Aija Makkonen

Investigation on Security Improvements for Open Radio Access Networks

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

07 September 2022

PREFACE

This thesis was an exciting journey into the world of telecommunications and industry standards and the definitions of product security requirements. The amount of available open information was larger than expected and the future areas to study is ever growing. This work gave me the background knowledge to the challenges telecommunication industry in the transformation of architecture solutions from bare metal to virtualized and AI/ML based solutions. As a side benefit, I not only got technical knowledge but also learned how organizations manage security topics and how employees are eager to learn more about security.

I want to thank my instructor in the case company for all the times we discussed about my thesis and the positive attitude which encourage me to balance throughout these challenging months. I want to thank my children who tolerated me when being occasionally absent-minded.

Espoo, 07/09/2022
Aija Makkonen

Abstract

Author:	Aija Makkonen
Title:	Investigation on Security Improvements for Open Radio Access Networks
Number of Pages:	40 pages + 6 appendices
Date:	07 September 2022
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services
Supervisors:	Kimmo Rekola, Security Lead Ville Jääskeläinen, Principal Lecturer

This thesis was a study on telecommunication industry security requirements and the management of these requirements though the product lifecycle. The target was to find improvement areas in the security technologies in the case company's portfolio and discuss and analyse these areas with the experts. The analysis of the security requirements and the adoption of these requirements gave confidence on the understanding how these are supported and implemented by the case company. This thesis did not include detailed study on security testing or verification, or security requirements virtualized environments. As a result, four security improvement recommendation areas are noted into this thesis, discussed with relevant organizations and the results recorded into this study.

URN:NBN:fi:amk-2022090719970

Keywords: RAN Security, 5G Security, O-RAN, Supply Chain, Telecommunications Standardization, Industry Standardization, Product Security

Contents

List of Abbreviations

1 Introduction 1

1.1 Case Company 1
1.2 Motivation and Research Problem 2

2 Theoretical Background 4

2.1 Network Standardization and Regulations 4
2.2 RAN Infrastructure and Management 7
2.3 Supply Chain 9
2.4 Cybersecurity Framework and Classification 10

3 Radio Access Network Security 13

3.1 Vulnerabilities and Threats 13
3.2 Resilience 15
3.3 RAN and Open RAN 15
3.4 Product Security 17

4 Security Framework 20

4.1 O-RAN Security 20
4.2 Secure Operation and Maintenance 23
4.3 Supply Chain Security 25
4.4 Zero Trust Architecture 29

5 Findings and Verification 31

6 Conclusions 37

References 39

Appendix 1: O-RAN Statement of compatibility with 3GPP
Appendix 2: ENISA Threat Landscape for 5G Access Networks
Appendix 3: 3GPP Vulnerability Scanning
Appendix 4: 3GPP Protection at the Transport Layer
Appendix 5: 3GPP: Network Product Software package integrity
Appendix 6: Overview of Security Mechanisms in IoT PLC

List of Abbreviations

2G	Second Generation (mobile network)
3G	Third Generation (mobile network)
3GPP	Third Generation Partnership Project
4G	Fourth Generation (mobile network)
5G	Fifth Generation (mobile network)
6G	Sixth Generation (mobile network)
AI	Artificial Intelligence
ANSI	American National Standards institute
BC	Block Chain
BCMS	Business Continuity Management Systems
BoL	Beginning of Life
CA	Certificate Authority
CIA	Confidentiality, Integrity, Availability
C-Plane	Control Plane (real-time signals controlling RU operation)
CPRI	Common Public Radio Interface
eCPRI	ethernet CPRI
CU	Central Unit
CUS-Plane	Control, User and Synchronization Plane
CSCRM	Cybersecurity Supply Chain Risk Management
DL	Distributed Ledger
DLT	Distributed Ledger Technology
DoS	Denial of Service
DU	Distributed Unit
E2E	End to End
ENISA	European Union Agency for Cybersecurity
EoL	End of Life
F2F	Face to Face
FTPES	File Transfer Protocol Explicit-mode Secure
ETSI	European Telecommunications Standards Institute
gNB	New Radio generation Node B
FH	Front Haul
HTTPS	Hypertext Transfer Protocol
HW	Hardware
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISA	International Society of Automation
ISO	International Standardization Organization
ITU	International Telecommunications Union

JSON/REST	JavaScript Object Notation/Representational State Transfer
M2M	Machine to Machine
MANO	Management and Network Orchestrator
ML	Machine Learning
M-Plane	Management Plane (non-real-time management of RU)
MoL	Middle of Life
NETCONF	Network Configuration Protocol
NIST	National Institute of Standards and Technology
NMS	Network Management System
N-RT	Non-Real Time
NSO	National Standards Organizations
O-CU	O-RAN Centralized Unit
O-DU	O-RAN Distributed Unit
O-RU	O-RAN Remote Unit
O-RAN	Open Radio Access Network Alliance
PDCP	Packet Data Convergence Protocol
PKI	Public Key Infrastructure
PLC	Product Life Cycle
RAN	Radio Access Network
RFC	Request for Comments
RFIC	Radio Frequency Integrated Circuit
RIC	RAN Intelligent Controller
RPC	Remote Procedure Call
SC	Supply Chain
SCAS	Security Assurance Specification
SCM	Supply Chain Management
SCS	Supply Chain Security
sFTP	Secure File Transfer Protocol
SMO	Service Management and Orchestration
S-Plane	Synchronization Plane (provides clock reference to RU)
SSH	Secure Shell
SSL	Secure Socket Layer
SW	Software
THz	TeraHertz
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TVRA	Threat, Vulnerability and Risk Assessment
UE	User Equipment
U-Plane	User Plane (transport for IQ data carrying RF signal to/from RU)
V2V	Vehicle to Vehicle
VLC	Visible Light Communication
WG	Work Group
ZTA	Zero Trust Architecture

1 Introduction

This thesis gives an overview of the telecommunications and supply chain standardization, and how cyber security is included in the recommendations. The standards are mapped to the case company's security monitoring and security improvement features. Target is to identify missing standardization or regulations which are required to keep the End to End (E2E) network environment secure.

1.1 Case Company

The case company for which this study has been done is a telecommunications company, operating worldwide in 130 countries and a partner for critical communication networks for service providers, industries, and public sector. Looking into the future, the company provides its customers a value shift from bare metal E2E solution to cloud environment with new business models. For product and solution security the company has a wide portfolio of telecommunication security products, including consulting services.

Ensuring sustainability, safety, and security of the products and the environments where the products are used, is one of the key aspects in building a trustful partnership. Telecommunication industry is going through a change in automation and digitalization which raises the importance of security, as new ways for attacks and breaches occur. The case company participates actively in standardization, which is one key driver for providing reliable and interoperable networks even when operating with open interfaces.

Cloudification and virtualization of the human, machine and device communications changes the architecture framework of networks. Service providers must be prepared to support in parallel several technologies and device manufacturers in the common network, even interworking with old technology. The security services must be able to protect the valuable assets in the network by keeping expected network performance, cost efficiency and sustainability.

1.2 Motivation and Research Problem

Security attacks are an increasing threat in the network, while the features offering in telecommunications must keep the network secure. The company portfolio includes technologies to monitor, report and defend the network security by a selection of managed security technologies and operations. The objective in this thesis is to investigate the existing network security technologies and services and identify missing ones and suggest these into the requirements portfolio. This research aims to answer the question: “what emerging security functionality is missing from the current security offering and should be added into the case company portfolio?”

The thesis study steps are illustrated in Figure 1. First it investigates the security standardization status and Radio Access Network (RAN) security concept theoretical background and adaptation. Next is a description of the network evolution and its challenges. Finally, the thesis question is answered and verified within the case company organization. It is important to solve this problem so the customer can properly manage the risks in the network and keep its privacy. This study does not include company confidential information or any information that may identify any customer specific information.

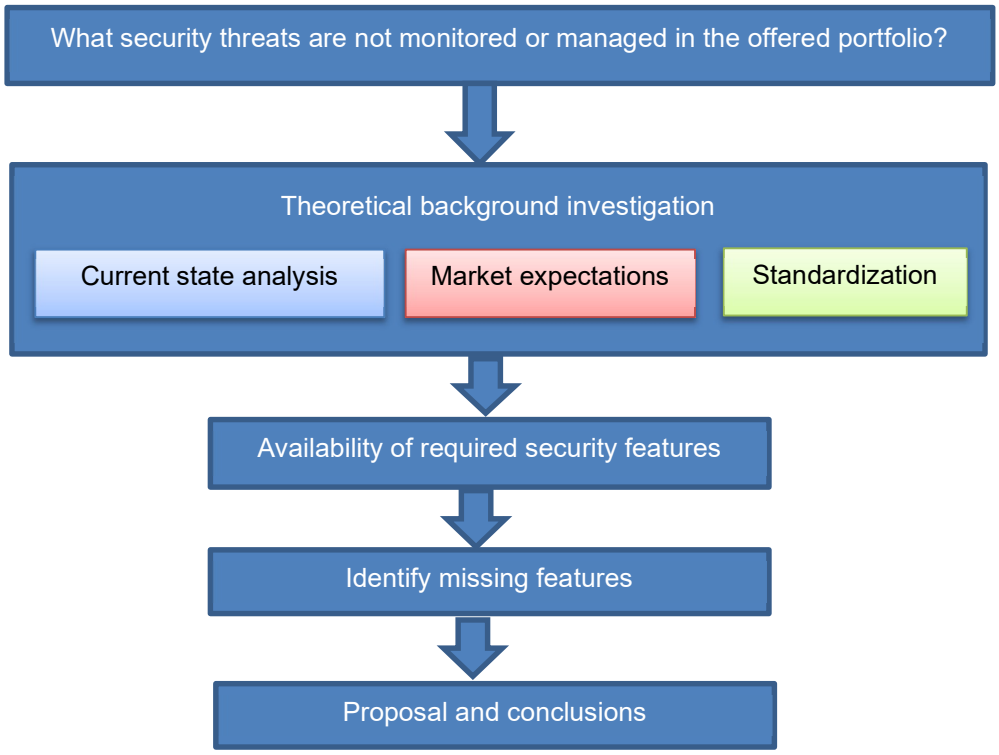

Figure 1 Research process

Notable is also that customer network monitoring environments may include monitoring tools from several providers, including customer's in-house built tools. Customers may also have fully or partly outsourced their network monitoring to a 3rd party company. As the Covid situation limited visits to labs and face to face (F2F) meetings, this thesis scope was limited to the available on-line information and study materials and remote discussions. This study includes a brief introduction to the standardization status and the security environment where mobile networks operate. There is a high need in standardization, regulations, and defined frameworks for network security. To limit the broadness of this study, security testing and verification were excluded from the study.

2 Theoretical Background

To deploy and orchestrate the telecommunication industry security environment there are market-driven cyber security standardization solutions and guidances for users, manufacturers, network infrastructure, operators, and regulators. This requires close co-operation between the stakeholders of connected domains, so the standards are properly developed, and this way increase the security of the system and its privacy.

This chapter gives an overview of the theoretical background, which is analyzed for this study. First, there is investigation of the standards and regulations which guides the architecture, procedures, and requirements for the systems, outlining specially security related areas. Next is a description of the network monitoring functions of current networks and evolution to open networks, and in the fourth chapter a description of the investigated security frameworks is provided.

2.1 Network Standardization and Regulations

To understand what security functionalities and technologies networks should implement, there are publicly available standards and recommendations, which guide the industry to develop and comply with the latest released industry lead standard specifications. Standards provide rules and/or guidelines to achieve order in a given context definition. Telecommunication networks must comply with a defined collection of standards, and telecommunication service providers and product manufacturers add the latest standards releases into their development packages, and this way provide compliance to their customers.

Table 1 lists the standardization organizations and alliances providing guidance to telecommunication industry and Radio Access Networks security standards. The list does not include cloud architecture security standards or standards for government information systems for cyber security.

Table 1 Telecommunications Industry Standardization Organizations

Organization	Overview of Telecom Industry Security Standards
ISO – International Organization for Standardization www.iso.org	ISO/IEC/IEEE 15288:2015 Systems and software engineering - System life cycle processes ISO 22301:2019 Security and Resilience – Business continuity management systems (BCMS) ISO 27000-series: Information Security Management Systems (ISMS) ISO 28000:2022 Security and resilience – Security management systems ISO 31000-series: Risk management ISO/TC 292 Supply chain security ISO/TC 307 Blockchain and distributed ledger technologies ISO 9000 -series: Quality Management Systems
ISA – International Society of Automation www.isa.org	ANSI/ISA-62443 framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs), e.g. 3-2 Security Risk Assessment, System Partitioning and Security Levels 3-3 System security requirements and security levels 4-1 Product Security Development Lifecycle (SDL) requirements 4-2 Security for industrial automation and control systems
ITU – International Telecommunication Union www.itu.int	United Nations specialized agency for ICT. Recommendations for defining how telecommunication networks operate and interwork. SG17 X.509 format of public key certificates for cryptography SG17 X.805 Security architecture for systems providing end-to-end communications Y.3172 architectural framework and requirements of ML in future networks
ANSI – American National Standards Institute www.ansi.org	Facilitates development of ANS by accrediting the procedures of standards developing organizations (SDOs) and proving their documents as ANS. Represents U.S interests in dialogues with key international markets.
IEEE - Institute of Electrical and Electronics Engineers www.ieee.org	802.11 Wireless LAN 802.1X-2020: “IEEE Standard for local and Metropolitan Area Networks – Port-Based Network Access Control 802.1x MAC authentication and authorization

Organization	Overview of Telecom Industry Security Standards
IETF - Internet Engineering Task Force www.ietf.org	RFCs for Internet standards, e.g..TLS, HTTPS and FTP protocols RFC 4252: SSH Authentication Protocol RFC 5280: certification path validation algorithm for CA issued PKIs
NIST – National Institute of Standards and Technology, U.S. Department of Commerce www.nist.gov	Develops cybersecurity standards, guidelines and best practices C-SCRM Cybersecurity Supply Chain Risk Management CSRC Computer Security Resource Center SP800-50 Building an Information Technology Security Awareness and Training Program SP800-150 Considerations for a Multidisciplinary Approach in the engineering of trustworthy secure systems SP800-207 for Zero Trust Architecture (ZTA)
ETSI – European Telecommunication Standard www.etsi.org	Regulations how to deploy and access networks, incl. Cybersecurity, Digital Signature, IoT, Lawful Interception (LI), Secure Elements, Quantum Key Distribution, Quantum-Safe Cryptography, Secure Elements, Securing AI, Security, Security Algorithms, etc. Subgroups to address system security ETSI NFV, ETSI NFV SEC, ETSI SAGE, ETSI TC CYBER
NSO – National Standards Organizations (ETSI partnerships)	European national standards and regulations, e.g. TRAFICOM – Finland (www.traficom.fi) NCSC-FI DKE – Germany (www.dke.de) BSI – United Kingdom (www.bsigroup.com)
3GPP - 3rd Generation Partnership Project for Mobile Broadband Standard www.3gpp.org	“33-series” collects security related specifications TS33.501 Security architecture and procedures for 5Gsystem “35-series”: Security algorithms related specifications Organizational partners: ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC
O-RAN Open Radio Access Network Alliance www.o-ran.org	Transforms the RAN towards Open, Intelligent, Virtualized and Fully Interoperable RAN WG4 Open Fronthaul Interfaces WG documents Management (M), User (U), Control (C) and Synchronization (S) plane security recommendations WG11 Security WG documents just started
QuestFORUM www.questforum.org	TL 9000 Quality management system. Supply chain directives for telecom industry (extension to ISO 9001:2015).

Organization	Overview of Telecom Industry Security Standards
	Includes Telecommunications Industry Association (TIA) www.tiaonline.org SCS 9001 Supply Chain Security Standard
COSO – Committee of Sponsoring Organizations of the Treadway Commission www.coso.org	Advisory group that designs frameworks to help organizations with risk management.
Common Criteria (CC) www.commoncriteriaportal.org	Common Criteria for Information Technology Security Evaluation List of some Certification Authorities and licensed laboratories for product evaluation

Standardization stakeholders have different levels of memberships and typically those are:

- **Full member** can influence standards development and strategy by participating and voting in meetings.

- **Correspondent member** observes the development by attending meetings as observers of the work.

- **Subscriber member** keeps up to date on standardization work but cannot participate in the work.

Standards ensure interconnection and interoperability in open markets where providers can mix and match equipment and services from different suppliers and where suppliers can benefit from economies of scale. Standards are referenced by regulators and legislators for protecting user and business interests, and in support of government policies. There is no one way to implement security, but best industry practices and standards should be used.

2.2 RAN Infrastructure and Management

Telecommunications networks are built, configured, and managed based on the network operator's business needs. Target is to keep the network up and running

without disruption, as any downtime or capacity reduction of the network means loss of connections and causes monetary loss, risks impacting the infrastructure and community health. Future evolution from a closed RAN infrastructure to an open infrastructure where there are several hardware (HW) providers requires a trusted and monitored environment to minimize security threats. 3GPP sets requirements e.g. for network products vulnerability scanning as in Appendix 3.

Based on the 2021 5G Cyber Security study by ENISA [1], network operators should consider strengthened access control, resilience, and monitoring capabilities. Technical specifications and standards make the foundation for the overall security and resilience of mobile networks and guarantee that the security requirements are known. These specifications must be properly followed in product supply, testing and deployment, as well as in operator's network configuration and operation. Essential here is that the security is functional, and its effectiveness is tested and assessed.

Figure 2 illustrates an example of the O-RAN Reference Architecture for network monitoring. In North-bound there is the Service Management and Network Orchestrator (MANO) and Non-Real Time RIC which manage e.g., the network SW and configurations.

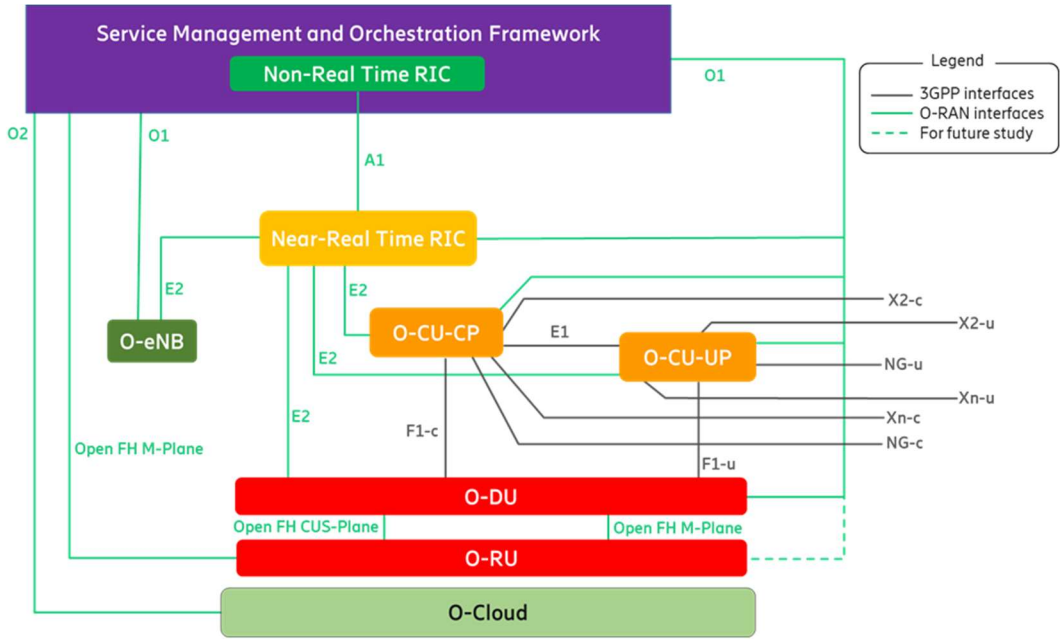

Figure 2 O-RAN Reference Architecture. [2]

The 5G RAN infrastructure is in most cases built on top of existing legacy RAN technologies, e.g., 2G, 3G or 4G, which provide an excellent basis for extending and improving the network efficiency. It is possible to upgrade existing infrastructure to 5G with a SW upgrade, but in some cases, it requires new 5G compatible HW to be installed on site. To manage and monitor the network behaviour, there are network monitoring products and services which can be used, and these can similarly be adapted to the new technologies. In many future networks existing concepts will extend to cover also 6G environments.

2.3 Supply Chain

When product hardware (HW) and software (SW) are developed, manufactured, and delivered, it goes through the supply chain. If an outsider can interrupt or access the chain, there is high risk of product contamination. HW is expected to last 20–30-year use in the field and the HW must be protected through its lifecycle. Attacks in the supply chain target to attack 3rd party products via network protocols, unprotected server infrastructures, and unsafe coding practices. Attackers break in, change source codes, and hide malware in build and update processes. Figure 3 shows the SC workflow with a four-layered traceability architecture, using a RFIC or bar-code as a product identifier.

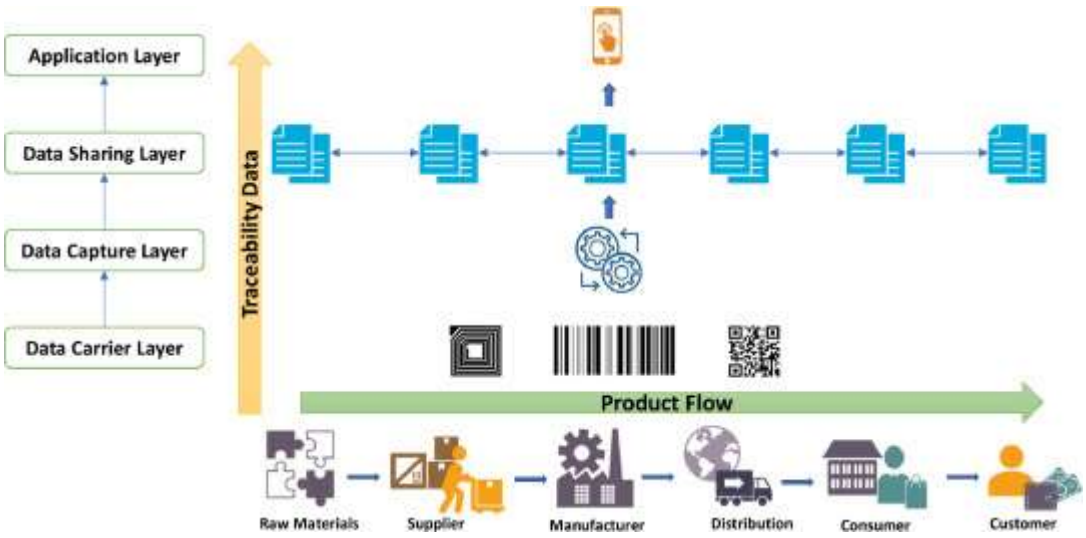

Figure 3 Four-layered Generic SC Traceability Architecture. [3]

SW development companies rely on processes which ensure the quality of the SW, starting from the early requirements planning, continuing to coding and testing of the SW. Many SW companies have moved from traditional waterfall development to agile fast integration cycle development, which is more flexible for fixing coding errors in security requirements.

During the past years we have seen geopolitical and pandemic influence into the supply chains. The target for SC orders should be digital transparency of the E2E orchestration and standardization and digitization of order creation and delivery. Industry should document and follow standards based on best practices, adopt security as part of operations lifecycle, ensure compliance across the SC, and include cybersecurity in operational risk management profiles [4].

2.4 Cybersecurity Framework and Classification

To support telecommunication industry to keep up with security requirements, NIST has published a Cyber Security Framework, and its categories are shown in Figure 4. The purpose of the framework is to protect the network from security attacks which aim to cause harm and damage the trust of the network environment. One challenging issue for most of the conducted studies is how to justify the results and select the correct way to protect the assets.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 4 NIST Framework Core's Functions and Categories. [5]

The NIST cybersecurity framework was originally published in 2014 for operators of critical infrastructure. In 2018 it was extended to include guidance for self-assessments and details on supply chain risk management, including a vulnerability disclosure process. The framework can be broken down into actions to be done before, during and after a security incident. Before actions are ways and procedures to identify possible vulnerabilities of the system or processes and how to report identified vulnerability risks in the system. Once the assets are known, protection of the assets can be planned by application security, recording, controlling, monitoring the assets so unwanted anomality can be detected. As part of protection there are e.g., policies, audits, asset classifications, and role assignments. Actions during the incident, or responding to the incident, can cover physical and controlled destroying, isolating, data protection or deleting the cause of the incident. Steps after the incident requires recovery which restores the information or services and collects learnings on how to further harden and improve security.

Risks classification can be divided into physical threats, breakdown, indirect and direct attacks, and insider threats as illustrated in Figure 5. All threats are not intentional and sometimes security may be broken due untested requirement or lack of knowledge.

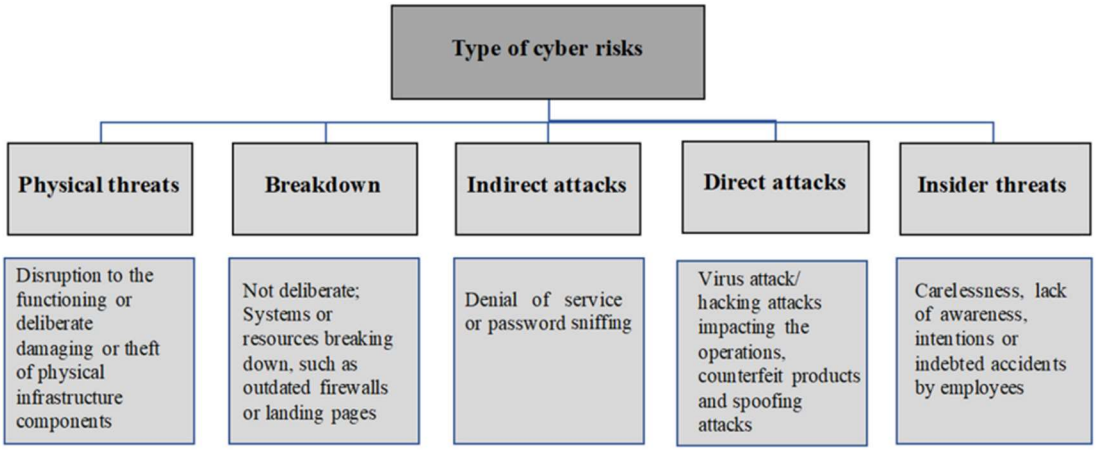

Figure 5 Classification of Cyber Risks. [4]

In the studied literature insider threat has been frequently brought up but least discussed or solved, probably due technical scope of the texts. Zero Trust Architecture addresses exactly this point. The above classified cyber risks should be planned and be prepared for, as those are possible to occur.

3 Radio Access Network Security

The previous section gave an insight to the generic security environments, this section first gives an overview on the current 5G RAN vulnerabilities and threats. 5G assets may include vulnerabilities that allow tampering in identity and access management, supply-chain poisoning, masquerade and bot attacks, loopholes in source codes. Machine learning (ML) in this context can help to provide heavily dynamic and robust security mechanisms for the software-centric architecture of 5G Networks. ML-based device authentication, and three-phase multidimensional attribute-based authentication mechanism employing supervised, unsupervised, and reinforcement-based learning is suggested [6]. To understand the RAN ecosystem the last section gives an introduction to the RAN systems and products.

3.1 Vulnerabilities and Threats

The ITU-T X.802 defined 5G security architecture provides best proven approaches for securing the existing and future E2E networks. Typically, it requires experimental work and evidence by research institutes and industry to find the best solutions before adding the recommendations into standards. RAN environment vulnerabilities and threats can be divided into:

- Architectural threats, including functions, interfaces, and protocols.
- Cloud threats, including cloud hardware and software infrastructure.
- Supply chain threats, including use of open-source software.
- Physical threats.

Figure 6 summarizes the threat landscape of the 5G network. User equipment (UE), on the left side of the figure, can be regarded as IoT devices, such as machine to machine (M2M) or vehicle to vehicle (V2V), and have risk of phishing, spoofing, signal jamming or Denial of Service (DoS). The Air Interface connects the devices to the network and exposes interfaces which are vulnerable for e.g.,

protocol manipulation, session hijacking or power manipulation. On the node B (gNB) side the interfaces or even the whole base station may be attacked by manipulating data which enables DoS, and connection or inter-operator handover failure, if security mechanisms are not adopted. More details on threats are listed in Appendix 2.

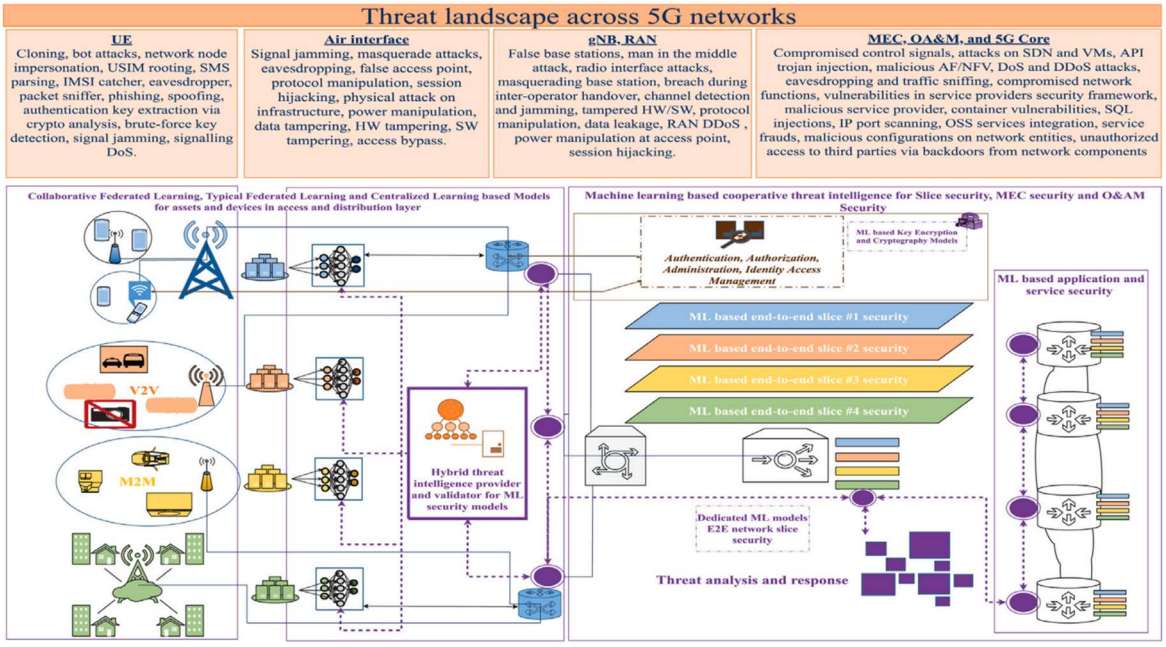

Figure 6 Threat landscape across 5G Networks. [6]

Figure 6 includes a proposal for a ML based E2E security architecture. The most critical part of the network is the core layer packet inspection due high-level virtualization and is therefore prone to zero-day supply-chain and compromised control signaling type attacks [5]. This is also the area where most powerful ML models are used to employ automated intelligence in 5G and beyond wireless networks. Real-time threat and anomaly detection out of terabytes of data requires efficient ML. Delivering this high amount of confidential data to a central controller raises the security and privacy risk as well as cost of power. It is useful to analyze the option of using de-centralized control.

To plan, manage and asses the threats and risks, organizations must create a security baseline; threat, vulnerability, and risk assessment (TVRA) for its assets and products and run security hardening activities to mitigate the risks. Each security risk must be

tested internally. To meet the potential risks with 3rd party components, those must be included as part of the E2E TVRA. An example use case for TVRA can output a list of requirements for IoT product lifetime security mechanisms which are listed in Appendix 6.

3.2 Resilience

Product resilience means that if one part of the product or network goes malfunctional the product or network operation can be kept running without any or with minimal effect to the services. ENISA study [1] expects secure product development is ensured and mandatory and optional security features are built-in, using a robust, mature, and secure product development process built with security and resilience in mind, e.g., source code review process, application of coding best practices, using of static and dynamic code analysis, and external code review process. Learnings from vulnerabilities must be taken into product planning and ensure resiliency and multilayer security e.g., in deployment of network elements in configuration phase or by using AI/ML.

Due importance of resiliency, it is part of supply chain security [4]. The human/behavioral elements within cyber security risk are found to be critical; however, behavioral risks have attracted less attention because of a perceived bias towards technical (data, application, and network) risks. There is a need for raising risk awareness, standardized policies, collaborative strategies, and empirical models for creating supply chain cyber-resilience. Good product configuration and SC resiliency reduce environment downtime and secure the expected capacity.

3.3 RAN and Open RAN

In traditional telecommunication networks there are gNB devices using vendor-proprietary protocols and interfaces. Open RAN will allow multi-vendor interfaces and infrastructure combinations for gNB units by introducing white box product approach. White box means openness and fair competition of the product and service integration to the operator network. At the same time, the benefits of innovation and supplier

diversity in an open ecosystem will bring forward additional diverse security solutions to address potential threats and mitigate risk because of the ability to monitor, detect, prevent, and respond more quickly [6]. Open networks means that more players are functioning in the same network. As networks are moving to be more open and virtualized, standards like O-RAN need to focus on security threats in defined components, interfaces and protocols specified by the O-RAN alliance [7].

In Figure 7 the high-level RAN architecture shows the O-RAN products and their connections via the logical planes. The SMO framework connects to the four key interfaces, namely, A1, O1, Open Fronthaul M-plane and O2. The architecture consists of one or more Radio Units (RU) which are connected to the Distributed Units (DUs) via the Fronthaul (FH) interface, both being managed from the SMO. The management functions via the FH interface are defined, but the O1 interface termination definition work is still ongoing. This study will not analyse the interfaces E2 and F1 for Centralized Unit Control Plane (CU-CP) and Centralized Unit User Plane (CU-UP) functions, which are defined also by the O-RAN standard.

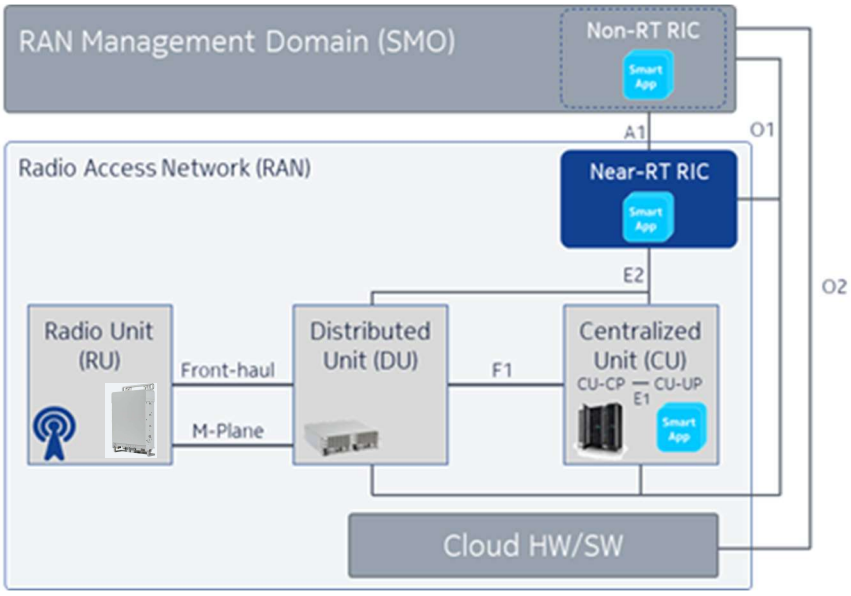

Figure 7 RAN High Level Architecture

The network is managed by the Management and Orchestration Domain (SMO), and two control domains, the Non-Realtime (RT) and Near-RT RIC, which are defined by O-RAN. The RIC platform is developed as Linux based open-source SW. The role of

he SMO domain is to take care of SON -like functions which includes anomaly detection and SW management. In this study the connection of a 3rd party RU to the proprietary RAN was investigated. Those suppliers who already support the CPRI/eCPRI standard based FH interface, have the benefit of reusing the existing SW code and functionalities, but must be adjusted to meet O-RAN requirements and ensure the integrated product is secured and compatible.

3.4 Product Security

Product has a lifecycle which can be simply divided into Beginning of Life (BoL), Middle of Life (MoL) and End of Life (EoL) as shown in Figure 8. There are tens of other ways to illustrate the life cycle, the timeline of each phase can last from months to years, and the product may never even reach the end of BoL due it is not produced. It is essential to secure the product through the supply chain and increase trust from bottom to top by ensuring the root of trust.

Figure 8 Product Lifecycle (PLC). [8]

Product HW and SW security requirements must be designed and maintained throughout the PLC with authentication keys, cryptograph, resiliency, sufficient monitoring, etc. The generic 3GPP user authentication and SW package integrity verification requirements are defined in [9], and the requirements for integrity validation in Appendix 5.

The studied literature had identified plenty of security threats and requirements for BoL and MoL phases, but EoL is usually forgotten. When the product is discontinued, the last stage will be commenced. Depending on the type of product and its possible

problems, EoL might be scheduled to recycle, refurbish, or dispose of the product [7]. The thesis discusses IoT device EoL security topics during the

- re-ownership phase, the device is sold to another person. As a result, all personal or secret information such should be erased or updated from it before handing over the device. One important secret information on all the devices to be updated are keys and/or certificates.
- decommissioned phase, the device is no longer operational and must be disposed of.
- removal, it is important to have all secret information such as private key and associated certificate revoked so that no information leaks from the system.

From an information and software development point of view, some generic attributes are commonly used to describe the actions associated with security: confidentiality, integrity, and availability (CIA) [10]. Confidentiality prevents unauthorized sources to access information and the used method can be e.g. encryption or access control. Integrity protects information from being altered and the protected information update and delete actions must be controlled and permitted only for authorized users. Integrity can be verified by cryptographic functions of hashing and can be used to ensure that digitally signed code has not been altered. Availability means the system is available for authorized users only, even in adverse circumstances.

Authentication assures the identity of the user and authorization allows the authenticated users to access the information. There is no one way to process authentication, but one method is to use an issued certificate for information access. The certificate is used to store a signed public key by the Certification Authority (CA) so that the end entity who has generated the private-public key, can demonstrate to whoever asks that she/he is in the possession of the private key for that public key which was signed/certified by a third trusted CA. The certificate is a digital file attached to a message for message originator verification. Credentials is a set of identity information and is defined by X.509 and includes certificate serial number, signature algorithm (hashing and digital signature algorithms used to digitally sign the certificate), CA issuer identificatory, validity dates, certificate owner, public key bound to the certified item and the algorithm to create the private/public key pair and intended use of this public key. The network product cannot boot from a memory device that is

not configured in its firmware, and access to the firmware is only possible with the correct authentication [9].

It is the purpose of the 3GPP Security Assurance Specification (SCAS) to identify security requirements from the 5G security architecture that require special attention in testing as they may:

(a) lead to vulnerabilities when not satisfied.

(b) not be captured through ordinary testing activity for non-security procedures.

(c) address security-relevant failure cases and exceptions or 'negative' requirements of the kind: "The network product shall not…".

O-RAN states its compatibility with 3GPP/SCAS security assets, threats, and requirements in the standards, see Appendix 1. O-RAN will have mixed product architecture by more than one supplier which sets requirements for high security level and resilience for the end products. The supplier must secure product development process and have security as a part of its product development and systematically assess and verify that these are applied. This includes software version control, secure software distribution, update and launching. It is expected every supplier meets the high-level quality with its products and SW and ability to manage security risks and notify of any detected vulnerability which may impact the use of the product as this may result in potential modification of product E2E settings and software configurations by attackers.

The zero-trust architecture is often mentioned in the literature and is gaining wide adoption and praise to prevent attacks by exploiting zero-day vulnerabilities. The zero-trust model, along with strong encryption techniques, can overcome some of the challenges [5]. The new technologies to develop are being introduced and can improve product security. More about Zero Trust Architecture (ZTA) in chapter 4.4.

4 Security Framework

This section gives an overview of the security frameworks which have been investigated for this study. It gives an overview on O-RAN security standardization, RAN security management and Supply chain security standardization for HW and SW production. Finally, a view on the zero-trust architecture (ZTA) and the future of RAN security is given.

4.1 O-RAN Security

Open RAN Policy Coalition is working with its collaborators to enable secure digitalization in 5G and supports industries in their transformation. The achievements are documented into the O-RAN released documents. For the interface security, there are agreed approaches which can be implemented, if not yet supported by the product vendor.

This chapter is divided into two interface plane security recommendations, the M-Plane and the CUS-Plane. There are three types of requirements [11]:

- **Mandatory**: The unit shall support the described capability to be O-RAN compliant.
- **Conditional Mandatory**: The unit shall support the described capability to be O-RAN compliant, but the additional information column describes the conditions under which the capability is mandatory.
- **Optional**: The unit need not support the capability and still be O-RAN compliant, but if the unit does support the described capability, it shall support it in the way described within the present document.

M-Plane standard [11] describes the capabilities required from O-DU and O-RU units and its role is to provide E2E security as a mandatory feature. The mandatory security protocols are Secure Shell (SSHv2) and Transport Layer Security (TLS), and as optional JSON/REST over Hypertext Transfer Protocol (HTTPS). File transfer uses secure File Transfer Protocol (sFTP) over SSH and File Transfer Protocol Explicit-mode Secure (FTPES) over TLS. These recommendations follow IETF standards.

Table 2 M-Plane Security [11].

Plane	Integrity (protection from modifications)	Confidentiality (encryption protection)	Authentication (validity of the originator)	Remarks
M-Plane/ NETCONF	Yes	Yes	Yes	NETCONF transport: a) Mandatory support for NETCONF/SSHv2, as specified in RFC 6242 [5] b) Mandatory support for NETCONF/TLS 1.2, as specified in RFC 7589 [41] c) Optional support for TLS 1.3, as specified in RFC 8446 [42]
Optional support of JSON/REST	Yes	Yes	Yes	HTTPS used for JSON/REST transport

Operators may select the authentication mechanism and protocol to use as shown in Table 3. TLS 1.2 is the mandatory protocol for authentication approach based on X.509 certificates. Transport security shall have aes128-ctr as the mandatory ciphering protocol. Further details are found in [11]. The 3GPP requirements for the protection of the transport layer with the pre-conditions and expected results of the requirement are described in Appendix 4.

Table 3 Mandatory and Optional Features for O-RU Authentication. [11]

Protocol	PKIX (Public Key Infrastructure with X.509 Certificates)	Simple Public Key	Password-based Authentication
TLS 1.2	Mandatory to support / Optional to use	Not specified in RFCs 5246/8446	Not specified for use with NETCONF
SSHv2	Optional to support/Optional to use	Used for SSH Server authentication by SSH client. Mandatory to support / Optional to use	Used for SSH Client authentication by SSH server. Mandatory to support / Optional to use

For the CUS-Plane the standard proposes to use the authentication and authorization defined by the IEEE 802.1x NAC [12] for all planes as optional. The definition work for the CUS-Plane protection work is still ongoing and will include the best practices. In addition, it is noted that all 3GPP messages transported via the Open FH U-Plane are protected by the Packet Data Convergence Protocol (PDCP).

Table 4 O-RAN Security requirements for CUS-Plane. [13]

Plane	Authentication and Authorization (at interface level)	Integrity (protection from packet modifications and injection)	Confidentiality (encryption protection)	Availability (including performance degradation)	Remarks
C-Plane	Optional to support IEEE 802.1x NAC [51]	Not currently specified	Not currently specified	Optional to support IEEE 802.1x NAC [51]	
U-Plane	Optional to support IEEE 802.1x NAC [51]	No additional protection mechanisms are specified	No additional protection mechanisms are specified	Optional to support IEEE 802.1x NAC [51]	3GPP Control Plane and User Plane messages that are transported via the Open Fronthaul U-Plane (LLS-UP) are confidentiality and integrity protected by the Packet Data Convergence Protocol (PDCP) [52].
S-Plane	Optional to support IEEE 802.1x NAC [51]	Not currently specified	Not currently specified	Optional Grand Master Clock redundancy [33]. Optional to support IEEE 802.1x NAC [51]	

Table 5 proposes additional optional security features for the O-DU and O-RU. As we can see, O-RAN partially relies on IEEE standardized approach, which is commonly recommended and supported by the producers and requires ~~no or~~ minimal changes into the infrastructure.

Table 5 O-RAN CUS-Plane additional optional features. [13]

Category	Feature of O-DU or O-RU	O-DU support	O-RU support	Additional information
Security	IEEE 802.1X [51]	Optional	Optional	
	Grand Master Clock Redundancy [33]	Optional	Optional	

Product SW download is initiated by Network Configuration protocol (NETCONF) remote procedure calls (RPCs) and supported by X.509 certificate for TLS authentication of FTPES client and FTPES server.

4.2 Secure Operation and Maintenance

As stated in earlier chapter 2.2, the future networks are based on existing network solutions. Potential technologies are predicted to serve as the foundation of next 6G networks. These include upcoming and current technologies such as post-quantum cryptography, Artificial Intelligence (AI), ML, enhanced edge computing, molecular communication, THz frequency bands, visible light communication (VLC) and distributed ledger technologies (DLT) such as block chain (BC). New novel authentication, encryption, access control, communication, and malicious activity detection must satisfy the higher significant requirements of future networks [14].

As the mobile networks will move from traditional bare metal RAN and fixed core network to virtualized and cloudified structure, it sets more demanding requirements for securing the distributed software components. Figure 9 shows a general 5G network architecture and related enabling technologies; RAN domain, core network (CN) domain, and cloud infrastructure domain.

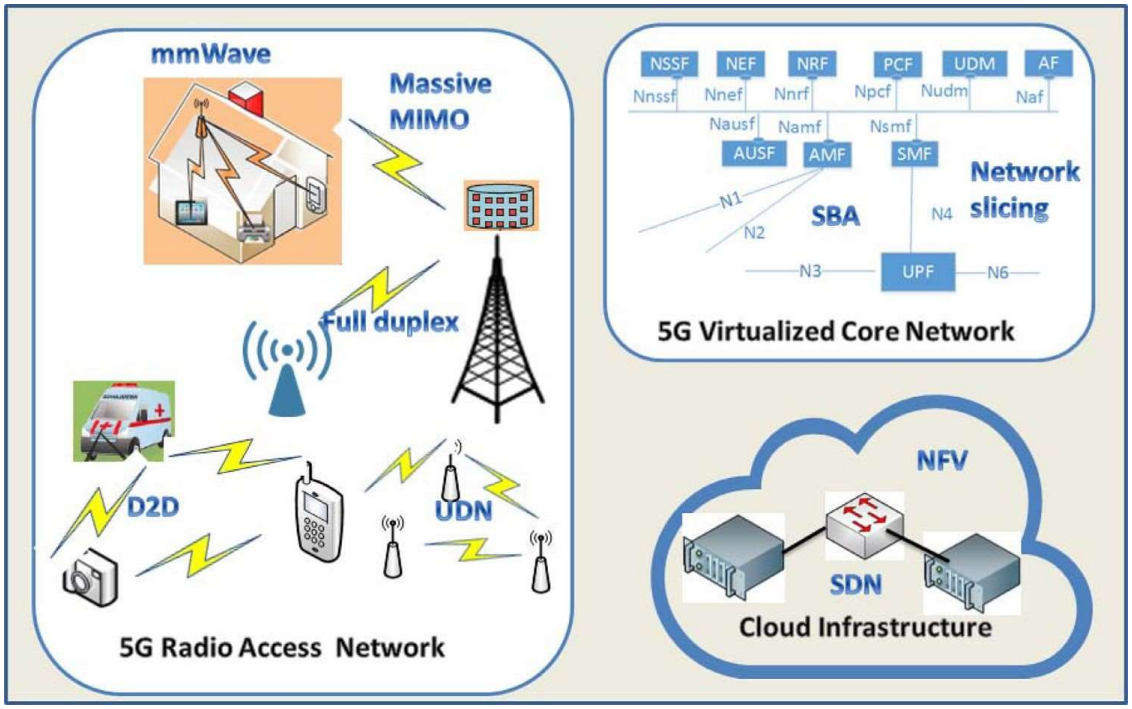

Figure 9 5G Structure and Key Components [15]

The network security operations should not reduce the network or service E2E latency and performance, so security actions should be designed to be fast and with minimum impact over the network and services. Some known 5G security threats to the three domains are [15]:

- Introduction of new RAN radio technologies, which target to improve spectrum and energy efficiency but on other hand can be misused by highly sophisticated eavesdropping.
- High number of new cost efficient and/or massive IoT devices have DoS and DDoS attack risk which impact the network. Attacks can be mitigated on the IoT application layer security and privacy.
- Mobile edge computing (MEC) enables operators and 3rd party to deploy services close to users and reduce E2E latency. Due high number of players MEC technology opens interfaces for malicious attacks and requires efficient user access control and encryption methods.
- Vertical service providers using an open network interface with 3rd parties which opens a new security risk through 3rd party applications. There should be a security business model which builds trust between the parties.
- Virtualization of network functions (e.g., NFV) which brings physical and virtual risks due decoupling HW and SW. Outside attackers can be protected with systems like firewalls and intrusion prevention systems. Infrastructure attacks can be detected by continuously monitoring the resource consumption and improving visibility into the network events and activities. E.g., attack to the routing loop would benefit of knowing the virtual network topology and the real-time resource redundancy.

As part of the 3rd party open interfaces, this study identifies need to ensure secure 3rd party product SW delivery and download, and it is expected that there is a certificate issued by a trusted certificate authority (CA) and PKI procedures are followed, as example in Figure 10. The CA is an organization that validates the identities of entities and bind them to cryptographic keys by issuing digital certificates. CA provides authentication, to validate the identity of the entity that it is issued to,

encryption for secure communication, and integrity check of signed files with the certificate.

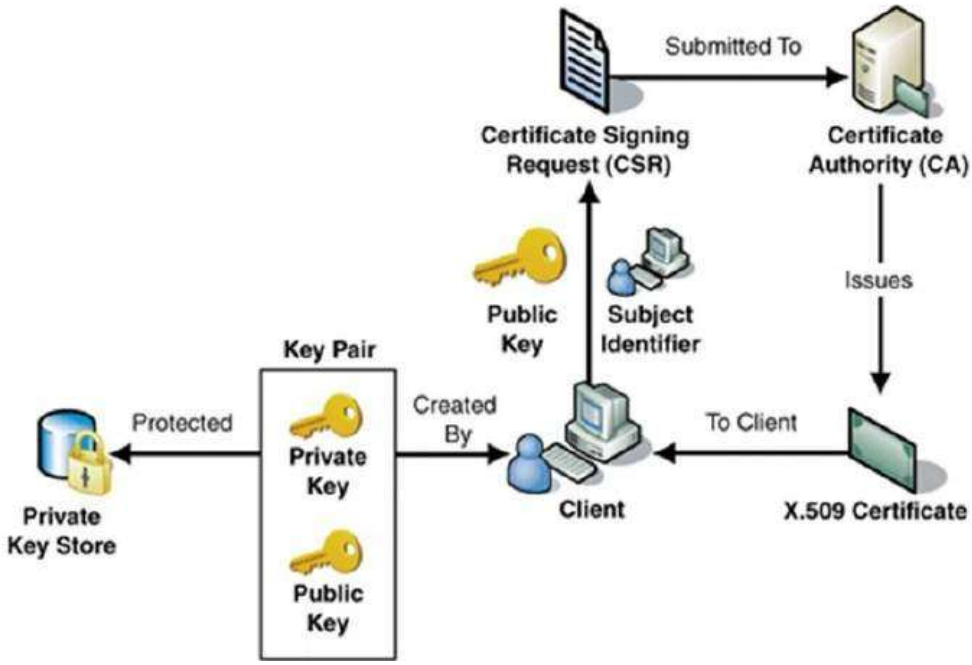

Figure 10 PKI Use Case Diagram. [16]

The use of Public Key Infrastructure (PKI) and certificate management security mechanisms is commonly used and a trusted way to bind certain identities with corresponding public/private static key pairs, which are used for cryptographic operations.

4.3 Supply Chain Security

Cyber supply chain risk management (CSCRM) defines the risk management in the E2E process for IT networks, HW and SW systems and combines product supply processes from cyber security, enterprise risk management and Supply Chain Management (SCM). The propagation of cyber consequences means companies cannot afford to focus only on their security systems but must also be aware of their partner's security conditions [4]. The risk increases specially if the parties share same IT systems to control the shared data which may be partly in the cloud, and the lack of accepted standards and guidelines is hindering the development of robust cyber defenses. The proposed SC cyber security concept in Figure 11 splits the SC sources

into IT security system (direct or indirect attack), Supply Chain security system (physical threat) and Organizational security system (insider threat). To reduce security risks and manage the SC cyber security system, all three sources need to be aligned and have closer collaboration, also between the suppliers and customers.

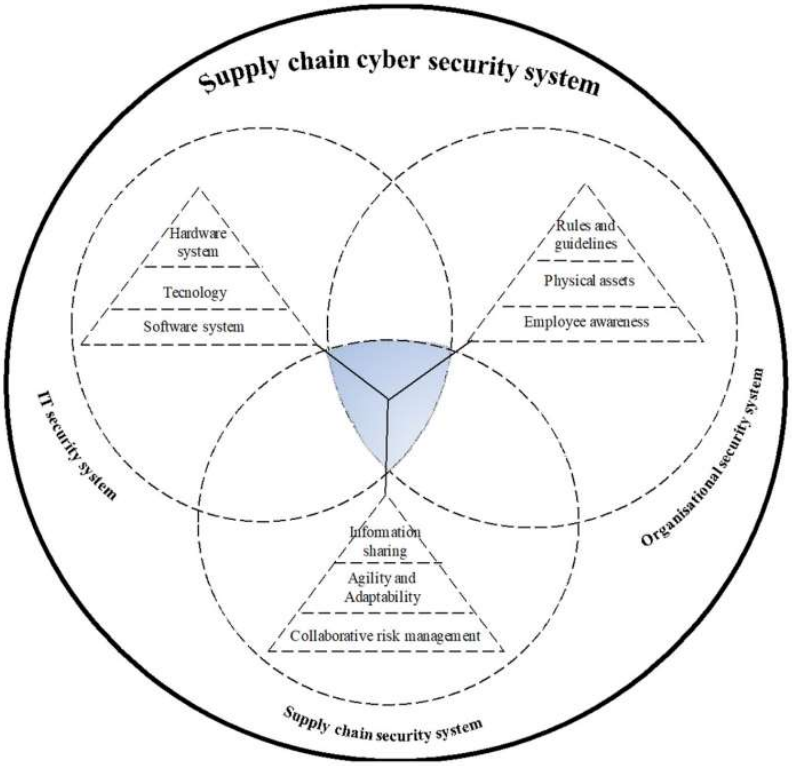

Figure 11 Conceptual model for Supply chain cybersecurity. [4]

As mentioned in Chapter 4.2, BC or DLT can be implemented to improve the execution of cryptographic transactions. According to [17] BC and DLT provide superior data integrity to mitigate cyber risks in the E2E SC, but there are not enough studies how SC should apply block chain technology. Possibility to combine block chain with SC risks management together with other digital technologies could improve the resilience and robustness of the SC. The authors refer also to new security solutions, such as: digital identity, authentication and access management, security platforms, privacy management, and DoS protection.

TL9000 standard expects risk management and production continuity, which can be based on ISO 22301 standard. Certification ensures the product and production is tested against compliance with the reference specification and the product is

authorized to carry a specific set of credentials that indicate that it is conformant. [17] proposes the use of BC to mitigate cyber risks of products, identity, credentials, and digital rights in E2E supply chains for IoT devices. For IoT the number of devices and users is much higher than in RAN products.

An example of the SW Supply chain complexity is shown in Figure 12. The SW suppliers over the lifecycle sets challenging requirements for security, e.g. improving security with audit of security policy compliance, fake SW chain recovery, and identifying hacks.

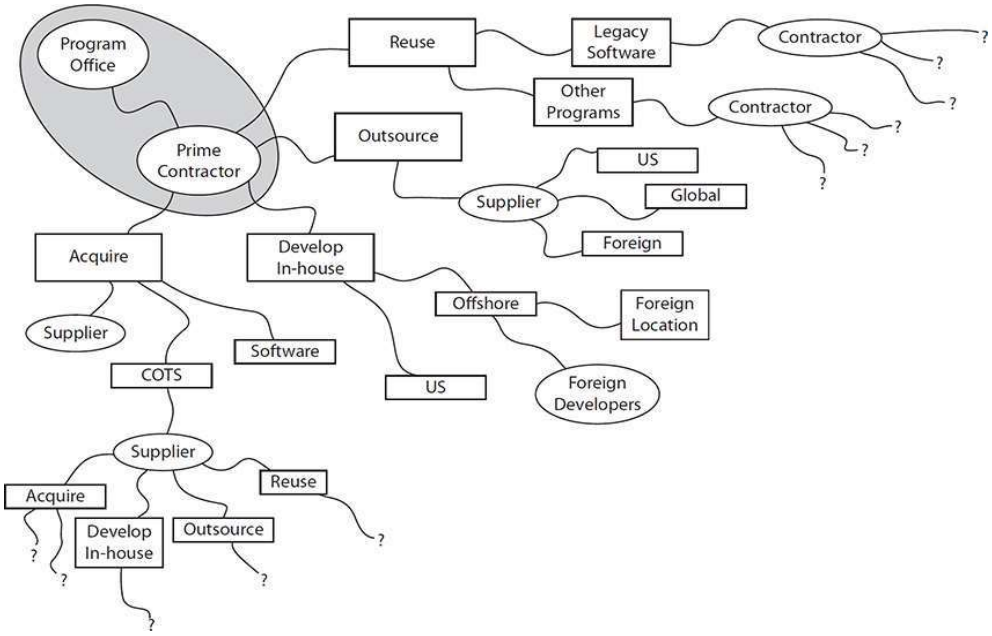

Figure 12 Complexity of the SW Supplier chain (ch19). [18]

To ensure high level of security and resilience for end-products, suppliers need to have a secure product development process and security by design as a basic principle, systematically and verifiably applied [1]. In the 5G networks, where most important elements will be SW based, the development process must take care of secure SW development, security assessment and testing, version control, secure software update and alike matters. This also includes systematic source code review process, application of coding best practices, using of static and dynamic code analysis, external code review process and individual product vulnerability scanning. Moreover,

due to the prominence of supply-chain risks for security of 5G networks, suppliers also need to have adequate measures in place to adequately manage such security risks.

Recommendations for SW code security improvements of 3rd party components' quality and availability e.g., by lowering the risk of integrating vulnerable, unavailable, or unsupported 3rd party components into network products [18]. To lower the risk and improve traceability: "During the entire lifetime of a Network Product, the Equipment Vendor shall utilize a version control system on hardware, source code, build tools and environment, binary software, 3rd party components and customer documentation ensuring accountability, authorization, and integrity of all changes." The diligent use and management of the components benefit also O-RAN 3rd party product accountability.

Even if security risks are minimized during SW development, there is still a threat of cyber-attack. DevOps is a SW development environment combining software developers (dev) and operations (ops) [19]. The methodology aims to integrate the work of software development and software operations teams by facilitating a culture of collaboration and shared responsibility. DevSecOps target is to ensure the teams have the knowledge of security and how the code is integrated. A study by [18] results in leveling the SW development into five levels, where the lower level is dependent on the upper level. Here we can see the importance of standards. Figure 13 shows the levels of DevSecOps knowledge areas levels from 1 to 5.

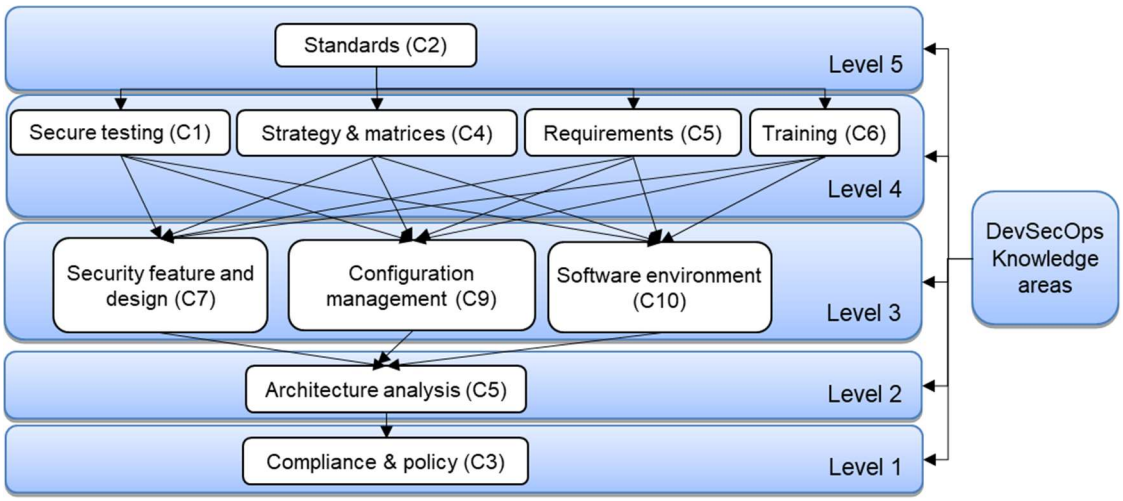

Figure 13 DevSecOps knowledge area levels. [18]

Despite the DevSecOps knowledge areas levels description was found at the end of the study, they surprisingly well match the intention of this thesis and gives confidence to the approach.

4.4 Zero Trust Architecture

3GPP security control is not specified in standards but NIST Special Publication SP 800-207 defines a Zero Trust Architecture (ZTA). ZTA is gaining wide adoption to prevent attacks by exploiting zero-day vulnerabilities and together with strong encryption techniques can overcome some of the challenges [6].

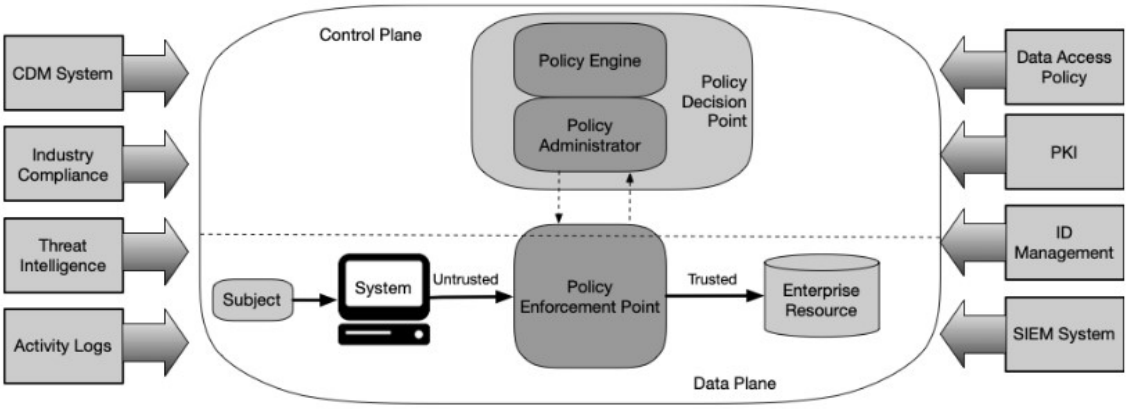

Figure 14 NIST ZTA Logical Components. [20]

Open RAN architecture has increasingly higher number of integrated open components. Digital transformation and migration to the cloud impacts security operations in a multi technology and open network. Here zero trust, “never trust always verify”, is a strategic concept that secures an organization by continuously validating every stage of digital interaction [21]. Organization should continuously test the network data to find problems. The principle is that anything that connects to a network should inherently not be trusted unless it can be verified. Zero trust networking can enhance security in a variety of ways [22]:

(1) Visibility and Critical Asset Identification.

(2) Users require strong authentication with multiple layers of authentication.

(3) Applications cannot be trusted and continuous monitoring at runtime is mandatory to validate their behavior by securing the technology, application and the application interfaces.

(4) HW Infrastructure must be addressed with a zero-trust approach.

5 Findings and Verification

This section provides the results of this thesis study. There are four findings which were seen important to be raised and are shown in

Figure 16. These four findings resulted into four proposals:

1. **Industry and technology supply chain security**

   The analysed material for this thesis shows that in most cases industry and technology standards and requirements are discussed and handled separately. The standards are often cross-referred to and it needs expertise to map them with each other. It would be beneficial to discuss these more together, especially with open network products, so each party would have a better view on how industry threats and their security improvements impact the product's SW solution security needs. HW device and application-level security is complementary.

2. **Product security management**

   Companies create TVRA for their products and assure compliance with internal testing. When 3rd party products are integrated into the system there is a new landscape for threats because it must be ensured that the 3rd party complies with the mandatory security requirements and some of the optional requirements. This leaves a gap which requires update to the TVRA and additional verification in integration to close this gap. This sets also additional requirements to the intelligence of network monitoring to detect any anomality in the network behaviour. A new trust model is required together with compatibility management and verification through PLC.

3. **SW management**

   Standardization does not define the SW distribution procedure as a whole, but all network players can have their own way of issuing the SW and verifying its origin and integrity. In 3GPP and O-RAN there are requirements which need to

be fulfilled, but there is still a gap which requires clarification on the certificate management and integrity verification. At high level example view on the SW trust procedure is illustrated in Figure 15.

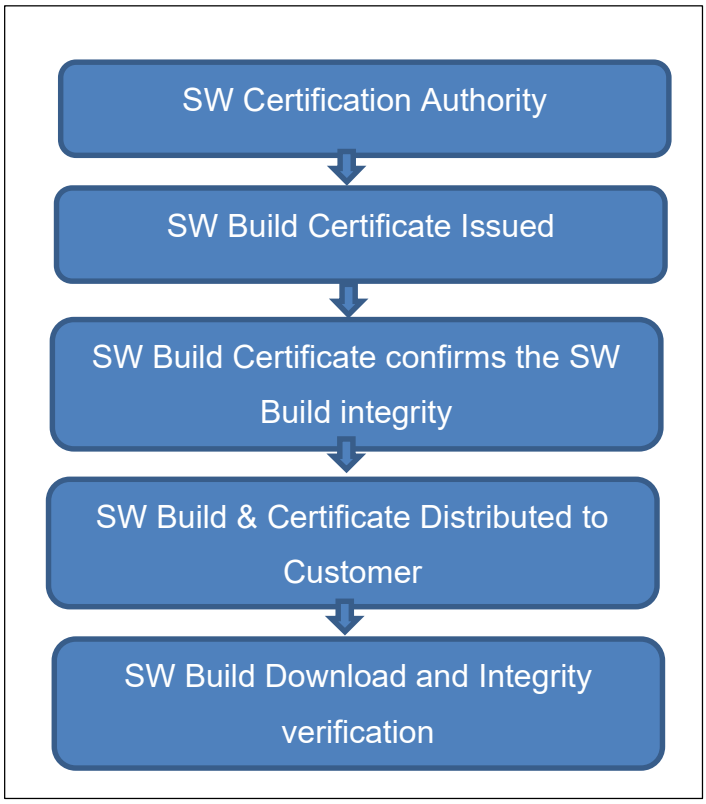

Figure 15 Example of SW Build Trust Procedure

To improve the trust of the SW builds, some additional compliance verification for 3rd party products this study proposes improvements into the O-RAN standard.

4. Innovation to reduce insider threat

For background on insider threat, see chapter 2.4 and 3.2 which raise the risk of human as an insider threat for security risks. As many people use their mobile for hours every day, could an easily approachable mobile security training game be one option for increasing the knowledge of everyday risks without distracting time from regular tasks?

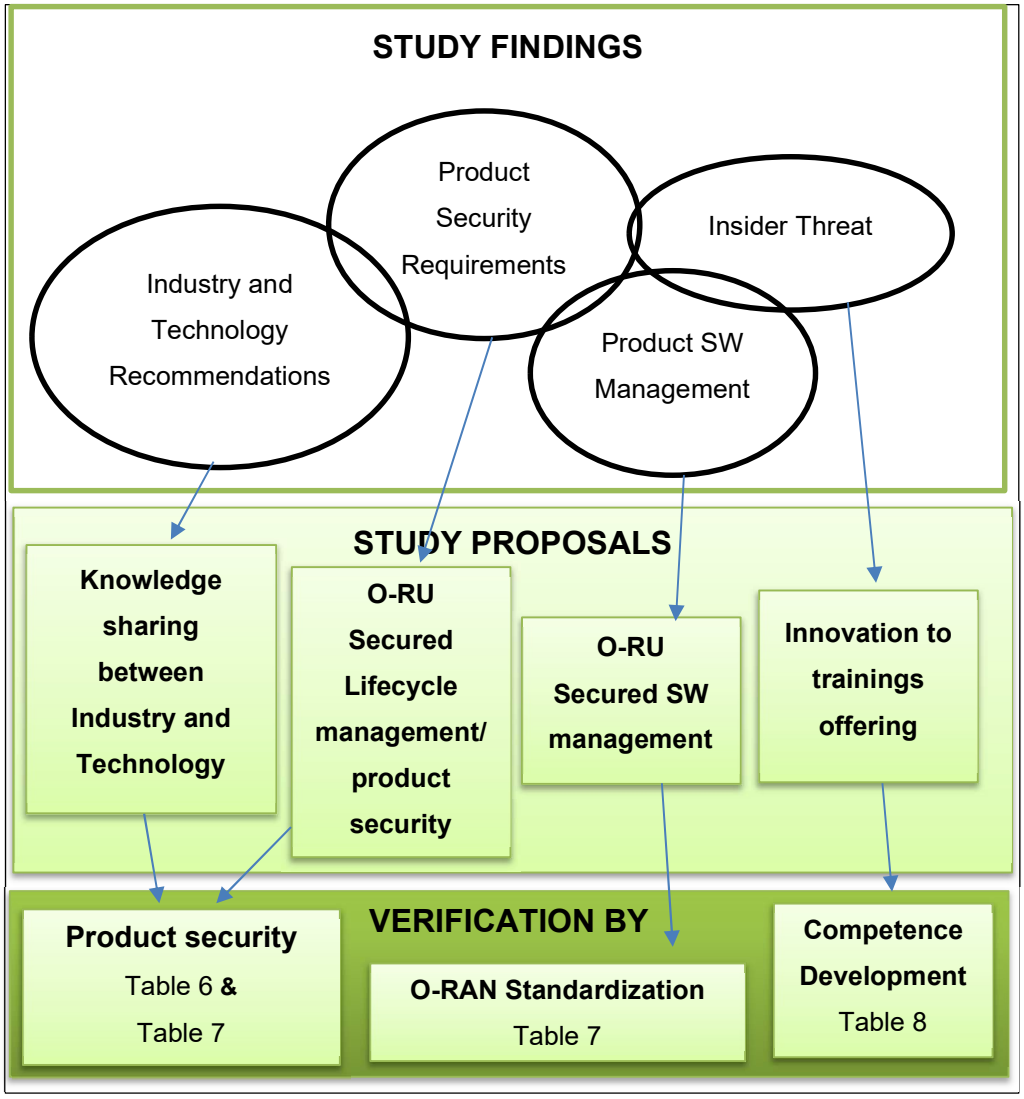

Figure 16 Study findings and proposals

Table 6 Industry and Technology Supply Chain and Product Security

Finding	Product and SW supply chain are mostly separated by standards and requirements, but security is a combining element for both, as there are stages where it is possible to insert malicious or vulnerable parts or code into the supply processes. Visibility to the processes is 3rd party Supply Chain Security is not sufficient and it must be trusted that the manufactured and delivered product has best security measures in use. As a general note, the way how standards are managed between organizations required a lot of “jumping” between documentation. This takes unnecessary time and a tool to organize standards between organizations would reduce the time.
Proposal	Certification to verify secure processes, HW production chain and SW code production. Improve compatibility check with versioning.
Verification	Product Security
Response	Received for further analysis.

Table 7 O-RAN SW Management

Finding	Each RAN supplier has closed SW management actions and O-RAN standard does not describe supplier's internal processes. Once 3rd party HW is integrated to the configuration, there must be a secured SW distribution, installation, boot, and activation which does not give any outsider possibility to intrude the management process. 1) SW management and 2) Access management
Proposal	Recommend ensuring best security practices are used to secure 3rd party SW file load from an external server. Prevent unauthorized SW download via other product interfaces. To ensure the above, study proposes to 1) describe or refer to the recommended procedures for trusted 3rd party SW file loading, and 2) prevent unauthorized SW download.
Verification	SW management R&D team
Response	1) Additional security verification is added. Future challenge is in virtualized SW download from cloud, which will require further study. 2) Product SW disables SW file download via other product interfaces and is already in use.

Table 8 Insider Threat

Finding	Insider threat is a large potential risk for cyber security attacks and based on public studies and experiences insider risk can be best prevented by sharing knowledge and by training. Security risk should not distract people from performing their daily tasks and security should not be outsourced. There should be easily approachable security leaders who give support with Q&A.
Proposal	There could be two levels of security trainings, one for Security Champion and other for Security Practitioner. Security champion or leader would have completed company level online and practical trainings and for the security practitioner there could be a yearly mandatory training and an easily approachable mobile security game which can be shared with colleagues. Often information security is taken care of, but product security awareness is limited to few people. There should be practical exercises for more employees, not just a handful of employees.
Verification	Product Security and Competence development teams
Response	Training needs are compliant. Mobile game option is under checking.

6 Conclusions

The scope of this study was to investigate RAN security monitoring functions from production to distribution and activation functions. To achieve the target this required the analysis of existing security technologies and features in the case company including the HW and SW product lifecycle management. The investigated lifecycle included product planning and production or coding, up to the product deployment for customers to take the product into use. Analysis was approached by studying the public industry and telecommunication standards and recommendations, which are for use of any company and organization to comply with.

To understand how the standards are used, the standards were viewed against the case company's processes to identify possible improvement areas. As a result of this analysis there were four improvements found and these were mapped to organizational areas. Special attention was set to risks which are challenging to manage but can be overcome with available technologies. This study concentrated much on deployment and integration of 3rd party products into a closed radio access network. Because security threat is a rapidly evolving area, it is realistic to understand that whenever there is a 3rd party involved, there are security threats which cannot be predicted unless those are understood, maintained, and monitored.

This study improved the standardization knowledge transfer between organizations, specially between manufacturing and product development, and there was seen benefit in cross-organization discussions. The product security management must be well organized, and the procedures defined and followed. This study showed the excellent condition of this area, due regular information sharing from standardization organizations and authorities.

As telecommunications services are moving more into the cloud, where there will be more challenges for services to identify the environment where it is running on, and cyber security will have new challenges. With open networks and the expanding number of connected devices, new methods need to be investigated and taken into use, like block chain, and other AI/ML solutions should overcome cyber security threats and replace rule-based security management solutions with more agile and

self-learning solutions. For sure there are risks and the management of risks is most important.

This thesis is a good basis for a next step to study the security of virtual network functions (VNF) and leaves thoughts how to transform into a self-learning shield against security threats. In many discussions, it could be noticed it is important to understand which infrastructure environment is discussed, as standardization is already handling more virtualized network security.

References

1 Security in 5G Specifications, Controls in 3GPP Security Specifications (5G SA), Feb 2021, www.enisa.europe.eu

2 O-RAN Architecture Description O-RAN.WG1.O-RAN-Architecture-Description-v07.00

3 Syed NF, Shah SW, Trujillo-Rasua R, Doss R, Traceability in supply chains: A Cyber security analysis, Computers & Security, Volume 112, 2022,102536, ISSN 0167-4048

4 Ghadge A., Weiss M., Caldwell ND., Wilding R., Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management: An International Journal 25/5 (2020) p. 223-240

5 https://www.nist.gov/cyberframework/online-learning/components-framework

6 Afaq A, Haider N, Baig MZ, Khan KS, Imran M, Razzak I; Machine learning for 5G security: Architecture, recent advances, and Challenges, Ad Hoc Networks 123 (2021) 102667

7 Open RAN Security in 5G, 2021 https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

8 Yousefnezhad N., Malhi A., Främling K., Security in product lifecycle of IoT devices: A survey, Journal of Network and Computer applications 171 (2020) 102779

9 3GPP TS 33.117 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Catalogue of general security assurance requirements

10 Conklin A, Shoemaker DP, CSSLP Secure Software Lifecycle Professional All-in-one Guide, 3rd Edition, Information and Software Technology, Vol 147, 2022 (Book)

11 WG4: Open Fronthaul Interfaces Workgroup, O-RAN Management Plane Specification O-RAN.WG4.MP.0-v09.00 https://orandownloadsweb.azurewebsites.net/specifications

12 IEEE Std 802.1X-2020: “IEEE Standard for local and Metropolitan Area Networks – Port-Based Network Access Control”, Feb 2020

13 WG4: Open Fronthaul Interfaces Workgroup, Control, User and Synchronization Plane Specification Open Fronthaul Interfaces Workgroup, O-RAN O-RAN-WG4.CUS.0-v09.00 p. 65, 193 https://orandownloadsweb.azurewebsites.net/specifications

14 Hakeem A, Hussein SA, Kim H. Security Requirements and Challenges of 6G Technologies and Applications. Sensors 2022, 22, 1969

15 Zhang S, Wang Y, Zhou W, Towards secure 5G networks: A Survey, Computer Networks, 162, 2019

16 https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm

17 Etemadi N, Borbon-Galvez Y, Strozzi F, Etemadi T, Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review Information 2021, 12, 70.

18 Akbar MA, Smolander K, Mahmood S, Alsanad A, Toward successful DevSecOps in Software development organizations: A decision-making framework, Information and Software Technology 147 (2022)

19 https://about.gitlab.com/topics/devops/

20 NIST SP800-207 Zero Trust Architecture

21 GSM Association, Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements, version 2.1, Jan 2022

22 www.paloaltonetworks.com/zero-trust

Appendix 1 O-RAN Statement of compatibility with 3GPP

This chapter gives the statement of compatibility with 3GPP/SCAS security Assets, Threats and Requirements. The statement of compatibility shows that 3GPP Assets/Threats/Requirements are applicable and that there is no conflict affecting the security of O-RAN components.

3.1 Assets and Threats

Table 6-1 : Statement of compatibility with 3GPP – Assets and Threats

3GPP/SCAS document reference/section	Description	Applicable to O-RAN	Rationale
TR 33.926, clauses 5 and 6	It describes the generic assets and threats of 3GPP network products	Yes	Since these assets/threats are for generic 3GPP (virtualized) network products, they are also applicable to O-RAN. It means that there is no need to repeat those assets/threats in this document.
TR 33.818, clause 5.2.4	It describes the generic assets, threats and requirements of 3GPP/ETSI NFV virtualized network products.	Yes	
TR 33.848, clause 5	It considers the consequences of virtualization on 3GPP architectures, in order to identify threats and subsequent security requirements relating to ETSI-defined interfaces and Security functional requirements related to Virtualization layer, hardware and resource isolation.	Yes	

In addition, O-RAN also needs to consider the assets/threats related to the additional specific O-RAN interfaces and components. As a result, sections §4.3 and §5.4 elaborates the O-RAN specific assets and threats respectively.

3.2 Security requirements

Table 6-2 : Statement of compatibility with 3GPP – Security requirements

3GPP/SCAS document reference/section	Description	Applicable to O-RAN	Rationale
TS 33.117, clauses 4.3 and, 4.42	It describes the general approach taken towards security functional requirements deriving from 3GPP specifications and the corresponding test cases, independent of a specific network product class.	Yes	Since these requirements are for generic 3GPP (virtualized) network products, they are to be fulfilled by O-RAN. It means that there is no need to repeat those requirements in this document.
TR 33.818, clauses 5.2.5 and 5.3	It describes the generic assets, threats and requirements of 3GPP/ETSI NFV virtualized network products.	Yes	
TR 33.848, clause 5	It considers the consequences of virtualization on 3GPP architectures, in order to identify threats and subsequent security requirements relating to ETSI-defined interfaces and Security functional requirements related to Virtualization layer, hardware and resource isolation.	Yes	
TS 33.501	It describes the security architecture and procedures for 5G system including gNodeB	Yes	
TS 33.511	It describes the security requirements for the next generation Node B (gNodeB) network product class	Yes	

In addition, O-RAN also needs to consider the security requirements related to the additional specific O-RAN interfaces and components. As a result, chapter §6 focus on the O-RAN security principles.

In future versions of the document, security requirements, recommendations and countermeasures will be derived from security principles.

O-RAN.SFG.Threat-Model-v02.01, O-RAN Security Threat Modeling and Remedation Analysis

Appendix 2 ENISA Threat Landscape for 5G Access Networks

5.3 ACCESS NETWORK THREATS

Abuse of spectrum resources: The illegal use of these resources, due to the dynamic allocation/ reallocation of the same, may allow the occupation of specific idle spectrum band by imitating the characteristics of a legitimately licensed unit and causing interference in radio frequencies. This illicit occupation of the spectrum may also induce a network node to reject spectrum resources requested by unlicensed units - due to the apparent lack of idle resources – thus blocking someone out of the core network.

Address Resolution Protocol (ARP) poisoning: This kind of attack is also called ARP cache spoofing: a technique by which an attacker sends spoofed ARP messages onto the network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

Fake access network node: Classified as a nefarious activity, this threat considers the compromise of a base station (gnB) by masquerading as legitimate, facilitating different types of attacks such as man-in-the-middle or network traffic manipulation. The threat considers tampering the communication between the mobile user equipment (UE) and the network to initiate other malicious actions.

Flooding attack: This threat involves flooding radio interfaces with requests. Flooding occurs through the transmission of data that can exhaust component resources and lead to a reduction or complete shutdown of the radio frequency provided by the component.

IMSI catching attacks: This threat relates to cellular paging protocols that can be exploited by a malicious actor in the vicinity of a victim to associate the victim's soft-identity (e.g., phone number, Twitter handle) with its paging occasion. Through an attack dubbed ‘$mathsf{ToRPEDO}$’ a malicious actor can verify a victim's coarse-grained location information, inject fabricated paging messages, and mount denial-of-service attacks.

Jamming the radio frequency: Classified as a nefarious activity/abuse of asset, this threat refers to an intentional disruption/interference of the network radio frequency (NRF) causing the core network (and related services) to become unreachable for affected users. The threat also refers to the unavailability of the transport layer when using radio-based networks and interference with the geo-positioning system (GPS).

MAC spoofing: MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity to conduct an attack.

Manipulation of access network configuration data: This threat involves compromising an access network element (e.g. base stations) to forge configuration data and launch other attacks (e.g. DoS).

Radio interference: A threat in which the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely interfering or disrupting the Radio Access Network service. The introduction of compromised 5G devices in a radio access network will present a more substantial DoS threat.

Radio traffic manipulation: This threat considers the manipulation of network traffic at the base station level. A man-in-the-middle attack can be launched based on a rogue base station when malicious actor masquerades its Base Transceiver Station (BTS) as a real network’s BTS. This threat is still considered valid due to backwards compatibility to previous generations of mobile technology. Other associated threats follow:

- Traffic redirecting

Session hijacking: This threat is classified as nefarious activity or abuse of asset and relates to attacks to open-air interfaces. The threat considers the theft of legitimate authenticated conversation session ID by a malicious actor, to control the whole session of specific traffic to conduct other types of attacks.

Signalling fraud: One of the areas of concern is the international signalling interconnection between networks which may be misused for fraud (e.g., false charging). Another example is the threat of greedy mobile nodes that transmit fake incumbent signals and force all other users to vacate a specific band (spectrum hole) to acquire its exclusive use.

Signalling storms: Mobile networks are subject to ‘signalling storms’ launched by malware or apps, which overload the bandwidth at the cell, the backbone signalling servers, and Cloud servers, and may also deplete the battery power of mobile devices. Signalling storms will be more challenging due to the excessive connectivity of UEs, small base stations, and high user mobility.

Appendix 3 3GPP Vulnerability Scanning

4.4.3 Vulnerability scanning

Requirement Name: Vulnerability scanning

Requirement Description:

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

Vulnerability scanning tools may also report false positives and they shall be investigated and documented in the test report.

The test for this requirement can be carried out using a suitable tool or manually performed as described below. If a tool is used then the tester needs to provide evidence, e.g. by referring to the documentation of the tool, that the tool actually provides functionality equivalent to the steps described below.

Test case:

Test Name: TC_BVT_VULNERABILITY_SCANNING

Purpose:

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

Procedure and execution steps:

Pre-Conditions:

A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:

- all interfaces providing IP-based protocols;
- the available transport layer protocols on these interfaces;
- their open ports and associated services;
- and a free-form description of their purposes.

NOTE 1: This list is to be validated as part of the BVT port scanning activity.

The used vulnerability scanning tool shall be capable to detect known vulnerabilities on common services. The used vulnerability information shall be reasonably recent at the time of testing.

Execution Steps

The accredited evaluator's test lab is required to execute the following steps:

1. Execution of the suitable vulnerability scanning tool against all interfaces providing IP-based protocols of the Network Product.
2. Evaluation of the results based on their severity.

Expected Results:

The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation.

The discovered vulnerabilities (including source, example CVE ID), together with a rating of their severity, shall be highlighted in the testing documentation.

COTS Vulnerability scanners, by their nature, (e.g. depending on how they are configured) may result in false findings/positives. The tool's documentation may even mention that the failing test shall be repeated to check whether it is really a recurring problem or not. The tester shall make best effort to determine if there is an issue with NE or the test tool and if necessary, work with the vendor of the network product to come to a consensus on the test result outcome.

NOTE 2: This testing documentation is input to the vulnerability mitigation process (that may include patching). This is part of the product lifecycle management process developed by GSMA SECAG.

Expected format of evidence:

Output of BVT tool.

Appendix 4 3GPP Protection at the Transport Layer

Ch 4.2.2.2.2 Protection at the transport layer

Requirement Name: Protection at the transport layer
Requirement Reference: TS 33.501 [10], clause 5.9.2.1, clause 13.1, clause 13.3.2
Requirement Description:
"NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer" as specified in TS 33.501 [10], clause 5.9.2.1;
"All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.
The TLS profile shall follow the profile given in Annex E of TS 33.310 [9] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11]. "
as specified in TS 33.501 [10], clause 13.1.
"Authentication between network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between NFs."

as specified in TS 33.501 [10], clause 13.3.2.

Threat References: TR 33.926 [4], clause 5.3.6.3, Weak cryptographic algorithms

Test case:

Test Name: TC_PROTECT_TRANSPORT_LAYER
Purpose:
Verify that TLS protocol for NF mutual authentication and NF transport layer protection is implemented in the network products based on the profile required.
Procedure and execution steps:
Pre-Conditions:
Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

A peer implementing the TLS protocol configured by the vendor shall be available.

The tester shall base the tests on the profile defined by 3GPP in Annex E of TS 33.310 [9] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11].

Execution Steps

1. The tester shall check that compliance with the TLS profile can be inferred from detailed provisions in the network product documentation.
2. The tester shall establish a secure connection between the network product under test and the peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test.
3. The tester shall try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile.

Expected Results:

- The network product under test and the peer establish TLS if the TLS profiles used by the peer are compliant with the profile requirements in TS 33.310 [9] Annex E and RFC 7540 [11].
- The network product under test and the peer fail to establish TLS if the TLS profiles used by the peer are forbidden in TS 33.310 [9] Annex E or RFC 7540 [11].

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

Appendix 5 3GPP Network Product Software package integrity

Network Product software package integrity

Requirement name: Network product Software integrity validation

Requirement reference: to be done later

Requirement Description:

1) Software package integrity shall be validated in the installation/upgrade stage.
2) Network product shall support software package integrity validation via cryptographic means, e.g. digital signature. To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.
3) Tampered software shall not be executed or installed if integrity check fails.
4) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet 2.

Security Objective references: SOFTWARE INTEGRITY

Test case:

Test Name: TC_SW_PKG_INTEGRITY_1

Purpose:

Verify that:

1. The Network Product validates the software package integrity during the installation/upgrade stage.
2. The software package integrity validation mechanism is performed using cryptographic mechanisms, e.g. digital signature using the public keys or certificates configured in the network product.
3. Software that fails an integrity check is rejected by the network product.
4. Only authorized users are allowed to install software.

Procedure and execution steps:

Pre-Conditions:

- A network product document containing information regarding software package integrity checks, including details of how the integrity check is carried out, where public keys or certificates of sources authorised to sign software packages are stored on the network product and who these sources are, and what evidence is created to prove that the integrity check has been executed and what the result of the check was. Documentation which describes the installation procedure including how a user is authorized and authenticated to perform installation process.
- A valid network product software load/package and one that is not-valid (or could be deemed to have been tampered with) are available.

Execution Steps

The tester checks the permissions required to install software on the network product ensuring that a user is properly authenticated by the network product and that they have the required access privileges to perform the installation activity.

The tester checks, when a software package is attempted to be installed on the network product, that the software package integrity check is executed (check for evidence of execution as described in network product documentation) and that valid software is allowed to be installed but invalid software is rejected.

The tester checks the access control permissions for the software package integrity checking process, the list of public keys of authorised software sources, and any related credentials or keys for the process, to ensure that the process cannot be controlled by persons that are not authorized to do so.

Expected Results:

- Evidence that the software package integrity check has been executed for both cases of software installation (valid and invalid software packages).
- Authentication and access control mechanisms are in operation for software package installation and around the software package integrity checking mechanism.
- The installation/upgrade operation fails when using an invalid software package.
- The installation/upgrade operation is successful when using a valid software package.

Expected format of evidence:

Snapshots containing the result of the installation of package A and B.

Appendix 6 Overview of Security Mechanisms in IoT PLC