Im Auftrag des:

Bundesamt
für Sicherheit in der
Informationstechnik

In Zusammenarbeit mit:

secunet

Studie

Open-RAN Risikoanalyse

5GRANR

Version: 1.2.1
Datum: 21. Februar 2022
Autoren: Stefan Köpsell (Barkhausen Institut)
Andrey Ruzhanskiy (Barkhausen Institut)
Andreas Hecker (Advancing Individual Networks GmbH)
Dirk Stachorra (Advancing Individual Networks GmbH)

Norman Franchi (Advancing Individual Networks GmbH)

Executive Summary

Diese Studie beschäftigt sich mit der Frage, welche **Sicherheitsrisiken** sich aus der durch die **O-RAN** Alliance spezifizierten O-RAN-Umsetzung eines 3GPP-RANs ergeben. Dabei erfolgt zunächst eine funktionale Beschreibung eines 3GPP-RANs sowie der O-RAN-Architektur. Basierend darauf wurde eine Risikoanalyse vorgenommen, wobei die Schutzziele **Vertraulichkeit, Integrität, Zurechenbarkeit, Verfügbarkeit und Privacy** berücksichtigt werden. Zur Einschätzung der Risiken, die mit einer Schutzzielverletzung einhergehen werden dabei **drei Stakeholder** berücksichtig, nämlich ein **Nutzer** eines 5G-Netzes, der **Betreiber** eines 5G-Netzes sowie der **Staat** als Persona für eine gesellschaftliche Perspektive.

Da die aktuell vorliegenden O-RAN-Spezifikationen an vielen Stellen noch recht unspezifisch sind und gerade im Bereich Sicherheit wenig Vorgaben machen, wurden bei der Risikoanalyse zwei Perspektiven berücksichtigt. Zum einen eine **worst-case Perspektive**, in der keine der optionalen Sicherheitsmaßnahmen umgesetzt ist und eine **best-case Betrachtung**, bei der unterstellt wurde, dass alle (optionalen) Sicherheitsmaßnahmen auch tatsächlich umgesetzt wurden.

Bei der Risikoanalyse wurden ferner **verschieden mächtige Angreifer** berücksichtigt: ein **außenstehender Angreifer, ein 5G-Nutzer, ein Insider, der Cloud-Betreiber** sowie der **RAN-Betreiber**.

Im Ergebnis der Risikoanalyse konnte festgestellt werden, dass von einer **Vielzahl** der in O-RAN spezifizierten Schnittstellen und Komponenten **mittlere bis hohe Sicherheitsrisiken** ausgehen. Dies ist wenig überraschend, da sich der aktuelle Entwicklungsprozess der O-RAN-Spezifikationen nicht an dem Paradigma von „**security/privacy by design/default“** orientiert und auch die Prinzipien der **mehrseitigen Sicherheit** (minimale Vertrauenswürdigkeitsannahmen bezüglich aller Beteiligten) **nicht berücksichtigt** wurden.

Im Zuge der Durchführung der Risikoanalyse konnten einige **Verbesserungsmöglichkeiten** zur Risikominimierung identifiziert werden. Diese finden sich als Empfehlungen am Ende der Studie. Wichtig ist, dass Sicherheitsverbesserung **jetzt** in die Spezifikation aufgenommen werden, um ein **Sicherheitsdebakel**, wie es bei der Entwicklung der 3GPP-Standards erfolgte, diesmal zu **vermeiden**.

Im Auftrag des:

Bundesamt
für Sicherheit in der
Informationstechnik

Diese Risikoanalyse wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragt und finanziert. Eine Einflussnahme des BSI auf die Ergebnisse fand nicht statt.

Inhaltsverzeichnis

1 Einführung

Mobilfunknetze der 5. Generation (5G) bieten eine Vielzahl neuer Anwendungsfälle, die insbesondere den Bereich der Vernetzung von „Dingen“ betreffen. Dadurch gewinnt 5G eine immer zentralere Rolle im Bereich der Basiskommunikationsinfrastrukturen — insbesondere auch als Basiskommunikationsinfrastruktur für kritische Infrastrukturen wie etwa Energie- und Wasserversorgung, Logistik und Verkehr. Daher ist es notwendig, sich der Risiken, die sich aus dem Einsatz von 5G als Kommunikationsinfrastruktur im Sinne von IT-Sicherheit und Datenschutz ergeben, bewusst zu sein. Eine derartige Risikoanalyse ist daher das primäre Ziel dieser Studie. Dabei geht es in dieser Studie einschränkend nicht um ein 5G-Gesamtsystem, bestehend im Wesentlichen aus 5G-Funkzugangsnetz (5G-RAN) und dem 5G-Kernnetz (5G-Core). Vielmehr wird bei der Risikoanalyse lediglich das 5G-RAN betrachtet. Dabei wiederum liegt der Fokus auf einem konkreten Umsetzungsvorschlag eines 5G-RAN, welcher durch die O-RAN ALLIANCE[1] spezifiziert wird. Dieser Umsetzungsvorschlag wird als O-RAN bezeichnet.

Das primäre Ziel dieser Studie ist also eine O-RAN-Risikoanalyse. Diese stellt die sich aus den aktuellen Spezifikationen ergebenden Bedrohungen und Risiken dar und kann als Entscheidungsgrundlage bezüglich notwendiger zukünftiger Maßnahmen zur Risikominimierung dienen.

Zunächst erfolgt ein Überblick über das Next Generation Radio Access Network (NG-RAN) aus technisch-funktionaler Sicht. Dabei wird insbesondere auf die O-RAN-Architektur eingegangen. Dem schließt sich eine Vorstellung der in dieser Studie angewendeten Methodologie zur Risikoanalyse an. Dabei werden insbesondere die betrachteten Schutzziele und das zugrunde gelegte Angreifermodell näher erläutert. Im nachfolgenden 4. Kapitel wird kurz auf existierende Studien im Bereich Risiko- bzw. Bedrohungsanalyse im Bereich NG-RAN bzw. O-RAN eingegangen. Hervorzuheben sind hier insbesondere die Analysen, die von der O-RAN ALLIANCE selber stammen.

Dem schließt sich der Hauptteil dieser Studie an, die eigentliche O-RAN-Risikoanalyse. Eine entsprechende Risikoanalyse bezüglich NG-RAN allgemein befindet sich in Anhang A. Für das Verständnis der O-RAN-Risikoanalyse ist Hintergrundwissen zu den allgemeinen NG-RAN Risiken notwendig. Ist dies nicht vorhanden, so wird dem Leser empfohlen zunächst Anhang A zu lesen und dann die O-RAN-Risikoanalyse in Kapitel 5. Die Risikoanalyse erfolgt dabei zunächst bezüglich einzelner Komponenten und Schnittstellen von O-RAN, um darauf basierend eine Einschätzung zu Sicherheitsrisiken für O-RAN insgesamt abzugeben.

Die Studie schließt mit Empfehlung bezüglich Maßnahmen, die zu einer Verbesserung der O-RAN-Sicherheit führen können.

[1] https://www.o-ran.org/

2 Next Generation Radio Access Network (NG-RAN)

NG-RAN, Open-RAN, O-RAN; diese Begriffe sind aktuelle Bestandteile des hier betrachteten Themenbereichs RAN und tauchen durch das gesamte Dokument immer wieder auf. Insbesondere die beiden letzten Ausdrücke werden gerne unbedarft als Synonyme verwendet. Verständlicherweise, weil sie nicht nur ähnlich klingen, sondern auch untrennbar verbunden sind. Die Kurzform lautet: Die „O-RAN Alliance“ hat sich gebildet, um das Konzept „Open-RAN“ zu verwirklichen. Wie sich der Kontext aller drei Bezeichnungen untereinander weiter darstellt, erläutert der einleitende Abschnitt 2.1.

Abschnitt 2.2 geht tiefer in die NG-RAN-Architektur ein, angefangen mit dem 3GPP-Standard hin zu den Spezifikationen durch O-RAN. Abschnitt 2.3 erläutert die durch O-RAN eingeführten Schnittstellen, die für die Sicherheitsbetrachtungen in den späteren Kapiteln wesentlich sind. Abschnitt 2.4 behandelt das Thema Anwendungen, wobei insbesondere das Thema „Maschinelles Lernen“ (engl. Machine Learning, ML) durch O-RAN in den Fokus gerückt wird. Abschnitt 2.5 schließt mit Informationen zu der existierenden O-RAN-Software, die zur Entwicklung eigener Lösungen für alle Interessierten offen ist.

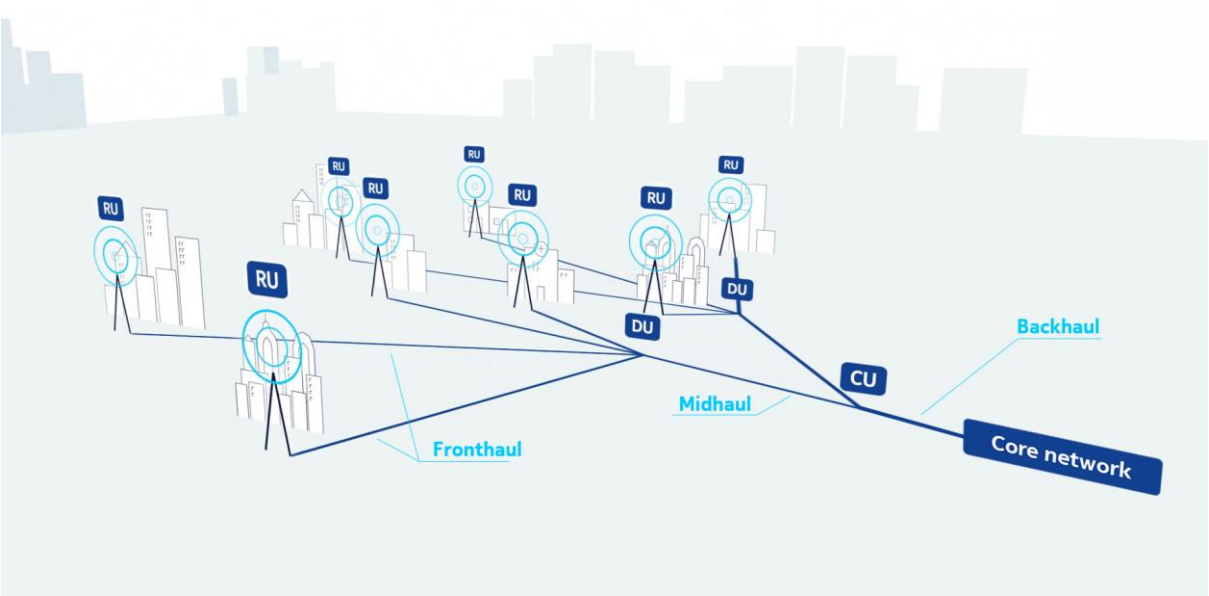

Abbildung 1: Vereinfachte Darstellung einer Open-RAN-Architektur (Quelle: Nokia)

2.1 Einleitung und Begriffe

Das Funkzugangsnetz (engl. Radio Access Network, RAN) bildet in einem Mobilfunknetz das Bindeglied zwischen Endgeräten und dem Kernnetz. Für die fünfte Generation (5G) der Mobilfunknetze spezifizierte die 3GPP in Release 15 die Mobilfunk-Luftschnittstelle New Radio (NR) und das Next Generation RAN (NG-RAN). NG-RAN bietet den Zugang sowohl über NR als auch über E-UTRA (Evolved UMTS Terrestrial Radio Access), die Luftschnittstelle von 4G/LTE (Long Term Evolution). Der Mischbetrieb von LTE- und NR-Basisstationen, die an ein Kernnetz (4G oder 5G) angebunden sind, wird als Non-Standalone-Modus (NSA-Mode) bezeichnet; der ausschließlich auf NR und 5G-Kernnetz basierende Betrieb als Standalone-Modus (SA-Mode) [1].

Die ersten 3GPP-Studien zu NG-RAN begannen in Release 14 und mündeten in den Technical Report [2]. Neben der Möglichkeit, sowohl im SA- als auch im NSA-Mode zu arbeiten, ist dort bereits ein weiteres charakteristisches Merkmal von NG-RAN enthalten: die Möglichkeit, die 5G-Basisstation in eine zentralisierte Einheit (engl. Centralized Unit, CU) und eine oder mehrere verteilte Einheiten (engl. Distributed Units, DUs) aufzutrennen. Diese Aufteilung der Basisstation ergibt zusätzliche Möglichkeiten und Freiheiten für das Deployment, wie in Abbildung 1 beispielhaft skizziert.

2.1.1 Open-RAN[2]

Parallel zu den NG-RAN-Arbeiten von 3GPP wird seit einigen Jahren das Konzept der sogenannten “Öffnung des RANs” („Open-RAN“) als Gegensatz zur „traditionellen Art“ verfolgt. Beim traditionellen Ansatz der RAN-Bereitstellung, wie sie in den meisten öffentlichen Mobilfunknetzen vorzufinden ist, stellt das RAN eine monolithische Lösung dar. Die internen Schnittstellen innerhalb dieser Lösung sind proprietär und für Drittanbieter weitestgehend nicht offengelegt. Die zugehörige Hardware ist eine eigenständige Lösung, die nicht mit Geräten anderer Hersteller kompatibel ist. Die Funktionen und die proprietären Schnittstellen einer solchen monolithischen RAN-Lösung sind hochgradig optimiert, dadurch jedoch unflexibel. Das Ziel bei der Verfolgung des Open-RAN-Konzepts ist dementsprechend, das RAN unabhängiger von proprietärer Technik zu machen, indem Spezifikationen für offene Schnittstellen definiert und Netzelemente bzw. -funktionen von der Hardware abstrahiert werden.

Für die Betreiber von Mobilfunknetzen besteht bezüglich der Realisierung des Open-RAN-Konzepts eine hohe Motivation, weil die Ausrüstung ihrer Netze mit sehr hohen Kosten verbunden und gleichzeitig der Markt für RAN-Equipment von geringem Wettbewerb geprägt ist. Mit jeder neuen Mobilfunkgeneration muss die gesamte Technik für Milliardensummen ausgetauscht oder parallel aufgebaut werden. Zusätzlich wird die Hardware mit jeder Erweiterung komplexer, mehr Anwendungen und Features müssen unterstützt werden, und damit steigen die Preise. Mit Ericsson, Nokia und Huawei stehen dagegen lediglich drei Hauptanbieter zur Verfügung. Hinzu kommt, dass die Produkte von Huawei in einigen Ländern von den Mobilfunkbetreibern nicht eingesetzt werden dürfen. Der üblicherweise schrittweise Einstieg neuer Anbieter ist nicht möglich, weil die Ausrüstung für ein RAN durch die Eigenständigkeit der Produktlösungen vollständig von einem Anbieter geliefert werden muss [3]. Mit der Verfolgung des Open-RAN-Konzepts soll es daher in Zukunft ermöglicht werden, den Wettbewerb zu erhöhen und die Kosten zu senken, indem das RAN mit Hilfe von interoperablen Komponenten verschiedener Hersteller aufgebaut und betrieben werden kann. Und die Modularisierung soll die Möglichkeit eröffnen, bei erforderlichen Erweiterungen des RANs lediglich (Software-)Komponenten austauschen zu können und nicht die komplette Technik.

Mit Bezug auf die durch 3GPP bereits standardisierten Elemente werden bei der Verfolgung des Open-RAN-Konzepts die nächsten Schritte ausfindig gemacht. So unterteilt die Open-RAN-Umgebung zusätzlich zu den bereits standardisierten Elementen CU und DU die Radio Unit (RU), die in der Antenne integriert oder in der Nähe dieser angesiedelt ist. Damit wird durch Open-RAN das Fronthaul als Verbindung zwischen RU und der DU definiert. Das Midhaul zwischen der DU und der CU sowie das Backhaul zur Verbindung des RANs mit dem Core sind bereits durch das von 3GPP standardisierte NG-RAN festgelegt (s. Abbildung 1).

2.1.2 O-RAN

Basierend auf der Idee von Open-RAN wurde 2018 die O-RAN Alliance mit Firmen aus dem Telekommunikationssektor, hauptsächlich einem internationalen Konsortium von Netzbetreibern, gegründet. Das Ziel dieser Vereinigung ist die Standardisierung eines NG-RAN, welches weitgehend auf virtualisierten und interoperablen Komponenten basiert. Die angestrebte Flexibilität soll maßgeschneiderte Lösungen für individuelle Anwendungen ermöglichen, die bei Bedarf kurzfristig neu konfiguriert und effizient optimiert werden sollen. Ergebnis dieser Bemühungen ist die Entwicklung der O-RAN-Architektur, welche sich mit der durch die 3GPP standardisierte RAN-Architektur verzahnt. Die O-RAN-Architektur sollte

[2] Es gibt verschiedene Schreibweisen dieses Begriffs, die vielerorts synonym verwendet werden: mit oder ohne Bindestrich oder zusammengeschrieben. In dieser Studie wird die Schreibweise „Open-RAN“ gewählt, sofern die Verknüpfung zu einer Referenz nicht eine andere Schreibweise vorgibt.

generell als Ergänzung zu den bestehenden 3GPP-Standards gesehen werden. Auf Dauer können die Ergebnisse von O-RAN wieder in den Standards der 3GPP münden. Bis dahin existiert die O-RAN-Architektur als Zusatz zu der 3GPP-Architektur.
Die O-RAN Alliance unterstützt die O-RAN-Software-Community in einer Kooperation mit der Linux Foundation. Im Sommer 2020 gab die Allianz bekannt, dass sie gemeinsam mit der ONF (Open Network Foundation) das Projekt 5G SD-RAN (5G Software-Defined Radio Access Network) starten wird, um die Erstellung von Open-Source-Software für mobile 4G- und 5G-RAN-Implementierungen zu fördern und zu erleichtern.
Die Existenz der SD-RAN-Gruppe bedeutet nicht, dass alle Komponenten der O-RAN-Architektur Open Source sein werden oder sogar, dass sie auf dem von der Projektgruppe entwickelten Open-Source-Code basieren müssen. Allerdings wird die Software-Community, die um dieses Open-Source-Projekt herum entstehen soll, die Entwicklung von Anwendungen für die Konfiguration und Optimierung beeinflussen. Ein Beispiel dafür ist die Beteiligung von der RIA (RAN Intelligence and Automation), eine Untergruppe der TIP (s. Abschnitt 2.1.3), am 5G SD-RAN-Programm. Die RIA zielt darauf ab, KI/ML[3]-basierte Anwendungen für eine Vielzahl von RAN-Anwendungsfällen zu entwickeln und einzusetzen, darunter SON (Self-Organizing Network), RRM (Radio Resource Management) und mMIMO (massive Multiple Input and Multiple Output) [4].

2.1.3 TIP

Das Telecom Infra Project (TIP) wurde 2016 als ingenieursorientierte Kollaboration gegründet. Das Ziel dieses Projekts besteht in dem Aufbau und der Bereitstellung einer globalen Telekommunikationsnetzinfrastruktur mit der Ermöglichung eines globalen Zugangs für alle Interessenten. TIP schafft ein Ökosystem von Hardware- und Softwareanbietern, initiiert Plugfests und entwickelt Blueprints. TIP schreibt keine Spezifikationen, sondern betätigt sich weltweit in Förderungen, Schulungen und Implementierungen von Open-RAN-Lösungen.
Das „OpenRAN“-Projekt von TIP und die O-RAN Alliance haben 2020 eine Liaison-Vereinbarung bekannt gegeben, um ihre Übereinstimmung bei der Entwicklung interoperabler, disaggregierter und offener RAN-Lösungen sicherzustellen [5].

2.1.4 Weitere Gruppen

Neben der 3GPP und dem TIP existieren noch weiteren Organisationen, die an Open-RAN bzw. an der O-RAN-Spezifikation und O-RAN-Entwicklung beteiligt sind und dazu einen Beitrag leisten. Genannt seien das Small Cell Forum, die bereits erwähnte Open Networking Foundation (ONF) und die OpenAirInterface Software Alliance (OSA) [4].

2.2 NG-RAN-Architektur

In diesem Abschnitt wird die Architektur des NG-RANs näher erläutert. Begonnen wird mit der 3GPP-Spezifikation (Abschnitt 2.2.1) und einer Ausführung zu der Aufteilung der Nutzer- und Kontrollebenen (Abschnitt 2.2.2), die als Basis für die O-RAN-Architektur dienen (Abschnitt 2.2.3). Abschnitt 2.2.4 geht auf die Herausforderungen ein, die bei der Integration von RAN-Komponenten unterschiedlicher Hersteller entstehen, bevor eine Darstellung zum Thema RAN-Sharing (Abschnitt 2.2.5) folgt sowie eine Auswahl von Möglichkeiten, welche die O-RAN-Allicance auf der Basis der bisher existierenden Konzepte sieht.

[3] KI steht für „Künstliche Intelligenz“ (engl. Artificial Intelligence, AI), bezeichnet die Fähigkeit eines Computers, menschliches Denkverhalten nachzuahmen, und ist ein Oberbegriff für die Leistungsbeschreibung einer Maschine. Maschinelles Lernen (ML) hingegen beschreibt eine Verfahrensgruppe zum Extrahieren von Erkenntnissen aus Daten für KI-Anwendungen.

2.2.1 Spezifikation nach 3GPP

Abbildung 2 zeigt ein aus zwei 5G-Basisstationen (Next Generation NodeBs, gNBs) bestehendes NG-RAN sowie die Schnittstellen zur Anbindung an das Core und die Endgeräte. Die gNB ist in zwei logische Funktionen aufgeteilt, die CU und DU (s. Einleitung in Abschnitt 2.1).

Die DU ist die Basisbandeinheit in einem 5G-RAN. Sie führt die Layer-1- und Layer-2-Verarbeitung durch und führt kritische Funktionen wie Kodierung/Dekodierung, Scheduling, MIMO-Verarbeitung und Beamforming aus. Sie trifft im Sub-Millisekundenbereich Entscheidungen über die Zuweisung von Funkressourcen innerhalb einer Zelle, basierend auf Faktoren wie verbindliche Regeln (Policies), Interferenzbedingungen oder dem Typ und der Verteilung der Benutzergeräte.

Die CU ist ein neuer Knoten in 5G, der in 4G nicht als diskrete Funktion existiert. In der 3GPP-RAN-Architektur bietet die CU Layer-3-Funktionen wie Verbindungs- und Mobilitätsmanagement. Sie ist aufgeteilt in die CU-UP für die User-Plane-Verarbeitung und die CU-CP für die Control-Plane-Verarbeitung (s. folgenden Abschnitt 2.2.2). Für den Austausch von Konfigurationsdaten und weiteren Informationen zwischen diesen disaggregierten Einheiten dient die E1-Schnittstelle, die in [6] definiert ist. Weiterhin sind CU-CP und CU-UP jeweils mit der DU über die Schnittstellen F1-C und F1-U verbunden, welche in [7] definiert sind. Richtung 5G-Core bestehen die NG-C Schnittstelle zwischen der CU-CP und der AMF (Access and Mobility Management Function) sowie die NG-U Schnittstelle zwischen der CU-UP und der UPF (User Plane Function).

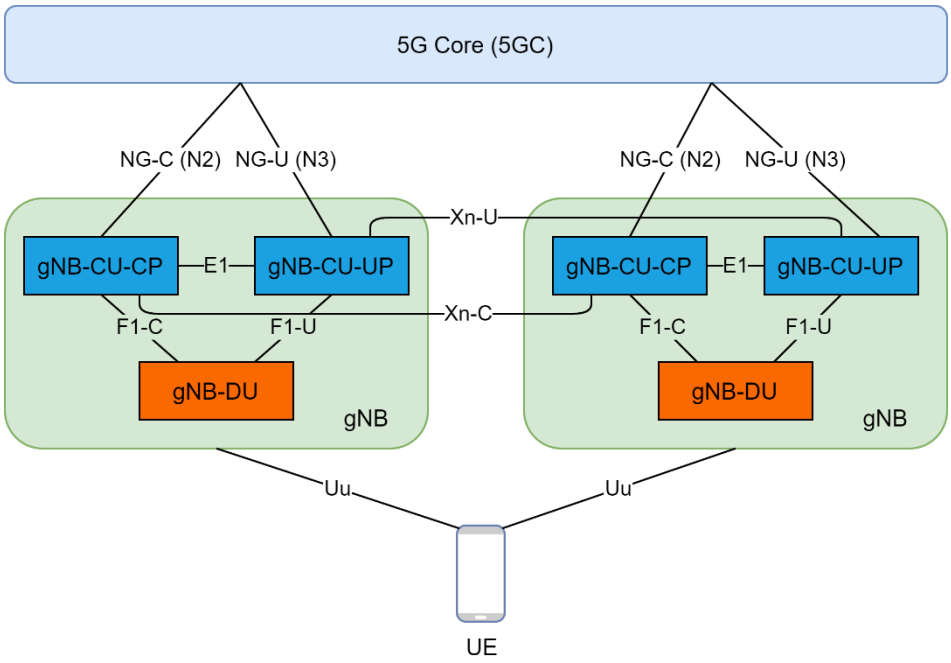

Abbildung 2: 3GPP-Architektur für 5G NR

Es ist anzumerken, dass die 3GPP-Architektur nicht die Remote Radio Unit (RRU) spezifiziert, d. h. die Implementierung der Schnittstelle zwischen PHY- und HF-Schicht wird den Anbietern überlassen.

2.2.2 Control/User Plane Separation

Die Control/User Plane Separation (CUPS) bezeichnet in Mobilfunknetzen die vollständige Trennung der Control Plane (Steuerebene) und der User Plane (Benutzerebene). Die Control Plane ist für Funktionen wie Verwaltung der Benutzerverbindung, Festlegung von QoS-Richtlinien oder die Benutzerauthentifizierung zuständig. Die User Plane ist für den Transport des Datenverkehrs verantwortlich.

Bezüglich 4G wurde CUPS erstmals in 3GPP-Release 14 für den EPC (Evolved Packet Core) eingeführt [8] und in Release 15 auf 5G-Systeme erweitert [9]. Die Hauptmotivation für diese Auftrennung besteht darin, die User Plane unabhängig von der Control Plane skalieren zu können und somit den Betreibern eine größere Flexibilität in der Dimensionierung ihrer Netze zu ermöglichen. Beispielsweise kann die User Plane bei Zunahme des Datenverkehrs erweitert werden, ohne die Funktionen der Control Plane zu verändern.
CUPS ermöglicht eine freie Konfigurierung der User Plane, um anwendungsspezifische Anforderungen an die Weiterleitung, Datenkapselung, Verkehrssteuerung oder an andere Aufgaben zu erfüllen, die entsprechend den Vorgaben aus der Control Plane empfangen werden. Dies ermöglicht die Implementierung verschiedener Lösungen für die Nutzerdatenübertragung, die in derselben User Plane nebeneinander bestehen und dynamisch entsprechend den Erfordernissen des spezifischen Verkehrs ausgewählt werden können. Zudem ermöglicht eine separate User Plane kürzere Delays beim Transport des Datenverkehrs und erlaubt somit die Erfüllung höherer Latenzanforderungen.
Abbildung 3 zeigt die verwendeten Protokolle in der User Plane zwischen dem UE und der gNB auf der Uu-Schnittstelle und ihre Umwandlung zu den Protokollen, die auf der Schnittstelle NG-U (N3) zwischen der gNB und der UPF im 5G-Core verwendet werden. Standartmäßig existieren die physikalische Schicht L1 sowie die MAC-Schicht L2 für den Netzzugang. Die RLC (Radio Link Control) wird über IP abgebildet. Das PDCP (Packet Data Convergence Protocol) wird im gNB auf das UDP (User Datagram Protocol) umgesetzt. UDP ist ein verbindungsloses und nicht zuverlässiges Übertragungsprotokoll, das außerdem weder gesichert noch geschützt ist. Das SDAP (Service Data Adaptation Protocol) wird zu GTP-U (GPRS Tunneling Protocol – User) umgesetzt. GTP-U-Tunnel werden zur Übertragung von gekapselten Nutzerdatenpaketen (Transport Packet Data Units, T-PDUs) verwendet sowie für Signalisierungsnachrichten zwischen einem bestimmten Paar von GTP-U-Tunnelendpunkten. Die im GTP-Header enthaltene Tunnel-Endpunkt-ID (TEID) gibt an, zu welchem Tunnel eine bestimmte T-PDU gehört [10].

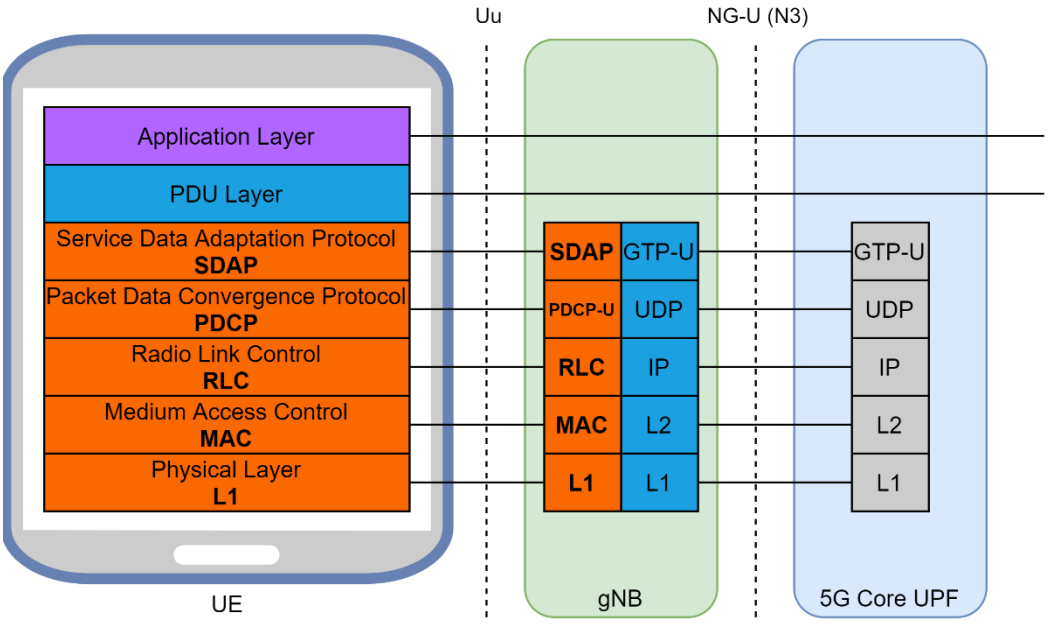

Abbildung 3: Protokollschichten der User Plane

Abbildung 4 zeigt die verwendeten Protokolle in der Control Plane und die Umwandlung im gNB zu den Protokollen, die auf der Schnittstelle NG-C (N2) zwischen der gNB und dem AMF im 5G-Core zum Einsatz kommen. Die untersten drei Schichten bestehen analog zu den Schichten in der User Plane (s.o.). Für die Control Plane wird PDCP zu SCTP (Stream Control Transmission Protocol) umgesetzt. Im Gegensatz zu UDP ist SCTP ein zuverlässiges,

verbindungsorientiertes Netzwerkprotokoll [11]. Das RRC-Protokoll (Radio Resource Control Protocol) wird im gNB zu NG-AP (Next Generation Application Protocol) umgesetzt, welches in [12] beschrieben ist.

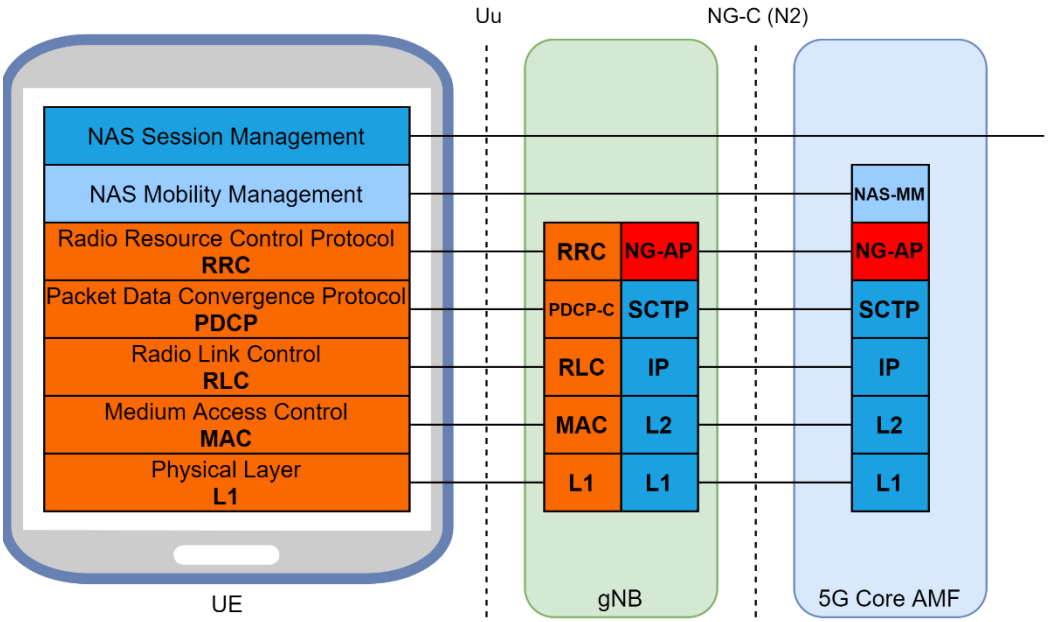

Abbildung 4: Protokollschichten der Control Plane

Das NAS (Non-Access Stratum) [13] beschreibt eine Menge von Protokollen, die zur Übertragung von funkunabhängigen Signalisierungsnachrichten zwischen dem UE und bestimmten Funktionen des Kernnetzes verwendet werden. Die zwei grundlegenden Protokolle sind das 5GS Mobility Management (5GMM) und das 5GS Session Management (5GSM). Das Protokoll 5GMM wird zwischen der UE und dem AMF verwendet, um Nachrichten für die UE-Registrierung, die Mobilität und die Sicherheit zu transportieren. Außerdem dient es für den Transport des 5GSM-Protokolls, welches das Management der PDU Session Connectivity unterstützt und zwischen UE und SMF (Session Management Function) über das AMF angewendet wird.

2.2.3 Spezifikation nach O-RAN

Die O-RAN Alliance teilt die CU- und DU-Netzwerkfunktionen gemäß der 3GPP-Definition weiter auf. Abbildung 5 zeigt die Architektur mit ihren Funktionen und Schnittstellen und verdeutlicht die Funktions- und Schnittstellenaufteilung zwischen 3GPP und O-RAN [14]. Die in 3GPP definierten Elemente CU-CP, CU-UP, DU und eNB (Evolved Node B) erhalten in den O-RAN-Spezifikationen zur Verdeutlichung von Unterschieden das „O-“ Präfix, welches kurz für O-RAN steht. Zum Beispiel ist die O-DU in ausgeschriebener Form die „O-RAN Distributed Unit“.

Die neuen durch O-RAN definierten Funktionen sind

- das Service Management and Orchestration (SMO) Framework,
- die RAN Intelligent Controllers (RICs) in den Varianten nicht echtzeitfähig (non-real time) und beinahe echtzeitfähig (near-real time), im Folgenden jeweils mit Non-RT RIC und Near-RT RIC abgekürzt,
- die Remote Unit (O-RU) und
- die O-Cloud.

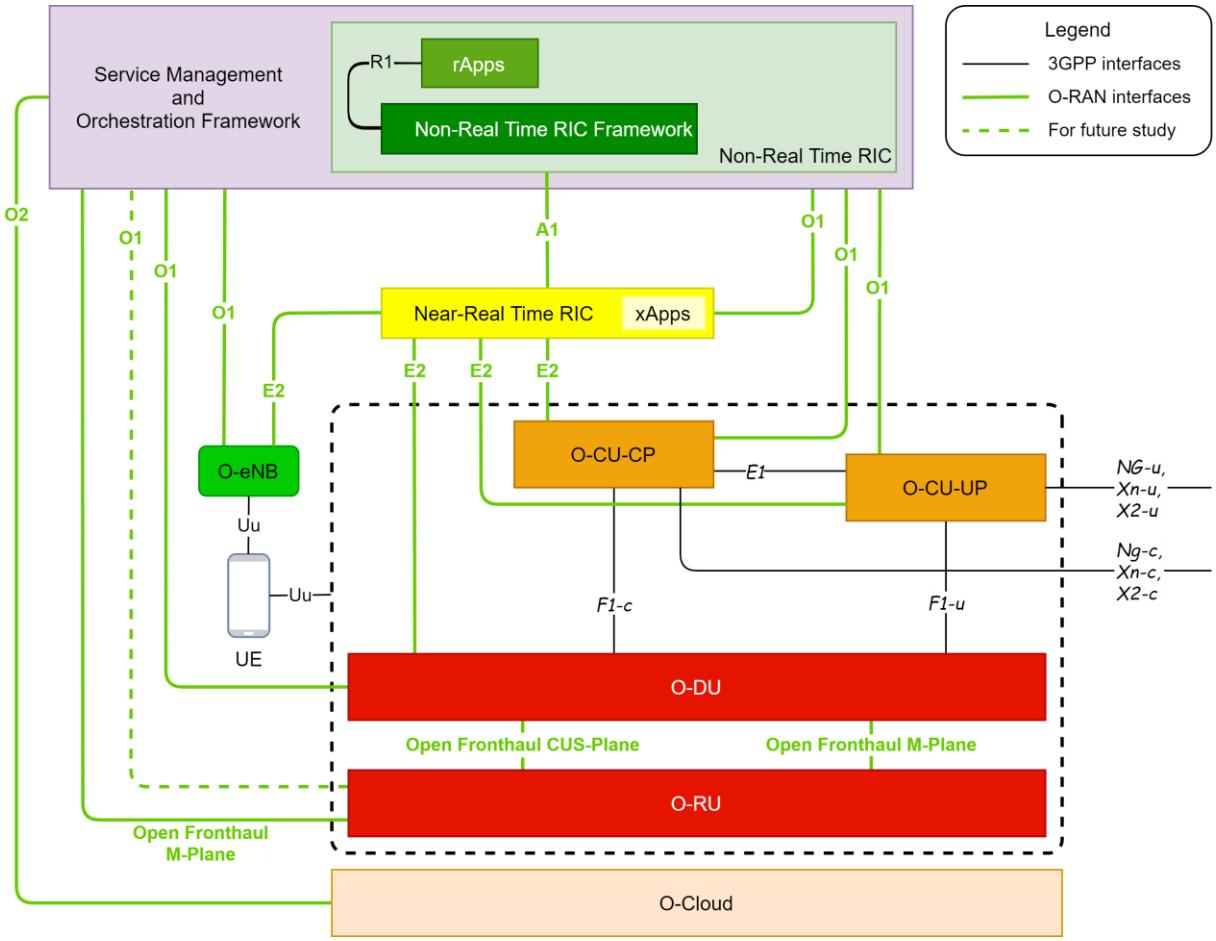

Abbildung 5: Logische O-RAN-Architektur einschließlich Uu-Schnittstelle zu O-RAN-Komponenten und O-eNB [14]

Entsprechend der definierten Funktionen sind die zugehörigen Schnittstellen definiert:

- A1 zwischen Non-RT RIC und Near-RT RIC,
- E2 zwischen dem Near-RT RIC und den als E2-Knoten bezeichneten O-CU-CP, O-CU-UP, O-DU und O-eNB,
- O1 zwischen dem SMO und den gemanagten Einheiten Near-RT RIC, O-CU-CP, O-CU-UP, O-DU und O-eNB sowie, noch in der Untersuchung, O-RU,
- O2 zwischen SMO und O-Cloud sowie
- Open Fronthaul zwischen O-DU und O-RU bzw. zwischen SMO und O-RU.

Jede dieser Funktionen könnte prinzipiell von verschiedenen Anbietern unter Einsatz herkömmlicher Hardware entwickelt und bereitgestellt werden, während der Datenaustausch zwischen den Komponenten über die offenen, spezifizierten Schnittstellen gewährleistet wird. Auf diese Weise soll das Ziel des Open-RAN-Konzepts realisiert werden.
Mit dem Aufbau ihrer Architektur auf der Basis der 5G NR-Architektur von 3GPP profitiert die O-RAN Alliance laut [15] von den erweiterten 3GPP-Sicherheitsfunktionen, die für 5G eingeführt wurden und in [16] beschrieben sind, einschließlich

- verbesserter Schutz der Benutzeridentität über Subscription Concealed Identifier (SUCI),
- vollständiger Schutz des Datenverkehrs der Control/User Plane zwischen UE und gNB (Verschlüsselung und Integritätsschutz) über die Luftschnittstelle,
- vollständiger Schutz der gNB-Schnittstellen, einschließlich der E1-Schnittstelle zwischen CU-CP und CU-UP und der F1-Schnittstelle zwischen CU und DU,
- erweiterte Heimnetzkontrolle (Authentifizierung) sowie

- zusätzliche Sicherheit für Network-Slices auf Basis von Service Level Agreements (SLAs).

2.2.3.1 Service Management and Orchestration (SMO) Framework

In der O-RAN-Architektur ist das SMO-Framework für die Verwaltung der RAN-Domäne zuständig [14]. Dazu zählen die Aufgaben:

- Unterstützung von FCAPS über die O1-Schnittstelle zwischen SMO und den O-RAN-Netzfunktionen bzw. im Hybridmodell über die Open Fronthaul M-Plane-Schnittstelle zwischen SMO und O-RU,
- RAN-Optimierung über die A1-Schnittstelle zwischen dem Non-RT RIC im SMO-Framework und dem Near-RT RIC,
- O-Cloud-Management und Orchestrierung für die Bereitstellung von Plattformressourcen sowie Workflow-/Workload-Management über die O2-Schnittstelle zwischen der SMO und der O-Cloud.

Eine formale Schnittstelle zwischen SMO und Non-RT RIC ist aktuell nicht definiert. Die Implementierung von SMO und der Grenze zum Non-RT RIC-Framework ist daher eine freie Design-Entscheidung. Bestimmte Funktionalitäten können in eine Non-RT RIC-Implementierung einbezogen oder ausgeschlossen sein. Wesentlich ist, dass die Schnittstellen A1 und R1 inhärent zum Non-RT RIC sind, während die Schnittstellen O1 und O2 es nicht sind.

2.2.3.2 O-Cloud

Die O-Cloud ist eine cloudbasierte Rechenplattform, die eine Sammlung physischer Infrastrukturknoten umfasst und die folgenden Bestandteile hostet [14]:

- die relevanten O-RAN-Funktionen Near-RT RIC, O-CU-CP, O-CU-UP und O-DU,
- die unterstützenden Softwarekomponenten wie Betriebssystem, Virtual Machine Monitor, Container Runtime, usw. sowie
- die entsprechenden Verwaltungs- und Orchestrierungsfunktionen.

2.2.3.3 RAN Intelligent Controller (RIC)

Der RIC wird von der O-RAN Alliance als integraler Bestandteil der O-RAN-Architektur spezifiziert. Wie in Abbildung 5 zu erkennen ist, erscheint der RIC in zwei Ausprägungen, die jeweils an spezifische Regelkreis- und Latenzanforderungen angepasst sind. Eine ausführliche Einführung in das Thema RIC bietet [4].

Der Near-RT RIC hat über das E2-Interface direkte Schnittstellen zur O-CU-CP, O-CU-UP und O-DU. Er ermöglicht ihre programmatische Steuerung in Zeitzyklen von 10 ms bis 1 Sekunde. Aufgrund strenger Latenzanforderungen mit Regelkreisen von weniger als 10 ms verbleiben Echtzeit-Funktionen wie das RRM auf der DU; der Near-RT RIC kann diese nicht übernehmen [14]. Prinzipiell und für die Zukunft vorstellbar kann der Near-RT RIC die O-DU programmatisch konfigurieren, um die Funktionsweise zu verbessern. Beispielsweise könnte der Near-RT-RIC verwendet werden, um das Scheduler-Verhalten auf der DU zu ändern. Zuständig für die Spezifikation des Near-RT RICs in der O-RAN Alliance inklusive des E2-Interfaces ist die Working Group 3 (WG3).

Der Non-RT RIC ist für Regelkreise von mehr als 1 Sekunde spezifiziert. Er stellt Policies für die höheren Netzschichten auf. Sie können im RAN entweder über den Near-RT RIC durch das A1-Interface oder über die SMO-Verbindung zu den RAN-Knoten durch das O1-Interface implementiert werden. Umgekehrt sammelt der Non-RT RIC über die O1-Schnittstelle Daten von den RAN-Komponenten ein, die in standardisierten Formaten anfallen, um damit traditionelle RAN-Optimierungsfunktionen zu bedienen. Durch seine weiter oben angesiedelte Platzierung in der Architektur kann der Non-RT RIC auf größere RAN-Datensätze zugreifen,

die über längere Zeiträume generiert wurden, um einen tieferen Einblick in die Leistung zu erhalten und potenzielle Optimierungen zu identifizieren, die bei der Verarbeitung im Sub-Sekunden-Bereich nicht sichtbar sind.
Der Non-RT RIC kann zudem mit anderen Netzdatenquellen verbunden werden (z. B. zur gemeinsamen Optimierung der Funk-, IP-Netzwerk- und Edge-Cloud-Leistung). Er kann auch auf Datensätze außerhalb des Netzes selbst zugreifen, z. B. auf solche, die sich auf Verkehr, Notdienste, Wetter, öffentliche Massenveranstaltungen usw. beziehen, so dass das Netz sich auf Ereignisse in der realen Welt vorbereiten oder darauf reagieren kann.
Zuständig für die Spezifikation in der O-RAN Alliance für den Non-RT RIC ist die Working Group 2 (WG2) zusammen mit dem zugehörigen Interface A1. Das O1-Interface ist Bestandteil der Working Group 1 (WG1).
Es ist anzumerken, dass die vom RIC eingeführten Regelkreise potenziell mit den von den Mobilfunkanbietern eingeführten Verfahren zur Aktualisierung von Policies für die DU- und CU-Funktionen in Konflikt geraten können.

2.2.3.4 O-CU und O-DU

Die RAN-Knoten O-CU-CP, O-CU-UP und O-DU entsprechen den in 3GPP definierten Einheiten CU-CP, CU-UP und DU. Als Folge dessen bedienen die O-CU-CP und O-CU-UP die in 3GPP spezifizierte Schnittstelle E1 und gegenüber der O-DU die Schnittstellen F1-C/F1-U. Wie in [17] spezifiziert bedienen der O-CU-CP die RRC- und PDCP-Protokolle und der O-CU-UP die PDCP- und SDAP-Protokolle gegenüber dem UE, während die O-DU die RLC-, MAC- und High-PHY-Funktionen der Funkschnittstelle bedient (vgl. Abschnitt 2.2.2).
Die O-RAN-Architektur führt die folgenden Änderungen ein [14]: Die O-CU-CP, O-CU-UP und O-DU terminieren die E2-Schnittstelle zum Near-RT RIC und die O1-Schnittstelle zum SMO-Framework. Die O-DU bedient die Open Fronthaul-Schnittstelle inkl. der Open Fronthaul M-Plane-Schnittstelle gegenüber der O-RU, um das O-RU-Management entweder im hierarchischen Modell oder im Hybridmodell (s. [18] bzw. Abschnitt 2.3.7) zu unterstützen.

2.2.3.5 O-eNB

Die O-RAN-Architektur bezieht 4G/LTE über die O-eNB ein. Die O-eNB kann dabei eine entsprechend nach [17] definierte eNB oder eine nach [19] definierte ng-eNB (Next Generation eNB) sein. Dementsprechend müssen die zugehörigen Schnittstellen und Protokolle bedient werden. Für die O-RAN-Kompatibilität müssen zusätzlich die Schnittstellen E2 und O1 unterstützt werden.

2.2.3.6 O-RU

Die O-RAN-Architektur beinhaltet gegenüber 3GPP auch die Antenneneinheit, die als O-RAN Radio Unit (O-RU) bezeichnet wird. Sie beinhaltet die Antennenstruktur sowie die analoge Hochfrequenz- (HF) und Endstufen-Technik. Die O-RU ist über die Schnittstelle Open Fronthaul (Open FH) mit der O-DU verbunden. Sie bildet Low-PHY-Funktionen der Funkschnittstelle gegenüber dem UE ab. Gegenüber den anderen RAN-Knoten handelt es sich hierbei um einen physikalischen Knoten. Die Virtualisierung der O-RU ist ein Thema für zukünftige Studien [14].

2.2.4 Open-RAN Integrations-Modell

Den Netzbetreibern entstehen im RAN der größte Teil der Kosten in CapEx (Capital Expenditure; z. Dt. Investitionskosten) und OpEx (Operational Expenditure, z. Dt. Betriebskosten). Deshalb sind effiziente Strukturen und Prozesse für Deployment, Integration und laufenden Betrieb eines RANs besonders relevant. Mit der Einführung der O-RAN-Architektur nimmt die Bedeutung der Integration der verschiedenen Komponenten potentiell unterschiedlicher Hersteller sogar noch zu, einerseits für eine erfolgreiche Inbetriebnahme und

andererseits für den sicheren Betrieb und das Management von HW- und SW-Upgrades. Es wird erwartet, dass in den meisten Fällen nicht der Netzbetreiber selber die Integration verantwortet, sondern darauf spezialisierte Systemintegratoren (SI) oder Managed Service Provider (MSP).
Über die Kosten verschiedener Ansätze wird breit diskutiert, allerdings sind die Komplexität und Sicherheitsrelevanz der Integrationsaufgaben unbestritten. Neue Abnahmeprozeduren und Interoperabilitätstest sind notwendig und müssen ggf. auch zertifiziert werden. Im Betriebskonzept müssen dedizierte Monitoring-Funktionen eingesetzt werden, die sich ausschließlich auf die permanente Verifizierung der Betriebs- und Datensicherheit der verteilten RAN-Komponenten richtet, insbesondere, wenn DevOps-Prozesse zu automatisierten Software-Updates von den Netzwerkfunktionen eingesetzt werden.
Zur Illustration eines möglichen Szenarios ist in der Abbildung 6 der Fall dargestellt, dass ein CU-Anbieter und jeweils mehrere DU- und RU-Anbieter mit verschiedenen Software-Versionen im O-RAN integriert werden sollen, unter der Annahme, dass die Software auf COTS-Hardware (Commercial Off-The-Shelf, z. Dt. Kommerzielle Produkte aus dem Regal) installiert wird.

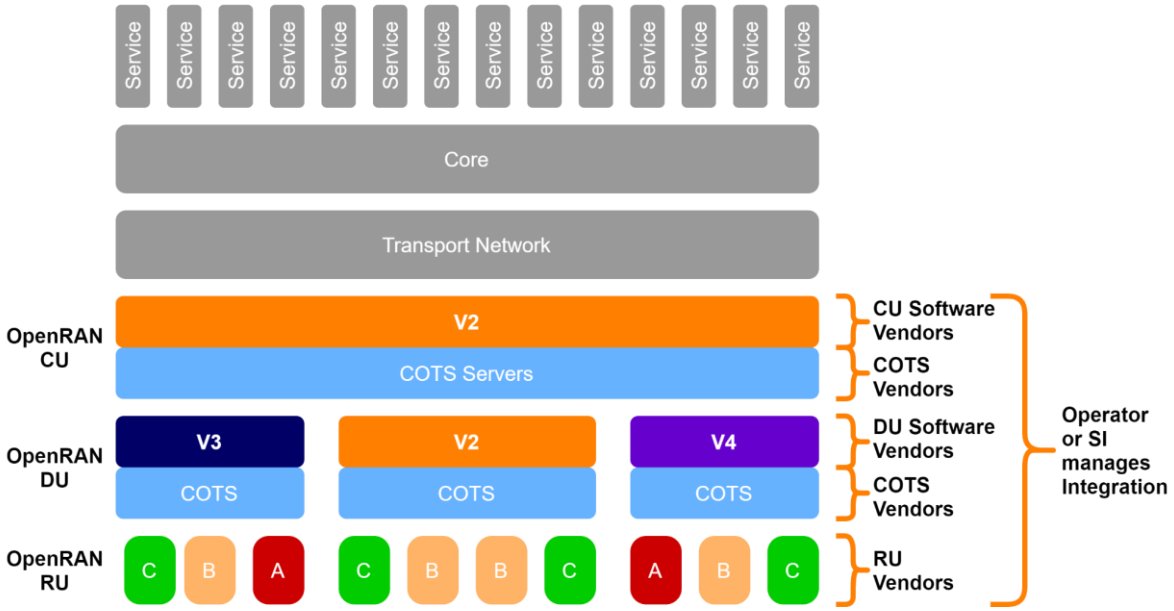

Abbildung 6: Integrationsmodelle für Open-RAN, gemanagt durch die Betreiber oder Systemintegratoren ([Quelle: Parallel Wireless], vgl. [20])

Angemerkt sei hier, dass alle in Betrieb befindlichen Komponenten der herkömmlichen Technologien von 2G bis 4G/LTE neben der neu zu integrierenden NG-RAN-Funktionalität zusätzlich einbezogen werden müssen. Ausnahmen bilden isolierte Campusnetze, sofern sie kein Legacy-Netz einbinden.

2.2.5 RAN-Sharing-Konzepte

Zu den grundsätzlichen Unterscheidungsmerkmalen in den RAN-Sharing-Konzepten zählen das passive und aktive Sharing. Unter passivem Sharing wird die gemeinsame Nutzung passiver Netzelemente verstanden. Dazu zählt die gemeinsame Nutzung von Standorten, Masten, Stromversorgung und Kühlung sowie die Anschlüsse zwischen den Standorten und den jeweiligen Konzentrationspunkten bis hin zu den Kernnetz-Standorten. Dazu zählen auch standortbezogene Dienstleistungen und Kosten, wie etwa Security, Brand- oder Objektüberwachung. Die gemeinsame Nutzung aktiver Netzelemente wird als aktives Sharing bezeichnet. Gemeinsames Merkmal ist die gemeinschaftliche Nutzung elektronischer Netzelemente.

2.2.5.1 MORAN und MOCN

Für aktives Sharing existieren zwei RAN-Sharing-Konzepte [21], die in Abbildung 7 dargestellt sind: Multi-Operator Radio Access Network (MORAN) und Multi-Operator Core Network (MOCN). Bei MORAN werden alle Bestandteile des RANs (RAN-Systemtechnik, Antenne, Mast, Standort, Stromversorgung) von zwei oder mehr Betreibern gemeinsam genutzt. Jeder Betreiber nutzt dedizierte Funkfrequenzen. Bei diesem Ansatz können sie unabhängig voneinander die Zellebene steuern, z. B. kann jeder Betreiber seine eigenen Optimierungsparameter und die Sendeleistung festlegen, um Zellreichweite und Interferenzen zu kontrollieren.

Bei MOCN teilen sich zwei oder mehr Kernnetze das gleiche RAN, d. h. die Betreiber teilen sich auch die Frequenzen. Die Träger werden gemeinsam genutzt. Die Betreiber können somit ihre Netze nicht auf Zellebene kontrollieren. Die bestehenden Kernnetze können getrennt gehalten werden. MOCN ist die ressourceneffizienteste Lösung, da es den Mobilfunkbetreibern die Möglichkeit gibt, ihre jeweiligen Frequenzzuweisungen in einen gemeinsamen Pool zu legen. MOCN ist von der 3GPP für 5G in [9] spezifiziert und für die vorherigen Mobilfunkgenerationen in [22]. Bereits seit Release 6 wird es für UMTS unterstützt, für LTE seit Release 8, und die Unterstützung für GERAN wurde im Rahmen von Release 11 hinzugefügt.

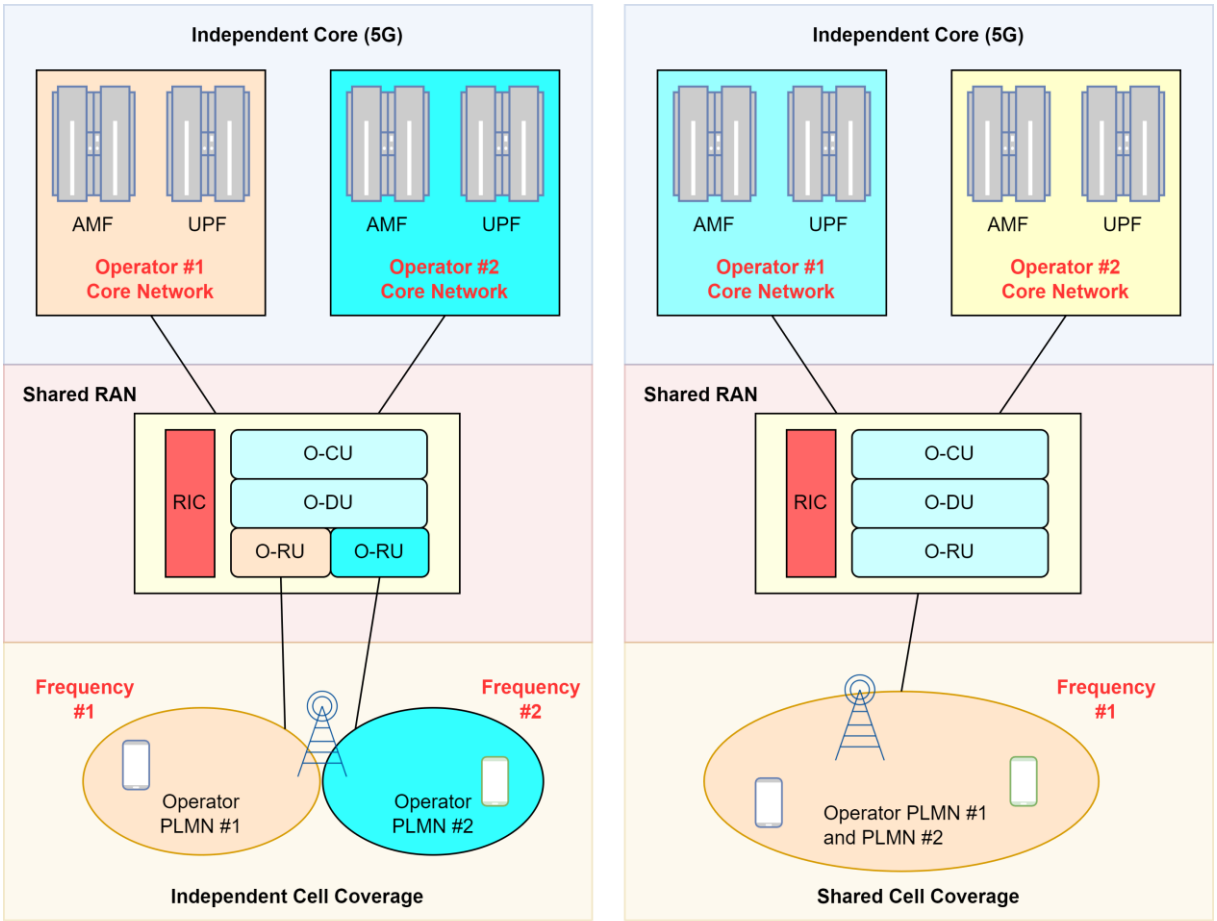

Abbildung 7: RAN-Sharing-Konzepte MORAN und MOCN (angelehnt an: Techplayon)

Bei beiden Ansätzen, MORAN und MOCN, können die Mobilfunkbetreiber wählen, ob sie die Übertragungsleitungen gemeinsam oder getrennt (in der gleichen physikalischen Verbindung) nutzen wollen.

2.2.5.2 Sharing-Konzepte bei O-RAN

Es existieren viele verschiedene Entwürfe für das Sharing der RAN-Komponenten O-RU, O-DU, O-CU und der Transportebenen Fronthaul, Midhaul und Backhaul. Entscheidend ist jeweils die Platzierung der einzelnen Elemente im RAN und die Realisierung in Hardware, VMs oder in der Cloud (s. Abbildung 8). Die O-RU ist immer am Antennenstandort (Radio Site) angesiedelt. Der Server und die Software für die O-DU können an einem eigenen Standort oder in einer Edge-Cloud (regionales Rechenzentrum oder Zentrale) gehostet werden. Der Server und die Software für die O-CU können gemeinsam mit der O-DU gehostet werden, entweder am Antennenstandort oder in einer Edge Cloud, oder von ihr getrennt in einem regionalen Cloud-Rechenzentrum.

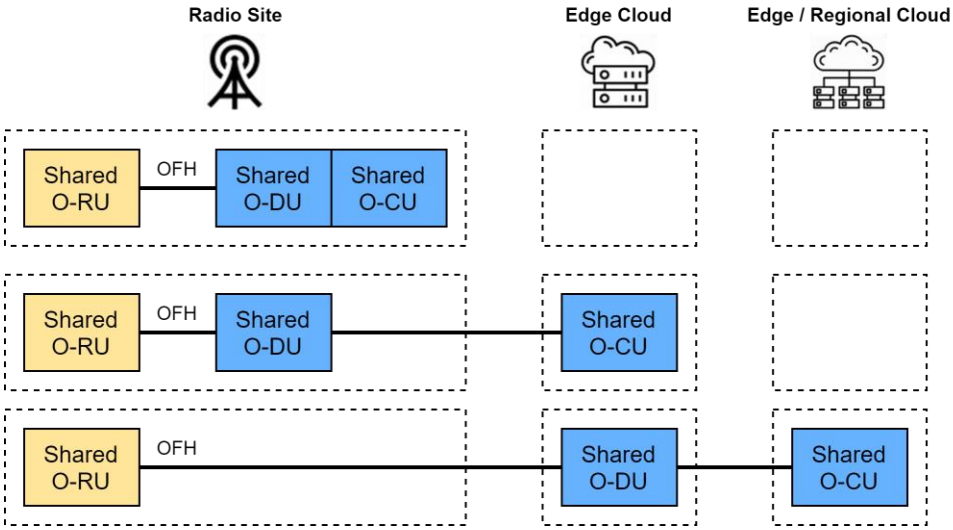

Abbildung 8: Grundlegende Aufteilungsmöglichkeiten beim RAN-Sharing von O-RU, O-CU und O-DU

Eine ausführliche Zusammenstellung möglicher Szenarien ist in dem Anforderungsdokument [23] zusammengestellt, das von Deutsche Telekom, Orange, Telefónica, TIM und Vodafone erstellt wurde. Die Abbildung 9 zeigt eine Auswahl von drei Szenarien daraus (Szenarien 9, 10 und 17 aus dem Anforderungsdokument). In Szenario 9 sind die virtualisierten RANs (CU und DU) verschiedener Hersteller auf an den Antennenstandorten bereitgestellten Recheninfrastrukturen gehostet (verteiltes vRAN auf geteilter Infrastruktur). In Szenario 10 sind die virtualisierten DUs an den Antennenstandorten verteilt, während die zugehörigen CUs auf verschiedenen Edge Clouds gehostet sind, die jeweils herstellereigene Recheninfrastrukturen sein können (verteilte DUs, zentralisierte CUs). Szenario 17 schließlich stellt ein typisches Indoor-Szenario dar, in dem ähnlich zu Szenario 9 die vRANs der Hersteller am Antennenstandort (oder einer Edge Cloud) gehostet sind. Die O-RUs werden über einen Multiplexer an die DUs angeschlossen.

Zwischen verschiedenen Netzbetreibern wird das Sharing der Infrastruktur gegenüber dem Sharing der O-RAN-Units bevorzugt. Das Sharing von Infrastruktur für VMs oder Cloud-Infrastruktur lässt sich momentan einfacher abstimmen als das gemeinsame Management der Units im O-RAN. Das Konfigurationsmanagement bei geteilten RANs ist zwischen den Betreibern noch nicht spezifiziert.

Für das Benutzererlebnis (User Experience) ist in der Regel der ausschlaggebende Faktor die RAN-Performance in Bezug auf Durchsatz, Latenz und Zuverlässigkeit. In Bezug auf RAN-Sharing ist daher das RAN-Network-Slicing ein kritischer Teil von Ende-zu-Ende-Network-Slices. Dagegen sind die Vorteile, dass über eine Slice-spezifische Ressourcenzuweisung, Scheduling und Admission Control eine differenzierte Verkehrsabwicklung und eine Isolierung von Teilnehmern oder Gruppen ermöglicht wird.

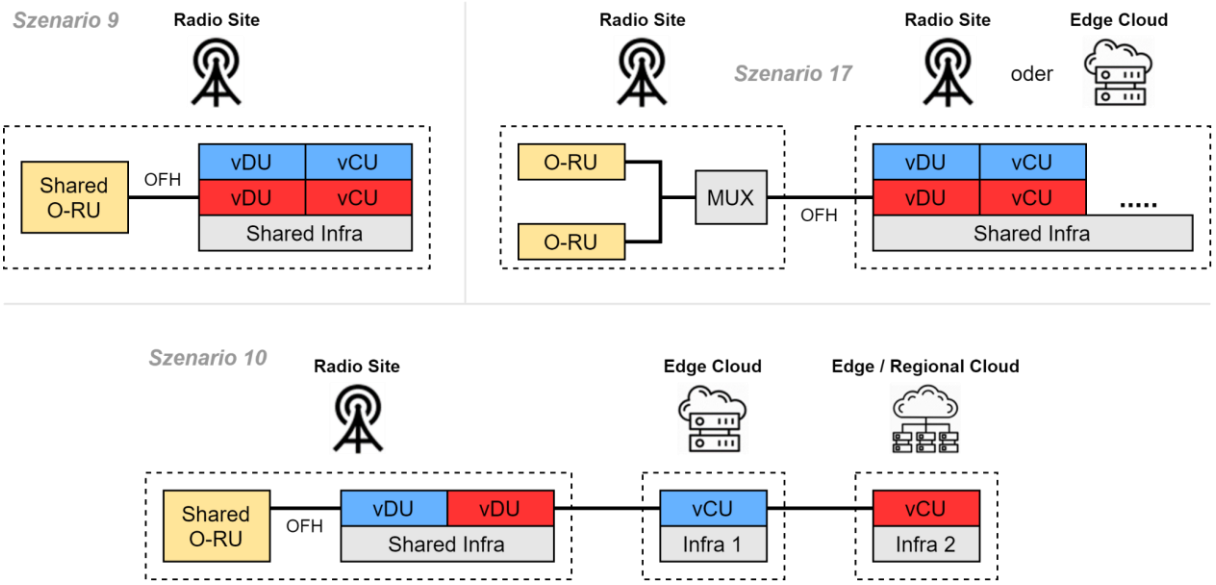

Abbildung 9: Auswahl von RAN-Sharing-Konzepten: Distributed vRAN / Shared Infra (Szenario 9), Distributed vDU, Centralized cVU (Szenario 10) und Multi-op Shared Infra (Indoor Szenario 17) [23]

2.3 Beschreibung von O-RAN-Schnittstellen

Im Folgenden werden die durch O-RAN definierten Schnittstellen näher erläutert. Abbildung 10 zeigt dazu die O-RAN-Architektur mit allen Schnittstellen ohne die Schnittstelle zur UE (vgl. Abbildung 5). Dagegen ist die Fronthaul-Referenzarchitektur mit Bezug auf die Spezifikation der O-RAN-CUS-Plane und -M-Plane um die kooperative Transportschnittstelle (engl. Cooperative Transport Interface, CTI) und um das Transportnetz erweitert. Zusätzlich sind die von außen einwirkenden Schnittstellen für Mensch-Maschine-Interaktionen, AI/ML, externe Zusatzinformationen und Software-Updates eingetragen.

2.3.1 O1-Schnittstelle

Die O1-Schnittstelle ist die Verbindung zwischen allen sog. „O-RAN Managed Elements (MEs)“ und den eigentlichen „Management Entities“ des SMO-Frameworks. Das Ziel ist es, den Betrieb und das Management (z.B. FCAPS MGMT, Software MGMT, File MGMT) der O-RAN-Komponenten über diese Schnittstelle sicherzustellen. Das heißt, die O1-Schnittstelle wird dafür verwendet, um das Management sämtlicher O-RAN-Komponenten, die orchestriert werden müssen, bzw. der dazugehörigen O-RAN-Netzwerkfunktionen zu ermöglichen. Zu den über O1 gemanagten Komponenten gehören im Fall von 5G NR der Near-RT RIC, die O-CU, die O-DU und im Fall von O-RAN-kompatiblen 4G/LTE-Netzen die O-eNB. Die O-CU entspricht dabei einer vorab definierten Zusammenfassung von O-CU-CP und O-CU-UP. Zur Veranschaulichung der O1-Schnittstelle und ihres Einflusses auf O-RAN-MEs ist sie in **Fehler! V erweisquelle konnte nicht gefunden werden.**, unter Einbezug der ME O-eNB, aus der logischen Architektur von O-RAN isoliert dargestellt. Für die O-RU stehen die Arbeiten derzeit im Stadium der Untersuchung. Aus diesem Grund ist die Schnittstellenverbindung gestrichelt dargestellt.

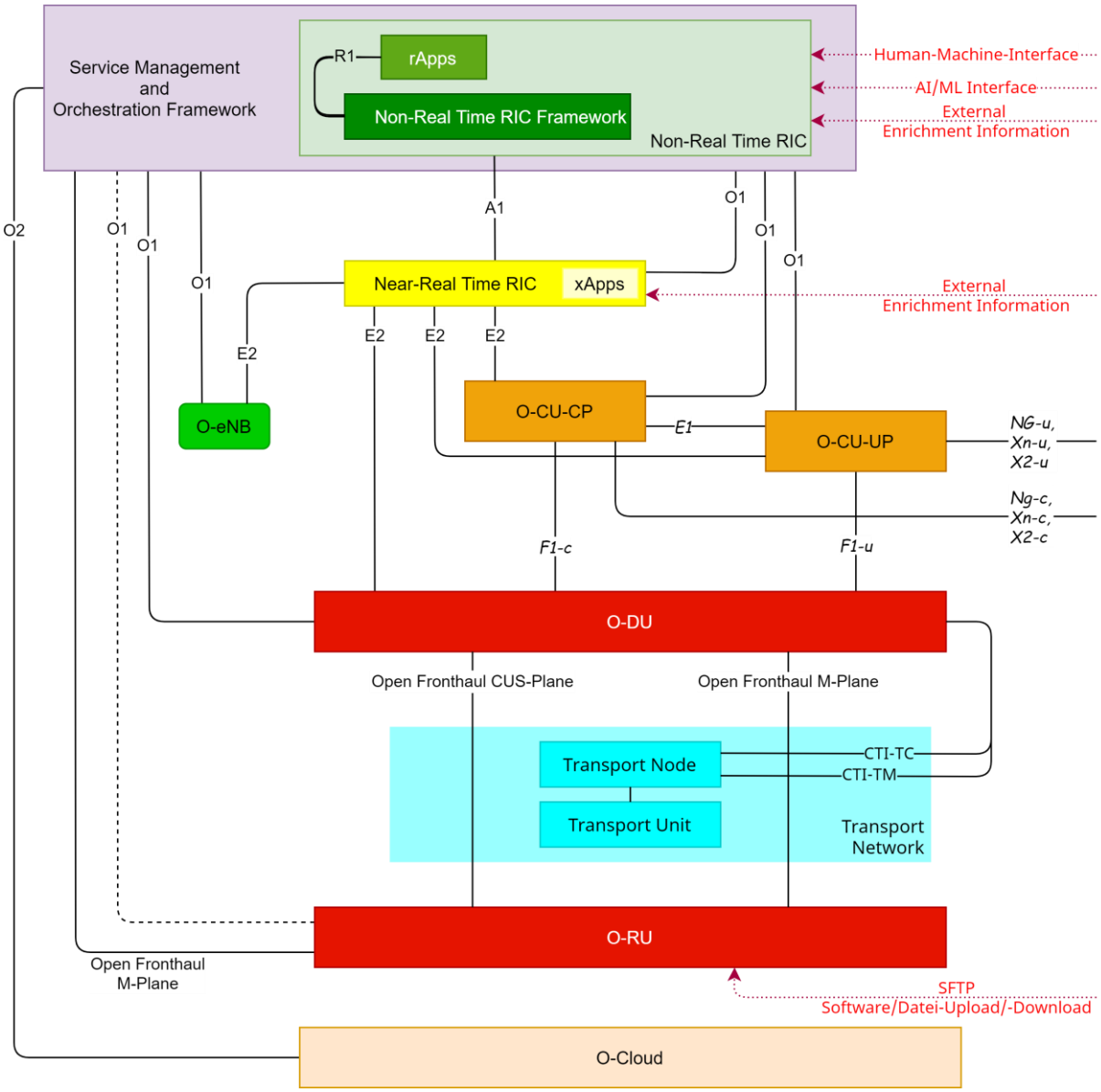

Abbildung 10: O-RAN-Schnittstellen

O1 ermöglicht dem SMO-Framework Zugriff auf die O-RAN-Netzwerkfunktionen. Dabei wird ein Netzwerkmanagement nach dem FCAPS-Modell unterstützt. FCAPS entspricht dabei dem ISO-Modell für Netzwerkmanagement, welches die fünf Aufgabenbereiche Fault-, Configuration-, Accounting-, Performance- und Security-Management beschreibt und umfasst. Der O1-Schnittstelle kommt damit eine zentrale Rolle in der O-RAN-Gesamtarchitektur und dem Netzwerkbetrieb zu. O1 unterstützt typische FCAPS- wie auch andere Management-Funktionen, wozu bspw. folgende Funktionen gehören [24]:

- Discovery bzw. Registrierung,
- Konfiguration in Bezug auf die Adressierung,
- Versionsverwaltung,
- Komponentenüberwachung (Monitoring).

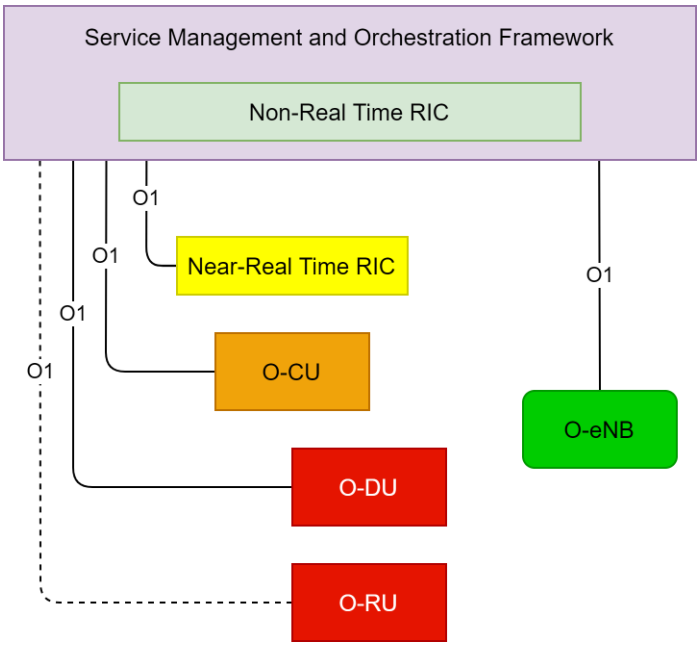

Abbildung 11: Netzmanagement und Betrieb: O1-Schnittstelle als Verbindung zwischen SMO und den O-RAN Managed Elements (ME) unter Berücksichtigung des ME O-eNB bei O-RAN-kompatiblen 4G/LTE-RAN-Komponenten (Ref. [14])

Zudem können im Detail folgende Management Services (MnS) über die O1-Schnittstelle unterstützt werden (siehe auch [18], [25]):

- Services für das Bereitstellungsmanagement (Provisioning)
  - Allgemeine NETCONF-Anforderungen
  - Erstellen, Modifizieren und Löschen von MOIs (Managed Object Instances)
  - Lesen von MOI-Attributen
  - Benachrichtigen über Änderungen von MOI-Attributwerten
  - Subscription-Kontrolle
- Services für das Fault Supervision Management
  - Fehlerbenachrichtigung
  - Fehlerüberwachungssteuerung
- Services für das Performance Assurance Management
  - File Reporting und Streaming von Performance-Daten
  - O-RAN-definierte Leistungsmessungen und Steuerung von Messaufträgen
- Services für das Trace Management
  - Anruf-Trace und Streaming-Trace
  - Minimierung von Drive-Tests (MDT)
  - Radio Link Failure (RLF) und RRC-Verbindungsaufbaufehler (RCEF)
  - Trace-Steuerung
- Services für das Datei-Management
  - Dateibereitschaftsbenachrichtigung
  - Liste verfügbarer Dateien und Datei-Download
  - Bidirektionale Übertragung von Dateien (bspw. Konfigurationsdateien für Beamforming, Zertifikate, ML-Dateien) zwischen Client (File Management MnS Consumer) und File-Server (File Management MnS Provider)
- Kommunikationsüberwachung (Communication Surveillance)
- Services für das Heartbeat Management
  - Heartbeat-Benachrichtigung
  - Heartbeat-Kontrolle
- Startup- und Registrierungsmanagement für Physical Network Functions (PNFs)

    - PNF-Plug-n-Play
    - PNF-Registrierung
- Services für das (PNF) Software Management
    - Benennung und Inhalt von Software-Paketen
    - Software-Download, Pre-Check und Aktivierung von Software
- Instanziieren sowie Beenden einer virtualisierten Netzwerkfunktion (VNF)
- Services für das Skalierungs-Management von VNFs

Die Management-Funktionalitäten werden durch die Verwendung von Standard-Protokollen (z.B. SSH, TLS, NETCONF) und Datenmodellen (z.B. YANG) realisiert. So kann das SMO-Framework bspw. mit Hilfe des Provisioning Management Service über die O1-Schnittstelle Informationen (Updates), z.B. zur aktuellen Ressourcennutzung, aus den MEs erhalten und im Gegenzug eine optimierte Konfiguration der MEs veranlassen.
In O-RAN-basierten Mobilfunknetzen, die KI/ML-Ansätze unterstützen, wird die O1-Schnittstelle dafür verwendet, um die (Trainings-)Daten, die für ML-Zwecke genutzt werden können, von den MEs O-DU und O-CU einzusammeln. Der sich im SMO befindende (und ML-basiert lernende) Non-RT RIC kann Policies bereithalten, die bei der Optimierung auf Zellebene zu berücksichtigen sind, indem er über die O1-Schnittstelle (zeitlich variable) optimale Konfigurationsvorgaben für Zellparameter bereitstellt.
Die O-RAN-Architektur erlaubt das Erheben, den Zugriff auf und die Verwaltung von Datenverläufen (Historie) in Bezug auf den im RAN transferierten Verkehr, das gewählte Routing sowie die durchgeführten Handover-Vorgänge. Die Daten werden dafür über die O1-Schnittstelle übertragen.
Im Fall von RAN-Sharing, bei dem bspw. ein externer Operator mittels virtueller RAN-Funktionen (VNF) als „Gast-Operator“ auf die RAN-Infrastruktur und Rechenressourcen des eigentlichen Netzbetreibers (Home-Operator) Zugriff bekommt, müssen Optionen zur Fernsteuerung (Remote Control) und Fernkonfiguration (Remote Configuration) dieser VNFs ermöglicht werden. In solch einem Szenario können ebenfalls „Remote-Schnittstellen“ (O1, O2) eingeführt werden, um dem Gast-Operator die Möglichkeit zu geben, die gewünschte Konfiguration für die jeweilige VNF am Standort des Home-Operators zu übermitteln. Die VNFs stellen dabei jeweils eine logische Implementierung der O-CU- und O-DU-Funktionaltäten dar. Die O-RAN-Architektur kann eine Reihe von offenen Schnittstellen als Remote-Interfaces, so auch für O1, zur Verfügung stellen, um die Performancewerte von Remote-Nutzern überwachen zu können. Dies ermöglicht verschiedene Optimierungsstrategien in Bezug auf die Funkressourcenzuteilung als auch die QoS-Parameter-Anpassung.
Aktuell gibt es in der O-RAN-Standardisierung ein Joint Work Item (JWI) zwischen den Working Groups WG1 und WG4, um festzulegen, wie genau O-RU-Komponenten Management Services im RAN über die O1-Schnittstelle unterstützen können. Die Entscheidungen des JWI werden in zukünftige Revisionen und Updates der O1-Schnittstellenspezifikation eingearbeitet.

2.3.2 O2-Schnittstelle

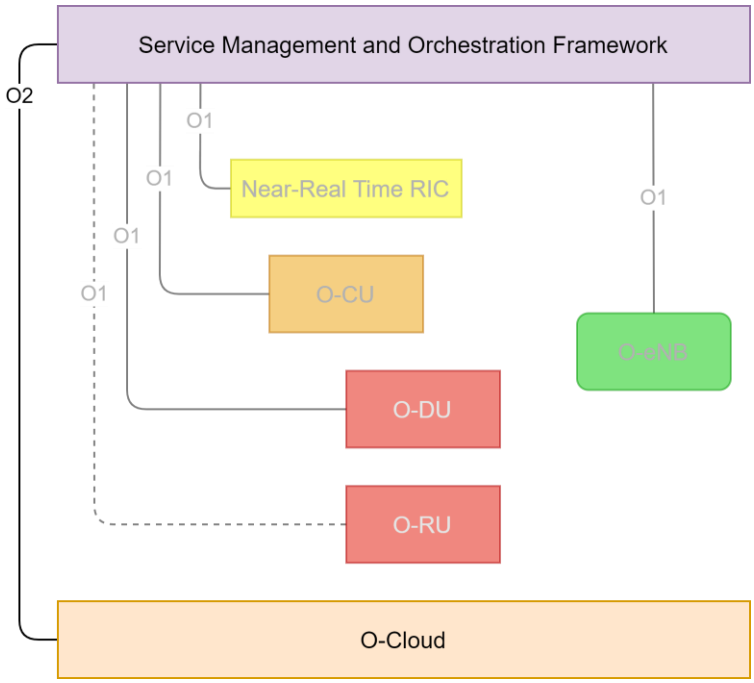

Abbildung 12: Management und Betrieb der O-Cloud-Plattform durch das SMO-Framework und Einfluss der O-Cloud auf den Netzbetrieb: O2-Schnittstelle als Verbindung zwischen SMO-Framework und der O-Cloud-Plattform unter Berücksichtigung des ME O-eNB bei O-RAN-kompatiblen 4G/LTE-RAN-Komponenten (Ref. [14])

Die O2-Schnittstelle ist eine offene, logische Schnittstelle innerhalb der O-RAN-Architektur und wird wie die O1-Schnittstelle als ein Instrument für die Ausführung von Open Management & Orchestration Services genutzt. Ihr Zweck ist die Sicherstellung einer sicheren Kommunikation zwischen dem SMO-Framework und der O-Cloud-Plattform. Die O-Cloud-Plattform kann, abhängig vom jeweils innerhalb einer O-Cloud-Instanz gewählten Deployment-Szenario, verschiedene Netzfunktionen (engl. Network Function, NF) virtualisieren und damit RAN-Funktionen innerhalb der Gesamtarchitektur übernehmen. Das SMO-Framework bietet die Möglichkeit, eine Vielzahl von O-Cloud-Instanzen parallel zu verwalten und bei der Orchestration von verfügbaren Plattform- und Anwendungselementen/-ressourcen sowie das Management von Workflow und Workload zu unterstützen. Zur Umsetzung dieser SMO-Aufgaben wird die O2-Schnittstelle benötigt und genutzt, d.h. sie ermöglicht ein zentrales Management der Cloud-Infrastruktur und der Cloud-Ressourcen-Nutzung durch das RAN und darüber hinaus ein „Deployment Life Cycle Management“ für die in der O-Cloud ausgeführten virtualisierten Netzfunktionen (Virtual NFs, VNFs). So sollen über O2 die VNFs, die virtuellen Maschinen (Virtual Machines, VMs) und Container-Instanzen verwaltet werden können. Allerdings sind derzeit die Abhängigkeiten von den Cloud-Instanziierungen und den dort auszuführenden Softwareanwendungen (Apps) im Standard nicht vollständig spezifiziert. Die in der WG 6 „The Cloudification and Orchestration Workgroup“ erfolgende Spezifikation der O2-Schnittstelle ist erst in den Grundzügen vorhanden (siehe [26]).
Zur Veranschaulichung der O2-Schnittstelle und ihres Einflusses auf die O-Cloud ist sie in Abbildung 12, unter Einbezug der über die O1-Schnittstelle gemanagten MEs (inklusive der O-eNB), hervorgehoben.
Netzbetreiber können über die O-Cloud-Plattform Zugang zum Netzwerk bekommen und das RAN mit Hilfe der Schnittstellen O2 sowie O1 betreiben wie auch warten. Dabei können bspw. Systemupdates und -upgrades gehandhabt und Netzelemente/MEs (re-)konfiguriert werden.
Die O-Cloud-Plattform bietet dem SMO-Framework über die O2-Schnittstelle verschiedene Dienste bzw. Funktionen an. Die O-RAN-Architekturbeschreibung in [14] definiert in der aktuellen Version folgende exemplarische Funktionen, die über O2 abgebildet werden sollen,

und zeigt an, dass der Umfang der Funktionen jedoch nicht auf die aufgeführten beschränkt sein muss. In Bezug auf die O-Cloud-Infrastruktur sind diese Funktionen:

- Ermittlung (Discovery) und Administrierung der infrastrukturellen Cloud-Ressourcen,
- Positive Skalierung (Scale-in) sowie negative Skalierung (Scale-out) der O-Cloud,
- FCAPS-Management (insbesondere Performance, Configuration und Fault Management sowie Kommunikationsüberwachung) der O-Cloud,
- Software Management für die O-Cloud-Plattforminfrastruktur.

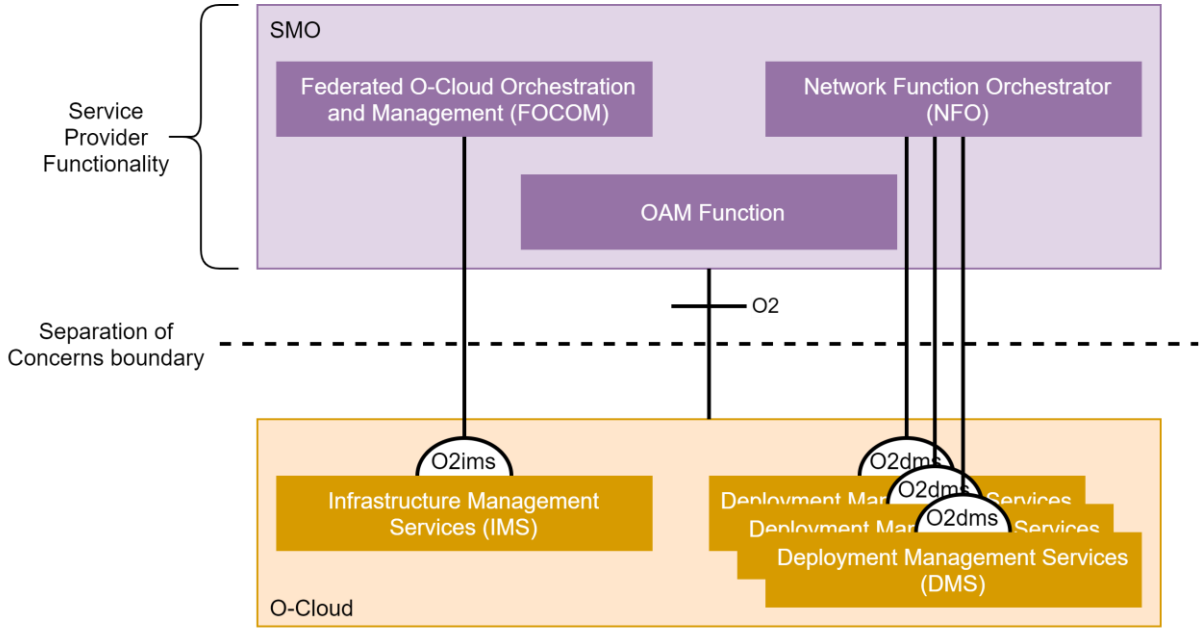

Abbildung 13: Aufteilung der O2-Schnittstelle in Service Bases Interfaces (Ref. [26])

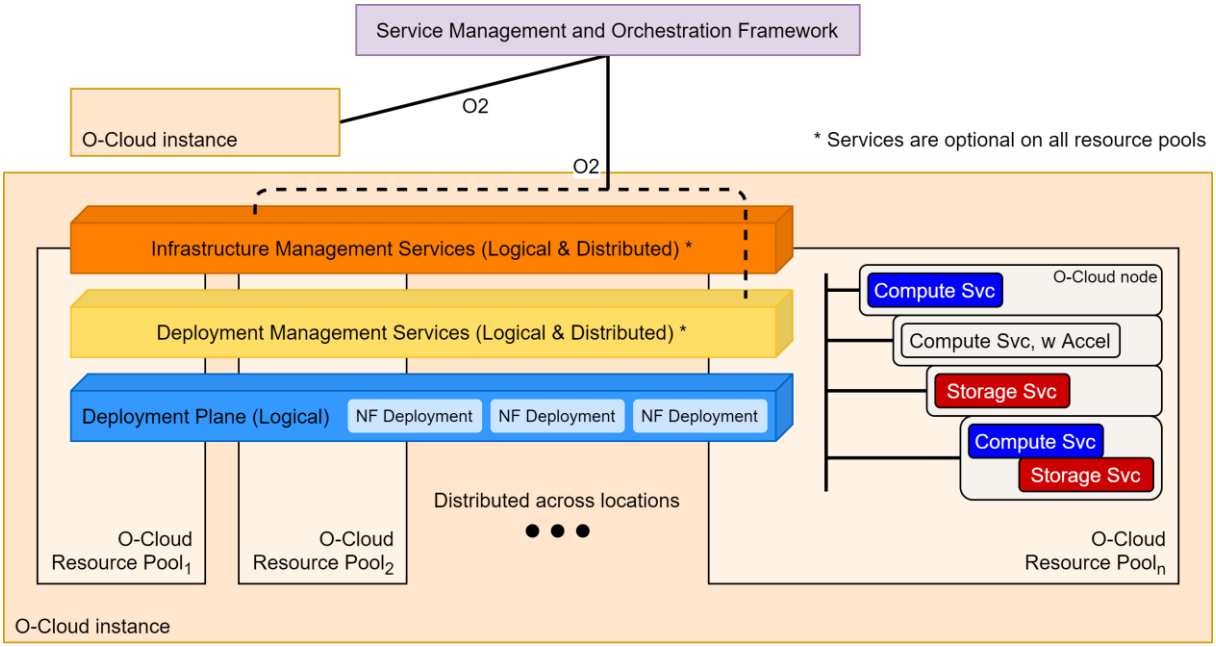

Abbildung 14: Zusammenspiel zwischen SMO-Framework und O-Cloud-Instanzen sowie Übersicht zu den O-Cloud-Kernkomponenten (Ref. [27])

In Bezug zu den Softwareumsetzungen (Deployments) auf der O-Cloud-Infrastruktur sind diese Funktionen:

- Einrichten und Löschen von Deployments sowie der jeweils zugeordneten O-Cloud-Ressourcen,

- FCAPS-Management (insbesondere Performance und Fault Management) für Deployments sowie der jeweils zugeordneten O-Cloud-Ressourcen,
- Scale-in/Scale-out der Deployments und der zugeordneten O-Cloud-Ressourcen,
- Software Management für die Deployments.

Zudem sendet die O-Cloud-Plattform Alarmbenachrichtigungen über die O2-Schnittstelle an das SMO-Framework, wenn bei der O-Cloud-Ressourcen-Nutzung Probleme oder Veränderungen identifiziert werden. Zusätzlich soll O2 das Management von Komponenten zur Hardware-Beschleunigung in der O-Cloud-Plattform ermöglichen.
Die Aufzählung oben zeigt bereits, dass sich die O2-Funktionen zu zwei logischen Gruppen von Diensten zuordnen lassen, die zum einen die O-Cloud-Infrastruktur allein und zum anderen die Softwareumsetzungen (Deployments) auf dieser adressieren:

(1) Infrastructure Management Services (IMS) und
(2) Deployment Management Services (DMS).

Für IMS bietet die O2-Schnittstelle Funktionen, welche für die Bereitstellung und das Management von Cloud-Infrastrukturressourcen verantwortlich sind. Für DMS hingegen stellt die O2-Schnittstelle einen Satz an Schnittstellenfunktionen bereit, der für das Management der Virtualisierungsumgebungen („virtualized/containerized Deployments“) auf der Infrastruktur der O-Cloud verantwortlich ist. O2 unterteilt sich daher in zwei Service Based Interfaces (SBIs) zwischen dem SMO-Framework und der O-Cloud-Plattform, welche jeweils einen eigenen Funktionssatz umfassen. Abbildung 13 veranschaulicht diese Aufteilung. [26]
Abbildung 14 dient dafür, die vorangehend erklärten Zusammenhänge und Funktionen in Bezug auf die O2-Schnittstelle im Zusammenspiel mit den relevanten Komponenten des RANs und der O-Cloud-Architektur besser verstehen zu können. Der Überblick zeigt zum einen die Kernkomponenten einer O-Cloud-Instanz und zum anderen das Zusammenspiel zwischen dem SMO-Framework und den O-Cloud-Instanzen. Dieses Zusammenspiel erfolgt unter Nutzung der O2-Schnittstelle und den O2-Management-Services IMS und DMS.
Abschließend ist darauf hinzuweisen, dass die O2-Dienste und die dafür erforderlichen assoziierten Schnittstellen aktuell erst noch spezifiziert werden. Die Verfassung und Veröffentlichung einer dedizierten O2-Spezifikation ist in der Planung.

2.3.3 A1-Schnittstelle

Die A1-Schnittstelle wird in der O-RAN Working Group 2 spezifiziert [28]. Sie dient der Kommunikation zwischen dem Non-RT RIC und dem Near-RT RIC. Zur Veranschaulichung der A1-Schnittstelle und ihres Einflusses auf die Funktionen außerhalb der RICs zeigt Abbildung 15 den für diesen Abschnitt relevanten Auszug aus der O-RAN-Architektur.

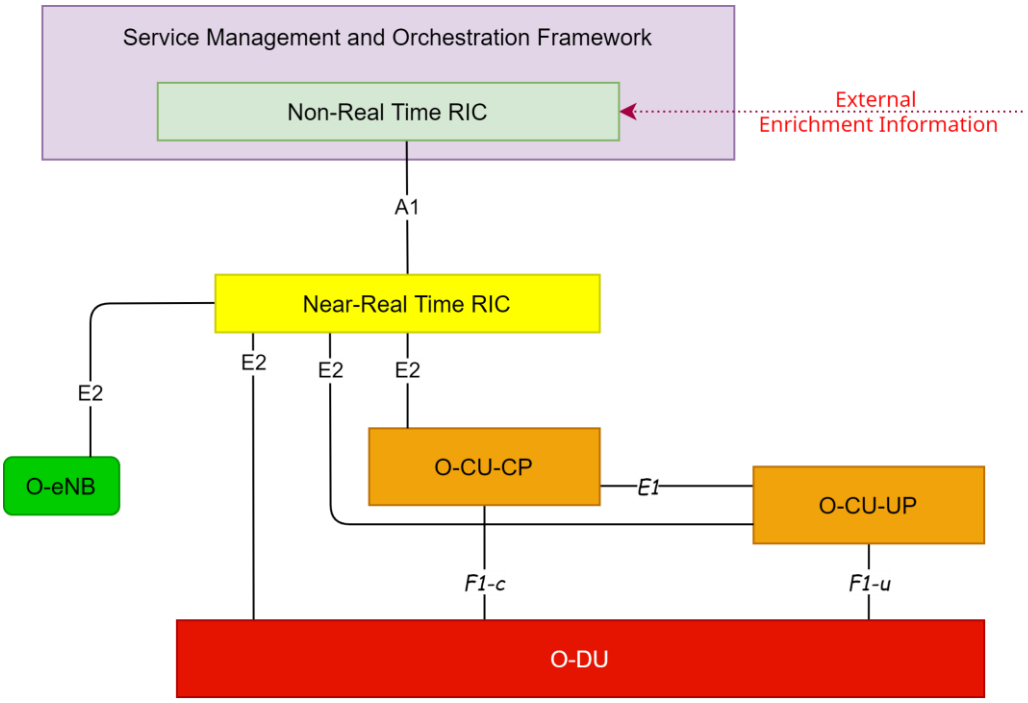

Abbildung 15: Auszug aus der O-RAN-Architektur: die A1-Schnittstelle als Verbindung zwischen Non-RT RIC und Near-RT RIC unter Berücksichtigung der Auswirkungen auf weitere Funktionen (Ref. [14])

Der Non-RT RIC übermittelt die im SMO-Framework erfassten Informationen aus diversen internen und externen O-RAN-Quellen über die A1-Schnittstelle an den Near-RT-RIC. Diese Informationen sind:

- Policy-basierte Richtlinien in deklarativer Form (A1-Policy), die Aussagen über Ziele und Ressourcen für UEs und Zellen enthalten.
- Informationen über das ML-Modellmanagement (Training, Aktualisierung, Deployment von ML-Modellen).
- A1 Enrichment Information (Anreicherungsinformationen) aus internen oder externen O-RAN-Datenquellen, wobei deren Verfügbarkeit oder Nutzung nicht entscheidend für die Aufgabenerfüllung einer Einheit ist, sondern ausschließlich für ihre Verbesserung.

Der Near-RT RIC soll diese Informationen verwenden, um die Konfiguration der E2-Knoten über die E2-Schnittstelle zu vollziehen. Auf diese Weise soll das RAN unter definierten Bedingungen optimiert werden können (z. B. das RRM).
Die deklarative Form der A1-Policies hat zur Folge, dass die konkrete Umsetzung in dem Near-RT RIC erfolgen muss. Die A1-Policies sind bis zur Veränderung oder Löschung durch den Non-RT RIC gültig. Der Near-RT RIC hat die Aufgabe, den Non-RT RIC über den Status der Durchsetzung einer A1-Policy als Feedback über die A1-Schnittstelle zu unterrichten. Dabei ist zu erwähnen, dass die A1-Policies im Falle eines Neustarts des Near-RT RICs dort nicht gesichert sind. Daher ist die Aufgabe des Non-RT RICs, die Präsenz von A1-Policies zu überprüfen.
Ist eine A1-Policy auf ein UE (oder eine Gruppe von UEs) bezogen, so wird die UE durch die Kennung UE Id identifiziert. Die UE Id soll über die dem RAN bekannte RAN UE Id, die für die E1-Schnittstelle [6] bzw. für die F1-Schnittstelle [7] definiert ist, gebildet werden. Das Ziel ist die Identifizierung der mit einer UE verbundenen Messungen, um Korrelationen von O1-PM-Daten mit den Zielen eines Service zu berechnen (z.B. bei Beschwerden über den Service) und die Erfüllung von Policies zu bewerten. Es werden weder Hardware-Ausrüstung noch Benutzerdaten identifiziert.
Die A1 Enrichment Information kann über die A1-Schnittstelle gesucht, beantragt und übermittelt werden. Bei der Bereitstellung von Daten aus externen Quellen wird der Non-RT

RIC für die Authentifizierung der Quelle und die Sicherheit der Verbindung zuständig sein. Aktuell ist weder geklärt, wie die Verbindungen zu den externen Quellen gehandhabt werden soll, noch ist die Suche nach und die Bereitstellung von externen Daten definiert.
Für die Unterscheidung von Enrichment Information definiert der Standard die Verwendung von Enrichment Information Types (EI Types). Allerdings existieren bisher außer dem generischen Begriff keine Definitionen von spezifischen Typen.

2.3.4 R1-Schnittstelle

Die R1-Schnittstelle wird in der O-RAN Working Group 2 in Verbindung mit dem Non-RT RIC spezifiziert [29]. Sie ist die im Non-RT RIC definierte Verbindung zwischen den inhärenten Framework-Funktionen und den im Non-RT RIC laufenden Applikationen (rApps). Abbildung 16 zeigt die R1-Schnittstelle über die Darstellung der Funktionen des Non-RT RICs. Die Funktionen im Framework des Non-RT RICs umfassen das Management von rApps, die Unterstützung der rApps über Zugangsdienste (R1 Service Exposure Function), Funktionen für die A1-Schnittstelle, AI-/ML-Workflow, und andere Funktionen des Non-RT RICs, sofern vorhanden. Vermutlich durch die interne Verwendung als API für die rApps lautet eine andere Bezeichnung für die R1-Schnittstelle „Open APIs for rApps“.
Die rApps sind dazu gedacht, die über die R1-Schnittstelle offengelegten Funktionalitäten des Non-RT RICs zu nutzen, um damit einen Mehrwert für den Betrieb und die Optimierung des RANs zu bieten. Dazu zählen:

- Bereitstellung von Policy-basierten Richtlinien und Enrichment Information über die A1-Schnittstelle,
- Durchführung von Datenanalysen, KI/ML-Training und Informationsgewinnung für die RAN-Optimierung oder für die Nutzung durch andere rApps,
- Empfehlung von Konfigurationen, die über die O1-Schnittstelle verschickt werden können.

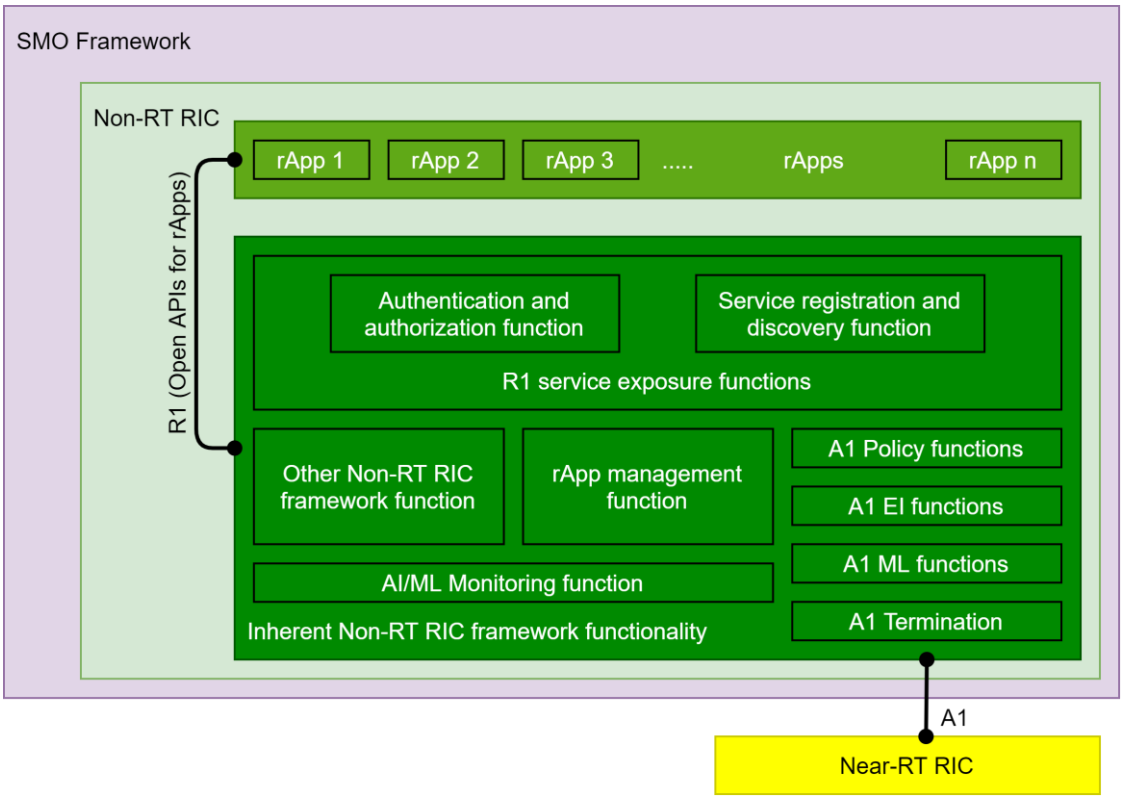

Abbildung 16: Illustration der R1-Schnittstelle über das funktionale Diagramm der Non-RT RIC-Architektur (Ref. [29])

Als Bestandteil des SMO-Frameworks hat der Non-RT RIC auch Zugriff auf deren Funktionen. Dies schließt die Beeinflussung der Informationen ein, die über die O1-Schnittstelle übertragen werden. Der Non-RT RIC benötigt diesen Zugriff für die Optimierung der RAN-Ressourcen. Allerdings impliziert die aktuelle O-RAN-Definition lediglich, dass der Non-RT RIC nur zu diesem Zweck auf die SMO-Rahmenfunktionalität zugreifen darf. Dementsprechend sollte der Non-RT RIC die Übertragung über die O2-Schnittstelle nur beeinflussen dürfen, wenn die O-Cloud als RAN-Ressource betrachtet wird.

2.3.5 E2-Schnittstelle

Die E2-Schnittstelle wird in der O-RAN Working Group 3 spezifiziert [30] und verbindet den Near-RT RIC mit den sogenannten E2-Knoten (E2 Nodes). Dabei handelt es sich um einen Sammelbegriff für alle Einheiten, die an der Südseite der E2-Schnittstelle angebunden sind, nämlich O-CU-CP, O-CU-UP und O-DU im Falle von 5G NR und O-eNB im Falle von 4G/LTE (s. Abbildung 17). Dementsprechend sollen die E2-Knoten alle Protokollschichten und Schnittstellen unterstützen, die in 3GPP-Funkzugangsnetzen definiert sind, einschließlich eNB für LTE/E-UTRAN [17] und gNB/ng-eNB für NR/NG-RAN [19].
Der Near-RT RIC wird über die E2-Schnittstelle mit einem oder mehreren E2-Knoten verbunden, d. h im Falle von NR mit einem oder mehreren O-CU-CPs, einem oder mehreren O-CU-UPs und einem oder mehreren O-DUs. Entsprechend verbindet sie im Falle von LTE den Near-RT RIC mit einem oder mehreren O-eNBs. Während ein Near-RT RIC also eine Eins-zu-Viele Beziehung zu seinen Einheiten hat, ist umgekehrt nur eine Eins-zu-Eins Beziehung möglich. Jedes O-CU-CP, O-CU-UP, O-DU und O-eNB kann jeweils nur mit einem Near-RT RIC verbunden sein, so wie auch ein Near-RT RIC nur mit einem Non-RT RIC verbunden sein kann.

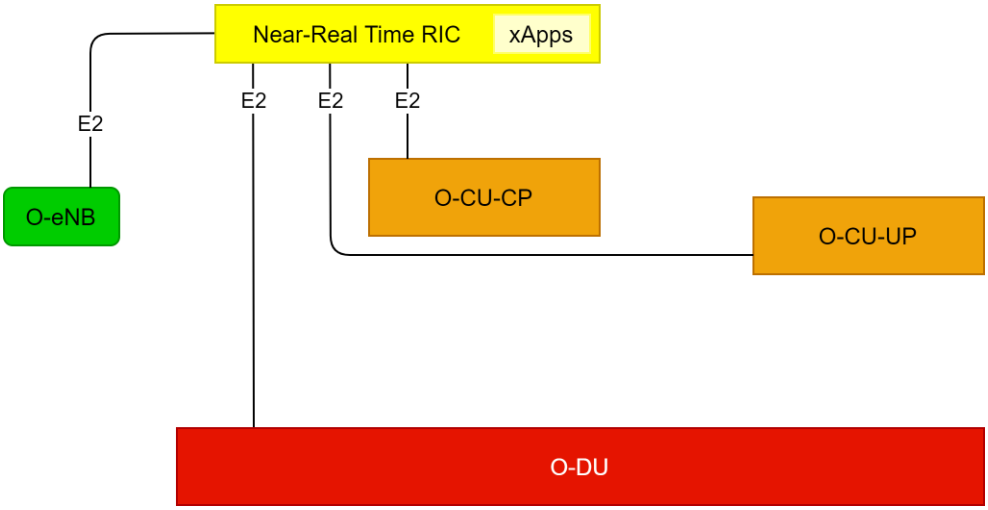

Abbildung 17: Auszug aus der O-RAN-Architektur: die E2-Schnittstelle als Verbindung zwischen dem Near-RT RIC und den als E2-Knoten bezeichneten RAN-Funktionen (Ref. [14])

Als kritische Schnittstelle zwischen den von der 3GPP standardisierten Funkknoten und den von O-RAN spezifizierten Funktionen besteht der in der Spezifikation vertretene allgemeine Grundsatz, dass diese E2-Schnittstelle offen sein muss. Das ist eine wesentliche Voraussetzung für die Realisierung der Interoperabilität. Ein wichtiger Test bzgl. der Unterstützung von O-RAN wird sein, inwiefern die E2-Schnittstelle von den RAN-Ausrüstern unterstützt wird [4].
Ein weiterer allgemeiner Grundsatz in der O-RAN-Spezifikation lautet, dass die Funktionen des Near-RT RICs und der E2-Knoten vollständig von den Transportfunktionen getrennt sind. Das im Near-RT RIC und den E2-Knoten verwendete Adressierungsschema darf nicht an die Adressierungsschemata der Transportfunktionen gebunden sein. Weiterhin basieren die

Protokolle der E2-Schnittstelle ausschließlich auf Protokollen der Steuerungsebene (Control Plane). Ein Zugriff auf die User Plane in irgendeiner Form ist nicht Bestandteil der Spezifikation. Das Ziel besteht in der Steuerung und Optimierung der E2-Knoten und der von ihnen verwendeten Ressourcen. Die xApps, die in dem Near-RT RIC gehostet sind, nutzen die E2-Schnittstelle, um Informationen in Echtzeit zu sammeln (z.B. auf UE-Basis oder Funkzellbasis), um wie die rApps Mehrwertdienste bereitzustellen. Zu diesen Zwecken werden die RIC-Dienste REPORT, INSERT, CONTROL und POLICY vom Near-RT RIC eingesetzt, um Mess-Reports anhand bestimmter Trigger-Events anzufordern oder neue Policies an bestimmte E2-Knoten zu senden.
Durch die Eins-zu-Viele Beziehung zwischen Near-RT RIC und den E2-Knoten muss die E2-Schnittstelle die Fehlerbehandlung bei Ausfällen und eine verbesserte Ausfallsicherheit unterstützen. Bei einem Ausfall der E2-Schnittstelle oder des Near-RT RICs soll ein E2-Knoten in der Lage sein, seine Funktion unabhängig zu erfüllen. Allerdings kann es zu Ausfällen bei bestimmten Mehrwertdiensten kommen, die nur über den Near-RT RIC bereitgestellt werden können, z.B. wenn eine Ressourcenoptimierung auf einer O-CU stattfindet, die durch xApps berechnet werden und diese Berechnungen auf der Grundlage von regelmäßig über E2 mitgeteilten Messdaten basieren. Ein solcher Kreislauf kann in einer Ausfallsituation nicht weitergeführt werden.

2.3.6 Open FH CUS-Schnittstelle

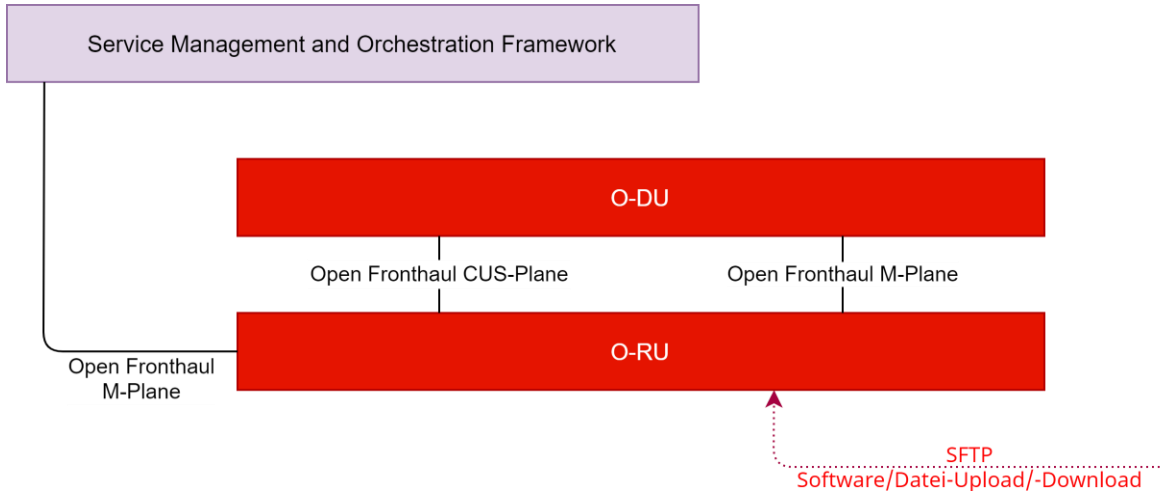

Abbildung 18: Auszug aus der O-RAN-Architektur: die Open Fronthaul-Schnittstelle als Verbindung zwischen den Funktionen O-DU und O-RU bzw. SMO und O-RU (Ref. [14])

Das Open Fronthaul Interface verbindet die Funktionen O-DU und O-RU bzw. im hybriden Modell zusätzlich das SMO-Framework mit der O-RU. Das Open Fronthaul umfasst die CUS-Plane (Control, User und Synchronization) sowie die M-Plane (Management). Die M-Plane mit ihrem Bezug zur Open FH M-Plane-Schnittstelle wird in Abschnitt 2.3.7 erläutert. Abbildung 18 zeigt den Auszug aus der O-RAN-Architektur mit den für das Open Fronthaul relevanten Funktionen und Schnittstellen.
Die Schnittstellen für die C-, U- und S-Planes sind in der Spezifikation [31] beschrieben. Über diese werden die User- und Control-Plane-Daten der Uu-Schnittstelle übertragen. Weiterhin erfolgt darüber die Zeitsynchronisation.

2.3.6.1 C-Plane (Control Plane)

Über die Control Plane werden Nachrichten ausgetauscht, die die Prozessierung von User-Daten bestimmen. Dazu zählen:

1. Informationen zum Scheduling oder zum Beamforming, falls diese Konfiguration nicht über die M-Plane (siehe Abschnitt 2.3.7) ausgetauscht wird. Diese Nachrichten werden getrennt für Uplink und Downlink übertragen.
2. UL- und DL-spezifischen Informationen zur verwendeten Numerologie, d.h. Slot- und Subcarrier-Definitionen.
3. Im Fall, dass das Precoding in der O-RU durchgeführt wird, werden die Konfigurationsdaten von der O-DU übertragen.
4. Informationen für Funktionen wie Dynamic Spectrum Sharing (DSS).

Auf der C-Plane werden entweder eCPRI- oder IEEE 1914.3-Protokolle genutzt.

2.3.6.2 U-Plane (User Plane)

Über die User Plane (auch als Data Plane bezeichnet) werden Nachrichten übertragen, die die eigentlichen Nutzdaten beinhalten. Der Schwerpunkt liegt hier auf einer effizienten Übertragung, insbesondere unter den hohen Anforderungen durch Latenz in den verschiedenen 5G-Numerologien. Die wichtigsten bereitgestellten Funktionen sind:

1. I/Q-Datenübertragung der Nutzdaten, wobei jedes Symbol in einer U-Plane-Nachricht übertragen wird.
2. Datenkompression, wobei verschiedene Methoden pro Physical Resource Block (PRB) definiert sein können, welche in zugehörigen Control Messages angegeben werden.
3. Downlink Data Precoding.

Es ist anzumerken, dass die I/Q-Datenübertragung auch ohne die C-Plane möglich ist (z.B. über den Packet Random Access Channel, PRACH). In dem Fall muss die entsprechende Konfiguration über die M-Plane erfolgen.
Die unterstützten Methoden zur Kompression variieren zwischen O-RU und O-DU. Es ist anzunehmen, dass verschiedene O-RUs nur eine Methode implementieren, um die Komplexität gering zu halten. Dementsprechend muss die O-DU mehrere Methoden implementieren, um mit verschiedenen O-RU-Herstellern interoperabel zu sein.
Auf der U-Plane werden, wie auf der C-Plane, entweder eCPRI- oder IEEE 1914.3-Protokolle genutzt.

2.3.6.3 S-Plane (Synchronization Plane):

Die Synchronisationsanforderungen zwischen O-DU und O-RU sind ein wesentlicher und kritischer Teil für die Umsetzung des TDD-Betriebs sowie von mMIMO oder der Carrier Aggregation über mehrere O-RUs. Über die S-Plane kann eine Synchronisation über Frequenz, Phase oder Zeit erfolgen, wobei verschiedene Topologien zum Austausch von Synchronisationsinformationen möglich sind, z.B.:

- Netzwerk als Master für die O-RU,
- O-DU als Master für die O-RU oder
- O-RU mit lokalem GNSS-Receiver als Master.

Protokolle wie PTP und SyncE werden entsprechend der O-RAN-Fronthaul-Spezifikation genutzt. Bei Verlust der Synchronisation durch die O-DU werden alle HF-Verbindungen der verbundenen O-RUs beendet (‚FREERUN State').

2.3.7 Open FH M-Plane-Schnittstelle

Entsprechend der Spezifikation [32] stellt die M-Plane der Komponente O-RU folgende Hauptfunktionalitäten zur Verfügung:

- „Start up"-Initiierung der Prozeduren zur Inbetriebnahme,
- Software Management für Upgrades in der Betriebsphase,

- Initialisierung und Konfiguration der Betriebsparameter,
- Performance Reporting über Messwerte und Counter,
- Alarm-Konfiguration und -Übermittlung sowie
- File Upload zum O-RU-Controller.

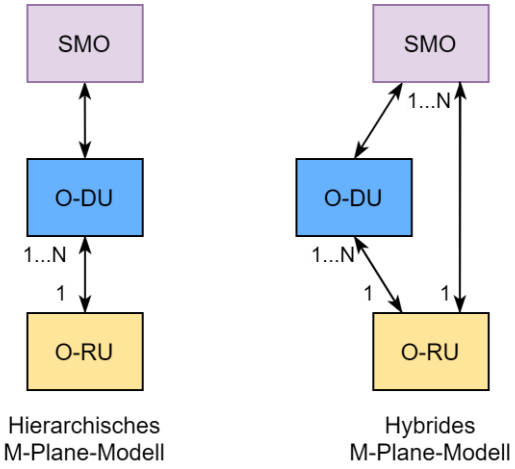

Abbildung 19: M-Plane-Architektur

Die M-Plane-Schnittstelle kann hierarchisch oder auch hybrid implementiert sein, wie in Abbildung 19 dargestellt. Im hierarchischen Modell wird die O-RU von einer oder mehreren DUs kontrolliert, z. B. um Redundanz zu ermöglichen. Im Fall des hybriden Modells bestehen gleichzeitig logische Verbindungen von der O-RU zur O-DU und zum SMO-Layer, die ggf. dieselben physischen Verbindungen nutzen. Im hybriden Fall können die Funktionen für das Management der O-RU zwischen den O-RU-Controllern aufgeteilt werden. Beispielsweise kann das Software Management im SMO-Framework angesiedelt werden.
Typischerweise wird die Konfiguration für die O-RU initial sowie im laufenden Betrieb durchgeführt, wofür beispielsweise folgende Funktionen über das NETCONF-Protokoll genutzt werden:

- Upload, Commit und Cancel einer neuen Konfiguration,
- Lock/Unlock von Funktionen,
- Rollback zur alten Konfiguration bei Fehlern sowie
- Notifikation über Erfolg/Misserfolg von Aktionen.

Ebenfalls stehen eine Reihe von marktüblichen Funktionen für die Konfiguration bzw. ihre Auslösung zur Verfügung sowie zur Übertragung von Performance-Messungen und Alarmbenachrichtigungen der O-RU. Auf diese soll hier nicht im Detail eingegangen werden.

2.3.8 Cooperative Transport Interface (CTI)

Das CTI ist eine Schnittstelle zwischen O-DUs und Transportknoten eines paketbasierten Transportnetzes, die dazu dient, die O-DUs mit einer Vielzahl von O-RUs zu verbinden [33]. CTI zielt speziell auf Transportknoten ab, die ein gemeinsames Punkt-zu-Multipunkt-Zugangsnetz verwalten. Transportknoten (Router und Switches), die nur Punkt-zu-Punkt-Verbindungen verwalten, tauschen keine CTI-Nachrichten mit den O-DUs aus. CTI besteht aus einer Transport-Kontroll-Ebene (Transport Control, TC) und einer Transport-Management-Ebene (TM).

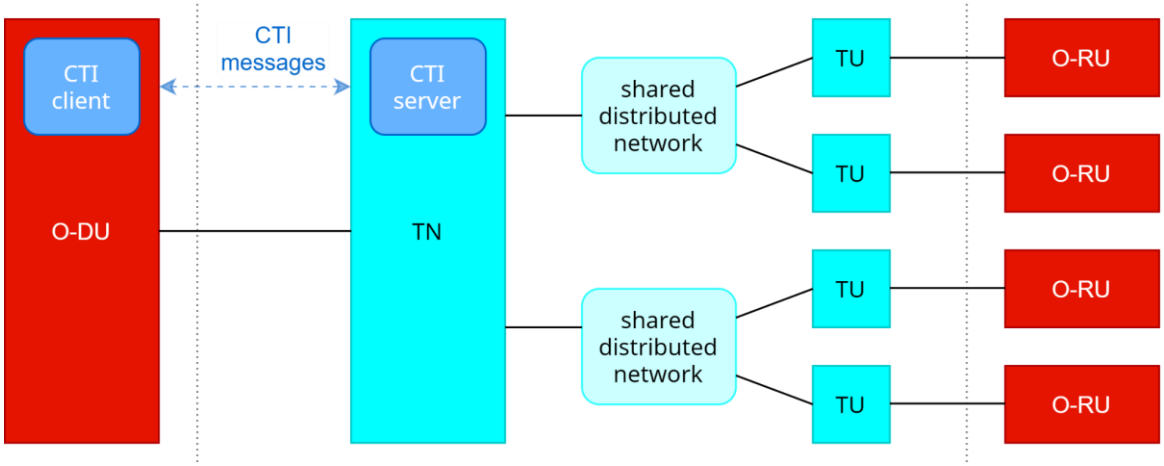

Abbildung 20: Zusammenhang zwischen CTI und dem für das Fronthaul verwendete Transportnetz (Ref. [33])

Die Verwendung von CTI zielt auf paketbasierte Transportnetze ab, die Transportknoten (Transport Nodes, TNs) enthalten, die ein oder mehrere gemeinsame Verteilnetze abschließen, wobei jedes Verteilnetz (ein Port an einem TN) eine Vielzahl von Transport Einheiten (Transport Units, TUs) aggregiert (s. Abbildung 20). Dies impliziert, dass die Bandbreite eines Verteilernetzes von mehreren TUs gemeinsam genutzt wird. In der Upstream-Richtung verwaltet der TN diese Aufteilung, indem er die Bandbreitenzuweisungen an die TUs plant. Es gibt zwei Möglichkeiten, die zuzuweisende Bandbreite zu bestimmen, entweder statisch oder dynamisch.

2.4 Optimierungsanwendungen und Machine Learning

2.4.1 RIC-Funktionen für die RAN-Optimierung

Der RIC ist als eine wesentliche Einheit in der O-RAN-Architektur geplant. Ein Teil des RICs soll aus Funktionen bestehen, die in den Verarbeitungseinheiten der traditionellen Basisstation enthalten sind und im Zuge der Aufsplittung herausgelöst werden sollen. Dadurch wird es ermöglicht, die Management-Schnittstellen zu erreichen, wie z. B. RRM oder SON-Funktionen, die die Funkressourcen und den Netzbetrieb kontrollieren.
Zur Anpassung der RAN-Funktionalität optimiert der RIC die Funkressourcen entsprechend den Betreiber-Policies. Dabei wirkt er sich in drei Hauptbereichen auf die RAN-Leistung aus [4]:

- Netzwerkintelligenz: Durch Messungen und Reports über das Verhalten des RANs werden Daten in standardisierten Formaten generiert, die analysiert werden können (z. B. mit KI/ML-Techniken), um neue Algorithmen und Policies zu erstellen.
- Ressourcen-Sicherung: Ziel ist die Sicherstellung, dass Geräte/Nutzer und Dienste die erforderliche Leistung erhalten (z. B. durch Optimierung der Funkstreckensteuerung, Handover-Optimierung oder Priorisierung).
- Ressourcenkontrolle: Zur Sicherstellung, dass das RAN-System effizient arbeitet, wenn mehrere Benutzergruppen um adäquate Ressourcen konkurrieren können.

Prinzipiell lässt sich sagen, dass im RIC die durch das O-RAN-Konzept angedachte Intelligenz sitzt. Diese Intelligenz soll in Zukunft durch ML-Modelle für Selbstoptimierungs- und Funknetzautomatisierung realisiert werden. Die dazu benötigten Daten werden durch den Non-RT RIC über die O1-Schnittstelle in standardisierten Formaten von den RAN-Komponenten eingesammelt. Zuvorderst werden traditionelle SON-Optimierungsfunktionen bedient. Im späteren Verlauf wird damit Modelltraining durch KI/ML ermöglicht, so dass neue ML-Ansätze für die RAN-Optimierung entwickelt und zum Einsatz kommen können. Die daraus gewonnenen Policies implementiert der Near-RT RIC über die E2-Schnittstelle in den CU-CPs und CU-UPs oder wendet dort dynamische Steuerungen an. Beispielsweise mögen bestimmte

Geräte (wie Kraftfahrzeuge) hohe Mobilitätsanforderungen haben, wofür sich ein anderer, überlegener Handover-Management-Algorithmus anbietet könnte.

2.4.2 xApps/rApps

Neben seiner Funktion als RAN-Controller ist der RIC eine offene Plattform, die RAN-Steuerungsanwendungen hosten kann. Diese Anwendungen werden von spezialisierten Softwareanbietern entwickelt, die nicht zum RIC-Anbieter selbst gehören müssen. Diese sogenannten „xApps“ (im Near-RT RIC) und „rApps“ (im Non-RT RIC) sollen Innovationen in Form von RAN-Steuerungsalgorithmen ermöglichen bzw. Software-Innovatoren für den Mobilfunkbereich gewinnen. xApps und rApps haben dazu die Möglichkeit, Daten aus dem RAN um Größenordnungen schneller zu verarbeiten als dies mit den heutigen herstellerproprietären Systemen oder zentralisierten SON-Methoden der Fall ist. Dadurch sollen differenzierte Netzwerkerlebnisse geschaffen werden, die eine an bestimmte Servicetypen, Benutzergruppen oder Standorte angepasste Leistung bieten.
Umgekehrt bestehen die von einem RIC bereitgestellten Dienste entweder aus xApps oder rApps oder einer Kombination aus beidem. Es gibt keine feste Grenze für die Arten von xApps oder rApps, die programmiert werden können, und es wird erwartet, dass mehr als eine xApp oder rApp gleichzeitig im RAN ausgeführt wird.
Zu den bisher vorgeschlagenen Beispielen für xApps/rApps gehören [24]:

- Kontextbasiertes dynamisches Handover-Management für Vehicle-to-Everything (V2X),
- dynamische Funkressourcenzuweisung für unbemannte Luftfahrzeuge,
- Steuerung des Datenverkehrs,
- Optimierung der Dienstgüte/Qualität der Erfahrung (QoS/QoE),
- Optimierung von Massive-MIMO-Beamforming,
- RAN-Sharing,
- QoS-basierte Ressourcen-Optimierung,
- Servicegarantie für RAN-Slices,
- Multi-Vendor-Slice-Leistungsmanagement,
- dynamische gemeinsame Nutzung des Spektrums,
- Optimierung der Ressourcenzuweisung für Network-Slice-Subnetz-Instanzen (NSSI),
- lokale Indoor-Positionierung im RAN.

[4] führt aus, dass die ersten xApps sich auf Health-Check-Funktionen konzentrieren werden, z. B. die Betriebsbereitschaft von RAN-Knoten. In einer zweiten Phase werden xApps tiefer in die Beobachtungen eindringen, indem sie detailliertere Daten von RAN-Knoten für die Analyse sammeln. xApps, die nahezu in Echtzeit Änderungen vornehmen (d. h. Zeitzyklen von weniger als 1 Sekunde), werden in späteren Phasen erwartet. In Bezug auf Entscheidungen auf der Steuerungsebene wird ein erster Ansatz darin bestehen, die aktuellen RRM-Funktionen, die in der CU und DU implementiert sind, zu ergänzen, wobei die Richtlinien von einem RIC die lokale RRM-Logik ändern oder außer Kraft setzen könnten. Ein aggressiverer Ansatz, bei dem die RRM-Funktion vollständig in den RIC verlagert wird, ist ein längerfristiger Prozess.
Anfängliche rApps, die im Non-RT RIC gehostet werden, werden zunächst den heutigen zentralisierten SON-Anwendungen ähneln. Sie haben das Potenzial, sich schnell weiterzuentwickeln, wenn die RAN-Datenerfassung mit ML-Techniken gepaart wird, um Algorithmen zu erstellen, die neue Formen der Optimierung für das RAN ermöglichen.
Ein Bestandteil der Near-RT RIC-Plattform ist der "E2-Manager", der manchmal auch als "xApp Zero" bezeichnet wird. Er wird verwendet, um E2-Verbindungen mit den RAN-Knoten zu initiieren und dann RAN-Konfigurationsinformationen zu speichern, die beim Verbindungsaufbau erlernt wurden (und im Laufe der Zeit aktualisiert werden).

Die ersten Versionen der RIC-Spezifikationen sind unter [29] und [30] verfügbar. Die O-RAN-Arbeitsgruppe 3 wird die Entwicklung fortsetzen, um weitere Funktionen hinzuzufügen wie die E2SM-Spezifikationen (E2 Service Model). Zu den wichtigen derzeit laufenden Arbeiten laut [4] zählen die Standardisierung von E2SMs, die Traffic Steering und QoS/QoE-Optimierung durch den RIC ermöglichen sollen. Traffic Steering zielt auf Idle Mode Mobility Load Balancing (MLB), Inter-Intra-Frequency MLB, Carrier Aggregation und Dual Connectivity ab. Die QoS/QoE-Optimierung ermöglicht dem RIC die Steuerung von Netzwerkfunktionen im Zusammenhang mit QoS-Steuerung, Funkressourcenzuweisung, Funkzugangssteuerung, Mobilitätsfunktionen und Verbindungsmanagement.
Zu den Betreibern, die öffentlich erklärt haben, dass sie RIC-Lösungen testen, gehören AT&T, Deutsche Telekom, KDDI und China Mobile [4].

2.4.3 Machine Learning (ML)

Die Verfügbarkeit und Leistungsstärke von KI und ML haben die Spezifikation von Architektur und Prozessen für O-RAN in WG2 vorangetrieben. Insbesondere für den Netzbetrieb sind ML-unterstützte Anwendungsfälle vielseitig und können deshalb an verschiedenen Stellen der O-RAN-Architektur sinnvoll eingesetzt werden. Entsprechend der geforderten Antwortzeiten, der Verfügbarkeit und Menge der Daten für ML-Training und ML-Inference (Inferenz; automatisierte bzw. computergestützte Ableitung von Schlussfolgerungen) sowie der Rechenkomplexität variiert der Ort für die Komponenten des ML-Workflows. Der allgemeine Ablauf und die Komponenten für ML-Prozesse sind in Abbildung 21 dargestellt. Eine Indikation zur Zuordnung der ML-Komponenten, Datenflüsse und Aktionen zu den Netzwerkfunktionen ist beispielhaft angegeben.

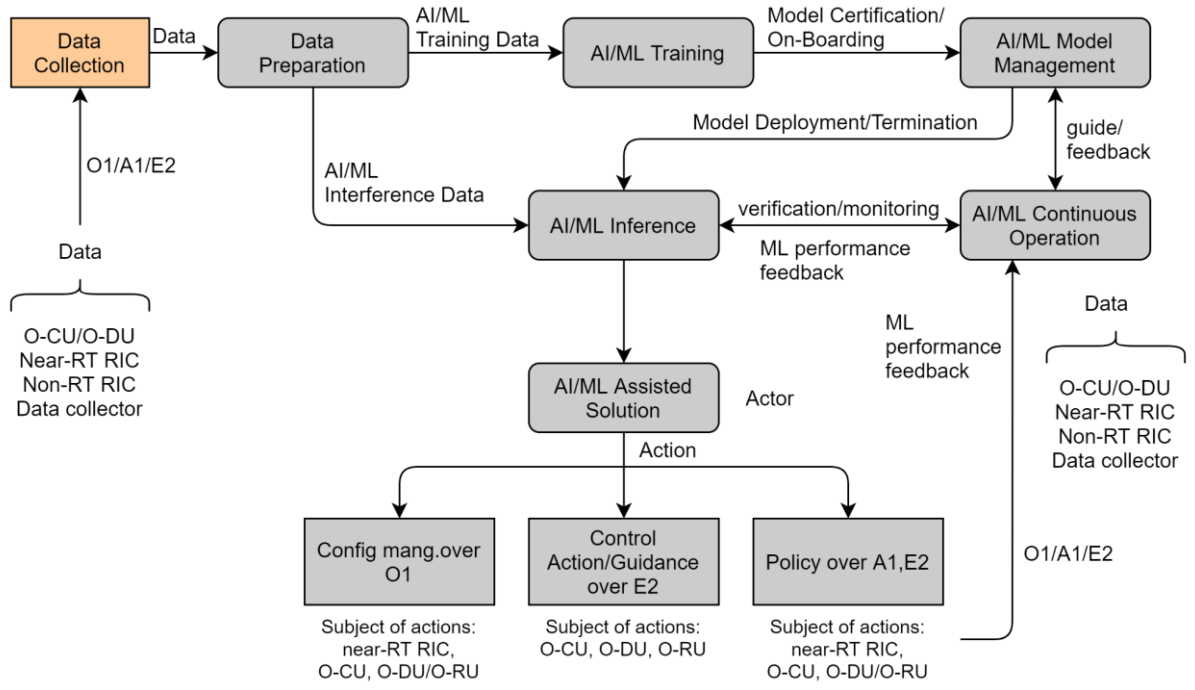

Abbildung 21: Allgemeine Prozeduren in AI/ML [34]

Zu Beginn wird eine Implementierung des ML-Training-Hosts – in erster Linie im Non-RT RIC – erwartet, wobei Daten über O1 und A1 übertragen werden. Im Non-RT RIC werden aus der Model-Inference Aktionen abgeleitet, die z. B. über die A1-Schnittstelle (Policies, Konfiguration) an den Near-RT RIC bzw. über E2 (Konfiguration) an O-CU, O-DU und O-RU weitergegeben werden. Für Prozesse und Entscheidungen, die kürzere Control-Loops erfordern, wird ML-Model-Inference im Near-RT RIC ausgeführt, um Aktionen für den Near-RT RIC abzuleiten oder Befehle/Policies über E2 an die O-RAN Komponenten zu übergeben.

In der Zukunft ist es vorgesehen, dass ML-Prozesse auch für die O-DU-/O-RU-Control-Loop spezifiziert werden.
Trainingsdaten werden durch Datensammler von allen O-RAN-Komponenten über E2, A1 und O1 erfasst und über Aggregations- und Filterkomponenten dem Trainingsprozess bereitgestellt. Besonders relevant sind dabei die Daten vom E2-Interface in verschiedenen Granularitäten bzgl. Ort und Zeit. Enrichment-Daten können dabei jeweils über alle verfügbaren Schnittstellen bzw. intern im SMO-Layer bereitgestellt werden. Letzteres ist bei den Sicherheitsbetrachtungen zu beachten, da Funktionen im SMO-Layer auch proprietäre Schnittstellen zu Rohdatenquellen haben können.
Eine typische Anwendung für ML-unterstützte Prozesse ist die RAN-Optimierung. Aufgrund der dafür oft notwendigen großen Datenmengen und deren komplexe Verarbeitung bietet sich hier der Non-RT RIC sowohl für Training als auch für Inferenz an. Zudem können Enrichment-Daten korreliert werden, die aus externen OSS-Systemen (Operations Support System) herangezogen werden.
Für einen sicheren kontinuierlichen Betrieb der ML-Prozesse muss auch eine Reihe von Funktionen bereitstehen, die basierend auf KPI-Definitionen die Komponenten, Prozesse und Aktionen bzgl. Aktivität, Performance, Timing, Ressourcenverbrauch und Konsistenz überwachen und ggf. Änderungen triggern. Auch diese Aufgaben könnten ihrerseits durch ML unterstützt sein.

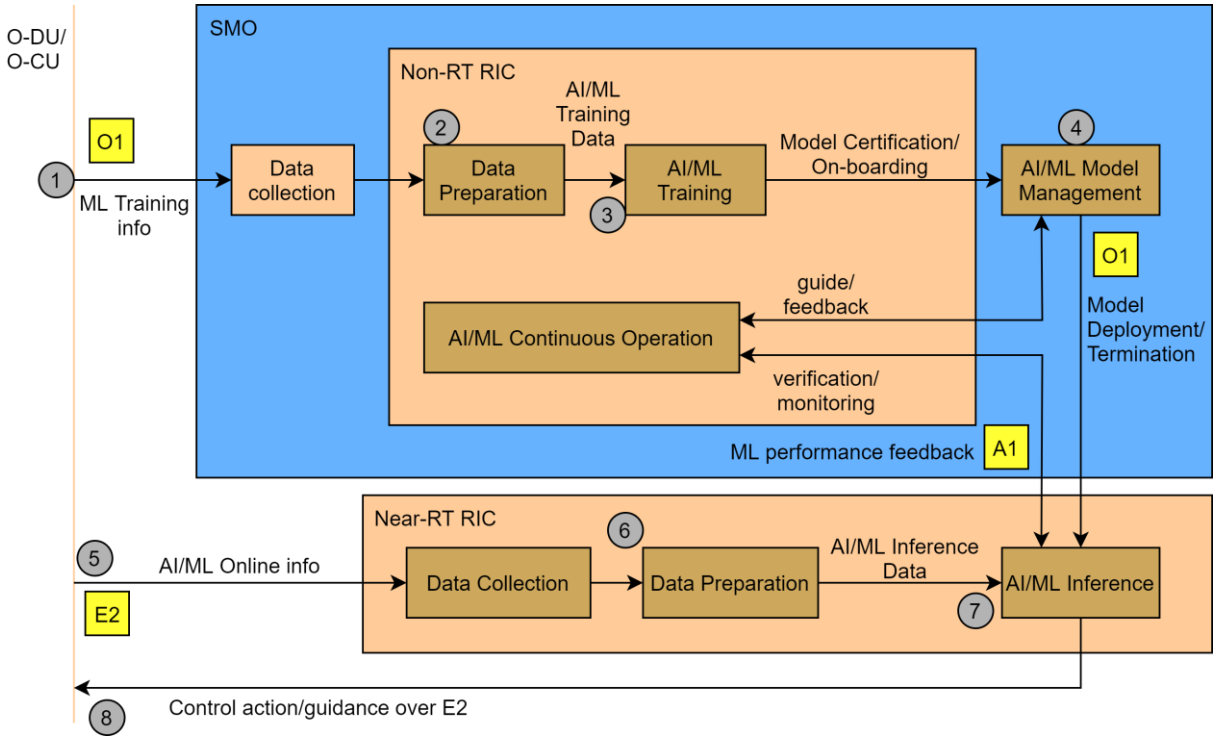

Abbildung 22: Deployment-Szenario für AI/ML [34]

Basierend auf dem entsprechenden Feedback des Model-Inference-Hosts kann im SMO-Layer z.B. entschieden werden über

- die zu ändernde Modell-Auswahl,
- zusätzliches Training für das Modell oder
- die Terminierung des Modells.

Von den Systemherstellern wie auch 3rd-Party-Anbietern werden zunehmend ML-basierte Algorithmen entwickelt, die auf O-CU und O-DU in Betrieb sind und im Bereich von Millisekunden Aktionen generieren, um UE-spezifisch mit Optimierungsmaßnahmen zu reagieren, also unmittelbar auf die User Experience und die funktionale Sicherheit einwirken.

Umso wichtiger ist es auch für O-RAN-Architekturen, nicht nur neue Integrations- und Abnahmeprozeduren, sondern auch betriebliche Konzepte weiterzuentwickeln, die sich auf interne Abläufe des Betreibers in der Multi-Vendor-Umgebung richten. Als Beispiel ist in Abbildung 22 ein Deployment-Szenario angegeben, in dem die ML-Komponenten und ML-Prozesse wie folgt in den O-RAN-Funktionen eingebettet sind:

- im SMO das Modell-Management,
- im Non-RT RIC die Aufbereitung der Trainingsdaten, das Training und die Prozesse für den kontinuierlichen Betrieb sowie
- im Near-RT RIC der ML-Inference-Prozess.

2.5 O-RAN-Software

Neben den Spezifikationen wird von der O-RAN Alliance in Kooperation mit der Linux Foundation auch eine Open-Source-Referenzimplementierung für den Betrieb eines O-RAN entwickelt. Die für die Entwicklung zuständige Organisation ist die O-RAN Software Community (kurz: OSC)[4]. Gemäß des aktuellen White Papers „O-RAN Minimum Viable Plan and Acceleration towards Commercialization“ vom 29. Juni 2021 [35] ist das Ziel der OSC-Entwicklungen „*to achieve a solution that can be utilized for industry deployment*“. Um dieses Ziel zu erreichen, werden für die verschiedenen O-RAN-Komponenten Referenzimplementierungen entwickelt. Diese Entwicklungen werden durch das „Requirements and Software Architecture Committee“ (RSAC) und das „Technical Oversight Committee“ (TOC)[5] koordiniert.
Das TOC hat 12 stimmberechtigte Mitglieder. Aktuell sind 10 Positionen besetzt. Die TOC-Mitglieder stammen dabei von Telekommunikationsunternehmen (AT&T, China Mobile, Deutsche Telekom, NTT Docomo, Orange, TIM) sowie von Ausrüstern (Ericsson, Nokia) und Zulieferern (Radisys, Wind River Systems). Die Meeting Minutes (einschließlich Aufzeichnungen der Online-Meetings) sind dabei auf der Web-Seite des TOCs frei zugänglich. Zusätzlich werden auch Synergieeffekte mit anderen Projekten gesucht. Insbesondere zu erwähnen sind hier die Entwicklungen im Rahmen der ONF[6] sowie der Open Network Automation Platform (ONAP)[7].
Es ist geplant, dass ca. alle 6 Monate ein neues Release veröffentlicht wird. Die Releases sind dabei mit Buchstaben und zugehörigen Wörtern gekennzeichnet. Aktuell befindet sich das vierte Release (D — Dawn) im Veröffentlichungsprozess.
Prinzipiell steht eine Beteiligung an der Open Source Softwareentwicklung jedem Interessierten offen. Um sich zu beteiligen, muss dabei dem „Contributor License Agreement“ (CLA) zugestimmt werden. Die Beiträge werden dabei unter die Apache Lizenz, Version 2.0[8] gestellt. Für die Quellkodeverwaltung wird `git` verwendet. Für das Management von Änderungsvorschlägen wird auf `Gerrit` gesetzt. Die zugehörige öffentlich zugängliche Web-Seite befindet sich hier: https://gerrit.o-ran-sc.org/

[4] https://o-ran-sc.org/
[5] https://wiki.o-ran-sc.org/display/TOC
[6] https://opennetworking.org/
[7] https://onap.org/
[8] https://www.apache.org/licenses/LICENSE-2.0

3 Methodologie und Scope

In diesem Kapitel wird ein Überblick über die in dieser Studie angewendete Methodologie zur Risikoanalyse bezüglich O-RAN gegeben. Dabei werden sehr kurz existierende Vorgehensmodell zur Risikoermittlung beschrieben. Darüber hinaus werden wesentliche Grundlagen und Annahmen vorgestellt.

3.1 Allgemeines und Scope

Die in dieser Studie durchgeführte Risikoanalyse beschränkt sich ausschließlich auf das 3GPP-RAN in seiner Umsetzungsvariante O-RAN. Die Grenzen der Betrachtungen sind insofern durch die RAN-Schnittstellen zum Endgerät (Uu-Schnittstelle) und zum 5G-Core gegeben. Risiken für das 5G-Gesamtsystem, die sich aus unsicheren Endgeräten einschließlich Endgeräte-nahen Komponenten (USIM etc.) sowie aus einem unsicheren 5G-Core ergeben, spielen insofern in dieser Studie keine Rolle.

In dieser Studie wird ferner lediglich ein 5G-RAN (NG-RAN) betrachtet. Dies bedeutet insbesondere, es wird davon ausgegangen, dass das RAN mit einem 5G-Core verbunden ist.

Die der Risikoanalyse zugrundeliegenden Informationen stammen aus öffentlich zugänglichen Dokumenten. Dies betrifft insbesondere die durch 3GPP bereitgestellten Dokumente (Standards, Reports etc.) und die durch die O-RAN Alliance bereitgestellten Dokumente. Dabei wurde jeweils auf die im Zeitraum der Erstellung dieser Studie (Mai–September 2021) aktuellen, öffentlich zugänglichen Versionen der Dokumente zurückgegriffen. Bei Verweis auf die benutzten Standards und Spezifikationen wird dabei jeweils die exakte Version des benutzten Dokuments angegeben. Nicht berücksichtigt wurden davon gegebenenfalls abweichende, in der Praxis tatsächlich eingesetzte Systeme bzw. konkrete Implementierungen der Standards und Spezifikationen. Ebenso wenig wurde der konkrete Betrieb eines RANs durch einen Netz- bzw. RAN-Betreiber berücksichtigt. Insofern ist es möglich, dass ein praktisch ausgerolltes RAN tatsächlich weniger Sicherheitsrisiken besitzt, im Vergleich zu den im Ergebnis dieser Studie identifizierten Risiken, da der Betreiber gegebenenfalls zusätzliche Sicherheitsmaßnahmen zur Risikominimierung umgesetzt hat.

Bei der Risikoanalyse wurden im Wesentlichen nur Bedrohungen und Schwachstellen berücksichtigt, die 3GPP- bzw. O-RAN spezifisch sind. Generische IT-Risiken, die eher allgemein dem Bereich der Informations- und Kommunikationstechnologie zuzuordnen sind, wie beispielsweise fehlerhafte Implementierungen, fehlerhafte Konfigurationen etc. werden nur an einigen wenigen Stellen explizit erwähnt und berücksichtigt. Hauptgrund ist, dass eine Vielzahl von Risikoanalysen für den IT-Bereich existieren, die hier nicht wiederholt werden sollen, die bei der Gesamtrisikoeinschätzung bezüglich eines konkreten RAN-Deployments aber natürlich zu berücksichtigen sind.

3.2 Risikoanalyse Methodologien

Im Rahmen dieser Studie wird ein Risiko als „*Auswirkung von Unsicherheit auf Ziele*“ [36] angesehen. Dabei werden die „Auswirkungen auf Ziele“ als Schäden verstanden—positive Auswirkungen auf Ziele werden im Rahmen dieser Studie daher nicht betrachtet. Die „Unsicherheit“ betrifft dabei das Eintreten von Ereignissen mit bestimmten Wahrscheinlichkeiten, wobei diese Ereignisse ursächlich für die auftretenden Schäden sind (Risikoquellen/Risikoursachen [36]). Zur quantitativen bzw. qualitativen Beschreibung der Höhe eines Risikos wird auf die übliche Formel zurückgegriffen:

$$\text{Risiko} = \text{Eintrittswahrscheinlichkeit} \cdot \text{Schadenshöhe}$$

Es gibt eine Vielzahl von Vorgehensmodellen bezüglich der Risikoermittlung (ISO 27005 [37], ISO 31000 [36], IEC 31010 [38], BSI-Standard 200-3 [39], etc.). Dabei ist das Vorgehen oft ähnlich und erfolgt gemäß den folgenden Schritten:

1. Festlegung des zu berücksichtigenden Angreifers
2. Bestimmung der schützenswerten Assets
3. Bestimmung der Kritikalität von Schutzzielverletzungen bezüglich der Assets, d. h. Ermittlung des potenziellen Schadens
4. Ermittlung von Bedrohungen bezüglich Schutzzielen und Assets
5. Ermittlung und Bewertung von Schwachstellen bezüglich der identifizierten Bedrohungen und unter Berücksichtigung existierender Sicherheitsmaßnahmen
6. Ermittlung des Risikos anhand der Schwachstellen und der möglichen Schäden
7. Bewertung der Risiken einschließlich der Planung von Maßnahmen zum Umgang mit den Risiken

Nachfolgend werden zunächst die im Rahmen die Studie relevanten Schutzziele und Angreifermodell beschrieben. Ferner werden die verschiedenen, betrachteten Szenarien erläutert. Darauf basierend wird das für diese Studie konkret gewählte Vorgehensmodell beschrieben.

3.3 Betrachtete Schutzziele

In dieser Studie werden zum einen die üblichen drei Schutzziele: **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** betrachtet, sowie darüber hinaus noch **Zurechenbarkeit** und **Privacy**. Nachfolgend erfolgen kurze Erläuterungen bezüglich der Bedeutung dieser Schutzziele im Rahmen der vorliegenden Studie.

Vertraulichkeit meint, dass Daten und Informationen nur Berechtigten zu Kenntnis gelangen.

Integrität bedeutet, dass Daten und Informationen vollständig, korrekt und aktuell sind oder dass dies erkennbar nicht der Fall ist. Letzteres bedeutet insbesondere, dass unberechtigte Manipulationen an den Daten und Informationen erkannt werden können. Die Formulierung „vollständig, korrekt und aktuell“ bezieht sich dabei auf eine Sicht innerhalb des betrachteten IT-Systems—es wird insofern explizit nicht berücksichtigt, ob die Daten und Informationen bezüglich der realen Welt vollständig, korrekt und aktuell sind.

Zurechenbarkeit bedeutet, dass Aktionen (beispielsweise Senden von Daten) der beteiligten Entität (im Beispiel: dem Sender) gegenüber Dritten beweisbar zugerechnet werden können. Angemerkt sei, dass bei der Risikoanalyse bezüglich Vertraulichkeit, Integrität und Zurechenbarkeit Sicherheitsmaßnahmen, die gegebenenfalls innerhalb eines gegebenen Anwendungsfalls auf Anwendungsschicht erfolgen nicht berücksichtigt werden, da derartige Sicherheitsmaßnahmen außerhalb des betrachteten Systems 5G-RAN erfolgen.

Verfügbarkeit meint zunächst allgemein, dass Daten und Informationen sowie Dienste dann und dort für Berechtigte verfügbar sind, wo und wann sie von Berechtigten benötigt werden. In Rahmen dieser Studie umfasst das Schutzziel darüber hinaus unberechtigte Beeinträchtigungen der Dienstgüte (Quality of Service, QoS) bzw. eine Erhöhung der mit der Diensterbringung bzw. Bereitstellung von Daten und Informationen verbundenen Kosten—also etwa eine Erhöhung der Verzögerungszeit, eine Verringerung des Durchsatzes oder eine Erhöhung des Energieverbrauchs. Analysen bezüglich des Schutzziele Verfügbarkeit sind insofern von besonderer Bedeutung, da im Allgemeinen—im Gegensatz etwa zu den Schutzzielen Vertraulichkeit, Integrität und Zurechenbarkeit—die Durchsetzung dieses Schutzziels aus Anwendungssicht nur mit erheblichen Kosten bzw. gar nicht möglich ist, wenn das benutzte Kommunikationssystem (im Falle der Studie: 5G) nicht bezüglich Verfügbarkeit verlässlich ist.

In dieser Studie subsummiert das Schutzziel „*Privacy*“ Schutzziele, die üblicherweise mit Datenschutz in Zusammenhang stehen wie etwa Anonymität, Unverkettbarkeit oder Unbeobachtbarkeit. Bei den Betrachtungen bezüglich des Schutzziele „Privacy“ geht es insofern um die Frage, inwiefern Meta-Daten anfallen, die genutzt werden können, um die Vertraulichkeit der Umstände der Kommunikation zu verletzen. Dies können beispielsweise Meta-Daten sein, die es erlauben mehrere Kommunikationsvorgänge zu verketten, so dass eine Profilbildung bezüglich des Kommunikationsverhaltens (Häufigkeit, Dauer, Ort etc.) möglich

ist. Ferner können Meta-Daten in Zusammenhang mit Ortsinformationen dazu dienen Bewegungsprofile zu erstellen oder generell offenlegen, wer mit wem (ggf. pseudonymisiert) kommuniziert. Ähnlich wie Verfügbarkeit handelt es sich auch bei Privacy um ein Schutzziel, welches ohne entsprechende Unterstützung durch das Kommunikationsnetz gar nicht bzw. nur mit erheblichem Aufwand umsetzbar ist.

3.4 Betrachtete Angreifer — Angreifermodell

Ein wesentliches Element bei der Durchführung einer Risikoanalyse ist der bei der Bewertung der Risiken unterstellte Angreifer und dessen Fähigkeiten. Diese werden üblicherweise in einem Angreifermodell zusammengefasst. Im Rahmen dieser Studie werden dabei fünf verschiedene Angreifermodelle berücksichtigt, die sich an folgenden Rollen orientieren (siehe Abbildung 23):

- **Außenstehender**: Ein Angreifer, der seine Angriffe nur unter Benutzung der im System definierten Schnittstellen durchführen kann, da er zunächst keine Kontrolle über am System beteiligte Komponenten hat. Bezüglich 5G-RAN bedeutet dies konkret, dass der Angreifer sowohl über die drahtlose Luftschnittstelle als auch über die durch 3GPP bzw. die O-RAN Alliance spezifizierten Schnittstellen angreifen kann. Dabei wird davon ausgegangen, dass der Angreifer über das jeweils verwendete Transportmedium die volle Kontrolle hat, also sowohl bezüglich der Funkverbindung als auch der verwendeten (IP-basierten) Verbindungen zwischen den 5G- bzw. O-RAN-Komponenten alle ausgetauschten Daten belauschen und beliebig manipulieren kann (verändern, löschen, verzögern, generieren etc.).
- **Nutzer**: Ein Angreifer, der End-Nutzer bezüglich des 5G-Systems im Sinne des 5G-System ist, also die Kontrolle über ein oder mehrere UE besitzt, welche berechtigterweise Dienste des 5G-Systems in Anspruch nehmen können. Im Rahmen dieser Studie werden diesem Angreifer zusätzlich die Fähigkeiten des „Außenstehenden“ zugesprochen. Der Angreifer „Nutzer“ unterscheidet sich vom Angreifer „Außenstehender“ im Wesentlich dadurch, dass er Credentials/Geheimnisse kennt bzw. nutzen kann, die für die legitime Nutzung des 5G-Netzes notwendig sind.
- **Cloud-Betreiber:** Ein Angreifer, der die physische und logische Kontrolle über die durch das 5G-RAN benutzte (Edge-)Cloud Infrastruktur hat. Diese betrifft alle Cloud-Komponenten, die nicht explizit 5G-RAN-Komponenten (spezifiziert durch 3GPP bzw. die O-RAN Alliance) sind und umfasst sowohl Hardware- als auch Software-Komponenten. Der Angreifer hat darüber hinaus sämtliche Möglichkeiten, die dem Angreifer „Nutzer“ zur Verfügung stehen.
- **Insider:** Ein Angreifer, der die Kontrolle über genau eine 5G-RAN- bzw. O-RAN-Komponente hat und der zusätzlich die Fähigkeiten des „Nutzers“ hat. Dieser Angreifer ist insbesondere deshalb interessant, um zu untersuchen, ob die fein-granularere Aufteilung in Komponenten im Falle von O-RAN aus Sicherheitssicht ein Gewinn sein kann im Vergleich zum (zumindest konzeptionell) eher monolithischen 3GPP-RAN. Wie unten noch ausgeführt wird, erfolgt die Risikoanalyse zunächst einzeln für die relevanten O-RAN-Schnittstellen, bevor daraus eine zusammenfassende Gesamteinschätzung abgeleitet wird. Für die Risikoanalyse einzelner Schnittstellen wird dabei jeweils unterstellt, dass der Insider eine Komponente kontrolliert, die mit dieser Schnittstelle verbunden ist, der Insider somit also Zugriff auf die Schnittstelle hat–hier geht es also im Wesentlichen um die Frage, inwiefern sich bezüglich eines Insiders auf Grund von zusätzlichem Wissen oder Rechten neue Risiken im Vergleich zum Angreifer „Nutzer“ ergeben.
- **RAN-Betreiber**: Ein Angreifer, der die volle Kontrolle über das 5G-RAN hat. Dieser Angreifer ist insbesondere deshalb interessant, um die Risiken, die von einem kompromittierten RAN ausgehen, einschätzen zu können. Dieser Angreifer erweitert

die Fähigkeiten des Angreifers „Insider“ und besitzt auf triviale Weise die Fähigkeiten des Angreifers „Nutzer“.

Allen betrachteten Angreifern liegen dabei folgende gemeinsame Annahmen zu Grunde:

- erhebliche, wenn auch nicht unbegrenzte Ressourcen (Rechenleistung, Speicherplatz, Geld etc.) stehen zur Verfügung. Hiermit sollen Fälle von staatlich unterstützten Angreifern bzw. finanzkräftige Cyberkriminelle abgedeckt werden.
- aktive, verändernde Angreifer, die insofern bereit sind, die Regeln auch außerhalb der von ihnen kontrollierten Systemteile (etwa durch das Manipulieren von übertragenen Daten) zu brechen.
- Kryptographie ist sicher, d. h. es wird angenommen, dass die Angreifer nicht in der Lage sind, nach den derzeitigen Erkenntnissen als sicher angesehene kryptographische Algorithmen und Protokolle zu brechen.
- Kryptographische Geheimnisse sind sicher, d. h. es wird angenommen, dass die Angreifer initial keine Kenntnisse über kryptographische Geheimnisse (kryptographische Schlüssel etc.) haben, die sie nicht auf Grund ihrer Rolle (siehe oben) kennen.

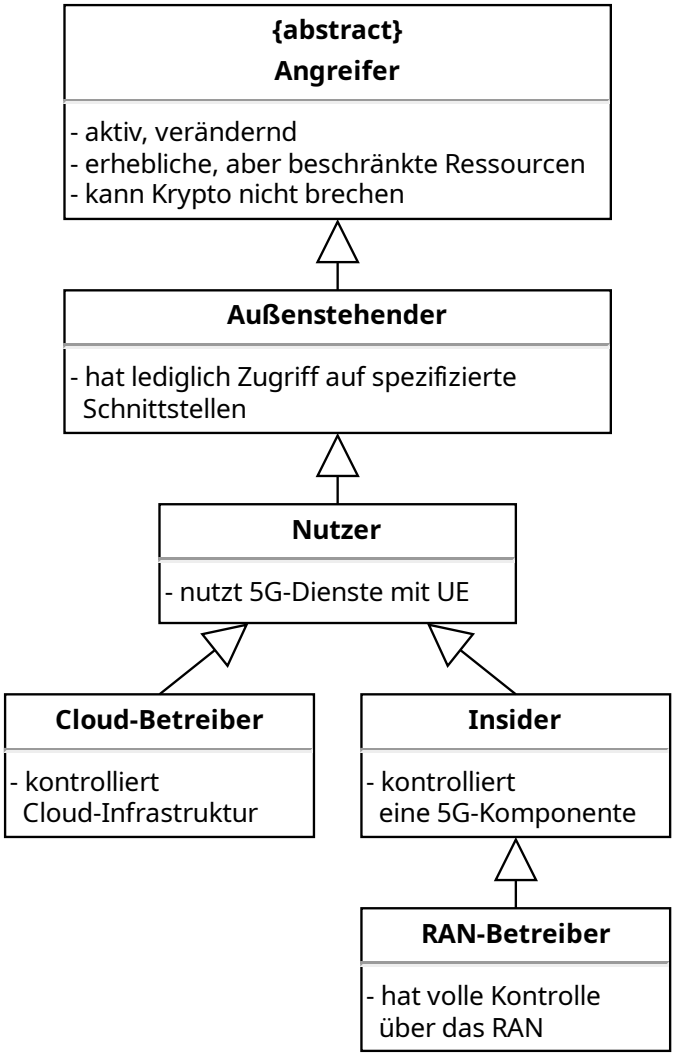

Abbildung 23: Hierarchie der betrachteten Angreifermodelle

3.5 Perspektiven

Die Analyse der Risiken bezüglich 5G-RAN und dessen Implementierung O-RAN erfolgt unter Berücksichtigung verschiedener Perspektiven, die nachfolgend näher erläutert werden. Dies betrifft zum einen Perspektiven bezüglich unterschiedlicher Stakeholder und zum anderen Perspektiven bezüglich der Umsetzung von Sicherheitsmaßnahmen.

3.5.1 Stakeholder Perspektive

Mit Hilfe der Stakeholder Perspektive sollen bei der Risikoanalyse unterschiedliche Interessensgruppen berücksichtigt werden, die jeweils spezifische Interessen und Anforderungen bezüglich der Sicherheit des 5G-RAN bzw. des 5G-Gesamtsystems haben. Dies ermöglicht eine differenzierte Betrachtung der 5G-RAN-Risiken.

3.5.1.1 End-Nutzer

Unter einem End-Nutzer wird eine Entität verstanden, die ein oder mehrere Geräte (UE) mit einem 5G-Netz verbunden hat und die Dienste des betreffenden 5G-Netzes entsprechend nutzt. Als primäres Interesse des End-Nutzer wird dabei unterstellt, dass die oben aufgeführten Schutzziele (Vertraulichkeit, Integrität, Zurechenbarkeit, Verfügbarkeit und Privacy) bezüglich der übertragenen Nutzdaten (einschließlich Sprachkommunikation) bzw. bezüglich der Nutzung des 5G-Netzes gewahrt sind. Da kein konkreter End-Nutzer unterstellt wird, betrifft die Zusicherung der Sicherheitseigenschaften alle Arten von 5G-Diensten und alle Anwendungsfälle, bei denen ein 5G-Netz involviert ist. Insofern ist zu unterstellen, dass jede Verletzung eines der oben aufgeführten Schutzziele kritisch ist und potenziell sehr hohen Schaden verursachen kann. Insbesondere betrifft dies die Schutzziele Verfügbarkeit und Privacy, da ein End-Nutzer nur mit erheblichem Aufwand einer entsprechenden Schutzzielverletzung begegnen kann.

3.5.1.2 Gesellschaftliche Perspektive / Staat

Wie einführend ausgeführt, stellen die Mobilfunknetze bereits jetzt eine wichtige Kommunikationsinfrastruktur dar. Deren Bedeutung wird in den nächsten Jahren aller Voraussicht nach weiter stark steigen, wobei zunehmend auch kritische Dienste bzw. kritische Infrastrukturen (Strom-, Wasser-, Gesundheitsversorgung, Logistik und Verkehr etc.) stark von einer funktionierenden 5G-Infrastruktur abhängen werden. Insofern sind Sicherheit, Vertrauenswürdigkeit und Verlässlichkeit der 5G-Netze von großer gesellschaftlicher Relevanz. Dem soll durch den Stakeholder „Staat“ Rechnung getragen werden.

Da auch dieser Perspektive eine Vielzahl von konkreten—insbesondere auch kritischen—Anwendungsfällen zu Grunde liegt, ist auch bezüglich der gesellschaftlichen/staatlichen Perspektive zu unterstellen, dass eine Verletzung der erwähnten Schutzziele von sehr hoher Kritikalität ist. Als besonders relevant wird hier insbesondere eine Verletzung der Verfügbarkeit angesehen.

3.5.1.3 5G-Netzbetreiber / Telco

Ein 5G-RAN stellt einen wesentlichen Bestandteil eines 5G-Systems dar. Je nach Betreibermodell kann es dabei sein, dass das 5G-RAN weder unter der unmittelbaren physischen noch logischen Kontrolle des 5G-Netzbetreibers steht, sondern dass der Betrieb des 5G-RANs einer Dritten Partei übertragen wurde. Dabei kann es insbesondere auch sein, dass 5G-Komponenten (Hardware, Software) von verschiedenen 5G-Netzbetreibern gemeinsam genutzt werden (RAN-Sharing). Gleichzeitig besitzt das 5G-RAN bestimmungsgemäß Schnittstellen zum 5G-Core-Netz.

Auf Grund dieser Tatsachen ist es für einen 5G-Netzbetreiber[9] notwendig, die Risiken zu kennen, die von einem potenziell nicht-vertrauenswürdigen 5G-RAN für den Gesamtbetrieb des 5G-Netzes und für die damit verbundenen Assets ausgehen. Angemerkt sein, dass bei

[9] Im Rahmen der Studie wird verkürzend zur besseren Lesbarkeit für die Bezeichnung 5G-Netzbetreiber synonym auch der Begriff „Telco“ verwendet.

der 5G-Netzbetreiber-Perspektive primär Risiken bezüglich der Control Plane betrachtet werden und Risiken bezüglich der übertragenen Nutzdaten eher sekundär sind, da entsprechende Analysen bereits im Rahmen der End-Nutzer-Perspektive erfolgen.

3.5.2 Umsetzung von Sicherheitsmaßnahmen

Die der Risikoanalyse zugrundeliegenden Informationen stammen im Wesentlichen aus den durch 3GPP bzw. der O-RAN Alliance veröffentlichten Standards und Spezifikationen. Die Risikoanalyse beruht also insbesondere nicht auf einer konkreten 5G-RAN Implementierung mit genau spezifizierten Eigenschaften. Vielmehr geben die Standards und Spezifikationen einen gewissen Rahmen vor, innerhalb dessen sich konforme Umsetzungen eines 5G-(O-)RAN bewegen können. Von besonderer Relevanz für diese Studien sind dabei die vorgesehen Sicherheitsmaßnahmen und -mechanismen und ob deren Umsetzung jeweils verbindlich vorgeschrieben oder lediglich optional ist. Um insbesondere die optionalen Sicherheitsmaßnahmen angemessen bei der Risikoanalyse zu berücksichtigen, werden zwei Szenarien angenommen:

- **worst case**: keine der optionalen Sicherheitsmaßnahmen ist umgesetzt.
- **best case**: alle optionalen Sicherheitsmaßnahmen sind umgesetzt.

Angemerkt sei hier, dass dabei lediglich Sicherheitsmaßnahmen berücksichtigt werden, die in den Standards und Spezifikationen zumindest als optional erwähnt sind. Bezüglich aller denkbaren darüber hinaus gehenden Sicherheitsmaßnahmen, die ein 5G-RAN-Betreiber zusätzlich umsetzen könnte, wird insofern angenommen, dass diese nicht umgesetzt sind.

3.5.3 Zusammenfassung

Die drei aufgeführten Stakeholder-Perspektiven analysieren die 5G-RAN-Risken jeweils aus einem anderen Blickwinkel. Vereinfachend kann man sagen, dass die End-Nutzer-Perspektive Risiken bezüglich *User Plane* analysiert, die 5G-Netzbetreiber-Perspektive fokussiert auf die *Control Plane* und die staatliche-Perspektive kombiniert *User Plane und Control Plane* Risiken. Die *worst-case* / *best-case* Betrachtungen spiegeln dabei die Extremsituationen bezüglich umgesetzter Schutzmaßnahmen wider.

3.6 Angewandte Methodologie zur Risikoanalyse

Gemäß den in den vorangegangenen Kapiteln dargelegten Ausführungen wurde im Rahmen der Risikoanalyse die nachfolgend erläuterte Methodologie angewendet.

Bezüglich der *Risikoformel* (Risiko=Eintrittswahrscheinlichkeit · Schaden) ist anzumerken, dass die Risikoermittlung lediglich die Eintrittswahrscheinlichkeit berücksichtigt, da der Schaden vom konkreten 5G-Anwendungsfall abhängig ist und allgemein betrachtet sehr hoch sein kann (siehe Kapitel 3.5.1).

Bezüglich der *Eintrittswahrscheinlichkeit* wiederum erfolgt keine genaue quantitative Analyse, da hierzu zum einen keine Daten vorliegen, zum anderen eine genau quantitative Analyse ebenfalls Anwendungsfall abhängig ist. Im Rahmen der Studie wird vielmehr auf eine qualitative Einschätzung zurückgegriffen, wobei drei Abstufungen vorgenommen werden:

- **hoch**: Eine hohe Eintrittswahrscheinlichkeit liegt vor, wenn es einem gegebenen Angreifer prinzipiell mit geringem Aufwand möglich ist, eine Schwachstelle auszunutzen und insofern das risikobehaftete Ereignis auszulösen, welches dann wiederum zu einem entsprechenden Schaden führt. Dies trifft insbesondere dann zu, wenn das Ausnutzen der Schwachstellen im Rahmen der dem Angreifer klar zugebilligten Möglichkeiten liegt. Ein Beispiel ist das unverschlüsselte Übertragen von schützenswerten Daten über eine Schnittstelle bzw. ein Transportmedium, auf die der Angreifer gemäß Angreifermodell Zugriff hat. Angemerkt sei, dass hier zusätzliche Aufwände, die etwa mit der räumlichen Verteilung des Angreifers zusammenhängen, unberücksichtigt bleiben. So kann eine ungesicherte Funkschnittstelle beim zellular aufgebauten Mobilfunknetz bedeuten, dass ein Angreifer für flächendeckende Massenüberwachung einen hohen Aufwand betreiben muss, was als Argument für eine Bewertung als insgesamt

eher mittleres Risiko herangezogen werden könnte. Nichtsdestotrotz bleibt das Risiko für gezielte Angriffe auf einzelne Endgeräte bzw. geographisch beschränkte Regionen hoch. Als Anwendungsfall ergeben sich hier insbesondere Angriffe auf Campusnetze, für die das Risiko weiterhin als hoch einzuschätzen ist. Darüber hinaus bedeutet die Voraussetzung des Zugriffs auf großflächig verteilte Sende-/Empfangsanlagen nicht notwendigerweise, dass diese durch den Angreifer physisch aufgebaut werden müssen. Vielmehr kann der Angreifer Unsicherheit in Endgeräte (UE) ausnutzen, um sich Zugriff auf diese Endgeräte zu verschaffen und diese dann für seine Angriffe benutzen. Hierbei ist insbesondere zur berücksichtigen, dass zukünftige die Anzahl von Endgeräte weiter stark wachsen wird—mit voraussichtlich einem hohen Anteil unsicherer Endgeräte etwa aus dem IoT-Bereich. Da eine Berücksichtigung des räumlichen Verbreitungsaspektes des Angreifers insofern wieder nur bezüglich eines konkreten Anwendungsfalls wirklich sinnvoll durchführbar ist, wird dieser (gegebenenfalls Risikoverringernde) Aspekt im Rahmen dieser Studie nicht berücksichtigt.

- **mittel**: Von einer mittleren Eintrittswahrscheinlichkeit wird ausgegangen, wenn das Auslösen des risikobehafteten Ereignisses zwar prinzipiell im Rahmen des Möglichen gemäß Angreifermodell liegt — sich im Allgemeinen und ohne weitere Annahmen allerding nur mit erheblichem Aufwand für den Angreifer umsetzen lässt. Ein Beispiel bezüglich des Angreifers „Nutzer“ ist, dass der Angreifer eine Vielzahl von Geräten (die sich ggf. an unterschiedlichen geographischen Positionen befinden) mit dem 5G-Netz verbindet, um so etwa eine Überlastung des Netzes zu provozieren[10].
- **gering**: Von einer geringen Eintrittswahrscheinlichkeit wird ausgegangen, wenn das Auslösen des risikobehafteten Ereignisses außerhalb der festgelegten Möglichkeiten gemäß Angreifermodell liegt oder wenn es nur mit vernachlässigbarer Wahrscheinlichkeit oder extremen Aufwand auslösbar ist. Ersteres betrifft beispielsweise das unerkannte Manipulieren von mit Hilfe von kryptographischen Verfahren gesichert übertragenen Daten, letzteres etwa das Erraten von geheimen kryptographischen Schlüsseln.

Im Rahmen der Risikoanalyse geht es insofern darum, pro Angreifer (Kapitel 3.4), Perspektive (Kapitel 3.5) und Schutzziel (Kapitel 3.3) zu bewerten, wie wahrscheinlich eine Schutzzielverletzung ist.

Anzumerken ist, dass bei der Analyse der Wahrscheinlichkeit von Schutzzielverletzungen nicht nur bekannte Bedrohungen und Schwachstellen berücksichtigt werden, sondern auch die gemäß Standards und Spezifikationen anzuwendenden, Risikoverringernden Sicherheitsmaßnahmen. Hier wiederum ergeben sich die 5G-RAN bezogenen Gesamtrisiken als Kombination aus den durch die 3GPP-Standards implizierten Bedrohungen und Sicherheitsmaßnahmen und den gemäß O-RAN-Spezifikationen implizierten Bedrohungen und Sicherheitsmaßnahmen. Dabei werden die in Kapitel 3.5.2 eingeführten best-case/worst-case Betrachtungen angewendet. Hier ist anzumerken, dass die best-case/worst-case Betrachtungen jeweils bezüglich der 3GPP-Standards und der O-RAN-Spezifikationen angewendet werden können. Insofern ergeben sich vier Kombinationsmöglichkeiten:

- best-case-Annahmen sowohl bezüglich 3GPP als auch O-RAN (abgekürzt als: *bb*)
- worst-case-Annahmen sowohl bezüglich 3GPP als auch O-RAN (*ww*);
- best-case-Annahmen bezüglich O-RAN kombiniert mit worst-case-Annahmen bezüglich 3GPP (*bw*)

[10] In einigen der existierenden Risikoanalysen zu 5G wird dieses Angriffsszenario mit dem Internet der Dinge in Verbindung gebracht, wobei das Szenario ist, dass sich ein Angreifer (Hacker) Zugriff zu einer Vielzahl von mit dem 5G-Netz verbundenen IoT-Geräten verschafft und diese dann für Angriffe auf das 5G-Netz nutzt (insbesondere für Verfügbarkeits-Angriffe). Dieses Beispiel verdeutlich auch, dass eine Einschätzung, wie aufwendig das Auslösen von risikobehafteten Ereignissen für den Angreifer tatsächlich ist, schwierig ist und von vielen Faktoren abhängt. Im konkreten Beispiel etwa von dem Umstand, dass der Angreifer nicht eigene Geräte für den Angriff benötigt, sondern sich fremder Geräte bedienen kann.

- worst-case-Annahmen bezüglich O-RAN kombiniert mit best-case-Annahmen bezüglich 3GPP (*wb*).

Die Kombination von best-case mit worst-case Annahmen wurde insbesondere deshalb vorgenommen, um zu ermitteln, inwiefern die O-RAN-Spezifikationen einen Einfluss auf das Gesamtrisiko bezüglich des 5G-RAN haben. Das Ergebnis lässt sich überblicksartig gemäß Tabelle 1 darstellen.

Angreifer	**Perspektive (Stakeholder)**														
	End-Nutzer					Staat					Netzbetreiber				
	Schutzziele					**Schutzziele**					**Schutzziele**				
	C	**I**	**A**	**Z**	**P**	**C**	**I**	**A**	**Z**	**P**	**C**	**I**	**A**	**Z**	**P**
Außen-stehender	*bb* *bw* *wb* *ww*														
Nutzer															
Cloud-Betreiber															
Insider															
RAN-Betreiber															

*Tabelle 1: Schema für die überblicksartige Darstellung der Risikobewertung. Die Zellen der Tabelle spiegeln dabei farblich kodiert die Eintrittswahrscheinlichkeit im best-case (**b**) bzw. worst-case (**w**) für eine Schutzzielverletzung bezüglich eines gegebenen Angreifers und einer gegebenen Perspektive (Stakeholder) wider. Dabei bedeuten grün: geringe, gelb: mittlere und rot: hohe Eintrittswahrscheinlichkeit; ein weißes Feld bedeutet, dass (aktuell) keine Aussage möglich ist. Die Abkürzungen für die Schutzziel stehen für: C: Vertraulichkeit (Confidentiality), I: Integrität, A: Verfügbarkeit (Availability), Z: Zurechenbarkeit und P: Privacy.*

Um eine (zusammenfassende) Risikoanalyse für ein (Gesamt)system zu erstellen, erfolgt in manchen Fällen (insbesondere bezüglich O-RAN) zunächst eine Risikoanalyse bezüglich der einzelnen Komponenten des (Gesamt)systems. Diese Einzelbewertungen werden dann bei der Risikoermittlung für das (Gesamt)system im Sinne einer „pro Sicherheit"-Strategie zusammengeführt. Dies bedeutet, dass das Gesamtrisiko bezüglich eines Stakeholders, Angreifers und Schutzziels in der Regel mindestens so hoch ist, wie das höchste Einzelrisiko bezüglich dieses Stakeholders, Angreifers und Schutzziels. Sollten sich aus der Komposition der Komponenten darüber hinaus zusätzliche Risiken ergeben, so kann das Gesamtrisiko auch höher sein als jedes Einzelrisiko. In diesem Fall werden bei der Beschreibung der Risikoanalyse für das (Gesamt)system entsprechende Begründungen gegeben. Anzumerken ist, dass eine Verringerung des Gesamtrisikos durch Komposition nicht auftreten kann, da bei der Analyse der einzelnen Komponenten deren Rolle im (Gesamt)system bereits berücksichtigt wird (insbesondere Berücksichtigung von Schutzmaßnahmen, wie oben erläutert). Werden also beispielsweise über eine ungesicherte Schnittstelle nur Ende-zu-Ende gesicherte Daten ausgetauscht, so wird (bezüglich Vertraulichkeit und Integrität) von einem geringen Risiko ausgegangen.

Abschließend sei nochmals darauf hingewiesen, dass die konkreten Einschätzungen bezüglich eines hohen, mittleren bzw. niedrigen Risikos nicht „mathematisch beweisbar" sind, sondern oftmals eine gewisse subjektive Bewertung enthalten. Dies ergibt sich auch aus der Tatsache, dass im Rahmen der zur Verfügung stehenden Zeit und Ressourcen nicht jedes denkbare Szenario detailliert analysiert werden konnte. Dies betrifft beispielsweise den Angreifer Insider, der insofern eine vergröbernde Verallgemeinerung darstellt, als das bei einer detaillierteren Betrachtung bezüglich jeder einzeln O-RAN-Komponente untersucht werden könnte, welche Sicherheitsrisiken sich ergeben, wenn eben genau die jeweils betrachtet O-

RAN-Komponente böswillig ist. Der Leser ist also gehalten, die textlichen Anmerkungen zu den einzelnen Risiken zu berücksichtigen. Diese sind im Zweifelsfall maßgeblich bezüglich der Risikoeinschätzung.

4 Existierende Studien

In der Literatur existieren einige Studien, die sich mit Bedrohungen, Schwachstellen und Risiken bezüglich des 5G-Gesamtsystems sowie einzelner Komponenten, wie etwa dem 5G-RAN, beschäftigen. Nachfolgend wird eine Auswahl davon kurz vorgestellt. Besonders erwähnt sei dabei die von der O-RAN Alliance veröffentlichte Bedrohungsanalyse.

4.1 ENISA Threat Landscape for 5G Networks

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat im Dezember 2020 eine Aktualisierung ihrer Bedrohungsanalyse [40] bezüglich 5G vom November 2019 [41] veröffentlicht. In der aktuellen Bedrohungsanalyse werden eine Vielzahl von Bedrohungen für 5G-Systeme vorgestellt, gruppiert gemäß 5G-Komponenten und 5G-Funktionalitäten. Dabei erfolgt auch eine Bedrohungsanalyse spezifisch bezüglich des 5G-RANs — wenngleich auch nicht unter Einbeziehung von O-RAN.

Als wesentliche Bedrohungen wurden dabei identifiziert:

- Beeinträchtigung der Quality-of-Service bezüglich der Ultra-Reliable Low-Latency Communication (URLLC) Anwendungsfälle. Diese Bedrohung wird lediglich erwähnt— es bleibt jedoch unklar, aus welchen konkreten und detailliert aufgeführten Bedrohungen sich diese Einschätzung ableitet.
- Stören der Funkübertragung mittels Störsender (Jamming).
- „*Failure to meet General Security Assurance Requirements: a set of weaknesses will arise through the update requirements of various elements of RAN due to implementation of migration steps and the ability of early-deployed systems to comply with specification updates regarding security functions.*“ Hier bleibt unklar, was genau gemeint ist. Auch bleibt unklar, aus welchen der detailliert aufgeführten Bedrohungen sich diese Bedrohung ableitet. Vermutet wird, dass darauf Bezug genommen wird, dass in Praxis auch neuere Systeme abwärtskompatibel mit älteren, unsicheren Standards sein müssen und sich daher Schwachstellen auch in diesen neueren Systemen und Komponenten befinden.
- Angriffe auf die F1-Schnittstelle auf Grund der nur optionalen Sicherheitsmaßnahmen

Darüber hinaus werden eine Vielzahl mehr oder weniger allgemeiner Bedrohungen aufgeführt, die daher — obwohl im konkreten für das 5G-RAN illustriert — nicht spezifisch für 5G-RAN sind. Dazu zählen etwa Implementierungsfehler (in den diversen Komponenten einschließlich der verwendeten Hardware/Software), Konfigurationsfehler, das Nichtanwenden von vorgesehenen (kryptographischen) Sicherheitsmaßnahmen, ein unberechtigter Zugriff auf Geheimnisse, die beispielsweise im Rahmen kryptographischer Sicherungsmaßnahmen zum Einsatz kommen (geheime kryptographische Schlüssel). Die identifizierten Bedrohungen werden in Anhang E des ENISA-Dokuments aufgeführt, wobei eben auffällt, dass die meisten angegebenen Bedrohungen auch ohne den 5G-Kontext relevant sind (etwa: „*Improper authorisation and access control policy: The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.*“).

4.2 EU 5G Risikoanalyse

Im Oktober 2019 hat die NIS Cooperation Group einen Bericht zur 5G-Risikoanalyse veröffentlicht [42]. Grundlage des Berichtes ist eine Befragung der EU-Mitgliedsstaaten bezüglich einer Einschätzung der 5G-Risiken. In dem Bericht werden lediglich sehr allgemeine Risiken aufgeführt —eine detailliertere Bedrohungsanalyse wird von der ENISA mit dem in Kapitel 4.1 beschriebenen Bericht geliefert.

Das Risiko für das Radio Access Network wurde mit „hoch“ eingeschätzt, der zweit höchsten Stufe (hinter „kritisch“). Konkrete Informationen, wie es zu dieser Einschätzung kam, lassen sich dem Bericht nicht entnehmen.

Bezüglich der allgemeinen Risiken, die in dem Bericht behandelt werden, ist für die vorliegende Studie die fehlende Diversität und die damit verbundene Abhängigkeit von wenigen Herstellern besonders relevant, da gerade Open RAN als ein Ansatz verstanden werden kann, diesem Risiko zu begegnen. Zusätzlich wird in der Risikoanalyse an verschiedenen Stellen auf das Risiko durch staatliche Angreifer hingewiesen, die versuchen könnten, Hersteller von 5G-Komponenten zu beeinflussen, so dass diese böswillige 5G-Komponenten liefern. Auch hier könnte Open RAN ein sinnvoller Bestandteil der Gegenmaßnahmen sein.
Darüber hinaus sind allgemeine Risiken, die in dem Bericht erwähnt werden, wie beispielsweise Fehlkonfigurationen und unzureichende Zugriffskontrolle auch für das Radio Access Network und hier insbesondere auch für O-RAN relevant.

4.3 EU Toolbox

Basierend auf den in den Kapiteln 4.1 und 4.2 erwähnten Berichten zu Risiken und Bedrohungen bezüglich 5G hat die NIS Cooperation Group im Januar 2020 einen Vorschlag zu allgemeinen Gegenmaßnahmen zur Verminderung der Risiken vorgelegt [43]. Dieser Vorschlag ist unter dem Begriff „EU Toolbox“ bekannt. Die Gegenmaßnahmen werden dabei in drei Gruppen eingeteilt: strategische, technische und unterstützende.
Bezüglich der strategischen Gegenmaßnahmen sind im Zusammenhang mit dieser Studie insbesondere relevant:

- *SM05*: Diversität der Hersteller von 5G-Komponenten
- *SM08*: Vielfalt bei zukünftigen Netztechnologien; Aufbau von EU-Expertise auf diesem Gebiet

Die Vergrößerung der Diversität und die Verringerung der Abhängigkeit von einzelnen Herstellern wird dabei an vielfältigen Stellen und in unterschiedlichsten Zusammenhängen erwähnt, was die Rolle von Diversität als eine sehr wesentliche Gegenmaßnahme unterstreicht.
Wie oben bereits erwähn kann Open RAN einen Beitrag zur Umsetzung dieser beiden strategischen Gegenmaßnahmen darstellen. Insofern ist es wichtig, die mit Open RAN/O-RAN neu hinzukommenden Risiken zu evaluieren, um letztendlich einschätzen zu können, ob Open RAN/O-RAN Teil der Lösung oder Teil des Problems ist bzw. welche Maßnahmen getroffen werden müssen, damit Open RAN /O-RAN Teil der Lösung und nicht Teil des Problems ist bzw. wird.
Die 11 in der EU-Toolbox empfohlen technischen Gegenmaßnahmen betreffen im Wesentlichen die vollumfängliche Anwendung von üblichen IT-Sicherheitsmaßnahmen. Insofern gilt es auch hier zu analysieren, inwiefern O-RAN diese Empfehlungen bezüglich technischer Gegenmaßnahmen umsetzt.
Bezüglich der unterstützenden Gegenmaßnahmen sei hier die Maßnahme *SA03* „Beteiligung an 5G Standardisierung“ erwähnt, da ein damit verfolgtes Ziel wiederum die Erhöhung der Diversität durch das Schaffen von wohl definierten Schnittstellen ist.

4.4 US-amerikanische Studien und Berichte

Im US-amerikanischen Bereich existieren eine ganze Reihe von Initiativen und Berichten, die sich mit 5G-Risiken und entsprechenden Maßnahmen auseinandersetzen. Dazu gehören unter anderem:

- „CISA 5G Strategy“ [44]
- „Potential Threat Vectors to 5G Infrastructure“ [45]
- „National Strategy to Secure 5G“ [46]
- „National Strategy to Secure 5G Implementation Plan“ [47] (einschließlich der als separates Dokument veröffentlichten Anhänge [48])

Neben den „üblichen“ Risiken und Bedrohungen, die sich auch in einer Vielzahl Dokumenten von anderen Staaten und Organisationen finden, treten zwei Risiken und zugehörige

Maßnahmen hervor, welche auch gleichzeitig in Bezug zu den Untersuchungen dieser Studie stehen. Dabei handelt es sich um:

- Supply Chain Risiken, insbesondere auch, weil gerade bezüglich des 5G-RAN aktuell US-amerikanische Abhängigkeit von internationalen Herstellern besteht (im „National Strategy to Secure 5G Implementation Plan“ werden dabei als Hersteller genannt: Huawei, Ericsson, Nokia, Samsung und ZTE—wobei Huawei und ZTE als nicht-vertrauenswürdig eingestuft werden und somit effektiv nicht als Ausrüster in Frage kommen).
- Risiken durch die Beeinflussung von Standardisierung.

Zur Minimierung dieser Risiken werden eine Vielzahl von Gegenmaßnahmen beschrieben, die zusammengefasst den folgenden zwei Zielen dienen:

- Erhöhung der Diversität bezüglich 5G-Komponenten-Herstellern, idealerweise dabei ein hoher Anteil US-amerikanischer Hersteller
- Führerschaft im Bereich der Standardisierung, um die Entwicklung von Standards entsprechend der US-amerikanischen Interessen zu beeinflussen

Dabei wiederum wird Open RAN/O-RAN als eine konkrete Möglichkeit angesehen, um die genannten beiden Ziele zu erreichen bzw. deren Umsetzung zu befördern.

4.5 „The Prague Proposals“

„The Prague Proposals“[11] ist ein Dokument, welches im Ergebnis der ersten Prager 5G-Sicherheitskonferenz[12] entstand. Es enthält einige allgemeine Empfehlungen bezüglich der Absicherung und des Roll-outs von 5G-Netzen. Dabei ist anzumerken, dass die Empfehlungen derart allgemein gehalten sind, dass sie nicht nur auf 5G-Netze zutreffen, sondern im Prinzip auf jegliche IT-Infrastruktur („*Communication networks and service should be designed with resilience and security in mind*.“, „*Stakeholders should regularly conduct vulnerability assessments*.“, „*Risk management framework... should be implemented*.“ etc.). Darüber hinaus werden Supply Chain Risiken und die Notwendigkeit von Diversität bezüglich Herstellern von 5G-Komponenten betont. Erwähnenswert sind die „Prague Proposals“ vor allem deshalb, weil sie in einer Reihe der US-amerikanischen Dokumente und Berichte (siehe Kapitel 4.4) als Grundlage referenziert werden.

4.6 O-RAN Security Threat Modeling and Remediation Analysis

Wie bereits erwähnt, hat die O-RAN Alliance selbst vor kurzem (Juli 2021) ein Dokument veröffentlich, welches sich mit Bedrohungen und Risiken bezüglich O-RAN beschäftigt [49]. Den Analysen liegt dabei ein Vorgehen gemäß ISO 27005 zu Grunde. Verbindliche Maßnahmen zur Risikominimierung sind in der aktuellen Version des Dokuments nicht festgelegt. Dies ist aber für eine zukünftige Version geplant.

Im Dokument selbst sind zahlreiche Bedrohungen aufgeführt. Einige von diesen wurden auch bei der in dieser Studie durchgeführten Risikoanalyse berücksichtigt. Viele der aufgeführten Bedrohungen sind allerdings auch eher allgemeiner Natur und nicht (O-)RAN spezifisch, was den Autoren der O-RAN Alliance Studie bewusst ist. Dadurch ist nur eine Untermenge der Bedrohungen O-RAN spezifisch, wobei ein spezieller Fokus auf den Open Fronthaul Schnittstellen (CUS, M-Plane) liegt und andere Schnittstellen (O1, O2 etc.) (möglicherweise vorrübergehend) eher unbeachtet sind.

Ein großer Unterschied zwischen der O-RAN eigenen Risikoanalyse und der hier vorliegenden ist die Betrachtungsweise, was ein Risiko überhaupt ist. In O-RAN wird im aktuellen Dokument lediglich der „Impact“ des Risikos identifiziert, jedoch nicht die Eintrittswahrscheinlichkeit, wohingegen in der hier vorliegenden Studie genau umgekehrt vorgegangen wirds: Es wird nur

[11] https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf
[12] https://www.prague5gsecurityconference.com/

die Eintrittswahrscheinlichkeit betrachtet. Allerdings soll eine einer zukünftigen Version der O-RAN eigenen Risikoanalyse auch die Eintrittswahrscheinlichkeit berücksichtigt werden.
Die „Impact“ Klassen werden in gering, mittel und hoch klassifiziert, wobei hier die Anzahl der beeinträchtigten Komponenten (O-DUs, O-RUs etc.), die Schwere der Bedrohung gegenüber den jeweiligen Schutzzielen (Privacy, Confidentiality, Integrity, Availability) und die Auswirkungen auf mögliche Synchronisierungstopologien (Clock Model) mit einfließt.
Als Ergebnis identifiziert die O-RAN Alliance 32 Bedrohungen als hoch, 16 als mittel und 5 als gering in ihren Auswirkungen. Es bleibt abzuwarten, wie die O-RAN Alliance die Eintrittswahrscheinlichkeit[13] von diesen Bedrohungen einschätzt, ebenso inwiefern die anderen existierenden Schnittstellen (O1, O2 etc.) noch untersucht werden.

4.7 GSMA Mobile Telecommunications Security Landscape

Der im März 2021 veröffentlichte Report [50] von der GSMA (Global System for Mobile Communications Association) befasste sich mit den aus ihrer Sicht wichtigen und teilweise neuen Veränderungen in der Sicherheitslandschaft der Mobilfunkindustrie. Der Report befasste sich mit:

- „Signalling & Inter-connect“
- „Supply Chain“
- „Software & Virtualisation“
- „Cyber & Operational Security“
- „Security Skills Shortage“
- „Device & IoT“
- „Cloud Security“
- „Securing 5G“

Die meisten Risiken, die aus den Themengebieten abgeleitet wurden, sind im Report durch allgemeine Maßnahmen entschärft. Um die Gefahren aus dem Bereich “Cyber & Operational Security” beispielsweise zu verringern, wird folgendes geraten: *„Good security practices can mitigate this risk through secure networks, strong authentication, least privilege practices alongside strong privileged access management (PAM).”* [50]. Diese stellen (wie schon erwähnt) jedoch nur generelle Richtlinien dar und eignen sich daher weniger für die konkrete Gefahrenprävention, da diese wesentlich konkreter auf die Domäne sein muss.
In Bezug auf 5G wird im Report darauf hingewiesen, dass zwar 5G viele Sicherheitslücken durch die Architektur geschlossen hat, die entsprechenden Sicherheitsmaßnahmen aber in der Praxis noch nicht immer vollständig umgesetzt wurde. Die Autoren begründen dies damit, dass die meisten Architekturen von 5G noch keinen 5G Kern besitzen; *„At present Non Stand Alone deployments are not making full use of the standards based security, as much of this only comes when a 5G core (5GC) is deployed.*“ [50].
Wie auch bei den vorherigen Studien wird das Risiko im Bereich „Supply Chain“ auch in dem Report beleuchtet, nicht zuletzt wegen immer mehr nationalen Eingriffen: *„In 2020, we saw an increasing trend towards national responses to supply chain threats.“*
Als generelle Richtlinien empfiehlt die GSMA Komponenten von verschiedenen Herstellern einzeln hinsichtlich der der von ihnen ausgehenden Risiken zu untersuchen. Insbesondere wird empfohlen, konkrete Pläne für den Fall aufzustellen, dass ein konkreter Hersteller und damit seine Komponente aus dem Netz entfernt werden muss: *„Build business continuity plans that consider the removal of critical vendors; understand the impact if one were to be removed.“*[50]. Es wird ebenfalls empfohlen, sich mit Open Network Solutions zu befassen und in Testumgebungen diese auszuprobieren.

[13] In internen Dokumenten der ORAN werden diese schon diskutiert, allerdings sind diese noch nicht veröffentlicht, weswegen hier darauf kein Bezug genommen wird.

Generell lässt sich feststellen, dass keine der im Report vorgestellten Risiken 5G-RAN spezifisch sind. Sie zeigen keine konkreten Risiken auf, die beispielsweise von Schnittstellen oder Komponenten eines 5G-Netzes ausgehen. Die Richtlinien befassen sich vorwiegend mit Risiken, die generell auf viele Infrastrukturen auch außerhalb von Mobilfunknetzwerken vorzufinden sind.

5 O-RAN Risikoanalyse

In den nachfolgenden Kapiteln wird die Risikoanalyse bezüglich O-RAN hergeleitet. Dabei erfolgen in Kapitel 5.1 Betrachtungen bezüglich der Angreifer „Cloud-Betreiber“ und „RAN-Betreiber“ zusammenfassend bezüglich des gesamten O-RAN. Dies geschieht im Wesentlich auf Grund der herausgehobenen Position dieser beiden Entitäten/Angreifer.
Für die anderen Angreifer erfolgt die Risikoanalyse zunächst separat bezüglich der einzelnen in O-RAN spezifizierten Schnittstellen und Basis-Bausteine. Daraus wird dann in Kapitel 5.15 eine Gesamtrisikoanalyse abgeleitet. Dabei wird jeweils das höchste Risiko aus den jeweiligen Einzelbetrachtungen als Gesamtrisiko übernommen (siehe auch Kapitel 3.2), da es aus Angreifersicht ausreichend ist, eine im System vorhandene Schwachstelle erfolgreich für Angriffe ausnutzen zu können — vereinfacht gesagt ist das schwächste Glied in der Kette das entscheidende bezüglich einer Risikoanalyse.
Anzumerken ist darüber hinaus, dass die Ergebnisse der Risikoanalyse bezüglich des 3GPP-RANs (Anhang A:) in die Risikoanalyse bezüglich O-RAN eingeflossen sind, da O-RAN als Umsetzung eines 3GPP-RANs manche der sich aus den 3GPP-Standards ergebenden Sicherheitsrisiken wie auch positive Effekte auf Grund von 3GPP-Sicherheitsmaßnahmen „erbt“.

5.1 Angreifer: Cloud-Betreiber und 5G-RAN-Betreiber

Die Angreifer „Cloud-Betreiber“ und „5G-RAN-Betreiber“ haben herausgehobene Positionen. Beide haben letztlich die volle Kontrolle über das RAN: der 5G-RAN-Betreiber bestimmungsgemäß, der Cloud-Betreiber, da die aktuellen O-RAN Spezifikationen keine Sicherheitsmaßnahmen bezüglich nicht-vertrauenswürdiger Cloud-Betreiber vorsehen. Vielmehr wird einfach von vertrauenswürdigen Cloud-Betreibern ausgegangen: „*Administrators, integrators, operators and orchestrators must be trustworthy, …*“ [49].
Insofern ergeben sich bezüglich des Angreifers „Cloud-Betreiber“ keine Unterschiede bezüglich der O-RAN-bezogenen best-case/worst-case Betrachtungen. Ähnliches gilt auch für den Angreifer „RAN-Betreiber“, der unter anderem die volle Kontrolle über die O-RAN Sicherheitsmaßnahmen hat. Daher werden nachfolgend generell nur worst-case (*ww*) und best-case (*bb*) Betrachtungen durchgeführt.
Worst-case: Sind keinerlei der als optional spezifizierten 3GPP- bzw. O-RAN-Sicherheitsmaßnahmen umgesetzt, so ist für alle Schutzziele und für alle Stakeholder das Risiko einer Schutzzielverletzung als hoch einzuschätzen, da in diesem Fall der Cloud-Betreiber/5G-RAN-Betreiber vollen Zugriff auf alle verarbeiteten Daten und die volle Kontrolle über die Datenverarbeitung selbst hat. Einzige Ausnahme stellt hier die Ende-zu-Ende-Sicherung der Control Plane Daten bezüglich Integrität da. Die verbessert die Situation für die 3GPP-Control-Plane Daten – die O-RAN internen Konfigurations- und Managementdaten sind aber ungeschützt, weswegen sich in Summe ein mittleres Risiko ergibt.
Best-case: Auch der best-case ergibt nur eine unwesentlich bessere Situation. Für alle Stakeholder stellt die Verletzung des Schutzziels Verfügbarkeit ein hohes Risiko dar. Bezüglich der Perspektive „End-Nutzer“ End-Nutzers ist darüber hinaus auch von einer Verletzung der Schutzziele Vertraulichkeit, Integrität, Privacy und Zurechenbarkeit auszugehen, da die kryptographischen Schlüssel zur Absicherung der Luftschnittstelle (Uu) dem RAN bekannt sind. Auf Grund des flächendeckend leicht durchzuführenden Angriffs wird auch bzgl. des Stakeholders „Staat“ ein hohes Risiko bezüglich der Verletzung der Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Privacy gesehen. Für den Stakeholder „Telco“ — also speziell die Control Plane Perspektive — stellt sich die Situation leicht besser dar, da die entsprechenden Control Plane Nachrichten (NAS) zwischen UE und Core-Netz Ende-zu-Ende gesichert sind (zwischen UE und 5G-Core). Allerdings sind Manipulationen an den O-RAN spezifischen Konfigurations- und Managementdaten möglich, so das insgesamt von einem mittleren Risiko ausgegangen wird.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer						Staat						Netzbetreiber					
	Schutzziele						Schutzziele						Schutzziele					
	C	I	A	Z	P		C	I	A	Z	P		C	I	A	Z	P	
Cloud-Betreiber																		
RAN-Betreiber																		

Tabelle 2: Risikobewertung für die Angreifer "Cloud-Betreiber" und "RAN-Betreiber" bezüglich der gesamten O-RAN Architektur

5.2 Risikoanalyse O-Cloud

Die O-Cloud ist die zentrale Ausführungsumgebung der O-RAN-Komponenten. Wie oben bereits erwähnt entstehen durch einen nicht-vertrauenswürdigen Cloud-Betreiber sehr hohe Sicherheitsrisiken. Gleiches gilt im Falle einer durch den Angreifer kompromittierten O-Cloud. Insofern sind wirkungsvolle Sicherheitsmaßnahmen wie etwa Zugriffskontrolle und Separierung von entscheidender Bedeutung. Die O-RAN-Spezifikationen machen hier nur wenige Vorgaben bzw. enthalten sogar sicherheitskritische Anforderungen.

So befindet sich etwa in der „Security Requirements“ Spezifikation [51] die nur empfohlene Anforderung nach Zugriffskontrolle: „*User should be authenticated and authorized*.“ Positiv ist hier zu erwähnen, dass Isolationsmechanismen durchaus gefordert werden: „*Means of isolation of control and resources among different users shall be implemented*“ – wobei derartige Isolationsmechanismen ohne ein gleichzeitig zwingend vorgeschriebene Nutzerauthentikation wirkungslos sind.

Im O-RAN-worst-case ergibt sich somit bezüglich des Angreifers „Außenstehender“ eine Risikosituation, die mit der Situation bezüglich des Angreifers „RAN-Betreiber“ vergleichbar ist, da eine kompromittierte O-Cloud im Wesentlichen gleichzusetzen ist mit der vollen Kontrolle über die O-RAN-Komponenten.

Der best-case aus O-RAN Sicht lässt sich aktuell nicht einschätzen, da es bezüglich der O-Cloud praktisch keine Sicherheitsvorgaben gibt.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer						Staat						Netzbetreiber					
	Schutzziele						Schutzziele						Schutzziele					
	C	I	A	Z	P		C	I	A	Z	P		C	I	A	Z	P	
Außenstehender																		
Nutzer																		
Insider																		

Tabelle 3: Risikobewertung der O-Cloud

5.3 Risikoanalyse O2-Schnittstelle

Wie in Kapitel 2.3.2 beschrieben, dient die O2-Schnittstelle zur Konfiguration der O-Cloud und dem Deployment der RAN-Komponenten von O-RAN, also der VNFs. Die O2-Schnittstelle kann insofern als sehr „mächtig“ angesehen werden, da mit ihrer Hilfe die gesamte Ausführungsumgebung und die ausgeführten Software-Komponenten bestimmt werden können. Dies gilt umso mehr, da die in den O-RAN Dokumenten zu findenden Deployment-Szenarien und Use-Cases sehr viel Flexibilitäten vorsehen und insofern die O2-Schnittstelle genügend mächtig sein muss, um diese Dynamik zu unterstützen. Unberechtigte Zugriffe auf die O2-

Schnittstelle bergen insgesamt das Potential einer Kompromittierung des RAN, d. h. ermöglichen einem Angreifer eine vollständige Kontrolle über das gesamte RAN.
Eine detaillierte Risikobewertung gestaltet sich aktuell als schwierig, da bezüglich der O2-Schnittstelle lediglich Anforderungen beschrieben sind bzw. spezifiziert ist, welche Dienste mit Hilfe der O2-Schnittstelle zur Verfügung gestellt werden sollen. Es ist aber nicht spezifiziert, wie genau die Schnittstelle ausgestaltet ist, d. h. welche konkreten Protokolle zum Einsatz kommen etc. („*The O2 services and their associated interfaces shall be specified in the upcoming O2 specification.*“ [27])
Das die O2-Schnittstelle gesichert werden muss, ist den Autoren der O-RAN-Spezifikationen durchaus bewusst, da sie die generelle Anforderung `REQ-O2-GEN-TLS-FUN-1` und `REQ-SEC-O2-1` definiert haben. Allerdings sind diese recht „weich“ formuliert: „*Management Service providers and consumers that use TLS shall support TLS v1.2 or higher.*“ [26]. Die Verwendung von Sicherheitsprotokollen (konkret TLS) ist also nicht prinzipiell vorgeschrieben — es wird lediglich eine minimale TLS-Version festgelegt, falls TLS zum Einsatz kommt. Insofern ist die zugehörige, erklärende Beschreibung: „*Communications between SMO and O-Cloud are secure.*“ [26] als irreführend zu bezeichnen und stellt eher den Ausdruck eines Wunsches als einer aus der Spezifikation ableitbaren Tatsache bzw. Anforderung dar.
Neben der reinen Absicherung der Verbindung, etwa mit Hilfe von TLS ist es ferner wichtig, genau festzulegen, welche Komponenten bzw. welche Rollen welche Management- und Deployment-Services nutzen dürfen. Darauf basierend muss dann ein entsprechendes Rechtemanagement und eine zugehörige Zugriffskontrolle umgesetzt werden. Wichtig dabei ist, dass die O2-Schnittstelle so ausgestaltet wird, dass eine Umsetzung des Least-Privilege-Prinzips auf natürliche Weise unterstützt wird, d. h., dass die Schnittstelle wohl definierte Funktionalitäten mit wohl definierten Parametern anbietet, welche ein hinreichend feingranulares Rechtemanagement ermöglichen. Das Gegenteil von dem wäre eine eher allgemeine Schnittstelle, beispielsweise Remote-Zugriff mittels SSH, da hier eine klare Bestimmung der Möglichkeiten eines prinzipiell Berechtigten bzw. die Umsetzung entsprechender Restriktion seiner Möglichkeiten sehr aufwendig und fehleranfällig sind.
Die genaue Ausgestaltung der O2-Schnittstelle ist wie angemerkt unklar — allerdings existiert eine von der O-RAN Software Community bereitgestellte Referenzimplementierung. Diese basiert auf einer Reihe existierende Softwarekomponenten wie beispielsweise OpenStack, Kubernetes und ONAP. Allein diese Basiskomponenten besitzen eine hohe Komplexität, so dass Fehlkonfigurationen wahrscheinlich sind [52], welche wiederum im Falle einer wenig restriktiven O2-Schnittstelle eine Schwachstelle darstellen und Potential für Angriffe sind, etwa im Bereich der Rechteausweitung.
Bezüglich der definierten Perspektiven, Angreifer und Schutzziele ergibt sich insgesamt folgende Einschätzung:
O-RAN-Worst-Case/3GPP-Worst-Case (*ww*): Da keine Sicherheitsmechanismen zwingend vorgesehen sind, kann selbst ein Außenstehender auf die O2-Schnittstelle zugreifen und auf Grund ihrer Mächtigkeit die komplette Kontrolle über das RAN übernehmen. Dies ermöglicht eine Verletzung des Schutzziels Verfügbarkeit bezüglich aller betrachteten Stakeholder. Bezüglich des End-Nutzers ist zusätzlich von einer Verletzung der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten auszugehen, da der Angreifer Kontrolle über die relevanten Verschlüsselungsschlüssel erlangen kann. Ebenso ist bezüglich des 5G-Netzbetreibers/Telcos mit Verletzungen der Schutzziele Vertraulichkeit, Zurechenbarkeit und Privacy zu rechnen. Dies betrifft alle bezüglich des O-RAN relevanten Daten, wie etwa Konfigurationsdaten einschließlich kryptographischer Schlüssel, Modelle aus dem Bereich des maschinellen Lernens, O-RAN-Softwarekomponenten (einschließlich rApps und xApps), Log-Dateien etc. Da ein entsprechender Angriff leicht großflächig ausgeführt werden kann, ist auch für den Stakeholder „Staat“ von einem hohen Risiko bezüglich aller Schutzziele auszugehen. Hier bildet allerdings die Integrität aus Sicht des Netzbetreibers eine Ausnahme: Trotz

kompletter Übernahme des RAN sollten die Control Plane Daten zwischen UE und AMF durch die verpflichtende Integritätssicherung mittels 3GPP-Mechanismen gesichert sein.

O-RAN-Worst-Case/3GPP-Best-Case (*wb*): Hier ist die Einschätzung der Risiken analog zu der zum worst-case/worst-case Fall. Allerdings werden die Control Plane Daten durch die 3GPP-Vorgaben zwischen UE und AMF im best case verschlüsselt, wodurch das Risiko für das Schutzziel Vertraulichkeit bezüglich des Stakeholders „Telco“ als „mittel“ eingestuft werden kann. Mittel deshalb, da die sonstigen O-RAN spezifischen Control Plane Daten ungeschützt sind.

O-RAN-Best-Case/3GPP-Best-Case (*bb*): Da alle optionalen Sicherheitsmaßnahmen in diesem Fall umgesetzt werden, ist im best-case von einer geringen Eintrittswahrscheinlichkeit bezüglich erfolgreicher Angriffe von Außenstehenden und Nutzern unter Ausnutzung der O2-Schnittstelle auszugehen. Bezüglich des Angreifers „Insider“ ist demgegenüber von einer hohen Wahrscheinlichkeit auszugehen. Da konkrete Aussagen zu einem Rechtemanagement und zu einer feingranularen Zugriffskontrolle auf die O2-Schnittstelle fehlen, ist aktuell davon auszugehen, dass Insider-Angreifer vergleichsweise leicht eine Ausweitung ihrer Rechte vornehmen können. Dies trifft insbesondere zu, wenn es sich bezüglich der durch den Insider kompromittierten Komponente um das SMO-Framework handelt.

Durch die Absicherung im O-RAN Bereich sollte das Risiko einer Verletzung des Schutzzieles Verfügbarkeit sinken, da triviale Zugriffe von außen und durch den Nutzer auf die O2 Schnittstelle nicht mehr möglich sein sollten.

O-RAN-Best-Case/3GPP-Worst-Case (*bw*): Hier sind die Risiken für die Schutzzielverletzungen analog zu dem best-case/best-case Fall einzuschätzen. Lediglich werden hier keine Control Plane Daten zwischen UE und AMF verschlüsselt, wodurch sich das Risiko von „mittel“ auf „hoch“ verändert.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer					Staat					Netzbetreiber							
	Schutzziele					Schutzziele					Schutzziele							
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P			
Außenstehender																		
Nutzer																		
Insider																		

Tabelle 4: Risikobewertung der O2-Schnittstelle

5.4 Risikoanalyse O1-Schnittstelle

Wie in Kapitel 2.3.1 beschrieben, dient die O1-Schnittstelle dem Management sämtlicher O-RAN-Komponenten (außer der Management-Komponente selbst). Ein Zugriff auf diese Schnittstelle ermöglicht einem Angreifer entsprechend weitreichende Zugriffe, die nur geringfügig weniger mächtig sind als unberechtigte Zugriffe mit Hilfe der O2-Schnittstelle.

Allerdings existiert für diese Schnittstelle mehrere Spezifikationen: Einerseits [17], die sich generell mit der O1-Schnittstelle befasst und andererseits beispielsweise [53], die vertiefend die Verbindung zwischen O-DU und SMO mit Hilfe der O1-Schnittstelle untersucht. Letztere ist insbesondere deshalb relevant im Kontext der Studie, da sie bezüglich Sicherheitsanforderungen und -maßnahmen über die allgemeine O1-Schnittstellenbeschreibung hinausgeht. Dementsprechend wird nachfolgend ebenfalls eine Fallunterscheidung durchgeführt.

5.4.1 Risikoanalyse der allgemeinen O1-Schnittstelle

Für die O1-Schnittstelle sind optionale Sicherheitsmaßnahmen in den aktuellen Spezifikationsdokumenten vorgesehen. Konkret werden hier SSH und TLS erwähnt [25]. Darüber hinaus wird auch die Umsetzung des „Least Privilege"-Prinzips erwähnt.

Anzumerken ist, dass das „Security Requirements"-Dokument [51] im Vergleich zur eigentlichen O1-Schnitstellenspezifikation strikter formulierte Aussagen trifft: „*O1 interface will enforce confidentiality, integrity, authenticity through an encrypted transport, and least privilege access control using the network configuration access control model.*" Allerdings wird bei den konkreten Anforderungen zum Teil auch wieder nur auf ein „shall support" abgestellt – wohingegen bei den im selben Dokument zu findenden Anmerkungen zu den anzuwendenden „Security Controls" wieder striktere Aussagen getroffen werden: „*As defined in the previous section, the O1 will use TLS 1.2 or higher to enforce confidentiality, integrity, and authenticity; and will use NACM [10] to enforce least privileged access*".

In der O1-Schnittstellenbeschreibung wird zwar generell auf das „Security-Requirements"-Dokument Bezug genommen – aber nur bezüglich „Least Privilege Access Control", nicht jedoch bezüglich der Transportschichtabsicherung. Insgesamt lassen sich hier aber positive Tendenzen hin zu einer Absicherung der O1-Schnittstelle feststellen.

Auf Grund der zum Teil unklaren Formulierung wird bezüglich der allgemeinen O1-Schnittstelle jedoch weiterhin angenommen, dass im worst-cast die Sicherungsmaßnahmen nicht umgesetzt sind. Diese Entscheidung erfolgt insbesondere auch deshalb, da in den in Kapitel 5.4.2 vorgenommenen Betrachtungen zur spezifischeren Spezifikation der O1-Schnittstelle zur O-DU sich klar ergeben wird, dass hier die Sicherheitsmaßnahmen auch im worst-case anzuwenden sind. Je nach Betrachtungsweise kann insofern auch diese Einschätzung als allgemeine Einschätzung bezüglich der O1-Schnittstelle insgesamt übernommen werden.

Bezüglich der Absicherungsoptionen TLS vs. SSH muss die Verwendung von SSH als risikobehafteter angesehen werden. Dies liegt an der in Kapitel 5.1 bereits erwähnten potenziellen „Mächtigkeit" von SSH. Konkret verwendet die O1-Schnittstelle das NETCONF-Protokoll, im Falle einer Kombination mit SSH kommt daher NETCONF-over-SSH [54] zum Einsatz. Dabei wird explizit das SSH connection Protokoll [23] mit einem Kanal von Type „session" verwendet. Dieser Kanal-Typ erlaubt prinzipiell das Ausführen beliebiger Programme. Es ist aus Sicherheitssicht daher notwendig, den zugehörigen SSH-Dienst so zu implementieren bzw. zu konfigurieren, dass tatsächlich nur das NETCONF-Subsystem gestartet werden kann. Gerade für den Fall, dass die entsprechenden Beschränkungen mittels Konfiguration umgesetzt werden müssen, ergibt sich hier die Schwachstelle einer Fehlkonfiguration.

Ein weiteres Risiko ergibt sich bezüglich SSH aus der expliziten Verpflichtung, auch unsichere kryptographische Algorithmen zu unterstützen: „*O-RAN and 3GPP interfaces that implement authentication, confidentiality and integrity using SSH shall: … Enable an O-RAN deployer to configure SSH to offer less secure ciphers using standard SSH configurations to enable backward compatibility with older SSH implementations*" [55].

Ausgehend von den skizzierten SSH-basierten Risiken ist die Empfehlung, lediglich NETCONF-over-TLS [56] für die O1-Schnittstelle zu unterstützen. Insofern wird bezüglich der best-case-Analyse davon ausgegangen, dass die O1-Schnittstelle mit Hilfe von TLS 1.3 unter Benutzung von als sicher geltenden kryptographischen Algorithmen sowie gegenseitiger Authentifizierung gesichert ist.

Ebenfalls soll das NETCONF Access Control Model (NACM) optional zum Einsatz kommen, um „Least Privilege Access Control" durchzusetzen, wobei in [51] die folgenden Gruppen definiert werden:

- O1_nacm_management – Erlaubt das Ändern von Zugriffsrechten
- O1_user_management – Erlaubt das Erstellen und Löschen von Nutzern für die O1-Knoten

- O1_network_management – Erlaubt das Lesen, Schreiben und Ausführen auf der NETCONF-<running>-Datenbank, also der NETCONF-Datenbank, welche alle aktuell in Anwendung befindlichen Konfigurationsparameter speichert. Gleiches gilt auch für die NETCON-<candidate>-Datenbank (falls vorhanden), also jener NETCONF-Datenbank, die konfigurierte aber noch nicht aktivierte Parameter enthält.
- O1_network_monitoring – Erlaubt das Lesen von Konfigurationen
- O1_software_management – Erlaubt Installation neuer Software

Allerdings ist auch hier ausdrücklich die optionale Natur in den Spezifikationen anzumerken: „*Management Service providers and consumers that use NETCONF SHALL support the Network Configuration Access Control Model (NACM) […]*“ [56].

O-RAN-Worst-Case/3GPP-Worst-Case (*ww*): Da keine Sicherheitsmechanismen zwingend vorgeschrieben sind und die O1-Schnittstelle — zumindest bezüglich der (O-)RAN-Kernfunktionalität — ähnlich mächtig ist wie die O2-Schnittstelle gelten die Betrachtungen aus Kapitel 5.1 analog. Allerdings wird das Risiko einer Integritätsverletzung aus Sicht des Netzbetreibers als Mittel eingestuft. Durch die verpflichtende Integritätssicherung der Control Plane Daten (nur NAS Signale) seitens 3GPP sollte es selbst einem „Insider“ nicht möglich sein, zumindest die ausgetauschten Control Plane Daten zwischen UE und AMF unbemerkt zu verändern. Allerdings hat er nach wie vor auf die Control Plane Daten im O-ORAN Zugriff, wodurch die Integritätsverletzung als mittel eingestuft wird.

O-RAN-Worst-Case/3GPP-Best-Case (*wb*): Hier ist die Betrachtung analog zum worst-case/worst-case Fall: Da die Integritätssicherung der ausgetauschten Control Plane Daten zwischen UE und AMF verpflichtend ist, bringt der 3GPP-best-case hier keine Verbesserung gegenüber dem 3GPP-worst-case-Szenario. Zwar werden nun die User Plane Daten des UE verschlüsselt und integritätsgesichert, allerdings kann ein Angreifer über die O1-Schnittstelle auf die entsprechenden Schlüssel zugreifen, wodurch das Risiko unverändert bleibt. Ein wichtiger Unterschied ist allerdings, dass die Control Plane Daten zwischen UE und AMF in diesem Fall Ende-zu-Ende verschlüsselt sind. Daher wird hier aus Sicht des Netzbetreibers das Risiko als mittel eingeschätzt, da trotz allem die O-RAN spezifischen Control Plane Daten unverschlüsselt sind.

O-RAN-Best-Case/3GPP-Best-Case (*bb*): Auf Grund der (optional) vorgesehen Sicherheitsmaßnahmen sieht es bezüglich der O1-Schnittstelle im best-case ähnlich wie auch bei der O2-Schnittstelle besser aus. Gegenüber dem Angreifer „Nutzer“ und „Außenstehender“ wird das Risiko einer Verletzung der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit insofern als gering bezüglich aller Stakeholder eingeschätzt. Bei Verfügbarkeit wird das Risiko für alle Stakeholder als mittel eingestuft. Der Angreifer könnte durch Verfügbarkeitsangriffe auf die O1-Schnittstelle Konfigurationsänderungen und Statusmeldungen unterbinden. Dies wiederum kann in der Konsequenz zu Beeinträchtigungen der Quality-of-Service des RAN also zu erfolgreichen Verfügbarkeitsangriffen auf das RAN selber führen. Anzumerken ist hier, dass im Gegensatz zur Spezifikation der E2-Schnittstelle ein Ausfall der O1-Schnittstelle in den Spezifikationsdokumenten aktuell nicht explizit berücksichtigt wird.

Da die O1-Schnittstelle Software-Management erlaubt, kann ein Insider mit Zugriff auf diese Schnittstelle prinzipiell die ausgeführten O-RAN-Komponenten manipulieren und dadurch wie schon erwähnt Zugriff auf beispielsweise hinterlegte kryptographische Schlüssel im Fall der O-CU erlangen. Hier ist es entscheidend, wie strikt das „Least-Privileged“-Prinzip umgesetzt ist und welche Rechte ein konkreter Insider im Ergebnis tatsächlich hat. Insofern wird bezüglich eines Insiders das Risiko für die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit bezüglich der Stakeholder „Nutzer“ und „Staat“ als mittel eingeschätzt. Eine ähnliche Einschätzung ergibt sich auch für den Stakeholder „Telco“. Zwar sind hier Teile der Control Plane Kommunikation Ende-zu-Ende gesichert (und insofern vor dem Zugriff durch den Insider geschützt), allerdings bietet die O1-Schnittstelle Zugriff auf viele sensible Netzmanagement

Informationen, die aus Sicht des Netzbetreibers als schützenswert (sowohl bezüglich Vertraulichkeit als auch bezüglich Integrität/Zurechenbarkeit) anzusehen sind.

O-RAN-Best-Case/3GPP-Worst-Case (*bw*): Obwohl hier die Absicherungen durch die 3GPP-Schutzmaßnahmen nicht greifen, ergeben sich dieselben Risiken wie beim best-case/best-case Fall, da die Angreifer „Außenstehende“ und „Nutzer“ im O-RAN-best-case keinen Zugriff auf die O1-Schnittstelle haben. Bezüglich des Angreifers „Insider“ wiederum bringen die nunmehr nicht mehr vorhandenen 3GPP-Sicherheitsmassnahmen keine Verschlechterung, da sie auch im 3GPP-best-case nicht effektiv waren.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer					Staat					Netzbetreiber							
	Schutzziele					Schutzziele					Schutzziele							
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P			
Außen-stehender																		
Nutzer																		
Insider																		

Tabelle 5: Risikobewertung der allgemeinen O1-Schnittstelle

5.4.2 Risikoanalyse der O1-Schnittstelle zwischen O-DU und SMO

In [53] wird die O1-Schnittstelle zwischen O-DU und SMO für die „start up“ Installation, Software-, Konfigurations-, Performance-, Fault- und Dateimanagement genutzt.

Für die Sicherheit der Verbindung soll ***verpflichtend*** TLS für die Authentifizierung der O-DU genutzt werden, wobei der verpflichtende Charakter normalerweise selten in den Spezifikationen so zu finden ist. Zusätzlich dazu soll auch der NETCONF Datenaustausch mittels TLS ***verpflichtend*** abgesichert werden: „*In this version of O1 Interface Specification, the security of the NETCONF protocol is realized using TLS.“* [53].

Ebenfalls soll das NETCONF Access Control Model (NACM) ***verpflichtend*** zum Einsatz kommen, um „Least Privilege Access Control“ durchzusetzen. Generell findet sich in der Spezifikation hauptsächlich verpflichtende Umsetzung von Sicherheitsmechanismen im Gegensatz zu den Sicherheitsmechanismen in 5.3.1.

Es wird zwar nicht wie üblich mittels „shall“ erwähnt, dass die Schuttziele Vertraulichkeit, Integrität und Zurechenbarkeit durchgesetzt werden sollen, allerdings lässt die Formulierung: „*[…] the O1 interface will enforce confidentiality, integrity, authenticity [..] and least privilege access controll […].“* [56] den Schluss zu, dass dasselbe gemeint ist.

O-RAN-Worst-Case/3GPP-Worst-Case (*ww*): Da selbst im wort-case die Schnittstelle durch den verpflichtenden Charakter der Sicherheitsmaßnahmen gesichert ist, besteht zumindest für „Außenstehende" kaum die Möglichkeit, auf diese Schnittstelle lesend und insbesondere schreibend zuzugreifen. Die grundlegenden Verfügbarkeitsangriffe, die bestimmte Status- und Konfigurationsmeldungen unterbinden, lassen sich jedoch nicht verhindern.

Wie auch bei der allgemeinen Einschätzung der O1-Schnittstelle lässt sich auch über den Angreifer „Nutzer“ sagen, dass die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit ein geringes Verletzungsrisiko aufweisen.

Ein „Insider“ dagegen kann im worst-case die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit brechen, da die O-RAN-Schutzmaßnahmen nicht die in diesem Fall nicht vorhandenen 3GPP-Absicherungen ausgleichen können. Hier wird dabei von der O-DU als „Insider“ ausgegangen. Darüber hinaus kann ein Insider ggf. (je nach Zugehörigkeit in bzgl. Rechtegruppen) im schlechtesten Fall eigene Software auf der O-DU installieren und somit die Kontrolle über die O-DU erlangen. Dadurch ergibt sich ein hohes Risiko für die Verfügbarkeit. Allerdings kann der Insider trotz allem nicht die Integrität der Control Plane Daten zwischen UE und AMF brechen, da diese durch die 3GPP Maßnahmen verpflichtend gesichert sind.

O-RAN-Worst-Case/3GPP-Best-Case (*wb*): Da alle Maßnahmen zur Sicherung der Schutzziele verpflichtend sind, sollten die Risiken dieselben sein wie im „ww“ Fall. Aus Sicht der 3GPP Sicherung wird zusätzlich zur Integritätssicherung auch die Vertraulichkeit der Control Plane Daten zwischen UE und AMF gesichert, wodurch das Risiko als „mittel“ bei einem „Insider“ eingestuft werden kann.
O-RAN-Best-Case/3GPP-Best-Case (*bb*): Bezüglich des best-case ist die Einschätzung bezüglich der Angreifer „Außenstehender“ und „Nutzer“ durch die verpflichtende Natur der O-RAN-Sicherheitsmaßnahmen mit der des worst-case deckungsgleich. Lediglich bei dem Angreifer „Insider“ kann bezüglich der Schutzziele Vertraulichkeit, Integrität, und Zurechenbarkeit festgestellt werden, dass die 3GPP-Sicherheitsmaßnahmen eine Verletzung der Schutzziele verhindern. Bezüglich der Verfügbarkeit kann argumentiert werden, dass auch im best-case der Insider durch NACM zwar keine Schadsoftware einschleusen kann, da er die notwendigen Rechte nicht besitzt, allerdings kann er je nach Betrachtungsweise selbst die O-DU sein, wodurch er problemlos die Verfügbarkeit einschränken kann.
O-RAN-Best-Case/3GPP-Worst-Case (*bw*): In diesem Fall ist die Einschätzung der Risiken die gleiche wie bei dem vorherigen Fall „bb“. Lediglich die Vertraulichkeit ist in diesem Fall im Control Plane zwischen UE und AMF nicht durch die 3GPP abgesichert, wodurch das Risiko als „mittel“ eingeschätzt wird.

Angreifer	Perspektive (Stakeholder)															
	End-Nutzer					Staat					Netzbetreiber					
	Schutzziele					Schutzziele					Schutzziele					
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P	
Außen-stehender																
Nutzer																
Insider																

Tabelle 6: Risikobewertung der O1-Schnittstelle zwischen O-DU und SMO

5.5 Risikoanalyse A1-Schnittstelle

Wie in Kapitel 2.3.3 beschrieben, dient die A1-Schnittstelle vor allem dazu, dem Near-Real-Time RIC Richtlinien bezüglich der Konfiguration/Optimierung des RAN mitzuteilen. Dabei sind diese Richtlinien als deklarative Policies gestaltet. Ausgedrückt wird dabei, *was* erreicht werden soll, nicht jedoch, *wie* es erreicht werden soll. Die konkreten Umsetzungsentscheidungen sind insofern Teil des Near-Real-Time RICs und der xApps.
Die A1-Schnittstelle soll Möglichkeiten zur Durchsetzung von Vertraulichkeit, Integrität und Authentizität (einschließlich Schutz vor Replay-Angriffen) bieten [51]. Dazu ist für die Absicherung der Kommunikation optional TLS vorgesehen [57], [51], [49]. Eine Bedrohung bezüglich der A1-Schnittstelle ergibt sich daraus, dass zur Umsetzung einer bidirektionalen Kommunikation vorgesehen ist, dass beide Endpunkte (Non-Real Time RIC, Near-Real Time RIC) der A1-Schnittstelle als Server agieren [57]. Die sich aus den dafür notwendigen offenen Ports ergebende Angriffsfläche sollte minimiert werden, indem nur ein Endpunkt als Server agiert und eine bidirektionale Kommunikation über eine bestehende Verbindung durchgeführt wird. Zur Umsetzung können zusätzlich Techniken wie reverse connection angewendet werden.
Bezüglich der best-case/worst-case Analyse ist anzumerken, dass die entsprechenden Risiken hier im Wesentlichen von der best-case/worst-case Situation bezüglich der O-RAN-Spezifikationen abhängig sind. Auf Grund der Funktionalität der A1-Schnittstelle ist das

resultierende Risiko demgegenüber weitestgehend unabhängig von der best-case/worst-case Situation bezüglich der 3GPP-Standards.

Worst-Case: Da im worst-case die A1-Schnittstelle ungesichert ist, besteht für Außenstehende die Möglichkeit, auf diese Schnittstelle lesend und schreibend zuzugreifen. Durch entsprechend manipulierte Policies ist zumindest eine Beeinträchtigung der Verfügbarkeit (Verringerung der Servicequalität) möglich. Insofern wird bezüglich Verfügbarkeit von einem hohen Risiko für alle Stakeholder ausgegangen.

Bezüglich der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit wird für die Nutzer-Perspektive selbst im worst-case von einem geringen Risiko ausgegangen, da aktuell keine Angriffe identifiziert werden konnten, die es einem Angreifer selbst mit Zugriff auf die A1-Schnittstelle ermöglichen, lesend oder manipulierend auf die User Plane Daten zuzugreifen.

Anzumerken ist hier, dass es tiefergehender Analysen bedarf, um tatsächlich ausschließen zu können, dass über die A1-Schnittstelle keine User Plane Daten übertragen werden. Dabei ist insbesondere bei zukünftigen Versionen der Spezifikationen zu überprüfen, welche Dienste konkret über die A1-Schnittstelle angeboten werden und ob hier User Plane Daten übertragen werden.

Bezüglich der Perspektive „Telco“ ändert sich diese Einschätzung hin zu einem mittleren Risiko, da über die A1-Schnittstelle (bezüglich Vertraulichkeit und Integrität) schützenswerte Netzmanagementinformationen übertragen werden. Diese Einschätzung wurde auch für die Perspektive „Staat“ übernommen.

Best-Case: Auf Grund der Absicherung mit TLS ist es im best-case weder einem Außenstehenden noch einem Nutzer möglich, die A1-Schnittstelle bezüglich Vertraulichkeit und Integrität erfolgreich anzugreifen. Lediglich Verfügbarkeitsangriffe auf die A1-Schnittstelle sind vorstellbar. Auf Grund der Funktionalität der A1-Schnittstelle ist davon auszugehen, dass durch intelligente Verfügbarkeitsangriffe auf diese Schnittstelle die Verfügbarkeit des RAN beeinträchtigt werden kann — zumindest im Sinne einer Verringerung der Servicequalität. Dies gilt insbesondere auch deshalb, da ein Ausfall der A1-Schnittstelle in den Spezifikationen nicht explizit berücksichtigt wird. Insofern wird für alle Stakeholder hier von einem mittleren Risiko ausgegangen.

Da die Sicherheitsmaßnahmen nur Schutz gegenüber Außenstehenden vorsehen (Verbindungsverschlüsselung) — ein Rechte- und Rollenkonzept bezüglich Zugriffskontrolle auf die A1-Schnittstelle aber bestenfalls zwischen den Zeilen der Spezifikation zu erahnen ist, wird aktuell davon ausgegangen, dass ein Insider auch im best-case vollen Zugriff auf die A1-Schnittstelle hat. Für ihn stellt sich die Situation also ähnlich dar, wie im wort-case für einen Außenstehenden. Auf der anderen Seite konnten aktuell keine Angriffe identifiziert werden, mit deren Hilfe ein Insider bezüglich der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit einen signifikanten Vorteil basierend auf Zugriffen auf die A1-Schnittstelle erlangen kann. Zu beachten sind hier die oben getroffenen Anmerkungen bezüglich einer notwendigen tiefergehenden Analyse.

Angreifer	**Perspektive (Stakeholder)**																			
	End-Nutzer								Staat								Netzbetreiber							
	Schutzziele								**Schutzziele**								**Schutzziele**							
	C		**I**		**A**		**Z**		**P**		**C**		**I**		**A**		**Z**		**P**		**C**		**I**		**A**		**Z**		**P**	
Außenstehender																														
Nutzer																														
Insider																														

Tabelle 7: Risikobewertung der A1-Schnittstelle

5.6 Risikoanalyse R1-Schnittstelle

Wie in Kapitel 2.3.4 ausgeführt, dient die R1-Schnittstelle den rApps zum Zugriff auf die Non-Real-Time RIC Funktionalitäten sowie weiteren Diensten, die eine rApp zur Erfüllung ihrer Aufgaben benötigt. Dabei ist vorgesehen, dass: „*The R1 interface is the sole interface between an rApp and the functionality of the Non-RT RIC and SMO. Therefore, the R1 interface should be defined to meet all functional needs of rApps, with appropriate interface extensibility capabilities as needed.*“ [29]. Die R1-Schnittstelle ist somit als sehr mächtig anzusehen. Gleichzeitig ist sie aktuell weitestgehend unspezifiziert. Es finden sich einige allgemein Aussagen und einige Anforderungen, aber keine konkrete Ausgestaltung. Folgende Informationen sind dabei aus Sicherheitssicht relevant:

- „*it would be useful for the O-RAN Alliance to define an open and standard interface through which the Non-RT RIC exposes SMO Framework functionalities to "rApps" via the R1 Services exposure functionality. We will refer to this as the "R1" interface"* [29]
- „*capabilities are offered for consumption and usage through the R1 services. Such services include, but are not limited to: A1-related services, O1-related services, O2-related services, …*“ [29]

Die Art und Weise der Ausgestaltung der Schnittstelle ist auch unklar. Es liegt eine gewisse Vermutung nahe, dass aktuell von eher internen API-Aufrufen ausgegangen wird, die nicht über eine Netzschnittstelle zwischen verschiedenen Rechnern stattfinden. Diese Vermutung ergibt sich unter anderem daraus, dass in verschiedenen O-RAN-Dokumenten bezüglich der neuen, offenen Schnittstellen die R1-Schnittstelle nicht erwähnt wird. Umgekehrt lässt sich aus der allgemeinen Definition der R1-Schnittstelle: „*R1 Interface: Interface between rApps and Non-RT RIC framework via which R1 Services can be produced and consumed*“ [58] nicht ausschließen, dass die R1-Schnittstelle als Netz-basierte Schnittstelle umgesetzt wird. Im Rahmen dieser Studie wird daher bezüglich des best-case Szenarios davon ausgegangen, dass es sich bei der R1-Schnittstelle lediglich um interne APIs handelt, bezüglich der worst-case Betrachtung wird angenommen, dass die R1-Schnitstelle über das Netz zugänglich ist.
Sicherheitsmaßnahmen sind bezüglich der R1-Schnittstelle aktuell nicht spezifiziert. Lediglich bezüglich rApps ist erwähnt, dass der Zugriff auf R1-Dienste nur nach Authentifizierung und Autorisierung möglich sein soll. Details, wie dies umgesetzt werden soll, sind aktuell nicht spezifiziert.
Auf Grund der prinzipiellen Anbindung von O1-, O2- und A1-Diensten und da aktuell keine Einschränkungen bezüglich der Nutzung dieser Schnittstellen spezifiziert sind, werden bei der Risikoanalyse bezüglich der R1-Schnittstelle die Ergebnisse bezüglich der O1-, O2- und A1-Schnittstelle zu Grunde gelegt. Dabei wird das jeweils höchste Risiko bezüglich einer dieser Schnittstellen als untere Schranke für das betreffende Risiko bezüglich der R1-Schnittstelle angesehen — die R1-Schnittstelle kann aus Risikosicht (im worst-case) also nicht besser sein als die O1-, O2- bzw. A1-Schnittstelle.
Anzumerken ist ferner, dass für die best-case/worst-case Betrachtungen die Situation bezüglich der O-RAN-Spezifikationen maßgeblich ist. Im O-RAN-worst-case kann mit Hilfe der O1-/ O2-Schnittstelle die Kontrolle über die O-RAN-Komponenten übernommen werden. Daher können in diesem Falle gegebenenfalls umgesetzte 3GPP-Sicherheitsmassnahmen kaum greifen bzw. umgangen werden. Umgekehrt wird im O-RAN-best-case ein Missbrauch der R1-Schnittstelle verhindert – insofern spielt es eine untergeordnete Rolle, ob in diesem Fall 3GPP-Schutzmassnahmen umgesetzt sind oder nicht. Eine Ausnahme ist hier die Telco-Perspektive bezogen auf das Schutzziel Vertraulichkeit, da hier im 3GPP-best-case eine Ende-zu-Ende-Sicherung der Control Plane stattfindet, die auch im O-RAN-worst-case Schutz bietet.

Angreifer	Perspektive (Stakeholder)																			
	End-Nutzer										Staat									
	Schutzziele										Schutzziele									
	C		I		A		Z		P		C		I		A		Z		P	
Außen-stehender																				
Nutzer																				
Insider																				

Tabelle 8: Risikobewertung der R1-Schnittstelle

5.7 Risikoanalyse E2-Schnittstelle

Wie in Kapitel 2.3.5 beschrieben, dient die E2-Schnittstelle vor allem dem Management der E2-Knoten. Im Zuge dessen existiert ein Service („RAN Function Network Interface (NI)“ [59]), der es ermöglicht, mit Hilfe der E2-Schnittstelle sämtlichen Datenverkehr der Netzschnittstellen der E2-Knoten zu beobachten und zu verändern. Konkret werden unter anderem folgende Dienste angeboten:

- „*Copy of Complete message with header providing network interface type, identifier and direction with optional network interface timestamp*“
- „*Injection of Complete message with header providing target network interface type, identifier and direction and optional RIC Control Message Priority*“

Diese Dienste bergen ein hohes Risikopotential aus Sicherheitssicht.

Die gemäß Spezifikation vorgesehenen Sicherheitsmaßnahmen werden dabei aktuell als optional angesehen. Konkret wird als Anforderung definiert, dass die E2-Schnitstelle: „*shall support confidentiality, integrity and replay protection*“ [30]. Ein ähnliche Aussage findet sich auch in [51]. In [49] wird bezüglich der Absicherung IPSec vorgeschlagen: „*IPSEC: Should be used to protect E2 traffic*“ (ähnlich in [51]: „*For the security protection at the IP layer on E2 interface, IPsec shall be supported*“).

Basierend auf den funktionalen Möglichkeiten der E2-Schnittstelle und den Sicherheitsmaßnahmen erfolgt die nachfolgende Risikoeinschätzung.

O-RAN-Worst-Case/3GPP-Worst-Case (*ww*): Da im worst-case keine Sicherheitsmaßnahmen – abgesehen vom Integritäts-Schutz der Control Plane Daten – umgesetzt sind und die E2-Schnittstelle vollen Zugriff auf sämtlichen 3GPP-Datenverkehr der E2-Knoten ermöglicht, wird bezüglich eines Außenstehenden im Wesentlichen von einem hohen Risiko bezüglich Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit bezüglich aller Stakeholder ausgegangen. Bezüglich des Stakeholders „Telco“ wird auf Grund der 3GPP-Integritätssicherung der Control Plane Daten von einem mittleren Risiko ausgegangen, da gleichzeitig O-RAN spezifische (Konfigurations)Daten ungeschützt sind.

O-RAN-Worst-Case/3GPP-Best-Case (*wb*): Die Situation ändert sich hier, da die 3GPP-Sicherheitsmaßnahmen Schutz bezogen auf die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit bieten. Hier stellt sich lediglich die Frage, inwiefern der Angreifer „Insider“ Zugriff auf die Schlüssel zur Absicherung der User-Plane bzw. auf die unverschlüsselten User-Plane Daten erlangen kann. Die entsprechenden Schlüssel sind prinzipiell in der CU vorhanden. Es bedarf weiterer Analysen, um derartige Risiken mit Sicherheit ausschließen zu können, was zu der Einschätzung eines mittleren Risikos führt.

O-RAN-Best-Case/3GPP-Best-Case (*bb*): Im best-case sind die E2-Schnittstelle sowie die 3GPP-Schnittstellen gesichert. Ein Außenstehender kann somit im Wesentlichen nur Denial-of-Service Angriffe auf die E2-Schnittstelle durchführen. Für Vertraulichkeit, Integrität und Zurechenbarkeit wird daher für alle Stakeholder von einem geringen Risiko ausgegangen.

„Dumme“ DoS-Angriffe sind dabei nur von eingeschränkter Wirkung, da die ORAN-Spezifikationen vorsehen, dass das RAN funktionsfähig sein soll, auch wenn die E2-Schnittstelle ausfällt. Allerdings ist hier von einer Funktionsfähigkeit mit eingeschränkter Dienstgüte auszugehen — andernfalls bräuchte es keine E2-Schnittstelle. Darüber hinaus hängen die Auswirkungen vom konkreten Design eines E2-Knoten ab. Durch geschickt manipulierten Datenverkehr auf der E2-Schnittstelle kann ein Angreifer eine hohe Rechenlast bei einem E2-Knoten auf Grund der mit IPSec verbundenen kryptographischen Operationen erreichen. Dies könnte im Extremfall (bei nicht gut umgesetzter Separierung) dazu führen, dass nicht genügend Rechenleistung für die eigentlichen Aufgaben eines E2-Knoten zur Verfügung steht. Offen ist darüber hinaus, inwiefern „intelligente“ DoS-Angriffe zu einer stärkeren Beeinträchtigung der Servicequalität führen können. Denkbar sind hier Angriffe, die Datenpakete gezielt so verzögern, dass die Detektionsmechanismen bezüglich eines Ausfalls der E2-Schnittstelle (Timer etc.) gerade noch nicht ausgelöst werden. Darüber hinaus ist zu untersuchen, inwiefern es trotz IPSec-Verschlüsselung möglich ist, den verschlüsselten Datenverkehr einzelnen E2-Diensten bzw. E2-Funktionen zuzuordnen (etwa durch Verkehrsanalysen bezüglich spezifischer Servicekommunikationsverkehrsmuster). Dies würde die gezielte Störung einzelner E2-Dienste bzw. E2-Funktionen ermöglichen und könnte zu stärkeren Auswirkungen führen, im Vergleich zu einem kompletten „Ausfall“ der E2-Schnittstelle. Insgesamt wird daher das Risiko für Verfügbarkeit bezüglich Außenstehenden und bezüglich aller Stakeholder als mittel angesehen.

Der Angreifer „Nutzer“ ist nur in einer (aktuell) geringfügig besseren Position. Als neu hinzukommendes Risiko/neue Bedrohung ergibt sich, dass der Nutzer als prinzipiell legitim anzusehenden Datenverkehr bezüglich User Plane und Control Plane erzeugen kann. Dabei kann der Nutzer diesen Datenverkehr geschickt so gestalten, dass er in die durch die E2-Schnittstelle bereitgestellten Analyse- und Auswertungsfunktionen (bezüglich der 3GPP-Schnittstellen) mit einbezogen wird. Je nachdem wie konkret diese Analyse und Auswertungsfunktionen aussehen, kann diese Einflussmöglichkeit als „Sprungbrett“ für weitere Angriffe angesehen werden. Dies ist insbesondere dann der Fall, wenn die entsprechenden Systeme nicht mit der Prämisse entwickelt wurden, dass die aufgezeichneten Analyse- und Auswertungsdaten prinzipiell als potenziell „bösartig“ anzusehen sind. Beispielsweise könnten geschickt erstellte User Plane bzw. Control Plane Daten zu Angriffen aus dem Bereich „Bufferoverflow“ oder Injection-Angriffe (SQL-Injection etc.) benutzt werden. Eine andere Möglichkeit ist, ein auf den aufgezeichneten Daten basierendes Training von maschinellem Lernen zu beeinflussen. Insgesamt dürften derartige Angriffe zunächst primär Auswirkungen auf die Verfügbarkeit haben. Da jedoch im Rahmen der best-case Analyse prinzipiell davon ausgegangen wird, dass alle Systeme fehlerfrei arbeiten, ergibt sich insgesamt keine erhöhte Risikoeinschätzung im Vergleich zum Angreifer „Außenstehender“.

Bezüglich des Angreifers „Insider“ wird ein Angreifer unterstellt, der Zugriff auf die E2-Schnittstelle hat. Ein gutes Beispiel hierfür ist eine xApp. Zwar ist in den Spezifikationen hier und da allgemein von „Policies“ und „Berechtigungen“ bezüglich xApps die Rede — da aber jegliche Ausdifferenzierung fehlt und auch bezüglich der aktuellen Spezifikation der E2-Schnittstelle kein Rechtemanagement erkennbar ist, wird aktuell davon ausgegangen, dass auch im best-case eine xApp die E2-Schnittstelle uneingeschränkt benutzen kann. Sollte dies bezüglich einer xApp tatsächlich nicht zutreffen sein, so gilt es aller Wahrscheinlichkeit nach in jedem Fall jedoch für die Komponente „Near-Real Time RIC“.

Durch den unterstellten Zugriff auf die E2-Schnittstelle sind einem Insider leicht Verfügbarkeitsangriffe möglich, woraus sich ein hohes Risiko für alle Stakeholder ergibt. Bezüglich Vertraulichkeit, Integrität und Zurechenbarkeit kommt es bezüglich der Perspektive eines End-Nutzer darauf an, welche Komponente der Insider kontrolliert. Hat diese Komponente sowohl Zugriff auf die E2-Schnittstelle als auch Kenntnis von den bezüglich der Absicherung der Uu-Schnittstelle eingesetzten Schlüsseln, so besteht ein hohes Risiko. Sollte ein Zugriff auf die kryptographischen Schlüssel dem Insider nicht möglich sein, so besteht ein geringes Risiko.

In verallgemeinernder Konsequenz wird hier von einem mittleren Risiko ausgegangen. Diese Risikobetrachtung wird auch für den Stakeholder „Staat“ übernommen. Bezüglich des Stakeholders „Telco“ ergibt sich zwar auf der einen Seite eine etwas bessere Situation, da der Control Plane Datenverkehr Ende-zu-Ende gesichert ist. Auf der anderen Seite ermöglicht die E2-Schnittstelle: „*Exposure of selected E2 Node data (e.g. configuration information (cell configuration, supported slices, PLMNs etc.), network measurements, context information, etc.) towards the Near-RT RIC*“ [30]. Diese Daten werden zum einen als schützenswerte Betriebsgeheimnis angesehen, zum anderen wird die Umsetzung von Integrität als wichtig angesehen, da diese Daten eine Grundlage für den Netzbetrieb bilden. Insofern wird bezüglich des Telco und der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit von einem mittleren Risiko ausgegangen.

O-RAN-Best-Case/3GPP-Worts-Case (*bw*): Durch die Absicherung der E2-Schnittstelle im O-RAN-best-case ergeben sich für die Angreifer „Nutzer“ und „Außenstehender“ keine direkten Möglichkeiten, die E2-Schnittstelle für Angriffe zu nutzen. Dem Insider ermöglicht der Zugriff auf die E2-Schnittstelle bei gleichzeitig nicht vorhandenen 3GPP-Sicherheitsmassnahmen erfolgreiche Schutzzielverletzungen bezüglich nahezu aller Schutzziele und Perspektiven (Ausnahme bildet hier wieder die auch im 3GPP-worts-case vorhandene Integritätssicherung der Control Plane Daten) – es ergibt sich hier ein entsprechend hohes Risiko.

Angreifer	**Perspektive (Stakeholder)**																			
	End-Nutzer					Staat					Netzbetreiber									
	Schutzziele					**Schutzziele**					**Schutzziele**									
	C		**I**		**A**		**Z**		**P**		**C**		**I**		**A**		**Z**		**P**	
Außen-stehender																				
Nutzer																				
Insider																				

Tabelle 9: Risikobewertung der E2-Schnittstelle

5.8 Risikoanalyse Open Fronthaul M-Plane

Die Open Fronthaul M-Plane Schnittstelle erlaubt, wie in Kapitel 2.3.7 beschrieben, das Management der O-RU Komponenten. Aus Risikosicht besonders relevant ist dabei die Möglichkeit, mit Hilfe der Open Fronthaul M-Plane Schnittstelle ein Softwareupdate bezüglich der O-RU-Komponenten durchführen zu können. Dies ermöglicht es einem Angreifer prinzipiell durch Einspielen einer entsprechend manipulierten Software die volle Kontrolle über die O-RU zu übernehmen. Gemäß O-RAN-Spezifikation ist die Absicherung der Software dabei nicht festgelegt, sondern „*The use of compression and ciphering for the content of the software build is left to vendor implementation. The only file which shall never be ciphered is the manifest.xml file*“ [32]. Gerade das Manifest enthält jedoch Informationen, die vor Manipulation geschützt werden sollten. Ein spezielles Risiko ergibt sich daraus, dass mit Hilfe der Open Fronthaul M-Plane Schnittstelle die Download-URL bezüglich der zu installierenden Software frei angegeben werden kann. Hier wäre es besser, Beschränkungen vorzusehen, so dass beispielsweise der Host in der O-RU „fest“ konfiguriert ist, so dass die Auswirkungen möglicher manipulativer Eingriffe in die Übermittlung der Download-URL (Umlenkung auf einen Server unter der Kontrolle des Angreifers) in ihren negativen Auswirkungen beschränkt bleiben.

Darüber hinaus wird davon ausgegangen, dass ein Zugriff auf die Open Fronthaul M-Plane Schnittstelle erfolgreiche Angriffe auf die Verfügbarkeit erlaubt, da mit Hilfe der Open Fronthaul M-Plane Schnittstelle die in der O-RU hinterlegten Konfigurationsdaten geändert werden

können, was für die Beeinträchtigung der Servicequalität bzw. für einen vollständigen Ausfall der O-RU Funktionalität genutzt werden kann.
Im Gegensatz zu nahezu allen anderen Schnittstellen, sind die Überlegungen zur Absicherung der Open Fronthaul M-Plane Schnittstelle vergleichsweise umfangreich – und je nach Interpretation – sogar als verpflichtend vorgesehen. Konkret ist hier die Anwendung von SSH (verpflichtend unterstützt) oder TLS (optional) möglich. In Sinne der Risikominimierung sollte (wie bereits bei der O1- und O2-Schnittstelle erläutert) auf den Einsatz von SSH zu Gunsten von TLS verzichtet werden. Bezüglich der Absicherung ist eine gegenseitige Authentifizierung (mutual authentication) vorgeschrieben.
Der Interpretationsspielraum bezüglich verpflichtend *anzuwendender* Sicherheitsmechanismen ergibt sich im Wesentlichen aus den unklaren Formulierungen in den Spezifikationsdokumenten. So findet sich dort etwa die Aussage: „*The M-Plane provides end to end security as a mandatory feature.*“ [32]. Ein „Feature“ ist aber eine Eigenschaft oder Fähigkeit einer Komponente und muss insofern nicht zwingend angewendet werden. Demgegenüber wird in einer nachfolgenden Tabelle aufgeführt, dass die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit umgesetzt sind – allerdings wird als Begründung hier auch nur auf die prinzipielle Unterstützung von SSH bzw. TLS verweisen, nicht jedoch auf deren zwingende Anwendung. In der später aufgeführten Tabelle „*Mandatory and Optional Features for O-RU Authentication*“ sind alle Authentifizierungsmechanismen als „*optional to use*“ gekennzeichnet. Hier wäre es besser klarzustellen – falls dies die Absicht der Spezifikation ist – dass zwar jeder einzelne Mechanismus optional ist, dass aber mindestens einer zwingend eingesetzt werden muss.
Insgesamt ist jedoch einzuschätzen, dass die Open Fronthaul M-Plane Schnittstelle bezüglich Sicherheit sehr viele Überlegungen enthält. Anzumerken sei hier, dass die Beschreibung der Open Fronthaul Schnittstellen auch insgesamt deutlich umfangreicher im Vergleich zu den anderen Schnittstellen ausfällt.
Bezüglich Sicherheit ist darüber hinaus zu erwähnen, dass ein Rechte/Rollen-Konzept vorgesehen ist. Dabei sind 6 Rollen in der Spezifikation erwähnt:

- sudo
- smo
- hybrid-odu
- nms
- fm-pm
- swm

Bezüglich der Rechte wird unterschieden in: read, write, execute. An Hand der Rolle sind dann die Rechte für verschiedene funktionale Gruppen (in der Spezifikation als „namspace“ bezeichnet) festgelegt. Die Rolle „sudo“ besitzt dabei die meisten Privilegien. Sie ist als administrative Rolle angedacht und ermöglicht insofern Vollzugriff auf die O-RU, einschließlich der Möglichkeit Nutzer anzulegen und diesen Rollen zuzuweisen.
Als nicht so günstig wird bezüglich der aktuellen Spezifikation angesehen, dass im Auslieferungszustand ein Standard-Nutzer mit Standard-Passwort und „sudo“-Rechten vorgesehen ist. In der Literatur wird immer wieder darüber berichtet, dass derartige Standard-Zugänge Ausgangspunkt für erfolgreiche Angriffe sind—egal wie eindringlich ein Nutzer darauf hingewiesen wird, im Zuge der Ersteinrichtung die Zugangsdaten bezüglich des Standard-Nutzers zu ändern. Hier sollten Mechanismen vorgesehen werden, die eine Ersteinrichtung auch ohne bekannten Standard-Nutzernamen und bekanntes Standard-Passwort ermöglichen, etwa indem diese Daten zufällig generiert und als Dokumentation der O-RU beigefügt werden.
O-RAN-Worst-Case/3GPP-Worst-Case (*ww*): Unter der Annahme, dass die O-RAN-Sicherheitsmaßnahmen auch im worst-case zwingend vorgesehen sind, ergibt sich für die Schutz-

ziele Vertraulichkeit, Integrität und Zurechenbarkeit für alle Stakeholder bezüglich des Angreifers „Nutzer“ und „Außenstehender“ ein geringes Risiko. Auf Grund der unklaren Formulierungen und der damit verbundenen Unsicherheit, ob die O-RAN-Sicherheitsmaßnahmen wirklich zwingend umgesetzt werden müssen, erfolgt hier allerdings eine Abwertung zu einem mittleren Risiko. Ebenso wird bezüglich Verfügbarkeit wird von einem mittleren Risiko ausgegangen, da—wie auch bereits bei den anderen Schnittstellen beschrieben—Verfügbarkeitsangriffe auf die Open Fronthaul M-Plane Schnittstelle möglich sind. Da auch bezüglich der Open Fronthaul M-Plane Schnittstelle keine expliziten Aussagen bezüglicher der Tolerierung eines Ausfalls der Schnittstelle gefunden werden konnten, wird auch bezüglich der Open Fronthaul M-Plane Schnittstelle davon ausgegangen, dass geschickt durchgeführte Verfügbarkeitsangriffe zu einer Beeinträchtigung der RAN-Servicequalität führen können.
Bezüglich des Angreifers „Insider“ sieht die Situation etwas anders aus. Ein Insider mit Zugriff auf die Open Fronthaul M-Plane Schnittstelle kann die Software auf den O-RU-Komponenten aktualisieren, was ihm wiederum Zugriff auf die über die Uu-Schnittstelle übertragenen User Plane und Control Plane Daten gewährt. Da diese im worst-case nicht weiter geschützt sind, ergibt sich so ein manipulativer Vollzugriff auf diese Daten, was sich in einer entsprechenden Einschätzung als hohes Risiko für alle Stakeholder manifestiert. Einzig und allein die Integrität der zwischen UE und AMF ausgetauschten Control Plane Daten ist davon unberührt, da diese verpflichtend Integritätsgesichert sind, wodurch da ein geringes Risiko herrscht. Allerdings wird davon ausgegangen, dass auch in der O-RU aus Telco-Sicht schützenswerte (Netzmanagement-)Daten (bezüglich Vertraulichkeit, Integrität und Zurechenbarkeit) vorliegen, auf die ein Insider Zugriff hat. Insofern wird insgesamt von einem mittleren Risiko ausgegangen.
O-RAN-Worst-Case/3GPP-Best-Case (*wb*): In diesem Fall ist die Einschätzung ähnlich zu dem worst-case/worst-case Fall. Verbesserungen ergeben sich aus den nun gesicherten User und Control Plane Daten durch die 3GPP-Maßnahmen. Dadurch kann ein „Insider“ weder die Vertraulichkeit noch die Integrität der Control-Plane-Daten brechen, wodurch das Risiko auch hier insgesamt als mittel eingeschätzt wird. Auch bezüglich der User-Plane-Daten wird angenommen, dass diese geschützt sind, da als Insider hier die O-RU bzw. O-DU unterstellt werden, die beide keinen Zugriff auf die kryptographischen Schlüssel haben, die zur Absicherung der User-Plane angewendet werden.
O-RAN-Best-Case/3GPP-Best-Case (*bb*): Die Einschätzungen bezüglich der Angreifer „Außenstehender“ und „Nutzer“ folgen aus der bereits sehr positiven Risikoeinschätzung im worst-case. Im Falle eines Insider-Angreifers hat dieser zwar Zugriff auf die Uu-Schnittstelle, jedoch sind die Daten (wie schon erläutert) im best-case durch die 3GPP Maßnahmen geschützt, wodurch das Risiko der Verletzung der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit als gering eingestuft wird.
O-RAN-Best-Case/3GPP-Worst-Case (*bw*): Bezüglich der Angreifer „Nutzer“ und „Außenstehender“ verhindern die O-RAN-Sicherheitsmaßnahmen erfolgreiche Angriffe auf Vertraulichkeit, Integrität, Zurechenbarkeit und Privacy der User- und Control-Plane-Daten. Hier ergibt sich insofern ein geringes Risiko. Bezüglich des Angreifers „Insider“, welcher Zugriff auf die O-RU hat, entsteht durch die nicht vorhandene Absicherung der User Plane Daten ein großes Risiko. Beim Netzbetreiber ist das Risiko für die Vertraulichkeit genauso, wobei die Integrität wieder durch die verpflichtende Sicherung im Control Plane Daten zwischen UE und AMF gesichert sind, aber nicht die Management Daten in der O-RU bzw. O-DU.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer					Staat					Netzbetreiber							
	Schutzziele					Schutzziele					Schutzziele							
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P			
Außen-stehender																		
Nutzer																		
Insider																		

Tabelle 10: Risikobewertung der Open Fronthaul M-Plane

5.9 Risikoanalyse Open Fronthaul CUS-Plane

Über die Open Fronthaul CUS-Plane Schnittstelle werden die User und Control Plane Daten der Uu-Schnittstelle übertragen. Außerdem erfolgt die Zeitsynchronisation zwischen O-DU und O-RU. Für diese Schnittstelle ist eine Absicherung explizit *nicht* vorgesehen („*security requirements: no requirements*“ [31]). Begründet wird dies zum einen damit, dass die hohen Anforderungen an Verzögerungszeit und Bandbreite eine Absicherung nicht zulassen, zum anderen wird davon ausgegangen, dass die übertragenen Daten durch Sicherheitsmaßnahmen, die in den 3GPP-Standards vorgesehen sind, bereits abgesichert sind.

Auf Grund der nicht vorgesehenen Sicherheitsmaßnahmen unterscheiden sich die O-RAN worst-case/best-case Betrachtungen nicht. Wesentlich für das Risiko sind also die 3GPP-Sicherheitsmaßnahmen (siehe auch Anhang A). Daher wird nachfolgend auch nur die Unterscheidung in 3GPP-best-case/3GPP-worst-case vorgenommen.

3GPP-Worst-Case (*ww*): Der Zugriff auf die Open Fronthaul CUS-Plane Schnittstelle ermöglicht einem Angreifer den manipulativen Vollzugriff auf die ungeschützten User und Control Plane Daten der Uu-Schnittstelle. Insofern ergibt sich für den Angreifer „Außenstehender“ und alle Stakeholder ein hohes Risiko. Lediglich für die Control Plane Daten ist hinsichtlich der Integrität auf Grund der Ende-zu-Ende Absicherung zwischen UE und AMF von einem geringeren Risiko auszugehen. Davon unberührt bleiben aber Verletzungen der Integrität der O-RAN spezifischen Management-Daten und hier insbesondere der sehr wichtigen Zeitsynchronisationsdaten (siehe auch Kapitel 2.3.6.3).

3GPP-Best-Case (*bb*): Für die Perspektive „Nutzer“ verbessert sich im best-case die Situation bezüglich der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit, da die Uu-Schnittstelle in diesem Fall durch 3GPP-Sicherheitsmaßnahmen abgesichert ist. Bei Zurechenbarkeit wird das Risiko als mittel eingeschätzt, da 3GPP keine Schutzmaßnahmen bezüglich Zurechenbarkeit vorsieht und ein Nutzer (im Vergleich zum Angreifer „Außenstehender“) User-Plane-Nachrichten in das System einspielen kann, die bezüglich Integritätsprüfung als korrekt anerkannt werden.

Verfügbarkeitsangriffe auf die Open Fronthaul CUS-Plane Schnittstelle resultieren in Verfügbarkeitsangriffen auf die Nutzbarkeit des 5G-Gesamtsystems, weswegen bezüglich Verfügbarkeit auch im best-case von einem hohen Risiko ausgegangen wird.

Auch gegenüber dem Angreifer „Insider“ besteht durch die 3GPP-Absicherung ein geringes Risiko für die auf der Uu-Schnittstelle übertragenen User Plane Daten, da die zur Absicherung verwendeten symmetrischen Schlüssel in der O-CU liegen.

Die Control Plane Daten, die zwischen UE und AMF ausgetauscht werden, sind durch die im 3GPP-best-case stattfindende Sicherung abgesichert, wodurch ein geringeres Risiko beim Netzbetreiber herrscht. Allerdings sind auch im 3GPP-best-case die Zeitsynchronisationsdaten (S-PLANE) nicht gesichert, so dass sich hier bezüglich des Schutzziels „Integrität“ insgesamt mindestens ein mittleres Risiko ergibt.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer						Staat						Netzbetreiber					
	Schutzziele						Schutzziele						Schutzziele					
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Außen-stehender																														
Nutzer																														
Insider																														

Tabelle 11: Risikobewertung der Open Fronthaul CUS-Plane

5.10 Risikoanalyse CTI-Schnittstelle

Die CTI-Schnittstelle dient der Reservierung von Kapazitäten im Transportnetz, welches für die Open Fronthaul CUS-Plane verwendet wird. Grund hierfür ist, dass insbesondere im Falle eines mit anderen Diensten gemeinsam genutzten Transportnetzes stets genügend Ressourcen vorhanden sind, um die hohen Anforderungen an Bandbreite und Verzögerungszeit der Open Fronthaul CUS-Plane zu erfüllen. Aktuell wird davon ausgegangen, dass ein Umkonfigurieren der Netzpfade selbst (mit Hilfe der CTI-Schnittstelle) nicht vorgesehen ist. Insofern ergeben sich durch Angriffe bzw. Zugriff auf die CTI-Schnittstelle keine Verletzungen der Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Privacy. Anzumerken ist, dass als Absicherung für die CTI-Schnittstelle aktuell lediglich eine digitale Signatur vorgesehen ist, deren genaue Spezifikation aber erst zukünftig festgelegt werden sollen („*The full details of the CTI Signature will be specified in a future version of this specification*.“) [33]. Dies ermöglicht die Umsetzung von Integrität und Zurechenbarkeit. Vertraulichkeit ist demgegenüber nicht gegeben. So kann ein Angreifer durch ein Belauschen der CTI-Schnittstelle gegebenenfalls Informationen über das Netzmanagement und Netzmanagementstrategien erlangen, was insbesondere bezüglich des Stakeholders „Telco“ zu berücksichtigen ist. Anzumerken ist, dass die erwähnte digitalen Signatur optional ist. Darüber hinaus ist unklar, wie der Mechanismus konkret funktionieren soll. Im CTI-Header ist ein Bit vorgesehen, dass signalisiert, ob eine digitale Signatur zum Einsatz kommt. Da dieses Bit selbst nicht geschützt ist, bleibt unklar, ob die vorgesehene digitale Signatur tatsächlich eine sinnvolle Schutzwirkung entfalten kann.

Da mit Hilfe der CTI-Schnittstelle die Verfügbarkeit des 5G-RANs (insbesondere bezüglich Uu-Schnittstelle) sichergestellt werden soll, ermöglichen Verfügbarkeitsangriffe auf die CTI-Schnittstelle selbst entsprechende Angriffe auf die 5G-RAN-Verfügbarkeit. Hier wird im worst-case von einem hohen Risiko bezüglich des Angreifers „Außenstehender“ und aller Stakeholder ausgegangen. Auf Grund der digitalen Signatur kann es im best-case etwas besser aussehen. Da unklar ist, ob das aktuelle Design der digitalen Signatur tatsächlich sinnvolle Schutzwirkung entfalten kann, wird von einem mittleren Risiko ausgegangen—insbesondere auch, weil Angriffe, die CTI-Nachrichten unterdrücken, trotz digitaler Signatur möglich sind und die aktuellen Spezifikationen einen Ausfall der CTI-Schnittstelle nicht explizit berücksichtigen.

Angreifer	Perspektive (Stakeholder)																	
	End-Nutzer						Staat						Netzbetreiber					
	Schutzziele						Schutzziele						Schutzziele					
	C	I	A	Z	P		C	I	A	Z	P		C	I	A	Z	P	
Außen-stehender																		
Nutzer																		
Insider																		

Tabelle 12: Risikobewertung der CTI-Schnittstelle

5.11 Risikoanalyse sonstiger Schnittstellen

Zu den „sonstigen“ Schnittstellen zählen insbesondere die Schnittstellen zum Zugriff/Download von externen „Enrichment Informationen“, die AI/ML-Schnittstellen und das bezüglich SMO vorgesehene Human-Machine-Interface. Dabei ist die genaue Ausgestaltung dieser Schnittstellen im Moment weitestgehend unspezifiziert.

Bezüglich des Zugriffs auf die „Enrichment Informationen“ ist vorgesehen, dass dieser nur über gesicherte Verbindungen erfolgen sollte. In jedem Fall stellt diese Schnittstelle sowie die AI/ML-Schnittstelle insofern ein Sicherheitsrisiko dar, als das nicht-vertrauenswürdige Provider der zugehörigen Informationen und Daten Einfluss auf Management- und Konfigurationsentscheidungen von rApps/xApps nehmen können. Dies ermöglicht zumindest eine negative Beeinflussung der Verfügbarkeit. Es wird aktuell nicht davon ausgegangen, dass eine direkte Verletzung der Schutzziele Vertraulichkeit, Integrität sowie Zurechenbarkeit bezüglich der 3GPP User Plane sowie Control Plane Daten möglich ist.

Allerdings ist hier anzumerken, dass die durch potentiell nicht-vertrauenswürdige externe Quellen bereitgestellten Daten auch geschickt so erzeugt werden können, um möglicherweise in den verarbeitenden Komponenten (insbesondere in den rApps/xApps) vorhandene Sicherheitslücken (Stichwort: bufferoverflow etc.) auszunutzen und auf diese Weise Kontrolle über die betroffenen Komponenten zu nehmen. Die Auswirkungen hiervon hängen dann sehr stark von der kompromittierten Komponente ab und welche Rechte diese hat bzw. inwiefern hier sogar eine Rechteausweitung möglich ist. Prinzipiell kann sich so ein hohes Risiko auch für die anderen Schutzziele ergeben.

Das Human-Machine-Interface dient zur Beeinflussung (Konfiguration etc.) der SMO-Komponenten durch einen Menschen. Die konkret damit verbundenen Sicherheitsrisiken hängen sehr stark von den — aktuell im Wesentlichen unspezifizierten — Möglichkeiten ab, die diese Benutzungsschnittstelle bietet. Erlaubt sie beispielsweise das Aufspielen von Software-Updates auf die verschiedenen O-RAN Komponenten, so ist damit prinzipiell eine Kompromittierung dieser O-RAN Komponenten möglich, was in der Konsequenz zu vergleichbaren Sicherheitsrisiken führt, wie sie in Kapitel 5.1 bezüglich des Angreifers „RAN-Betreiber“ angegeben wurden.

5.12 Risikoanalyse rApps

Gemäß der Spezifikation soll die R1-Schnittstelle die einzige Schnittstelle sein, die rApps zur Verfügung steht. Insofern ist die Risikoanalyse bezüglich der R1-Schnittstelle eine wesentliche Grundlage bezüglich der Risikoanalyse der rApps. Anzumerken ist hier lediglich, dass in den Spezifikationen allgemein von Zugriffsbeschränkungen von einzelnen rApps bezüglich der R1-Schnittstelle die Rede ist—wie dies genau umgesetzt werden soll, welches Rechte- und Rollenkonzept damit verbunden ist und insbesondere wie feingranular ein mögliches Rechtemanagement eine Beschränkung von Zugriffen auf die R1-Schnittstelle ermöglich, ist aktuell unklar.

Neben der R1-Schnittstelle ergeben sich weitere Bedrohung aus der Tatsache, dass davon auszugehen ist, dass eine gegebene rApp auf einer gemeinsamen Hardware/Ausführungsumgebung zusammen mit anderen rApps und SMO-Funktionalitäten ausgeführt wird. Zumindest finden sich in den Spezifikationen keine Hinweise darauf, dass bezüglich rApps eine strenge (physische) Separierung geplant ist. Insofern stellen ungenügende Separierung und Isolation eine mögliche Schwachstelle dar. Dies gilt insbesondere, da ein vorgesehener Ansatz zur Umsetzung von rApps in der Nutzung von Container-basierter Separierung (beispielsweise mit Hilfe von Kubernetes) liegt. Dabei ist anzumerken, dass die ursprüngliche Zielsetzung bei der Separierung mit Hilfe von Container nicht unbedingt eine Isolierung aus Sicherheitsüberlegungen war, sondern vielmehr zur Vermeidung von Abhängigkeiten zu der durch das Betriebssystem bereitgestellten Laufzeitumgebung. Dementsprechend schwach sind die in aktuellen Containerlösungen zur Zeit umgesetzten und angewendeten Separierungsmechanismen. Insofern besteht also die Gefahr, dass eine rApp aus der Isolierung ausbricht und so die ihr zugebilligten Rechte ausweitet.
Aus Sicht des Angreifers „Nutzer“ ist es zwar denkbar, sogenannte Parserangriffe durchzuführen, die das Ziel haben, durch geschickt manipulierte Nutzerdaten Einfluss auf die rApp zu üben was im Extremfall zu einer Kompromittierung der rApp führen kann. Allerdings ist für eine Risikoeinschätzung dafür die Datengrundlage (im Sinne von Nachrichtenformaten) nicht gegeben, weswegen an dieser Stelle nur darauf hingewiesen wird.
Die Spezifikation macht darüber hinaus keine Vorgaben zu den für die Implementierung einer rApp zu verwendenden Programmiersprachen. Dies ermöglicht prinzipiell die Verwendung von eher „unsicheren“ Programmiersprachen wie C oder C++, bei denen die Wahrscheinlichkeit von durch Angriffe ausnutzbaren Sicherheitslücken (etwa durch Buffer Overflows) deutlich höher ist als bei „sicheren“ Programmiersprachen wie etwa Rust. Da die Kommunikation von rApps untereinander ein wesentliches Design-Element der Gesamtarchitektur ist, könnte eine böswillig rApp Programmierfehler in anderen rApps ausnutzen, um die Kontrolle über eine anfällige rApp zu erlangen, um dann unter Ausnutzung der dieser rApp zugebilligten Rechte böswillige Aktivitäten auszuführen.
Generell sei angemerkt, dass die in der Tabelle dargestellte Risikoanalyse sich nur auf die rApps selbst bezieht und insofern Angriffe auf die rApps bzw. auf das RAN mit Hilfe der rApp-Schnittstellen und anderen Schnittstellen unberücksichtigt lässt. Entsprechende Analysen finden sich in den Kapiteln zu den einzelnen Schnittstellen (insbesondere in dem Kapitel, welches sich mit den sonstigen Schnittstellen beschäftigt.). Dies erklärt das geringe Risiko bezüglich der Angreifer „Außenstehender“ und „Nutzer“, da diese Angreifer eine Schnittstelle angreifen müssen, um eine rApp zu kompromittieren bzw. eine kompromittiere rApps ins System einzuschleusen.
Demgegenüber wird bezüglich des Angreifers „Insider“ angenommen, dass der Insider eine rApp kompromittiert hat. Aufgrund der nicht oder nur sehr eingeschränkt vorhandenen O-RAN Sicherheitsmechanismen bedarf es an dieser Stelle keiner tiefergehenden Fallunterscheidung in ORAN-best-case und O-RAN worst-case. Im Übrigen ergibt sich die Risikoeinschätzung aus der Risikoeinschätzung der R1-Schnittstelle bezüglich des Angreifers „Insider“.

Angreifer	Perspektive (Stakeholder)																			
	End-Nutzer										Staat									
	Schutzziele										Schutzziele									
	C		I		A		Z		P		C		I		A		Z		P	
Außen-stehender																				
Nutzer																				
Insider																				

Tabelle 13: Risikobewertung der rApps

5.13 Risikoanalyse xApps

Für die Risikoanalyse bezüglich der xApps gilt analog das für die rApps Gesagte. Wesentlicher Unterschied dabei ist, dass die xApps Zugriff auf die A1- und E2-Schnittstelle haben. Insofern bilden die Risikoanalysen bezüglich dieser Schnittstellen die Grundlage der Einschätzung. Darüber hinaus sind die xApps „näher“ an den 3GPP-Schnittstellen (Xn, NG, X2, E1, F1), da die xApps Teil der Central Unit (CU) sind. Sollte es einer xApp gelingen, die (möglicherweise) vorhandenen Isolationsmechanismen zu durchbrechen, so bestände hier (im Gegensatz zu den rApps[14]) eine unmittelbarere Gefahr des Zugriffs auf die 3GPP User Plane bzw. Control Plane Daten. Ob sich daraus im Allgemein ein im Vergleich zu den rApps höheres Sicherheitsrisiko ableiten lässt, hängt von der zukünftigen, konkreteren Ausgestaltung der jeweiligen Frameworks und Schnittstellen ab, da die rApps im Vergleich zu den xApps den „Vorteil“ haben, auf die O1- und O2-Schnittstelle zugreifen zu können. Folgend wird konservativ davon ausgegangen, dass beider Arten von Apps dasselbe Risiko gegenüber den Sicherheitszielen aufweisen.

Angreifer	Perspektive (Stakeholder)																			
	End-Nutzer										Staat									
	Schutzziele										Schutzziele									
	C		I		A		Z		P		C		I		A		Z		P	
Außen-stehender																				
Nutzer																				
Insider																				

Tabelle 14: Risikobewertung der xApps

5.14 Risikoanalyse maschinelles Lernen

Maschinelles Lernen ist ein weiteres wesentliches Design-Element der O-RAN-Architektur. Dabei gibt es unterschiedliche Umsetzungsvarianten bezüglich des Trainings der zugehörigen Modelle. Einige Varianten sehen dabei ein Training innerhalb der O-RAN Komponenten vor, wobei neben Messwerten, die aus den O-RAN-Komponenten selbst stammen, auch auf externe Daten zugegriffen werden soll.

Neben den generellen Unsicherheiten, die sich aus dem Einsatz von maschinellem Lernen ergeben (Entscheidungen basieren auf Korrelationen, nicht auf Kausalitäten), ergibt sich aus Sicherheitssicht insbesondere das Problem, dass zahlreiche Angriffe bekannt sind, die mit

[14] Die Risikoanalyse der O-RAN ALLIANCE beschreibt, dass beide Arten von Apps gleichermaßen die Schutzziele verletzen können. Allerdings wird nicht ausgeführt, wie die O-RAN ALLIANCE zu dieser Einschätzung gelangte, weswegen hier dies lediglich erwähnt sei.

Hilfe von manipulierten Eingabedaten das trainierte Modell negativ beeinflussen. Im Ergebnis entsteht ein trainiertes Modell, welches entweder generell fehlerhafte Ergebnisse bei der Inferenz (Anwendung des Modelles) liefert oder—und das kann für manchen Anwendungsfälle das größere Risiko sein—in nahezu allen Fällen ein korrektes Ergebnis liefert und nur in vom Angreifer bestimmbaren Situationen ein vom Angreifer gewünschtes, fehlerhaftes Ergebnis liefert.
Basierend auf den beschriebenen Angriffsmöglichkeiten und der Art und Weise, wie gemäß aktueller Spezifikation—die insgesamt bezüglich des maschinellen Lernens noch recht allgemein und unspezifisch ist—maschinelles Lernen in O-RAN eingesetzt werden soll, wird von einem mittleren Risiko bezüglich Verfügbarkeit, d. h. einer negativen Beeinflussung der Servicequalität ausgegangen. Je nachdem, welche Parameter konkret in das Training eines Modells einfließen, besteht das Risiko bereits bezüglich Außenstehenden, mindestens jedoch gegenüber legitimen RAN-Nutzern.
Aus Sicht des Betreibers (Telcos) besteht ein weiteres Sicherheitsrisiko darin, dass die Vertraulichkeit bezüglich des trainierten Modelles selbst gefährdet sein kann. Die Annahme dabei ist, dass die trainierten Modelle ein schützenswertes Asset darstellen, d. h. im Sinne eines Betriebsgeheimnisses nicht bekannt werden sollen. In der Literatur existieren entsprechende „Model Stealing"-Angriffe, die es einem Angreifer erlauben können, durch geschickte Anfragen oder durch geschickte Beeinflussung des Systems entweder an Hand der Antworten oder allgemein an Hand der Reaktionen des Systems die Parameter des Modells abzuleiten oder zumindest in ihrem jeweiligen Wertebereich (stark) einschränken zu können. Ob derartige Angriffe im Falle von O-RAN tatsächlich erfolgreich durchführbar sind, hängt in starkem Maße vom konkreten Anwendungsszenario eines gegebenen Modells ab. Auf Grund der im Moment existierenden Unklarheit wird hier von einem mittleren Risiko für den Telco ausgegangen, wobei auch hier gegebenenfalls bereits Außenstehende erfolgreiche Angriffe durchführen könnten, zumindest jedoch (vermutlich) legitime RAN-Nutzer.
Abschließend sei noch auf die Möglichkeit von Angriffen auf die Vertraulichkeit von User bzw. Control Plane Daten hingewiesen, wenn diese Eingaben für das Training des Modells sind. Auch hier sind Angriffsstrategien aus der Literatur bekannt, die es ermöglichen, an Hand des trainierten Modells Schlüsse bezüglich der für das Training verwendeten Eingaben durchzuführen. Ob und mit welchen Auswirkungen dies im Falle von O-RAN möglich ist und welche konkreten Sicherheitsrisiken sich daraus ergeben, lässt sich an Hand der aktuell vorliegenden Spezifikationen nicht sinnvoll einschätzen.
Insgesamt ist anzumerken, dass bei der fortschreitenden Spezifikation des Einsatzes von maschinellem Lernen in O-RAN die oben aufgeführten Angriffe berücksichtigten werden müssen, um—wenn immer möglich—durch entsprechende Designentscheidungen bezüglich der O-RAN-Architektur das Risiko erfolgreicher Angriffe zu minimieren.

5.15 Zusammenfassende Risikoanalyse O-RAN

Die zusammenfassende Einschätzung bezüglich der mit der O-RAN-Architektur insgesamt verbundenen Sicherheitsrisiken ergibt sich aus den für die einzelnen Schnittstellen und Komponenten ermittelten Risiken und deren Zusammenführung gemäß des in Kapitel 3.6 beschriebenen „pro Sicherheit"-Vorgehens. Bezüglich des Angreifers Insider wird dabei unterstellt, dass der Angreifer Kontrolle über die CU hat, was dem Angreifer somit Zugriff auf die zur 3GPP-Absicherung der User Plane verwendeten kryptographischen Schlüssel ermöglicht.
In der nachfolgenden Tabelle sind einige Einträge mit einem „+" versehen. Dies soll ausdrücken, dass die Autoren bei der Einschätzung des Risikos – insbesondere auf Grund konkreter Angriffsszenarien – recht sicher sind, dass die Einschätzungen zutreffen.

Angreifer	Perspektive (Stakeholder)																									
	End-Nutzer										Staat										Netzbetreiber					
	Schutzziele										Schutzziele										Schutzziele					
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Außen-stehender		+		+	+	+		+				+		+	+	+		+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
Nutzer		+		+	+	+		+				+		+	+	+		+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
Insider	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+	+	+		
Cloud-Betreiber	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+	+	+		
RAN-Betreiber	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+	+	+		

Tabelle 15: Zusammenfassende Risikobewertung bezüglich O-RAN

6 Zusammenfassung und Ausblick

Die O-RAN Spezifikationen werden aktuell nicht gemäß des Paradigmas „security/privacy by design/default“ entwickelt. Insofern ist es wenig überraschend, dass im Ergebnis ein System entstand, das vielfältige Sicherheitsrisiken beinhaltet. Mit der Erstellung der Bedrohungs- und Risikoanalyse und eines ersten Versuchs, anzuwenden Sicherheitsmechanismen festzulegen, sind erste Ansätze erkennbar, dass die O-RAN Alliance sich zukünftige verstärkt dem Thema Sicherheit widmen könnte. Inwiefern dies tatsächlich passiert, wird sich zeigen müssen. Aus der Erfahrung ergibt sich in jedem Fall, dass ein spätes Hinzufügen von Sicherheitsmaßnahmen entweder zu sehr hohen Aufwänden oder zu unsicheren Lösungen bzw.—nicht unüblich—zu beidem führt. Die Entwicklungen der 3GPP-Standards sind ein gutes Beispiel dafür. Der anfänglich stark vernachlässigte Bereich der IT-Sicherheit hat zunächst zu einem unsicheren System geführt. Der Versuch, diese Fehler in nachfolgenden Versionen des Standards zu korrigieren, war mit viel Aufwand verbunden und führt oftmals—insbesondere auf Grund zu beachtender Kompatibilitätsanforderungen—zu weiterhin unsicheren Lösungen. Tatsächlich ist es so, dass bei vielen praktisch betrieben, öffentlichen Mobilfunknetzen die sicherheitskritischen Altlasten auch in modernen 5G-Netzen zu Unsicherheiten führen. Es gilt eine derartige Entwicklung bei O-RAN zu verhindern. Insofern sollten die O-RAN Spezifikationen mit einem deutlich stärkeren Sicherheitsfokus überarbeitet werden, bevor es zu ersten produktiven Anwendungen von O-RAN kommt.
Bezüglich der Umsetzbarkeit von Sicherheitslösungen zur Risikominimierung wird aktuell eingeschätzt, dass es eine Vielzahl von bekannten Sicherheitsmaßnahmen gibt, die ohne großen Aufwand und Kosten umgesetzt werden können und die dabei effektiv zur Risikominimierung bezüglich einzelner Bedrohungen beitragen können. Es wird aber auch eingeschätzt, dass zur Verringerung einiger Sicherheitsrisiken durchaus einiger—gegebenenfalls sogar erheblicher—Aufwand bei der Anpassung der Spezifikationen und bei der Umsetzung der entsprechenden Sicherheitsmaßnahmen notwendig ist.
Nachfolgend werden einige Vorschläge zur Risikominimierung unterbreitet.

6.1 Empfehlungen

6.1.1 3GPP

O-RAN profitiert als Umsetzung eines 3GPP-RANs unmittelbar von Sicherheitsverbesserungen an den 3GPP-Standards. Hier ist zum einen zu erwähnen, dass die vielen optionalen Sicherheitsmechanismen verpflichtend vorgeschrieben werden sollten. Darüber hinaus sollte auch bezüglich der User Plane Daten eine Ende-zu-Ende Sicherung zwischen UE und 5G-Core eingeführt werden, ähnlich wie dies bei den Control Plane Daten vorgesehen ist. Generell sollten auch die 3GPP-Standards noch deutlich stärker nach dem Paradigma „security/privacy by design/default“ entwickelt werden—und dabei insbesondere unter Abkehr von dem derzeit verfolgten Perimeter-Sicherheitsmodell hin zu den Prinzipien der mehrseitigen Sicherheit[15], d. h. mit minimalen Vertrauensannahmen bezüglich sämtlicher Stakeholder und Komponenten. Dieses könnte die aktuell möglichen, von einem kompromittierten RAN bzw. von einem nicht-vertrauenswürdigen RAN-Betreiber sowie von nicht-vertrauenswürdigen RAN-Komponenten ausgehenden Sicherheitsrisiken stark verringern.

Zusammenfassend ergeben sich folgende Vorschläge:

- Verpflichtende Einführung optionaler Sicherheitsmaßnahmen
- Ende-zu-Ende Sicherung von User Plane Daten zwischen UE und 5G-Core
- stärkere Berücksichtigung des Paradigmas „security/privacy by design/default“
- Berücksichtigung der Prinzipien von mehrseitiger Sicherheit

[15] Dieses Konzept ist auch unter dem irreführenden Marketing-Begriff „zero trust“ bekannt.

6.1.2 O-RAN

Als eine der wichtigsten Maßnahmen zur Verringerung der O-RAN Sicherheitsrisiken wird eine ernsthafte Umsetzung des Paradigmas „security/privacy by design/default“ unter Berücksichtigung der Prinzipien der mehrseitigen Sicherheit angesehen. Die Prozesse bei der Erstellung der O-RAN-Spezifikationen sollten entsprechend angepasst werden, etwa, indem Sicherheitsexperten bei der Erstellung der Standards hinzugezogen werden und Sicherheitsüberlegungen und Einschätzungen verpflichtender Teil jeder Spezifikation werden, wie dies beispielsweise bei IETF RFCs der Falls ist [60], [61].

Die aktuell nur optional vorgesehen Sicherheitsmaßnahmen sollten verpflichtend vorgeschrieben sein. Dabei sollte gleichzeitig eine Unterstützung veralteter Sicherheitsprotokolle oder als unsicher anzusehender kryptographischer Algorithmen explizit ausgeschlossen sein. Hier gilt es insbesondere klare und eindeutige Formulierungen bezüglich der zwingend notwendigen Anwendung der Sicherheitsmaßnahmen in die Standards aufzunehmen. Ein reines Vorhandensein ist hier nicht ausreichend. Das es besser geht zeigt beispielsweise die Spezifikation zur O1-O-DU-Schnittstelle.

Bei der Auswahl der Sicherheitsprotokolle sollte darauf geachtet werden, dass diese selbst möglichst wenig neue Bedrohungen und Sicherheitsrisiken bieten. So sollte statt der Verwendung von SSH besser TLS zur Transportabsicherung verwendet werden. Dabei sollte ferner berücksichtigt werden, dass Daten (einschließlich Programmen) nicht nur bei der Übertragung („in transit“) gesichert werden, sondern auch „at rest“, also im Zuge der persistenten Speicherung. Dabei sollten mindestens die Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit umgesetzt werden.

Darüber hinaus sollte bezüglich sämtlicher Schnittstellen und bezüglich der rApps/xApps ein klares Rechte- und Rollenkonzept umgesetzt werden. Dabei sind die üblichen Sicherheitsprinzipien, wie etwa „least privileges“, „need to know“ etc. umzusetzen. Voraussetzung dafür ist, dass die Schnittstellen möglichst konkret spezifiziert sind (beispielsweise O2- sowie R1-Schnittstelle) und die grundlegenden Sicherheitsmechanismen eine möglichst feingranulare Zugriffskontrolle ermöglichen. Dies betrifft insbesondere auch Schnittstellen, die aktuell nur am Rande eine Rolle spielen, wie etwa die Schnittstellen für die „Enrichment Information“ oder das „Human-Machine-Interface“. In diesem Zuge sollten auch aktuell nicht gesicherte Schnittstellen, wie etwa die Open Fronthaul CUS Schnittstelle abgesichert werden. Darüber hinaus sollten die Schnittstellen so gestaltet sein, dass sie „bei Design“ möglichst wenig Angriffsfläche bieten. Dabei sind insbesondere Verfügbarkeitsangriffe auf die Schnittstellen zu berücksichtigen, da sich hier negative Auswirkungen nicht einfach durch Anwendung von Transportsicherung verhindern lassen. Die Protokolle und das Gesamtsystem sollten also so gestaltet sein, dass die Auswirkungen von Verfügbarkeitsangriffen auf die Schnittstellen in ihrer schädlichen Wirkung begrenzt sind. Neben einer funktionalen Beschränkung auf das tatsächlich Notwendige betrifft dies auch Design-Entscheidung, die beispielsweise die Anzahl offener Ports beeinflussen. Um eine aus Sicherheitsmanagementsicht möglichst gut zu konfigurierende und überwachbar Lösung zu haben, sollten möglichst wenig Dienstzugangspunkte existieren.

Bezüglich xApps/rApps sollte ein Konzept von starker Separierung und Isolation umgesetzt werden, so dass die Kompromittierung einer xApp/rApp nicht zu einer Kompromittierung weiterer O-RAN-Komponenten oder anderer Apps führt. Darüber hinaus sollte die Kommunikation zwischen den Apps End-zu-Ende abgesichert werden. Ferner sollten Vorgaben bzw. Umsetzungsrichtlinien für Apps existieren. Diese sollten beispielsweise die Verwendung von sicheren Programmiersprachen vorschreiben.

Besonderes Augenmerk sollte auf die Absicherung der O-Cloud, also der zugrundeliegenden Cloud-Infrastruktur gelegt werden. Hierbei sollten Maßnahmen umgesetzt werden, die auch im Falle von nicht-vertrauenswürdigen Cloud-Betreibern ein möglichst hohes Maß an Sicherheit ermöglichen. Insbesondere sollte von der Annahme von vertrauenswürdigen Cloud-Betreibern Abstand genommen werden. Dies schließt auch die Berücksichtigung von potentiell

kompromittierenten Komponenten der Cloud-Infrastruktur mit ein. Insofern sollte zum einen die O-RAN-Architektur so (um)gestaltet werden, dass möglichst wenig negative Auswirkungen entstehen können. Zum anderen sollten Vorgaben im Sinne von Sicherheitsanforderungen an die Komponenten der Cloud-Infrastruktur gemacht werden. Dabei sollte auch evaluiert werden, inwiefern aktuelle Cloud-Standardlösungen wie etwa Container und deren Implementierungen wie etwa Kubernetes den Sicherheitsanforderungen prinzipiell genügen. Es sollte untersucht werden, inwiefern Trusted Execution Environments (TEEs) geeignet sind, einen sicheren O-RAN Betrieb auch im Falle von nicht-vertrauenswürdigen Clouds zu ermöglichen und die Benutzung von TEEs gegebenenfalls vorgeschrieben werden.
Bei der hier vorliegenden Risiko- und Sicherheitsanalyse hat sich gezeigt, dass sich aus den 3GPP-Standards in Verbindung mit den O-RAN-Spezifikationen eine Komplexität ergibt, die eine verlässliche Einschätzung allein durch „scharfes Hinsehen“ nicht mehr möglich macht. Insofern sollte als ein wesentliches Element für die Entwicklung sicherer Systeme auf eine formale Verifikation der Spezifikationen (und idealerweise auch der Implementierungen) zurückgegriffen werden. Dies sollte auch im Falle von O-RAN erfolgen. Um den sich ergebenden Aufwand für die formale Verifikation im Rahmen zu halten, wird dabei vorgeschlagen, zunächst die Menge an kritischer Minimalfunktionalität zu bestimmen und daraus die zur Umsetzung notwendige Minimalfunktionalität und die sich daraus ergebenen minimal notwendigen, vertrauenswürdigen Komponenten abzuleiten. Diese sollten dann einer formalen Verifikation unterzogen werden. Dabei sollte das System insgesamt so gestaltet sein, dass sich das Minimalsystem um gegebenenfalls nicht-vertrauenswürdige Komponenten erweitern lässt, ohne dass der sichere Betrieb bezüglich der Minimalfunktionalität gefährdet wird. Dieses Vorgehen ist also beispielsweise mit den Konzepten einer Mikrokern-basierten Ausführungsumgebung (Betriebssystem etc.) zu vergleichen. Auch in diesem Fall lassen sich potentiell nicht-vertrauenswürdige Softwarekomponenten integrieren bei gleichzeitig möglich Aussagen und Garantien bezüglich Sicherheit. Insgesamt lassen sich durch eine formaleres Vorgehen Sicherheitsrisiken identifizieren, die auf Grund der Komplexität der Spezifikationen allein „durch scharfes Hinsehen“ typischerweise nicht entdeckt werden.

Zusammenfassend ergeben sich somit folgende Empfehlungen:

- Security/privacy by design/default umsetzen
- „zero trust“ / mehrseitige Sicherheit tatsächlich umsetzen
- optionale Sicherung auf Transportschicht vorschreiben
- klare Formulierungen verwenden, Zweideutigkeiten vermeiden, um die verpflichtende Anwendung von Sicherheitsmechanismen klarzustellen
- SSH2 durch TLS ersetzen
- veraltete Protokolle, unsichere kryptographische Algorithmen verbieten
- Dateien „at rest“ sichern (Verschlüsselung, Integritätssicherung)
- Klares Rechte/Rollenkonzept bezüglich der Schnittstellen und Dienste festlegen
    - insbesondere für R1- und E2- Schnittstelle (rApps, xApps)
- O2-Schnittstelle (Cloud Management) klar spezifizieren
- R1-Schnittstelle klar spezifizieren
- Open Fronthaul CUS Schnittstelle absichern
- Auswirkungen von DoS auf Schnittstellen einschränken
- Firewall-friendly Design umsetzen
    - wenige Zugangspunkte, wenige Server-Endpunkte
- Absicherung der Anbindung externer Datenquellen spezifizieren
- Separierungskonzept xApps/rApps zumindest bezüglich Anforderungen klar spezifizieren
- Kommunikation zwischen rApps absichern
- xApps/rApps nur mit sicheren Programmiersprachen (Rust etc.)

- Sicherheitsmaßnahmen zur Absicherungen gegenüber nicht-vertrauenswürdigen Cloud-Betreibern vorsehen (TEEs etc.)
- Sicherheitsmechanismen bezüglich O-Cloud vorschreiben, dabei insbesondere die Nutzerauthentikation zwingend vorschreiben
- formale Verifizierbarkeit vorbereiten und idealerweise auch durchführen

7 Quellenverzeichnis

[1] X. Lin und N. Lee, „5G and Beyond Fundamentals and Standards“, *Springer eBook Collection*, 2021, Zugegriffen: 15. September 2021. [Online]. Verfügbar unter: http://wwwdb.dbod.de/login?url=https://doi.org/10.1007/978-3-030-58197-8

[2] 3GPP, „Study on new radio access technology: Radio access architecture and interfaces“, 3GPP, V14.0.0, Technical Report TR 38.801, Apr. 2017.

[3] U. Schulze, „Endlich offen: Kurz erklärt: Open RAN“, *iX*, Bd. 2020, Nr. 9, Heise, S. 120, 26. August 2020.

[4] G. Brown, „The Role of the RAN Intelligent Controller in Open RAN Systems“. Heavy Reading White Paper produced for Sterlite Technologies Limited, Oktober 2020.

[5] „The O-RAN Alliance and the Telecom Infra Project (TIP) Reach New Level of Collaboration for Open Radio Access Networks“, 25. Februar 2020. https://www.businesswire.com/news/home/20200225005180/en/The-O-RAN-Alliance-and-the-Telecom-Infra-Project-TIP-Reach-New-Level-of-Collaboration-for-Open-Radio-Access-Networks (zugegriffen 17. September 2021).

[6] 3GPP, „NG-RAN; E1 Application Protocol (E1AP)“, 3GPP, V16.6.0, Technical Specification TS 38.463, Juli 2021.

[7] 3GPP, „NG-RAN; F1 Application Protocol (F1AP)“, 3GPP, V16.6.0, Technical Specification TS 38.473, Juli 2021.

[8] 3GPP, „Architecture enhancements for control and user plane separation of EPC nodes“, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.214, Dez. 2018.

[9] 3GPP, „System architecture for the 5G System (5GS)“, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.501, Dez. 2020.

[10] 3GPP, „General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)“, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.281, März 2021.

[11] R. R. Stewart, „Stream Control Transmission Protocol“, Nr. 4960. RFC Editor, September 2007. Zugegriffen: 3. August 2021. [Online]. Verfügbar unter: https://rfc-editor.org/rfc/rfc4960.txt

[12] 3GPP, „NG-RAN; NG Application Protocol (NGAP)“, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.413, Juli 2021.

[13] 3GPP, „Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3“, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 24.501, Juni 2021.

[14] O-RAN ALLIANCE e.V., „O-RAN Architecture Description“, O-RAN WG1: Use Cases and Overall Architecture Workgroup, V05.00, Technical Specification O-RAN.WG1.O-RAN-Architecture-Description-v05.00, Juli 2021.

[15] Mavenir, Inc., „Security in Open RAN“. White Paper, Januar 2021.

[16] 3GPP, „Security architecture and procedures for 5G system“, 3GPP, V17.1.0, Technical Specification TS 33.501, März 2021.

[17] 3GPP, „Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Architecture description“, 3GPP, V16.0.0, Technical Specification TS 36.401, Juli 2020.

[18] O-RAN ALLIANCE e.V., „O-RAN Operations and Maintenance Architecture“, O-RAN WG1: Use Cases and Overall Architecture Workgroup, V04.00, Technical Specification O-RAN.WG1.OAM-Architecture-v04.00, 2021.

[19] 3GPP, „NR; NR and NG-RAN Overall description; Stage-2“, 3GPP, V16.6.0, Technical Specification TS 38.300, Juli 2021.

[20] Parallel Wireless, „Everything You Need to Know about Open RAN“. E-Book, 2020. Zugegriffen: 29. Juli 2021. [Online]. Verfügbar unter: https://www.parallelwireless.com/wp-content/uploads/Parallel-Wireless-e-Book-Everything-You-Need-to-Know-about-Open-RAN.pdf

[21] GSMA, „5G Implementation Guidelines“. E-Book, März 2019. Zugegriffen: 29. Juli 2021. [Online]. Verfügbar unter: https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/5G-Implementation-Guidelines_v1_nonconfidential-R2.pdf

[22] 3GPP, „Network sharing; Architecture and functional description“, 3GPP, V16.0.0, Technical Specification TS 23.251, Juli 2020.
[23] Deutsche Telekom, Orange, Telefónica, TIM and Vodafone, „Open RAN Technical Priorities under the Open RAN MoU“. Downloadable Document. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://telecominfraproject.com/openran-mou-group/
[24] O-RAN ALLIANCE e.V., „O-RAN Use Cases and Deployment Scenarios; Towards Open and Smart RAN“, White Paper, Feb. 2020.
[25] O-RAN ALLIANCE e.V., „O-RAN Operations and Maintenance Interface Specification“, O-RAN WG1: Use Cases and Overall Architecture Workgroup, V04.00, Technical Specification O-RAN.WG1.O1-Interface.0-v04.00, Aug. 2020.
[26] O-RAN ALLIANCE e.V., „O-RAN O2 Interface General Aspects and Principles“, O-RAN WG6: Cloudification and Orchestration Workgroup, V01.00.04, Technical Specification O-RAN.WG6.O2-GA & P-v01.01, Juli 2021.
[27] O-RAN ALLIANCE e.V., „Cloud Architecture and Deployment Scenarios for O-RAN Virtualized RAN“, O-RAN WG6: Cloudification and Orchestration Workgroup, V02.02, Technical Report O-RAN.WG6.CAD-v02.02, Juli 2021.
[28] O-RAN ALLIANCE e.V., „O-RAN Working Group 2 (Non-RT RIC and A1 interface WG); A1 interface: General Aspects and Principles“, O-RAN WG2: Non-real-time RAN Intelligent Controller and A1 Interface Workgroup, V02.02, Technical Specification O-RAN.WG2.A1GAP-v02.03.01, Juni 2021.
[29] O-RAN ALLIANCE e.V., „Non-RT RIC: Functional Architecture“, O-RAN WG2: Non-real-time RAN Intelligent Controller and A1 Interface Workgroup, V01.01, Technical Report O-RAN.WG2.Non-RT-RIC-ARCH-TR-v01.01, März 2021.
[30] O-RAN ALLIANCE e.V., „Near-Real-time RAN Intelligent Controller Architecture & E2 General Aspects and Principles“, O-RAN WG3: Near-real-time RIC and E2 Interface Workgroup, V02.00, Technical Specification O-RAN.WG3.E2GAP-v02.00, Aug. 2021.
[31] O-RAN ALLIANCE e.V., „Control, User and Synchronization Plane Specification“, O-RAN WG4: Open Fronthaul Interfaces Workgroup, V07.00, Technical Specification O-RAN.WG4.CUS.0-v07.00, Juli 2021.
[32] O-RAN ALLIANCE e.V., „Management Plane Specification“, O-RAN WG4: Open Fronthaul Interfaces Workgroup, V07.00, Technical Specification O-RAN.WG4.MP.0-v07.00, Juli 2021.
[33] O-RAN ALLIANCE e.V., „Cooperative Transport Interface Transport Control Plane Specification“, O-RAN WG4: Open Fronthaul Interfaces Workgroup, V02.00, Technical Specification O-RAN.WG4.CTI-TCP.0-v02.00, März 2021.
[34] O-RAN ALLIANCE e.V., „O-RAN Working Group 2; AI/ML workflow description and requirements“, O-RAN WG2: Non-real-time RAN Intelligent Controller and A1 Interface Workgroup, V01.02, Technical Report O-RAN.WG2.AIML-v01.03.02, Juni 2021.
[35] O-RAN ALLIANCE e.V., „O-RAN Minimum Viable Plan and Acceleration towards Commercialization“, White Paper, Juni 2021. Zugegriffen: 28. Juli 2021. [Online]. Verfügbar unter: https://www.o-ran.org/s/O-RAN-Minimum-Viable-Plan-and-Acceleration-towards-Commercialization-White-Paper-29-June-2021.pdf
[36] DIN ISO, „Risikomanagement – Leitlinien (ISO 31000:2018)“, DIN, Deutsche Norm DIN ISO 31000:2018-10, Okt. 2018.
[37] ISO/IEC, „Information technology — Security techniques — Information security risk management“, ISO/IEC, Third Edition, International Standard ISO/IEC 27005:2018, Juli 2018.
[38] IEC, „Risk management – Risk assessment techniques“, IEC, Edition 2.0, IEC 31010:2019, Juni 2019.
[39] BSI, „BSI-Standard200-3 --- Risikoanalyse auf der Basis von IT-Grundschutz“, BSI, Version 1.0, BSI-Standard200-3, Okt. 2017.
[40] ENISA, „ENISA Threat Landscape for 5G Networks --- Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)“, ENISA, Dez. 2020. [Online]. Verfügbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/at_download/fullReport

[41] ENISA, „ENISA Threat Landscape for 5G Networks --- Threat assessment for the fifth generation of mobile telecommunications networks (5G)“, ENISA, Nov. 2019. [Online]. Verfügbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport
[42] NIS Cooperation Group, „EU coordinated risk assessment of the cybersecurity of 5G networks“, Report, Okt. 2019. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[43] NIS Cooperation Group, „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures“, CG Publication, Jan. 2020. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[44] CISA, „CISA 5G STRATEGY --- Ensuring the Security and Resilience of 5G Infrastructure In Our Nation“, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, 2020. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf
[45] CISA, NSA, und DNI, „POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE“, 2021. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf
[46] President of the United States, „NATIONAL STRATEGY TO SECURE 5G of the United States of America“, März 2020. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://www.hsdl.org/?view&did=835776
[47] NTIA, „National Strategy to Secure 5G Implementation Plan“, Jan. 2021. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf
[48] NTIA, „National Strategy to Secure 5G Implementation Plan Appendices“. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://www.ntia.gov/files/ntia/publications/5g_ip_appendices_1-5.pdf
[49] O-RAN ALLIANCE e.V., „O-RAN Security Threat Modeling and Remediation Analysis“, O-RAN SFG: Security Focus Group, V02.00.01, Technical Specification O-RAN.SFG.Threat-Model-v02.00.01, Juli 2021.
[50] GSMA, „Mobile Telecommunications Security Landscape“, März 2021. Zugegriffen: 29. September 2021. [Online]. Verfügbar unter: https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf
[51] O-RAN ALLIANCE e.V., „O-RAN Security Requirements Specifications“, O-RAN SFG: Security Focus Group, V01.00.01, Technical Specification O-RAN.SFG.Security-Requirements-Specifications-v01.00, Juli 2021.
[52] Red Hat, „State of Kubernetes Security Report“, E-book, Juni 2021. Zugegriffen: 27. Juli 2021. [Online]. Verfügbar unter: https://www.redhat.com/en/resources/state-kubernetes-security-report
[53] O-RAN ALLIANCE e.V., „ORAN O1 Interface specification for O-DU“, ORAN Open F1/W1/E1/X2/Xn interface Workgroup, V02.00, Technical Specification O-RAN.WG5.MP.0-v02.00, Aug. 2021.
[54] M. Wasserman, „Using the NETCONF Protocol over Secure Shell (SSH)“, IETF, Proposed Standard RFC 6242, Juni 2011.
[55] O-RAN ALLIANCE e.V., „Security Protocols Specifications“, O-RAN SFG: Security Focus Group, V02.00.06, Technical Specification O-RAN.SFG.Security-Protocols-Specifications-v02.00, Juli 2021.
[56] M. Badra, A. Luchuk, und J. Schoenwaelder, „Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication“, IETF, Proposed Standard RFC 7589, Juni 2015.
[57] O-RAN ALLIANCE e.V., „A1 interface: Transport Protocol“, O-RAN WG2: Non-real-time RAN Intelligent Controller and A1 Interface Workgroup, V01.01, Technical Specification O-RAN.WG2.A1TP-v01.01, März 2021.

[58] O-RAN ALLIANCE e.V., „Non-RT RIC & A1 Interface: Use Cases and Requirements“, O-RAN WG2: Non-real-time RAN Intelligent Controller and A1 Interface Workgroup, V04.00.03, Technical Specification O-RAN.WG2.Use-Case-Requirements-v04.00.03, Juli 2021.
[59] O-RAN ALLIANCE e.V., „RAN Function Network Interface (NI)“, O-RAN WG3: Near-real-time RIC and E2 Interface Workgroup, V01.00.00, Technical Specification ORAN-WG3.E2SM-NI-v01.00.00, Jan. 2020.
[60] H. Flanagan und S. Ginoza, „RFC Style Guide“, IAB, Informational RFC 7997, Sep. 2014.
[61] E. Rescorla und B. Korver, „Guidelines for Writing RFC Text on Security Considerations“, Network Working Group, Best Current Practice RFC 3552 / BCP 72, Juli 2003.
[62] 3GPP, „Packet Data Convergence Protocol (PDCP) specification“, 3GPP, V16.3.0, Technical Specification TS 38.323, März 2021.
[63] 3GPP, „Non-Access-Stratum (NAS) protocol for 5G System (5GS)“, 3GPP, V17.3.1, Technical Specification TS 24.501, Juni 2021.

8 Abkürzungsverzeichnis

3GPP	3rd Generation Partnership Project
5G	5. Generation
5G SD-RAN	5G Software-Defined Radio Access Network
5GC	5G Core
5GMM	5GS Mobility Management
5GS	5G System
5GSM	5GS Session Management
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
CapEx	Capital Expenditure
CLA	Contributor License Agreement
CN	Core Network
COTS	Commercial (oder Components) off-the-shelf
CP	Control Plane
CTI	Cooperative Transport Interface
CU	Centralized Unit
CU-CP	Centralized Unit Control Plane
CUPS	Control and User Plane Separation
CUS-Plane	Control, User, Synchronization Plane
CU-UP	Centralized Unit User Plane
DMS	Deployment Management Services
DSS	Dynamic Spectrum Sharing
DU	Distributed Unit
E2E	End-to-End
E2SM	E2 Service Model
eCPRI	Enhanced Common Public Radio Interface
EDGE	Enhanced Data Rates for GSM Evolution
EI	Enrichment Information
eNB	Evolved Node B
EPC	Evolved Packet Core
E-UTRA	Evolved UMTS Terrestrial Radio Access
FCAPS	Fault, Configuration, Accounting, Performance, Security
FH	Fronthaul
FM	Fault Management
FOCOM	Federated O-Cloud Orchestration and Management
GERAN	GSM EDGE Radio Access Network
gNB	Next Generation Node B
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP-U	GPRS Tunneling Protocol - User
HF	Hochfrequenz
HW	Hardware
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers

IMS	Infrastructure Management Services
IP	Internet Protocol
ISO	International Organization for Standardization
JWI	Joint Work Item
KI	Künstliche Intelligenz
KPI	Key Performance Indicator
L1/L2/L3	Layer 1/2/3 im OSI-Modell
LTE	Long Term Evolution
MAC	Medium Access Control
MDT	Minimization of Drive Test
ME	Managed Element
MIMO	Multiple Input/Multiple Output
ML	Machine Learning
MLB	Mobility Load Balancing
mMIMO	Massive MIMO
MnS	Management Service
MOCN	Multi-Operator Core Network
MOI	Managed Object Instance
MORAN	Multi-Operator Radio Access Network
M-Plane	Management Plane
MSP	Managed Service Provider
NAS	Non-Access Stratum
NAS-MM	NAS Mobility Management
Near-RT RIC	Near-Real-Time RAN Intelligent Controller
NETCONF	Network Configuration Protocol
NF	Network Function
NFO	Network Function Orchestrator
NG-AP	Next Generation Application Protocol
ng-eNB	Next Generation Evolved Node B
NG-RAN	Next Generation RAN
Non-RT RIC	Non-Real-Time RAN Intelligent Controller
NR	New Radio
NSA	Non-Stand-Alone
NSSI	Network Slice Subnet Instance
OAM	Operation, Administration and Maintenance
O-Cloud	O-RAN Cloud
O-CU	O-RAN Centralized Unit
O-CU-CP	O-RAN Centralized Unit Control Plane
O-CU-UP	O-RAN Centralized Unit User Plane
O-DU	O RAN Distributed Unit
O-eNB	O RAN Evolved Node B
ONAP	Open Network Automation Platform
ONF	Open Network Foundation
Open FH	Open Fronthaul
OpEx	Operational Expenditure
O-RU	O-RAN Radio Unit
OSA	OpenAirInterface Software Alliance
OSC	O-RAN Software Community

OSS	Operations Support System
PDCP	Packet Data Convergence Protocol
PDCP-C	Packet Data Convergence Protocol - Control
PDCP-U	Packet Data Convergence Protocol - User
PDU	Packet Data Unit
PHY	Physical Layer
PLMN	Public Land Mobile Network
PM	Performance Management
PNF	Physical Network Function
PRACH	Packet Random Access Channel
PRB	Physical Resource Block
PTP	Precision Time Protocol
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RCEF	RRC Connection Establishment Failure
RIA	RAN Intelligence and Automation
RIC	RAN Intelligent Controller
RLC	Radio Link Control
RLF	Radio Link Failure
RRC	Radio Resource Control
RRM	Radio Resource Management
RRU	Remote Radio Unit
RSAC	Requirements and Software Architecture Committee
RT	Real-Time
RU	Radio Unit
SA	Stand-Alone
SBI	Service Based Interface
SCTP	Stream Control Transmission Protocol
SDAP	Service Data Adaptation Protocol
SD-RAN	Software-Defined Radio Access Network
SFTP	Secure File Transfer Protocol
SI	Systemintegrator
SLA	Service Level Agreement
SMF	Session Management Function
SMO	Service Management and Orchestration
SON	Self-Organizing Network
SSH	Secure Shell
SUCI	Subscription Concealed Identifier
SW	Software
SyncE	Synchronous Ethernet
TC	Transport Control
TDD	Time Division Duplex
TEID	Tunnel-Endpunkt-ID
TIM	Telecom Italia Mobile
TIP	Telecom Infra Project
TLS	Transport Layer Security
TM	Transport Management

TN	Transport Node
TOC	Technical Oversight Committee
T-PDU	Transport Packet Data Unit
TU	Transport Unit
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
V2X	Vehicle-to-Everything
vCU	Virtual Centralized Unit
vDU	Virtual Distributed Unit
VM	Virtual Machine
VNF	Virtual Network Function
vRAN	Virtual Radio Access Network
WG	Working Group (der O-RAN Alliance)
YANG	Yet Another Next Generation

Anhang A: 3GPP 5G RAN Risikoanalyse

Die nachfolgende Zusammenfassung einer Risikoanalyse bezüglich des durch 3GPP standardisierten RANs basiert auf einer Auswertung relevanter 3GPP Standards sowie einer Einbeziehung von existierenden Bedrohungs- und Risikoanalysen sowie aus der (wissenschaftlichen) Literatur bekannten Angriffsmöglichkeiten. Ein Verständnis bezüglich der RAN-inhärenten Sicherheitsrisiken und potenziellen Gegenmaßnahmen ist essentiell, um die Risiken, die mit O-RAN als einer konkreten RAN-Umsetzung einhergehen, besser einschätzen und verstehen zu können.

Gemäß [62], [16] erfolgt die Sicherung der User Plane Daten der Uu-Schnittstelle innerhalb der PDCP-Schicht. Dabei werden sowohl symmetrische Verschlüsselung als auch symmetrische Integritätssicherung (Message Authentication Codes) eingesetzt. Auf Grund der symmetrischen Integritätssicherung wird das Schutzziel Zurechenbarkeit nicht umgesetzt. Die dabei verwendeten symmetrischen Schlüssel sind dem gNB bekannt. Es erfolgt also keine Ende-zu-Ende-Sicherung zwischen UE und 5G-Core. Die Absicherung der Übertragung der User Plane Daten zwischen gNB und 5G-Core über die NG-U Schnittstelle erfolgt mit Hilfe von IPSec. Insgesamt ist anzumerken, dass die Absicherung sowohl der Uu als auch der NG-U Schnittstelle optional ist: „*Confidentiality protection of user data between the UE and the gNB is optional to use. […] Integrity protection of the user data between the UE and the gNB is optional to use, and shall not use NIA0.“* [16].

Die Vorgabe, ob eine Absicherung durchgeführt werden soll, erfolgt dabei im 5G-Core, konkret durch die lokal zuständig SMF. Im best-case wird insofern davon ausgegangen, dass die Sicherheitsmechanismen aktiviert sind, bei der worst-case Betrachtung wird unterstellt, dass die Übertragung der User Plane Daten ungesichert erfolgt.

Vergleichbar zur User Plane sind auch für die Control Plane Sicherungsmaßnahmen prinzipiell vorgesehen [62], [16], [63]—wobei auch bezüglich der Control Plane die Sicherungsmaßnahmen bezüglich Vertraulichkeit nur optional sind: *“Confidentiality protection NAS-signalling is optional to use.”* [16]. Die Integrität der Control Plane Daten ist hingegen verpflichtend: *“All NAS signalling messages except those explicitly listed in TS 24.501* [63] *as exceptions shall be integrity-protected with an algorithm different to NIA-0 except for emergency calls.”* [16]. Die Fälle, die in [63] aufgelistet werden, sind die folgenden:

> *a) for an unauthenticated UE for which establishment of emergency services is allowed;*
> *b) for an W-AGF acting on behalf of an FN-RG; and*
> *c) for a W-AGF acting on behalf of an N5GC device.* [63]

Dadurch sind die Randfälle, bei denen keine Integritätssicherung stattfindet, zum einen gut definiert und zum anderen tatsächlich Randfälle (beispielsweise Notruf). Ein wesentlicher Unterschied im Vergleich zu der Übertragung der User Plane Daten ist, dass die Nachrichten der Control Plane Ende-zu-Ende gesichert (bezüglich UE und 5G-Core) übertragen werden. Dies verringert entsprechende Risiken bezüglich Verletzungen der Schutzziel Vertraulichkeit und Integrität durch das 5G-RAN.

Der Angreifer Cloud-Betreiber wird bei den Risikoanalysen nicht berücksichtigt, da die 3GPP-Spezifikation keine konkreten Vorgaben zur Umsetzung eines 5G-RANs macht. Insofern kann hier ein Cloud-basiert Lösung zum Einsatz kommen, genauso kann aber auch eine Cloud-freie, monolithische Umsetzung erfolgen.

Bezüglich der nachfolgenden Analysen ist anzumerken, dass sie insgesamt aus Sicherheitssicht betrachtet insofern den „best-case“ darstellen, da auf Grund der zeitlichen Beschränkungen nicht alle möglichen Angriffsszenarien tiefgreifend analysiert werden konnten. Offene Fragen sind hier unter anderem:

- Kann das RAN die Wahl der Sicherheitsmechanismen bezüglich der Control-Plane-Absicherung beeinflussen, so dass hier ggf. trotz vorgesehener End-zu-Ende Sicherung doch erfolgreiche Angriffe durch ein böswilliges RAN möglich sind?
- Welches Risiko ergibt sich aus den Lawful-Interception-Schnittstellen?

Worst-Case: Auf Grund der oben getroffenen Aussagen ergibt sich für den wort-case, dass keinerlei Sicherheitsmaßnahmen (ausgenommen Integritätsschutz bezüglich Control Plane) umgesetzt sind. Insofern ergibt sich für den Angreifer „Außenstehender“ und die Perspektive „Nutzer“ ein hohes Risiko für die Verletzung der Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit. Gleiches gilt auch für die Perspektive des Netzbetreibers. Auf Grund des hohen Risikos für diese beiden Stakeholder wird auch für den Stakeholder „Staat“ von einem hohen Risiko ausgegangen. Einzig und allein die Integrität bildet hier die Ausnahme, wodurch das Risiko als gering eingeschätzt wird.
Best-Case: Im best-case verbessert sich die Situation durch die Anwendung der vorgesehenen Sicherheitsmaßnahmen. Für den Angreifer „Außenstehender“ und alle Stakeholder-Perspektiven wird insofern von einem geringen Risiko für eine Verletzung der Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit ausgegangen. Bezogen auf den Angreifer „Nutzer“ ergibt sich als einziger Unterschied, dass das Risiko für Schutzzielverletzungen bezüglich Zurechenbarkeit als mittel eingeschätzt wird, da ein Nutzer „gültige“ Nachrichten erzeugen kann, bei denen Dritte nicht feststellen können, ob sie vom Nutzer oder vom RAN stammen. Bezüglich des Schutzziels Verfügbarkeit wird sowohl für den Angreifer „Außenstehender“ als auch für den Angreifer „Nutzer“ von einem mittleren Risiko ausgegangen. In der Literatur werden hier bezüglich des Angreifers „Nutzer“ Angriffsmöglichkeiten skizziert, die darauf basieren, dass der Angreifer die Kontrolle über eine Vielzahl von mit dem 5G-RAN verbundenen (IoT-)Geräten erlangt und diese dann für einen verteilten Verfügbarkeitsangriff (dDoS) auf das 5G-RAN nutzt. Bezüglich des Angreifers „Außenstehender“ finden sich in der Literatur Hinweise, dass durch intelligentes Aussenden von Funksignalen die Übertragung auf der Uu-Schnittstelle stark beeinträchtig werden kann (Jamming-Angriffe). Von den Verfügbarkeitsangriffen sind sowohl die User Plane als auch die Control Plane betroffen. Insofern wird davon ausgegangen, dass sowohl ein 5G-Nutzer als auch der 5G-Netzbetreiber betroffen sein kann, was in der Konsequenz dann auch ein mittleres Risiko für den Stakeholder „Staat“ impliziert.
Bezüglich des Angreifers „RAN-Betreiber“ wird auch im best-case für die Nutzer-Perspektive von einem hohen Risiko ausgegangen, da dem RAN die Schlüssel zur Absicherung von Vertraulichkeit und Integrität bekannt sind und insofern diese Sicherungsmaßnahmen nicht gegen einen böswilligen RAN-Betreiber schützen. Hier sollte der 3GPP-Standard dahingehend überarbeitet werden, dass auch für die Übertragung der User Plane Daten eine Ende-zu-Ende Sicherung zwischen UE und 5G-Core möglich ist. Bezüglich des Stakeholders „Netzbetreiber“ wird die Situation etwas besser eingeschätzt, da zumindest die Control Plane Nachrichten Ende-zu-Ende gesichert sind. Für alle Stakeholder gilt, dass ein hohes Risiko bezüglich Verfügbarkeit besteht, da ein funktional-ordnungsgemäßer Betrieb des RAN entscheidend für die Verfügbarkeit eines 5G-Netzes ist.
Das Risiko bezüglich eines Insiders, also einer kompromittierten Komponente, wird ähnlich eingeschätzt, wie das Risiko bezüglich eines nicht-vertrauenswürdigen RAN-Betreibers. Hat der Angreifer Zugriff auf die 5G-RAN-Komponente, die die Schlüssel zur Sicherung der Kommunikation verwaltet, so kann der Insider ebenfalls die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit bezüglich User Plane Daten erfolgreich angreifen. Gleichzeitig kann er die Verfügbarkeit trivial einschränken, indem falsche Schlüssel zur Entschlüsselung angewendet bzw. zur Verfügung gestellt werden.
Für das Schutzziel Privacy wurde bezüglich der Angreifer „Außenstehender“ und „Nutzer“ von einem geringen Risiko ausgegangen, da durch 3GPP eine Reihe von Maßnahmen vorgesehen sind, um ein Tracking von UE zu unterbinden. Hier ist anzumerken, dass Angriffe mit Hilfe von „wireless fingerprinting“ der UE unberücksichtigt blieben. Unter Berücksichtigung dieser Art von Angriffen ist von einem mittleren Risiko auszugehen. Da Privacy-Risiko im Falle der Angreifer „Insider“ und „RAN-Betreiber“ kann nicht verlässlich eingeschätzt werden. In der

Literatur sind Angriffsmöglichkeiten erwähnt, allerdings bedarf es hier umfangreicher weiterführender Analysen, um zu einer fundierten Einschätzung gelangen zu können.

Angreifer	Perspektive (Stakeholder)														
	End-Nutzer					Staat					Netzbetreiber				
	Schutzziele					Schutzziele					Schutzziele				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Außen-stehender															
Nutzer															
Insider															
Cloud-Betreiber															
RAN-Betreiber															

Tabelle 16: Risikobewertung des 3GPP 5G RAN