-gebundene Applikationen von erhöhter Flexibilität und Skalierbarkeit auf Cloud-Umgebungen profitieren können. Die Konsolidierung der zuvor auf dem Shopfloor verteilten Applikationen eröffnet die Entwicklung neuer Software-Architekturen und der Steigerung der Nachhaltig- und Wirtschaftlichkeit. Abschließend konnte auch das Konzept der partiellen Synchronisation erfolgreich getestet werden.

Die dritte Forschungsfrage in Abschnitt 2.4 handelt von der Erfüllung der steigenden Cybersicherheitsanforderungen im Kontext der IT/OT-Konvergenz. Hierzu wurde das entwickelte IT/OT-Security-Konzept auf Basis von drei verschiedenen Methoden evaluiert. Es zeigt sich, dass alleinige Maßnahmen innerhalb des Kommunikationsnetzwerkes bereits einen weitreichenden Schutz gegenüber einer Vielzahl an Bedrohungen erbringen. Gleichzeitig wurden auch die Limitierungen der Möglichkeiten durch Netzwerk-basierte Maßnahmen deutlich, da die anderen Ebenen nach dem DiD-Ansatz nicht geschützt werden können.

Tabelle 5.11: Vergleich der Anforderungen gemäß Abschnitt 4.3 exemplarischen Anwendungsfalles einer vSPS auf einer Edge Cloud.

Anforderungsgruppe	Anforderung	Ergebnis	Mechanismen
IE über IP	Übertragung von IE-Protokollen über ein IP-basiertes Netzwerk	Schicht 2-Kommunikation über IP ist möglich, inklusive Schicht 2-Multicast	VXLAN
	Rekonfigurationsaufwand gering	Die Migration zur vSPS benötigt keine Anpassungen des SPS-Programms	VXLAN
	Skalierbarkeit	Die gesamte Netzwerkstrecke zwischen den Kommunikationsteilnehmern ist zentralisiert konfigurierbar und automatisierbar	SDN
	LLDP-basierte Mechanismen funktionieren	Ein Gerätetausch ist auch möglich, wenn die vSPS keine LLDP-Telegramme erhält	Keine notwendig
Determinismus	Ein-Wege-Latenz geringer als 0,5 ms	Latenzzeiten unter 0,5 ms werden dauerhaft erreicht	QoS oder DetNet
	Jitter geringer als 0,5 ms	Latenzzeiten unter 0,5 ms werden dauerhaft erreicht	QoS oder DetNet
	Echtzeitfähigkeit der virtuellen Plattform	Ergebnisse des Cyclictests geringer als 50 µs	Echtzeit-Tuning Plattform und VM
HA - Netzwerk	Zwei Pfade durch das Netzwerk	Ermöglicht durch getrennte Underlays	Dedizierte Fabrics
	Minimale Anzahl an SPOF	Verlagerung der PRP-RedBox so nah wie möglich an Kommunikations-Quelle und -Ziel	PRP / Half&Half
	WDT = 3 ms wird bei Ausfall eines Netzwerkgerätes nicht ausgelöst	Im Fehlerfall wird maximal ein Telegramm in Folge verloren, sodass kein WDT ausgelöst wird	PRP / Half&Half
HA - vSPS	Sicherung der Daten im Fehlerfall	Synchronisation der Puffer in eine Backup-Applikation	Aktiv/Backup-Konzept
	Vermeidung eines Split Brain-Szenarios	Übertragung eines Heartbeats im selben physikalischen und virtuellen Netzwerk	Heartbeat
	Synchronisationszeit im akzeptablen Rahmen	Synchronisation des Puffers mittels RDMA-Technologie	RDMA
	RDMA über DetNet	RoCE basiert auf UDP, DetNet erfüllt RoCE-Anforderungen	RoCE
	Stoßfreie Hochverfügbarkeit	Notwendigkeit der Protokoll- und Geräteunterstützung	Beispielsweise PROFINET S2
IT/OT-Security	Level an Security soll gleich oder erhöht werden	SL wurden erhöht, die häufigsten Angriffsvektoren reduziert	Ineinandergreifende IT/OT-Security
Betreibbarkeit	Komplexität für OT-Personal nicht erhöht	Sowohl Bedienmöglichkeiten als auch physikalische Anbindungen bleiben weitestgehend unverändert - genutzte Applikationen identisch	VXLAN und Remote Desktop
	Beobachtbarkeit des Systems möglich	Metriken und Logs sind erfassbar	Loggenerierung und Messungen mit TWAMP

6 Zusammenfassung und Ausblick

Dieses Kapitel fasst die Ergebnisse der Arbeit zusammen. Hierbei werden Vorgehensweise, Konzepterstellung, und Validierung kritisch diskutiert. Ein Ausblick auf weiterführende Arbeiten schließt das Kapitel ab.

6.1 Zusammenfassung

Die fortschreitende Konvergenz von IT und OT erzeugt eine Vielzahl an Herausforderungen für Steuerungstechnik, Kommunikationsnetzwerke, Organisation und Unternehmen. Die Komplexität dieses Wandels wird vor allem in der Kommunikationstechnik deutlich, welche nicht nur gleichzeitig die Anforderungen aus unterschiedlichen Domänen erfüllen muss, sondern auch die zentrale Rolle als Wegbereiter für Innovation einnimmt. Die zunehmende Virtualisierung von zuvor Hardware-gebundenen Applikationen bietet neue Möglichkeiten in der Handhabung von Applikationen und der Steigerung der Effizienz und Flexibilität von Prozessen.

In den Kapiteln 2 und 3 wird die Notwendigkeit für ein Architekturkonzept deterministischer Kommunikationsnetzwerke motiviert. Auf Basis von geschichtlichen Ereignissen und dem Stand der Wissenschaft werden Barrieren für die Adoption Industrie 4.0-Technologien identifiziert, die durch ein neuartiges Konzept überwunden werden können. Auch die Akzeptanz durch den Menschen wird im Rahmen dieser Kapitel und den folgenden Anforderungen an Steuerungs- und Kommunikationstechnologie viel Beachtung geschenkt.

Das Kapitel 4 beschreibt die Entwicklung eines deterministischen Architekturkonzeptes für IT/OT-Konvergenz. Hierzu werden zunächst Anforderungen an ein solches Konzept definiert und in verschiedene Gruppen unterteilt, auf dessen Basis Architekturbausteine entwickelt werden. Die Übertragung von Industrial Ethernet und klassischem IT-Datenverkehr wird mittels VXLAN-Technologie auf einer gemeinsamen Netzwerkinfrastruktur ermöglicht. Durch die konsequente Integration der Virtualisierungstechnologie wird ein hochverfügbares Konzept für Netzwerk und Applikation entwickelt, welches auf Paketduplizierung und Lastverteilung als auch zyklische Synchronisation von Applikationsdaten beruht. Das netzwerkbasiertes IT/OT-Security-Konzept erlaubt eine sichere Integration der Edge Cloud mit der Automatisierungsdomäne und sichert Steuerungs-Datenverkehr und -Applikationen vor Angreifern.

Die Mechanismen wurden anschließend in Kapitel 5 experimentell validiert und die Ergebnisse kritisch diskutiert. Eine Gegenüberstellung mit den in Abschnitt 4.3 definierten Anforderungen und den in Abschnitt 2.4 beschriebenen Forschungsfragen verdeutlicht die Reife des entwickelten Architekturkonzeptes. Die Betrachtung von Software und Hardware, virtueller und physischer Welt, führt zu industriellen Netzwerken, die nicht nur leistungsfähi-

ger, sondern auch sicherer und flexibler sind. Dies ermöglichte die Entwicklung eines robusten Konzeptes für die Migration zur Edge Cloud-basierten Produktion und zur Erfüllung der Visionen nach Industrie 4.0.

6.2 Weiterführende Arbeiten

Automatisierung der Netzwerk-Administration und -Konfiguration sind bereits Teil von modernen Netzwerkinfrastrukturen [APC23]. Aufgrund der Kritikalität der Kommunikationsnetzwerke werden auch zunehmend formale und experimentelle Verifikationen von Änderungen der Konfiguration notwendig werden, um die Verfügbarkeit der Kommunikationsnetzwerke hoch zu halten [Pad+23]. Diese bieten auch im Kontext der IT/OT-Konvergenz eine vielversprechende Methodik zur Erreichung einer zuverlässigen Infrastruktur.

Im Bereich der IT/OT-Security werden durch die Einführung neuer Technologien und Standards neue Konzepte ermöglicht. Auch die weitflächige Adoption von künstlicher Intelligenz eröffnet neue Mechanismen in der Detektion von schädlichem Code und Angreifern. Weiterhin empfiehlt sich die Kombination mit Ansätzen aus der physikalischen, Host- und applikativen Schichten zur Erreichung eines holistischen Schutzes.

Die Erweiterung durch kabellose Kommunikation stellt einen wichtigen Aspekt der IT/OT-Konvergenz dar, um die Gruppe der Applikationen mit Mobilitätsanforderungen in das Architekturkonzept zu integrieren. Hierbei ist im besonderen Maße auf die IT/OT-Security-Anforderungen zu achten, die durch die Nutzung kabelloser Kommunikation entstehen. Weiterhin erfordert die Erreichung des notwendigen Determinismus aufgrund von Interferenzen und anderen Umwelteinflüssen robuste, skalierbare Konzepte. Zur selben Zeit sollten einige der Erkenntnisse und Konzepte wie Paketduplizierung zur Erreichung der notwendigen Verfügbarkeit, auch in Roaming-Szenarien zwischen Antennen, eingesetzt werden.

Die Weiterentwicklung von vorherrschenden Standards innerhalb der Automatisierungsdomäne stellt einen zentralen Pfeiler für weiterführende Arbeiten dar. Jegliche Ethernet-basierten Standards sollten hierbei mit dem vorgestellten Konzept evaluiert werden, inklusive Protokolle für Bewegungsregelungen. Insbesondere hervorzuheben ist auch die Entwicklung von Verschlüsselungs- und Integritätsmechanismen zur Absicherung der jeweiligen Prozesse und der Auflösung des Zielkonfliktes, Automatisierungsgeräte günstig und einfach zu halten.

Eine Analyse der mit der Veränderung des Betriebsmodells einhergehende Anpassung von notwendigen Fähigkeiten und Berufsbildern innerhalb der industriellen Produktion stellt einen weitere vielversprechende Forschungsfrage dar. Dies schließt auch den Sachverhalt der Koexistenz mit vorhanden Strukturen ein.

Einige der entwickelten Architekturbausteine können auch in anderen Anwendungsbereichen Fortschritte erbringen. Als Beispiel erfordern KI-Rechencluster bereits heute niedrige Übertragungszeiten mit kontrolliertem Fehlerverhalten und zuverlässiger Infrastruktur. Determinismus in der Kommunikation und im Training von KI-Modellen könnte die Effizienz von vorhandener Trainings-Mechanismen verbessern oder neue Ansätze in verteilten Be-

rechnungen ermöglichen. Weiterhin gilt es den eindeutigen Einfluss dieser Parameter auf neuartige Trainings- und Inferenzkonzepte zu untersuchen.

Abschließend wird sich vermutlich auch der Verbraucherbereich vermehrt in Richtung Cloudtechnologie und einem Thin Client-Konzept entwickeln [Cha+14]. Hier stellt sich die Frage, wie eine Infrastruktur basierend auf (Edge) Cloud-Installationen und robusten, schnellen Kommunikationsnetzwerken die zukünftigen Anforderungen von Applikationen wie Extended Reality, Künstliche Intelligenz, und Videospielen erfüllen kann [Las+24].

Literaturverzeichnis

Eigene Publikationen

[Amb+22] Niklas Ambrosy, Thomas Kampa, Ulrich Jumar und Daniel Großmann. „5G and DetNet: Towards holistic determinism in industrial networks“. In: *2022 IEEE International Conference on Industrial Technology (ICIT)*. 2022, S. 1–6.

[KEG23] Thomas Kampa, Amer El-Ankah und Daniel Grossmann. „High Availability for virtualized Programmable Logic Controllers with Hard Real-Time Requirements on Cloud Infrastructures“. In: *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*. IEEE, 2023. DOI: 10.1109/indin51400.2023.10218014.

[KG23a] Thomas Kampa und Daniel Grossmann. „Experimental Validation of a RDMA-based High Availability Concept over a deterministic IP-based network“. In: *KommA 2023 - 14. Jahreskolloquium Kommunikation in der Automation*. 2023.

[KG23b] Thomas Kampa und Daniel Grossmann. „Half&Half: Intra-Flow Load Balancing and High Availability for Edge Cloud-enabled Manufacturing“. In: *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*. 2023, S. 1–4.

[KMG22] Thomas Kampa, Christian Klaus Mueller und Daniel Grossmann. „IP-based Architecture for an Edge Cloud enabled Factory: Concept and Requirements“. In: *2022 IEEE 18th International Conference on Factory Communication Systems (WFCS)*. IEEE, 2022, S. 1–6. DOI: 10.1109/wfcs53837.2022.9779162.

[KMG24] Thomas Kampa, Christian Klaus Müller und Daniel Großmann. „Interlocking IT/OT security for edge cloud-enabled manufacturing“. In: *1570-8705* 154 (2024), S. 103384. ISSN: 1570-8705. DOI: 10.1016/j.adhoc.2023.103384.

[Vog+21] Anna Vogt, Ralph Klaus Müller, Thomas Kampa, Rainer Stark und Daniel Großmann. „Concept and Architecture for Information Exchange between Digital Twins of the Product (CPS) and the Production System (CPPS)“. In: *2212-8271* 104 (2021), S. 1292–1297. ISSN: 2212-8271. DOI: 10.1016/j.procir.2021.11.217. URL: https://www.sciencedirect.com/science/article/pii/s221282712101115x.

Literatur

[5A21] 5G Alliance for Connected Industries und Automation. *Security Aspects of 5G for Industrial Networks*. 2021. URL: https://5g-acia.org/?jet_download=7644 (besucht am 12. 10. 2023).

[5A23] 5G Alliance for Connected Industries und Automation. *Industrial 5G Edge Computing – Use Cases, Architecture and Deployment*. 2023. URL: https://5g-acia.org/?jet_download=12597 (besucht am 12. 10. 2023).

[APC23] Mahmoud Abbasi, Javier Prieto und Juan Manuel Corchado. „Network Automation: From Intent-Based Networking to Cloud-Native Networking“. In: *Distributed Computing and Artificial Intelligence, Special Sessions I, 20th International Conference*. Hrsg. von Rashid Mehmood, Victor Alves, Isabel Praça u. a. Bd. 741. Lecture Notes in Networks and Systems. Cham: Springer Nature Switzerland, 2023, S. 418–427. ISBN: 978-3-031-38317-5. DOI: 10.1007/978-3-031-38318-2{\textunderscore}41.

[Abd+19] Leila Abdollahi Vayghan, Mohamed Aymen Saied, Maria Toeroe und Ferhat Khendek. „Microservice Based Architecture: Towards High-Availability for Stateful Applications with Kubernetes“. In: *IEEE 19th International Conference on Software Quality, Reliability and Security (QRS)*. 2019. DOI: 10.1109/qrs.2019.00034.

[Abr+19] Marcelo Abranches, Sepideh Goodarzy, Maziyar Nazari, Shivakant Mishra und Eric Keller. „Shimmy: Shared Memory Channels for High Performance Inter-Container Communication“. In: 2019. URL: https://www.usenix.org/conference/hotedge19/presentation/abranches.

[Aij19] Adnan Aijaz. „Packet Duplication in Dual Connectivity Enabled 5G Wireless Networks: Overview and Challenges“. In: *IEEE Communications Standards Magazine* 3.3 (2019), S. 20–28. ISSN: 2471-2825. DOI: 10.1109/mcomstd.001.1700065.

[ÅB09] Johan Åkerberg und Mats Björkman. „Exploring Network Security in PROFIsafe“. In: Springer, Berlin, Heidelberg, 2009, S. 67–80. ISBN: 978-3-642-04468-7. DOI: 10.1007/978-3-642-04468-7{\textunderscore}7. URL: https://link.springer.com/chapter/10.1007/978-3-642-04468-7_7.

[All+19] Tejasvi Alladi, Vinay Chamola, Reza M. Parizi und Kim-Kwang Raymond Choo. „Blockchain applications for industry 4.0 and industrial IoT: A review“. In: *IEEE Access* 7 (2019), S. 176935–176951.

[ACZ20] Tejasvi Alladi, Vinay Chamola und Sherali Zeadally. „Industrial control systems: Cyberattack trends and countermeasures“. In: *Computer Communications* 155 (2020), S. 1–8. ISSN: 0140-3664.

[ADM16] Thiago Alves, Rishabh Das und Thomas Morris. „Virtualization of Industrial Control System Testbeds for Cybersecurity“. In: *Proceedings of the 2nd Annual Industrial Control System Security Workshop on - ICSS '16*. Hrsg. von Unknown. New York, New York, USA: ACM Press, 2016, S. 10–14. ISBN: 9781450347884. DOI: 10.1145/3018981.3018988.

[And17] Volker P. Andelfinger, Hrsg. *Industrie 4.0: Wie cyber-physische Systeme die Arbeitswelt verändern*. Wiesbaden: Springer Gabler, 2017. ISBN: 978-3-658-15557-5.

[APP21] Murshedul Arifeen, Andrei Petrovski und Sergei Petrovski. „Automated micro-segmentation for lateral movement prevention in industrial internet of things (IIoT)“. In: *2021 14th International Conference on Security of Information and Networks (SIN)*. Bd. 1. 2021, S. 1–6.

[AL15] Michael J. Assante und Robert M. Lee. „The industrial control system cyber kill chain“. In: *SANS Institute InfoSec Reading Room* 1 (2015), S. 24.

[Aut+18] Philipp Autenrieth, Christian Lörcher, Christian Pfeiffer, Tobias Winkens und Ludwig Martin. „Current Significance of IT-Infrastructure Enabling Industry 4.0 in Large Companies“. In: *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. 2018, S. 1–8. DOI: 10.1109/ICE.2018.8436244.

[Bad+19] Amjad Badar, David Zhe Lou, Ulrich Graf, Christian Barth und Christian Stich. „Intelligent Edge Control with Deterministic-IP based Industrial Communication in Process Automation“. In: *15th International Conference on Network and Service Management: 1st International Workshop on Analytics for Service and Application Management (AnServApp 2019) : International Workshop on High-Precision Networks Operations and Control, Segment Routing and Service Function Chaining (HiPNet + SR/SFC 2019) : October 21-25 2019, Halifax, Canada*. Hrsg. von Hanan Lutfiyya. [Piscataway, NJ]: IEEE, 2019, S. 1–7. ISBN: 9783903176249. DOI: 10.23919/CNSM46954.2019.9012680.

[Bak20] Brandon Baker. „BeyondProd: The origin of Cloud-Native security at google“. In: *San Francisco, CA: USENIX Association* (2020).

[Bar+17] Nina Barthelmäs, Daniel Flad, Tobias Haußmann u. a. „Industrie 4.0 – eine industrielle Revolution?“ In: *Industrie 4.0*. Hrsg. von Volker P. Andelfinger. Wiesbaden: Springer Gabler, 2017, S. 33–56. ISBN: 978-3-658-15557-5. DOI: 10.1007/978-3-658-15557-5{\textunderscore}3. URL: https://link.springer.com/chapter/10.1007/978-3-658-15557-5_3.

[Bau+14] Wilhelm Bauer, Sebastian Schlund, Dirk Marrenbach und Oliver Ganschar. „Industrie 4.0–Volkswirtschaftliches Potenzial für Deutschland“. In: *Berlin/-Stuttgart* (2014).

[Bau17] Thomas Bauernhansl. „Die Vierte Industrielle Revolution – Der Weg in ein wertschaffendes Produktionsparadigma“. In: *Handbuch Industrie 4.0*. Hrsg. von Birgit Vogel-Heuser, Thomas Bauernhansl und Michael ten Hompel. Springer Reference Technik. Berlin: Springer Vieweg, 2017, S. 1–31. ISBN: 978-3-662-53254-6. DOI: 10.1007/978-3-662-53254-6{\textunderscore}1. URL: https://link.springer.com/chapter/10.1007/978-3-662-53254-6_1.

[BH14] Thomas Bauernhansl und Michael ten Hompel. *Industrie 4.0 in Produktion, Automatisierung und Logistik*. Springer Fachmedien Wiesbaden, 2014. ISBN: 978-3-658-04681-1. URL: https://mediatum.ub.tum.de/1236629.

[Bla+98] Steven Blake, David Black, Mark Carlson u. a. *An architecture for differentiated services*. 1998.

[Bos+14] Pat Bosshart, Dan Daly, Glen Gibb u. a. „P4“. In: *ACM SIGCOMM Computer Communication Review* 44.3 (2014), S. 87–95. ISSN: 0146-4833. DOI: 10.1145/2656877.2656890.

[BM13] Juergen Braun und Juergen Mottok. „Fail-safe and fail-operational systems safeguarded with coded processing“. In: *Eurocon 2013*. IEEE, 2013, S. 1878–1885. DOI: 10.1109/eurocon.2013.6625234.

[Bre24] Josh Bressers. *Why are vulnerabilities out of control in 2024?* 2024. URL: https://opensourcesecurity.io/2024/06/03/why-are-vulnerabilities-out-of-control-in-2024/ (besucht am 10. 08. 2024).

[Bro24] Broadcom Ltd. *VMware Compatibility Guide*. 2024. URL: https://www.vmware.com/resources/compatibility/search.php?deviceCategory=io&details=1&releases=589&deviceTypes=6&pFeatures=373&page=15&display_interval=10&sortColumn=Partner&sortOrder=Asc (besucht am 05. 10. 2024).

[Bun22] Bundesamt für Sicherheit in der Informationstechnik. *Industrial Control System Security Top 10 Bedrohungen und Gegenmaßnahmen 2022*. 2022. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/Empfehlungen-fuer-ICS-Betreiber/empfehlungen-fuer-ics-betreiber.html (besucht am 03. 10. 2024).

[But+05] Giorgio Buttazo, Giuseppe Lipari, Luca Abeni und Marco Caccamo. *Soft Real-Time Systems*. 2005. URL: https://link.springer.com/content/pdf/10.1007/0-387-28147-9.pdf.

[CSV16] Gianluca Cena, Stefano Scanzio und Adriano Valenzano. „Seamless link-level redundancy to improve reliability of industrial Wi-Fi networks“. In: *IEEE Transactions on Industrial Informatics* 12.2 (2016), S. 608–620. ISSN: 1551-3203.

[Cha+21] G. S. S. Chalapathi, Vinay Chamola, Aabhaas Vaish und Rajkumar Buyya. „Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions“. In: *Fog/Edge Computing For Security, Privacy, and Applications* 83 (2021), S. 293–325. ISSN: 2512-2193. DOI: 10.1007/978-3-030-57328-7{\textunderscore}12. URL: https://link.springer.com/chapter/10.1007/978-3-030-57328-7_12.

[Cha+14] Hyunseok Chang, Adiseshu Hari, Sarit Mukherjee und T. V. Lakshman. „Bringing the cloud to the edge“. In: *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2014. DOI: 10.1109/infcomw.2014.6849256.

[Che+17] Manuel Cheminod, Luca Durante, Lucia Seno u. a. „Leveraging SDN to improve security in industrial networks“. In: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. 2017, S. 1–7.

[Che+18] Baotong Chen, Jiafu Wan, Antonio Celesti u. a. „Edge Computing in IoT-Based Manufacturing“. In: *IEEE Communications Magazine* 56.9 (2018), S. 103–109. DOI: 10.1109/MCOM.2018.1701231.

[CHJ16] Inho Cho, Dongsu Han und Keon Jang. *ExpressPass: End-to-End Credit-based Congestion Control for Datacenters*. 2016.

[Cis21] Cisco. *CCNA - Implementing and Administering Cisco Solutions: Version 1.0.26*. 2021.

[Cis23] Cisco. *Cisco DNA Center User Guide, Release 2.3.4: Configure a Fabric Zone*. 2023. URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-4/user_guide/b_cisco_dna_center_ug_2_3_4/b_cisco_dna_center_ug_2_3_4_chapter_01110.html (besucht am 03. 10. 2024).

[Cra+20] Mihai Craciunescu, Oana Chenaru, Radu Dobrescu, Gheorghe Florea und Stefan Mocanu. „IIoT Gateway for Edge Computing Applications“. In: *Service oriented, holonic and multi-agent manufacturing systems for industry of the future*. Hrsg. von Theodor Borangiu, Damien Trentesaux, Paulo Leitão, Adriana Giret Boggino und Vicente Botti. Studies in Computational Intelligence. Cham: Springer International Publishing, 2020, S. 220–231. ISBN: 978-3-030-27477-1. DOI: 10.1007/978-3-030-27477-1{\textunderscore}17. URL: https://link.springer.com/chapter/10.1007/978-3-030-27477-1_17.

[CSM16] Tiago Cruz, Paulo Simoes und Edmundo Monteiro. „Virtualizing Programmable Logic Controllers: Toward a Convergent Approach“. In: *IEEE Embedded Systems Letters* 8.4 (2016), S. 69–72. ISSN: 1943-0663. DOI: 10.1109/les.2016.2608418.

[Cul+08] Brendan Cully, Geoffrey Lefebvre, Dutch Meyer u. a. „Remus: High availability via asynchronous virtual machine replication“. In: (2008). URL: https://www.usenix.org/event/nsdi08/tech/full_papers/cully/cully_html.

[Dec09] Jean-Dominique Decotignie. „The many faces of industrial ethernet [past and present]“. In: *IEEE Industrial Electronics Magazine* 3.1 (2009), S. 8–19. ISSN: 1932-4529.

[DSV15] Zakarya Drias, Ahmed Serhrouchni und Olivier Vogel. „Analysis of cyber security for industrial control systems“. In: *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 2015. DOI: 10.1109/ssic.2015.7245330.

[Duk+06] M. Duke, R. Braden, W. Eddy und E. Blanton. *A Roadmap for Transmission Control Protocol (TCP) Specification Documents*. 2006. DOI: 10.17487/rfc4614.

[Far+13] Dino Farinacci, Vince Fuller, David Meyer und Darrel Lewis. *The locator/ID separation protocol (LISP)*. 2013.

[Fel05] M. Felser. „Real-Time Ethernet - Industry Prospective“. In: *Proceedings of the IEEE* 93.6 (2005), S. 1118–1129. ISSN: 0018-9219. DOI: 10.1109/jproc.2005.849720.

[FRK19] Max Felser, Markus Rentschler und Oliver Kleineberg. „Coexistence standardization of operation technology and information technology“. In: *Proceedings of the IEEE* 107.6 (2019), S. 962–976. ISSN: 0018-9219.

[Fos+21] Luca Foschini, Valentina Mignardi, Rebecca Montanari und Domenico Scotece. „An sdn-enabled architecture for it/ot converged networks: A proposal and qualitative analysis under ddos attacks“. In: *Future Internet* 13.10 (2021), S. 258.

[Fra+20] D. Franke, D. Sibold, K. Teichel, M. Dansarie und R. Sundblad. *RFC 8915: Network Time Security for the Network Time Protocol*. 2020.

[FHH23] Antônio Augusto Fröhlich, Leonardo Passig Horstmann und José Luis Conradi Hoffmann. „A Secure IIoT Gateway Architecture based on Trusted Execution Environments“. In: *Journal of Network and Systems Management* 31.2 (2023), S. 1–30. ISSN: 1573-7705. DOI: 10.1007/s10922-023-09723-6. URL: https://link.springer.com/article/10.1007/s10922-023-09723-6.

[Fu+24] Meixia Fu, Zhenqian Wang, Jianquan Wang u. a. „Multicrane Visual Sorting System Based on Deep Learning With Virtualized Programmable Logic Controllers in Industrial Internet“. In: *IEEE Transactions on Industrial Informatics* 20.3 (2024), S. 3726–3737. ISSN: 1551-3203. DOI: 10.1109/tii.2023.3313641.

[Gba+24] Bolaji Gbadamosi, Luigi Leonardi, Tobias Pulls u. a. *The eBPF Runtime in the Linux Kernel*. 2024. URL: http://arxiv.org/pdf/2410.00026.

[GG21] A. Shaji George und A. HovanS George. „A Brief Overview of VXLAN EVPN“. In: *Ijireeiceinternational Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering* 9.7 (2021), S. 1–12.

[Gil16] Alasdair Gilchrist. *Industry 4.0: the industrial internet of things*. Springer, 2016. URL: https://link.springer.com/content/pdf/10.1007/978-1-4842-2047-4.pdf.

[Gol+15] Thomas Goldschmidt, Mahesh Kumar Murugaiah, Christian Sonntag u. a. „Cloud-Based Control: A Multi-tenant, Horizontally Scalable Soft-PLC“. In: *2015 IEEE 8th International Conference on Cloud Computing*. IEEE, 2015. DOI: 10.1109/cloud.2015.124.

[Gov+16] Ramesh Govindan, Ina Minei, Mahesh Kallahalla, Bikash Koley und Amin Vahdat. „Evolve or Die“. In: *Proceedings of the 2016 ACM SIGCOMM Conference*. New York, NY, USA: ACM, 2016. DOI: 10.1145/2934872.2934891.

[GS91] J. Gray und D. P. Siewiorek. „High-availability computer systems“. In: *Computer* 24.9 (1991), S. 39–48. ISSN: 0018-9162. DOI: 10.1109/2.84898.

[HH12] Kjell Hansson und Olof Hagsand. „System for establishing and maintaining a clock reference indicating one-way latency in a data network“. US8792380B2. 2012. URL: https://patents.google.com/patent/US20170294979A1/en.

[Hau16] Iris Hausladen. *IT-gestützte Logistik*. Wiesbaden: Springer Fachmedien Wiesbaden, 2016. ISBN: 9783658130794. DOI: 10.1007/978-3-658-13080-0.

[He+20] Zhiqiang He, Dongyang Wang, Binzhang Fu u. a. „MasQ: RDMA for Virtual Private Cloud“. In: *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*. 2020.

[Her+18] Ekbert Hering, Rolf Martin, Jürgen Gutekunst und Joachim Kempkes. *Elektrotechnik und elektronik fr maschinenbauer*. [Place of publication not identified]: Morgan Kaufmann, 2018. ISBN: 978-3-662-57579-6. DOI: 10.1007/978-3-662-57580-2.

[HMS24] HMS. *Jährliche Marktanalyse zeigt stetes Wachstum für industrielle Netzwerke: Marktanteile industrieller Netzwerke 2024 aus Sicht von HMS Networks*. 2024. URL: https://www.hms-networks.com/de/news/news-details/17-06-2024-annual-analysis-reveals-steady-growth-in-industrial-network-market#:~:text=Marktanteile%202024%20aus%20Sicht%20von%20HMS%20Networks%20%E2%80%93 (besucht am 06. 10. 2024).

[HMS21] Stephan Hohmann, Tobias Mueller und Marius Stübs. „Bridge Me If You Can! Evaluating the Latency of Securing Profinet“. In: *2021 International Conference on Information Networking (ICOIN)*. 2021, S. 621–626. DOI: 10.1109/ICOIN50884.2021.9333897.

[Hus04] Iftekhar Hussain. „Overview of MPLS technology and traffic engineering applications“. In: *2004 International Networking and Communication Conference*. 2004, S. xvi.

[IEC19] IEC. *IEC 61784-2:2019*. 2019.

[IEE16] IEEE. *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks – Amendment 25: Enhancements for Scheduled Traffic: IEEE Std 802.1Qbv-2015*. 2016.

[IEE17] IEEE. „IEEE Standard for Local and metropolitan area networks–Frame Replication and Elimination for Reliability“. In: *IEEE Std 802.1 CB-2017* (2017), S. 1–102.

[IEE18] IEEE. „Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks“. In: *IEEE 802.1Q-2018* (2018).

[IEE20] IEEE. „IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation“. In: *IEEE Std 802.1AX-2020* (2020).

[IEE23] IEEE. *IEEE Recommended Practice for Electrical Installations on Shipboard–Controls and Automation*. Piscataway, NJ, USA, 2023. DOI: 10.1109/IEEESTD.2024.10600164.

[IEE24] IEEE. *Time-Sensitive Networking (TSN) Task Group*. 2024. URL: https://1.ieee802.org/tsn/ (besucht am 11. 10. 2024).

[IEE19] IEEE/ISO/IEC. „IEEE/ISO/IEC International Standard - Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 1Q: Bridges and bridged networks - AMENDMENT 7: Cyclic queuing and forwarding“. In: (2019). DOI: 10.1109/IEEESTD.2019.8664711.

[IET22] IETF. *Deterministic Networking (detnet)*. 2022. URL: https://datatracker.ietf.org/wg/detnet/documents/ (besucht am 12. 10. 2024).

[Inf21a] Infiniband Trade Association. *Infiniband Architecture Specification Volume 1 Release 1.5*. 2021.

[Inf21b] Infiniband Trade Association. *Infiniband Architecture Specification Volume 2 Release 1.5*. 2021.

[Int11] International Electrotechnical Commission. „Functional safety of electrical/electronic/programmable electronic safety related systems“. In: *IEC 61508* (2011).

[Int+16] International Electrotechnical Commission u. a. „Industrial communication networks-High availability automation networks-Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) Methods“. In: *IEC, Geneva, Switzerland, IEC* (2016), S. 62439–3.

[ID20] International Electrotechnical Commission und D.I.N. „62443-3-3: 2020.01“. In: *Industrielle Kommunikationsnetze–IT-Sicherheit für Netze und Systeme–Teil* (2020), S. 3.

[Jun24] Juniper. *Layer 2 Protocol Tunneling over VXLAN Tunnels in EVPN-VXLAN Bridged Overlay Networks*. 2024. URL: https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/topic-map/l2pt-evpn-vxlan-bridged-overlay.html (besucht am 03. 09. 2024).

[Kat95] Vamshi K. Katukoori. „Standardizing availability definition“. In: (1995).

[KW10] D. Katz und D. Ward. *Bidirectional Forwarding Detection (BFD)*. 2010. DOI: 10.17487/RFC5880. URL: https://www.rfc-editor.org/rfc/rfc5880.

[KW21] Kahiomba Sonia Kiangala und Zenghui Wang. „An effective communication prototype for time-critical iiot manufacturing factories using zero-loss redundancy protocols, time-sensitive networking, and edge-computing in an industry 4.0 environment“. In: *Processes* 9.11 (2021), S. 2084.

[KAV17] Daniel Kiel, Christian Arnold und Kai-Ingo Voigt. „The influence of the Industrial Internet of Things on business models of established manufacturing companies – A business level perspective“. In: *Technovation* 68 (2017), S. 4–19. ISSN: 0166-4972. DOI: 10.1016/j.technovation.2017.09.003. URL: https://www.sciencedirect.com/science/article/pii/s0166497216303169.

[Kim+19] Daehyeok Kim, Tianlong Yu, Hongqiang Harry Liu u. a. „FreeFlow: Software-based Virtual RDMA Networking for Containerized Clouds“. In: *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. 2019, S. 113–126. URL: https://www.usenix.org/conference/nsdi19/presentation/kim.

[Kin+10] John Kindervag u. a. „Build security into your network's dna: The zero trust network architecture“. In: *Forrester Research Inc* 27 (2010).

[Kle+17] Christian Klettner, Thomas Tauchnitz, Ulrich Epple u. a. „Namur Open Architecture“. In: *atp edition - Automatisierungstechnische Praxis* 59.01-02 (2017), S. 17. ISSN: 2190-4111. DOI: 10.17560/atp.v59i01-02.620. URL: https://ojs.di-verlag.de/index.php/atp_edition/article/view/620.

[Kob+18] Thomas Kobzan, Sebastian Schriegel, Simon Althoff u. a. „Secure and time-sensitive communication for remote process control and monitoring“. In: *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*. Bd. 1. 2018, S. 1105–1108.

[Koc+23] Amy Koch, Nazanin Hamedi, Lukas Furtner u. a. „Standards for Information Models Considering Knowledge Distribution in Modular Plants“. In: *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*. IEEE, 2023. DOI: 10.1109/indin51400.2023.10218218.

[Kot+13] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brünig und Georg Carle. „DTLS based security and two-way authentication for the Internet of Things“. In: *Ad Hoc Networks* 11.8 (2013), S. 2710–2723.

[Kra07] Herbert Krause. *Virtual commissioning of a large LNG plant with the DCS 800XA by ABB*. 6th EUROSIM Congress on Modelling und Simulation, 2007. URL: https://secolon.de/p172.pdf.

[Kri+22] Umesh Krishnaswamy, Rachee Singh, Nikolaj Bjørner und Himanshu Raj. „Decentralized cloud wide-area network traffic engineering with BLASTSHIELD“. In: 2022, S. 325–338. ISBN: 978-1-939133-27-4. URL: https://www.usenix.org/conference/nsdi22/presentation/krishnaswamy.

[Kum+19] Sam Kumar, Yuncong Hu, Michael P. Andersen, Raluca Ada Popa und David E. Culler. „JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT“. In: *USENIX Security Symposium*. 2019, S. 1519–1536.

[LKS19] Tim Lackorzynski, Stefan Köpsell und Thorsten Strufe. „A comparative study on virtual private networks for future industrial communication systems“. In: *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*. 2019, S. 1–8.

[LB22] Martin Langer und Rainer Bermbach. „NTS4PTP—A comprehensive key management solution for PTP networks“. In: *Computer Networks* 213 (2022), S. 109075.

[Las+24] Stefanos Laskaridis, Stylianos I. Venieris, Alexandros Kouris, Rui Li und Nicholas D. Lane. „The future of consumer edge-ai computing“. In: *IEEE Pervasive Computing* (2024).

[Le+15] Quan Ha Le, Jeff Xie, Darrell Millington und Amgad Waniss. „Comparative Performance Analysis of PostgreSQL High Availability Database Clusters through Containment“. In: *IJARCCE* 4.12 (2015), S. 526–533. DOI: 10.17148/IJARCCE.2015.412150.

[Li+16] Ming Li, Andrey Lukyanenko, Zhonghong Ou u. a. „Multipath Transmission for the Internet: A Survey“. In: *IEEE Communications Surveys & Tutorials* 18.4 (2016), S. 2887–2925. ISSN: 1553-877X. DOI: 10.1109/comst.2016.2586112.

[Li+98] T. Li, B. Cole, P. Morton und D. Li. *Cisco Hot Standby Router Protocol (HSRP)*. 1998. DOI: 10.17487/RFC2281. URL: https://www.rfc-editor.org/rfc/rfc2281.html.

[LAS20] Christoph Lipps, Pascal Ahr und Hans Dieter Schotten. „The PhySec Thing“. In: *Journal of Information Warfare* 19.3 (2020), S. 35–49.

[Loc21] Lockheed Martin. *Cyber Kill Chain®*. 2021. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (besucht am 04. 10. 2024).

[LMZ16] Tomáš Lojka, Martin Miškuf und Iveta Zolotová. „Industrial IoT Gateway with Machine Learning for Smart Manufacturing“. In: *Advances in Production Management Systems. Initiatives for a Sustainable World*. Hrsg. von Rodrigo Franco Gonçalves, Dimitris Kiritsis, João Mendes Reis u. a. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing und Imprint: Springer, 2016, S. 759–766. ISBN: 978-3-319-51133-7. DOI: 10.1007/978-3-319-51133-7{\textunderscore}89. URL: https://link.springer.com/chapter/10.1007/978-3-319-51133-7_89.

[LG20] Andriy Luntovskyy und Dietbert Gütter. *Moderne Rechnernetze: Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken*. 1. Auflage 2020. Wiesbaden: Springer Fachmedien Wiesbaden, 2020. ISBN: 9783658256173.

[LT09] T. T. Lwin und T. Thein. *High Availability Cluster System for Local Disaster Recovery with Markov Modeling Approach*. 2009.

[LB20] Guolin Lyu und Robert William Brennan. „Towards IEC 61499-based distributed intelligent automation: A literature review“. In: *IEEE Transactions on Industrial Informatics* 17.4 (2020), S. 2295–2306. ISSN: 1551-3203.

[M E+19] M. Ehrlich, H. Trsek, L. Wisniewski und J. Jasperneite. „Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing“. In: *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*. 2019, S. 2849–2854. DOI: 10.1109/IECON.2019.8927559.

[Mah+14] M. Mahalingam, D. Dutt, K. Duda u. a. *Rfc 7348: virtual extensible local area network (vxlan): a framework for overlaying virtualized layer 2 networks over layer 3 networks*. 2014.

[Mah+18] Sumit Maheshwari, Dipankar Raychaudhuri, Ivan Seskar und Francesco Bronzino. „Scalability and Performance Evaluation of Edge Cloud Systems for Latency Constrained Applications“. In: *2018 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, 2018. DOI: 10.1109/sec.2018.00028.

[Man+22] Soujanya Mantravadi, Charles Møller, Chen LI und Reto Schnyder. „Design choices for next-generation IIoT-connected MES/MOM: An empirical study on smart factories“. In: *Robotics and Computer-Integrated Manufacturing* 73 (2022), S. 102225. ISSN: 07365845. DOI: 10.1016/j.rcim.2021.102225.

[McK+08] Nick McKeown, Tom Anderson, Hari Balakrishnan u. a. „OpenFlow“. In: *ACM SIGCOMM Computer Communication Review* 38.2 (2008), S. 69–74. ISSN: 0146-4833. DOI: 10.1145/1355734.1355746.

[Mey14] Martin Meyer. *Kommunikationstechnik: Konzepte der modernen Nachrichtenübertragung ; mit 38 Tabellen*. 5., korrigierte Aufl. Springer-Lehrbuch. Wiesbaden: Springer Vieweg, 2014. ISBN: 3658033754.

[Mit+15] Radhika Mittal, Vinh The Lam, Nandita Dukkipati u. a. „TIMELY“. In: *ACM SIGCOMM Computer Communication Review* 45.4 (2015), S. 537–550. ISSN: 0146-4833. DOI: 10.1145/2829988.2787510.

[Mit+18] Radhika Mittal, Alexander Shpiner, Aurojit Panda u. a. „Revisiting network support for RDMA“. In: *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*. New York, NY, USA: ACM, 2018. DOI: 10.1145/3230543.3230557.

[Miz11] Tal Mizrahi. „Time synchronization security using IPsec and MACsec“. In: *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*. 2011, S. 38–43.

[Mos+20] Aintzane Mosteiro-Sanchez, Marc Barcelo, Jasone Astorga und Aitor Urbieta. „Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0“. In: *Journal of Manufacturing Systems* 57 (2020), S. 367–378.

[Mue+24] Kevin Mueller, Marco Giani, Darius Deubert und Michael Massoth. „Virtualization in Industrial Production - A Survey Focusing on Virtual and Virtualized Industrial Controls“. In: *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2024.

[MPR15] Gerald Münzl, Michael Pauly und Martin Reti. *Cloud Computing als neue Herausforderung für Management und IT*. Springer-Verlag, 2015.

[Nad10] S. Nadas. *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*. 2010. DOI: 10.17487/RFC5798. URL: https://www.rfc-editor.org/rfc/rfc5798.html.

[Nas+19] Ahmed Nasrallah, Akhilesh S. Thyagaturu, Ziyad Alharbi u. a. „Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research“. In: *IEEE Communications Surveys & Tutorials* 21.1 (2019), S. 88–145. DOI: 10.1109/COMST.2018.2869350.

[Nel16] Nell Nelson. „The impact of dragonfly malware on industrial control systems“. In: *SANS Institute* (2016).

[Net18] Victor Netes. „End-to-end availability of cloud services“. In: *2018 22nd Conference of Open Innovations Association (FRUCT)*. 2018, S. 198–203.

[Net+17] Hylson V. Netto, Lau Cheuk Lung, Miguel Correia, Aldelir Fernando Luiz und Sá de Souza, Luciana Moreira. „State machine replication in containers managed by Kubernetes“. In: *Journal of Systems Architecture* 73 (2017), S. 53–59. ISSN: 13837621. DOI: 10.1016/j.sysarc.2016.12.007.

[Pad+23] Jitendra Padhye, Karthick Jayaraman, Wei Bai u. a. *Ghost routing*. 2023.

[Pol+13] F. Poletti, N. V. Wheeler, M. N. Petrovich u. a. „Towards high-capacity fibre-optic communications at the speed of light in vacuum“. In: *Nature Photonics* 7.4 (2013), S. 279–284. ISSN: 1749-4893. DOI: 10.1038/nphoton.2013.45.

[Pv17] Paul Pols und Jan van den Berg. „The unified kill chain“. In: *CSA Thesis, Hague* (2017), S. 1–104.

[Pop+16] Miroslav Popovic, Maaz Mohiuddin, Dan-Cristian Tomozei und Jean-Yves Le Boudec. „iPRP—The Parallel Redundancy Protocol for IP Networks: Protocol Design and Operation“. In: *IEEE Transactions on Industrial Informatics* 12.5 (2016), S. 1842–1854. ISSN: 1551-3203. DOI: 10.1109/tii.2016.2530018.

[Rai+18] Silviu Raileanu, Theodor Borangiu, Octavian Morariu und Iulia Iacob. „Edge Computing in Industrial IoT Framework for Cloud-based Manufacturing Control“. In: *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)*. IEEE, 2018. DOI: 10.1109/icstcc.2018.8540725.

[Rei+06] S.-A. Reinemo, T. Skeie, T. Sodring, O. Lysne und O. Trudbakken. „An overview of QoS capabilities in infiniband, advanced switching interconnect, and ethernet“. In: *IEEE Communications Magazine* 44.7 (2006), S. 32–38. ISSN: 0163-6804. DOI: 10.1109/mcom.2006.1668378.

[RPZ10] Jonas Repschläger, Danny Pannicke und Rüdiger Zarnekow. „Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale“. In: *HMD Praxis der Wirtschaftsinformatik* 47.5 (2010), S. 6–15. ISSN: 2198-2775. DOI: 10.1007/BF03340507. URL: https://link.springer.com/article/10.1007/bf03340507.

[Roh19] Sebastian Rohr. *Industrial IT Security: Effizienter Schutz vernetzter Produktionslinien*. Vogel, 2019. ISBN: 978-3-8343-3382-7.

[Ros+23] Lorenzo Rosa, Andrea Garbugli, Lorenzo Patera und Luca Foschini. „Supporting vPLC networking over TSN with kubernetes in industry 4.0“. In: *Proceedings of the 1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum*. 2023, S. 15–21.

[Sau10] T. Sauter. „The Three Generations of Field-Level Networks—Evolution and Compatibility Issues“. In: *IEEE Transactions on Industrial Electronics* 57.11 (2010), S. 3585–3595. ISSN: 0278-0046. DOI: 10.1109/tie.2010.2062473.

[SNV10] Daniel J. Scales, Mike Nelson und Ganesh Venkitachalam. „The design of a practical system for fault-tolerant virtual machines“. In: *ACM SIGOPS Operating Systems Review* 44.4 (2010), S. 30–39. ISSN: 0163-5980. DOI: 10.1145/1899928.1899932.

[Sch+23] Florian Schade, Tobias Dörr, Alexander Ahlbrecht u. a. „Automatic Deployment of Embedded Real-Time Software Systems to Hypervisor-Managed Platforms“. In: *2023 26th Euromicro Conference on Digital System Design (DSD)*. IEEE, 2023. DOI: 10.1109/dsd60849.2023.00067.

[Sch23] Sebastian Schmied. *Methodik für die systematische Entwicklung und Validierung von Informationsmodellen für cyber-physische Produktionssysteme*. Bd. Nr. 882. Fortschritt-Berichte VDI Reihe 10, Informatik/Kommunikation. Düsseldorf: VDI Verlag GmbH, 2023. ISBN: 9783186882103. DOI: 10.51202/9783186882103.

[SSM22] Christoph Schmittner, Abdelkader Magdy Shaaban und Georg Macher. „ThreatGet: Ensuring the Implementation of Defense-in-Depth Strategy for IIoT Based on IEC 62443“. In: *2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS)*. 2022, S. 1–6.

[SK11] Klaus Schubert und Martina Klein. „Das Politiklexikon: Begriffe“. In: *Fakten. Zusammenhänge* 5 (2011).

[Sch16] Wolfgang Schulte. *Handbuch der Routing-Protokolle: eine Einführung in RIP, IGRP, EIGRP, HSRP, VRRP, OSPF, IS-IS und BGP*. VDE Verlag GmbH, 2016.

[Sch17] Klaus Schwab. *The fourth industrial revolution*. Crown Currency, 2017.

[ST12] Vanessa Romero Segovia und Alfred Theorin. „History of Control History of PLC and DCS“. In: *University of Lund* 44 (2012), S. 45.

[Sie22] Siemens. *SIMATIC S7-1500 R/H for redundancy and high availability*. 2022. URL: https://new.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500/redundant-and-high-availability-cpus.html (besucht am 03. 10. 2024).

[Sie24] Siemens. *SIMATIC S7-1500 CPUs*. 2024. URL: https://new.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500/cpus.html (besucht am 10. 03. 2024).

[SHF24] Zeki Simsek, Ciaran Heavey und Brian C. Fox. *Handbook of research on strategic leadership in the fourth industrial revolution*. Cheltenham: Edward Elgar Publishing, 2024. ISBN: 9781802208818.

[SK16] Michael Smith und Larry Kreeger. *VXLAN Group Policy Option*. 2016.

[Sta+20] Stevan Stankovski, Gordana Ostojić, Igor Baranovski, Mladen Babić und Miloš Stanojević. „The impact of edge computing on industrial automation“. In: *2020 19th International Symposium Infoteh-Jahorina (Infoteh)*. 2020, S. 1–4.

[Ste21] Peter N. Stearns. *The industrial revolution in world history*. Fifth edition. London: Routledge, 2021. ISBN: 9781003050186. DOI: 10.4324/9781003050186. URL: https://www.taylorfrancis.com/books/mono/10.4324/9781003050186/industrial-revolution-world-history-peter-stearns.

[Sto00] Ion Stoica. *Stateless core: A scalable approach for quality of service in the internet*. Carnegie Mellon University, 2000.

[Sun+08] Yu-Wei Eric Sung, Sanjay G. Rao, Geoffrey G. Xie und David A. Maltz. „Towards systematic design of enterprise networks“. In: *Proceedings of the 2008 ACM CoNEXT Conference*. 2008, S. 1–12.

[Szi+13] Tim Szigeti, Christina Hattingh, Robert Barton und Kenneth Briley Jr. *End-to-End QoS network design: Quality of Service for rich-media & cloud networks*. Cisco press, 2013.

[TW12] Andrew S. Tanenbaum und David J. Wetherall. *Computernetzwerke*. 5. Auflage. Pearson Studium - IT. München: Pearson Deutschland Pearson Studium, 2012. ISBN: 1299747000. URL: https://www.pearson-studium.de/drm/reader/nu/code/ubbcnw.

[Tan+20] Koen Tange, Michele de Donno, Xenofon Fafoutis und Nicola Dragoni. „A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities“. In: *IEEE Communications Surveys & Tutorials* 22.4 (2020), S. 2489–2520. ISSN: 1553-877X.

[TE16] Daniel Thiele und Rolf Ernst. „Formal worst-case performance analysis of time-sensitive ethernet with frame preemption“. In: *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. 2016, S. 1–9.

[Tia+23] Zhen Tian, Li Ding, Qing Wang, Desheng Sun und Yunlong Li. „PHYSec: A Novel Physical Layer Security Architecture for Ethernet“. In: *Proceedings of the 7th Asia-Pacific Workshop on Networking*. 2023, S. 198–199.

[TH18] Nilufer Tuptuk und Stephen Hailes. „Security of smart manufacturing systems“. In: *Journal of Manufacturing Systems* 47 (2018), S. 93–106. DOI: 10.1016/j.jmsy.2018.04.007. URL: https://www.sciencedirect.com/science/article/pii/S0278612518300463.

[vvK14] Niels L.M. van Adrichem, Benjamin J. van Asten und Fernando A. Kuipers. „Fast Recovery in Software-Defined Networks“. In: *2014 Third European Workshop on Software Defined Networks*. IEEE, 2014. DOI: 10.1109/ewsdn.2014.13.

[VDI21] VDI/VDE. *Entwicklung Mechatronischer und Cyber-Physischer Systeme*. Beuth Verlag GmbH Düsseldorf, Germany, 2021.

[Ver07] Verein Deutscher Ingenieure. *VDI-Richtlinie 4003–Zuverlässigkeitsmanagement*. 2007.

[Ver20] Verein Deutscher Ingenieure, Verband der Elektrotechnik, Elektronik. „Funkgestützte Kommunikation in der Automatisierungstechnik (Radio based communication in industrial automation), VDI/VDE Richtlinie 2185“. In: (2020).

[Vie+20] Marcos am Vieira, Matheus S. Castanho, Racyus D. G. Pac\'\ifico u. a. „Fast packet processing with ebpf and xdp: Concepts, code, challenges, and applications“. In: *ACM Computing Surveys (CSUR)* 53.1 (2020), S. 1–36.

[VMw23] VMware. *Digitalization of Power Substations - ESXi Real-Time Configuration, Tuning, and Testing*. 2023. URL: https://docs.vmware.com/en/VMware-Edge-Compute-Stack/3.0/ecs-enterprise-edge-ref-arch/GUID-A191D284-1CDE-4602-9940-CE1B9376684C.html (besucht am 11. 10. 2024).

[VDB13] Birgit Vogel-Heuser, Christian Diedrich und Manfred Broy. „Anforderungen an CPS aus Sicht der Automatisierungstechnik/Requirements on CPS from the Viewpoint of Automation“. In: *at-Automatisierungstechnik* 61.10 (2013), S. 669–676.

[Vog+98] W. Vogels, D. Dumitriu, K. Birman u. a. „The design and architecture of the Microsoft Cluster Service-a practical approach to high-availability and scalability“. In: *Twenty-Eighth Annual International Symposium on Fault-Tolerant Computing (Cat. No.98CB36224)*. IEEE Comput. Soc, 1998. DOI: 10.1109/ftcs.1998.689494.

[Wal+23] Andreas Walz, Karl-Heinz Niemann, Julian Göppert u. a. „PROFINET Security: A Look on Selected Concepts for Secure Communication in the Automation Domain“. In: *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*. 2023, S. 1–6.

[WB14] Rory Ward und Betsy Beyer. *Beyondcorp: A new approach to enterprise security*. 2014.

[WG20] Alexander Willner und Varun Gowtham. „Toward a Reference Architecture Model for Industrial Edge Computing“. In: *IEEE Communications Standards Magazine* 4.4 (2020), S. 42–48. ISSN: 2471-2825. DOI: 10.1109/mcomstd.001.2000007.

[YR15] Tarun Yadav und Arvind Mallari Rao. „Technical aspects of cyber kill chain“. In: *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3*. 2015, S. 438–452.

[Zam+19] Erfan Zamanian, Xiangyao Yu, Michael Stonebraker und Tim Kraska. „Rethinking database high availability with RDMA networks“. In: *Proceedings of the VLDB Endowment* 12.11 (2019), S. 1637–1650. ISSN: 2150-8097. DOI: 10.14778/3342263.3342639.

[Zha+21] Jiao Zhang, Yali Zhang, Zixuan Guan u. a. „HierCC: Hierarchical RDMA Congestion Control“. In: *5th Asia-Pacific Workshop on Networking (APNet 2021)*. ACM Digital Library. New York,NY,United States: Association for Computing Machinery, 2021, S. 29–36. ISBN: 9781450385879. DOI: 10.1145/3469393.3469396.

[Zha+17] Yiwen Zhang, Juncheng Gu, Youngmoon Lee, Mosharaf Chowdhury und Kang G. Shin. „Performance Isolation Anomalies in RDMA“. In: *Proceedings of the Workshop on Kernel-Bypass Networks*. 2017. DOI: 10.1145/3098583.3098591.

[ZPC18] Luxi Zhao, Paul Pop und Silviu S. Craciunas. „Worst-case latency analysis for IEEE 802.1 Qbv time sensitive networks using network calculus“. In: *IEEE Access* 6 (2018), S. 41803–41815.

[Zhu+15] Yibo Zhu, Haggai Eran, Daniel Firestone u. a. „Congestion Control for Large-Scale RDMA Deployments“. In: *ACM SIGCOMM Computer Communication Review* 45.4 (2015), S. 523–536. ISSN: 0146-4833. DOI: 10.1145/2829988.2787484.

[Zol+19] Maede Zolanvari, Marcio A. Teixeira, Lav Gupta, Khaled M. Khan und Raj Jain. „Machine learning-based network vulnerability analysis of industrial Internet of Things“. In: *IEEE Internet of Things Journal* 6.4 (2019), S. 6822–6834.

A Anhang

A.1 Glossar

- Air Gap: Ein Air Gap beschreibt die physikalische Trennung eines Netzwerkes von anderen Netzwerken, insbesondere dem Internet.
- Anycast-Gateway: Ein Anycast-Gateway stellt ein Gateway für Anycast-Kommunikation dar. Diese zeichnet sich durch das Teilen derselben IP-Adresse aus, sodass ein Gerät mehrere Gateways nutzen kann, jedoch nur das Nächstgelegene erreicht.
- COTS-Hardware: Kommerziell erwerbbare Hardware
- Determinismus: Im Kontext der Kommunikationstechnik bezeichnet Determinismus die Eigenschaft, dass Telegramme zwischen Sender und Empfänger ausreichend schnell übermittelt werden, damit der ausführende Prozess in seiner festgelegten Geschwindigkeit vorhersagbar ist.
- Edge Cloud: Die Edge Cloud ist ein verteiltes System, welches in der Nähe der Geräte physikalisch verortet ist, mit denen die auf dem verteilten System betriebenen Applikationen interagieren.
- Fabric: Ein Logisches Konstrukt mit einer gemeinsamen Kontrollebene zum Austausch von Geräteinformationen
- FIB: Beschreibt die Datenbank im Hauptspeicher eines Switches zur schnellen Weiterleitung von Telegrammen
- Hop: Ein (Netzwerk)-Hop bezeichnet eine Netzwerkkomponente, beispielsweise einen Switch oder Router.
- Host: Ein PC oder Server, auf dem Applikationen physikalisch verortet sind
- Hypervisor: Abstrahierung der unterliegenden Hardware und Bereitstellung für verschiedene VM mit eigenen Betriebssystemen
- IEC-Task: Eine nach IEC 61131 definierte Abfolge von Berechnungen
- KI-Inferenz: Die Ausführung von Algorithmen basierend auf trainierten KI-Modellen
- Nord/Süd-Kommunikation: Bezeichnet aus Netzwerksicht die Kommunikation zwischen den einzelnen Netzwerk-Schichten, beispielsweise Zugriffs- und Vermittlungsschicht sowie die Kommunikation aus dem Border-Router zu angrenzenden Netzwerken.

- Ost/West-Kommunikation: Bezeichnet aus Netzwerksicht die Kommunikation auf einer Netzwerk-Schicht, beispielsweise eine Kommunikationsbeziehung zweier Geräte verbunden mit der Zugriffsschicht.
- Thin Client: Ein Computer, der mit minimalen Ressourcen ausgestattet ist und vor allem für die Verbindung zur Peripherie genutzt wird.
- Tunnelprotokoll: Ein Tunnelprotokoll ermöglicht die Einbettung eines Protokolls innerhalb eines anderen. Hierdurch erfolgt eine Kapselung der ursprünglichen Telegramme, sodass ein Transport über ein Netzwerk ermöglicht wird oder neue Eigenschaften hinzugefügt werden.
- VXLAN Overlay-Netzwerk: Virtuelles Schicht 2-Netzwerk, welches mittels Tunneln der Telegramme über ein Schicht 3-Netzwerk ermöglicht wird.
- vSPS: Eine Steuerung, die auf einem verteilten System innerhalb einer VM oder Container betrieben wird

A.2 Industrial Ethernet über IP-basierte Kommunikationsnetzwerke

Im Folgenden wird die beispielhafte Konfiguration eines Interfaces dargestellt, welches VXLAN-Datenverkehr überträgt. Neben der Anwendung von BFD für die schnelle Erkennung von Link-Problemen werden außerdem Multicast-Konfigurationen durchgeführt, um beispielsweise PROFINET DCP-Telegramme übertragen zu können.

```
1  description Fabric Physical Link
2   no switchport
3   dampening
4   ip address %.%.%.% 255.255.255.254
5   no ip redirects
6   ip pim sparse-mode
7   ip router isis
8   load-interval 30
9   bfd interval 250 min_rx 250 multiplier 3
10  clns mtu 1400
11  isis network point-to-point
```

Codebeispiel A.1: Interface-Konfiguration eines Ports innerhalb einer VXLAN-Fabric

A.3 Echtzeitapplikationen und Virtualisierung

Dieser Abschnitt beschreibt die notwendigen Schritte, um eine Applikation mit Echtzeitanforderungen auf einer virtualisierten Umgebung zu ermöglichen. Hierzu kann zunächst zwischen Konfigurationen außerhalb und innerhalb der VM unterschieden werden.

Innerhalb der VM sind vier verschiedene Bestandteile essenziell:

- Ein PREEMPT_RT-Patch, um im jeweiligen Linux-Derivat niederpriore Tasks mit Höherprioren zu unterbrechen

- Linux Header-Dateien, welche Schnittstellen zum Linux-Kernel Programmen bekannt machen
- CLIB-Bibliotheken, welche von vielen Programmen genutzt werden, um System API-Aufrufe durchzuführen
- Anpassung der GRUB Einstellungen, welche je nach Anwendungsfall unterschiedlich sein können. Hierzu zählen vor allem die Isolation von Prozessorkernen für echtzeitkritische Threads sowie das Deaktivieren des Energiesparmodus.

Mit dem Release des Linux Kernel Version 6.12-rc1 enthält dieser bereits den notwendigen PREEMPT_RT-Patch, sodass die Nutzung von Linux-basierten Systemen im Echtzeitumfeld vereinfacht wird.

Anpassungen an dem Bootloader können je nach verwendetem Prozessor und Hardware zu verschiedenen Ergebnissen führen. In den verwendeten Linux Debian 12-basierten Systemen mit Intel Xeon-P 8358-Prozessor konnten folgende GRUB-Einstellungen als geeignet ermittelt werden:

```
GRUB_CMDLINE_LINUX_DEFAULT="" #<-- die jeweiligen Konfigurationsbefehle gilt es zwischen die Anfuehrungszeichen einzufuegen

ro #Kernel Dateisystem besitzt nur Leserechte
noht #kein Hyperthreading
cstates #kein Energiesparmodus
idle=poll
clocksource=tsc #Zeit wird von der CPU bezogen
tsc=reliable
hpet=disable #Event-Timer mit hoher Praezision
mem_sleep_default=deep #Power Management
hugepages=1024
i915 #reduziert Priorisierung der Visualisierung
iommu=pt
igb.blacklist=no
isolcpus=domain
managed_irq
irqaffinity= 0 #Reduktion derCPU-Transaktionen
numa_balancing=disable
rcu_nocbs=all
rcupdate.rcu_cpu_stall_supress=1
nowatchdog #Deaktivierung den Kernel Watchdog
mce=off
efi=runtime
audit=0 #Kernel Audit
```

Codebeispiel A.2: GRUB-Einstellungen zur Erreichung der Echtzeitfähigkeit

Des Weiteren wird innerhalb der Virtualisierung ein Hypervisor genutzt, um die vorhandenen physikalischen Hardwareressorucen zu abstrahieren. Je nach verwendetem Produkt sind hier auch Einstellungen zu treffen, um den notwendigen Determinismus der Applikation

und Kommunikation zu erreichen. Im Rahmen dieser Arbeit wird der Baremetal-Hypervisor ESXi von VMware/Broadcom Ltd. genutzt. Auf Basis von Gesprächen mit Experten dieses Unternehmens, verfügbaren Quellen zum Tuning der Maschinen sowie einer iterativen Vorgehensweise konnte die Echtzeitfähigkeit der jeweiligen VM erreicht werden [VMw23]. Eine Prüfung wurde mittels verbreiteten Echtzeitvalidierungstests unter Nutzung des Programms Cyclictest durchgeführt. Eine beispielhafte Ausführung von Cyclictest ist in dem folgenden Code-Ausschnitt dargestellt:

```
taskset -c 0-1 cyclictest -m -p 99 -i 100 -t 1 - a 1 -h 120 -D 24h --
    mainaffinity=0 -M
```

Codebeispiel A.3: Überprüfung der Echtzeit mittels Cyclictest und isolierten CPU-Kern 1

Hierbei beschreibt der erste Teil taskset -c %CPU_CORE-Nummer den verwendeten CPU-Kern für den darauf benannten Befehl. Cyclictest wird darauf mit mehreren Optionen parametriert. Im Falle einer echtzeitkritischen Applikation würde im Anschluss der isolierte, validierte CPU-Kern für Berechnungen innerhalb der VM genutzt werden.

A.4 Quality of Service

Mittels QoS-Konfigurationen kann Datenverkehr priorisiert werden, um dadurch die Netzwerkmetriken für ausgewählte Datenströme zu verbessern.

Eine Überprüfung, ob QoS-Mechanismen im Falle einer Überlast des Kommunikationsnetzwerkes korrekt funktionieren, bieten Statistiken über verworfene Pakete je Hardware-Warteschlange der Netzwerkkomponente:

```
root@spine1-R# run show interfaces queue et-0/0/49

Physical interface: et-0/0/49, Enabled, Physical link is Up
  Interface index: 689, SNMP ifIndex: 518
  Description: facing_jnpr-rt-qfx-002-leaf1:et-0/0/49

Forwarding classes: 12 supported, 7 in use
Egress queues: 10 supported, 7 in use
Queue: 0, Forwarding classes: my-fwd-class-0
  Queued:
    Packets              :          221101727141               7898833 pps
    Bytes                :       320452669397026           91626448064 bps
  Transmitted:
    Packets              :          221101009840               7898795 pps
    Bytes                :       320451629311912           91626003248 bps
    Tail-dropped packets : Not Available
    RL-dropped packets   :                     0                     0 pps
    RL-dropped bytes     :                     0                     0 bps
    Total-dropped packets:                717301                    38 pps
    Total-dropped bytes  :            1040085114                444816 bps
Queue: 1...4, Forwarding classes: my-fwd-class-1...4
  Queued:
    Packets              :          160828187897               6111014 pps
```

```
    Bytes                :        20264351680188            6159903096 bps
  Transmitted:
    Packets              :          160828187897               6111014 pps
    Bytes                :        20264351680188            6159903096 bps
    Tail-dropped packets : Not Available
    RL-dropped packets   :                     0                     0 pps
    RL-dropped bytes     :                     0                     0 bps
    Total-dropped packets:                     0                     0 pps
    Total-dropped bytes  :                     0                     0 bps
```

Codebeispiel A.4: Paketverlust auf Hintergrund-Datenverkehr beschränkt

Eine beispielhafte Konfiguration für einen Edge Switch könnte folgendermaßen aussehen, in welchem auf Basis des EtherTypes von PROFINET Telegramme in eine dedizierte Hardware-Warteschlange geleitet werden, um eine Priorisierung gegenüber anderen Kommunikationsarten zu ermöglichen. Zudem wird der DSCP-Wert 50 für die Priorisierung der VXLAN-Telegramme genutzt:

```
mac access-list extended match_profinet
permit any any 0x8892 0x0

class-map match-any cm_match_dscp_50
  match dscp 50

class-map match-any cm_match_cos6
  match cos  6

class-map match-any cm_match_profinet
  match access-group name match_profinet


policy-map pm_switch_to_switch_out
class cm_match_dscp_50
  priority level 1 percent 50

policy-map pm_1G_in
class cm_match_profinet
  set dscp 50
class cm_match_dscp_50
  set dscp af13

policy-map pm_25G_edgecloud_in
class cm_match_profinet
  set dscp 50
class cm_match_dscp_50
  set dscp af13

policy-map pm_25G_edgecloud_out
class cm_match_dscp_50
  priority level 1 percent 50
  set cos 6
```

```
34
35 policy-map pm_1G_out
36 class cm_match_dscp_50
37   priority level 1
38   set cos 6
39
40
41 Int gi 2/0/12
42   service-policy input  pm_1G_in
43   service-policy output pm_1G_out
```

Codebeispiel A.5: QoS-Konfiguration für Cisco IOS-XE zur Priorisierung von PROFINET

A.5 Half&Half Validierung - eBPF XDP

Dies ist ein Code-Ausschnitt eines eBPF-Programms, welches jedes zweite eintreffende IE-Telegramm verwirft und somit die Validierung von Half&Half ermöglicht. Entscheidend ist hierfür die Nutzung der BPF_MAP als Schlüssel-Werte-Speicher für das Alternieren der gewünschten Aktionen XDP_PASS und XDP_DROP.

```
1
2 struct bpf_map def SEC("maps") mac_state = {
3     .type = BPF_MAP_TYPE_ARRY,
4     .key_size = sizeof(__u32),
5     .value_size = sizeof(__u32),
6     .max_entries = 1,
7     .map_flags = 0
8 };
9
10 SEC("prog")
11 __u32 action(struct xdp_md *ctx) {
12     void *data_end = (void *)(long)ctx->data_end;
13     void *data = (void *)(long)ctx->data;
14     struct ethhdr *eth = data;
15     __u32 key = 0;
16     __u32 *value;
17
18     if (eth + 1 > (struct ethhdr *)data_end)
19         return XDP_PASS;
20
21     if (eth->h_dest[0} == 0x00 && eth->h_dest[1] == 0x00 &&
22     (...)
23     }
24 }
```

Codebeispiel A.6: Auszug des eBPF-basierten Programms zum Verwerfen jedes zweiten Telegrammes

Ehrenerklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die Hilfe eines kommerziellen Promotionsberaters habe ich nicht in Anspruch genommen. Dritte haben von mir weder unmittelbar noch mittelbar geldwerte Leistungen für Arbeiten erhalten, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen. Verwendete fremde und eigene Quellen sind als solche kenntlich gemacht.

Ich habe insbesondere nicht wissentlich:

- Ergebnisse erfunden oder widersprüchliche Ergebnisse verschwiegen,
- statistische Verfahren absichtlich missbraucht, um Daten in ungerechtfertigter Weise zu interpretieren,
- fremde Ergebnisse oder Veröffentlichungen plagiiert,
- fremde Forschungsergebnisse verzerrt wiedergegeben.

Mir ist bekannt, dass Verstöße gegen das Urheberrecht Unterlassungs- und Schadensersatzansprüche des Urhebers sowie eine strafrechtliche Ahndung durch die Strafverfolgungsbehörden begründen kann.

Ich erkläre mich damit einverstanden, dass die Dissertation ggf. mit Mitteln der elektronischen Datenverarbeitung auf Plagiate überprüft werden kann.

Die Arbeit wurde bisher weder im Inland noch im Ausland in gleicher oder ähnlicher Form als Dissertation eingereicht und ist als Ganzes auch noch nicht veröffentlicht.

Ingolstadt, 18.10.2024

Thomas Kampa