



Estudar

Análise de risco open-RAN

***5GRANR***



Versão: 1.0.8

Data: 9 de novembro de 2021

Autores: Stefan Köpsell (Instituto Barkhausen) Andrey Ruzhanskiy (Instituto Barkhausen)

Andreas Hecker (Avançando redes individuais GmbH) Dirk Stachorra (avançando redes individuais GmbH) Norman Franchi (avançando redes individuais GmbH)

Resumo Executivo

Este estudo trata da questão de quais riscos de **segurança decorrem** da implementação do **O-RAN** de um 3GPP-RAT especificado pela Aliança O-RAN. Primeiro, é realizada uma descrição funcional de um RAN 3GPP e da arquitetura O-RAN. Com base nisso, foi realizada uma análise de risco, levando em conta os **objetivos de** proteção de **confiabilidade, integridade,** **atribuição,** **disponibilidade** **e** **privacidade.** Para avaliar os riscos associados à violação dos objetivos de proteção, **três** **partes interessadas** são levadas em conta, ou seja, um **usuário** de uma rede 5G, a **operadora** de uma rede 5G e o **Estado** como persona para uma perspectiva social.

Como as especificações O-RAN disponíveis atualmente ainda são bastante inespecíficas em muitos lugares e fazem poucas especificações, especialmente na área de segurança, duas perspectivas foram levadas em conta na análise de risco. Por umlado,uma **perspectiva de pior caso**, i n que nenhuma das medidasde segurança opcionais foi implementada e uma **consideração**melhor emque se presumia que todas as medidas de segurança (opcionais) foram realmente implementadas.

A análise de risco também levou em conta vários **atacantes poderosos:** um **atacante externo, um usuário 5G, um insider, o operador de nuvem** e o **operador RAN.**

Como resultado da análise de risco, verificou-se que um **grande número** de interfaces e componentes especificados em O-RAN representam riscos médios a altos **riscos de segurança.** Isso não é surpreendente, uma vez que o processo de desenvolvimento atual das especificações O-RAN não se baseia no paradigma da**"segurança/privacidade por design/padrão"** e também nos princípios da **segurança** **multilateral** (mínimo As garantias relativas a todas as partes envolvidas)  **não** foram levadas em **conta.**

Durante a realização da análise de risco, algumas **possibilidades de melhoria para** minimização de riscos poderiam ser identificadas. Estas podem ser encontradas como recomendações no final do estudo. É importante ressaltar que os aprimoramentos de segurança estão **agora** incluídos na especificação para **evitar** um desastre de **segurança,**como aconteceu no desenvolvimento das normas 3GPP, desta vez.



Essa análise de risco foi encomendada e financiada pelo Escritório Federal de Segurança da Informação (BSI). O BSI não influenciou os resultados.

Tabela de conteúdos

1. [Introdução 5](#_TOC_250068)
2. [Rede de acesso de rádio de próxima geração (NG-RAN) 6](#_TOC_250067) 
   1. [Introdução e termos 6](#_TOC_250066) 
      1. Open-RAN 7
      2. [O-RAN 7](#_TOC_250065)
      3. [DICA 8](#_TOC_250064)
      4. [Outros grupos 8](#_TOC_250063)
   2. [Arquitetura NG-RAN 8](#_TOC_250062) 
      1. [Especificação de acordo com 3GPP 9](#_TOC_250061)
      2. [Controle/separação do plano do](#_TOC_250060) usuário[9](#_TOC_250060)
      3. [Especificação de acordo com O-RAN 11](#_TOC_250059)
      4. [Modelo de integração](#_TOC_250058) open-RAN[14](#_TOC_250058)
      5. [Conceitos de compartilhamento RAN 15](#_TOC_250057)
   3. [Descrição de O-RAN-Schnit tstellen 18](#_TOC_250056) 
      1. [Interface O1 18](#_TOC_250055)
      2. [Interface O2 22](#_TOC_250054)
      3. [Interface A1 25](#_TOC_250053)
      4. [Interface R1 26](#_TOC_250052)
      5. [E2-Schnit tstelle 27](#_TOC_250051)
      6. [Abra fh](#_TOC_250050)  [cus interface 29](#_TOC_250050)
      7. [Interface FH M-Plane 30](#_TOC_250049)
      8. [Interface de Transporte](#_TOC_250048)  Cooperativo [(CTI) 31](#_TOC_250048)
   4. [Aplicações de otimização e machine](#_TOC_250047)  [learning 32](#_TOC_250047) 
      1. [Funções RIC para](#_TOC_250046)  [otimização RAN 32](#_TOC_250046)
      2. [xApps/rApps 32](#_TOC_250045)
      3. [Machine Learning (ML) 33](#_TOC_250044)
   5. [Software O-RAN 35](#_TOC_250043)
3. [Metodologia e Escopo 37](#_TOC_250042) 
   1. [Geral e Escopo 37](#_TOC_250041)
   2. [Metodologias de](#_TOC_250040) análise de risco[37](#_TOC_250040)
   3. [Objetivos de proteção previstos](#_TOC_250039)   [38](#_TOC_250039)
   4. [Atacantes](#_TOC_250038)  em consideração [—](#_TOC_250038)  [Modelo atacante 39](#_TOC_250038)
   5. [Perspectivas 41](#_TOC_250037) 
      1. [Perspectiva](#_TOC_250036) do stakeholder[41](#_TOC_250036)
      2. [Implementação de medidas de segurança 42](#_TOC_250035)
      3. [Resumo 42](#_TOC_250034)
   6. [Metodologia aplicada para](#_TOC_250033)  [análise de risco 42](#_TOC_250033)
4. [Estudos](#_TOC_250032) existentes[46](#_TOC_250032) 
   1. [Cenário de](#_TOC_250031)   [ameaça](#_TOC_250031)  ENISA para [redes](#_TOC_250031)  [5G](#_TOC_250031)  [46](#_TOC_250031)
   2. [Análise de risco](#_TOC_250030) 5G da UE[46](#_TOC_250030)
   3. [Caixa de ferramentas](#_TOC_250029) da UE[47](#_TOC_250029)
   4. [Eua estuda e relata 47](#_TOC_250028)
   5. ["As Propostas de Praga" 48](#_TOC_250027)
   6. [Análise de modelagem](#_TOC_250026)  [e remediação](#_TOC_250026) de ameaças de [segurança](#_TOC_250026)  O-RAN[48](#_TOC_250026)
   7. [GSMA Mobile Telecomunicações](#_TOC_250025)  [Segurança Paisagem 49](#_TOC_250025)
5. [Análise de risco](#_TOC_250024) O-RAN[51](#_TOC_250024) 
   1. [Atacantes: Operador de Nuvem](#_TOC_250023)  e Operador [5G RAN 51](#_TOC_250023)
   2. [Análise de risco O-Cloud 52](#_TOC_250022)
   3. [Análise de risco Interface O2 52](#_TOC_250021)
   4. [Análise de risco Interface O1 54](#_TOC_250020) 
      1. [Análise de](#_TOC_250019)  risco da [interface geral O1 54](#_TOC_250019)
      2. [Análise de](#_TOC_250018)  risco da [interface O1](#_TOC_250018)  entre [O-DU](#_TOC_250018)  [e](#_TOC_250018)  [SMO 57](#_TOC_250018)
   5. [Análise de risco Interface A1 58](#_TOC_250017)
   6. [Análise de risco Interface R1 59](#_TOC_250016)
   7. [Análise de risco Interface E2 61](#_TOC_250015)
   8. [Análise de Risco Open Fronthaul](#_TOC_250014)  [M-Plane 63](#_TOC_250014)
   9. [Análise de Risco Frente Aberta](#_TOC_250013)  [CUS-Plane 65](#_TOC_250013)
   10. [Análise de risco interface CTI 66](#_TOC_250012)
   11. [Análise de](#_TOC_250011)  risco de [outras interfaces 67](#_TOC_250011)
   12. [Análise de risco rApps 68](#_TOC_250010)
   13. [Análise de risco xApps 69](#_TOC_250009)
   14. [Aprendizado](#_TOC_250008)  [de](#_TOC_250008) máquina de análise de risco[70](#_TOC_250008)
   15. [Análise de risco sumária O-RAN 70](#_TOC_250007)
6. [Resumo e perspectiva 72](#_TOC_250006) 
   1. [Recomendações 72](#_TOC_250005)

[6.1.1 3GPP 72](#_TOC_250004)

[6.1.2 O-RAN 73](#_TOC_250003)

1. [Lista de fontes 76](#_TOC_250002)
2. [Lista de abreviaturas 80](#_TOC_250001)

[Anexo A: 3GPP 5G](#_TOC_250000)  [RAN Análise de risco 84](#_TOC_250000)

# Eintrodução

As redes móveis da 5ª geração (5G) oferecem uma variedade de novos casos de uso, que afetam particularmente o campo das "coisas" de rede. Como resultado, o 5G está se tornando cada vez mais central no campo das infraestruturas básicas de comunicação – especialmente como uma infraestrutura básica de comunicação para infraestruturas críticas como energia e abastecimento de água, logística e transporte. Portanto, é necessário estar atento aos riscos decorrentes do uso do 5G como infraestrutura de comunicação no sentido de segurança de TI e proteção de dados. Essa análise de risco é, portanto, o objetivo principal deste estudo. Este estudo não se trata de um sistema 5G global, consistindo essencialmente da rede de acesso à rádio 5Gz(5G RAN) e da rede principal 5G (núcleo 5G). Em vez disso, apenas o RAN 5G é considerado na análise de risco. Por sua vez, o foco está em uma proposta concreta de implementação de um RAN 5G, que é especificado pela O-RAN ALLIANCE[1.](#_bookmark0) Esta proposta de implementação é referida como O-RAN.

Assim, o objetivo principal deste estudo é uma análise de risco O-RAN. Isso apresenta as ameaças e riscos decorrentes das especificações atuais e pode servir de base para a tomada de decisões sobre as medidas futuras necessárias para minimizar o risco.

Primeiro, uma visão geral da Rede de Acesso por Rádio de Próxima Geração (NG-RAN) é fornecida do ponto de vista técnico-funcional. Em particular, a arquitetura O-RAN é discutida. Isso é seguido por uma introdução à metodologia de análise de risco utilizada neste estudo. Em particular, os objetivos de proteção considerados e o modelo de atacante subjacente são explicados com mais detalhes. Ocapítulo 4 a seguirdiscute brevemente os estudos existentes no campo da análise de risco e ameaças no campo do NG-RAN ou ng-RAN. O-RAN. Particularmente notáveis aqui são as análises realizadas pela própria Aliança O-RAN.

Isso é seguidopela parte principal deste estudo, a análise real de risco O-RAN. Uma análise de risco correspondente em relação ao NG-RAN em geral pode ser encontrada no apêndice A. Para a compreensão da análise de risco O-RAN, não é necessário conhecimento de fundo sobre os riscosgerais de NG-RAN. Se este não for o caso, o leitor é aconselhado a ler o apêndice A primeiro e, em seguida, a análise de risco O-RAN no Capítulo 5. A análise de risco é realizada pela primeira vez no que diz respeito a componentes individuais e interfaces do O-RAN, a fim de fornecer uma avaliação dos riscos de segurança para O-RAN como um todo.

O estudo conclui com uma recomendação sobre medidas que podem levar a uma melhoria na segurança do O-RAN.

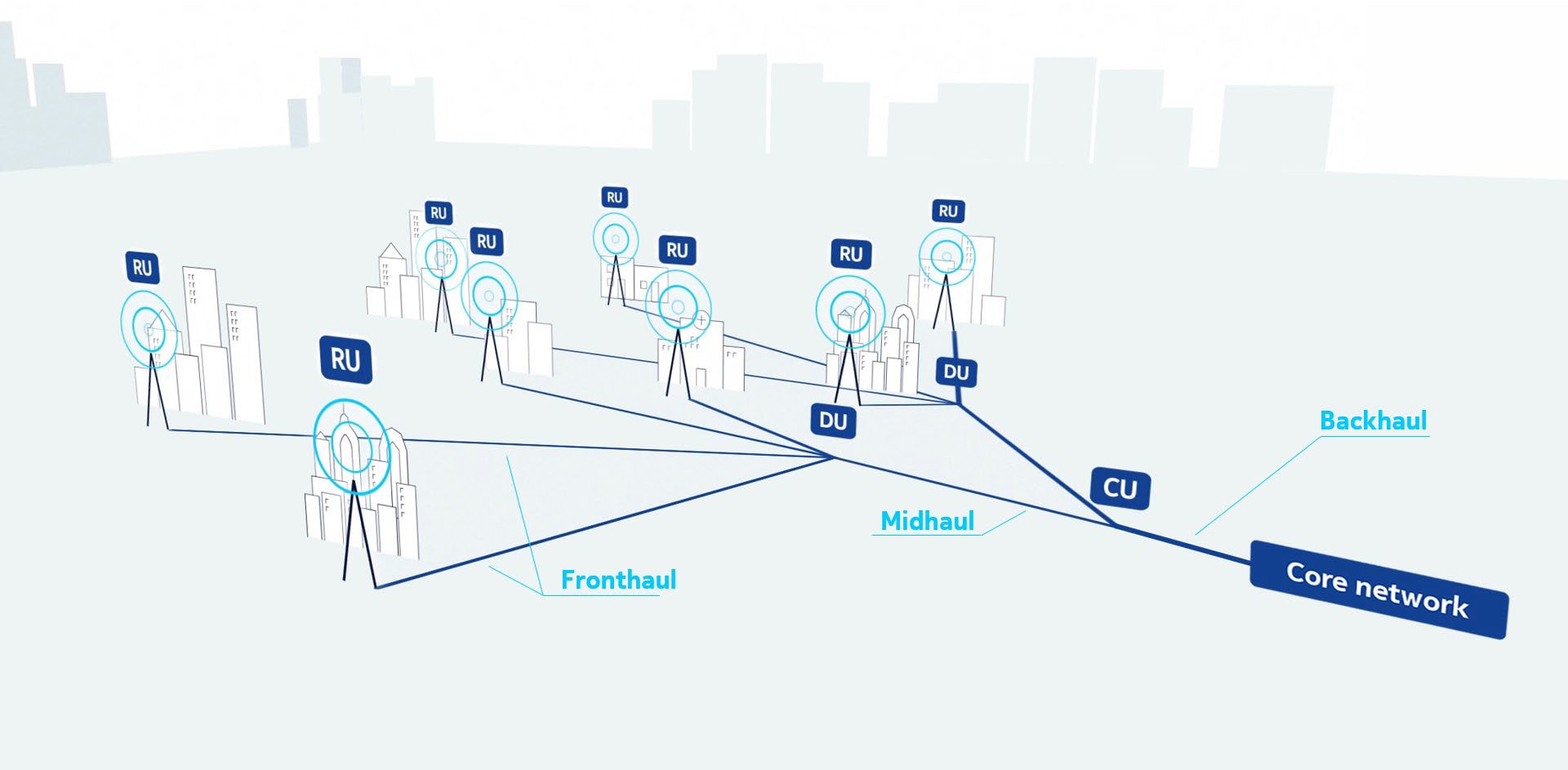
1 https[://w](http://www.o-ran.org/)ww[.o](http://www.o-ran.org/)-[ran.org/](http://www.o-ran.org/)

# Rede de acesso de rádio de próxima geração (NG-RAN)

NG-RAN, Open-RAN, O-RAN; estes termos são componentes atuais do tópico RAN considerado aqui e aparecem repetidamente ao longo de todo o documento. Em particular, as duas últimas expressões são muitas vezes usadas inocentemente como sinônimos. Obviamente,porque eles não só soam semelhantes, mas também estãoindissociáveis. A forma curta é: A "Aliança O-RAN" foi formada para realizar o conceito "Open-RAN". A seção2.1 explica como o contexto dos três nomes é desenvolvido no sub-termo.

A seção 2.2 vai mais fundo na arquitetura NG-RAN, começando com o padrão 3GPP e terminando com as especificações através do O-RAN. A Seção 2.3 explica as interfaces introduzidas pelo O-RAN que são essenciais para as considerações de segurança nos capítulos posteriores. A Seção 2.4 trata do tema das aplicações, em especial o tema

"Machine Learning" (ML) é colocado em foco pela O-RAN. A seção 2.5 conclui com informações sobre o software O-RAN existente, que está aberto a todas as partes interessadas para desenvolver suas próprias soluções.



*Figura 1:* *Representação simplificada*  *de* *uma*  *arquitetura* Ran Aberta *(Fonte:* *Nokia)*

## Eintrodução e termos

A Rede de Acesso de Rádio (RAN) forma o link entre dispositivos finais e a rede principal em uma rede móvel. Para a quinta geração (5G) de redes móveis, o 3GPP especificou o New Radio (NR) e o Next Generation RAN (NG-RAN) na Versão 15. O NG-RAN fornece acesso via NR e E-UTRA (Evolved UMTS Terrestrial Radio Access), a interface de ar do 4G/LTE (Evolução de Longo Prazo). A operação mista das estações base LTE e NR conectadas a uma rede central (4G ou 5G) é referida como modo não autônomo (modo NSA); operação baseada exclusivamente na rede central NR e 5G é referida como modo autônomo (modo SA) [1].

Os primeiros estudos do 3GPP sobre NG-RAN começaram na Versão 14 e resultaram no Relatório Técnico [2]. Além da capacidade de trabalhar nos modos SA e NSA, ele já inclui outra característica do NG-RAN: a capacidade de separar a estação base 5G em uma unidade centralizada (CU) e uma ou mais unidades distribuídas (DUs). Adivisão da estação base fornece possibilidades adicionais e liberdade para implantação, como descrito na Figura 1 como exemplo.

* + 1. Open-RAN[2](#_bookmark1)

Paralelamente ao trabalho ng-RAN do 3GPP, o conceito da chamada "abertura do RAN" ("Open-RAN") tem sido perseguido por vários anos em oposição à "maneira tradicional". Na abordagem tradicional da implantação do RAN, como encontrado na maioria das redes móveis públicas, o RAN é uma solução monolítica. As interfaces internas dentro desta solução são proprietárias e não reveladas para provedores de terceiros. O hardware associado é umasolução autônoma que não é compatível comdispositivos de outros fabricantes. As funções e interfaces proprietárias de uma solução RAN monolítica são altamente otimizadas, mas, portanto, inflexíveis. Assim, o objetivo na busca do conceito Open RAN é tornar o RAN menos dependente da tecnologia proprietária, definindo especificações para interfaces abertas e fornecendo elementos de rede ou funções a partir do O hardware pode ser abstraído.

As operadoras de redes móveis estão altamente motivadasa implementar o conceito Open RAN porque os equipamentos de suas redes estão associados acustos muito altos e, ao mesmo tempo, o mercado de equipamentos RAN é caracterizado pela baixa concorrência. A cada nova geração de comunicações móveis, toda a tecnologia deve ser substituída por bilhões de euros ou construída em paralelo. Além disso, o hardware se torna mais complexo a cada extensão, mais aplicativos e recursos devem ser suportados e, assim, os preços sobem. Com Ericsson, Nokia e Huawei, por outro lado, apenas três principais provedores estão disponíveis. Além disso, os produtos da Huawei não podem ser usados por operadoras móveis em alguns países. A entrada geralmente gradual de novos fornecedores não é possível porque o equipamento para ran deve ser fornecido completamente por um provedor devido à autonomia das soluções do produto [3]. A busca do conceito Open RAN deve, portanto, possibilitar, no futuro, aumentar a concorrência e reduzir custos, permitindo que o RAN seja construído e operado com a ajuda de componentes interoperáveis de diferentes fabricantes. E a modularização deve abrir a possibilidade de apenas poder substituir componentes (de software) porextensões necessárias do RAN e não da tecnologiacompleta.

Com relação aos elementos já padronizados pelo 3GPP, serão identificados os próximos passos na busca do conceito Open RAN. Assim, além dos elementos e DU já padronizados,o ambiente Open RAN divide a Unidadede Rádio (RU), que está integrada ou localizada perto da antena. Assim, o Open-RAN define o fronthaul como uma conexão entre ru e o DU. O midhaul entre o DU e o CU, bem como o backhaul para conectar a RAM ao núcleo já são definidos pelo NG-RAN padronizado por 3GPP (ver figura 1).

### O-RAN

Com base na ideia da Open-RAN, a Aliança O-RAN foi fundada em 2018 com empresas do setor de telecomunicações, principalmente um consórcio internacional de operadoras de rede. O objetivo desta associação é a padronização de um NG-RAN, que é em grande parte baseado em componentes virtualizados e interoperáveis. A flexibilidade desejada deve permitir soluções sob medida para aplicações individuais, que devem ser reconfiguradas e otimizadas eficientemente em curto prazo, se necessário. O resultado desses esforços é o desenvolvimento da arquitetura O-RAN, que se intercala com a arquitetura RAN padronizada pelo 3GPP. A arquitetura O-RAN deve

2 Existem diferentes ortografias deste termo, que são usadas sinônimo em muitos lugares: com ou sem hífen ou escritas juntas. Neste estudo, a grafia "Open-RAN" é escolhida, a menos que o link para uma referência especisse uma ortografia diferente.

são geralmente vistos como um suplemento aos padrões 3GPP existentes. A longo prazo, os resultados do O-RAN podem levar de volta aos padrões do 3GPP. Até então, a arquitetura O-RAN existe como uma adição à arquitetura 3GPP.

A O-RAN Alliance apoia a comunidade de software O-RAN em cooperação com a Linux Foundation. No verão de 2020, a aliança anunciou que fará uma parceria com a ONF (Open Network Foundation) para lançar o projeto 5G SD-RAN (5G Software-Defined Radio Access Network) para promover e facilitar a criação de software de código aberto para implementações móveis 4G e 5G RAN.

A existência do grupo SD-RAN nãoimplica que todos os componentes da arquitetura O-RAN sejam de código aberto ou mesmo que eles devem ser baseados no código-fonte aberto desenvolvido pelo grupo de projeto. No entanto, a comunidade de software que deve surgir em torno deste projeto de código aberto influenciará o desenvolvimento de aplicativos para configuração e otimização. Um exemplo disso é a participação do RIA (RAN Intelligence and Automation), um subgrupo da TIP (ver Seção 2.1.3), no programa 5G SD-RAN. O RIA visadesenvolver e implantaraplicativos baseados em IA/ML[3](#_bookmark2)para uma variedade de casos de uso ran, incluindo SON (Self-Organizing Network), RRM (Radio Resource Management) e mMIMO (Massive Multiple Input and Multiple Output) [4].

### TIP

O Telecom Infra Project (TIP) foi fundado em 2016 como uma colaboração orientada para engenharia. O objetivo deste projeto é construir e fornecer uma infraestrutura global de redes de telecomunicações com a possibilidade de acesso global para todas as partes interessadas. A TIP cria um ecossistema de fornecedores de hardware e software, inicia plugfests e desenvolve projetos. A TIP não escreve especificações, masestá ativa em todo o mundo no financiamento, treinamento e implementação de soluções Open RAN.

O projeto "OpenRAN" da TIP e a Aliança O-RAN anunciaram um acordo de ligação em 2020 para garantir sua consistência no desenvolvimento de soluções ran interoperáveis, desagregadas e abertas [5].

### Outros grupos

Além do 3GPP e do TIP, existem outras organizações que estão envolvidas no RAN aberto e contribuem para a especificação O-RAN e desenvolvimento de O-RAN. Estes incluem o Small Cell Forum, a já mencionada Open Networking Foundation (ONF) e a OpenAirInterface Software Alliance (OSA) [4].

## Arquitetura NG-RAN

Esta seção explica a arquitetura do NG-RAN com mais detalhes. Começa com a especificação 3GPP (Seção 2.2.1) e uma explicação da divisão dos níveis de usuário e controle (Seção 2.2.2), que servem de base para a arquitetura O-RAN (Seção 2.2.3). A seção 2.2.4 discute os desafiosde integrar componentes RAN de diferentes fabricantes antes de uma apresentação sobre o compartilhamento RAN (Seção 2.2.5) e uma seleção de opções que a allicance O-RAN pode oferecer com base no conceitos existentes.

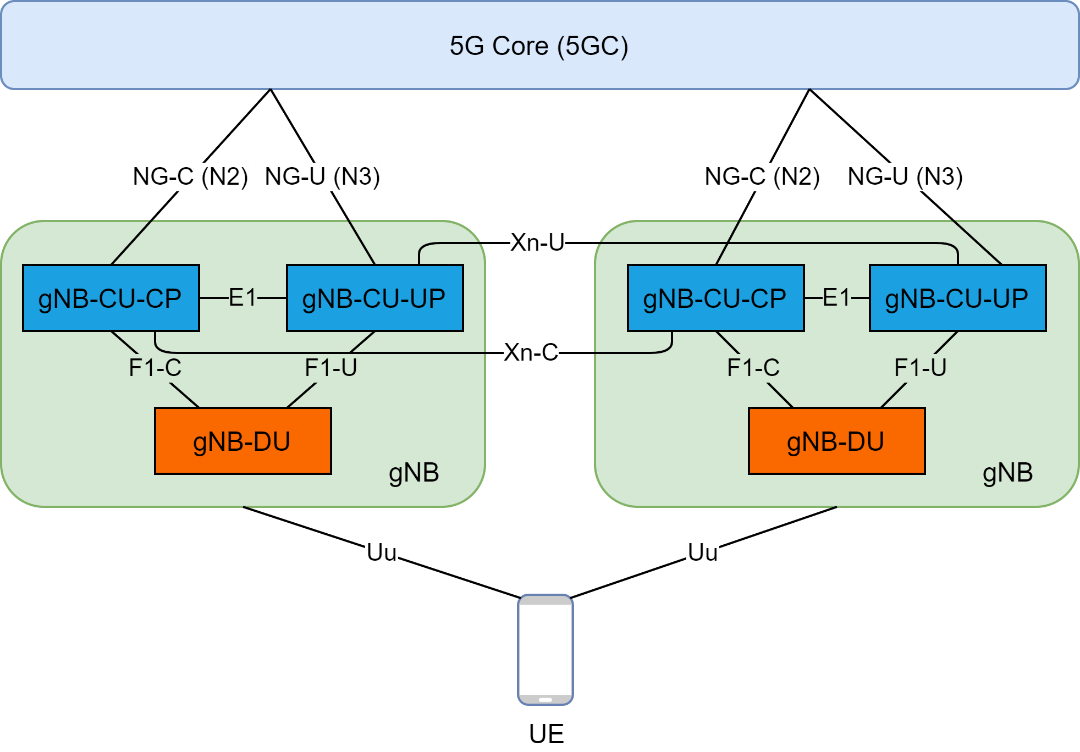
3 IA significa "Inteligência Artificial" (IA), refere-se à capacidade de um computador de imitar o comportamento do pensamento humano, e é um termo genérico para a descrição de desempenho de uma máquina. O machine learning (ML), poroutrolado, descreve um grupo de processos para extrair insights de dados para aplicações de IA.

### Especificação de acordo com o 3GPP

A Figura 2 mostra um NG-RAN composto por duas estações base 5G (NodeBs de próxima geração, gNBs), bem como as interfaces para conexão com o núcleo e os dispositivos finais. O gNB é dividido em duas funções lógicas, a e a DU (ver introdução na Seção 2.1).

O DU é a unidade de banda base em um RAN 5G. Ele executa o processamento da Camada 1 e da Camada 2 e executafunções críticas como codificação/decodificação, agendamento, processamento de MIMO e beamformagem. Na faixa de submegêmedo, toma decisões sobre a alocação de recursos de rádio dentro de uma célula, com base em fatores como regras vinculantes (políticas), condições de interferência ou o tipo e distribuição de dispositivos de usuário.

O CU é um novo nó em 5G que não existe como uma função discreta em 4G. Na arquitetura RAN 3GPP, a oferece recursos de Camada 3-F,como conectividade e gerenciamentode mobilidade. Ele é dividido no CU-UP para processamento de plano de usuário e o CU-CP para processamento de plano de controle (ver seção 2.2.2 abaixo). A interface E1 definida em [6] é usada para trocar dados de configuração e outras informações entre essas unidades desagregadas. Além disso, CU-CP e CU-UP estão conectados ao DU através das interfaces F1-C e F1-U, que são definidas em [7]. Na direção do núcleo 5G, há a interface NG-C entre o CU-CP e o AMF (Access and Mobility Management Function), bem como a interface NG-U entre o CU-UP e a UPF (User Plane Function).



*Figura 2:* *Arquitetura 3GPP* *para* *5G* *NR*

Deve-se notar que a arquitetura 3GPP não especifica a Unidade de Rádio Remota (RRU),

Ou seja, a implementação da interface entre as camadas PHY e RF é deixada aos provedores.

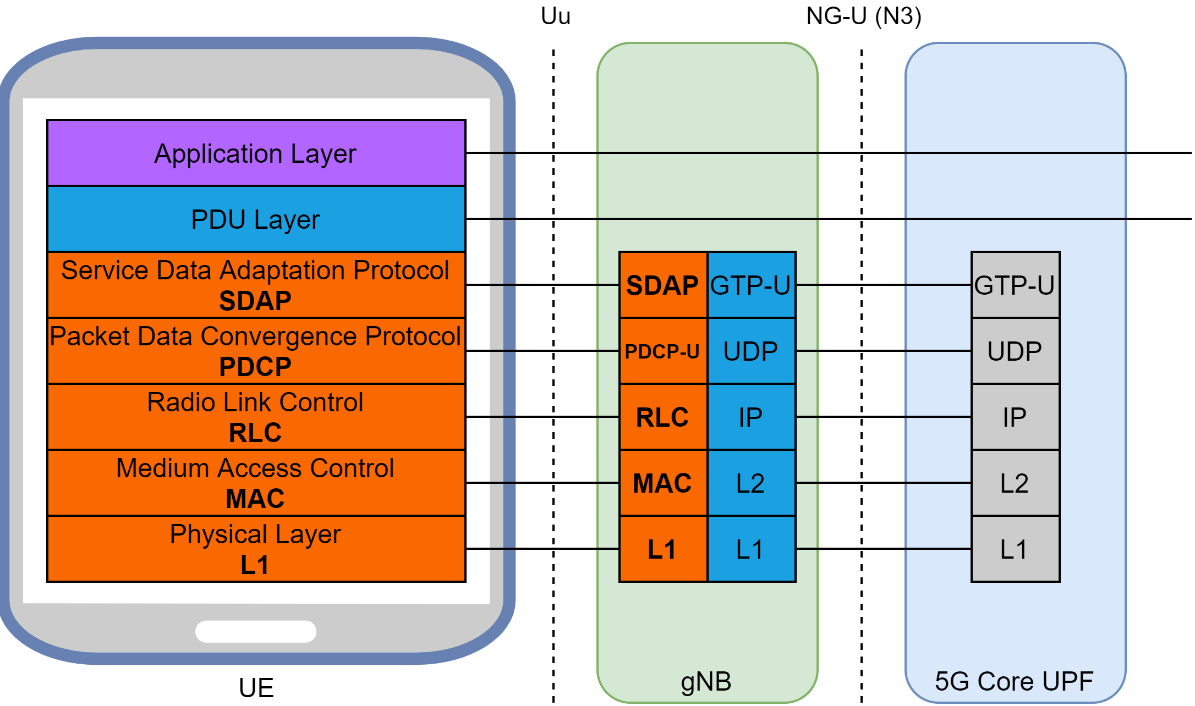
### Separação do plano de controle/usuário

Nas redes móveis, o Controle/Separação de Plano do Usuário (CUPS) refere-se à separação completa do Plano de Controle (plano de controle) e do Plano de Usuário (nível de usuário). O Control Plane é responsável por funções como gerenciar a conexão do usuário,definir políticas QoS ou autenticação do usuário. O Avião do Usuário é responsável pelo transporte do tráfego de dados.

Em relação ao 4G, o CUPS foi introduzido pela primeira vez na Versão 3GPP 14 para o EPC (Evolved Packet Core) [8] e estendido para sistemas 5G na Versão 15 [9]. A principal motivação para essa separação é poder escalar o avião do usuário independentemente do plano de controle e, assim, permitir aos operadores maior flexibilidade no dimensionamento desuasredes. Por exemplo, o Plano do Usuário pode ser estendido à medida que o tráfego de dados aumenta sem alterar as funções do Plano de Controle.

O CUPS permite a configuração gratuita do avião do usuário para atender aos requisitos específicos do aplicativo para encaminhamento, encapsulamento de dados, controle de tráfego ou outras tarefas recebidas de acordo com as especificações do plano de controle. Isso permite a implementação de diferentes soluções para transmissão de dados do usuário, que coexistem no mesmo plano de usuário e são selecionadas dinamicamente de acordo com as exigências do tráfego específico poder. Além disso, um plano de usuário separado permite atrasos mais curtos no transporte de tráfego de dados e, portanto, permite o cumprimento de requisitos de latência mais elevados.

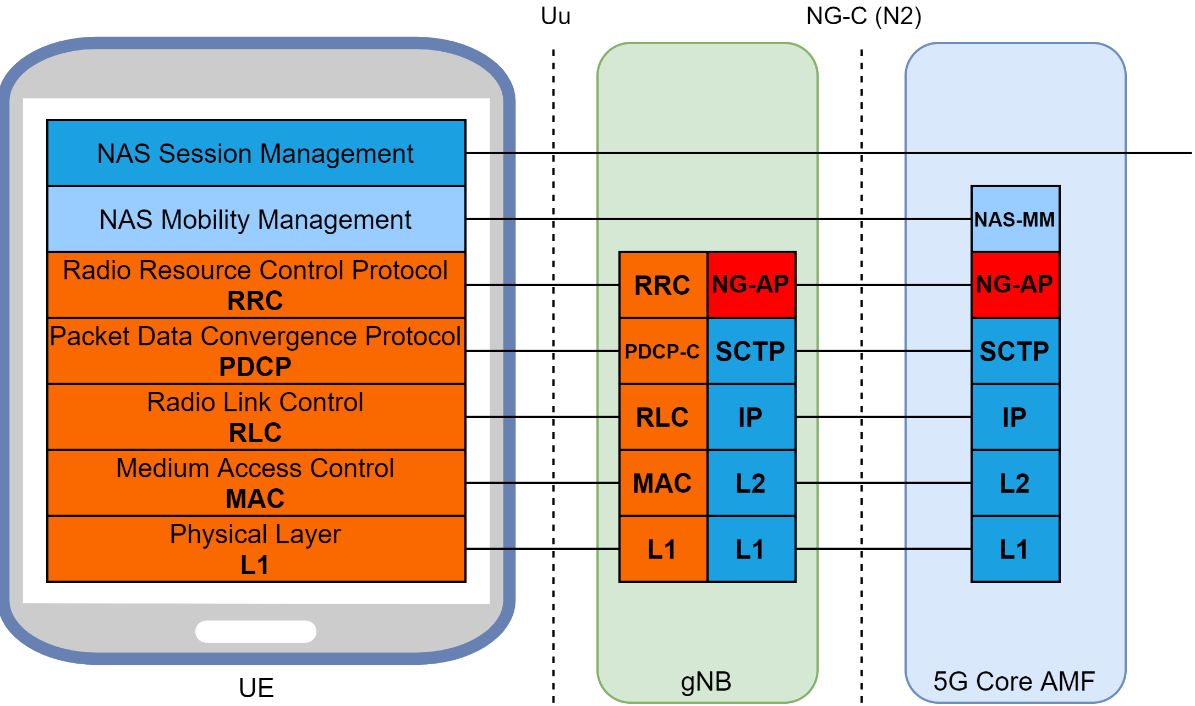
A Figura 3 mostra os protocolos utilizados no plano de usuário entre a UE e o gNB na interface Uu e sua conversão para os protocolos utilizados na interface NG-U (N3) entre o gNB e o UPF no núcleo 5G. Por padrão, existem a camada física L1 e a camada MAC L2 para acesso à rede. O RLC (Radio Link Control) é mapeado via IP. O PDCP (Packet Data Convergence Protocol) é convertido para o UDP (User Datagram Protocol) no gNB. UDP é um protocolo de transmissão sem conexão e não confiável que também não está protegido nem protegido. O SDAP (Service Data Adaptation Protocol) é convertido em GTP-U (GPRS Tunneling Protocol – User). Os túneis GTP-U são usados para transmitir unidades de dados de pacotes de transporte encapsulados (T-PDUs) e para sinalizar mensagens entre um par específico de pontos finais de túnel GTP-U. O ID do ponto final do túnel (TEID) contido no cabeçalho GTP indica qual túnel um T-PDU particular pertence a [10].



*Figura 3:* *Camadas* de protocolo do *avião*  *do* *usuário*

A Figura 4 mostra os protocolos utilizados no Plano de Controle e a conversão no gNB para os protocolos utilizados na interface NG-C (N2) entre o gNB e o AMF no núcleo 5G. As três camadas mais baixas são análogas às camadas do plano do usuário (veja acima). Para o Plano de Controle, o PDCP é convertido em SCTP (Protocolo de Transmissão de Controle de Fluxo). Ao contrário do UDP, o SCTP é confiável,

Protocolo de rede orientado à conexão [11]. O protocolo RRC (Radio Resource Control Protocol) é convertido no gNB para NG-AP (Next Generation Application Protocol), descrito em [12].



*Figura 4:* *Camadas* de registro *do* plano de *controle*

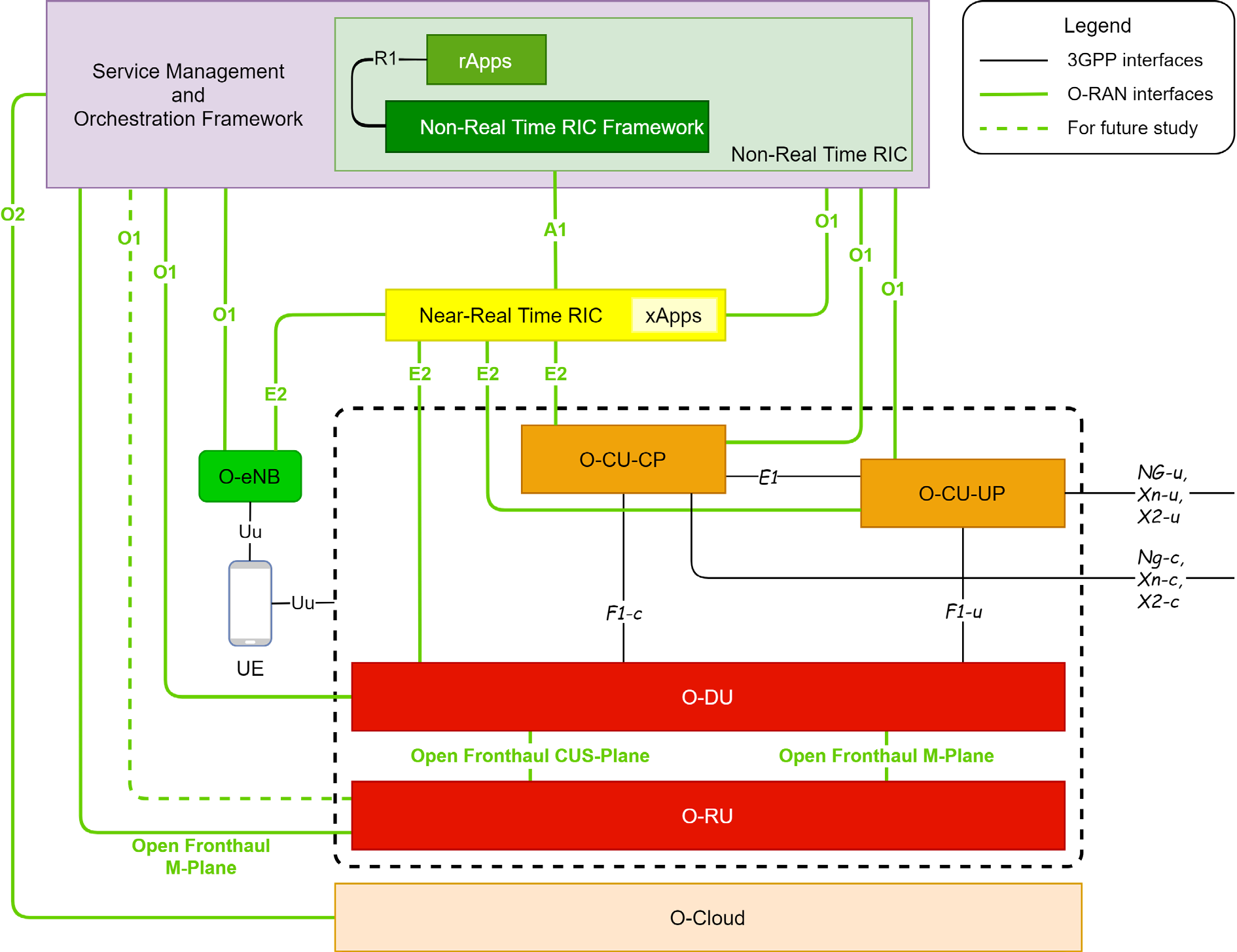
O NAS (Non-Access Stratum) [13] descreve um conjunto de protocolos usados para transmitir mensagens de sinalização radio independentes entre a UE e certas funções da rede central. Os dois protocolos básicos são 5GS Mobility Management (5GMM) e 5GS Session Management (5GSM). O protocolo 5GMM é utilizado entre a UE e a AMF para transportar mensagens para registro, mobilidade e segurança da UE. Também éutilizado para o transporte do protocolo 5GSM, que suporta o gerenciamento da conectividade de sessão de PDU e é aplicado entre UE e SMF (Session Management Function) via AMF.

### Especificação de acordo com O-RAN

A Aliança O-RAN divide ainda mais as funções de rede e DU de acordo com a definição 3GPP. A Figura 5 mostra a arquitetura com suas funções e interfaces e ilustra a divisão de função e interface entre 3GPP e O-RAN [14]. Os elementos CU-CP, CU-UP, DU e eNB (Evolved Node B) definidos em 3GPP recebem o prefixo "O-" nas especificações O-RAN para ilustrar diferenças, o que significa O-RAN. Por exemplo, o O-DU na forma anunciada é a "Unidade Distribuída O-RAN".

As novas funções definidas pelo O-RAN são

* a estrutura de Gestão de Serviços e Orquestração (SMO),
* os RICs (RAN Intelligent Controllers) nas variantes não capazes em tempo real (não-em tempo real) e quase em tempo real (quase em tempo real), abreviados de Non-RT RIC e Near-RT RIC,
* a Unidade Remota (O-RU) e
* a O-Cloud.



*Figura 5: Arquitetura O-RAN lógica, incluindo interface Uu para componentes O-RAN e O-eNB [14]*

As interfaces correspondentes são definidas de acordo com as funções definidas:

* A1 entre Non-RT RIC e Near-RT RIC,
* E2 entre o RIC Near-RT e o O-CU-CP, O-CU-UP, O-DU e O-eNB referidos como nós E2,
* O1 entre o SMO e as unidades gerenciadas Near-RT RIC, O-CU-CP, O-CU-UP, O-DU e O-eNB e, ainda sob investigação, O-RU,
* O2 entre SMO e O-Cloud, bem como
* ==Referências====Links externos== entre SMO e O-RU.

Em princípio, cada uma dessas funções poderia ser desenvolvida e fornecida por diferentes provedores usando hardware convencional, ao mesmo tempo em que assegurava a troca de dados entre os componentes através das interfaces abertas e especificadas. Dessa forma, o objetivo do conceito Open RAN é ser realizado.

Ao construir sua arquitetura baseada na arquitetura 5G NR do 3GPP, a Aliança O-RAN se beneficiará dos recursos avançados de segurança 3GPP introduzidos para 5G e descritos em [16], incluindo

* proteção aprimorada da identidade do usuário via Identificador Oculto por Assinatura (SUCI),
* proteção completa do tráfego do Plano de Controle/Usuário entre UE e gNB (proteção de criptografia e integridade) através da interface de ar,
* proteção total das interfaces gNB, incluindo a interface E1 entre CU-CP e CU-UP e a interface F1 entre e DU,
* controle de rede residencial estendida (autenticação), bem como
* segurança adicional para fatias de rede com base emS ervice Level Agreements (SLAs).
  + - 1. *Estrutura*  *de Gestão* *de Serviços e* *Orquestração* *(SMO)*

Na arquitetura O-RAN, a estrutura SMO é responsável pelo gerenciamento do domínio RAN [14]. Estas incluem as seguintes tarefas:

* + - * + Suporte de FCAPS através da interface O1 entre as funções de rede O-RAN ou no modelo híbrido através da interface Open Fronthaul M-Plane entre SMO e O-RU,
        + Otimização ran através da interface A1 entre o RIC não-RT na estrutura SMO e o RIC Near-RT,
        + Gerenciamento e orquestração o-cloud para o provisionamento de recursos da plataforma, bem como gerenciamento de fluxo de trabalho/carga de trabalho através da interface O2 entre o SMO e o O-Cloud.

Uma interface formal entre SMO e Non-RT RIC ainda não está definida. A implementação do SMO e da fronteira para o quadro RIC não-RT é, portanto, uma decisão de design livre. Certas funcionalidades podem ser incluídas ou excluídas em uma implementação ric não-RT. Essencialmente, as interfaces A1 e R1 são inerentes ao RIC não-RT, enquanto as interfaces O1 e O2 não são.

* + - 1. *Nuvem O*

O O-Cloud é uma plataforma de computação baseada em nuvem que inclui uma coleção de nódulos de infraestrutura física e hospeda os seguintes componentes [14]:

* + - * + as funções O-RAN relevantes Near-RT RIC, O-CU-CP, O-CU-UP e O-DU,
        + os componentes de software de suporte, como sistema operacional, monitor de máquina virtual, tempo de execução de contêineres, etc. bem como
        + as funções adequadas de gestão e orquestração.
      1. *Controlador*  *inteligente* RAN *(RIC)*

O RIC é especificado pela O-RAN Alliance como parte integrante da arquitetura O-RAN. Como pode ser visto na Figura 5, o RIC aparece em duas formas, cada uma adaptada a requisitos específicos de loop de controle e latência. Uma introdução detalhada ao tema do RIC é fornecida [4].

O Near-RT RIC tem interfaces diretas com o O-CU-CP, O-CU-UP e O-DU através da interface E2. Permite seu controle programático em ciclos de tempo de 10 ms a 1 segundo. Devido a rigorosos requisitos de latência com loops de controle inferiores a 10 ms, funções em tempo real como o RRM permanecem no DU; o RIC Near-RT não pode assumir isso [14]. Em princípio e concebível para o futuro, o RIC Near-RT pode configurar programmaticamente o O-DU para melhorar a funcionalidade. Por exemplo, o Near-RT-RIC pode ser usado para alterar o comportamento do agendador no DU. O Grupo de Trabalho 3 (WG3) é responsável pela especificação do RIC Near-RT na Aliança O-RAN, incluindo a interface E2.

O RIC não-RT é especificado para loops de controle de mais de 1 segundo. Estabelece políticas para camadas de rede mais altas. Eles podem ser implementados no RAN através do RIC Near-RT através da interface A1 ou através da conexão SMO com os nós RAN através da interface O1. Por outro lado, o RIC não-RT coleta dados dos componentes RAN através da interface O1, que é gerada em formatos padronizados para atender às funções tradicionais de otimização ran. Devido à sua colocação mais alta na arquitetura, o RIC não-RT pode acessar conjuntos de dados RAN maiores,

gerados ao longo de períodos mais longos de tempo para obter uma visão mais profunda do desempenho e identificar potenciais otimizações que não são visíveis durante o processamento do subato.

O RIC não-RT também pode ser conectado aoutras fontes de dados de rede n (e.B. para otimizar conjuntamente o desempenho da rede sem fio, da rede IP e da nuvem de borda). Também pode acessar conjuntos de dados fora da própria rede, e.B aqueles relacionados ao tráfego, serviços de emergência, clima,eventos públicos emmassa, etc., para que a rede possa se preparar ou responder a eventos no mundo real.

Responsável pela especificação na Aliança O-RAN para o RIC não-RT é o Grupo de Trabalho 2 (WG2) juntamente com a interface associada A1. A interface O1 faz parte do Grupo de Trabalho 1 (WG1).

Deve-se notar que os loops de controle introduzidos pelo RIC podem potencialmente entrar em conflito com os procedimentos colocados em prática pelas operadoras móveis para atualizar as políticas para as funções DE DU e CU.

* + - 1. *O-CU e* *O-DU*

Os acenos RAN O-CU-CP, O-CU-UP e O-DU correspondem às unidades cu-CP, CU-UP e DU definidas em 3GPP. Como resultado, o O-CU-CP e o O-CU-UP servem a interface E1 especificada em 3GPP e as interfaces F1-C/F1-U em comparação com o O-DU. Conforme especificado em [17], o O-CU-CP serve os protocolos RRC e PDCP e os protocolos O-CU-UP, o PDCP e SDAP sobre a UE, enquanto o O-DU serve as funções RLC, MAC e High PHY da interface de rádio (ver seção 2.2.2).

O arquiteto O-RAN introduz as seguintes alterações [14]: O O-CU-CP, O-CU-UP e O-DU terminam a interface E2 com o RIC Near-RT e a interface O1 à estrutura SMO. O O-DU opera a interface Open Fronthaul, incluindo a interface Open Fronthaul M-Plane em comparação com a O-RU para suportar o gerenciamento O-RU no modelo hierárquico ou no modelo híbrido (ver [18] ou Seção 2.3.7).

* + - 1. *O-eNB*

A arquitetura O-RAN incorpora o 4G/LTE através do O-eNB. O O-eNB pode ser um eNB definido de acordo com [17] ou um ng-eNB (Next Generation eNB) definido de acordo com [19]. Assim, as interfaces e protocolos associados devem ser operados. Para a compatibilidade O-RAN, as interfaces E2 e O1 também devem ser suportadas.

* + - 1. *Rio O-RU*

Em comparação com o 3GPP, a arquitetura O-RAN também inclui a unidade de antena, que é chamada de Unidade de Rádio O-RAN (O-RU). Inclui a estrutura da antena, bem como a tecnologia analógica de alta frequência (RF) e amplificador de energia. O O-RU está conectado ao O-DU através da interface Open Fronthaul (Open FH). Ele mapeia funções de baixa FIL da interface de rádio em comparação com a UE. Comparado com os outros nódulos RAN, este é um nó físico. A virtualização da O-RU é um tema para estudos futuros [14].

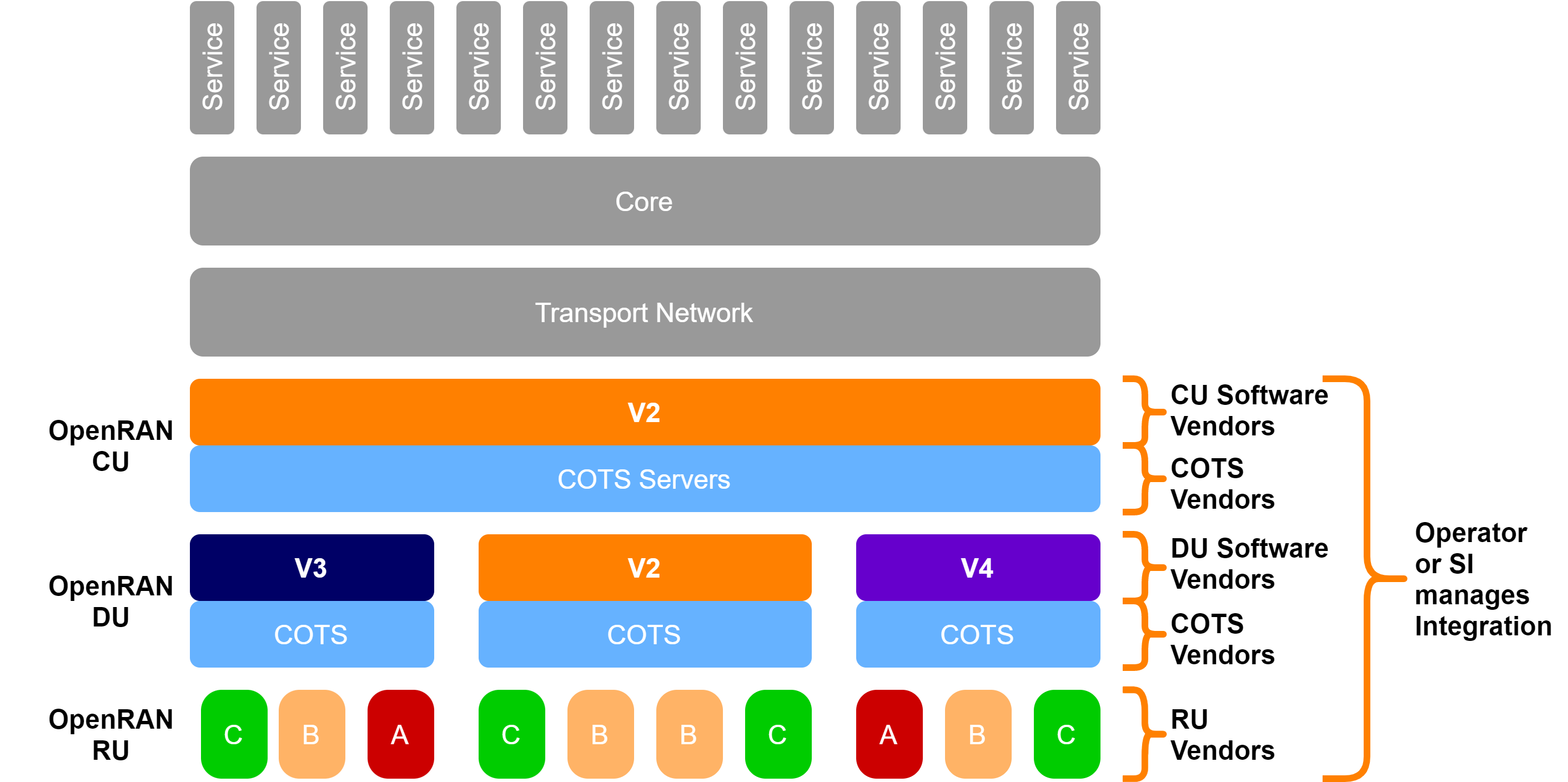
### Modelo de integração open-RAN

No RAN, as operadoras de rede incorrem na maior parte dos custos em CapEx (Despesas de Capital; z. Dt. Custos deinvestimento) e OpEx (Despesas Operacionais) Custos operacionais). Portanto, estruturas e processos eficientes são particularmente relevantes para a implantação, integração e operação contínua de um RAN. Com a introdução da arquitetura O-RAN, a integração dos vários componentes de fabricantespotencialmente diferentes está aumentando,por um lado, para um comissionamento bem-sucedido e

por outro lado, para a operação segura e gerenciamento de atualizações de HW e SW. Espera-se que, na maioria dos casos, não seja a própria operadora de rede que é responsável pela integração, mas integradores de sistemas especializados (SI) ou prestadores de serviços gerenciados (MSPs).

Os custos de diferentes abordagens são amplamente discutidos, mas a complexidade e a relevância de segurança das tarefas de integração são indiscutíveis. Novos procedimentos de aceitação e testes de interoperabilidade são necessários e devem ser necessários. também pode ser certificado. No conceito operacional, devem ser utilizadas funções de monitoramento dedicadas, que visam exclusivamente a verificação permanente da segurança operacional e de dados dos componentes RAN distribuídos, em particular, quen Os processos DevOps são usados para atualizações automatizadas de software pelas funções de rede.

Para ilustrar um possível cenário, a Figura 6 mostra que um fornecedor de CU e vários fornecedores de DU e RU cada um com diferentes versões de software devem ser integrados ao O-RAN, assumindo que o software está instalado no hardware COTS (Commercial Off-The-Shelf). Fica.



*Figura 6: Modelos de integração para Open-RAN, gerenciados pelos operadores ou integradores de sistemas ([Fonte: Parallel Wireless], cf. [20])*

Deve-se notar aqui que todos os componentes das tecnologias convencionais de 2G a 4G/LTE em operação devem ser incluídos, além da funcionalidade NG-RAN recém-integrada. As exceções são redes isoladas do campus, desde que não integrem uma rede herdeira.

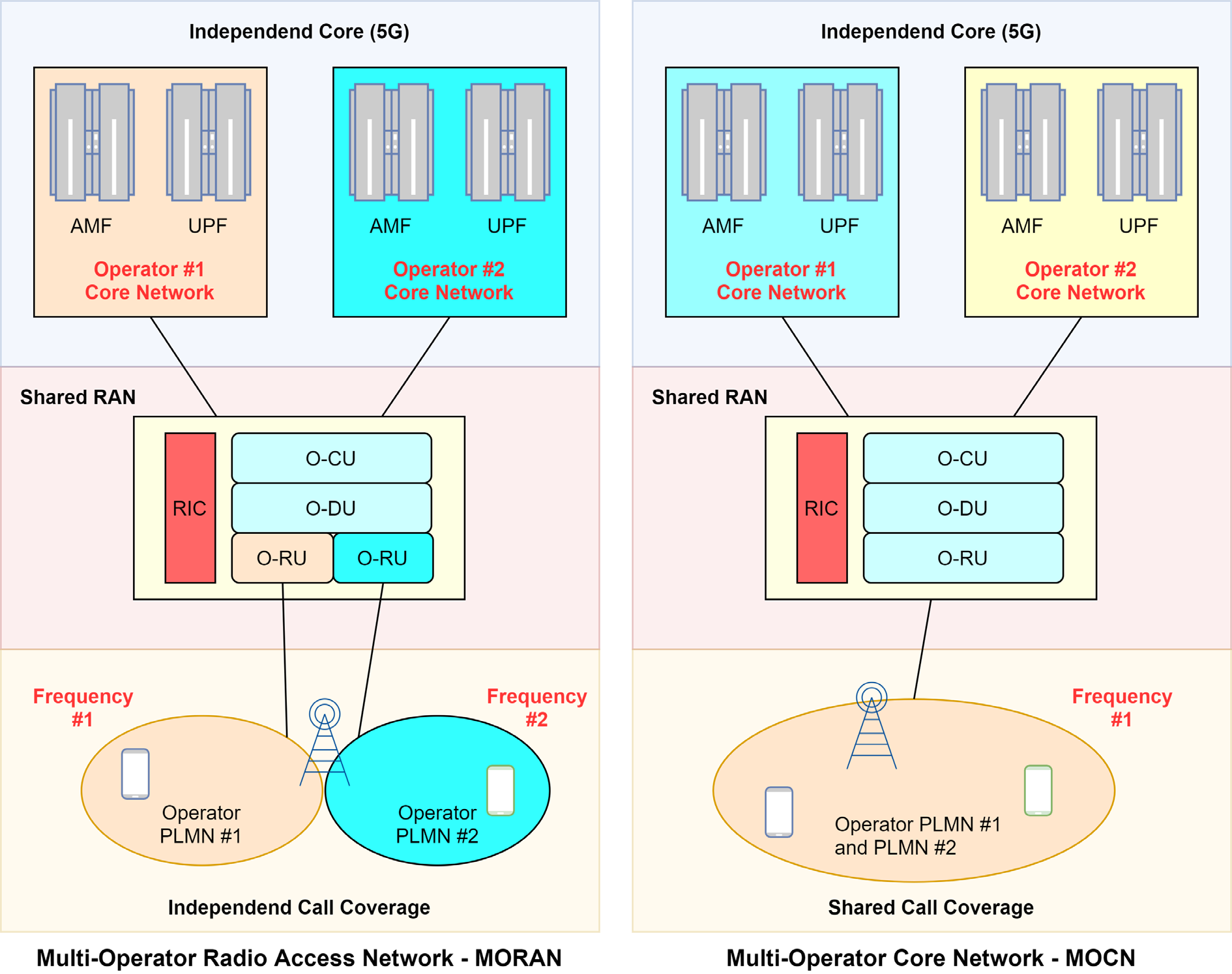
### Conceitosde compartilhamento R AN

As características básicas de distinção nos conceitos de compartilhamento RAN incluem compartilhamento passivo e ativo. Entende-se que o compartilhamento passivosignifica o compartilhamento de elementos passivos da rede. Isso inclui o compartilhamento de locais, mastros, fonte de alimentação e resfriamento, bem como as conexões entre os locais e os respectivos pontos de concentração para os locais de grade central. Isso também inclui serviços e custos baseados em localização, como segurança, incêndio ou monitoramento de objetos. O compartilhamento de elementos ativos da rede é chamado de compartilhamento ativo. Uma característica comum é o uso compartilhado de elementos de rede eletrônica.

* + - 1. *MORAN e* *MOCN*

Existem dois conceitos de compartilhamento RAN [21] para compartilhamento ativo, que são mostrados na Figura 7: Rede de Acesso de Rádio Multi-Operadora (MORAN) e Rede deMinério C Multi-Operadora (MOCN). Na MORAN, todos os componentes do RAN (tecnologia do sistema RAN, antena, mastro, localização, fonte de alimentação) são compartilhados por dois ou mais operadores. Cada operador usa frequências de rádio dedicadas. Nesta abordagem, eles podem controlar independentemente o nível celular, e.B. Cada operador pode definir seus próprios parâmetros de otimização e transmitir energia para controlar o alcance e a interferência da célula.

Com o MOCN, duas ou mais redes principais compartilham o mesmo RAN, ou seja, os operadores também compartilham as frequências. As transportadoras são compartilhadas. Os operadores não podem, portanto, controlar suas redes no nível celular. As redes principais existentes podem ser mantidas separadas. A MOCN é a solução mais eficiente em recursos, pois dá às operadoras móveis a oportunidade de colocar suas respectivas alocações de frequência em um pool comum. O MOCN é especificado pelo 3GPP para 5G em [9] e pelas gerações anteriores de comunicações móveis em [22]. Ele tem sido suportado para a UMTS desde o lançamento 6, para LTE desde o lançamento 8, e o suporte para GERAN foiadicionado como parte de v na Versão11.

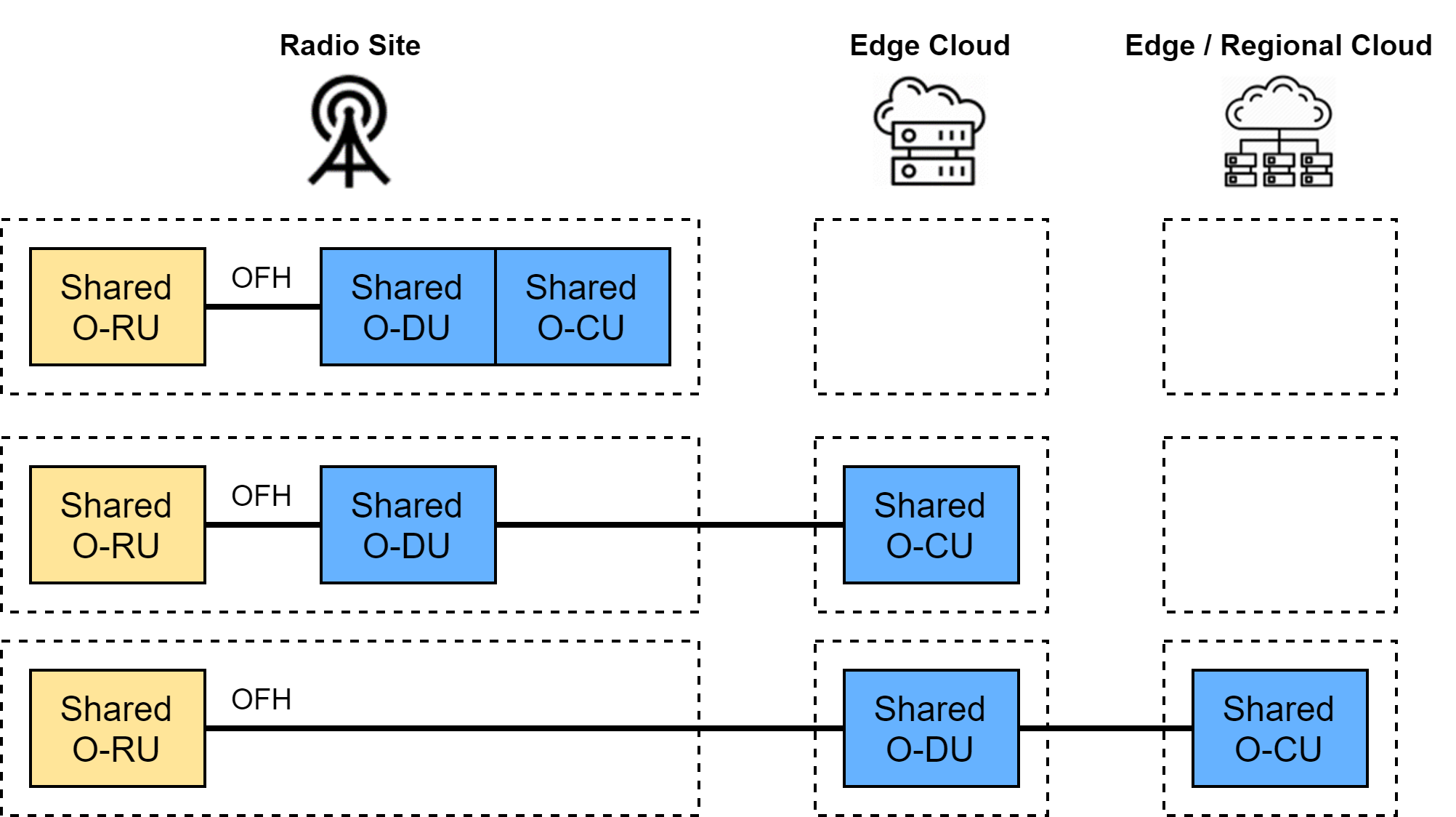


*Figura 7: CONCEITOS* *DE compartilhamento RAN* *MORAN* *e* *MOCN (baseado* *em:* *Techplayon)*

Com as duas abordagens, MORAN e MOCN, as operadoras móveis podem escolher se devem usar as linhas de transmissão juntas ou separadamente (na mesma conexão física).

* + - 1. *Compartilhando conceitos na* *O-RAN*

Existem muitos projetos diferentes para compartilhar os componentes RAN O-RU, O-DU, O-CU e os níveis de transporte Fronthaul, Midhaul e Backhaul. Decisivo é a colocação dos elementos individuais no RAN e a implementação em hardware, VMs ou na nuvem (ver Figura 8). O O-RU está sempre localizado no local da antena (site de rádio). O servidor e o software para o O-DU podem ser hospedados em um local separado ou em uma nuvem de borda (data center regional ou sede). O servidor e o software para o O-CU podem ser hospedados em conjunto com o O-DU, seja no site da antena ou em uma nuvem de borda, ou separadamente dele em um data center de nuvem regional.



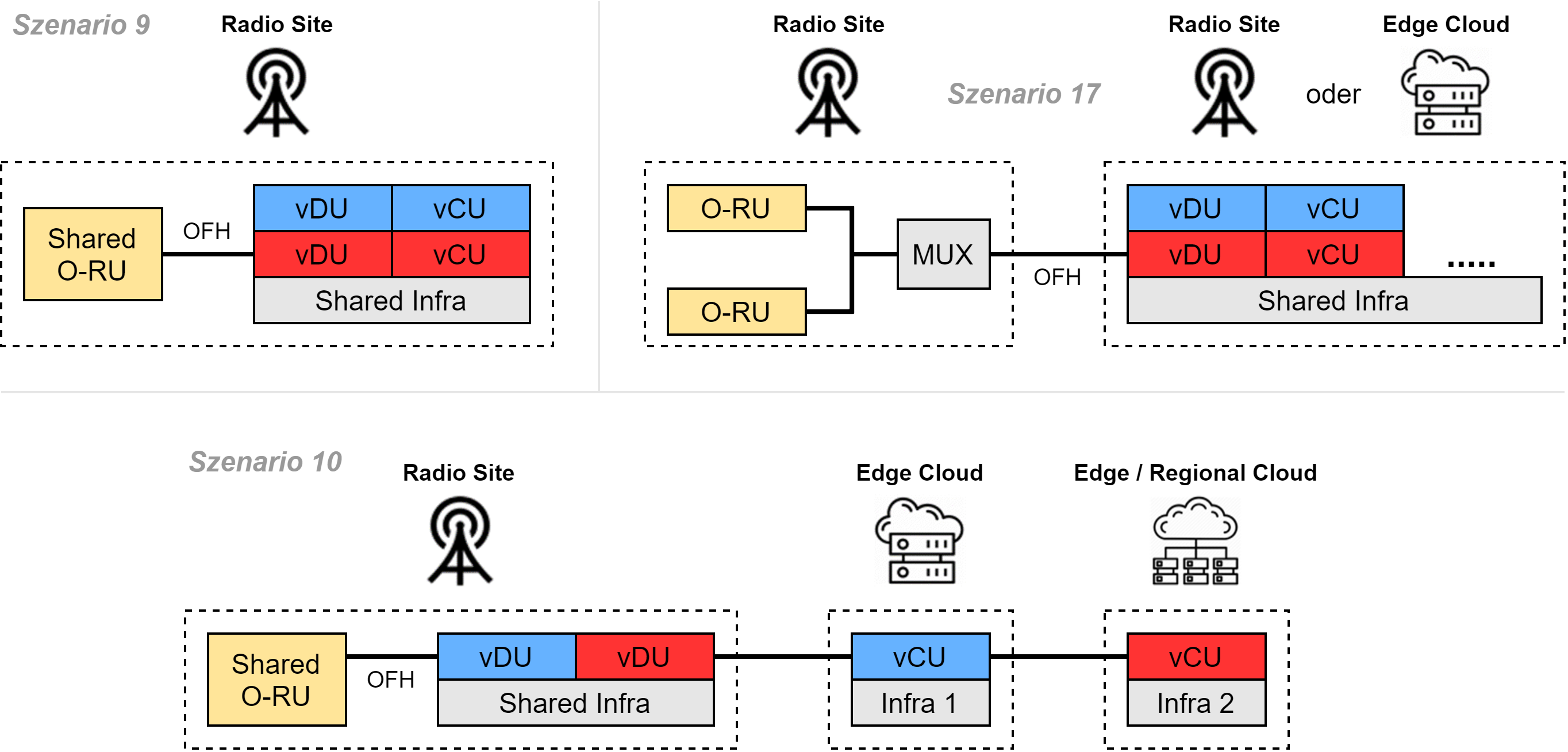
*Figura 8:* *Opções* *básicas* de *planejamento* *para* compartilhamento *ran de* *O-RU,* *O-CU e* *O-DU*

Um resumo detalhado dos possíveis cenários está disponível no documento de requisitos

[23] criado por Deutsche Telekom, Orange, Telefónica, TIM e Vodafone. A Figura 9 mostra uma seleção de três cenários (cenários 9, 10 e 17 do documento de requisitos). No cenário 9, as RANs virtualizadas (CU e DU) de diferentes fabricantes estão hospedadas em infraestruturas de computação fornecidas nos locais de antena (vRAN distribuído em infraestrutura compartilhada). No cenário 10, as DUs virtualizadas são distribuídas nos locais das antenas, enquanto as CUs associadas estão hospedadas em diferentes nuvens de borda, cada uma delas são infraestruturas de computação proprietárias. (DUs distribuídas, CUs centralizadas). Finalmente, o Cenário 17 representa um cenário interno típico no qual, semelhante ao Cenário 10, os vRANs dos fabricantes estão hospedados no local da antena (ou uma nuvem de borda). Os O-RUs estão conectados às DUs através de um multiplexer.

Entre diferentes operadores de rede, o compartilhamento da infraestrutura é preferido em relação ao compartilhamento das unidades O-RAN. O compartilhamento de infraestrutura para VMs ou infraestrutura em nuvem é atualmente mais fácil de coordenar do que a gestão conjunta das unidades no O-RAN. O gerenciamento de configuração de RANs compartilhadas ainda não está especificado entre os operadores.

Para a experiência do usuário, o fator decisivo geralmente é o desempenho ran em termos de throughput, latência e confiabilidade. Portanto, em termos de compartilhamento ran, o fatiamento de rede RAN é uma parte crítica das fatias de rede de ponta a ponta. Por outro lado, as vantagens são que a alocação de recursos específicos, o agendamento e o controle de admissão permitem o manuseio diferenciado do tráfego e o isolamento dos participantes ou grupos.



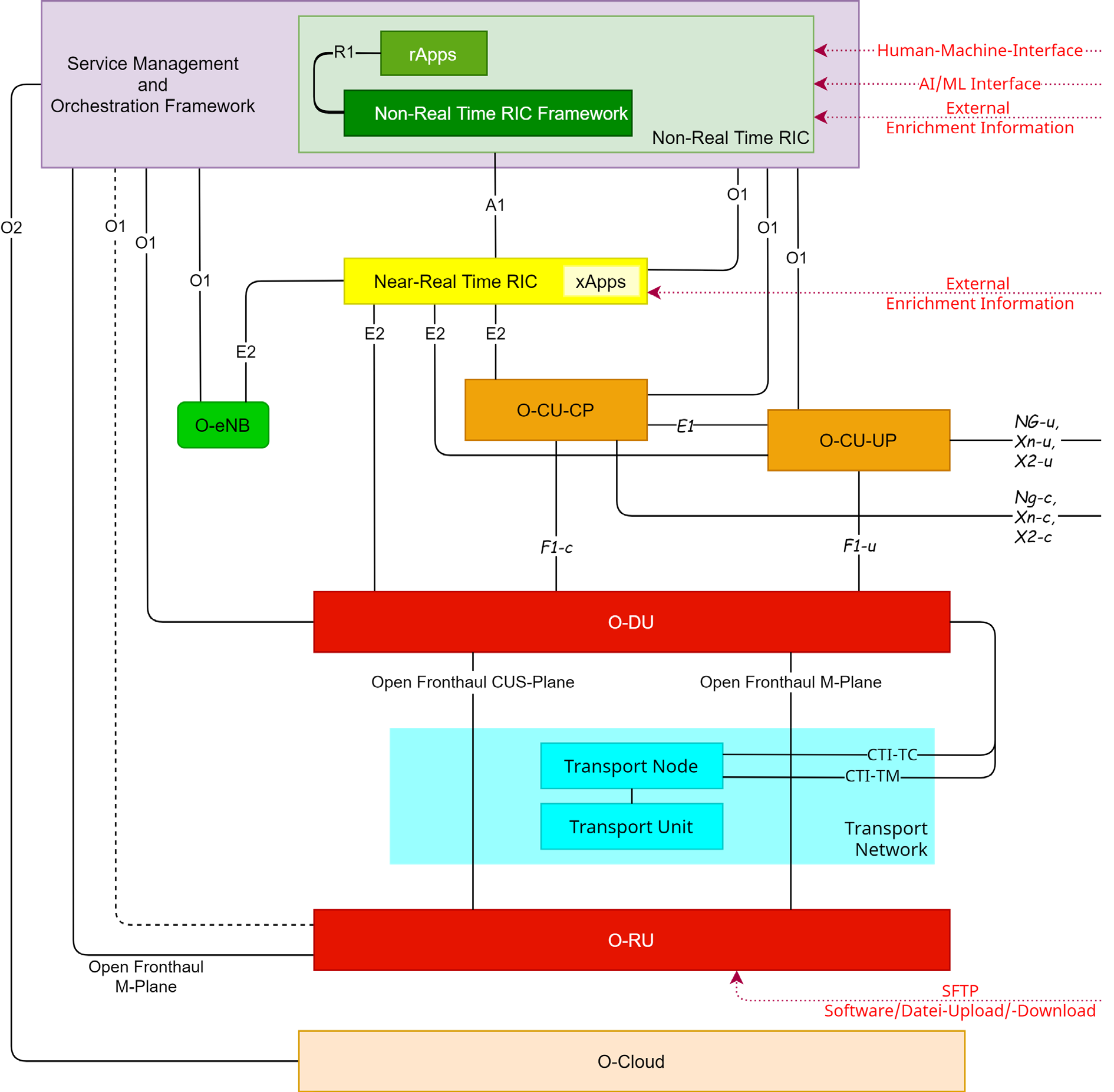
*Figura 9:* *Seleção* de conceitos de compartilhamento *RAN:* *VRAN* *distribuído* */* *Infra* *Compartilhada* *(Cenário* *9),* *VDU* *Distribuído,* *CVU* *Centralizado* *(Cenário 10)* e *Infra* Compartilhada *Multi-op* *(Cenário* *Interno* *17)* *[23]*

## Descrição das interfaces O-RAN

A seguir, as interfaces definidas por O-RAN são explicadas com mais detalhes. A Figura 10 mostra a arquitetura O-RAN com todas as interfaces sem a interface para a UE (ver Figura 5). Por outro lado, a arquitetura de referência Fronthaulé estendida pela Interface de Transporte Cooperativo (CTI) e pela rede de transporte no que diz respeito à especificação do plano O-RAN-CUS e M-Plane. Além disso, as interfaces externas para interações homem-máquina, IA/ML, informações adicionais externas e atualizações de software são inseridas.

### Interface O1

A interface O1 é a conexão entre todos os chamados "MEs (O-RAN Managed Elements,Elementos Gerenciados) e as"Entidades de Gestão" reais do framework SMO. O objetivo é garantir a operação e o gerenciamento (e.B. FCAPS MGMT, software MGMT, File MGMT) dos componentes O-RAN através desta interface. Ou seja, a interface O1 é usada para gerenciar todos os componentes O-RAN que precisam ser orquestrados. das funções de rede O-RAN associadas. Os componentes gerenciados via O1 incluem o RIC Near-RT no caso do 5G NR, o O-CU, o O-DU e no caso de redes 4G/LTE compatíveis com O-RAN, o O-eNB. O O-CU corresponde a um resumo predefinido de O-CU-CP e O-CU-UP. Para ilustrar a interface O1 e sua influência nos MEs O-RAN, ela é isolada da arquitetura lógica do O-RAN na Figura 11, incluindo o ME O-eNB. Retratado. Para a O-RU, o trabalho está atualmente em fase de investigação. Por essa razão, a conexão de interface é tracejada.

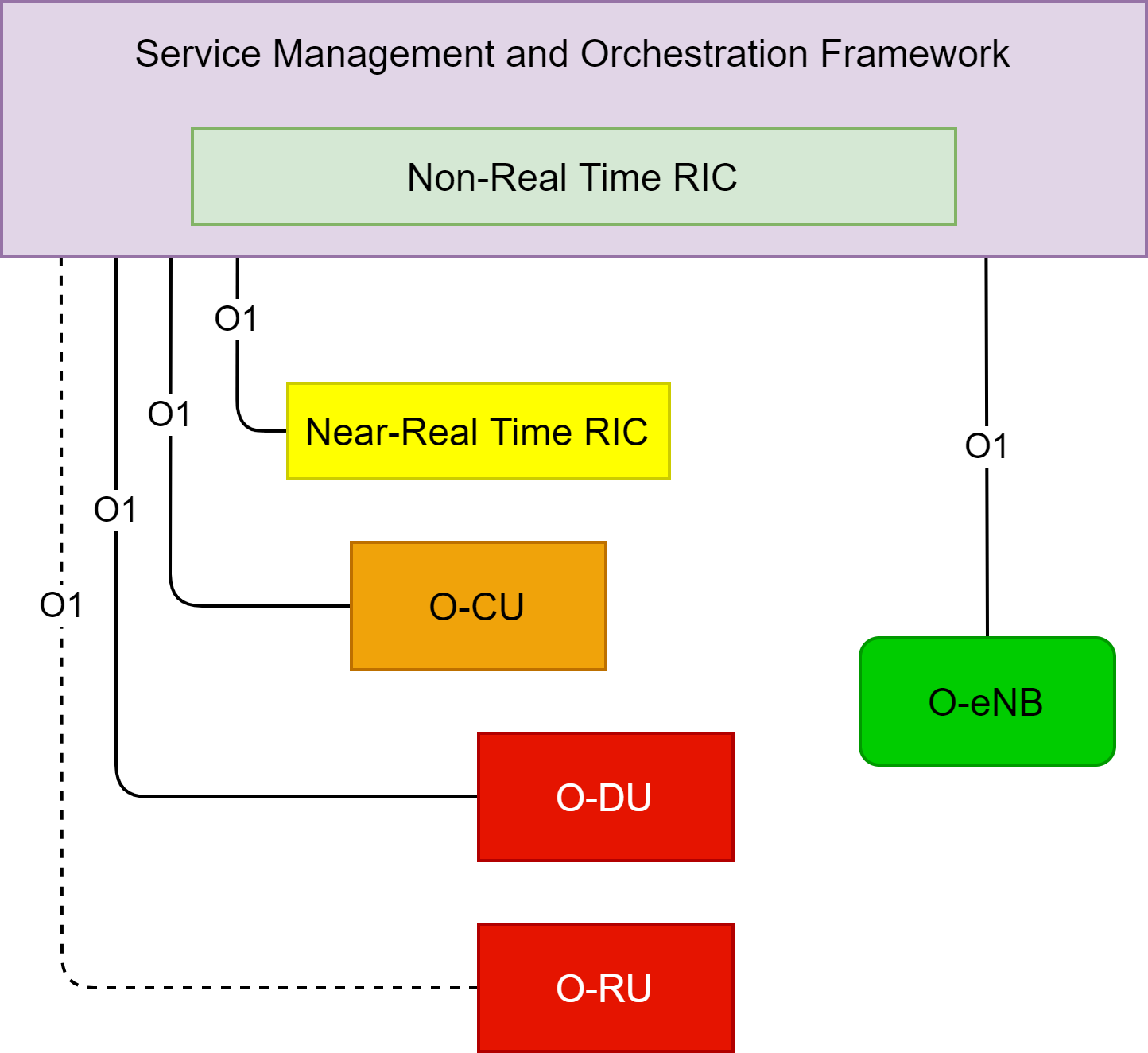


*Figura 10 -* *Interfaces O-RAN*

O O1 fornece à estrutura SMO acesso aos recursos de rede O-RAN. O gerenciamento de rede de acordo com o modelo FCAPS é suportado. O FCAPS corresponde ao modelo ISO para gerenciamento de rede, que descreve e inclui as cinco áreas de tarefas Fault, Configuration, Accounting, Performance e Security management. A interface O1 desempenha, assim, um papel central na arquitetura global O-RAN e na operação de rede. O O1 suporta FCAPS típicos, bem como outras funções de gerenciamento, por exemplo. as seguintes funções incluem:

* ==Referências== Inscrição
* configuração em termos de endereçamento,
* Controle de versão
* Monitoramento de componentes.

Além disso, os seguintes Serviços de Gestão (MnS) podem ser suportados em detalhes através da interface O1 (ver também [18], [24]):



*Figura11: Gerenciamento e operação de rede: Interface O1 como conexão entre o SMO e o O-RAN* *Managed Elements (ME) levando em conta o ME O-eNB para componentes 4G/LTE-RAN compatíveis com O-RAN* *(Ref. [14])*

* Serviços de Provisionamento
  + Requisitos Gerais do NETCONF
  + Criar, modificar e excluir moIs (Managed Object Instances, instâncias de objetos gerenciados)
  + Leitura de atributos MOI
  + Notifique-me de alterações nos valores de atributos MOI
  + Controle de assinatura
* Serviços de gerenciamento de supervisão de falhas
  + Notificação de erros
  + Controle de monitoramento de erros
* Serviços de gerenciamento de garantia de desempenho
  + Relatórios de arquivos e streaming de dados de desempenho
  + Medições de energia definidas por O-RAN e controle de ordens de medição
* Serviços de gerenciamento de rastreamento
  + Call Trace e Streaming Trace
  + Minimização dos testes de unidade (MDT)
  + Falha no link de rádio (RLF) e falha na conexão RRC (RCEF)
  + Controle de rastreamento
* Serviços de gerenciamento de arquivos
  + Notificação de prontidão de arquivos
  + Lista de arquivos disponíveis e download de arquivos
  + Transferência bidirecional de arquivos (por exemplo, arquivos de configuração para beamformagem, certificados, arquivos ML) entre cliente (File Management MnS Consumer) e servidor de arquivos (File Management MnS Provider)
* Vigilância de Comunicação
* Serviços de gerenciamento de batimentos cardíacos
  + Notificação de batimentos cardíacos
  + Ouçao controle do tbeat
* Gestão de inicialização e registro para Funções de Rede Física (PNFs)
  + PNF Plug-n-Play
  + Inscrição PNF
* Serviços para Gestão de Software (PNF)
  + Nomeação e conteúdo de pacotes de software
  + Download de software, pré-verificação e ativação de software
* Instanciar e parar uma função de rede virtualizada (VNF)
* Serviços de gerenciamento de escala vnf

As funcionalidades de gestão são realizadas através do uso de protocolos padrão (e.B. SSH, TLS, NETCONF) e modelos de dados (e.B. YANG). Por exemplo, com a ajuda do Serviço de Gerenciamento de Provisionamento, a estrutura SMO pode receber informações (atualizações), e.B. sobre o uso atual de recursos, a partir dos MEs através da interface O1 e, em troca, iniciar uma configuração otimizada dos MEs.

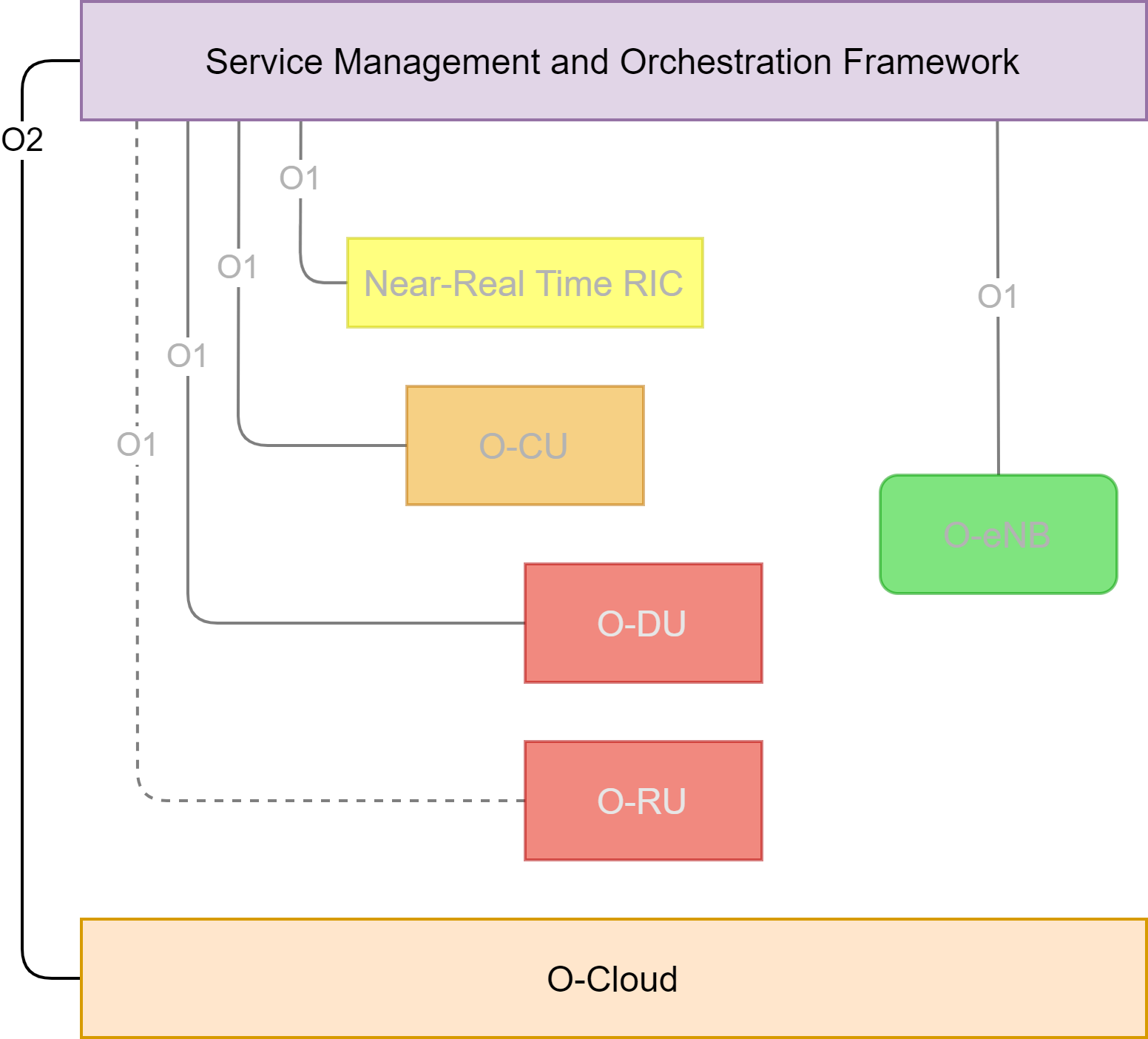
Em redes móveis baseadas em O-RAN que suportam abordagens AI/ML, a interface O1 é usada para coletar os dados (de treinamento) que podem ser usados para fins ML a partir dos MEs O-DU e O-CU. O RIC não-RT localizado no aprendizado baseado em SMO (e baseado em ML) pode fornecer políticas a serem levadas em conta ao otimizar um nível celular usando a interface O1 ( variável temporal) fornece especificações de configuração ideais para parâmetros celulares.

A arquitetura O-RAN permite a coleta, acesso e gerenciamento de históricos de dados (histórico) no que diz respeito ao tráfego transferido no RAN, ao roteamento selecionado e às operações de entrega realizadas. Os dados são transmitidos através da interface O1.

No caso do compartilhamento ran, por exemplo. um auditor externo por meio de funções de RAN virtuais (VNF) como um "operador convidado" tem acesso à infraestrutura RAN e recursos de computação do operador de rede real (operador doméstico), opções para controle remoto e configuração remota (configuração remota)deste deve ser VNFs. Nesse cenário, "interfaces remotas" (O1, O2) também podem ser introduzidas para dar ao operador convidado a oportunidade de transmitir a configuração desejada para o respectivo VNF na localização do operador doméstico. Os VNFs representam uma implementação lógica das funcionalidades O-CU e O-DU. A arquitetura O-RAN pode fornecer uma série de interfaces abertas como interfaces remotas, incluindo para O1, para monitorar os valores de desempenho dos usuários remotos. Isso permite várias taxas de otimização no que diz respeito à alocação de recursos por rádio, bem como ao ajuste do parâmetro QoS.

Atualmente, existe um JWI (Joint Work Item, item de trabalho conjunto) entre os grupos de trabalho WG1 e WG4 na padronização O-RAN para determinar como exatamente os componentes O-RU podem suportar serviços de gerenciamento no RAN através da interface O1. As decisões do JWI serão incorporadas em futuras revisões e atualizações da especificação da interface O1.

### Interface O2



*Figura 12: Gerenciamento e operação da plataforma O-Cloud pela estrutura SMO e influência da* *O-Cloud* *na* operação de *rede: interface O2* como *uma* *conexão* *entre* a estrutura *SMO* *e* *a* *O-Cloud*

*Plataforma*  *levando em conta* o *ME* *O-eNB* *para* *componentes 4G/LTE-RAN* *compatíveis com O-RAN* *(Ref.* *[14])*

A interface O2 é uma interface aberta e lógica dentro da arquitetura O-RAN e, como a interface O1, é usada como uma ferramenta para executar serviços de gerenciamento aberto & orquestração. Seu objetivo é garantir uma comunicação segura entre a estrutura SMO e a plataforma O-Cloud. Dependendo do cenário de implantação selecionado em uma instância de O-Cloud, a plataforma O-Cloud pode virtualizar várias funções de rede (NF) e, assim, assumir funçõesRAN dentro da arquiteturageral. A estrutura SMO fornece a capacidade de gerenciar uma variedade de instâncias O-Cloud em paralelo e auxiliar na orquestração de elementos/recursos disponíveis da plataforma e aplicativos, bem como fluxo de trabalho e gerenciamento de carga de trabalho. Para implementar essas tarefas SMO, a interface O2 é necessária e utilizada, ou seja, permite o gerenciamento central da infraestrutura em nuvem e uso de recursos em nuvem pelo RAN e, além disso, um "Gerenciamento do Ciclo de Vida de Implantação" para as funções de rede virtualizada (Virtual NFs, VNFs) em execução na O-Cloud. Por exemplo, VNFs, máquinas virtuais (VMs) e instâncias de contêineres podem ser gerenciados via O2. No entanto, as dependências das instanciações na nuvem e dos aplicativos de software (aplicativos) a serem executados lá atualmente não estão totalmente especificadas no padrão. A especificação da interface O2 em WG 6 "The Cloudification and Orchestration Workgroup" só está disponível em seus recursos básicos (ver [25]).

Para ilustrar a interface O2 e sua influência na O-Cloud, ela é destacada na Figura 12, incluindo os MEs gerenciados através da interface O1 (incluindo o O-eNB).

Os operadores de rede podem acessar a rede através da plataforma O-Cloud e operar e mantero RAN com a ajuda das interfaces O2 e O1. ==Referências== Atualizações e atualizações do sistema são manuseadas e os elementos/MEs de rede são (re-)configurados. A plataforma O-Cloud oferece à estrutura SMO vários serviços ou serviços através da interface O2. Funções. A descrição da arquitetura O-RAN em [14] define as seguintes funções exemplares na versão atual, que devem ser mapeadas via O2,

e indica que o escopo das funções não precisa ser limitado aos listados. Em termos de infraestrutura O-Cloud, esses recursos são:

* Descoberta e administração de recursos em nuvem infraestrutura,
* Dimensionamento positivo (scale-in) e dimensionamento negativo (scale-out) da Nuvem O,
* Gerenciamento FCAPS (em particular gerenciamento dedesempenho, configuração e falhas, bem como monitoramento de comunicação) do O-Cloud,
* Gerenciamento de software para a infraestrutura da plataforma O-Cloud.

Em relação às implementações de software (implantações) na infraestrutura O-Cloud, essas funções são:

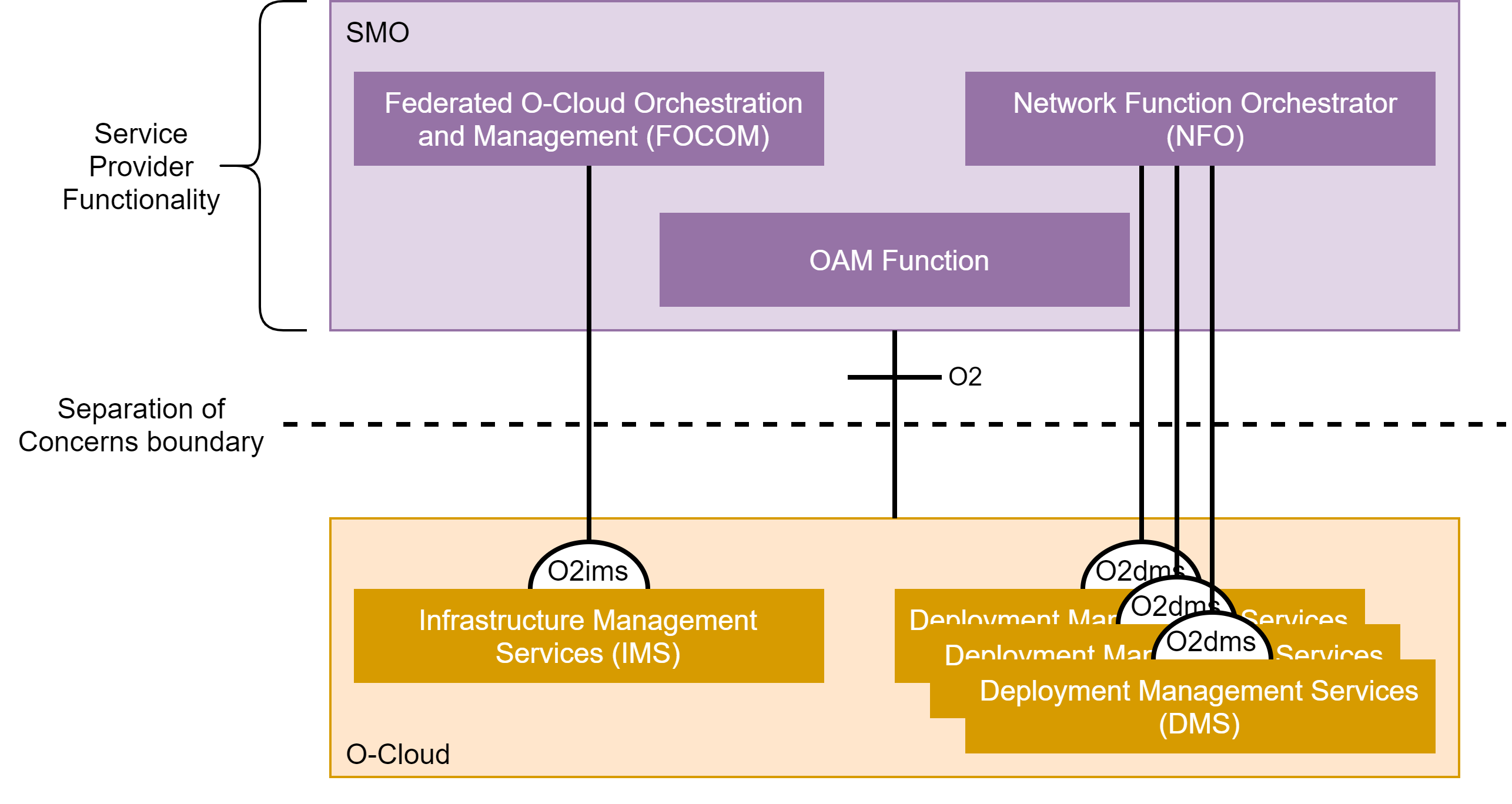
* Configuração e exclusão de implantações e os respectivos recursos atribuídos à Nuvem O,
* Gerenciamento FCAPS (em particular gerenciamento de desempenho e falhas) para implantações e os respectivos recursos O-Cloud atribuídos,
* Escala/escala das implantações e dos recursos atribuídos à Nuvem O,
* Gerenciamento de software para as implantações.

Além disso, a plataforma O-Cloud envia notificações de alarme através da interface O2 para a estrutura SMO se problemas ou alterações forem identificados durante o uso de recursos O-Cloud. Além disso, o O2 deve habilitar o gerenciamento de componentes para hardwsão aceleração na plataforma O-Cloud.

A lista acima já mostra que as funções O2 podem ser atribuídas a dois grupos lógicos de serviços, que por um lado abordam apenas a infraestrutura O-Cloud e, por outro lado, asimplementações de software (implantações) nela:

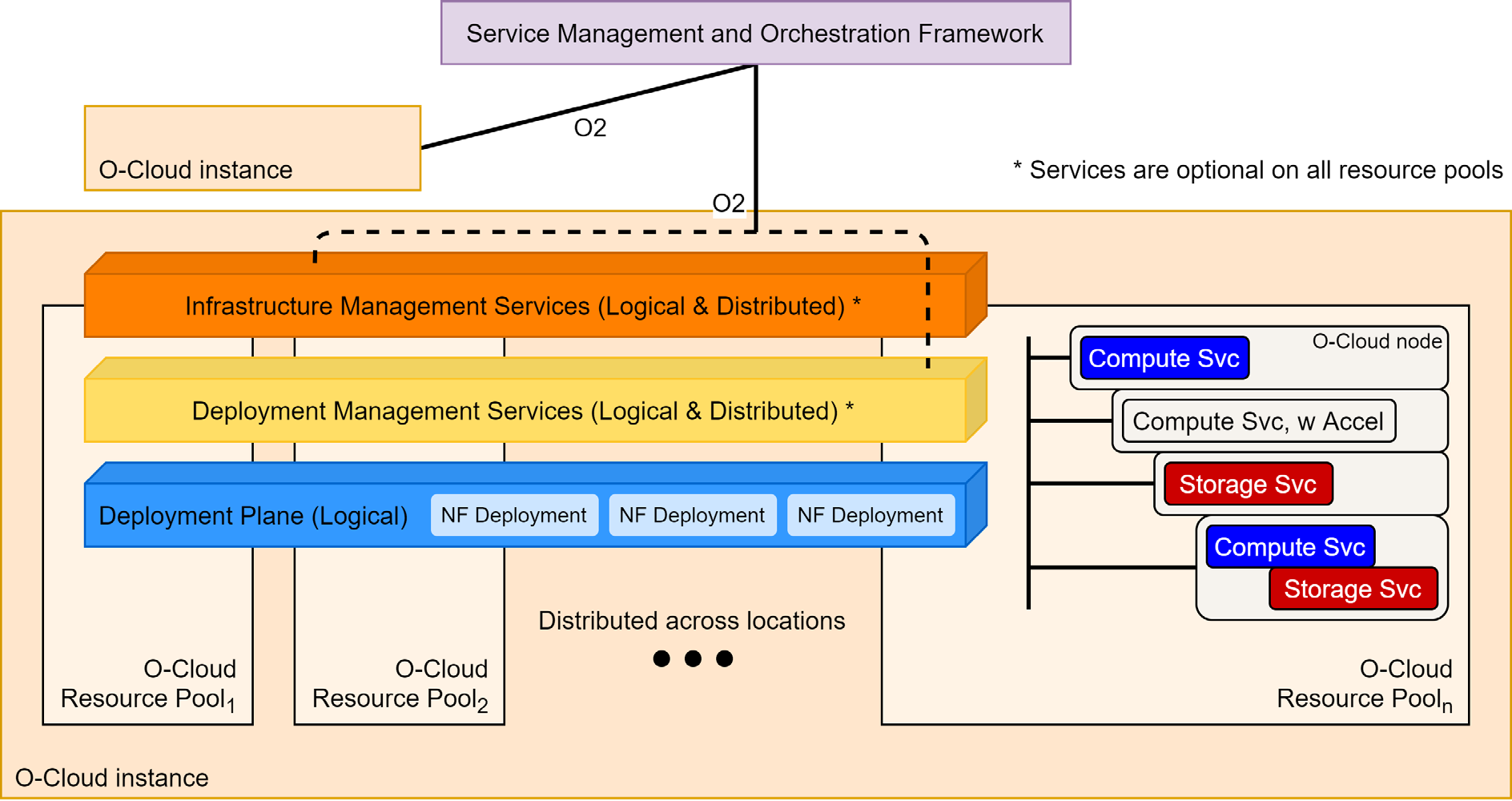
* + - 1. Serviços de Gerenciamento de Infraestrutura (IMS) e
      2. DMS (Deployment Management Services, serviços de gerenciamento de implantação).

Para o IMS, a interface O2 fornece recursos responsáveis pelo provisionamento e gerenciamento de recursos de infraestrutura em nuvem. Para o DMS, por outro lado, a interface O2 fornece um conjunto de funções de interface que são responsáveis pelo gerenciamento dos ambientes de virtualização ("implantações virtualizadas/contêiner") e a infraestrutura da O-Cloud. Portanto, o O2 é dividido em duas Interfaces Baseadas em Serviços (SBIs) entre a estrutura SMO e a plataforma O-Cloud, cada uma delas inclui seu próprio conjunto de funções. A Figura 13 ilustra este colapso. [25]



*Figura 13: Divisão* *da* interface *O2* *em* *Interfaces* de *Bases* de *Serviço* *(Ref.* *[25])*

A Figura 14 serve para entender melhor as relações e funções explicadas acima no que diz respeito à interface O2 em interação com os componentes relevantes do RAN e da arquitetura O-Cloud. A visão geral mostra os componentes principais de uma instância de O-Cloud por um lado e a interação entre a estrutura SMO e as instâncias O-Cloud por outro. Essa interação ocorre utilizando a interface O2 e os serviços de gestão O2 IMS e DMS.

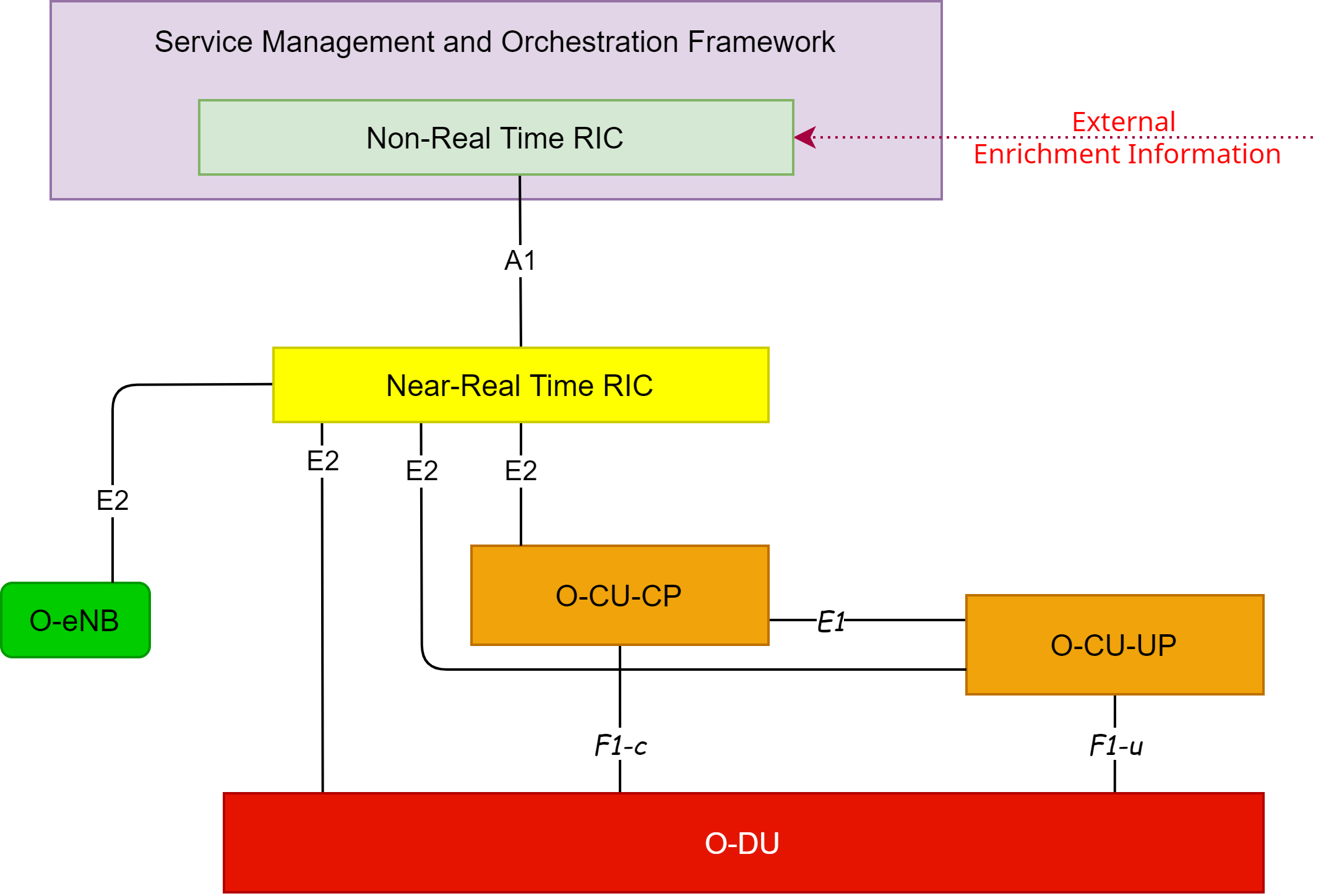


*Figura 14: Interação entre a estrutura SMO e as instâncias de O-Cloud, bem como a visão geral dos componentes do núcleo O-Cloud (Ref. [26])*

Finalmente, deve-se notar que os sistemas O2 e as interfaces associadas necessárias para eles ainda não foram especificados. Está sendo planejada a elaboração e publicação de uma especificação dedicada de O2.

### Umainterface 1

A interface A1 é especificada no Grupo de Trabalho O-RAN 2 [27]. É usado para comunicação entre o RIC não-RT e o Near-RT RIC. Para ilustrar a interface A1 e sua influência sobre as funções fora dos RICs, a Figura 15 mostra o trecho relevante da arquitetura O-RAN para esta seção.



*Figura 15: Trecho da arquitetura O-RAN: a interface A1 como uma conexão entre o RIC não-RT e o Near-RT* *RIC* *levando* *em conta* *os* *efeitos em* *outras* *funções* *(Ref).* *[14])*

O RIC não-RT transmite as informações registradas no quadro SMOde várias fontes internas e externas de O-RAN para o Near-RT-RIC através da interface A1. Esta informação é:

* Políticas baseadas em políticas em forma declarativa (política A1) que contêm declarações sobre metas e recursos para UEs e células.
* Informações sobre gerenciamento de modelos ML (treinamento, atualização, implantação de modelos ML).
* A1 Informações de enriquecimento de fontes internas ou externas de dados O-RAN, onde sua disponibilidade ou uso não é fundamental para o desempenho das tarefas de uma unidade, mas apenas para sua melhoria.

O RIC Near-RT destina-se a usar essas informações para completar a configuração dos nodes E2 através da interface E2. Desta forma, o RAN deve ser capaz de ser otimizado em condições definidas (por exemplo. a RRM).

A forma declarativa das políticas A1 significa que a implementação concreta deve ocorrer no RIC Near-RT. As políticas A1 são válidas até que sejam alteradas ou excluídas pelo RIC Near-RT. O Near-RT RIC tem a tarefa de informar o RIC não-RT sobre o status de aplicar uma política A1 como feedback através da interface A1. Deve-se mencionar que as políticas A1 não estão garantidas lá no caso de um reinício do RIC Near-RT. Portanto, a tarefa do RIC não-RT é verificar a presença de políticas A1.

Se uma política A1 estiver relacionada a uma UE (ou um grupo de UEs), a UE é identificada pelo identificador UE Id. O ID UE destina-se a ser utilizado através do RAN UE ID conhecido pelo RAN, que é usado para a interface E1 [6] ou o UE Id. para a interface F1 [7]. O objetivo é

a identificação de medidas associadas à UE a fim de calcular correlações de dados O1-PM com os objetivos de um serviço (e.B. no casode reclamações sobre oserviço) e avaliar o cumprimento de políticas. Nem equipamentos de hardware nem dados do usuário são identificados.

As Informações de Enriquecimento A1 podem ser pesquisadas, solicitadas e transmitidas através da interface A1. Ao fornecer dados parafontes externas, o RIC não-RT será responsável por autenticar a fonte e proteger a conexão. No momento, não está claro como as conexões com as fontes externas devem ser tratadas, nem a busca e criação de dados externos definidos.

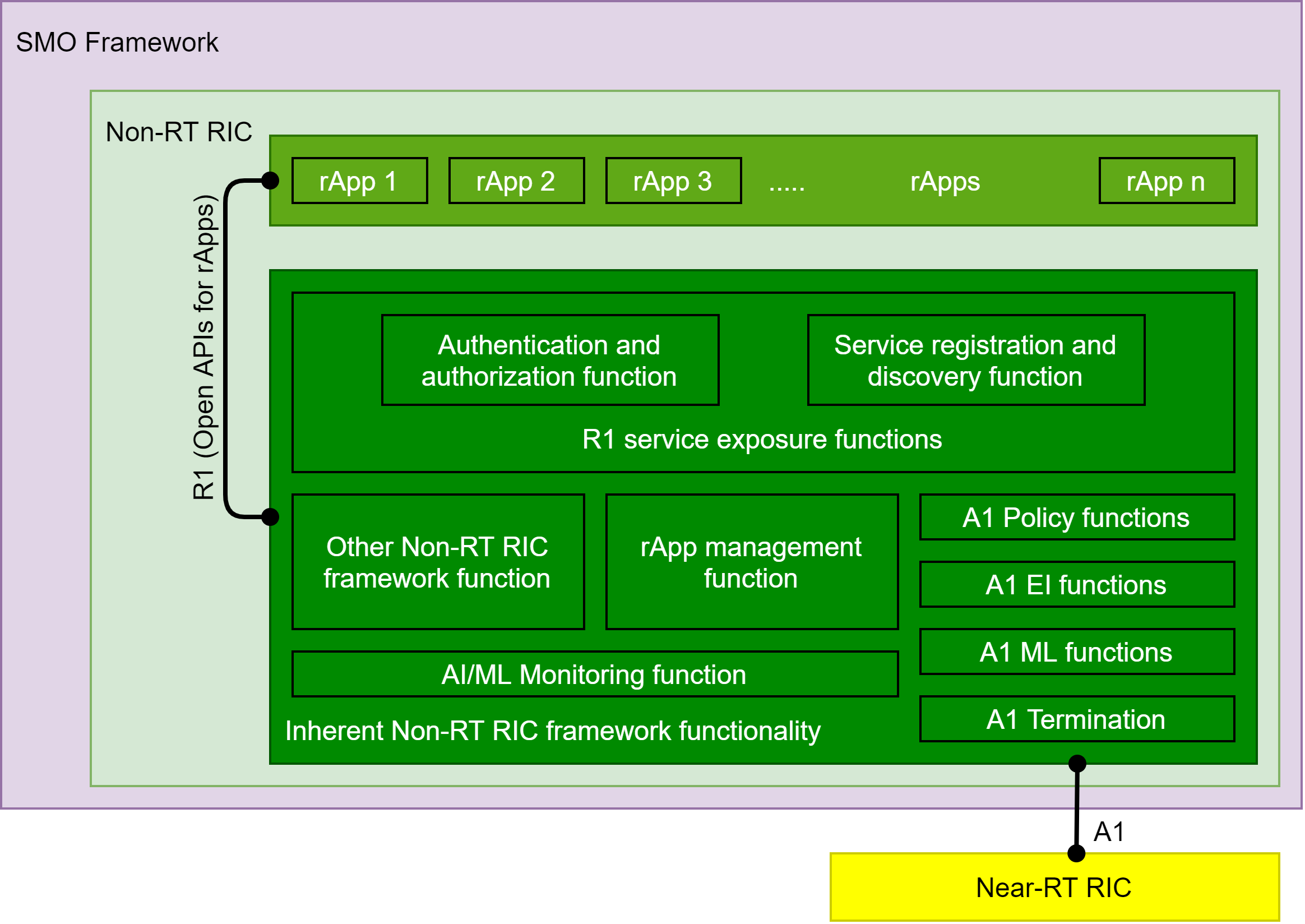
Para distinguir informações de enriquecimento, a norma define o uso de tipos de informações de enriquecimento (tipos de I). No entanto, além do termo genérico, não há definições de tipos específicos.

### InterfaceR1

A interface R1 é especificada no Grupo de Trabalho O-RAN 2 em conjunto com o RIC não-RT [28]. É a conexão definida no RIC não-RT entre as funções de estrutura inerentese osaplicativos (rApps) em execução no RIC não-RT. A Figura 16 mostra a interface R1 exibindo as funções do RIC não-RT. As funções no quadro do RIC Não-RT incluem o gerenciamento de rApps, o suporte do rApps via serviços de acesso (R1 Service Exposure Function), funções para a interface A1, fluxo de trabalho AI/ML e outras funções do RIC Não-RT, se disponível. Presumivelmente devido ao uso interno como API para os rApps, outro nome para a interface R1 é "Open APIs para rApps".

Os rApps destinam-se a usar as funcionalidades do RIC não-RT expostos através da interface R1, a fim de fornecer valor agregado para a operação e otimização do RAN. Estes incluem:

* Fornecimento de diretrizes baseadas em políticas e informações de enriquecimento através da interface A1,
* Realizando análise de dados, treinamento de IA/ML e coleta de informações para otimização ran ou para uso por outros rApps,
* Recomendação de configurações que podem ser enviadas através da interface O1.



*Figura 16: Ilustração da interface R1 através do diagrama funcional da arquitetura RIC não-RT (Ref. [28])*

Como parte da estrutura SMO, o RIC não-RT também tem acesso às suas funções. Isso inclui influenciar as informações transmitidas através da interface O1. O RIC não-RT precisa desse acesso para otimizar os recursos ran. No entanto, a definição atual do O-RAN implica apenas que o RIC não-RT pode acessar a funcionalidade da estrutura SMO apenas para este fim. Assim, o RIC não-RT só deve ser autorizado a influenciar a transmissão através da interface O2 se o O-Cloud for considerado um recurso RAN.

### Interface E2

A interface E2 é especificada no Grupo de Trabalho O-RAN 3 [29] e conecta o RIC Near-RT com os chamados nodes E2 (nodes E2). Este é um termo coletivo para todas as unidades conectadas ao lado sul da interface E2, ou seja, O-CU-CP, O-CU-UP eO-DU no caso do5G NR e O-eNB no caso do 4G/LTE (ver Figura 17). Assim, os nós do E2 destinam-se a suportar todas as camadas de protocolo e interfaces definidas em redes de acesso a rádio 3GPP, incluindo eNB para LTE/E-UTRAN [17] e gNB/ng-eNB para NR/NG-RAN [19].

O Near-RT RIC está conectado a um ou mais nodes E2 através da interface E2, ou seja, no caso de NR, a um ou mais CPs O-CU, um ou mais O-CU-UPs e um ou mais O-DUs. Assim, no caso do LTE, ele conecta o RIC Near-RT com um ou mais O-eNBs. Assim, enquanto um RIC quase-RT tem uma relação de um a muitos com suas unidades, por outro lado, apenas uma relação um-para-um é possível. Cada O-CU-CP, O-CU-UP, O-DU e O-eNB só podem ser conectados a um RIC Near-RT de cada vez, assim como um RIC Near-RT só pode ser conectado a um RIC não-RT.



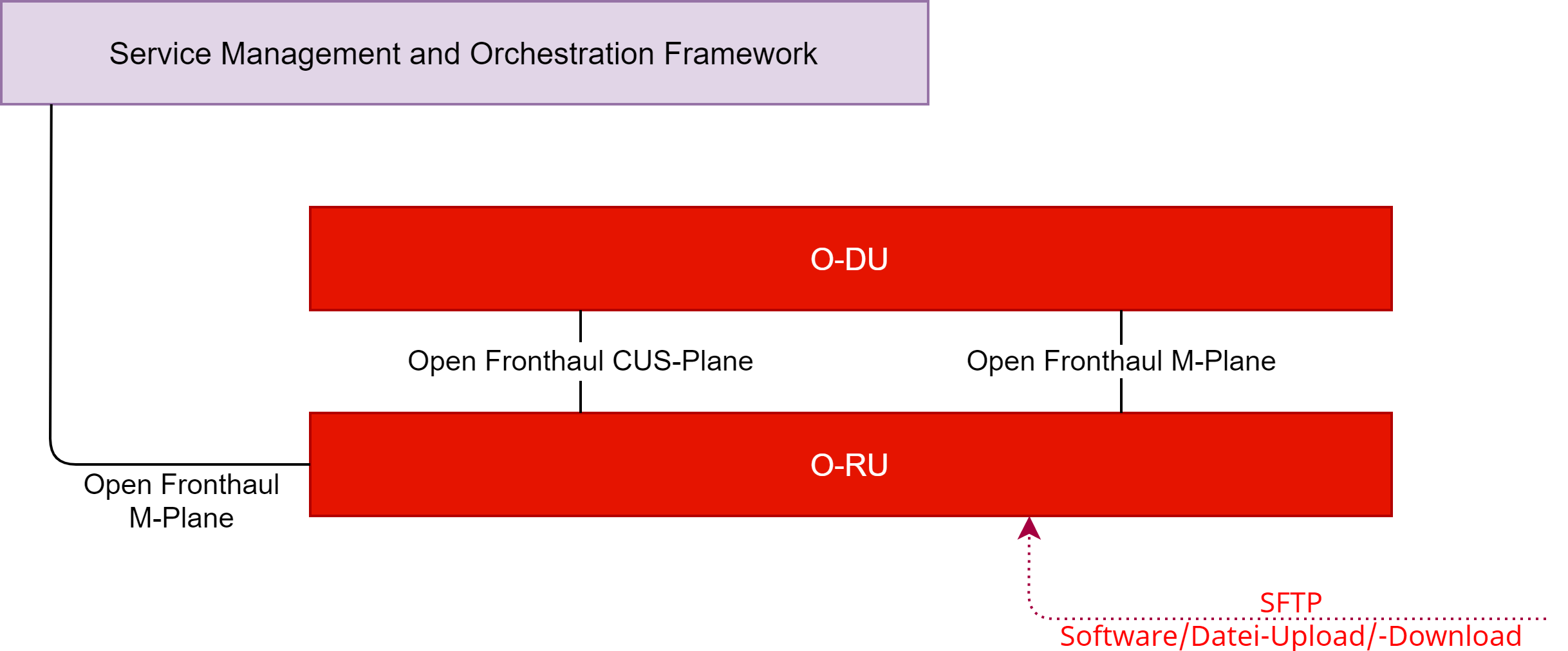
*Figura 17: Trecho da arquitetura O-RAN: a interface E2 como uma conexão entre as funções Near-RT RIC* *e* *RAN*  *registradas*  *como* nós *E2* *(Ref). [14])*

Como uma interface crítica entre os nós de rádio padronizados pelo 3GPP e as funções especificadas pelo O-RAN, há o princípio geral na especificação de que esta interface E2 deve estar aberta. Este é um pré-requisito essencial para a realização da interoperabilidade. ==Referências== dele apoiar o O-RAN será até que ponto a interface E2 é suportada pelos fornecedores RAN [4].

Outro princípio geral na especificação O-RAN é que as funções do RIC Near-RT e dos nós E2são completamente separadas das funções detransporte. O esquema de endereçamento utilizado nos nós RIC e E2 near-RT não deve estar vinculado aos esquemas de endereçamento das funções de transporte. Além disso, os protocolos da interface E2são baseados exclusivamente emprotocolos do plano de controle. O acesso ao Plano do Usuário de qualquer forma não faz parte da especificação. O objetivo é controlar e otimizar os nódulos E2 e os recursos que eles utilizam. Os xApps hospedados no RIC Near-RT usam a interface E2 para coletar informações em tempo real (e.B. em bases UE ou rádio-celular) para fornecer serviços de valor agregado como os rApps. Para esses fins, o RELATÓRIO de serviços RIC, INSERT, CONTROL e POLICY são usados pelo RIC Near-RT para solicitar relatórios de medição com base em eventos de gatilho específicos ou para enviar novas políticas para nós E2 específicos.

Devido à relação de um a muitos entre o Near-RT RIC e os nós E2, a interface E2 deve suportar o manuseio de falhas e a melhor resiliência. No caso de uma falha da interface E2 ou do TRIC próximo de RT, um nó E2 deve ser capaz de executar sua função de forma independente. No entanto, pode haver falhas em determinados serviços de valor agregado que só podem ser fornecidos através do Near-RT RIC, e.B. se a otimização de recursos ocorrer em um O-CU calculado por xApps e esses cálculos são baseados em dados de medição regularmente comunicados via E2. Tal ciclo não pode ser continuado em uma situação de fracasso.

### Interface FH CUS aberta



*Figura 18: Trecho da arquitetura O-RAN: a interface Open Fronthaul como uma conexão entre as funções* *O-DU* *e* O-RU ou *O-RU.* *SMO* *e* *O-RU (Ref. [14])*

A Interface Fronthaul Aberta combina as funções O-DU e O-RU ou, no modelo híbrido, a estrutura SMO com a O-RU. O Fronthaul Aberto inclui o plano CUS (Controle, Usuário e Sincronização) e o plano M (gerenciamento). O M-Plane com sua relação com a interface Open FH M-Plane é explicado na Seção 2.3.7. A Figura 18 mostra o trecho da arquitetura O-RAN com as funções e interfaces relevantes para o Open Fronthaul.

As interfaces para os planos C, você e S são descritas em especificação [30]. Os dados do usuário e do plano de controle da interface Uu são transmitidos através destes. Além disso, a sincronização do tempo ocorre através dele.

* + - 1. *C-Plane (Plano de Controle)*

As mensagens são trocadas através do plano de controle que determina o processamento dos dados do usuário. Estes incluem:

* + - * 1. Informações sobre agendamento ou formação de feixes se essa configuração não for executada através do Plano M (ver Seção 2.3.7). Essas mensagens são transmitidas separadamente para uplink e downlink.
        2. Informações específicas de UL e DL sobre a numerologia utilizada, ou seja, definições de slot e subcarrier.
        3. No caso de a precodificação ser realizada na O-RU, os dados de configuração são transferidos pelo O-DU.
        4. Informações para recursos como O Compartilhamento Dinâmico de Espectro (DSS).

Os protocolos eCPRI ou IEEE 1914.3 são usados no plano C.

* + - 1. *U-Plane (Avião do Usuário)*

O User Plane (também conhecido como Plano de Dados) transmite mensagens que contêm os dados reais do usuário. O foco aqui é a transmissão eficiente, especialmente sob as altas demandas de latência nas diversas numerologias 5G. As principais características fornecidas são:

* + - * 1. Transferência de dados de I/Q dos dados do usuário, pelo qual cada símbolo é transmitido em uma mensagem U-Plane.
        2. Compactação de dados, onde diferentes métodos podem ser definidos por PRB (Physical Resource Block), que são especificados em mensagens de controle associadas.
        3. Precodificação de dados de downlink.

Deve-se notar que a transmissão de dados I/Q também é possível sem o C-plane (e.B. através do Canal de Acesso Aleatório do Pacote, PRACH). Neste caso, a configuração correspondente deve ser feita através do Plano M.

Os métodos de compressão suportados variam entre O-RU e O-DU. Pode-se supor que diferentes O-RUs implementem apenas um método para manter a complexidade baixa. Assim, o O-DU deve implementar vários métodos para serem interoperáveis com diferentes fabricantes de O-RU.

No plano U, como no plano C, são utilizados protocolos eCPRI ou IEEE 1914.3.

* + - 1. *S-Plane (Plano de Sincronização):*

Os requisitos de sincronização entre O-DU e O-RU são uma parte essencial e crítica para a implementação da operação TDD, bem como mMIMO ou agregação de portadores em várias O-RUs. O S-Plane pode ser usado para sincronizar sobre frequência, fase ou tempo, pelo qual diferentes topologias para a troca de informações de sincronização são possíveis, e.B.:

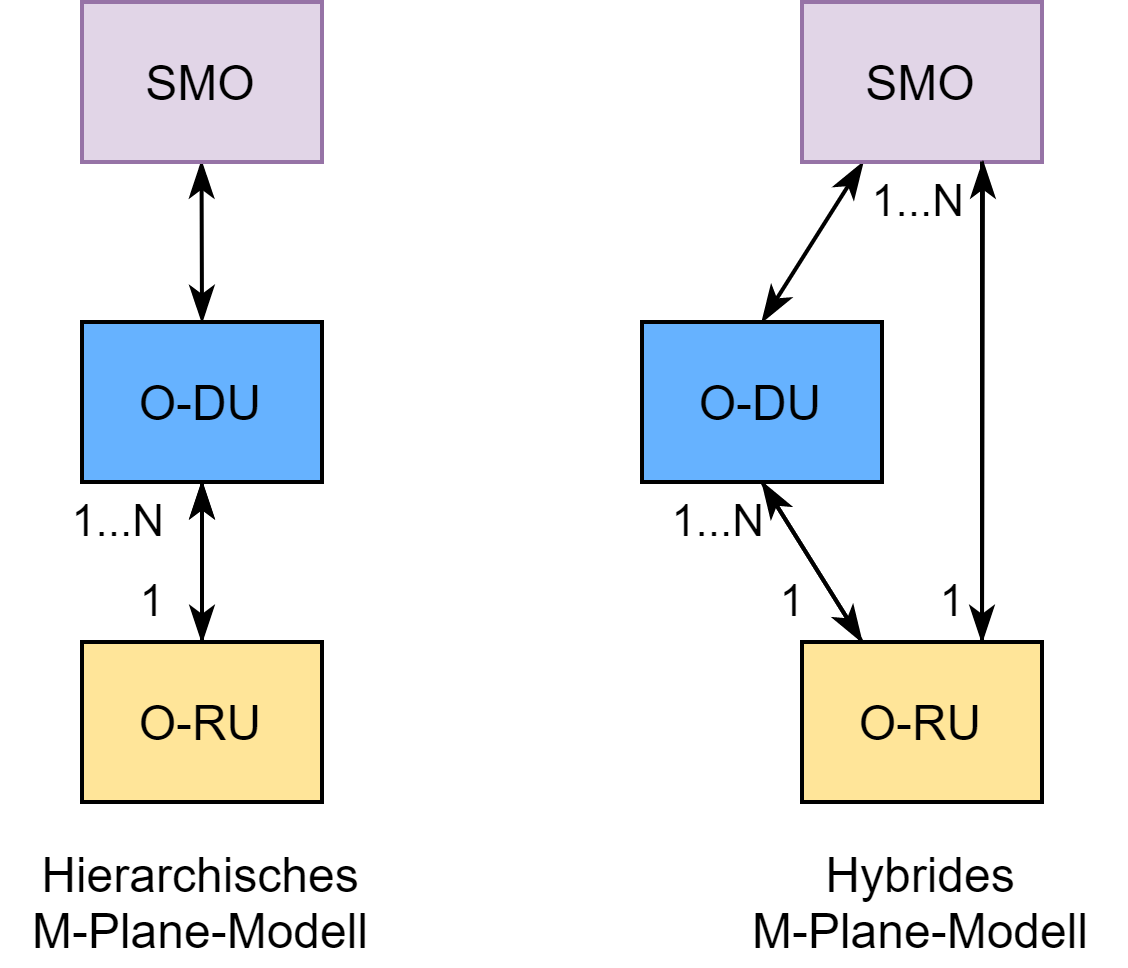
* Rede como mestre para O-RU,
* O-DU como Mestre para O-RU ou
* O-RU com receptor GNSS local comomestre s.

Protocolos como PTP e SyncE são usados de acordo com a especificação de fronthaul O-RAN. Se a sincronização for perdida pelo O-DU, todas as conexões RF das O-RUs conectadas ão encerradas ('Estado FREERUN').

### Interface FH M-Plane abertoe

De acordo com a especificação [31], o M-Plane fornece ao componente O-RU as seguintes funcionalidades principais:

* "Iniciar" o início dos procedimentos de comissionamento,
* Gerenciamento de software para upgrades na fase operacional,
* Inicialização e configuração dos parâmetros operacionais,
* Relatórios de desempenho através de valores e contadores medidos,
* Configuração e transmissão de alarme, bem como
* Upload de arquivo para o controlador O-RU.



*Figura 19:* *Arquitetura M-Plane*

A interface M-Plane pode ser hierárquica ou híbrida, como mostrado na Figura 19. No modelo hierárquico, o O-RU é controlado por uma ou mais DUs, e.B. para permitir a redundância. No caso do modelo híbrido, conexões lógicas do O-RU ao O-DU e à camada SMO sãocriadas ao mesmo tempo. usar as mesmas conexões físicas. No caso híbrido, as funções para o gerenciamento da O-RU podem ser divididas entre os controladores O-RU. Porexemplo, o gerenciamento de software pode ser localizado na estrutura SMO.

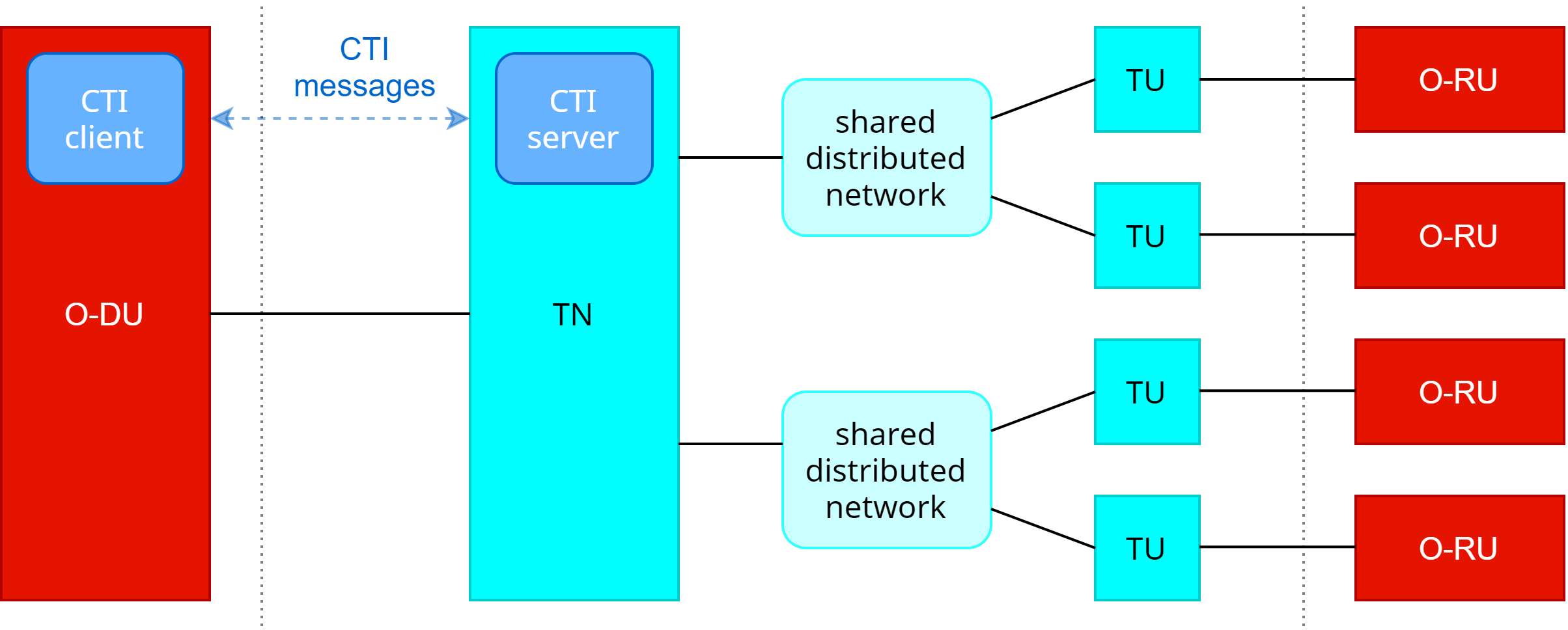
Normalmente, a configuração para o O-RU é realizada inicialmente e durante a operação, para a qual, por exemplo, as seguintes funções são usadas através do protocolo NETCONF:

* Carregar, comprometer e cancelar uma nova configuração,
* Bloquear/Desbloquear funções,
* Reversão para a configuração antiga em caso de erros, bem como
* Notificação de sucesso/falha das ações.

Uma série de funções disponíveis comercialmente também estão disponíveis para configuração ou seu acionamento, bem como para a transmissão de medições de desempenho e notificações de alarme da O-RU. Isso não será discutido em detalhes aqui.

### Interface de Transporte Cooperativo (CTI)

O CTI é uma interface entre O-DUs e nós de transporte de uma rede de transporte baseada em pacotes que serve para conectar os O-DUs a uma variedade de O-RUs [32]. O CTI tem como alvo especificamente os nódulos de transporte que gerenciam uma rede de acesso ponto a vários pontos comum. Nós de transporte (roteadores e switches) que gerenciam apenas conexões ponto a ponto não trocam mensagens CTI com os O-DUs. O CTI consiste em um nível de controle de transporte (TC) e um nível de gerenciamento de transporte (TM).



*Figura 20:* *Relação* *entre* *CTI* *e* *a*  *rede* de transporte *utilizada* *para* *o* *fronthaul* *(Ref.* *[32])*

O uso de redes de transporte baseadas em pacotes de CTI que contêm nódulos de transporte (TNs) que terminam uma ou mais redes de distribuição comuns, com cada rede de distribuição (uma porta em uma TN) agregando uma variedade de unidades de transporte (TUs) (ver Figura 20). Isso implica que a largura de banda de uma rede de distribuição é compartilhada por várias TUs. Na direção upstream, o TN gerencia essa divisão agendando alocações de largura de banda para os TUs. Existem duas maneiras de determinar a largura de banda para alocar, estática ou dinâmica.

## Aplicações de otimização e machine learning

### Funções RIC para otimização ran

O RIC é planejado como uma unidade essencial na arquitetura O-RAN. Parte do RIC consistirá em funções contidas nas unidades de processamento da estação base tradicional e será destacada no curso da divisão. Isso torna possível alcançar as interfaces de gerenciamento, por exemplo. B. Funções RRM ou SON que controlam recursos de rádio e operação de rede.

Para adaptar a funcionalidade ran, o RIC otimiza os recursos de rádio de acordo com as políticas do operador. Afeta o desempenho do RAN em três áreas principais [4]:

* Inteligência de rede: Medições e relatórios sobre o comportamento do RAN geram dados em formatos padronizados que podem ser analisados (por exemplo. com técnicas de IA/ML) para criar novos algoritmos e políticas.
* Backup de recursos: O objetivo é garantir que os dispositivos/usuários e serviços recebam o desempenho necessário(e.B. otimizando o controle de link de rádio, otimização ou priorização de entrega).
* Controle de recursos: Para garantir que o sistema RAN funcione de forma eficiente quando vários grupos de usuários possam competir por recursos adequados.

Em princípio, pode-se dizer que o RIC é o lar da inteligência prevista pelo conceito O-RAN. Essa inteligência deve ser realizada no futuro através de modelos ML para auto-otimização e automação de rede de rádio. Os dados necessários para isso são coletados pelo RIC não-RT através da interface O1 em formatos padronizados dos componentes RAN. Em primeiro lugar, as funções tradicionais de otimização do SON são operadas. Posteriormente, o treinamento de modelos através de IA/ML será possível para que novas abordagens de ML para otimização de RAN possam ser desenvolvidas e utilizadas. O Near-RT RIC implementa as políticas resultantes através da interface E2 nos CPs e CU-UPs do ou aplica controles dinâmicos lá. Por exemplo, certos dispositivos (como veículos automotores) podem ter altos requisitos de mobilidade, para os quais um algoritmo de gerenciamento de entrega diferente e superior poderiase emprestar.

### xApps/rApps

Além de sua função como controlador RAN, o RIC é uma plataforma aberta que pode hospedar aplicativos de controle RAN. Esses aplicativos são desenvolvidos por fornecedores de software especializados que não precisam pertencer ao próprio fornecedor RIC. Esses chamados "xApps" (no Near-RT RIC) e "rApps" (no RIC não-RT) destinam-se a permitir inovações na forma de algoritmos de controle RAN. xApps e rApps têm a capacidade de processar dados das ordens RAN de magnitude mais rapidamente do que é o caso dos sistemas proprietários atuais ou métodos SON centralizados. O objetivo é criar experiências de rede diferenciadas que ofereçam desempenho adaptado a tipos de serviços específicos, grupos de usuários ou locais.

Por outro lado, os serviços fornecidos por um RIC consistem em xApps ou rApps, ou uma combinação de ambos. Não há limite fixo para os tipos de xApps ou rApps que podem ser programados, e espera-se que mais deumxApp ou rApp seja executado no RAN ao mesmo tempo.

Exemplos de xApps/rApps propostos até agora incluem [33]:

* Gerenciamento dinâmico de entrega baseado em contexto para Veículo-para-Tudo (V2X),
* alocação dinâmica de recursos de rádio para veículos aéreos não tripulados,
* controle do tráfego de dados,
* Otimização da qualidade do serviço/qualidade da experiência (QoS/QoE),
* Otimização de biômo maciço de beamforming,
* Compartilhamento RAN,
* Otimização de recursos baseada em QoS,
* Garantia de serviço para fatias RAN,
* Gerenciamento de desempenho de fatias de vários fornecedores,
* Compartilhamento dinâmico de espectro,
* Otimização da alocação de recursos para instâncias de sub-rede de fatias de rede (NSSI),
* posicionamento interno local no RAN.

[4] afirma que os primeiros xApps se concentrarão em funções de verificação de saúde,

por exemplo, a prontidão operacional dos nódulos RAN. Em uma segunda fase, os xApps se aprofundarão nas observações coletando dados mais detalhados de acenos ran para análise. xApps que fazem alterações em tempo real (ou seja, ciclos de tempo inferiores a 1 segundo), são esperados em fases posteriores. No que diz respeito às decisões no nível de controle, uma abordagem será complementar as funções de RRM atuais implementadas na CU e DU, onde as políticas de um RIC poderiam mudar ou substituir a lógica RRM local. Uma abordagem mais agressiva, na qual a função RRM é completamente deslocada para o RIC, é um processo de longo prazo. Os rApps iniciais hospedados no RIC não-RT se assemelharão inicialmente aos aplicativos SON centralizados de hoje. Eles têm opotencial de evoluir rapidamente quando a coleta de dados RAN é emparelhada com técnicas de ML para criar algoritmos que criam novas formas de otimização para habilitar o RAN.

Um componente da plataforma Near-RT RIC é o "E2 Manager", às vezes chamado de "xApp Zero". Ele é usado para iniciar conexões E2 para os nódulos RAN e, em seguida, armazenar informações de configuração RAN aprendidas (e atualizadas ao longo do tempo) durante a configuração da conexão.

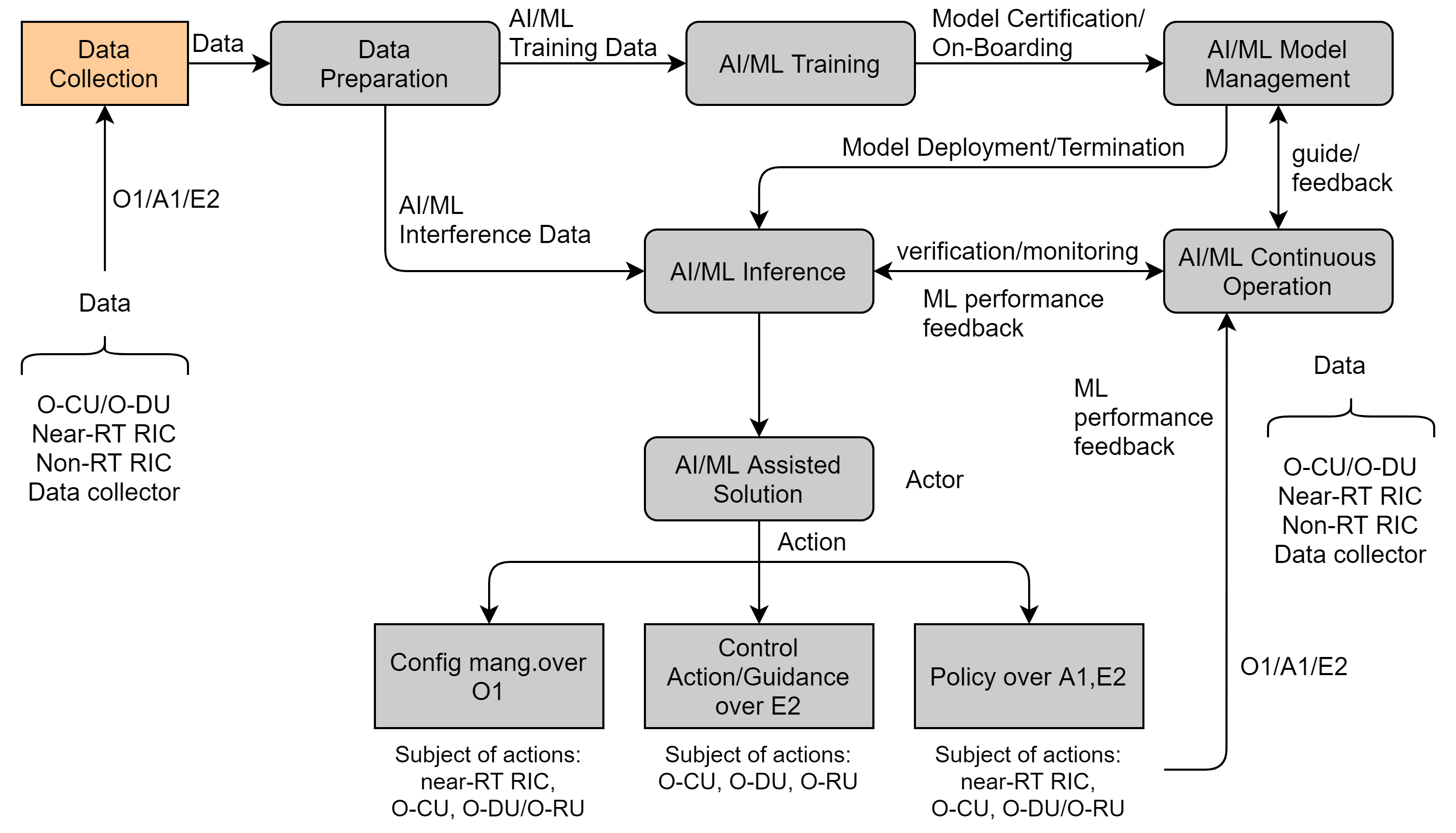
As primeiras versões das especificações RIC estão disponíveis em [28] e [29]. O O-RAN Working Group 3 continuará o desenvolvimento para adicionar mais recursos, como as especificações do E2SM (E2 Service Model). Sobre o importante trabalho em andamento de acordo com

[4] inclui a padronização dos E2SMs, que devem permitir a direção de tráfego e a otimização de QoS/QoE através do RIC. Os alvos da direção de tráfego são ociosos balanceamento de carga de mobilidade (MLB), MLB inter-intra-frequência, agregação de porta-aviões e conectividade dupla. A otimização de QoS/QoE permite que o RIC controle as funções de rede relacionadas ao controle QoS, alocação de recursos de rádio, controle de acesso por rádio, funções de mobilidade e gerenciamento de conexão.

Os drivers que declararam publicamente que estão testando soluções RIC incluem AT&T, Deutsche Telekom, KDDI e China Mobile [4].

### Machine Learning (ML)

A disponibilidade e o desempenho da IA e do ML impulsionaram a especificação de arquitetura e processos para O-RAN em WG2. Especialmente para a operação de rede, os casos de uso suportados por ML são versáteis e, portanto, podem ser usados de forma sensata em vários pontos da arquitetura O-RAN. De acordo com os tempos de resposta necessários, disponibilidade e quantidade de dados para treinamento de ML e inferência de ML (inferência; ==Referências== derivação de conclusões auxiliadas por computador) bem como a complexidade computacional, a localização para os componentes do fluxo de trabalho ML varia. O fluxo geral e os componentes dos processos ML são mostrados na Figura 21. Uma indicação para a atribuição dos componentes ML, fluxos de dados e ações para as funções de rede é dada como exemplo.



*Figura 21: Procedimentos* *gerais* *em* *IA/ML* *[34]*

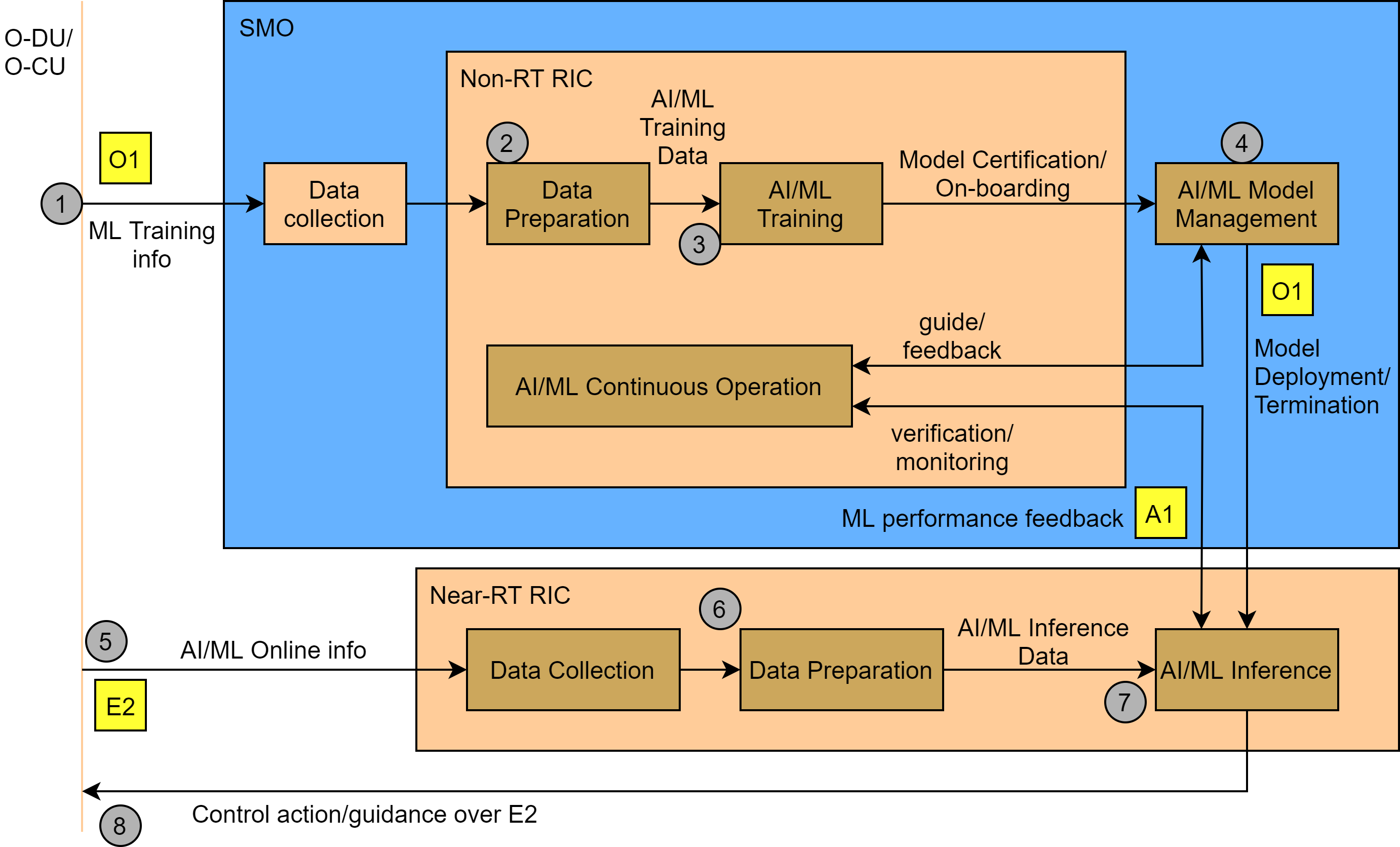
Inicialmente, uma implementação do host de treinamento ML – principalmente no RIC não-RT

– onde os dados são transmitidos via O1 e A1. No RIC Não-RT, as ações são derivadas da inferência do modelo, e.B. pode ser repassado para o Near-RT RIC através da interface A1 (políticas, configuração) ou para O-CU, O-DU e O-RU via E2 (configuração). Para processos e decisões que requerem loops de controle mais curtos, o ML-Model-Inferência é executado no RIC Near-RT para obter ações para o RIC T Near-R ou para passar comandos/políticas para os componentes O-RAN via E2. No futuro, está previsto que os processos de ML também serão especificados para o loop de controle O-DU/O-RU.

Os dados de treinamento são coletados por coletores de dados de todos os componentes O-RAN via E2, A1 e O1 e disponibilizados para o processo de treinamento através de componentes de agregação e filtro. Particularmente relevantes são os dados da interface E2 em várias granularidades no que diz respeito a Lugar e hora. Os dados de enriquecimento podemserfornecidos através de todas as interfaces disponíveis ou internamente na camada SMO. Este último deve ser considerado nas considerações de segurança, pois as funções na camada SMO também podem ter interfaces proprietárias para fontes de dados brutas.

Umaplicativo típico para processos suportados por ML é a otimização RAN. Devido às grandes quantidades de dados muitas vezes necessárias e seu processamento complexo, o RIC não-RT é adequado tanto para treinamento quanto para inferência. Além disso, os dados de enriquecimento podem ser correlacionados, que são usados a partir de sistemas oss externos (Sistema de Suporte de Operações).

Para uma operação contínua segura dos processos ML, também deve estar disponível uma série de funções que definem os componentes, processos e ações em relação ao KPI-D com base emefinições KPI-D. Monitore a atividade, o desempenho, o tempo, o consumo de recursos e a consistência e, se necessário, Mudanças no gatilho. Essas tarefas também podem ser suportadas pelo ML.



*Figura 22:* *Cenário de implantação* *para* *IA/ML* *[34]*

Com base no feedback apropriado do host de inferência do modelo, a camada SMO pode .B. será decidido em

* a seleção do modelo a ser alterada,
* treinamento adicional para o modelo ou
* o agendamento do modelo.

Os fabricantes de sistemas, bem como os provedores de terceiros, estão desenvolvendo cada vez mais algoritmos baseados em ML que são operados em O-CU e O-DU e geram ações na gama de milissegundos, a fim de alcançar medidas de otimização específicas da UE. reagir, ou seja, ter um impacto direto na experiência do usuário e segurança funcional. Isso torna ainda mais importante que as arquiteturas O-RAN desenvolvam não apenas novos procedimentos de integração e aceitação, mas também conceitos operacionaisque se concentram nos processos internos da operadora no ambiente de vários fornecedores. Como exemplo, a Figura 22 mostra um cenário de implantação no qual os componentes ML e os processos ML estão incorporados nas funções O-RAN da seguinte forma:

* em SMO, gerenciamento de modelos,
* no RIC Não-RT, a elaboração de dados de treinamento, treinamento e processos para operação contínua, bem como
* no processo de inferência near-RT RIC.

## Software O-RAN

Além das especificações, a Aliança O-RAN em cooperação com a Linux Foundation também está desenvolvendo uma implementação de referência de código aberto para a operação de um O-RAN. A organização responsável pelo desenvolvimento é o O-RAN Software Com-munity (abreviação:OSC)[4](#_bookmark3). De acordo com o documento branco atual "Plano Mínimo Viável O-RAN e Aceleração para comercialização" de 29. Junho de 2021 [35] é o objetivo dos desenvolvimentos da OSC "*para* *alcançar* *uma* *solução* *que* *possa* *ser* *utilizada* *para* a implantação *do* *setor* ". Para alcançar esse objetivo

4 https://o-ran-sc.org/

, implementações de referência são desenvolvidas para os vários componentes O-RAN. Esses desenvolvimentos são coordenados pelo Comitê de Requisitos e Arquitetura de Software (RSAC) e pelo Comitê técnico de Supervisão (TOC)[5.](#_bookmark4)

O TOC tem 12 membros votantes. Atualmente são 10 vagas. Os membros do TOC vêm de empresas de telecomunicações (AT&T, China Mobile, Deutsche Telekom, NTT Docomo, Orange, TIM) bem como de fornecedores (Ericsson, Nokia) e fornecedores (Radisys, Wind River Systems). As atas de reunião (incluindo gravações das reuniões online) são gratuitamente acessíveis no site do TOC. Além disso, efeitos de sinergia com outros projetos também são procurados. Destacam-se aqui os desenvolvimentos no âmbito da ONF[6](#_bookmark5) e da Plataforma de Automação de Rede Aberta (ONAP)[7](#_bookmark6).

Está planejado que aproximadamente. um novo lançamento é lançado a cada 6 meses. Os lançamentos são marcados com letras e palavras associadas. Atualmente, o quarto lançamento (D — Dawn) está em processo de lançamento.

Em princípio, a participação no desenvolvimento de software de código aberto é aberta a todos os interessados. Para participar, o "Contrato de Licença contributiva" (CLA) deve ser aprovado. As contribuições são colocadas sob a licença Apache, versão 2.0[8.](#_bookmark7) git é usado para gerenciamento de código fonte. Gerrit é usado para a gestão de propostas de mudança. O site de acesso público correspondente pode ser encontrado aqui: https://gerrit.o-ran-sc.org/

5 https://wiki.o-ran-sc.org/display/TOC

6 https://opennetworking.org/

7 https://onap.org/

8 www.apache.org/licenses/LICENSE-2.0[https://](http://www.apache.org/licenses/LICENSE-2.0)

# Metodologia e Escopo

Este capítulo fornece uma visão geral da metodologia de análise de risco O-RAN utilizada neste estudo. Os modelos de processo existentes para avaliação de riscos são descritos brevemente. Além disso, são apresentados os principais motivos e suposições.

## Geral e Escopo

A análise de risco realizada neste estudo é limitada exclusivamente ao 3GPP-RAN em sua variante de implementação O-RAN. Os limites das considerações são, portanto, dados pelas interfaces RAN para o dispositivo final (interface Uu) e para o núcleo 5G. Riscos para o sistema 5G global resultantes de dispositivos finais inseguros, incluindo componentes próximos a dispositivos finais (USIM, etc.) assim como de um núcleo 5G inseguro, não desempenham um papel neste estudo.

Neste estudo, apenas um 5G-RAN (NG-RAN) é considerado. Em particular, isso significa que se presume que o RAN esteja conectado a um núcleo 5G. As informações sobre as quais a análise de risco se baseia vem de documentos disponíveis publicamente. Isso se aplica, em particular, aos documentos fornecidos pelo 3GPP (normas, relatórios, etc.) e aos documentos fornecidos pela Aliança O-RAN. Dabei foi consultado sobre as versões atuais e disponíveis publicamente dos documentos durante o período de elaboração deste estudo (maio a setembro de 2021). Ao se referir às normas e especificações utilizadas, o versículo exatodo documento utilizado é indicado. Não foram levados em conta quaisquer sistemas depreciativos utilizados na prática ou implementações concretas das normas e especificações. Também nãofoi levada em conta a operação específica de umRAN por uma rede ou operador RAN. Nesse sentido, é possível que uma RAN praticamente implantada tenha menos riscos à segurança em comparação com os riscos identificados no resultado deste estudo, uma vez que o contratantepode ter implementado medidas adicionais de segurança para minimizar o risco.

A análise de risco essencialmente considerou apenas ameaças e vulnerabilidades específicas do 3GPP ou O-RAN. Os riscos genéricos de TI, que são mais geralmente atribuídos ao campo da tecnologia da informação e comunicação, como implementações defeituosas, configurações incorretas, etc., só são explicitamente mencionados e levados em conta em algunslugares. A principal razão é que há um grande número de análises de risco para o setor de TI, que não devem ser repetidas aqui, mas que devem, naturalmente, ser levadas em conta na avaliação geral de riscos no que diz respeito a uma implantação específica de RAN.

## Metodologias de Análise de Risco

Neste estudo, considera-se um*"efeito da incerteza sobre as metas"*[1]. O "impacto sobre as metas" é entendido como dano — os efeitos positivos sobre as metas não são, portanto, considerados neste estudo. O

"Incerteza" refere-se à ocorrência de eventos com determinadas probabilidades, pelo qual esses eventos são a causa do dano ocorrido (fontes de risco/causas de risco [36]). ==Referências== a descrição qualitativa do nível de risco é recorrida à fórmula usual:

Risco = probabilidade de ocorrência ⋅ Quantidade de dano

Existem uma variedade de modelos de processo de avaliação de risco (ISO 27005 [37], ISO 31000 [36], IEC 31010 [38], padrão BSI 200-3 [39], etc.). O procedimento é muitas vezes semelhante e é realizado de acordo com as seguintes etapas:

1. Determinação do atacante a ser considerado
2. Determinação de bens dignos de proteção
3. Determinação da criticidade das violações dos objetivos de proteção em relação aos ativos, ou seja. Determinação de danos potenciais
4. Identificar ameaças a objetivos e ativos de proteção
5. Identificação e avaliação das vulnerabilidades em relação às ameaças identificadas e levando em conta as medidas de segurança existentes
6. Determinação do risco com base nos pontos fracos e no possível dano
7. Avaliação de riscos, incluindo planejamento de medidas de gestão de riscos

A seguir, são descritos os objetivos de proteção relevantes e o modelo de abordagem no âmbito do estudo. Além disso, explicam-se os diferentes cenários considerados. Com base nisso, descreve-se o modelo de processo específico escolhido para este estudo.

## Objetivos de proteção considerados

Por um lado, este estudo considera os três objetivos habituais de proteção: **confidencialidade, integridade** e **disponibilidade,** bem como **imputabilidade** e **privacidade.** A seguir, breves explicações sobre a importância desses objetivos de proteção no contexto deste estudo.

*Confidencialidade* significa que dados e informações só chegam ao conhecimento de pessoas autorizadas. *Integridade* significa que os dados e informações são completos,precisos e atualizados, ou que isso claramente não é o caso. Este último significa, em particular, que a manipulação não autorizada dos dados e informações pode ser detectada. A formulação

"completo, correto eatualizado" refere-se a uma exibição dentro do sistema de TI em consideração — portanto, não é explicitamente levada em conta se os dados e informações sobre o mundo real estão completos, corretos e atualizados.

*Imputabilidade* significa que ações(por exemplo, envio de dados) da entidade envolvida (no exemplo: o remetente) podem ser comprovadamente atribuídas a terceiros. Deve-se notar que, na análise de risco em relação à confidencialidade, integridade e atribuição, as medidas de segurançaque podem ser realizadas dentro de um determinado caso de aplicação na camada de aplicação não são levadas em conta, uma vez que tais medidas de segurança fora do sistema considerado 5G-RAN seguir.

*A disponibilidade* geralmente significa que os dados e informações, bem como os serviços, estão então e lá disponíveis para pessoas autorizadas onde e quando são necessários por pessoas autorizadas. No contexto deste estudo, o objetivo de proteção também inclui prejuízos injustificados da qualidade do serviço (QS) ou aumento do número associado à prestação de serviços ou serviços. Fornecer dados e informações implica custos — como aumento do tempo de atraso, redução do rendimento ou aumento do consumode energia. As análises relativas ao objetivo de proteção da disponibilidade são de particular importância na medida em que, em geral — em contraste com os objetivos de proteção da confidencialidade, integridade e imputabilidade, a aplicação desse objetivo de proteção do ponto de vista da aplicação só é possível a um custo considerável ou não se a com... (no caso do estudo: 5G) não é confiável em termos de disponibilidade.

Neste estudo, o objetivo de proteção "*Privacidade*" subsue metas de proteção quegeralmente estão relacionadas à proteção de dados, como anonimato, incontrolabilidade ou desobservibilidade. As considerações relativas ao objetivo de proteção "Privacidade"estão, portanto, preocupadas com a questão da extensão em que se geram meta-dados que podem ser usados para violar a confidencialidade das circunstâncias da comunicação. Estes podem ser, por exemplo, meta-dados que permitem que vários processos de comunicação sejamacorrentados, de modo que um perfil seja formado no que diz respeito ao comportamento de comunicação (frequência, duração, localização, etc.) possível

É. Além disso, os meta-dados em conexão com as informações de localização podem ser usados para criar perfis de movimento ou geralmente divulgar quem se comunica com quem (possivelmente pseudônimo). Semelhante à disponibilidade, a privacidade também é umobjetivoútil, que sem o suporte adequado da rede de comunicação não é nem um pouco ou não. só pode ser implementado com um esforço considerável.

## Atacantes em consideração — Modelo de Atacante

Um elemento essencial na realização de uma análise de risco é o atacante e suas habilidades imputadas na avaliação dos riscos. Estes geralmente são combinados em um modelo de atacante. Este estudo leva em conta cinco modelos de atacantes diferentes com base nas seguintes funções (ver Figura 23):

* **Forasteiro:** Um atacante que só pode realizar seus ataques usando as interfaces definidas no sistema, pois inicialmente não tem controle sobre os componentes envolvidos no sistema. Em relação ao 5G-RAN, isso significa em termos concretos que o invasor pode usar tanto a interface de ar sem fio quanto o 3GPP ou 3GPP. pode atacar as interfaces especificadas da Aliança O-RAN. Presume-se que o invasor tenha controle total sobre o respectivo meio detransporte utilizado, ou seja, tanto no que diz respeito à conexão de rádio quanto às conexões usadas (baseadas em IP) entre os componentes 5G ou O-RAN, todos trocados Pode espionar dados e manipulá-los à vontade (alterar, excluir, atrasar, gerar, etc.).
* **Usuário: Um invasor que é**usuário final do sistema 5G no sentido do sistema 5G, ou seja, tem controle sobre um ou mais UE, que pode legitimamente usar serviços do sistema 5G. No contexto deste estudo, esse atacante também é atribuído as habilidades do "forasteiro". O "usuário" do atacante difere do atacante "outsider" na qual ele sabe credenciais/segredos ou que são necessários para o uso legítimo da rede 5G.
* **Operador de nuvem: Um invasor que tem** controle físico e lógico sobre a infraestrutura de nuvem (borda) usada pelo RAN 5G. Isso se aplica a todos os componentes de nuvem que não usam explicitamente componentes 5G-RAN (especificados por 3GPP ou 3GPP). a O-RAN Alliance) são e incluem componentes de hardware e software. Além disso, o atacante tem todas as possibilidades que o atacante

"Usuários".

* **Insider:** Um atacante que assume o controle exatamente de um RAN 5G ou 5G RAN. Componente O-RAN e que adicionalmente tem as capacidades do "usuário". Este atacante é particularmente interessante para investigar se a divisão fine-granular em componentes no caso de O-RAN pode ser um ganho do ponto de vista de segurança em comparação com o (pelo menos conceitualmente) bastante monolítico 3GPP-RAN. Como será explicado abaixo, a análise de risco é realizada pela primeira vez individualmente para as interfaces O-RAN relevantes antes que uma avaliação geral resumida seja derivada dela. Para a análise de risco de interfaces individuais, presume-se que o insider controla um componente que está conectado a essa interface,de modo que o insider tem acesso à interface –aqui vai essencialmente, a questão da extensão em que novos riscos surgem em relação a um insider devido a conhecimentos ou direitos adicionais em comparação com o "usuário" do invasor.
* Operador RAN: Um atacante que tem controle total sobre o 5G RAN. Este atacante é particularmente interessante para ser capaz de avaliar os riscos representados por um RAN comprometido. Este atacante estende

as habilidades do atacante "Insider" e possui de forma trivial as habilidades do atacante "Usuário".

Todos os atacantes considerados baseiam-se nas seguintes suposições comuns:

* recursos substanciais, embora não ilimitados (poder de computação, espaço de armazenamento, dinheiro, etc.) estão disponíveis. ==Referências====Links externos== cibercriminosos financeiramente fortes.
* ativos, modificando atacantes que relutam em quebraras regras mesmo fora das partes do sistema que controlam (por exemplo, manipulando dados transmitidos).
* A criptografia é segura, ou seja, acredita-se que os atacantes são incapazes de quebrar algoritmos e protocolos criptográficos que são considerados seguros de acordo com o conhecimento atual.
* Criptografia Segredos são seguros, ou seja, será assume que o Assaltante inicial nenhum Conhecimento sobre criptográfico Segredos (cryptogra- phische Chave etc.) ter o eles não em Razão dela Papel (veja acima) saber.
* ativo, mudando
* recursos significativos, mas limitados
* não pode quebrar cripto

**{resumo} Assaltante**

|  |  |
| --- | --- |
|  |  |
| **Estranho** | |
| - só tem acesso a interfaces especificadas | |

|  |  |
| --- | --- |
|  |  |
| **Utilizador** | |
| - utiliza serviços 5G com UE | |

|  |  |
| --- | --- |
|  |  |
| **Operadores RAN** | |
| - tem controle total sobre o RAN | |

*Ilustração 23: Hierarquia o Considerado Modelos de atacante*

- controlado

Infraestrutura em nuvem

**Operadores de Nuvem**

- controlado

em componente 5G

**Insider**

## Perspektiven

A análise dos riscos relacionados ao 5G-RAN e sua implementação O-RAN é realizada levando em consideração diferentes perspectivas, que são explicadas com mais detalhes abaixo. Por um lado, trata-se de perspectivas sobre diferentes stakeholders e, por outro, perspectivas sobre a implementação de medidas de segurança.

### Perspectivas das partes interessadas

Com a ajuda da perspectiva das partes interessadas, a análise de risco deve levar em conta diferentes grupos de interesse, cada um dos quais possui interesses e requisitos específicos em relação à segurança do RAN 5G ou do sistema global 5G. Isso permite uma visão diferenciada dos riscos 5G RAN.

* + - 1. *Usuários finais*

Um usuário final é uma entidade que conectou um ou mais dispositivos (UE) a uma rede 5G e usa os serviços da rede 5G relevante de acordo. Como principal interesse do usuário final, supõe-se que os objetivos de proteção listados acima (confidencialidade, integridade, imputabilidade, disponibilidade e privacidade) no que diz respeito aos dados do usuário transmitido (incluindo comunicação por voz) ou quanto ao uso da rede 5G. Como não se assume nenhum usuário final específico, a garantia de características de segurança se aplica a todos os tipos de serviços 5G e a todos os casos de aplicação nos quais uma rede 5G está envolvida. A este respeito, deve-se presumir que qualquer violação de um dos objetivos de proteção listados acima é crítica e pode potencialmente causar danos muito altos. Em particular, isso diz respeito às metas de proteção de disponibilidade e privacidade, uma vez que um usuário final só pode cumprir uma violação de alvo de proteção correspondente com um esforço considerável.

* + - 1. *Perspectiva* Social */* *Estado*

Como afirmado na introdução, as redes móveis já representam uma importante infraestrutura de comunicação. Sua importância provavelmente continuará a aumentar acentuadamente nos próximos anos, com serviços críticos e infraestruturas críticas (eletricidade, água, cuidados de saúde, logística e transporte, etc.) cada vez mais dependendo de uma infraestrutura 5G em funcionamento. Nesse sentido, a segurança, a confiabilidade e a confiabilidade das redes 5G são de grande relevância social. Isso deve ser levado em conta pelo "Estado" das partes interessadas.

Uma vez que essa perspectiva também se baseia em um grande número de casos concretos — especialmente críticos — de uso, também deve ser assumido no que diz respeito à perspectiva social/estatal de que uma violação dos objetivos de proteção mencionadosé de uma críticacertamente alta. Em particular, uma violação da disponibilidade é considerada particularmente relevante aqui.

* + - 1. *Operador de Rede 5G /* *Telco*

Um RAN 5G é uma parte essencial de um sistema 5G. Dependendo do modelo de operador, pode ser que o RAN 5G não esteja sob o controle físico direto nem lógico da operadora de rede 5G, mas que o funcionamento do RAN 5G de terceiros ==Referências== Em particular, também pode ser que os componentes 5G (hardware, software) sejam compartilhados por diferentes operadoras de rede 5G (compartilhamento RAN). Ao mesmo tempo, o 5G-RAN tem interfaces para a rede principal 5G como pretendido.

Com base nesses fatos, é necessário que uma operadora de rede[5G 9](#_bookmark8) conheça os riscos representados por um 5G RAN potencialmente não confiável para a operação global da rede 5G e os ativos associados a ela. Deve-se notar que aperspectiva da operadora de rede 5G considera principalmente os riscos em relação ao plano de controle.

9 No contexto do estudo, o termo 'telco' também é usado sinônimo para o termo operadora de rede 5G, a fim de melhorar a legibilidade.

Os riscos e riscos em relação aos dados de usuário transferidos são bastante secundários, uma vez que as análises correspondentes já são realizadas no âmbito da perspectiva do usuário final.

### Implementação de medidas de segurança

As informações sobre as quais a análise de risco se baseia, principalmente, são das informações fornecidas pelo 3GPP e 3GPP. da Aliança O-RAN publicou padrões e especificações. Em particular, a análise de risco não se baseia em uma implementação 5G-RAN concreta com propriedades precisamente especificadas. Em vez disso, as normas e especificações fornecem uma determinada estrutura dentro da qual as implementações compatíveis de um RAN 5G (O) podem ser justificadas. De particular relevância para esses estudos estão as medidas e mecanismos de segurança planejados e se sua implementação é obrigatória ou meramente opcional. Em particular, para levar em conta as medidas de segurança opcionais na análise de risco, dois cenários são assumidos:

* **pior caso**: nenhuma das medidas de segurança opcionais foram implementadas.
* **melhor caso**: todas as medidas de segurança opcionais foram implementadas.

Deve-se notar aqui que apenas medidas de segurança são tomadas em conta, que são pelo menos mencionadas como opcionais nas normas e especificações. Em relação a todas as medidas adicionais de segurança que um operador RAN 5G poderia implementar adicionalmente, presume-se que estas não tenham sido implementadas.

### Zusammenfassung

As três perspectivas de stakeholder listadas analisam os riscos do RAN 5G de um ângulo diferente. Para simplificar, pode-se dizer que a perspectiva do usuário final analizaos riscos em relação ao plano do *usuário,*  a perspectiva do operador de rede 5G se concentra no *plano* *de controle* e a perspectiva do governo combina *plano* *de usuário* *e* *plano* de controle Riscos. As *considerações de pior caso* /melhor *caso* refletem as situações extremas em relação às medidas protetivas implementadas.

## Metodologia aplicada para análise de riscos

De acordo com as explicações estabelecidas nos capítulos anteriores, utilizou-se a seguinte metodologia no contexto da análise de risco.

Em relação à  *fórmula* de risco (risco = probabilidade de ocorrência ∙ dano), deve-se notar que a avaliação de risco leva em conta apenas a probabilidade de ocorrência, uma vez que o dano depende da aplicação específica do 5G e pode ser muito alto em geral (ver Capítulo 3.5.1).

Quanto à probabilidade de *ocorrência,* por outro lado, não é realizada uma análise quantitativa exata, uma vez que, por um lado, não há dados disponíveis, por outro lado, uma análise quantitativa precisa também depende do caso de uso. Em vez disso, o estudo utiliza uma avaliação qualitativa, com três gradações sendo feitas:

* **alta**: Existe uma alta probabilidade de ocorrência se for, em princípio, possível para um determinado invasor com pouco esforço para explorar uma vulnerabilidade e, assim, desencadear o evento de risco, o que leva a um dano correspondente. Isso é especialmente verdade se a exploração das vulnerabilidades estiver dentro do escopo das possibilidades claramente concedidas ao invasor. Um exemplo é a transmissão não criptografada dedadosn sensíveis através de uma interface ou meio de transporte ao qual o invasor tem acesso de acordo com o modelo de invasor. Deve-se notar que despesas adicionais, que estão relacionadas à distribuição espacial do atacante, não são levadas em conta aqui. Por exemplo, uma interface de rádio não insegura na rede móvel celular pode significar que um invasor tem que fazer um grande esforço para a vigilância em massa nacional, que poderia ser usado como argumento para uma avaliação como um risco geral bastante médio. No entanto, o risco permanece

==Referências====Links externos== regiões geograficamente limitadas. Como caso de uso, há ataques em redes de campus em particular, para os quais o risco ainda deve ser avaliado como alto. Além disso, a exigência de acesso a sistemas de transmissão/recebimento amplamente distribuídos não significa necessariamenteque eles devem ser fisicamente construídos pelo invasor. usar seus ataques. Emparticular, deve-se levar em conta que, no futuro, o número de dispositivos finais continuará a crescer fortemente — com uma alta proporção de dispositivos finais inseguros, por exemplo, do setor de IoT, deve crescer fortemente. Uma vez que a consideração do aspecto de distribuição espacial do atacante é novamente apenas realmente significativa no que diz respeito a um caso de uso concreto, este aspecto (possivelmente redução de riscos) não está incluído neste estudo Levado em conta.

* **meio**: Umaprobabilidade média de ocorrência éassumida se o desencadeamento do evento de risco estiver, em princípio, no âmbito do que é possível de acordo com o modelo de atacante — em geral e sem suposições adicionais, no entanto, só pode ser implementado com considerável esforçopara oatacante. Um exemplo do "usuário" do invasor é que o invasor conecta uma variedade de dispositivos (que podem estar localizados em diferentes posições geográficas) à rede 5G, a fim de provocar uma sobrecarga da rede [10](#_bookmark9).
* **Baixa**: Uma baixa probabilidade de ocorrência é assumida se o desencadeamento do evento de risco estiver fora das possibilidades definidas de acordo com omodelo de aplicação ou se ele só pode ser acionado com probabilidade insignificante ou esforço extremo. O primeiro diz respeito, por exemplo, à manipulação não detectada de dados protegidos com a ajuda de métodos criptográficos, este último, por exemplo, a adivinhação de chaves criptográficas secretas.

Nesse sentido, a análise de risco preocupa-se em avaliar a probabilidade de violação do objetivo de proteção para cada invasor (Capítulo 3.4), perspectiva (Capítulo 3.5) e objetivo de proteção (Capítulo 3.3).

Deve-se notar que a análise da probabilidade de violações de alvos de proteção leva em conta não apenas ameaças e vulnerabilidades conhecidas,mas tambémas medidas de segurança de redução de riscos a serem aplicadas de acordo com as normas e especificações. Aqui, por sua vez, os riscos globais relacionados ao 5G-RAN como uma combinação resultam das ameaças e medidas de segurança implícitos pelas normas 3GPPe pelas ameaças e medidasde segurança implícitas de acordo com as especificações do O-RAN. As considerações de melhor caso/pior caso introduzidas no Capítulo 3.5.2 são aplicadas. Deve-se notar aqui que as melhoresconsiderações de e/pior caso podem ser aplicadas em relação às normas 3GPP e às especificações O-RAN. A este respeito, existem quatro combinações possíveis:

* melhores casos de suposições relativas tanto ao 3GPP quanto ao O-RAN (abreviados como: *bb*)
* piores hipóteses relativas tanto ao 3GPP quanto ao O-RAN *(ww);*
* as melhores suposições sobre O-RAN combinadas com as suposições do pior caso em relação ao 3GPP (bw)

10 Em algumas das análises de risco existentes no 5G, esse cenário de ataque está associado à Internet das Coisas, onde o cenário é que um invasor (hacker) ganha acesso a uma variedade de pessoas conectadas à rede 5G. Dispositivos IoT e depois os usa para ataques à rede 5G (especialmente para ataques de disponibilidade). Este exemplo também deixa claro que é difícil avaliar o quão demorado é para o atacante desencadear eventos de risco e depende de muitos fatores. No exemplo concreto, por exemplo, do fato de que o invasor não precisa de seus próprios dispositivos para o ataque, mas pode usar dispositivos estrangeiros.

* as premissas de pior caso em relação ao O-RAN combinadas com as suposições do melhor caso em relação ao 3GPP*(wb*).

A combinação de melhores casos com as suposições de pior caso foi feita em particular para determinar até que ponto as especificações do O-RAN têm um impacto sobre o risco global doRAN 5G. O resultado pode ser apresentado como uma visão geral de acordo com a Tabela 1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | Estado | | | | | Transportador comum | | | | |
| **Objetivos de proteção** | | | | | | | | **Objetivos de proteção** | | | | | **Objetivos de proteção** | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | **P** | **C** | **Eu** | **Um** | **Z** | **P** | **C** | **Eu** | **Um** | **Z** | **P** |
| Exterior em pé | *Bb* | *Bw* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Wb* | *Ww* |  |  |  |  |
| Utilizador |  | |  | |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| Operadores de Nuvem |  | |  | |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  | |  | |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| CORREU  Operador |  | |  | |  | |  |  |  |  |  |  |  |  |  |  |  |  |

*Tabela 1:* *Esquema* *para* *a* visão geral *da* avaliação *de* *risco.* *As* *células* da *tabela* *refletem* a probabilidade de ocorrência no melhor caso *(****b***) ou no pior dos casos (***w)***para uma violação*dealvo de proteção* em relação a um determinado invasor e uma determinada perspectiva *(stakeholder). Médias verdes:* *baixo,* *amarelo:* *médio* *e* *vermelho:* *alta* probabilidade de *ocorrência;* *um*  *campo* branco *significa* *que* *(atualmente)* *nenhuma* *declaração* é *possível.* *As* *abreviaturas* *para* o *objetivo* *de* proteção *são:* *C:* *Confidencialidade,* *I:* *Integridade,* *A:* *Disponibilidade,* *Z:* *Responsabilidade* *e* *P:* *Privacidade.*

A fim de criar uma análise de risco (sumária) para um sistema (geral), em alguns casos (especialmente no que diz respeito ao O-RAN) é realizada uma análise de risco pela primeira vez em relação aos componentes individuais do sistema (global). Essas avaliações individuais são então combinadas na avaliação de risco para o sistema (geral) no sentido de uma estratégia "por segurança". Isso significa que o risco global de um stakeholder, atacante e alvo de proteção é geralmente pelo menos tão alto quanto o maior risco único em relação a esse stakeholder, atacante e alvo de proteção. Se os riscos adicionais surgirem da composição dos componentes, o risco global também pode ser maior do que qualquer risco individual. Neste caso, a descrição da análise de risco para o sistema (global) devedarjustificativas adequadas. Deve-se notar que a redução do risco global por meio da composição não pode ocorrer, uma vez que na análise dos componentes individuais seu papel no sistema (geral) já é levado em conta (em particular, levando em conta medidas de proteção,como explicado acima). Se, por exemplo, apenas dados protegidos de ponta a ponta forem trocados por meio de uma interface sem garantia, um baixo risco será assumido (em termos de confidencialidade e integridade).

Por fim, deve-se ressaltar mais uma vez que as avaliações concretas relativas a um alto, médio ou baixo risco não são "matematicamente comprovadas", mas muitas vezes contêm uma certa avaliação subjetiva. Isso também resulta do fato de que nem todos os cenários possíveis poderiam ser analisados detalhadamente no quadro do tempo e dos recursos disponíveis. Isso diz respeito, por exemplo, ao insider atacante, que representa uma generalização grosseira na qual uma consideração mais detalhada de cada componente O-RAN individual poderia examinar quais riscos de segurança surgem se exatamente o em cada caso, o componente O-RAN é malicioso. Portanto, o leitor é obrigado a ler as notas textuais sobre

para levar em conta os riscos individuais. Em caso de dúvida, estes são decisivos no que diz respeito à avaliação de risco.

# Estudos existentes

Existem diversos estudos na literatura que tratam de ameaças, vulnerabilidades e riscos em relação ao sistema 5G global, bem como componentes individuais, como o RAN 5G. Abaixo está uma seleção deles brevemente apresentados. Particularmente notável é a análise de ameaças publicada pela Aliança O-RAN.

## Cenário de ameaça ENISA para redes 5G

Em dezembro de 2020, a Agência da União Europeia para a Cibersegurança (ENISA) publicou uma atualização de sua análise de ameaças [40] b e mais5G de novembro de 2019 [41]. A análise de ameaças atuais apresenta uma variedade de ameaças aos sistemas 5G, agrupados de acordo com componentes 5G e funcionalidades 5G. Uma análise de ameaças também é realizada especificamente no que diz respeito ao RAN 5G – embora não incluindo O-RAN.

Foram identificadas como principais ameaças:

* Comprometimento da qualidade de serviço em relação aos casos de uso de URLLC (Ultra-Reliable Low-Latency Communication, comunicação de baixa latência) ultra-confiável. Esta ameaça é meramente mencionada, mas ainda não está claro a partir de quais ameaças concretas e detalhadas esta avaliação é derivada.
* Interferência da transmissão de rádio por meio de transmissores de interferência.
* "*Falha em atender aos Requisitos Gerais de Garantia de Segurança: um conjunto de fraquezassurgirá* *através* *dos* *requisitos* de *atualização* *de* *vários* *elementos* *do* *RAN* devido *à* implementação de etapas de migração e à capacidade de sistemas de implantação antecipada para *cumprir as* atualizações de especificação *relativas às funções de segurança.* " Aqui permanece incerto o que exatamente significa. Também não está claro a partir de qual das ameaças detalhadas essa ameaça deriva. Supõe-se que se faz referência ao fato de que, na prática, sistemas mais novos também devem ser retrocompatíveis com padrões mais antigos e inseguros e, portanto, vulnerabilidades também são encontradas nesses sistemas e componentes mais recentes.
* Ataques na interface F1 devido às únicas medidas de segurança opcionais

Além disso, um grande número de ameaças mais ou menos gerais são listadas, que, portanto, não são específicas do 5G RAN, embora ilustradas em termos concretos para o RAN 5G. Estes incluem, por exemplo, erros de implementação (nos vários componentes, incluindo o hardware/software utilizado),erros de configuração, a não aplicação de medidas de segurançaplanejadas (criptográficas), acesso não autorizado a segredos que são usados, por exemplo, no contexto de medidas de segurança criptográfica (furos criptográficos secretos). As ameaças identificadas estão listadas no apêndice E do documento ENISA, embora seja impressionante que a maioria das ameaças especificadas sejam relevantes mesmo sem o contexto 5G (por exemplo: "Autoridade inadequadade autorização*e* controle *de* *acesso:* *As* *autorizações* *para*  *contas* *e* aplicativos *devem* *ser* *reduzidos* *ao* *mínimo* necessário *para* as tarefas que eles *têm*  *que*  *executar.* ").

## Análise de risco 5G da UE

Em outubro de 2019, o Grupo de Cooperação do NIS publicou um relatório sobre a análise de risco do 5G [42]. A base do relatório é um levantamento dos Estados-membros da UE sobre uma avaliação dos riscos do 5G. O relatório só lista riscos muito gerais — uma análise de ameaças mais detalhada é fornecida pela ENISA com o relatório descrito no Capítulo 4.1.

O risco para a Rede de Acesso ao Rádio foi classificado como "alto", o segundo nível mais alto (atrás de "crítico"). Informações concretas sobre como essa avaliação surgiu não podem ser encontradas no relatório.

No que diz respeito aos riscos gerais abordados no relatório, a falta de diversidade e a dependência associada a alguns fabricantes são importantes para o presente estudo. particularmente relevante, uma vez que o Open RAN, em particular, pode ser entendido como uma abordagem para combater esse risco. Além disso, a análise de risco aponta em vários pontos o risco representado pelos invasores do governo que poderiam tentar influenciar os fabricantes de componentes 5G para que eles entregassem componentes 5G maliciosos. Aqui, também, o Open RAN pode ser uma parte útil das contramedidas.

Além disso, os riscos gerais mencionados no relatório, como configurações erradas e controle de acesso inadequado, também são relevantes para a Rede de Acesso de Rádio e, em particular, para o O-RAN.

## Caixa de ferramentas da UE

Com base nos relatórios sobre riscos e ameaças relacionados ao 5G mencionados nos capítulos 4.1 e 4.2, o Grupo de Cooperação do NIS apresentou uma proposta de contramedidas gerais para mitigar os riscos em janeiro de 2020 [43]. Esta proposta é conhecida como "Caixa de Ferramentas da UE". As contramedidas estão divididas em três grupos: estratégico, técnico e solidário.

Em relação às contramedidas estratégicas, as seguintes são particularmente relevantes em relação ao presente estudo:

* *SM05*: Diversidade de Fabricantes de Componentes 5G
* *SM08*: diversidade em futuras tecnologias úteis; Construindo a expertise da UE neste campo

O aumento da diversidade e a redução da dependência de fabricantes individuais é mencionado em muitos lugares e em diferentes contextos, o que torna o papel da diversidade uma contramedida muito importante Sublinha.

Como mencionado acima, o Open RAN pode contribuir para a implementação dessas duas contramedidas estratégicas. Nesse sentido, é importante avaliar os novos riscos adicionados com o Open RAN/O-RAN para, em última análise, poder avaliar se o Open RAN/O-RAN faz parte da solução ou parte do problema ou quais medidas foram tomadas. Open RAN /O-RAN é parte da solução e não faz parte do problema. Fica.

As 11 contramedidas técnicas recomendadas na caixa de ferramentas da UEdizem respeito essencialmente à aplicação completa de medidas comuns de segurança de TI. Nesse sentido, também é importante analisar até que ponto a O-RAN implementa essas recomendações no que diz respeito às contramedidas técnicas.

No que diz respeito àscontramedidas de apoio, a medida *SA03* "Participação na padronização 5G" deve ser mencionada aqui, uma vez que uma das metas perseguidas é, por sua vez, aumentar a diversidade criando interfaces bem definidas.

## Estudos e Relatórios dos EUA

No setor norte-americano, há uma série de iniciativas e relatórios que lidam com riscos 5G e medidas correspondentes. Estes incluem, mas não se limitam a:

* "Estratégia CISA 5G" [44]
* "Potenciais vetores de ameaça para 5G Infrastructure" [45]
* "Estratégia Nacional para Garantir 5G" [46]
* "Estratégia Nacional para Garantir o Plano de Implementação do 5G" [47] (incluindo anexos publicados como documento separado [48])

Além dos riscos e ameaças "usuais", que também são encontrados em um grande número de documentos de outros estados e organizações, há dois riscos e associados

Medidas que também estejam relacionadas ao apoiodeste estudo. São elas:

* Os riscos da cadeia de suprimentos, especialmente porque atualmente há dependência dos EUA em fabricantes internacionais no que diz respeito ao RAN 5G (na "Estratégia Nacional para Garantir o Plano 5G Implementation" da Huawei, Ericsson, Nokia, Samsung e ZTE são apontados como fabricantes — pelo qual Huawei e ZTE são classificados como não confiáveis e, portanto, efetivamente fora de questão como fornecedores).
* Riscos de influenciar a padronização.

Para minimizar esses riscos, são descritas uma variedade de contramedidas, que em resumo servem aosdois objetivos:

* Aumento da diversidade em relação aos fabricantes de componentes 5G, idealmente uma alta proporção de fabricantes dos EUA
* Liderança no campo da padronização para influenciar o desenvolvimento de normas de acordo com os interesses americanos

Por sua vez, o Open RAN/O-RAN é visto como uma forma concreta de alcançar os dois objetivos mencionados. promover sua implementação.

## "As Propostas de Praga"

"As Propostasde Praga" [11](#_bookmark10) é um documento que surgiu como resultado da primeira Conferênciade Segurança 5G de Praga [12.](#_bookmark11) Ele contém algumas recomendações gerais sobre a segurança e implantação de redes 5G. Deve-se notar que as recomendações são tão gerais que se aplicam não apenas às redes 5G, mas, em princípio, a qualquer infraestrutura de TI ("Redes de comunicação e serviço devem ser projetados*com* *resiliência* *e* *ecuridade* *em* *mente*.", "*As partes interessadas* *devem*  *realizar regularmente* avaliações *de vulnerabilidade* *.",* " Estruturade *gerenciamento* *de* *riscos...* *deve* *ser* *implementado*." etc.). Além disso, são enfatizados os riscos da cadeia de suprimentos e a necessidade de diversidade no que diz respeito à fabricação de componentes 5G. As "Propostas de Praga" merecem ser mencionadas sobretudo porque são referenciadas como base em uma série de documentos e relatórios dos EUA (ver capítulo 4.4).

## Análise de modelagem e remediação de ameaças de segurança O-RAN

Como já mencionado, a própria Aliança O-RAN publicou recentemente (julho de 2021) um documento que trata de ameaças e riscos relacionados aoO-RAN [49]. As análises baseiam-se em um procedimento de acordo com a ISO 27005. As medidas de mitigação de risco vinculantes não estão especificadas na versão atual do documento. No entanto, isso está planejado para uma versão futura.

O documento em si lista inúmeras ameaças. Algumas delas também foram levadas em consideração na análise de risco realizada neste estudo. No entanto,muitas das ameaças listadas também são de natureza gerale não (O-)RAN específicas, como os autores do estudo da Aliança O-RAN estão cientes. Como resultado, apenas um subconjunto de ameaças são específicos de O-RAN, com um foco especial nas interfaces Fronthaul Abertas (CUS, M-Plane) e outras interfaces (O1, O2, etc.) (possivelmente temporárias) são bastante despercebidas.

Uma grande diferença entre a análise de risco da O-RAN e a apresentada aqui é a maneira como olhamos para o que realmente é um risco. Em O-RAN, o documento atual identifica apenas o "impacto" do risco, mas não a probabilidade de ocorrência, enquanto no presente estudo exatamente o oposto é feito:

11 https[://w](http://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf)ww[.v](http://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf)l[ada.cz/assets/media-centrum/aktualne/PRG\_proposals\_SP\_1.pdf](http://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf)

12 https://[www.prague5gsecurityconference.com/](http://www.prague5gsecurityconference.com/)

considera a probabilidade de ocorrência. No entanto, uma versão futura da análise de risco do próprio O-RAN também deve levar em conta a probabilidade de ocorrência.

As classes "Impacto" são classificadas em baixas, médias e altas, pelas quais o número de componentes prejudicados (O-DUs, O-RUs, etc.), a gravidade da ameaça às respectivas metas de proteção (Privacidade, Confidencialidade, Integridade, Disponibilidade) e os efeitos sobre possíveis topologias de sincronização (Modelo de Relógio) flui dentro

Como resultado, a Aliança O-RAN identifica 32 ameaças tão altas, 16 como médias e 5 como de baixo impacto. Resta saber até que ponto as outras interfaces existentes (O1, O2, etc.) ainda estão sendo investigados.

## Cenário de segurança de telecomunicações móveis da GSMA

O relatório [50] publicado pela GSMA (Global System for Mobile Communications Association) em março de 2021 tratou do que considera importante e em parte novas mudanças no país de segurança da indústria móvel. O relatório tratou com:

* "Sinalização & Inter-conexão"
* "Supply Chain"
* "Software & Virtualização"
* "Segurança Cibernética & Operacional"
* "Escassez de habilidades de segurança"
* "Dispositivo & IoT"
* "Segurança na nuvem"
* "Protegendo 5G"

A maioria dos riscos derivados das áreas sujeitas é mitigada no relatório por medidas gerais. A fim de reduzir os perigos do campo da "Segurança Cibernética & Operacional", por exemplo, recomenda-se: *"Bons practices de* segurança podem mitigar esse risco através de redes *seguras, autenticação forte, práticas de menor privilégio* ao lado *de* *uma forte* gestão de *acesso* *privilegiado*  *(PAM)."* [50]. No entanto, estas são (como já mencionado) apenas diretrizes gerais e, portanto, são menos adequadas para a prevenção de riscos concretos, pois isso deve ser muito mais específico para o domínio.

Em relação ao 5G, o relatório aponta que, embora o 5G tenha fechado muitas falhas de segurança através da arquitetura, as medidas de segurança correspondentes ainda não foram totalmente implementadas na prática. Os autores justificam isso com o fato de que a maioria das arquiteturas do 5G ainda não possuem um núcleo 5G; "*No* *present* *Non* *Stand* Alone as *implantações não estão fazendo uso pleno da segurança baseada em padrões, pois muito disso* *só* vem quando um núcleo *5G*  *(5GC)* é *implantado.* " [50].

Assim como nos estudos anteriores, o risco na área de "cadeia de suprimentos" também é destacado no relatório, especialmente por causa de cada vez mais intervenções nacionais: *"Em* *2020,* *vimos* *uma* *tendência* *crescente* *de respostas nacionais às* ameaças *da* *cadeia* *de suprimentos".*

Como diretrizes gerais, a GSMA recomenda que componentes de diferentes fabricantes sejam examinados individualmente em relação aos riscos que representam. Em particular, recomenda-se elaborar planos concretos no caso de um fabricante específico e, portanto, seu componente ser removido da rede: *"Construir* *planos* de *continuidade* de *negócios* que considerem *a* remoção de *fornecedores críticos; entender* *o* impacto *se one* *fosse* *removido.* [50]*. .* Também é recomendado olhar para soluções de rede aberta e experimentá-las em ambientes de teste.

13 Esses documentos já são discutidos nos documentos internos da ORAN, mas ainda não foram publicados, razão pela qual não se faz referência a eles aqui.

Em geral, pode-se afirmar que nenhum dos riscos apresentados no relatório são específicos para o 5G-RAN. Eles não identificam riscos específicos colocados por interfaces ou componentes de uma rede 5G, por exemplo. As diretrizes tratam principalmente de riscos que geralmente são encontrados em muitas infraestruturas fora das redes móveis.

# Análise de risco O-RAN

Nos capítulos seguintes, deriva-se a análise de risco sobre O-RAN. No capítulo 5.1, as considerações relativas aos atacantes "operadores de nuvem" e "operadores ran" são resumidas em relação a todo o O-RAN. Isso se deve essencialmente à posição proeminente dessas duas entidades/atacantes.

Para os outros atacantes, a análise de risco é inicialmente realizada separadamente em relação às interfaces individuais e blocos básicos especificados em O-RAN. A partir disso, uma análise geral de risco é então derivada no Capítulo 5.15. Em cada caso, o maior risco das respectivas considerações individuais é assumido como um risco global (ver também capítulo 3.2), uma vez que do ponto de vista do invasor é suficiente para ser capaz de explorar com sucesso uma vulnerabilidade no sistema para ataques — simplificando, O elo mais fraco da cadeia é o fator decisivo em termos de análise de risco.

Deve-se notar também que os resultados da análise de risco relativa ao RAN 3GPP (Anexo A:) foram incluídos na análise de risco sobre o O-RAN, como O-RAN como uma conversão de um 3GPP-RAT alguns dos riscos de segurança decorrentes das normas 3GPP, bem como efeitos positivos devido às medidas de segurança 3GPP

"herda".

## Atacantes: Operadores de nuvem e operadores 5G RAN

Os atacantes "operadores de nuvem" e "operadores RAN 5G" têm posições proeminentes. Ambos têm, em última análise, controle total sobre o RAN: o operador RAN 5G de acordo com as regulamentações, o operador de nuvem, uma vez que as especificações Atuais O-RAN não prevêemmedidas de segurança em relação aos operadores de nuvem não confiáveis. Em vez disso, é simplesmente assumido a partir de operadores de nuvem confiáveis:*"Administradores, integradores, oper-ators* *e orquestradores devem* ser *confiáveis,* *...* " [49].

A esterespeito, não há diferenças em relação ao "operador de nuvem" do atacante no que diz respeito às considerações relacionadas ao O-RAN. O mesmo se aplica ao invasor "OPERADOR RAN", que, entre outras coisas, tem controle total sobre as medidas de segurança O-RAN. Portanto, apenas as considerações de pior caso *(ww)* e best-case *(bb)* são realizadas abaixo.

**Na pior das hipóteses: Se nenhuma das medidas de segurança** 3GPP ou O-RAN especificadas como opcionais tiver sido implementada, o risco de violação dos objetivos de proteção deve ser avaliado como alto para todos os objetivos de proteção e para todas as partes interessadas, uma vez que neste caso o operador de nuvem/operador 5G-RAN tem acesso total a todos os dados processados e controle total sobre os dados processamento em si. A única exceção aqui é o backup de ponta a ponta dos dados do Plano de Controle no que diz respeito à integridade. Isso melhora a situação dos dados do plano de controle 3GPP – mas os dados internos de configuração e gerenciamento O-RAN estão desprotegidos, o que resulta em um risco médio.

**Melhor caso:** mesmo o melhor caso resulta em apenas uma situação marginalmente melhor. Para todos os stakeholders, a violação do objetivo de proteção da disponibilidade representa um alto risco. Em relação à perspectiva de "usuário final" do usuário final, uma violação dos objetivos de proteção de confidencialidade, integridade, privacidade e responsabilização também pode ser assumida, uma vez que as chaves criptográficas para proteger a interface aérea (Uu) são conhecidas pelo RAN. Devido ao ataque nacional fácil de realizar, também no que diz respeito a do stakeholder

O "Estado" vê um alto risco no que diz respeito àviolação dos objetivos de proteção da confidencialidade, integridade, imputabilidade e privacidade. Para o stakeholder "Telco" – ou seja, especialmente a perspectiva do plano de controle – a situação é ligeiramente melhor, uma vez que as mensagens correspondentes do Plano de Controle (NAS) entre A UE e a rede central são garantidas de ponta a ponta (entre UE e núcleo 5G). No entanto, a manipulação dos dados de configuração e gerenciamento específicos de O-RAN é possível, de modo que, no geral, um risco médio seja assumido.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Operadores de Nuvem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| CORREU  Operador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Análise de risco O-Cloud

O O-Cloud éo ambiente central de execução dos componentes O-RAN. Como já mencionado acima, um operador de nuvem não confiável cria riscos de segurança muito altos. O mesmo se aplica no caso de uma Nuvem O comprometida pelo invasor. Além disso,medidas eficazes de segurança, como controle de acesso e separação, são cruciais. As especificações O-RAN fazem apenas algumas especificações ou especificações. mesmo conter requisitos críticos de segurança.

Por exemplo, na especificação "Requisitos de Segurança" [51] há a única solicitação recomendada de controle de acesso: "O usuário deve ser*autenticado e autorizado*." Pelo lado positivo, deve-se mencionar aqui que os mecanismos de isolamento são certamente necessários: "*Meios* *de* *isolamento* de controle e recursos entre diferentes usuários devem ser *implementados*" –pelo qual tais mecanismos de isolamento são ineficazes sem uma autenticação de usuário simultaneamente obrigatória.

No pior caso do O-RAN, surge uma situação de risco em relação ao "forasteiro" do invasor, que é comparável à situação em relação ao "operador RAN" do invasor, uma vez que um O-Cloud comprometido é essencialmente equivalente ao controle total sobre os componentes O-RAN.

O melhor caso do ponto de vista O-RAN não pode ser avaliado no momento, pois praticamente não há requisitos de segurança em relação à O-Cloud.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Interface O2 de análise de risco

Conforme descrito no Capítulo 2.3.2, a interface O2 é usada para configurar o O-Cloud e implantar os componentes RAN de O-RAN, ou seja, os VNFs. A interface O2 pode ser considerada muito "poderosa" na medida em que pode ser usada para determinar toda a saídaeos componentes de software executados. Isso é ainda mais verdadeiro, uma vez que os cenários de implantação e casos de uso encontrados nos documentos O-RAN fornecem muita flexibilidade e, na medida em que a interface O2 deve ser suficientemente poderosapara suportar essadinâmica. O acesso não autorizado à interface O2 tem o potencial de comprometer o RAN, ou seja, permitir que um invasor controle total sobre toda a RAN.

Uma avaliação detalhada de risco é atualmente difícil, pois apenas os requisitos são descritos no que diz respeito à interface O2. especifica quais serviços devem ser disponibilizados com a ajuda da interface O2. No entanto, não está especificado como exatamente a interface é projetada, ou seja, quais protocolos específicos são usados, etc. ("*Os serviços O2 e suas interfaces associadas devem ser especificados na* *próxima* *especificação O2.* " [26])

Os autores das especificações O-RAN estão bem cientes de que a interface O2 deve ser protegida, pois definiram o requisito geral REQ-O2-GEN-TLS-FUN-1 e REQ-SEC-O2-1. No entanto, estes são formulados de forma bastante "suave": "Osprovedores de serviços*de envelhecimento* do homem e os consumidores que usam TLS devem suportar o TLS *v1.2 ou superior.* " [25]. O uso de protocolos de segurança (especificamente TLS) não é, portanto, prescrito em princípio

— apenas uma versão TLS mínima é definida se o TLS for usado. A este respeito, a descrição explicativa associada é: "As comunicações  *entre* *SMO* *e* *O-Cloud* são *seguras.* " [25] como enganoso e representa a expressãode um desejo em vez de um fato que pode ser derivado da especificação. Requisito.

Além de simplesmente proteger a conexão, por exemplo, com a ajuda do TLS, também é importante especificar exatamente quais componentes ou quais funçõespodem usar quais serviços de gerenciamentoe implantação. Com base nisso, uma gestão de direitos correspondente e um controle de acesso associado devem então ser implementados. É importante que a interface O2 seja projetada de tal forma que uma implementação do princípio de menor privilégio seja apoiada de forma natural, ou seja. h. que a interface oferece funcionalidades bem definidas com parâmetros bem definidos, quepermitem e em gestão de direitossuficientemente finos. O oposto disso seria uma interface bastante geral, por exemplo, acesso remoto via SSH, uma vez que aqui uma clara determinação das possibilidades de uma pessoa intitulada em princípio ou a implementação de restrições correspondentes em suas possibilidades é muito demorada e propensa a erros. are.

Como observado, o design exato da interface O2 não é claro — no entanto, há uma implementação de referência fornecida pela comunidade de software O-RAN. Isso é baseado em uma série de componentes de software existentes, como OpenStack, Kubernetes e ONAP. Esses componentes básicos por si só têm um alto grau de complexidade, de modo que configurações incorretassão prováveis [52], que por sua vez representam uma vulnerabilidade no caso de uma interface O2 menos restritiva e são potenciais para ataques, por exemplo, na área de escalada de privilégios.

Em relação às perspectivas definidas, atacantes e metas de proteção, a avaliação geral é a seguinte:

**O-RAN Pior Caso/3GPP-Pior Caso*(ww)***: Como nenhum mecanismo de segurança éobrigatório, até mesmo um forasteiro pode acessar a interface O2 e assumir o controle completo do RAN devido à sua potência. Isso permite uma violação da meta de proteção da disponibilidade em relação a todos os proprietários considerados. No que diz respeito ao usuário final, também deve ser assumida uma violação dos objetivos de proteção de confidencialidade, integridade e imputabilidade dos dados transmitidos, uma vez que o controle do invasor através das chaves de criptografia relevantes. No que diz respeito à operadora de rede 5G/telco, também são esperadas violações dos objetivos de proteção de confidencialidade, prestação de contas e privacidade. Isso se aplica a todos os dados relevantes para o O-RAN, como dados de configuração, incluindo chaves criptográficas, modelos de aprendizado de máquina, componentes de software O-RAN (incluindo rApps e xApps), arquivos de registro, etc. Uma vez que um ataque correspondente pode ser facilmente realizado em grande escala, um alto risco também pode ser assumido para o "Estado" das partes interessadas em relação a todas as metas de proteção. Aqui, porém, a integridade do ponto de vista do operador de rede é uma exceção: Apesar da adoção completa do RAN, os dados do Plano de Controle entre a UE e a AMF devem ser tratados pelo garantia de integridade obrigatória por meio de mecanismos 3GPP.

**O-RAN Pior Caso/3GPP-Best-Case*(fb):***  Aqui a avaliação dos riscos é análoga à do pior caso/pior caso. No entanto, os dados do Plano de Controle são criptografados na melhor das hipóteses pelas especificações do 3GPP entre a UE e a AMF, pelo qual o risco para o objetivo de proteção da confidencialidade em relação ao stakeholder "Telco" pode ser classificado como "meio". Issoocorre porque os outros dados do Plano de Controle específico do O-RAN estão desprotegidos.

O-RAN-Best-Case/3GPP-Best-Case **(*bb)***: Uma vez que todas as medidas de segurança opcionais são implementadas neste caso, na melhor das hipóteses, há uma baixa probabilidade de ataques bem-sucedidos por pessoas de fora e usuários que se aproveitam do O2- Interface. Em relação ao atacante "insider", por outro lado, uma alta probabilidade pode ser assumida. Uma vez que não há declarações concretas sobre gerenciamento de direitos e controle de acesso fino à interface O2, atualmente pode-se supor que atacantes de insider podem estender seus direitos comparativamente facilmente. Isso é especialmente verdadese o componente comprometido pelo insider for o quadro SMO.

A proteção na área O-RAN deve reduzir o risco de violação da disponibilidade objetiva de proteção, uma vez que o acesso trivial do exterior e do usuário à interface O2 não mais deve ser possível.

**O-RAN-Best-Case/3GPP-Worst-Case**  ***(bw):*** Aqui os riscos para as violações do alvo de proteção devem ser avaliados análogamente ao melhor caso/melhor caso. Só aqui nenhum dado de plano de controle entre UE e AMF é criptografado, o que aumenta o risco de

Mudou de "médio" para "alto".

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Análise de risco Interface O1

Conforme descrito no Capítulo 2.3.1, a interface O1 é usada para gerenciar todos os componentes O-RAN (exceto o próprio componente de gerenciamento). O acesso a esta interface permite que um invasor acesse acessos de longo alcance que são apenas um pouco menos poderosos do que o acesso não autorizado com a ajuda da interface O2.

No entanto, existem várias especificações para esta interface: Por um lado [17], que lida com a interface O1 em geral, e poroutro[53], por exemplo, que examina com mais detalhes a conexão entre O-DU e SMO com a ajuda da interface O1. Este último é particularmente relevante no contexto do estudo, pois vai além da descrição geral da interface O1 no que diz respeito aos requisitos e medidas de segurança. Assim, uma diferenciação de caso também é realizada abaixo.

### Análise de risco da interface geral do O1

Para a interface O1, as medidas de segurança ideais estão previstas nos documentos de especificação atuais. Especificamente, SSH e TLS são mencionados aqui [24]. Além disso, também é mencionada a implementação do princípio "Menos Privilégio".

Deve-se notar que o documento "Requisitosde Segurança" [51] faz declarações mais estritamente formuladas em comparação com a especificação real da interface O1: "A *interface* *O1* *quer*

*impor confidencialidade,* *integridade,* *autenticidade* através *de* *um* *transporte* *criptografado* *e* *menos* controle de acesso *privilegiado* usando o modelo de controle de acesso de configuração de *rede.* " No entanto, em alguns casos, os requisitos específicos baseiam-se novamente apenas em "suporte deve ser" – enquanto que no caso das notas a serem encontradas no mesmo documento no aplicável

"Conforme*definido na* *seção anterior, o O1 usará o TLS 1.2 ou superior para impor confidencialidade, integridade e autenticidade;* *e* *usará o NACM* *[10]* *para enforce menos* *privilegiado* *acesso*".

A descrição da interface do O1 geralmente se refere ao documento "Requisitos de Segurança" – mas apenas no que diz respeito ao "Controle de Acesso menos privilegiado", mas não no que diz respeito à proteção de camadas de transporte. No geral,no entanto, tendências positivas para garantir a interface O1 podem ser observadas aqui.

Devido à redação parcialmente incerta, no entanto, ainda se presume em relação à interface geral do O1 que as medidas de segurança não foram implementadas no pior elenco. Esta decisão é tomada em particular porque nas considerações feitas no Capítulo 5.4.2 sobre a especificação mais específica das interfaces O1para oO-DU ficará claro que as medidas de segurança também devem ser aplicadas no pior cenário. Dependendo do ponto de vista, essa avaliação também pode ser adotada como uma avaliação geral da interface O1 como um todo.

Em relação às opções de proteção TLS vs. SSH, o uso de SSH deve ser considerado mais arriscado. Isso se deve ao potencial "poder" do SSH já mencionado no Capítulo 5.1. Especificamente, a interface O1 usa o protocolo NETCONF, no caso de uma combinação com SSH, NETCONF-over-SSH [54] é, portanto, usado. O protocolo de conexão SSH [23] com um canal de Type é explicitamente usado

"sessão". Em princípio, esse tipo de canal permite a execução de qualquer programa. Do ponto de vista da segurança, é necessário, portanto, implementar o serviço SSH associado desta forma. configurar que apenas o subsistema NETCONF pode realmente ser iniciado. Especialmente no caso de as restrições correspondentes terem que ser implementadas por meio da configuração, isso resulta na vulnerabilidade de uma configuração errada.

Outro risco em relação ao SSH decorre da obrigação explícita de suportar algoritmos criptográficos inseguros: "As*interfaces O-RAN e 3GPP que implementam* *autenticação, confidencialidade e integridade usando ssh devem: ... Habilite um implantador O-RAN para* *configurar o SSH para oferecer* cifras menos seguras usando *configurações SSH padrão para permitir compatibilidade* *retrógrada* *com* *implementações SSH*mais *antigas* " [55].

Com base nos riscos baseados em SSH descritos acima, a recomendação é apoiar apenas o NETCONF-over-TLS [56] para a interface O1. A este respeito, no que diz respeito à análise do melhor caso, presume-se que a interface O1 seja garantida com a ajuda do TLS 1.3 usando algoritmos criptográficos que são considerados seguros, bem como autenticação mútua. É.

O MODELO DE CONTROLE DE ACESSO NETCONF (NACM) também será usado opcionalmente para impor o "Controle de Acesso de Menor Privilégio", pelo qual os seguintes grupos são definidos em [51]:

* O1\_nacm\_management – Permite alterar os direitos de acesso
* O1\_user\_management – Permite criar e excluir usuários para os nódulos O1
* O1\_network\_management — Permite que você leia, escreva e execute na base de dados <running>, que armazenatodos os parâmetros de configuraçãoatualmente em uso. O mesmo se aplica à base de dados <candidato> <candidato (se houver), ou seja, ao banco de dados NETCONF que contém parâmetros configurados, mas ainda não ativados.
* O1\_network\_monitoring – Permite ler configurações
* O1\_software\_management – Permite a instalação de novos softwares

No entanto, a natureza opcional nas especificações também deve ser expressamente notada aqui:

"*Os provedores de serviços de gerenciamento e os consumidores que utilizam o NETCONF devem apoiar o* *Modelo* de Controle de *Acesso* *de* Configuração de Rede *(NACM)* *[...]* " [56].

**O-RAN Pior Caso/3GPP-Pior Caso*(ww*):** Como nenhum mecanismo de segurança é obrigatório e a interface O1 — pelo menos no que diz respeito à funcionalidade do núcleo (O-)RAN — é tão poderosa quanto a interface O2, a Reflexões de capítulos

5.1 análogo. No entanto, o risco de uma violação de integridade é classificado como um meio do ponto de vista do operador de rede. Devido à garantia de integridade obrigatória dos dados do Plano de Controle (apenas sinais NAS) pelo 3GPP, não deve ser possível mesmo para um "insider" alterar pelo menos os dados do Plano de Controle trocados entre UE e AMF despercebidos. No entanto, ele ainda tem acesso aos dados do Plano de Controle no O-ORAN, que classifica a violação de integridade como média.

**O-RAN Pior Caso/3GPP-Best-Case (*wb*):** Aqui a consideração é análoga ao pior caso/pior caso: Uma vez que a garantia de integridade dos dados do Plano de Controle trocado entre UE e AMF é obrigatória, o melhor caso do 3GPP não traz qualquer melhoria sobre o pior cenário do 3GPP. Embora os dados do Plano de Usuário da UE sejam agora criptografados e protegidos por integridade, um invasor pode acessar as chaves correspondentes através da interface O1, o que significa que o risco permanece inalterado. Uma diferença importante,no entanto, é que os dados do plano de controle entre UE e AMF são criptografados de ponta a ponta neste caso. Portanto, do ponto de vista do operador de rede, o risco é avaliado como médio, uma vez que, apesar de tudo, os dados do plano de controle específico O-RAN sãocriptografados.

**O-RAN Best Case/3GPP** Best Case ***(bb):*** Devido às medidas de segurança (opcionais) fornecidas, a interface O1 fica melhor na melhor das hipóteses semelhante à interface O2. No que diz respeito ao invasor "usuário" e "forasteiro", o risco de violação dos objetivos de proteção de confidencialidade, integridade e responsabilização é, portanto, considerado baixo em relação a todas as partes interessadas. Se disponível, o risco é classificado como médio para todas as partes interessadas. O invasor poderia evitar alterações de configuração e mensagens de status por meio de ataques de disponibilidade na interface O1. Isso pode levar a prejuízos daqualidade de serviço doRAN, ou seja, a ataques de disponibilidade bem-sucedidos no próprio RAN. Deve-se notar aqui que, em contraste com a especificação da interface E2, uma falha da interface O1 atualmente não é explicitamente levada em conta nos documentos de especificação.

Uma vez que a interface O1 permite o gerenciamento de software, um insider com acesso a essa interface pode, em princípio, manipular os componentes O-RAN executados e, assim, obter acesso a chaves criptográficas armazenadas, por exemplo, no caso do O-CU, como já mencionado. Aqui é crucial o quão estritamente o princípio "menos privilegiado" é implementado e quais direitos um insider concreto realmente tem no resultado. Nesse sentido, o risco aos objetivos de proteção de confidencialidade, integridade e responsabilização em relação aos stakeholders "usuário" e "Estado" é avaliado como meio no que diz respeito a um insider. Uma avaliação semelhante também surge para o stakeholder "Telco". Embora partes da comunicação do Plano de Controle sejam protegidas de ponta a ponta (e, portanto, protegidas do acesso pelo insider), a interface O1 oferece acesso a muitas informações confidenciais de gerenciamento de rede, que do ponto de vista do operador de rede vale a pena proteger. (ambos no que diz respeito à confidencialidade, bem como no que diz respeito à integridade/imputabilidade).

**O-RAN-Best-Case/3GPP-Worst-Case** ***(bw):***  Embora as salvaguardas fornecidas pelas medidas protetivas 3GPP não se apliquem aqui, os mesmos riscos surgem como com o melhor caso/melhor caso, uma vez que os atacantes "forasteiros" e "usuários" no melhor caso O-RAN não têm acesso na interface O1. Sobre o atacante "Insider" novamente

as medidas de segurança 3GPP não mais existentes não pioram, pois não foram eficazes mesmo no melhor caso do 3GPP.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

### Análisesde risco da interface O1 entre O-DU e SMO

Em [53], a interface O1 entre O-DU e SMO é usada para instalação de inicialidade, software, configuração, desempenho, falha e gerenciamento de arquivos.

Para a segurança da conexão, o TLS ***deve*** ser usado para a autenticação do O-DU, pelo qual o caractere obrigatório geralmente é raramente encontrado nas especificações. Além disso, o backlog de dados NETCONF deveser protegido pormeio do TLS: "Nesta*versão da Especificação de Interface O1, a* *segurança* *do* *protocolo* *NETCONF* *é realizada usando* *TLS."* [53].

O MODELO DE CONTROLE DE ACESSO NETCONF (NACM) também deve ser usado ***para*** impor o "Controle de Acesso de Menor Privilégio". Em geral, a especificação contém principalmente a implementação obrigatória de mecanismos de segurança em contraste com os mecanismos de segurança em 5.3.1.

Embora não seja mencionado como de costume por meio de "deve" que os objetivos de escombros de confidencialidade, integridade e responsabilização devem ser aplicados, a redação deixa:

"*[...] a interface O1 aplicará confidencialidade, integridade, authenticidade [..] e menor* controle *de* *acesso* privilegiado *[...]."* [56] conclui que o mesmo se destina.

**O-RAN-Pior**  Caso/3GPP-Pior Caso **(ww):** Uma vez que mesmo no caso wort-case a interface é protegida pelo caráter obrigatório das medidas de segurança, há pelo menos para

"Forasteiros" dificilmente têm a oportunidade de acessar essa interface lendo e especialmente escrevendo. No entanto, os ataques de disponibilidade básica que impedem certas mensagens de status e configuração não podem ser evitados.

Assim como na avaliação geral da interface O1, também pode ser dito sobre o "usuário" do atacante que as metas de proteção de confidencialidade, integridade e responsabilização têm um baixo risco de lesão.

Um "insider", por outro lado, pode quebrar as metas de proteção de confidencialidade, integridade e responsabilização no pior dos casos, uma vez que as medidas protetivas da O-RAN não podem compensar as salvaguardas 3GPP que não existem neste caso. Aqui, o O-DU como

"Insider" saiu. Além disso, um insider pode (dependendo de sua afiliação emrelação a grupos de direitos) na pior das hipóteses, instale seu próprio software no O-DU e, assim, ganhe controle sobre o O-DU. Isso resulta em um alto risco de disponibilidade. No entanto, apesar de tudo, o insider não pode quebrar a integridade dos dados do Plano de Controle entre a UE e a AMF, pois estes são obrigatórios protegidos pelas medidas 3GPP.

**O-RAN Pior Caso/3GPP-Best-Case (*wb*):** Como todas as medidas para garantir os objetivos de proteção são obrigatórias, os riscos devem ser os mesmos do caso "ww". Do ponto de vista do backup 3GPP, além da garantia de integridade, a confidencialidade dos dados do Plano de Controle entre UE e AMF também é garantida, pelo qual o riscopode ser classificado como"médio" com um "insider".

**O-RAN Best-Case/3GPP-Best-Case*(bb):*** No que diz respeito ao melhor caso, a avaliação dos atacantes "forasteiros" e "usuários" é congruente com a do pior caso devido à natureza obrigatória das medidas de segurança O-RAN. Somente no caso do "insider" do invasor pode ser determinado no que diz respeito aos objetivos de proteção de confidencialidade, integridade e imputabilidade que as medidas de segurança do 3GPP impeçam uma violação das metas de proteção. Em relação à disponibilidade, pode-se argumentar que, mesmo no melhor cenário, o insider não pode injetar malware através do NACM, uma vez que ele não tem os direitos necessários, mas dependendo do ponto de vista, ele próprio pode ser o O-DU, o que lhe permite limitar facilmente a disponibilidade.

**O-RAN Melhor Caso/3GPP Pior Caso (*bw*):** Neste caso, a avaliação dos riscos é a mesma do caso anterior "bb". Neste caso, apenas o sigilo no plano de controle entre UE e AMF não é assegurado pelo 3GPP, pelo qual o risco é avaliado como "médio".

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Interface A1 de análise de risco

Como descrito no Capítulo 2.3.3, a interface A1 é usada principalmente para comunicar diretrizes sobre a configuração/otimização do RAN para o RIC quase em tempo real. Essas diretrizes são projetadas como políticas declarativas. Expressa *o que* deve ser alcançado, mas não *como* deve ser alcançado. As decisões concretas de implementação fazem parte do RIC quase em tempo real e dos xApps.

A interface A1 foi projetada para oferecer oportunidades para impor confidencialidade, integridade e autenticidade (incluindo proteção contra ataques de replay) [51]. Para isso, o TLS é opcionalmente fornecido para a proteção da comunicação [57], [51], [49]. Umaameaça à interface A1 surge do fato de que, para implementar a comunicação bidirecional, ambos os pontos finais (Não-Real Time RIC, Near-Real Time RIC) da interface A1 atuam como servidores [57]. A superfície de ataque resultante das portas abertas necessárias deve ser minimizada por apenas um ponto final atuando como um servidor e realizando comunicação bidirecional sobre uma conexão existente. Além disso, tecnologias como conexão reversa podem ser usadas para implementação.

Em relação à melhor análise do melhor caso/pior caso, deve-se notar que os riscos correspondentes aqui dependem essencialmente da melhor situação/pior caso em relação às especificações O-RAN. Em Gem torno da funcionalidade da interface A1, no entanto, o risco resultante é em grande parte independente da melhor situação caso/pior caso em relação aos padrões 3GPP.

**Pior caso:** Como a interface A1 não está insegura na pior das hipóteses, pessoas de fora têm a opção de ler e escrever acesso a esta interface. Políticas adequadamente manipuladas, pelo menos prejudicam a disponibilidade (redução da qualidade do serviço). Nesse sentido, assume-se um alto risco para todas as partes interessadas no que diz respeito à disponibilidade.

No que diz respeito aos objetivos de proteção da confidencialidade, integridade e responsabilização, assume-se um baixo risco para a perspectiva do usuário, mesmo no pior dos cenários, já que nenhum ataque é identificado atualmente que permitem que um invasor leia ou manipule o acesso aos dados do avião do usuário, mesmo com acesso à interface A1. Deve-se notar aqui que são necessárias análises mais aprofundadas para realmente descartar a possibilidade de que nenhum dado de avião do usuário seja transmitido através da interface A1. Em particular, no caso de versões futuras das especificações, deve ser verificado quais serviços são oferecidos especificamente através da interface A1 e se os dados do plano de usuário são transmitidos aqui. será.

Em relação à perspectiva "telco", essa avaliação muda para um risco médio, uma vez que as informações de gerenciamento de rede dignas de proteção são transmitidas através da interface A1 (no que diz respeito à confidencialidade e integridade). tornar. Essa avaliação também foi adotada para a perspectiva "estado".

**Melhor caso: Devido** à proteção com tls, não é possível para um estranho ou um usuárioatacar com sucesso a interface A1 em termos de confidencialidade e integridade no melhor caso. Somente ataques de disponibilidade na interface A1 podem ser imaginados. Devido à funcionalidade da interface A1, pode-se supor que ataques de disponibilidade inteligente nesta interface podem prejudicar a disponibilidade do RAN – pelo menos no sentido de reduzir aqualidade doserviço. Isso é especialmente verdade porque uma falha da interface A1 não é explicitamente levada em conta nas especificações. Nesse sentido, assume-se um risco médio para todas as partes interessadas aqui.

Uma vez que as medidas de segurança só fornecem proteção contra pessoas de fora (criptografia de conexão) — um conceito de direitos e papéis no que diz respeito ao controle de acesso à interface A1 pode, na melhor das hipóteses, ser adivinhado entre as linhas da especificação, atualmente se presumeque um insider tenha acesso total à interfaceA1, mesmo na melhor das hipóteses. Para ele, a situação é semelhante à palavra-caso para um estranho. Por outro lado, nenhum ataque poderia ser identificado atualmente com a ajuda de um informante no que diz respeito aos objetivos de proteção de confidencialidade, integridade e responsabilização pode obter uma vantagem significativa com base no acesso à interface A1. Por favor, note os comentários feitos acima sobre uma análise aprofundada necessária.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Interface R1 de análise de risco

Conforme explicado no Capítulo 2.3.4, a interface R1 serve os rApps para acessar as funcionalidades RIC não em tempo real, bem como outros serviços que um rApp precisa para executar suas tarefas. Está previstoque: "*A* *interface* *R1* *é* *a* *única* *interface* *entre* *um* *rApp* *e* *a* *funcionalidade* *do* *RIC* *e* SMO *não-RT.* *Portanto,* *a* *interface* *R1* *deve* ser definida para atender a todas as *necessidades funcionais de rApps, com recursos apropriados de extensibilidade de interface* *conforme* *necessário.* " [28]. A interface R1 é, portanto, considerada muito poderosa.

Ao mesmo tempo, atualmente é em grande parte não especificado. Há algumas declarações gerais e alguns requisitos, mas nenhum projeto concreto. As seguintes informações são relevantes do ponto de vista da segurança:

* + - "*seria útil para a Aliança O-RAN definir uma interface aberta e padrão* *através* da *qual* *o* *RIC* *não-RT* expõe *as funcionalidades* do *SMO* *Framework* *a* *"rApps"* *através* da funcionalidade de *exposição* *dos* *Serviços* *R1.* *Vamos* *nos referir* *a* *isso* *como* *a* interface *"R1"* [28]
    - "*recursos são oferecidos para consumo e uso através dos serviços R1. Tais* *serviços incluem, mas não se limitam a: serviços relacionados ao A1, serviços relacionados ao O1,* serviços *relacionados ao* O2, *...* " [28]

A forma como o sitefoi projetado também não está clara. É razoável supor que atualmente se presume que mais chamadas internas de API sejam feitas que não ocorram através de uma interface de rede entre diferentes computadores. Essa presunção surge, entre outras coisas, do fato de que a interface R1 não é mencionada em vários documentos O-RAN no que diz respeito às novas interfaces abertas. Por outro lado, a partir da definição geral da interface R1: "*Interface R1:* *Interface* *entre* *rApps* *e* *estrutura* *RIC* *não-RT* através *da* *qual* os Serviços *R1* *podem* *ser* *produzidos* *e*  *consumido*" [58] não excluem que a interface R1 seja implementada como uma interface baseada em rede. No contexto deste estudo, portanto, supõe-se no que diz respeito ao melhor cenário de que a interface R1 é apenas APIs internas, em termos de da análise mais importante, presume-se que a interface R1 esteja acessível através da rede. No momento,as medidas de segurança não estão especificadas em relação àinterface R1. Somente em relação aos rApps é mencionado que o acesso aos serviços R1 só deve ser possível após a autenticação e autorização. Os detalhes de como isso deve ser implementado ainda não estão especificados.

Devido à conexão básica dos serviços O1, O2 e A1 e como não são especificadas restrições relativas ao uso dessas interfaces, os resultados relativos à interface O1, O2 e A1 são utilizados como base para a análise de risco em relação à interface R1. O maior risco em relação a uma dessas interfaces é considerado o limite mais baixo para o risco em questão em relação à interface R1 — a interface R1 não pode, portanto, ser melhor do que as interfaces O1, O2 ou O1. Interface A1.

Deve-se notar também que, para as considerações de melhor caso/pior caso, a situação em relação às especificações O-RAN é decisiva. No pior cenário da O-RAN, o O1

/ Interface O2 assumir o controle dos componentes O-RAN. Portanto, neste caso, quaisquer medidas de segurança 3GPP implementadas dificilmente podem ter efeito ou ser ignorado. Por outro lado, no melhor caso do O-RAN, o uso indevido da interface R1 é evitado – a este respeito, desempenha um papel subordinado se as medidas de proteção do 3GPP são implementadas neste caso ou não. Uma exceção aqui é a perspectiva telco no que diz respeito ao objetivo de proteção da confidencialidade, uma vez que aqui no melhor caso do 3GPP ocorre um backup de ponta a ponta do plano de controle, que também oferece proteção no pior caso da O-RAN.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Interface E2 de análise de risco

Conforme indicado no Capítulo 2.3.5,a interface E2 é usada principalmente para gerenciar os nódulos E2. No decorrer disso, há um serviço ("REDE DE FUNÇÃO RAN (NI)" [59]), que permite observar e alterar todo o tráfego de dados das interfaces de rede dos nós E2 com a ajuda da interface E2. Especificamente, são oferecidos os seguintes serviços, entre outros:

* + - "*Cópia da mensagem completa com cabeçalho fornecendo*tipo de interface networ*k, identificador* *e* *direção com* *timestamp* *opcional* de interface de *rede* "
    - "*Injeção de mensagem completa com cabeçalho fornecendo tipo de interface de rede de destino,* *identificador* *e* direção *e*  *prioridade* *opcional* de mensagem *de controle* *RIC* "

Esses serviços têm um alto potencial de risco do ponto de vista da segurança.

As medidas de segurança previstas na especificação são atualmente consideradas opcionais. Especificamente, é definido como um requisito que a interface E2: "*deve* suportar *confidencialidade, proteção integrity e replay*"[29]. Uma declaração semelhante também pode ser encontrada em [51].   [49] propõe, no que diz respeito à proteção IPSec: " IPSEC: Deve ser usado para proteger o tráfego de E2 " (semelhante a [51]: " Para a proteção de segurança na camada IP na interface E2, o IPsec deve ser suportado ").

Com base nas possibilidades funcionais da interface E2 e nas medidas de segurança, é realizada a seguinte avaliação de risco.

**O-RAN-Worst-Case/3GPP-Worst-Case (*ww*):** Como nenhuma medida de segurança é implementada no pior cenário – além da proteção de integridade dos dados do Plano de Controle – e a interface E2 permite acesso total a todo o tráfego de dados 3GPP dos nós E2, um estranho está essencialmente exposto a um alto risco no que diz respeito a Confidencialidade, disponibilidade e prestação de contas em relação a todas as partes interessadas. Em relação ao stakeholder "Telco", um risco médio é assumido devido à garantia de integridade 3GPP dos dados do Plano de Controle, uma vez que os dados específicos de O-RAN (configuração) estão desprotegidos ao mesmo tempo.

**O-RAN Pior Caso/3GPP-Best-Case*(fx adj):***  A situação está mudando aqui, pois as medidas de segurança do 3GPP fornecem proteção em relação aos objetivos de proteção de confidencialidade, integridade e responsabilização. A única questão aqui é até que ponto o invasor "insider" tem acesso às chaves para proteger o plano do usuário ou o plano do usuário. sobre os dados do avião do usuário não criptografados. Em princípio, as chaves correspondentes estão disponíveis na U. É necessário fazer uma análise aprofundada para poder excluir tais riscos com certeza, o que leva à avaliação de um risco médio.

**O-RAN Best Case/3GPP Best Case*(bb*):** Na melhor das hipóteses, a interface E2 e as interfaces 3GPP são protegidas. Portanto, um estranho pode, portanto, essencialmente apenas realizar ataques de negação de serviço na interface E2. A confidencialidade, a integridade e a responsabilização são, portanto, consideradas de baixo risco para todas as partes interessadas.

Os ataques "estúpidos" do DoS são apenas de efeito limitado, uma vez que as especificações do ORAN estipulam que o RAN deve estar funcional mesmo se a interface E2 falhar. No entanto, uma funcionalidade com qualidade limitada de serviço pode ser assumida aqui — caso contrário, não haveria necessidade de uma interface E2. Além disso, os efeitos dependem do projeto concreto de um nó E2. Através do tráfego de dados manipulado inteligentemente na interface E2, um invasor pode obter uma alta carga de computação em um nó E2 devido às operações criptográficas associadas ao IPSec. Em casos extremos (se a separação não for bem implementada), isso pode levar à falta de poder computacional disponível para as tarefas reais de um nó E2. Também não está claro seataquesDoS "inteligentes" podem levar a um maior impacto na qualidade do serviço. Concebíveis aqui são ataques que especificamente atrasam pacotes de dados de tal forma que os mecanismos de detecção no que diz respeito a uma falha da interface E2

(Temporizador etc.) só que ainda não foi acionado. Além disso, é necessário investigar até que ponto é possível atribuir tráfego de dados criptografados a serviços individuais de E2 ou funções E2, apesar da criptografia IPSec (por exemplo, por meio de análises de tráfego em relação a padrões específicos de tráfego de comunicação de serviço). Isso permitiria a interrupção direcionada de serviços E2 individuais ou funções E2 e poderia levar a efeitos maiores em comparação com uma "falha" completa da interface E2. No geral, portanto, o risco de disponibilidade é visto como meio para pessoas de fora e para todos os stakeholders.

O "usuário" do atacante está apenas em uma posição (atualmente) ligeiramente melhor. Como um risco/nova ameaça recém-adicionado, o usuário pode gerar tráfego de dados em relação ao U ser Plane and Control Plane, que deve ser consideradocomo legítimo emprincípio. O usuário pode projetar habilmente esse tráfego de dados de tal forma que ele seja incluído nas funções de análise e avaliação fornecidas pela interface E2 (no que diz respeito às interfaces 3GPP). Dependendo do quão concretas essa análise e avaliação funcionam, essa possibilidade de influência pode ser vista como um "trampolim" para novos ataques. É particularmente o caso se os sistemas correspondentes não foram desenvolvidos com a premissa de que os dados de análise e avaliação registrados devem, em princípio, ser considerados potencialmente "maliciosos". Por exemplo, dados de plano de usuário ou plano de controle criados inteligentemente podem ser usados para ataques da área de "estouro de buffer" ou ataques de injeção (injeção SQL, etc.). Outra opção é influenciar o treinamento de machine learning com base nos dados registrados. No geral, esses ataques provavelmente terão um impacto primário na disponibilidade. No entanto, uma vez que a análise do melhor caso assume, em princípio, que todos os sistemas funcionam sem erros, não há uma avaliação geral de risco aumentada em comparação com o "remetente externo" do invasor.

Em relação ao atacante "Insider", um atacante que tem acesso à interface E2 é assumido. Um bom exemplo disso é um xApp. Embora as especificações aqui e ali geralmente falem de "políticas" e "autorizações" em relação aosxApps – mas como não há diferenciação e nenhum gerenciamento de direitos é reconhecível em relação à especificação atual da interface E2, atualmente se supõe que mesmo no melhor caso um xApppode usar a interface E2 emuma extensão limitada. Se este não for realmente o caso em relação a um xApp, é provável que ele se aplique em qualquer caso ao componente "Near-Real Time RIC".

O suposto acesso à interface E2 facilita a realização de ataques de disponibilidade por um insider, o que resulta em um alto risco para todas as partes interessadas. Em termos de confidencialidade, integridade e responsabilização, a perspectiva de um usuário final depende de qual componente o insider controla. Se este componente tiver acesso à interface E2, bem como conhecimento das chaves usadas para proteger a interface Uu, há um alto risco. Seo acesso às chaves criptográficas não for possível para o insider, há um baixo risco. Como consequência geral, um risco médio é assumido aqui. Essa avaliação de risco também é assumida para o stakeholder "Staat". Em relação ao titular da estaca "Telco", há uma situação um pouco melhor por um lado, uma vez que o tráfego de dados do Plano de Controle é garantido de ponta a ponta. Por outro lado, a interface E2 permite: "Exposição de dados*selecte*d*E2 Node (por exemplo, informações de configuração (configuração de célula,* *fatias suportadas, PLMNs etc.), medições de rede, informações* de contexto, *etc.) para o RIC Near-RT*"[29]. Por um lado, esses dados são considerados um segredo comercial digno de proteção, por outro, a implementação da integridade é considerada importante, pois esses dados formam uma base para a operação da rede. Nesse sentido, assume-se um risco médio em relação à telco e aos objetivos de proteção da confidencialidade, integridade e imputabilidade.

**O-RAN-Best-Case/3GPP-Worts-Case*(bw*):** Ao proteger a interface E2 no caso O-RAN-best-case, não há possibilidades diretas para que os atacantes "usuário" e "outsider" usem a interface E2 para ataques. O acesso à interface E2 permite que o insider viole alvos com sucesso em relação a quase todas as metas e perspectivas de proteção e, ao mesmo tempo, não sejam as medidas de segurança 3GPP existentes (com exceção do garantia de integridade dos dados do plano de controle no caso 3GPP-worts) – isso resulta em um risco correspondentemente alto.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Usuários |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Emsider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Risikoanalyse Open Fronthaul M-Plane

A interface Open Fronthaul M-Plane permite, conforme descrito no capítulo 2.3.7, o gerenciamento dos componentes O-RU. Do ponto de vista do risco, a possibilidade de ser capaz de realizar uma atualização de software em relação aos componentes O-RU com a ajuda da interface Open Fronthaul M-Plane é particularmente relevante. Em princípio, isso permite que um invasor assuma o controle total da O-RU instalando softwares apropriadamente manipulados. De acordo com a especificação O-RAN, a proteção do software não é fixa, mas "*O* *uso* *de* *compressão* *e* *cifra* *para* *o* *conteúdo* da *compilação* *de* *software* *é* *deixado* *para* *o* *fornecedor*  *implementação.* *O* *único* *arquivo* *que* *nunca* *deve* *ser* *cifrado* *é* *o* *arquivo* *manifesto.xml* "[31]. No entanto, o manifesto em particular contém informações que devem ser protegidas contra manipulação. Um risco especial surge do fato de que, com a ajuda da interface Open Fronthaul M-Plane, a URL de anúncio downlopode serlivremente especificada em relação ao software a ser instalado. Aqui seria melhor fornecer restrições, por exemplo, para que o host seja "fixo" configurado na O-RU, de modo que os efeitos de possíveis intervenções manipulativas na transmissão da URL de download (redirecionamento para um servidor sob o controle do invasor) sejam limitados em seus efeitos negativos.

Além disso, supõe-se que o acesso à interface Open Fronthaul M-Plane permite ataques bem-sucedidos à disponibilidade, uma vez que a interface Open Fronthaul M-Plane é usada para alterar os dados de configuração armazenados na O-RU pode ser usado para o comprometimento da qualidade do serviço ou para uma falha completa da funcionalidade O-RU.

Ao contrário de quase todas as outras interfaces, as considerações para garantir a interface Open Fronthaul M-Plane são relativamente extensas – e dependendo da interpretação – até mesmo destinadas a serem obrigatórias. Especificamente, a aplicação de SSH (suportado obrigatório) ou TLS (opcional) é possível aqui. Para minimizar o risco, deve-se evitar o uso de SSH em favor do TLS (como explicado com as interfaces O1 e O2). No que diz respeito à segurança, é necessária autenticação mútua.

O escopo de interpretação em relação aos mecanismos de segurança obrigatórios resulta, essencialmente, da redação pouco clara nos documentos de especificação. Por exemplo, há a declaração: "O  *M-Plane* *fornece* *segurança* de *ponta* *a* *ponta* *como*

*uma característica obrigatória.* " [31]. No entanto, um "recurso" é uma propriedade ou capacidade de um componente e não precisa necessariamente ser aplicado. Por outro lado, uma tabela a seguir mostra que os objetivos de proteção da confidencialidade, integridade e responsabilização foram implementados – no entanto, a razão aqui dada é apenas o apoio de princípios do SSH ou TLS, mas não sua aplicação obrigatória. Natabela "*Recursos Obrigatórios e Opcionais para* *Autenticação*O-RU" listada posteriormente, todos os mecanismos de autenticação são marcados como "*opcionais* *de* *usar*". Aqui seria melhor esclarecer – se essa é a intenção da especificação – que, embora cada mecanismo individual seja opcional, pelo menos um deve ser utilizado.

No geral, no entanto, pode-se estimar que a interface Open Fronthaul M-Plane contém muitas considerações em termos de segurança. Deve-se notar aqui que a descrição das interfaces Open Fronthaul também é muito mais extensa em geral em comparação com as outras interfaces.

No que diz respeito à segurança, deve-se mencionar também que um conceito de direitos/função é fornecido. Quando sind 6 funções mencionadas na especificação:

* sudo
* Smo
* híbrido-odu
* Nms
* fm-pm
* Swm

No que diz respeito aos direitos, faz-se uma distinção entre: ler, escrever, executar. Com base na função, os direitos para vários grupos funcionais (referidos na especificação como "namspace") são então definidos. O papel "sudo" tem mais privilégios. Destina-se a ser uma função administrativa e, assim, permite o acesso total à O-RU, incluindo a possibilidade de criar usuários e atribuir funções a eles.

Em relação à especificação atual, não é considerado tão favorável que um usuário padrão com senha padrão e direitos "sudo" esteja previsto no estado de entrega. Na literatura, é repetidamente relatado que esses acessos padrão são o ponto de partida para ataques bem-sucedidos — não importa o quão urgentemente um usuário seja instruído a alterar os dados de acesso em relação ao usuário padrão no curso da configuração inicial. Dern. Devem ser fornecidos mecanismos aqui que permitam uma configuração inicial mesmo sem um nome de usuário padrão e senha conhecidos, por exemplo, gerando esses dados aleatoriamente e anexando-os como documentação da O-RU.

**O-RAN Pior Caso/3GPP-Pior Caso*(ww*):** Assumindo que as medidas de segurança O-RAN também são obrigatórias no pior cenário, os objetivos de proteção resultam em confidencialidade, integridade e responsabilização de todas as partes interessadas no que diz respeito à abordagem "usuário" e "outsider" um baixo risco. No entanto, devido às formulações claras e à incerteza associada sobre se as medidas de segurança O-RAN realmente devem ser implementadas, há uma desvalorização para um meio Risco. A disponibilidade também é considerada um risco médio, uma vez que os ataques de disponibilidade na interface Open Fronthaul M-Plane são possíveis, como já descrito com as outras interfaces. Uma vez que não foram encontradas declarações explícitas sobre a tolerância de uma falha da interface em relação à interface Open Fronthaul M-Plane, também é assumido no que diz respeito à interface Open Fronthaul M-Plane que habilmente realizouataques de disponibilidadeprejudicam a qualidade do serviço RAN pode liderar.

Em relação ao atacante "Insider", a situação é um pouco diferente. Um insider com acesso à interface Open Fronthaul M-Plane pode instalar o software nos componentes O-RU

, que por sua vez lhe dá acesso aos dados do Plano de Controle e Plano de Controle do Usuário transmitidos através da interface Uu. Como estes não estão mais protegidos no pior cenário, isso resultaem um acesso quantitativo completo a essesdados, que se manifesta em uma avaliação correspondente como um alto risco para todas as partes interessadas. Apenas a integridade dos dados do plano de controle trocados entre UE e AMF não é afetada, pois são obrigatoriamente garantidas à integridade, o que significa que há uma baixa O risco prevalece. No entanto, presume-se que mesmo em O-RU do ponto de vista telco, dados sensíveis (gerenciamento de rede) (no que diz respeito à confidencialidade, integridade eimputabilidade) estão disponíveis aos quais um insider tem acesso. Nesse sentido, assume-se um risco médio em geral.

**O-RAN Pior Caso/3GPP-Best-Case*(wb):***  Neste caso, a avaliação é semelhante ao pior caso/pior cenário. As melhorias resultam dos dados do usuário e do plano de controle agora protegidos através das medidas 3GPP. Como resultado, um "insider" não pode quebrar a confidencialidade ou integridade dos dados do plano de controle, o que significa que o risco também é avaliado como médio global. Ainda em relação aos dados do avião do usuário, presume-se que eles estão protegidos, uma vez que, como insiders aqui, o O-RU ou O-DU são assumidos, ambos os quais não têm acesso às chaves criptográficas que são usadas para proteger o User-Plane.

**O-RAN Best Case/3GPP**  Best Case***(bb):*** As avaliações sobre os atacantes

"Forasteiros" e "usuários" seguem da avaliação de risco já muito positiva no pior cenário. No caso de um insider atacante, ele tem acesso à interface Uu, mas os dados (como já explicado) são protegidos na melhor das hipóteses pelas medidas P 3GP,pelas quais o risco de violação dos objetivos de proteção de confidencialidade, integridade e responsabilização é classificado como baixo.

**O-RAN-Best-Case/3GPP-Worst-Case**  ***(bw):*** Em relação aos  atacantes "usuário" e

Para"forasteiros", as medidas de segurança O-RAN evitam ataques bem-sucedidos à confidencialidade, integridade, responsabilidade e privacidade dos dados do usuário e do plano de controle. Nesse sentido, isso resulta em um baixo risco. Em relação ao invasor "insider", que tem acesso à O-RU, um grande risco surge devido à proteção inexistente dos dados do avião do usuário. Com o operador de rede, o risco de confidencialidade é o mesmo, pelo qual a integridade é novamente garantida pelo backup obrigatório nos dados defaixa do Controle P entre a UE e a AMF, mas não os dados de gestão no ==Referências== O-DU.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Risikoanalyse Open Fronthaul CUS-Plane

Os dados do plano de usuário e controle da interface Uu são transmitidos através da interface OPEN Fronthaul CUS-Plane. Além disso, ocorre a sincronização de tempo entre O-DU e O-RU. Requisitos de segurança: não há *requisitos* [30] explicitamente *não* previstos para esta interface. Por um lado, isso se justifica pelo fato de que os altos requisitos de tempo de atraso e largura de banda não permitem proteção, por outro, presume-seque os dados transmitidos já estão protegidos pelas medidas de segurança previstas nas normas 3GPP.

Devido às medidas de segurança infundadas, as considerações de pior caso/melhor caso da O-RAN não diferem. Essenciais para o risco são, portanto, as medidas de segurança 3GPP (ver também anexo A). Portanto, apenas a distinção entre 3GPP-best-case/3GPP-worst-case é feita abaixo.

**3GPP**  pior caso **(ww):** O acessof à interface Open Fronthaul CUS-Plane permite a um invasor manipulação acesso total ao usuário desprotegido e controlar dados de plano da interface Uu. A este respeito, há um alto risco para o atacante "forasteiro" e todas as partes interessadas. Somente para os dados do Plano de Controle pode ser assumido um menor risco em termos de integridade devido à proteção de ponta a ponta entre a UE e a AMF. No entanto, isso não afeta violações da integridade dos dados de gerenciamento específicos do O-RAN e, em particular, dos dados de sincronização temporal muito importantes (ver também o Capítulo 2.3.6.3).

**3GPP Best**  **Case** **(*bb*):** Para a perspectiva do "usuário", a situação melhora no melhor caso em relação às metas de proteção de confidencialidade, integridade e responsabilização, uma vez que neste caso a interface Uu é protegida por medidas de segurança 3GPP É. No caso da imputabilidade, o risco é avaliado como médio, uma vez que o 3GPP não prevê nenhuma medida de proteção em relação à atribuição e um usuário (comparado ao atacante "forasteiro") pode importar mensagens de avião do usuário para o sistema que são reconhecidos como corretos em termos de testes de integridade. tornar.

Os ataques de disponibilidade na interface FRONTHAUL-Plane Open resultam em ataques de disponibilidade à usabilidade do sistema global 5G, razão pela qual um alto risco é assumido em termos de disponibilidade, mesmo na melhor das hipóteses.

Mesmo em relação ao invasor "insider", há um baixo risco de dados do avião do usuário transmitidos na interface Uu devido à proteção 3GPP, uma vez que as chaves simétricas usadas para proteção estão localizadas no O-CU.

Os dados do Plano de Controle trocados entre UE e AMF são protegidos pelo backup da melhor caixa do 3GPP, o que reduz o risco para o operador de rede. No entanto,mesmo no melhor caso do 3GPP, os dados de sincronização de tempo (S-PLANE) não são protegidos, de modo que haja pelo menos um risco médio em relação à meta de proteção "integridade".

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Interface CTIde análise derisco

A interface CTI é usada para reservar capacidades na rede de transporte, que é usada para o plano Open Fronthaul CUS. A razão para isso é que, especialmente no caso de uma rede de transporte compartilhada com outros serviços,há sempre recursossuficientes disponíveis para atender aos requisitos de alta largura de banda e atraso de tempo do plano OPEN Fronthaul CUS. Atualmente, presume-se que não seja fornecida uma reconfiguração dos próprios caminhos de rede (com a ajuda da interface CTI). A este respeito, os ataques ou o acesso à interface CTI não resultam em violações dos objetivos de proteção de confidencialidade, integridade, responsabilização e privacidade. Deve-se notar que, como

Os detalhes completos da Assinatura CTI *serão especificados em uma versão futuradeste* *spe cification*."[32]. Isso permite a implementação da integridade e da prestação de contas. A confidencialidade, por outro lado, não é dada. Por exemplo, um invasor pode ser capaz de obter informações sobre o gerenciamento de rede e estratégias de gerenciamento de rede, espionando ainterface CTI,que deve ser levada em conta, em particular, em relação ao stakeholder "Telco". Deve-se notar que a assinatura digital mencionada é opcional. Além disso, não está claro como o mecanismo funcionará na prática. Ocabeçalho CTI é um pouco que sinaliza se uma assinatura digital está sendo usada. Como essa parte em si não está protegida, ainda não está claro se a assinatura digital pretendida pode realmente ter um efeito protetor significativo.

Uma vez que a interface CTI tem o objetivo de garantir a disponibilidade do RAN 5G (especialmente no que diz respeito à interface Uu), os ataques de disponibilidade na própria interface CTI permitem ataques correspondentes na disponibilidade 5G RAN. Na pior das hipóteses, um alto risco é assumido em relação ao atacante "outsider" e a todas as partes interessadas. Devido à assinatura digital, pode parecer um pouco melhor na melhor das hipóteses. Uma vez que não está claro se o design atual da assinatura digital pode realmente ter um efeito protetor significativo, um risco médio é assumido — especialmente porque ataques que suprimem mensagens CTI são possíveis apesar das assinaturas digitais e do especi atual As fikações não levam em conta explicitamente uma falha da interface CTI.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Análise de risco de outras interfaces

As interfaces "outras" incluem, em particular, as interfaces para acessar/baixar "informações externas de enriquecimento", as interfaces AI/ML e a interface humano-máquina fornecida para SMO. No momento, o design exato dessas interfaces é em grande parte não especificado.

No que diz respeito ao acesso às "informações de enriquecimento", é desde que isso só ocorra por meio de conexões seguras. De qualquer forma, essa interface, bem como a interface AI/ML, representam um risco de segurança, pois os provedores não confiáveis das informações e dados associados podem influenciar decisões de gerenciamento e configuração de rApps/xApps. Isso permite pelo menos uma influência negativa na disponibilidade. Atualmente, não se presume que uma violação direta dos objetivos de proteção de confidencialidade, integridade e responsabilização em relação aos dados do Plano de Usuário e Plano de Controle do 3GPP seja possível.

No entanto, deve-se notar aqui que os dados fornecidos por fontes externas potencialmente não confiáveis também podem ser gerados de forma inteligente, de forma a possivelmente explorar lacunas de segurança existentes nos componentes de processamento (especialmente nos rApps/xApps) (palavra-chave: bufferoverflow etc.) e, portanto, controlar sobre os componentes de segurança existentes nos componentes de processamento (especialmente nos rApps/xApps) (palavra-chave: bufferoverflow etc.) e, portanto, controlar sobre o fluxo de segurança existente nos componentes de processamento (especialmente nos rApps/xApps) (palavra-chave: bufferoverflow etc.) e, portanto, controlar sobre o fluxo de segurança existente nos componentes de processamento (especialmente nos rApps/xApps) (palavra-chave: bufferoverflow etc.) e, portanto, controlar sobre o fluxo de segurança existente pegue os componentes afetados. Os efeitos disso dependem muito do componente comprometido e que direitos ele tem ou até que ponto aqui

mesmo uma extensão de direitos é possível. Em princípio, isso também pode resultar em um alto risco para as outras metas de proteção.

A interface humano-máquina é usada para influenciar (configuração, etc.) de componentes SMO por um humano. Os riscos específicos de segurança associados a isso dependem muito das possibilidades oferecidas por esta interface de usuário, que atualmente são essencialmente não especificadas. Se, por exemplo, permitir que atualizações de software sejam instaladas nos vários componentes O-RAN, é, em princípio, possível comprometer esses componentes O-RAN, o que consequentemente leva a riscos de segurança comparáveis, conforme descrito no Capítulo 5.1 em relação ao capítulo 5.1 em relação ao O "operador RAN" do atacante foi especificado.

## RApps de análise de risco

De acordo com a especificação, a interface R1 deve ser a única interface disponível para rApps. Nesse sentido, a análise de risco em relação à interface R1 é uma base essencial para a análise de risco dos rApps. Deve-se notar apenas aqui que as especificações geralmente se referem a restrições de acesso de rApps individuais em relação à interface R1 — como isso é implementado exatamente,quais direitose conceito de papel estão associados a ele e, em particular, quão finos são os possíveis direitos A gestão permite uma restrição de acesso à interface R1, ainda não está clara.

Além da interface R1, outraameaça surge do fato de que um determinado rApp deverá ser executado em um ambiente comum de hardware/execução, juntamente com outras funcionalidades rApps e SMO. Em particular, não há indícios nas especificaçõesde que uma separação rigorosa (física) é planejada em relação aosrApps. Nesse sentido, a separação e o isolamento insuficientes representam um possível ponto fraco. Isso é especialmente verdade, uma vez que uma abordagem planejada para a implementação de rApps é o uso de separação baseada em contêineres (por exemplo, com a ajuda de Kubernetes). Deve-se notar que o objetivo original de separar com a ajuda de contêineres não era necessariamente o isolamento dos exercícios de segurança, mas sim evitar dependências do ambiente de tempo de execução proporcionado pelo sistema operacional. Assim, os mecanismos de separação atualmente implementados e aplicados nas soluções atuais de contêineres são fracos. Nesse sentido, há o risco de que um rApp saia do isolamento e, assim, amplie os direitos concedidos a ele.

Do ponto de vista do "usuário" do invasor, é concebível realizar os chamados ataques de parser, que têm o objetivo de exercer influência no rApp através de dados de usuários manipulados inteligentemente, o que em casos extremos pode levar a um compromisso do rApp. No entanto, a base de dados (no sentido de formatos de mensagem) não é dada para uma avaliação de risco, razão pela qual apenas isso é apontado neste momento.

Além disso, a especificação não especifica as linguagens de programação a serem usadas para a implementação de um rApp. Em princípio, isso permite o uso de linguagens de programação bastante "inseguras",como C ouC++, onde a probabilidade de vulnerabilidades que podem ser exploradas por ataques (por exemplo, estouros de buffer) é significativamente maior do que com linguagens de programação "seguras", como rust. Como a comunicação dos rApps abaixoé um elemento de design essencial da arquiteturageral, um rApp malicioso poderia explorar erros de programação em outros rApps para obter o controle de um rApp vulnerável e, em seguida, realizar atividades maliciosas usando os direitos concedidos a esse rApp.

Em geral, deve-se notar que a análise de risco apresentada na tabela refere-se apenas aos próprios rApps e, portanto, ataques nos rApps ou rApps. no RAN com a ajuda das interfaces rApp e outras interfaces. Análises correspondentes podem ser encontradas nos capítulos das interfaces individuais (em particular no capítulo,

que lida com as outras interfaces.) . Isso explica o baixo risco de invasores "forasteiros" e "usuários", já que esses invasores devem atacar uma interface para comprometer um rApp ou injetar um rApp comprometido no sistema.

Por outrolado, o invasor "Insider" supostamente comprometeu um rApp. Devido aos mecanismos de segurança O-RAN incompletos ou apenas muito limitados, não há necessidade de uma distinção de caso mais aprofundada entre o caso ORAN-best-case e O-RAN no pior caso neste momento. Aliás, a avaliação de risco resulta da avaliação de risco da interface R1 em relação ao atacante "Insider".

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## XApps de análise de risco

Para a análise de risco em relação aos xApps, o mesmo se aplica aos rApps. A principal diferença aqui é que os xApps têm acesso às interfaces A1 e E2. Nesse sentido, as análises de risco relativas a essas interfaces formam a base da avaliação. Além disso, os xApps estão "mais próximos" das interfaces 3GPP (Xn, NG, X2, E1, F1) porque os xApps fazem parte da Unidade Central (CU). Se um xApp conseguirromper os(possivelmente) mecanismos de isolamento existentes, haveria um perigo mais imediato de acesso aos dados do Plano de Usuário 3GPP ou do Plano de Controle (em contraste com os rApps[14).](#_bookmark13) Se um maior risco de segurança geralmente pode ser derivado disso em comparação com os rApps depende do futuro, o design mais concreto das respectivas frameworks e interfaces, uma vez que os rApps têm a "vantagem" em relação aos xApps para contar com o O1- e interface O2. Presume-se conservadoramente que ambos os tipos de aplicativos têm o mesmo risco em relação aos objetivos desegurança.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

14 A análise de risco da O-RAN ALLIANCE descreve que ambos os tipos de aplicativos podem violar igualmente os objetivos de proteção. No entanto, não se explica como a Aliança O-RAN chegou a esta avaliação, razão pela qual isso só é mencionado aqui.

## Aprendizado de máquina de análise de risco

O aprendizado de máquina é outro elemento de design essencial da arquitetura O-RAN. Existem diferentes variantes de implementação no que diz respeito ao treinamento dos modelos associados. Algumas variantes fornecem treinamento dentro dos componentes O-RAN, pelos quais os dados externos devem ser acessados, além de valores medidos que vêm dos próprios componentes O-RAN.

Além das incertezas gerais resultantes do uso de machine learning (as decisões são baseadas em correlações, não em causas), do ponto de vista da segurança, há um problema particular que se sabe que inúmeros ataques afetam negativamente o modelo treinado com a ajuda de dados de entrada manipulados. O resultado é um modelo treinado, que geralmente fornece resultados errôneos em inferência (aplicação do modelo) ou — e este pode ser o maior risco para alguns casos de uso — em quase todos os casos fornece um resultado correto eapenas no Os atacantes podem determinar situações com um resultado defeituoso desejado pelo atacante.

Com base nas possibilidades de ataque descritas e na forma como o aprendizado de máquina deve ser usado em O-RAN de acordo com uma especificação atualizada — que ainda é bastante geral e não específica em termos de aprendizado de máquina em geral —há um risco médio em termos de disponibilidade, ou seja. um impacto negativo na qualidade do serviço. Dependendo de quais parâmetros estão especificamente incluídos no treinamento de um modelo, o risco já existe em relação a pessoas de fora, mas pelo menos em relação aos usuários legítimos de RAN.

Do ponto de vista do operador (Telcos), outro risco à segurança é que a confidencialidade do modelo treinado em si possa ser comprometida. A suposição é que os modelos treinados representam um ativo digno de proteção, ou seja, não devem se tornar conhecidos no sentido de um sigilo de dados. Na literatura, existem ataques correspondentes de "roubo de modelo" que podem permitir que um invasor use solicitações inteligentes ou influenciando inteligentemente o sistema, seja com base nas respostas. ou geralmente ser capaz de derivar os parâmetros do modelo com base nas reações do sistema ou pelo menos ser capaz de (fortemente) restringi-los em sua respectiva gama de valores. Se tais ataques são realmente viáveis com sucesso no caso do O-RAN depende, em grande medida, do cenário concreto de aplicação de um determinado modelo. Devido à ambiguidade existente atualmente, um risco médio para o telco é assumido aqui, pelo qual pessoas de fora também poderiam realizar ataques bem sucedidos aqui, mas pelo menos (presumivelmente) usuários legítimos de RAN.

Finalmente, noch é a possibilidade de ataques à confidencialidade de usuários ou usuários. Controle os dados do plano se esta entrada for para treinar o modelo. Aqui, também, são conhecidas as estratégias de ataque da literatura, que possibilitam tirar conclusões sobre os insumos utilizados para o treinamento com baseno modelo treinado. Se e com quais efeitos isso é possível no caso do O-RAN e quais riscos concretos de segurança resultam dele não podem ser avaliados significativamente com base nas especificações disponíveis atualmente.

No geral, à medida que o uso de aprendizado de máquina em O-RAN progride, é importante considerar os ataques listados acima, a fim de minimizar o risco de ataques bem-sucedidos sempre que possível.

## Análise de risco sumária O-RAN

A avaliação sumária dos riscos gerais de segurança associados à arquitetura O-RAN resulta dos riscos identificados para cada interface e componente e sua combinação de acordo com os requisitos estabelecidos no Capítulo 3.6

descreveu o procedimento "por segurança". Em relação ao insider atacante, supõe-se que o invasor tenha controle sobre o, o que permite assim ao invasor acesso às chaves criptográficas usadas para proteger o avião do usuário 3GPP.

Na tabela a seguir, algumas entradas são marcadas com um "+". Isso é para expressar que, ao avaliar o risco – especialmente com base em cenários concretos de ataque – os autores têm certeza de que as avaliações estão corretas.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Usuários finais | | | | | | | | | | Estado | | | | | | | | | | Transportador comum | | | | | | | | | |
| **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | | **Objetivos de proteção** | | | | | | | | | |
| **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | | **C** | | **Eu** | | **Um** | | **Z** | | **P** | |
| Exterior em pé |  | + |  | + | + | + |  | + |  |  |  | + |  | + | + | + |  | + |  |  |  | + |  |  | + | + |  |  |  |  |
| + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + |  |  |  |  |
| Utilizador |  | + |  | + | + | + |  | + |  |  |  | + |  | + | + | + |  | + |  |  |  | + |  |  | + | + |  |  |  |  |
| + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + |  |  |  |  |
| Insider | + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + |  |  |  |  |
| + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + | + | + |  |  |
| Operadores de Nuvem | + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + |  |  |  |  |
| + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + | + | + |  |  |
| CORREU  Operador | + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + |  |  |  |  |
| + | + | + | + | + | + | + | + |  |  | + | + | + | + | + | + | + | + |  |  |  | + |  |  | + | + | + | + |  |  |

# Resumo e perspectiva

As especificações O-RAN não são desenvolvidas atualmente de acordo com o paradigma "segurança/privacidade por design/padrão". A este respeito, não é de surpreender que o resultado tenha sido um sistema quecontém onze riscosde segurança. Com a preparação da análise de ameaças e riscos e uma primeira tentativa de definir mecanismos de segurança aplicáveis, as abordagens iniciais são evidentes de que a Aliança O-RANpoderia dedicar mais atenção ao temada segurança no futuro. Até que ponto isso realmente acontece continua a ser visto. De qualquer forma, a experiência mostrou que uma adição tardia de medidas de segurança leva a gastos muito altos ou a soluções inseguras ou, não normalmente, a ambos. Os desenvolvimentos das normas 3GPP são um bom exemplo disso. A área inicialmente negligenciada da segurança de TI inicialmente levou a um sistema inseguro. A tentativa de corrigir esses erros nas versões subsequentes da norma foi muito esforço e muitas vezes leva a soluções inseguras, especialmente devido aos requisitos de compatibilidade que devem ser observados. De fato, para muitas redes móveis públicas praticamente operadas, as questões de legado críticas à segurança também levam a incertezas nas modernas redes 5G. É importante evitar tal desenvolvimento na O-RAN. A este respeito, as especificações O-RAN devem ser revisadas com um foco de segurança muito mais forte antes que as primeiras aplicações produtivas do O-RAN ocorram.

No que diz respeito à viabilidade de soluções de segurança para minimização de riscos, estima-se atualmente que existam um grande número de medidas de segurança conhecidas que podem ser implementadas sem grande esforço e custos e que podem contribuir efetivamente para a minimização de riscosde ameaçasindividuais. No entanto, estima-se também que, para reduzir alguns riscos de segurança, alguns — se necessários, ainda que consideráveis — são necessários esforços para adaptar as especificações e implementar as medidas de segurança apropriadas.

Abaixo estão algumas sugestões para minimização de riscos.

## ERecomendações

### 3GPP

Como a implementação de um 3GPP-RAN, o O-RAN se beneficia diretamente de melhorias de segurança para as normas 3GPP. Por um lado, deve-se mencionar aqui que os muitos mecanismos de segurança opcionais devem ser obrigatórios. Além disso, um backup de ponta a ponta entre UE e núcleo 5G também deve ser introduzido no que diz respeito aos dados do plano do usuário, semelhante ao que é fornecido para os dados do plano de controle. Em geral, as normas 3GPP também devem ser desenvolvidas muito mais fortemente de acordo com o paradigma de "segurança/privacidade por design/padrão" — e, em particular, afastando-se do modelo de segurança do perímetro atualmente perseguido em direção aos princípios de segurança multi-lateral [15,](#_bookmark14)

ou seja, com pressupostos mínimos de confiança em todas as partes interessadas e componentes. Isso poderia reduzir consideravelmente os riscos de segurança atualmente possíveis representados por um RAN comprometido ou por um operador RAN não confiável, bem como por componentes RAN não confiáveis.

Em resumo, surgem as seguintes propostas:

* Introdução obrigatória de medidas de segurança opcionais
* Backup de ponta a ponta de dados de plano de usuário entre UE e núcleo 5G
* Maior consideração do paradigma "segurança/privacidade por design/padrão"
* Consideração dos princípios da segurança multilateral

15 Esse conceito também é conhecido pelo termo de marketing enganoso "zero trust".

### O-RAN

Uma das medidas mais importantes para reduzir os riscos de segurança O-RAN é uma implementação séria do paradigma "segurança/privacidade por design/padrão" levando em conta os princípios da segurança multilateral. Os processos envolvidos na elaboração das especificações O-RAN devem ser adaptados em conformidade, por exemplo, os especialistas em segurança devem ser consultados na elaboração das normas e considerações e avaliações de segurança devem se tornar parte obrigatória de cada especificação, como é o caso das RFCs do IETF, por exemplo [60], [61].

As medidas de segurança atualmente apenas opcionalmente previstas devem ser obrigatórias. Ao mesmo tempo, o suporte a protocolos de segurança desatualizados ou algoritmos criptográficos que podem ser considerados inseguros deve ser explicitamente excluído. Em particular, formulações claras e inequívocas sobre a aplicação obrigatória de medidas de segurança devem ser incluídas nas normas. Uma mera presença não é suficiente aqui. A especificação para a interface O1-O-DU, por exemplo, mostra que ela pode ser melhor feita.

Ao selecionar protocolos de segurança, deve-se tomar cuidado para garantir que eles mesmos ofereçamo menor número possível de ameaças e riscos àsegurança. Em vez de usar o SSH, o TLS deve ser usado para a segurança do transporte. Deve-se também ter em conta que os dados (incluindo programas) não são apenas protegidos durante a transmissão ("em trânsito"), mas também "em repouso", ou seja, no curso do armazenamento persistente. No mínimo, devem ser implementados os objetivos de proteção de confidencialidade, integridade, reversibilidade e disponibilidade.

Além disso, um conceito claro de direitos e papéis deve ser implementado em relação a todas as interfaces eem relação aos rApps/xApps. Os princípios habituais de segurança, como "menos privilégios", "precisam saber", etc. devem ser implementados. O pré-requisito para isso é que as interfaces sejam especificadas da forma mais especificamente possível (por exemplo, interfaces O2 e R1) e que os mecanismos básicos de segurança permitam o controle de acesso o mais fino possível. Isso se aplica, em particular, a interfaces que atualmente desempenham apenas um papel na interface, como as interfaces para "informações de enriquecimento" ou a "interface homem-máquina". Neste contexto, interfaces atualmente não seguras, como a interface OPEN Fronthaul CUS, também devem ser protegidas. Além disso, as interfaces devem ser projetadas de tal forma que ofereçam o mínimo possível de superfície de ataque "com design". Em particular, os ataques de disponibilidade nas interfaces devem ser levados em conta, pois os efeitos negativos não podem ser evitados simplesmente pela aplicação da segurança do transporte. Os protocolos e osistema geral devem, portanto, ser projetados de tal forma que os efeitos nocivos dos ataques de disponibilidade nas interfaces sejam limitados. Além de uma limitação funcional ao que é realmente necessário, isso também se aplica a decisões de design que influenciam o número de portas abertas, por exemplo. Para ter uma solução que possa ser configurada e monitorada da melhor forma possível do ponto de vista da gestão de segurança, deve haver o menor número possível de pontos de acesso ao serviço.

Em relação aosxApps/rApps, um conceito de forte separação e isolamento deve ser implementado para que o compromisso de um xApp/rApp não leve a um compromisso de outros componentes O-RAN ou outros aplicativos. Além disso, a comunicação entreos aplicativos deve sergarantida de ponta a ponta. ==Referências====Links externos== Existem diretrizes de implementação para aplicativos. Estes devem, por exemplo, prescrever o uso de linguagens de programação seguras.

Deve-se prestar atenção especial paraproteger a Nuvem O, ou seja, a infraestrutura de nuvem subjacente. Devem ser implementadas medidas que permitam o maior nível de segurança possível, mesmo no caso de operadores de nuvem não confiáveis. Em particular, a aceitação de operadores de nuvem confiáveis deve ser abstendo-se. Isso também inclui a consideração do potencial

componentes comprometidos da infraestrutura de nuvem. A este respeito, por um lado, a arquitetura O-RAN deve ser (re)projetada de tal forma que o menor número possível de efeitos negativos possa ocorrer. Por outro lado, devem ser feitas especificações aos componentes da infraestrutura em nuvem no sentido de requisitos de segurança. Também deve ser avaliado até que ponto as soluções padrão de nuvem atuais, como contêineres e suas implementações, como kubernetes, atendem aos requisitos de segurança em princípio. Deve ser investigado até que ponto os Ambientes de Execução Confiável (TEEs) são adequados para permitir uma operação O-RAN segura, mesmo no caso de nuvens não confiáveis e o uso de TEEs deve ser prescrito, se necessário.

A análise atual de risco e segurança mostrou que as normas 3GPP em conjunto com as especificações O-RAN resultam em uma complexidade que torna uma avaliação confiávelnão mais possívelapenas por "aparência afiada". Nesse sentido, uma verificação formal das especificações (e idealmente também das implementações) deve ser utilizada como elemento essencial para o desenvolvimento de sistemas seguros. Isso também deve ser feito no caso de O-RAN. A fim de manter o esforço resultante para a verificação formal dentro dos limites, propõe-se primeiro determinar a quantidade de funcionalidade mínima crítica e a partir disso a funcionalidade mínima necessária para a implementação e a funcionalidade mínima resultante componentes necessários e confiáveis. Estes devem entãoser submetidosa verificação formal. O sistema como um todo deve ser projetado de tal forma que o sistema em miniatura possa ser estendido por componentes que podem não ser confiáveis sem colocar em risco a operação segura em termos de funcionalidade mínima. Este procedimento pode, portanto, ser comparado, por exemplo, com os conceitos de um ambiente de execução baseado em microrregião (sistema operacional, etc.). Neste caso, também, componentes de software potencialmente não confiáveis podem ser integrados e, ao mesmo tempo, fazer possíveis declarações e garantias em relação à segurança. No geral, uma abordagem mais formal pode identificar riscos de segurança que normalmente não são detectados "apenas por um olhar aguçado" devido à complexidade das especificações.

Em resumo, as seguintes recomendações resultam:

* Implementar segurança/privacidade por design/padrão
* "zero confiança" / implementar segurança multi-lateral na verdade
* Exigir backup opcional para transportar camada
* Use a redação clara, evite ambiguidades para esclarecer o uso obrigatório de mecanismos de segurança
* Substitua o SSH2 por TLS
* Proibir protocolos desatualizados, algoritmos criptográficos inseguros
* Fazer backup de arquivos "em repouso" (criptografia, garantia de integridade)
* Defina conceito de direitos/funções claros no que diz respeito a interfaces e serviços
  + especialmente para interface R1 e E2 (rApps, xApps)
* Especificar claramente a interface O2 (gerenciamento de nuvem)
* Especificar claramente a interface R1
* Interface CUS Fronthaul aberta segura
* Limitar os efeitos do DoS nas interfaces
* Implementar design amigável ao firewall
  + Poucos pontos de acesso, poucos pontos finais do servidor
* Especificando a conexão de fontes de dados externas
* Especificar claramente o conceito de separação de xApps/rApps, pelo menos no que diz respeito aos requisitos
* Comunicação segura entre rApps
* xApps/rApps apenas com linguagens de programação seguras (Rust etc.)
* Fornecer medidas de segurança para proteger contra operadores de nuvem não confiáveis (TEEs, etc.)
* Prescrever mecanismos de segurança no que diz respeito ao O-Cloud, em particular tornando obrigatória a autenticação do usuário
* Preparar e realizar idealmente a verificação formal

# Quellenverzeichnis

1. X. Lin e N. Lee, "5G e Além dos Fundamentos e Padrões", *Springer eBook*  Collection, 2021, Acessado: Sep. 15 de 2021. [Online]. Disponível em: [http://wwwdb.dbod.de/login?url=https://doi.org/10.1007/978-3-030-58197-8](http://wwwdb.dbod.de/login?url=https%3A//doi.org/10.1007/978-3-030-58197-8)
2. 3GPP, "Estudo sobre nova tecnologia de acesso a rádio: arquitetura de acesso por rádio e interfaces", 3GPP, V14.0.0, Relatório Técnico TR 38.801, Abr. 2017.
3. U. Schulze, "Endlich offen: Kurz erklärt: Open RAN", *iX*, Bd. 2020, Não. 9, Heise, P. 120, Aug. 26 de 2020.
4. G. Brown, "O Papel do Controlador Inteligente RAN em Sistemas RAN Abertos". Heavy Reading White Paper produzido para a Sterlite Technologies Limited, outubro de 2020.
5. "A Aliança O-RAN e o Telecom Infra Project (TIP) alcançam novo nível de colaboração pararedes de acessoa rádio abertas", 25 de fevereiro de 2020. https://[www.businesswire.com/news/home/20200225005180/en/The-O-RAN-Alliance-](http://www.businesswire.com/news/home/20200225005180/en/The-O-RAN-Alliance-) e-o-Telecom-Infra-Project-TIP-Reach-New-Level-of-Collaboration-for-Open-Radio-Access-Netw orks (acessado sep. 17 de 2021).
6. 3GPP, "NG-RAN; Protocolo de Aplicação E1 (E1AP)", 3GPP, V16.6.0, Especificação Técnica TS 38.463, julho de 2021.
7. 3GPP, "NG-RAN; F1 Protocolo de Aplicação (F1AP)", 3GPP, V16.6.0, Especificação Técnica TS 38.473, julho de 2021.
8. 3GPP, "Aprimoramentos da arquitetura para controle e separação de plano de usuário de nós EPC", Projeto de Parceria de 3ª Geração (3GPP), Especificação Técnica (TS) 23.214, Dez. 2018.
9. 3GPP, "Arquitetura de sistema para o Sistema 5G (5GS)", Projeto de Parceria de 3ª Geração (3GPP), Especificação Técnica (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, março de 2021.

[11] R. R. Stewart, "Protocolo de Transmissão de Controle de Fluxo", Não. 4960. Editor rfc, setembro. 2007.

Acesso em: 03 de agosto de 2021. [Online]. Disponível em: https://rfc-editor.org/rfc/rfc4960.txt [12]3GPP, "NG-RAN; NG Application Protocol (NGAP)", Projeto de Parceria de 3ª Geração

(3GPP), Especificação Técnica (TS) 38.413, julho de 2021.

[13]3GPP, "Protocolo não-access-Stratum (NAS) para sistema 5G (5GS); Etapa 3", Projeto de Parceria de 3ª Geração (3GPP), Especificação Técnica (TS) 24.501, junho de 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- Arquitetura-Descrição-v05,00, julho de 2021.

[15] Mavenir, Inc., "Segurança em Open RAN". White Paper, Jan. 2021.

[16]3GPP, "Arquitetura de segurança e procedimentos para sistema 5G", 3GPP, V17.1.0, Especificação Técnica TS 33.501, março de 2021.

[17]3GPP, "Rede Universal de Acesso a Rádio Terrestre (E-UTRAN); Descrição da arquitetura", 3GPP, V16.0.0, Especificação Técnica TS 36.401, julho de 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. Arquitetura OAM v04.00, 2021.

[19]3GPP, "NR; NR e NG-RAN Descrição geral; Estágio 2", 3GPP, V16.6.0, Especificação Técnica TS 38.300, julho de 2021.

1. Paralelo Wireless, "Everything You Need To Know about Open RAN". E-Book, 2020. Acesso: 29 de julho de 2021. [Online]. Disponível em: https://[www.parallelwireless.com/wp-](http://www.parallelwireless.com/wp-) conteúdo/uploads/Parallel-Wireless-e-Book-Everything-You-Need-to-Know-about-Open-

CORREU.pdf

1. GSMA, "Diretrizes de Implementação 5G". E-book, março de 2019. Acessado: 29 de julho de 2021. [Online]. Disponível em: https://[www.gsma.com/futurenetworks/wp-](http://www.gsma.com/futurenetworks/wp-) conteúdo/uploads/2019/03/5G-Implementação-Guidelines\_v1\_nonconfidential-R2.pdf

[22]3GPP, "Compartilhamento de rede; Arquitetura e descrição funcional", 3GPP, V16.0.0, Especificação Técnica TS 23.251, julho de 2020.

[23] Deutsche Telekom, Orange, Telefónica, TIM e Vodafone, "Open RAN Technical Priorities under the Open RAN MoU". Documento para download. Acesso em: 27 de julho de 2021. [Online]. Disponível em: https://telecominfraproject.com/openran-mou-group/

[24] 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, Ago. 2020.

[25] 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, julho de 2021.

[26] 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, julho de 2021.

[27] O-RAN ALLIANCE e.V., "O-RAN Working Group 2 (Non-RT RIC e A1 interface WG); Interface A1: Aspectos e Princípios Gerais", O-RAN WG2: Ran Intelligent Controller e A1 Interface Workgroup, V02.02, Technical Specification O-RAN. O WG2. A1GAP-v02.03.01, junho de 2021.

[28] 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. O WG2. Non-RT-RIC-ARCH-TR-v01.01, março de 2021.

[29] O-RAN ALLIANCE e.V., "Near-Real-time RAN Intelligent Controller Architecture & E2 General Aspects and Principles", O-RAN WG3: Near-real-time RIC e E2 Interface Workgroup, V02.00, Technical Specification O-RAN. O WG3. E2GAP-v02.00, Ago. 2021.

[30] O-RAN ALLIANCE e.V., "Control, User and Synchronization Plane Specification", O-RAN WG4: Open Fronthaul Interfaces Workgroup, V07.00, Technical Specification O-RAN. O WG4. CUS.0-v07.00, julho de 2021.

[31] 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, julho de 2021.

[32] O-RAN ALLIANCE e.V., "Cooperative Transport Interface Transport Transport Control Plane Specification", O-RAN WG4: Open Fronthaul Interfaces Workgroup, V02.00, Technical Specification O-RAN. O WG4. CTI-TCP.0-v02,00, março de 2021.

[33] O-RAN ALLIANCE e.V., "O-RAN Use Cases and Deployment Scenarios; Rumo ao Open and Smart RAN", White Paper, Fev. 2020.

[34] O-RAN ALLIANCE e.V., "O-RAN Working Group 2; Descrição do fluxo de trabalho de IA/ML e requirements", O-RAN WG2: Controlador inteligente RAN não em tempo real e Grupo de Trabalho de Interface A1, V01.02, Relatório Técnico O-RAN. O WG2. AIML-v01.03.02, junho de 2021.

[35] O-RAN ALLIANCE e.V., "O-RAN Plano Mínimo Viável e Aceleração para comercialização", White Paper, junho de 2021. Acesso em: 28 de julho de 2021. [Online]. Disponível em:[https://www.o](http://www.o-ran.org/s/O-RAN-Minimum-Viable-Plan-and-Acceleration-)-[ran.org/s/O-RAN-Minimum-Viable-Plan-and-Acceleration-](http://www.o-ran.org/s/O-RAN-Minimum-Viable-Plan-and-Acceleration-) para comercialização-White-Paper-29-junho-2021.pdf

1. DIN ISO, "Risk Management – PerformanceLines (ISO 31000:2018)", DIN, Padrão Alemão DIN ISO 31000:2018-10, outubro. 2018.
2. ISO/IEC, "Tecnologia da informação — Técnicas de segurança — Gerenciamento de risco de segurança da informação", ISO/IEC, Terceira Edição, Padrão Internacional ISO/IEC 27005:2018, julho de 2018.
3. IEC, "Gestão de riscos – Técnicas de avaliação de risco", IEC, Edição 2.0, IEC 31010:2019, junho de 2019.
4. BSI, "BSI-Standard200-3 --- Análise de Risco com base em TI-Grundschutz", BSI, Versão 1.0, BSI-Standard200-3, Out. 2017.
5. ENISA, "ENISA Threat Landscape for 5G Networks --- Avaliação atualizada de ameaças para a quinta geração de redes de telecomunicações móveis (5G)", ENISA, Dez. 2020. [Online]. Disponível em: https://[www.enisa.europa.eu/publications/enisa-threat-landscape-report-](http://www.enisa.europa.eu/publications/enisa-threat-landscape-report-) para-5g-networks/at\_download/fullReport
6. ENISA, "ENISA Threat Landscape for 5G Networks --- Avaliação de ameaças para a quinta geração de redes de telecomunicações móveis (5G)", ENISA, Nov. 2019. [Online].

Disponível em: https://[www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-](http://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-) redes/at\_download/fullReport

1. NIS Cooperation Group, "Avaliação de risco coordenada pela UE sobre a segurança cibernética das redes 5G", Relatório, outubro. 2019. Acesso: 27 de julho de 2021. [Online]. Disponível em: https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-redes-segurança
2. NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures", CG Publication, Jan. 2020. Acessado: 27 de julho de 2021. [Online]. Disponível em: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
3. CISA, "ESTRATÉGIA CISA 5G --- garantir a segurança e a resiliência da infraestrutura 5G em nossa nação", Agência de Segurança Interna, Segurança Cibernética e Infraestrutura dos EUA, 2020. Acesso em: 27 de julho de 2021. [Online]. Disponível em: https://[www.cisa.gov/sites/default/files/publications/cisa\_5g\_strategy\_508.pdf](http://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf)
4. CISA, NSA e DNI, "POTENCIAIS VETORES DE AMEAÇA À INFRAESTRUTURA 5G",

2021. Acesso: Juli 27, 2021. [Online]. Disponível em: [https://w](http://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-)ww[.c](http://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-)i[sa.gov/sites/default/files/publications/potential-threat-vectors-5G-](http://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-) infrastructure\_508\_v2\_0%20%281%29.pdf

1. Presidente dos Estados Unidos, "NATIONAL STRATEGY TO SECURE 5G of the United States of America", março de 2020. Acessado: 27 de julho de 2021. [Online]. Disponível em: https://[www.hsdl.org/?view&did=835776](http://www.hsdl.org/?view&did=835776)
2. NTIA, "Estratégia Nacional para Garantir o Plano de Implementação do 5G", Janeiro 2021. Acessado em 27 de julho de 2021. [Online]. Disponível em: https://[www.ntia.gov/files/ntia/publications/2021-1](http://www.ntia.gov/files/ntia/publications/2021-1-) 12\_115445\_national\_strategy\_to\_secure\_5g\_implementation\_plan\_and\_annexes\_a\_f\_fi nal.pdf
3. NTIA, "Estratégia Nacional para Garantir a Implementação 5G Plan Apêndices". Acesso em: 27 de julho de 2021. [Online]. Disponível em: https://[www.ntia.gov/files/ntia/publications/5g\_ip\_appendices\_1-5.pdf](http://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, sfg. Modelo de Ameaça v02.00.01, julho de 2021.

[50] GSMA, "Mobile Telecommunications Security Landscape", março de 2021. Acessado: 29 de setembro de 2021. [Online]. Disponível em: https://[www.gsma.com/security/wp-](http://www.gsma.com/security/wp-) conteúdo/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, sfg. Segurança- Requisitos-Especificações-v01.00, julho de 2021.

[52] Red Hat, "State of Kubernetes Security Report", e-book, junho de 2021. Acessado: 27 de julho de 2021. [Online]. Disponível em: https://[www.redhat.com/en/resources/state-kubernetes-relatório](http://www.redhat.com/en/resources/state-kubernetes-) de segurança

[53] O-RAN ALLIANCE e.V., " Especificação de Interface ORAN O1 para O-DU", ORAN Open F1/W1/E1/X2/Xn interface Workgroup, V02.00, Technical Specification O-RAN. WG5.MP.0-v02.00, Ago. 2021.

[54] M. Wasserman, "Usando o Protocolo NETCONF sobre Secure Shell (SSH)", IETF, Padrão Padrão RFC 6242, junho de 2011.

[55] O-RAN ALLIANCE e.V., "Security Protocols Specifications", O-RAN SFG: Security Focus Group, V01.00.04, Technical Specification O-RAN. SFG, sfg. Especificações dos protocolos de segurança v01.00, Ago. 2020.

[56] Badra, A. Luchuk e J. Schoenwaelder, "Usando o Protocolo NETCONF sobre segurança de camada de transporte (TLS) com autenticação mútua X.509", IETF, Padrão Padrão Proposto RFC 7589, junho de 2015.

[57] O-RAN ALLIANCE e.V., "Interface A1: Protocolo de Transporte", O-RAN WG2: Controlador inteligente RAN não em tempo real e Grupo de Trabalho de Interface A1, V01.01, Especificação Técnica O-RAN. O WG2. A1TP-v01.01, março de 2021.

[58] O-RAN ALLIANCE e.V., "Non-RT RIC & A1 Interface: Use Cases and Requirements", O-RA N WG2: Controlador inteligente RAN não-em tempo real e grupo de trabalho de interface A1,

V04.00.03, Especificação Técnica O-RAN. O WG2. Use-Case-Requirements-v04.00.03, julho de 2021.

[59] O-RAN ALLIANCE e.V., "RAN Function Network Interface (NI)", O-RAN WG3: Quase em tempo real RIC e E2 Interface Workgroup, V01.00.00, TechnicalAtion ORAN-WG 3.E2SM-NI-v01.00.00, Jan. 2020.

[60] H. Flanagan e S. Ginoza, "Guia de Estilo RFC", IAB, RFC Informativo 7997, Sep. 2014. [61]E. Rescorla e B. Korver, "Diretrizes para escrever texto rfc sobre considerações de segurança",

Grupo de Trabalho de Rede, Práticas Atuais Recomendadas RFC 3552 / BCP 72, julho de 2003.

[62] 3GPP, especificação do "Protocolo de Convergência de Dados de Pacotes (PDCP)", 3GPP, V16.3.0, Especificação Técnica TS 38.323, março de 2021.

[63]3GPP, "Protocolo não-access-Stratum (NAS) para sistema 5G (5GS)", 3GPP, V17.3.1, Especificação Técnica TS 24.501, junho de 2021.

# Lista de abreviação

Projeto de Parceria de 3ª Geração 3GPP

5G 5ª geração

5G SD-RAN 5G Rede de acesso de rádio definida por software 5GC 5G Core

Gerenciamento de mobilidade 5GMM 5GS

Sistema 5GS 5G

Gerenciamento de sessão 5GSM 5GS

Inteligência Artificial de IA

Função de gerenciamento de acesso e mobilidade da AMF

Interface de programação de aplicativos de API

Despesas de Capital CapEx

Contrato de Licença de Contribuinte da CLA

Rede core CN

Cots Commercial (ou Componentes) off-the-shelf CP Control Plane

Interface de Transporte Cooperativo CTI

Unidade Centralizada de CU

Plano de controle centralizado da unidade CU-CP

Controle cups e separação do avião do usuário CUS-Plane Controle, Usuário, Plano de Sincronização CU-UP Plano Centralizado da Unidade

Serviços de gerenciamento de implantação do DMS

Compartilhamento dinâmico de espectro DSS

Unidade Distribuída DU

E2E de ponta a ponta

Modelo de serviço E2SM E2

eCPRI Aprimorado Common Public Radio Interface EDGETaxas de dados aprimoradas para evolução GSM

Informações sobre enriquecimento do EI

eNB Evolved Node B

Núcleo de pacote evoluído do EPC

E-UTRA Evoluiu umts acesso de rádio terrestre

Falha, configuração, contabilidade, desempenho, security FH Fronthaul

Gerenciamento de Falhas FM

FOCOM Federado O-Cloud Orquestração e Gerenciamento GERAN GSM EDGE Rede de Acesso de Rádio

gNB Next Generation Node B

Sistema global de satélites de navegação GNSS

Serviço de rádio de pacote geral GPRS

Sistema Global GSM para Comunicações Móveis

GtP-U GPRS Tunneling Protocol - Usuário

Frequência de rádio RF

Hardware HW

Identificador de ID

Instituto IEEE de Engenheiros Elétricos e Eletrônicos

IMS Serviços de Gerenciamento de Infraestrutura

Protocolo de Internet IP

Organização Internacional da ISO para padronização

Item de trabalho conjunto JWI

Inteligência Artificial de IA

Indicador de desempenho da chave do KPI

L1/L2/L3 Camada 1/2/3 no modelo OSI

Evolução de Longo Prazo LTE

Controle de acesso médio mac

Minimização MDT do Teste de Acionamento

ME Managed Element

Mimo Multi entrada/saída múltipla

Aprendizado de máquina ML

Balanceamento de carga de mobilidade da MLB

mMIMO Massive MIMO

Serviço de Gestão MnS

Rede núcleo multi-operadora MOCN

Instância de objeto gerenciado pelo MOI

Avião de gerenciamento de m-planeda rede de acesso derádio multi-operadores MORAN

Provedor de Serviços Gerenciados da MSP

Estrato de não acesso do NAS

Nas-MM NAS Gestão de Mobilidade

Quase-RT RIC quase em tempo real RAN Intelligent Controller NETCONF Network Configuration Protocol

Função de rede NF

Orquestrador de função de rede NFO

Protocolo de aplicação de próxima geração NG-AP

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 não-autônomo

Instância de sub-rede de fatia de rede NSSI

Operação, Administração e Manutenção da OAM

Nuvem O-Cloud O-RAN

Unidade Centralizada O-CU O-RAN

* 1. U-CP O-RAN Centralizado Plano de Controle de Unidade O-CU-UP O-RAN Centralizado Usuário
  2. Unidade distribuída U O-RAN

O-eNB O-RAN Evolved Node B

Plataforma de Automação de Rede Aberta ONAP

Fundação ONF Open Network

Open FH Open Fronthaul

Despesas Operacionais OpEx

Unidade de rádio O-RU O-RAN

Osa OpenAirInterface Software Allicance

Comunidade de Software OSC O-RAN

Sistema de suporte de operações oss

Protocolo de convergência de dados de pacotes PDCP

PDCP-C Protocolo de convergência de dados de pacotes - Controle PDCP-UProtocolo de Convergência de Dados de Pacotes - Unidade de Dados do Pacote PDU do Usuário

Camada Física PHY

Rede Móvel terrestre plmn

Gerenciamento de Desempenho da PM

Rede Física PNF Function

Canal de acesso aleatório do pacote PRACH

Bloqueio de Recursos Físicos PRB

Protocolo de tempo de precisão PTP

Qualidade de experiência qoE

Qualidade de serviço QoS

Rede de acesso por rádio RAN

Falha no estabelecimento de conexão RCEF RRC

RIA RAN Inteligência e Automação

Controlador inteligente RIC RAN

Controle de link de rádio RLC

Falha no link de rádio RLF

Controle de recursos de rádio RRC

Gerenciamento de recursos de rádio RRM

Unidade de rádio remota RRU

Requisitos do RSAC e Comitê de Arquitetura de Software RT Em Tempo Real

Unidade de Rádio RU

SA Autônomo

Interface baseada em serviço SBI

Protocolo de transmissão de controle de fluxo SCTP

Protocolo de adaptação de dados do serviço SDAP

SD-RAN Software-definido Rádio Access Network SFTP Secure File Transfer Protocol

Integrador de sistemas SI

Contrato de nível de serviço SLA

Função de gerenciamento de sessão SMF

Gestão e Orquestração de Serviços SMO

Rede de Auto-organização SON

Concha segura SSH

Identificador oculto de assinatura DA SUCI

Software SW

Ethernet Síncroníncrosa

Controle de Transporte TC

Duplex da Divisão de Tempo TDD

ID do ponto final do túnel TEID

TIM Telecom Italia Mobile

Projeto TIP Telecom Infra

Segurança da camada de transporte TLS

Gestão de Transportes TM

TN Transport Node

Comitê de Supervisão Técnica do TOC

Unidade de dados do pacote de transporte T-PDU

Unidade de Transporte TU

Protocolo de datagrama de usuário udp

Equipamentos de Usuário da UE

Função do avião de usuário UPF do sistema de telecomunicações móvel da UMTS

V2X Veículo-para-Tudo

unidade centralizada virtual vCU

unidade virtual distribuída vDU

VM Virtual Machine

Função de rede virtual VNF

vRAN Virtual Radio Access Network

WG Working Group (da Aliança O-RAN)

YANG Ainda outra próxima geração

# Apêndice A: Análise de risco RAN 3GPP 5G

O resumo a seguir de uma análise de risco em relação ao RAN padronizado pelo 3GPP baseia-se em uma avaliação das normas relevantes do 3GPP, bem como na inclusão das análises de ameaças e riscos existentes, bem como nas possibilidades de ataque conhecidas da literatura (científica). A compreensão dos riscos de segurança inerentes ao RAN e das possíveis contramedidas é essencial para melhor avaliar e entender os riscos associados ao O-RAN como uma implementação de RAN concreta.

De acordo com [62], [16], os dados de faixa P do usuárioda interface Uu são backup dentro da camada PDCP. Tanto a criptografia simétrica quanto a garantia de integridade simétrica (códigos de autenticação de mensagens) são usadas. Devido à garantia de integridade simétrica, o objetivo de proteção da atribuição não é implementado. As teclas simétricas utilizadas são conhecidas pelo gNB. Nãohá backup de ponta a ponta entre UE e núcleo 5G. A transmissão de dados de plano de usuário entre o núcleo gNB e o núcleo 5G através da interface NG-U é protegida com a ajuda do IPSec. No geral, deve-se notar que a proteção tanto do Uu als quanto da interfaceNG-U é opcional:*"A proteção de confidencialidade dos dados do usuário entre a UE e o gNB* *é opcional de usar. [...] A proteção de integridade dos dados do usuário entre a UE e o gNB é* *opcional* de *uso e* *não* *deve* *usar o NIA0."* [16].

A especificação de se um backup deve ser realizado é realizada no núcleo 5G, especificamente pelo SMF localmente responsável. Na melhor das hipóteses, presume-se que os mecanismos de segurança sejam ativados, enquanto a análise mais na pior das hipóteses pressupõeque a transmissão dos dados do avião do usuário não estácurada.

Semelhante ao Plano de Usuário, também são fornecidas medidas de segurança para o Plano de Controle em princípio [62], [16], [63]— pelo qual, também no que diz respeito ao Plano de Controle, as medidas de segurança relativas à confidencialidade são apenas opcionais: *"A sinalização nas de proteção de confidencialidade é* opcional de *uso."* [16]. A integridade dos dados do plano de controle éobrigatória: *"Todas as* *mensagens de sinalização NAS, exceto aquelas explicitamente listadas no TS 24.501* [63] *como exceções devem* *ser* *protegidas pela integridade* *com* *um* *algoritmo* *diferente* *do* *NIA-0,* *exceto* *para* chamadas *de emergência."* [16]. Os casos listados em [63] são os seguintes:

1. *para uma* *UE* *não autenticada* para *a* *qual* *é* permitido *o estabelecimento* de *serviços* *de* *emergência;*
2. *para um W-AGF* *agindo* *em nome* *de* *um FN-RG;* *e*
3. *para um W-AGF agindo* em *nome* *de* *um* *dispositivo N5GC.* [63]

Como resultado, os casos marginais em que não ocorre garantia de integridade são, por um lado, bem definidos e, por outro lado, casos marginais (por exemplo, chamada de emergência). Uma diferença significativa em relação à transmissão dos dados do avião do usuário é que as mensagens do plano de controle são transmitidas de ponta a ponta (em relação à UE e ao núcleo 5G). Isso reduz os riscos correspondentes de violações do objetivo de proteção de confidencialidade e integridade pelo RAN 5G.

A operação da nuvem atacante não é levada em conta nas análises de risco, pois a especificação 3GPP não fornece especificações concretas para a implementação de um RAN 5G. A este respeito, uma solução baseada em nuvem pode ser usada aqui, mas uma implementação monolítica livre de nuvens também pode ocorrer.

Em relação às seguintes análises, deve-se notar que elas representam o "melhor caso" do ponto de vista da segurança, na medida em que nem todos os cenários de ataque possíveis poderiam ser analisados em profundidade devido às restrições de tempo. As perguntas abertas aqui incluem:

* O RAN pode influenciar a escolha de mecanismos de segurança no que diz respeito ao controle da proteção do plano, de modo que ataques bem sucedidos por um RAN maliciosopodem ser possíveis apesar da segurança pretendida de ponta a ponta?
* Qual é o risco representado pelas interfaces de interceptação legais?

**Pior caso**: Com base nas declarações feitas acima, segue-se para o caso de que nenhuma medida de segurança (excetoproteção de integridade em relação ao Plano deControle) tenha sido implementada. A este respeito, o atacante é "forasteiro" e a perspectiva

"Usuário" significa um alto risco de violação dos objetivos de proteção de confidencialidade, integridade, atribuição e disponibilidade. O mesmo se aplica à perspectiva da operadora de rede. Devido ao alto risco para esses dois stakeholders, o stakeholder

"Estado" assumiu um alto risco. Apenas a integridade é a exceção aqui, o que significa que o risco é avaliado como baixo.

**Na melhor**  dashipóteses, a situação melhora aplicando as medidas de segurança planejadas. Para o atacante "outsider" e todas as perspectivas das partes interessadas, assume-se um baixo risco de violação das metas de proteção de confidencialidade, integridade e imputabilidade. Relacionado com o atacante

A única diferença entre "usuário" é que o risco de violação dos objetivos de proteção é considerado médio em termos de imputabilidade, uma vez que um usuário pode gerar mensagens "válidas" para as quais terceiros não podem determinar se seoriginam do usuário oudo RAN. No que diz respeito ao objetivo de proteção da disponibilidade, um risco médio é assumido tanto para o atacante "forasteiro" quanto para o "usuário" do invasor. Na literatura, as possibilidades de ataque "usuário" do invasor são descritas aqui, que são baseadas no invasor ganhando controle sobre um grande número de dispositivos (IoT) conectados ao RAN 5G e, em seguida, usá-los para um ataque de disponibilidade distribuída. (dDoS) no 5G-RAN. Em relação ao atacante "outsider", há indícios na literatura de que o envio inteligente de sinais de rádio pode prejudicar severamente a transmissão na interface Uu (ataques de interferência). Tanto o avião do usuário quanto o avião de controle são afetados pelos ataques de disponibilidade. Nesse sentido, supõe-se que tanto um usuário 5G quanto a operadora de rede 5G podem ser afetados, o que, consequentemente, também implica um risco médio para o "estado" do stakeholder.

Em relação ao invasor "OPERADOR RAN", um alto risco também é assumidona melhor das hipóteses para a perspectiva do usuário, uma vez que o RAN está cientedas chaves para garantir confidencialidade e integridade e na medida em que essas medidas de segurança não protegem contra um operador RAN malicioso. Aqui, o padrão 3GPP deve ser revisto para que o backup de ponta a ponta entre UE e núcleo 5G também seja possível para a transmissão de dados de avião do usuário. Em relação ao "operador de rede" do stakeholder, a situação é avaliada um pouco melhor, uma vez que pelo menos as mensagens do plano de controle são garantidas de ponta a ponta. Para todos os stakeholders, há um alto risco de disponibilidade, pois o funcionamento funcionalmente adequado do RAN é crucial para a disponibilidade de uma rede 5G.

O risco de um insider, ou seja, um componente comprometido, é avaliado de forma semelhante ao risco de um operador RAN não confiável. Se o invasor tiver acesso ao componente RAN 5G quegerencia as chaves para proteger acomunicação, o insider também pode atacar com sucesso as metas de proteção de confidencialidade, integridade e responsabilização em relação aos dados do plano do usuário. Ao mesmo tempo, pode restringir trivialmente a disponibilidade usando chaves incorretas para descriptografia. pode ser fornecido.

Para o objetivo de proteção da privacidade, foi assumido um baixo risco em relação aos atacantes "forasteiros" e "usuários", uma vez que o 3GPP prevê uma série de medidas para alcançar um Para evitar o rastreamento da UE. Deve-se notar aqui que ataques com a ajuda de

Não foram levadas em conta as "impressões digitais sem fio" da UE. Levando em conta esse tipo de ataque, um risco médio deve ser assumido. Uma vez que o risco de privacidade no caso dos atacantes "insiders" e "operadores RAN" não podem ser avaliados de forma confiável. No

São mencionadas possibilidades de ataque na literatura, mas são necessárias análises adicionais extensas aqui para poder chegar a uma avaliação bem fundamentada.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assaltante** | **Perspectiva (Stakeholders)** | | | | | | | | | | | | | | |
| Usuários finais | | | | | Estado | | | | | Transportador comum | | | | |
| **Objetivos de proteção** | | | | | **Objetivos de proteção** | | | | | **Objetivos de proteção** | | | | |
| **C** | **Eu** | **Um** | **Z** | **P** | **C** | **Eu** | **Um** | **Z** | **P** | **C** | **Eu** | **Um** | **Z** | **P** |
| Exterior em pé |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Utilizador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Insider |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Operadores de Nuvem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| CORREU  Operador |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |