Private 5G Networks for Connected Industries

Deliverable D1.2

Report on Relevant Requirements and Concerns Regarding Suitable Operator Models

Co-funded by the Horizon 2020 programme of the European Union

Date of Delivery: 31.12.2020
Project Start Date: 01.10.2019 **Duration:** 36 Months

Document Information

Project Number:	861459
Project Name:	Private 5G Networks for Connected Industries

Document Number:	D1.2
Document Title:	Report on Relevant Requirements and Concerns Regarding Suitable Operator Models
Editor(s):	Henrik Klessig (Robert Bosch GmbH)
Authors:	Mickael Maman (CEA) Henrik Klessig (Robert Bosch GmbH) Bettina Kauth (Robert Bosch GmbH) Cheng-Yi Chien (Chunghwa Telecom, CHT) Jiun-Cheng Huang (Chunghwa Telecom, CHT) Shih-Chien Huang (Chunghwa Telecom, CHT) Yueh-Feng Li (Chunghwa Telecom, CHT) Ling-Chih Kao (Chunghwa Telecom, CHT) Kuan-Yi Chih (ITRI) Jack Shi-Jie Luo (ITRI)
Dissemination Level:	Public
Contractual Date of Delivery:	M15
Work Package	WP1 - Use Cases & Requirements
File Name:	861469-5G CONNI-D1.2_Report_on_Relevant_Requirements_and_Concerns_Regarding_Suitable_Operator_Models_v1.docx

Revision History

Version	Date	Comment
0.1	03.08.2020	Document created with initial outline.
0.2	05.10.2020	Update with questionnaire 1
0.3	26.10.2020	Update with questionnaire 2
0.31	29.10.2020	Revised version of v0.3
0.32	05.11.2020	Update introduction
0.4	25.11.2020	Update of section 3 and 4
0.5	25.11.2020	Update of section 5
0.6	02.12.2020	Update of section 3 (new input edited) and 5 (plain text)
0.7	09.12.2020	Review of Tables and Annexes, Section 6 added
0.71	10.12.2020	Abstract added
0.8	11.12.2020	Cleaned up
0.81	14.12.2020	Spelling errors corrected
1.0	16.12.2020	Final Version

Abstract

5G non-public networks along with technical enhancements revolving around softwarization, cloudification and increased modularity of the 5G System are expected to disrupt the current constellation not only regarding deployment models and architectures but also with respect to the stakeholders involved in the operation of a private network and their roles and responsibilities, i.e. operator model). Nevertheless, the different stakeholders might have concerns in regard to such operator models. To explore this new field, it is important to understand the different dimensions of operator models and how they are interrelated. 5G elements (e.g. 5G network functions, RAN components, etc.) and non-5G elements (e.g. enterprise IT), private 5G network lifecycle tasks and involved stakeholders (e.g. enterprise, MNO, service provider) are the most important dimensions, which have been identified as part of the 5G CONNI activities in WP1/T1.2. The dimensions are interrelated. For example, whether one stakeholder can carry out management task on a 5G component depends on a multitude of factors, incl. the physical and logical location of that element (e.g. 5G Core) and on what other stakeholder owns and governs it. A deep analysis revealed that 10 different stakeholders can own or govern 23 elements in total. This is even more complex taking into account seven different locations, at which the elements (in particular, 5G components) can be installed, and the plethora of different lifecycle tasks (49 in total). In addition, each task involves a specific set of elements that are touched by the responsible stakeholder. From this deep analysis, a 67 concerns and related requirements have been collected from the perspectives of different stakeholders. In general, the concerns regarding operator models are attributed to different perspectives: confidentiality, integrity and availability of information, access to and control of elements (specifically 5G components), the private 5G network lifecycle and responsibilities and expertise required by the stakeholders for each task, regulatory aspects, and applicability and practicability. Each requirement is assessed in terms of importance and they are grouped to form 13 general aspects, whose criticality is determined based on the number of requirements per aspect and their importance ratings. The top five aspects (in terms of criticality) are: (1) Wrong or missing access to 5G elements by the enterprise, MNO or SP, (2) interoperability of security systems and alignment of security concepts of different stakeholders, (3) the lack of expertise to carry out lifecycle tasks, (4) confidentiality, integrity and availability of data, and (5) a lack of autonomy of a stakeholder. Finally, a stakeholder-specific (enterprise, MNO, service provider) operator model evaluation template is designed, which considers the importance of each requirement and also how such a requirement can be fulfilled, i.e., either a requirement can be fulfilled inherently by the operator model, through technical features or by contractual agreements. The template will help to evaluate concrete operator models (distribution of roles and responsibilities of the private 5G network lifecycle among stakeholders) regarding all 13 aspects and from the perspectives of the three most important stakeholder perspectives, i.e. the ones by the enterprise, the MNO and the service provider.

List of Figures

List of Tables

List of Acronyms

3GPP	**3rd Generation Partnership Project**
5G	5th Generation Mobile Communications
3EC	Third-party Enterprise/Community
3NP	Third-party network/radio planner
3SI	Third-party system integrator
3WO	Third-party WAN operator
5G CONNI	5G for Connected Industries
AGV	Automated Guided Vehicle
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
BSS	Business Support System
CNC	Computer Numerical Control
CP	Cloud Provider
CPU	Central Processing Unit
DNN	Data Network Name
E	Enterprise
eNB	eNodeB
eSIM	Embedded-SIM
G	Government
gNB	gNodeB
GPU	Graphics Processing Unit
HA	High availability
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
I-UPF	Intermediate UPF
KPI	Key Performance Indicator
LAN	Local Area Network
MAC	Medium Access Control
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
MPLS	Multi-Protocol Label Switching
MVNO	Mobile Virtual Network Operator
NEF	Network Exposure Function
NEV	Network Equipment Vendor
NFV	Network Function Virtualization
OAM	Operations, Administration, and Maintenance
OSS	Operation Support System
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Packet Data Unit
PS	Power Supplier

QoS	Quality of Service
RAN	Radio Access Network
RAN-CU	Radio Access Network – Central Unit
RAN-DU	Radio Access Network – Distributed Unit
RF	Radio frequency
RLC	Radio Link Control
RRC	Radio Resource Control
RU	Radio Unit
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMF	Session Management Function
SMS	Short Message Service
SP	Service Provider
TAC	Tracking Area Code
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliably Low-Latency Communications
USIM	UMTS Subscriber Identity Module
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Table of Contents

1 Introduction

1.1 Objective of this Document

The 5G CONNI project aims at providing an integrated end-to-end 5G test and demonstration network for industrial applications. This network will be developed to serve a number of industrial use cases, which leverage 5G network and edge computing capabilities, and which will be implemented at two interconnected industrial trial sites in manufacturing facilities in both, Europe and Taiwan.

WP1 (Use Cases & Requirements) has identified innovative use cases for 5G networks in Smart Factories by elaborating on previously published scenarios and normative requirements and adding use cases based on recent 5G technology developments. The requirements and KPIs for industrial private 5G networks have been analyzed and derived in D1.1

In general, many factory owners have concerns regarding the usage of a public land mobile network for enabling 5G-based industrial production. Therefore, non-public networks are needed, as is also being discussed in 3GPP. However, there are many different flavors how such non-public networks may be operated with different pros and cons. What a pro or con is often depends on the concrete context. Therefore, the goal of task 1.2 is to identify, collect and analyze general aspects that have to be considered in this respect. In particular, this may include aspects like security, autonomy, worldwide applicability, etc.

This document identifies and analyzes relevant requirements and concerns regarding suitable operator models for non-public 5G factory networks, which then may lay the basis for the design and evaluation of suitable operator models in WP 2. This document also addresses an evaluation methodology that can be used to verify and validate that a certain operator model can be satisfactorily implemented in the end.

1.2 Structure of this Document

This deliverable is structured as follows. Section 2 defines and explains the main dimensions of operator models such as ownership and governance, stakeholders involved, element of operator model (directly related or not to the 5G system) and private network lifecycle. Section 3 describes operator models for private 5G networks and analyzes the different interrelationships between the dimensions. Section 4 assesses the interdependence between operator and deployment models. Section 5 analyzes concerns and requirements regarding operator models such as access & control of an element/information, ownership & governance of an element, confidentiality & integrity & availability of data, cost and coordination & organization between stakeholder competencies or sites. Finally, Section 6 provides a suitable evaluation methodology to support WP2 in developing and evaluating operator models.

2 Preliminary Considerations

In this section, definitions and explanations are provided that are relevant for the subsequent elaborations on the dimensions of operator models.

2.1 Ownership and Governance

As discussed in 6G Networking White paper[1], the sense of network ownership has evolved. Traditionally, the operator has owned the physical communication links, the service infrastructure, and the customer relationships. This model has been increasingly challenged and transformed by virtual network operators, infrastructure sharing, the current trend into asset divestiture and specialized infrastructure operators. Effectively, most end-to-end connections will pass through a multitude of stakeholders, who will not be bound by static service level agreements, but will have to pass through a rich ecosystem of dynamic technical (and economic) relationships. The ownership of and governance over various elements, in particular network elements, are crucial aspects in regard of operator models. If a stakeholder owns a network element, restrictions on the governance and access with respect to this network element by another stakeholder can be expected. In this regard, the following definitions are of importance:

2.1.1 Initial Ownership

Initial ownership is the designer or the developer of elements that will be used in the private 5G Network.

2.1.2 Owning Stakeholder

Owning Stakeholder is the legal proprietor of the deployed element (e.g. physical infrastructure, licenses).

2.1.3 Governing Stakeholder

Governing Stakeholder is the stakeholder responsible for management and operation of the element in question. Management and operation tasks during the lifecycle of the private 5G Network can also be delegated by the governing stakeholder to another stakeholder, such as a sub-contractor, while still remaining responsible and liable.

2.2 Stakeholders Involved in Operation Models

During the lifecycle of a private 5G network, a number of important stakeholders are involved, who are responsible for carrying out particular tasks on network elements and other components. Some of these stakeholders are also potential owning and governing parties. Table 1 collects all stakeholders important to the analysis and evaluation of operator model dimensions and explicit operator models.

Table 1: Description of Stakeholders.

Stakeholder	Description
Enterprise (E)	The enterprise is the owner or manager of the premises and it is responsible for the long-term innovation, efficiency and profitability of its operation. In large enterprises, teams can be dedicated to centrally or decentrally manage IT systems. In a factory environment, such as a shop floor, the user of the technology is usually the factory personnel. Factory personnel include machine builders, machine operators, local manufacturing IT management personnel, logistics workers, and others.

[1] White paper on 6G Networking, 6G Research Visions, No6, June 2020, https://www.6gchannel.com/items/6g-white-paper-networking/

Mobile Network Operator (MNO)	The MNO operates its mobile network infrastructure to provide connectivity to end-users. It merges the roles of mobile service provider and infrastructure provider.
Network Equipment Vendor (NEV)	They are responsible for building and delivering the hardware and software that compose the network infrastructure.
Cloud Provider (CP)	It is a third-party company offering a cloud-based platform, infrastructure, application, or storage services.
Service Provider (SP)	A Service Provider is the entity that offers services to consumers. It can take the local operator role specialized for the specific facility. It can provide radio & core service, cloud services, management service, IoT services or security service.
Third-party system integrator (3SI)	It is a third-party company, specialized in bringing together component subsystems into a whole and ensuring that those subsystems function together. The 3SI proposes a broad range of skills including software, system architecture [2] and enterprise architecture, software and hardware engineering and interface protocols.
Third-party network/radio planner (3NP)	It is a third-party company, specialized in the process of proposing locations, configurations and settings of the new network nodes to be rolled out in the private 5G Network. Its main objectives are to implement an economically efficient network infrastructure, to obtain sufficient coverage over a target area and to provide the demanded network capacity by taking into account the specification of technology-dependent parameters.
Third-party WAN operator (3WO)	The 3WO is the owner, in whole or in part, of the WAN infrastructure, and makes its assets available as a service.
Third-party Enterprise/Community (3EC)	Third-party Enterprises or the Community can participate regarding the private network, for example, if an access point must be installed at a third party roof top.
Government (G)	Government or office of communications / regulation licensing spectrum or certifying products.

2.3 Elements and Aspects Relevant for Ownership and Governance

Operator models are concerned with roles and responsibilities with respect to certain tasks on a large number of 5G-related and non-5G elements during the private 5G network lifecycle, which are collected subsequently.

2.3.1 Elements Directly Related to the 5G System

The elements that are relevant to ownership and governance, as well as for the lifecycle of the private 5G network and that are directly related to the 5G System are described in Table 2. All these elements can be attributed to the 5G Core, 5G Radio Access Network, the User Equipment or the 5G Operations and Management System. The list provided below is not exhaustive, yet present the most important elements in this context.

Table 2 : Description of 5G Elements.

5G Element	Description
Unified Data Management (Core-UDM)	The Unified Data Management (UDM) manages the subscriber information that is used for admission control and for defining the data path policies. Furthermore, it manages root keys for

[2] https://en.wikipedia.org/wiki/Systems_architecture

	confidentiality and integrity protection of the data and control planes.
Authentication Server Function (Core-AUSF)	The Authentication Server Function (AUSF) is responsible to authenticate the users
Session Management Function (Core-SMF)	The Session Management Function (SMF) is responsible for the data path setup and tracking and terminating based on the policy function.
Access and Mobility Management Function (Core-AMF)	The Access and Mobility Function (AMF) implements the access control and mobility aspects of the user context.
User Plane Function (Core-UPF)	The User Plane Function (UPF) defines the data path characteristics based on the users requirements and policy.
Network Exposure Function (Core-NEF)	The Network Exposure Function (NEF) provides a means to securely expose the services and capabilities provided by 3GPP network functions.
Transport Network	The transport network that is used to carry traffic between the 5G RAN and 5G Core network.
Radio Access Network – Distributed Unit (RAN-DU)	The Radio Access Network – Distributed Unit (RAN-DU) is responsible for real time L1 and L2 scheduling functions. RAN-DU sits close to the radio unit and runs the RLC, MAC, and parts of the PHY layer. This logical node includes a subset of the eNB/gNB functions, depending on the functional split option, and its operation is controlled by the RAN-CU.
Radio Access Network – Central Unit (RAN-CU)	The Radio Access Network – Central Unit (RAN-CU) is responsible for non-real time, higher L2 and L3. RAN-CU runs the RRC and PDCP layers. The split architecture enables a 5G network to utilize different distribution of protocol stacks between RAN-CU and RAN-DUs depending on midhaul availability and network design. It is a logical node that includes the gNB functions like transfer of user data, mobility control, RAN sharing, positioning, session management etc., with the exception of functions that are allocated exclusively to the RAN-DU. The RAN-CU controls the operation of several RAN-DUs over the midhaul interface.
Subscriber Identity Module (SIM)	The SIM is a fundamental element of the cellular system, because it allows authenticating the validity of a terminal as it tries to access the network. It contains the unique identifier of the subscriber and the related security keys
5G Operation, Administration and Management (5G OAM) System	Network operation and management systems, such as the operation support system (OSS) and the business support system (BSS), are complex applications that are required for a proper network configuration, operation and management, and for billing of customers (subscribers).
Spectrum	The electromagnetic spectrum is, for most parts, not a free resource, but in fact allocated and regulated into frequency bands by government bodies. Some of these frequency bands are unlicensed, which means that anyone who wants to use the spectrum can do so. Most of the spectrum however is licensed, which means that the license holder is the only authorized user of that spectrum range.
Control Plane Data	Control plane is concerned with protocols, which control the radio access bearers and the connection between the UE and the network.

2.3.2 Elements Not Directly Related to the 5G System

In addition to the 5G components, further non-5G elements are relevant to ownership and governance, and, more importantly, with respect to access and control by a number of stakeholders. Such elements, playing a crucial role during the private 5G lifecycle, are collected and described in Table 3.

Table 3 : Description of Non-5G Elements.

Non-5G Element	Description
Application	There exists a plethora of different applications, which can be offloaded to a MEC platform. In the industrial domain, such applications range from simple data collection and database systems to control logic functions of controllers to more complex systems, such as manufacturing execution systems or even enterprise resource planning software. Depending on the type of the application, the MEC platform is either deeply integrated with the 5G System and located close to a machine or production line, or it provides computing capabilities for a large number of machines, sensors etc. that can even span across multiple factories.
MEC Platform	The purpose of the edge-computing platform is to carry applications and connect telecom operators' network equipment, and thus telecom operators usually own the edge-computing platform. Owners of the edge-computing platform must maintain the network connectivity and assist in generating applications of the platform.
User Plane Data	User plane is responsible for the transfer of user data, such as voice or application data through the access stratum.
WAN Infrastructure	A wide area network (WAN) is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking. WAN infrastructure may be privately owned or leased as a service from a third-party service provider, such as a telecommunications carrier, internet service provider, private IP network operator or cable company. For operator models, in which multiple stakeholders are involved carrying out O&M tasks remotely, the WAN infrastructure plays a significant role, e.g. regarding availability of the entire distributed system.
Shop Floor	A shop floor is the area of a factory, machine shop, etc. where people work on machines, or the space in a retail establishment where goods are sold to consumers.
Shop Floor Plan	The map of the factory including information about physical objects, such as machines, walls, production lines, etc.
Enterprise Network IT	An enterprise IT network is the backbone for facilitating an organization's communications and consists of physical and virtual networks and protocols that serve the dual purpose of connecting all users, computers and devices throughout departments on a local area network (LAN) to applications in the data center and cloud as well as facilitating access to network data and analytics. These information networks can include local area networks (LANs), wide area networks (WANs), intranets and extranets. The enterprise network IT plays an important role

	regarding the deployment and integration of a private 5G network, especially with respect to IT security.
Third-party Cloud Platform	It is a third-party company platform proposing the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet to offer faster innovation, flexible resources, and economies of scale
Enterprise OAM Systems	Enterprise operations & maintenance systems plans and executes activities such as operating the system, or monitoring system performance. Such systems become important, when existing network infrastructures (incl. WLAN) converge with the private 5G infrastructure.
Enterprise Personnel and/or End Device Database	Enterprise Personnel and/or End Device Database corresponds to the database of enterprise personnel to provide them access or to end device such as computers, robots, machines, cameras, etc.
Power Supply	The power supply is a hardware component or network that supplies power to electrical devices. The plan of the enterprise power grid will also be necessary to deploy powered devices of private 5G Networks.

2.4 Private 5G Network Lifecycle

As operator models are concerned with the allocation of roles and responsibilities to the stakeholders with respect to all the relevant tasks from the definition of the 5G network aspects to network deployment to eventually tearing it down, it is important to detail the lifecycle of a private 5G network and the associated tasks. In general, a lifecycle model enables one to ensure that private 5G networks are delivered that fulfill the stakeholder's requirements, in particular the Enterprise's, to provide strong management controls over the projects, and to make the management process efficient. The lifecycle of a private 5G networks can be composed of four phases and nine high-level tasks, as depicted in Figure 1.

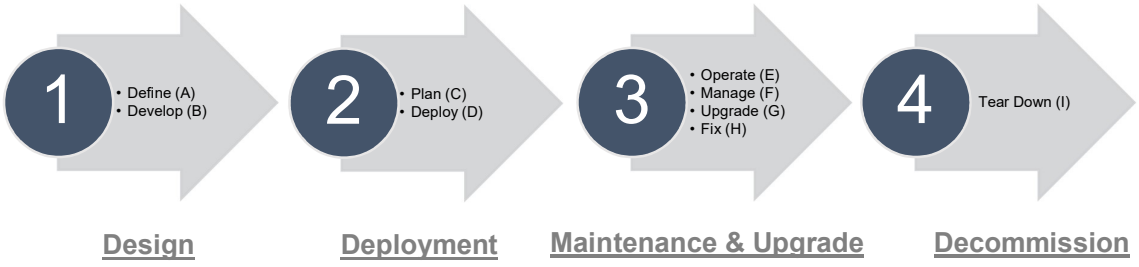

Figure 1 : Lifecycle of Private 5G Networks.

The first phase concerns the design of the private 5G network, where the objectives are to determine business goals, define a high-level design and develop all the elements of the private 5G network solution. The second phase includes the deployment of the solution at the selected site, e.g. the factory floor. The objectives are to plan (infrastructure and radio) and adapt the solution to the specific scenario at the particular site, and to configure, integrate, deploy and test the complete solution. In the third phase, the main concerns are operation, maintenance and network updates, e.g. hardware and software. The objectives are to operate the network by performing day-to-day management and to optimize the network with proactive management and design improvements. Finally, the last phase includes the decommissioning of the network.

For each of the nine high-level tasks during the lifecycle, Figure 2 and Figure 3 define sub-tasks on a more fine-granular basis. The definitions for each sub-task along with the required competencies are available in Annex 1 (Section 7) (with identifiers composed of the letter for the high-level task followed by a number indicating the sub-task).

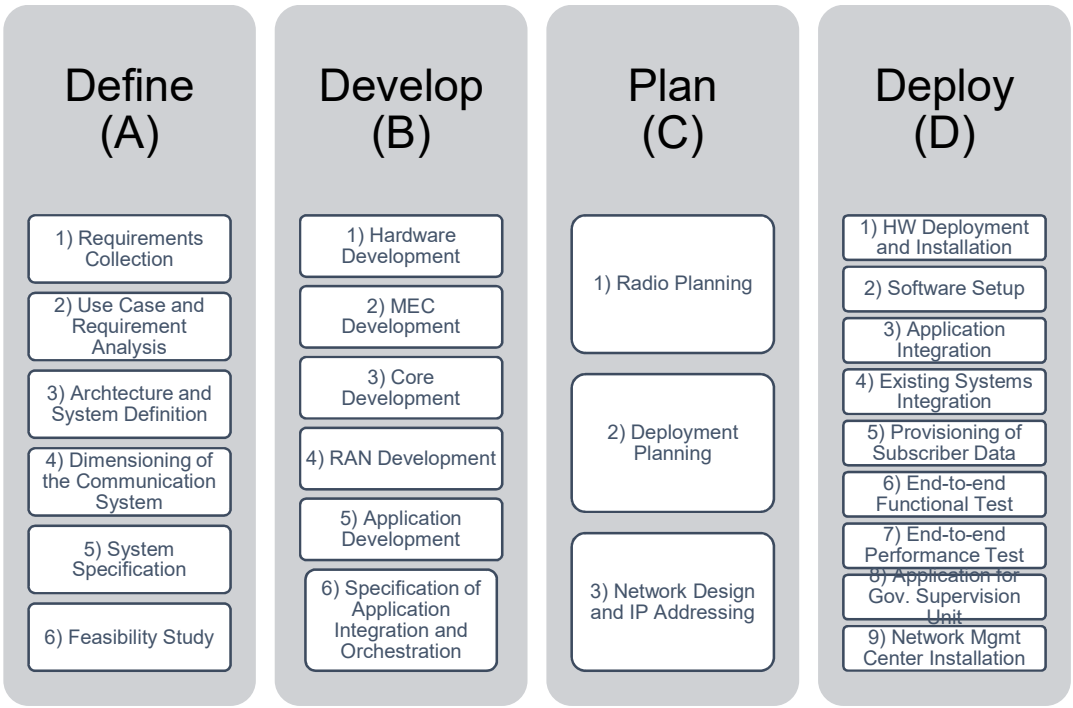

Figure 2 : Tasks and Sub-tasks of Private 5G Networks Life Cycle (Part 1).

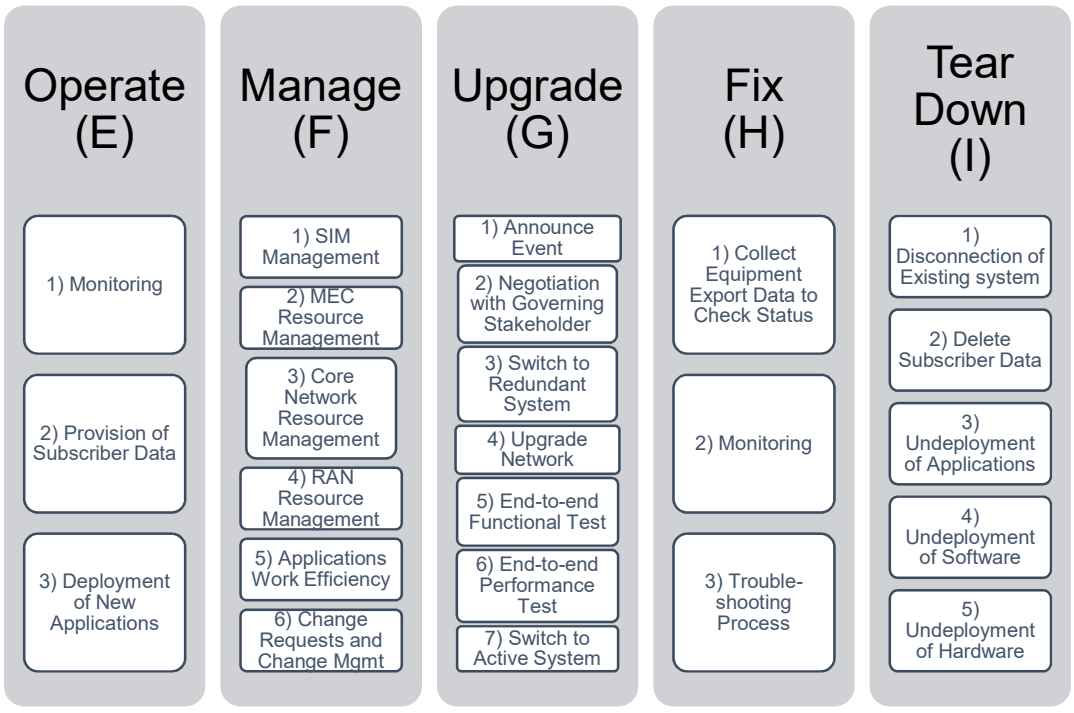

Figure 3 : Tasks and Sub-tasks of Private 5G Networks Life Cycle (Part 2).

3 Characteristics of an Operator Model for Private 5G Networks

This section describes the characteristics of an operator model for private 5G networks. Such an operator model involves a number of dimensions, each of them essential to a concise definition of a particular instance. Section 3.1 describes the operator model dimensions, and Section 3.2 to Section 3.7 analyzes the different interrelationships between the operator model dimensions.

3.1 Description of the Different Operator Model Dimensions

A specific operator model should ideally provide answers to a number of questions, including: Who owns or governs an element (incl. components such as core network, RAN, MEC platform, and applications)? Who is responsible for a certain task and what are the competencies that are required for carrying out that task? What other stakeholders have to cooperate in each task? What elements are touched and/or accessed in each task? And what is the location, at which the element resides or is installed? From the questions above, five different interrelated dimensions can be derived, which are depicted in Figure 4.

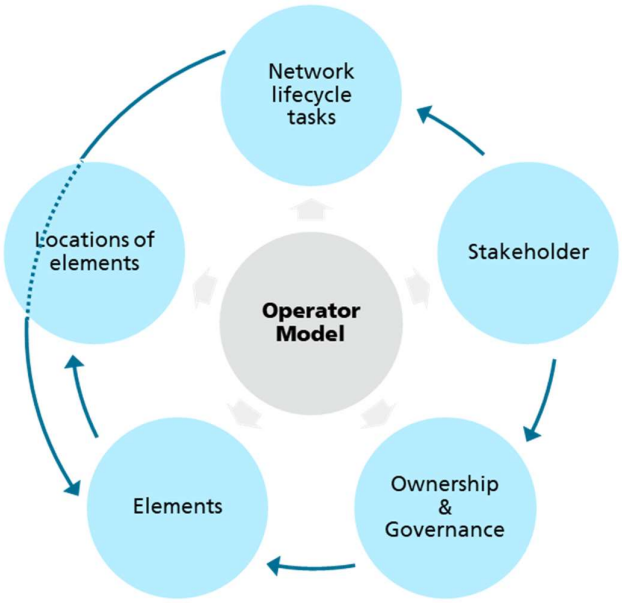

Figure 4: Interrelation between Operation Model Dimensions.

1. **Elements** (see Section 2.3)
   Elements include 5G and non-5G system components, and all other physical and non-physical materials, information, etc. that are being touched during the lifecycle of a private 5G network. Elements must be clearly known in the operator model in order to understand the exact network elements used and how they are related to their locations and the stakeholders in terms of governance and ownership.
2. **Ownership & Governance** (see Section 2.1)
   In the private 5G network, ownership relates to which stakeholder manufactures, produces and owns elements, and governance defines which stakeholder is responsible for management and operation of a certain element.
3. **Stakeholders** (see Section 2.2)
   Stakeholders are organizations, institutions, persons, etc. involved during the entire lifecycle of the network. Responsibilities of stakeholders are defined with respect to all network lifecycle tasks, including the deployment of elements, operations and maintenance,

etc. There are often more than one stakeholder involved in building and operating the private 5G network.

4. **Locations of Elements**
   Possible locations of elements include enterprise data center, enterprise headquarter data center, enterprise site, service/cloud provider central cloud, MNO central cloud MNO edge cloud and MNO site. The locations of elements specify the distribution of 5G elements, i.e. the 5G deployment model or architecture, which has certain implications with respect to the operator model, operation and management;.
5. **Tasks during the lifecycle** (see Section 2.4)
   Point out that the life cycle of the private 5G network and clearly know the detail subtask of the lifecycle. This dimension can be used to know what tasks are involved in building the private 5G network.

Definition of an Operator Model:

An operator model is a logical construct that connects the different dimensions above and, thereby, defines a concrete instantiation of the relationship between every single pair of items belonging to two dimensions, either in the form whether the items are connected or pointing to another item of a third dimension. Therefore, a concrete operator model defines the following:

1. A particular set of tasks during the entire lifecycle of a private 5G network,
2. A particular set of stakeholders that are involved during the entire lifecycle of a private 5G network,
3. The particular information about which stakeholders are involved in (responsible for) a certain task,
4. A particular set of 5G-related elements as well as non-5G-related elements, and the information during which task of the private 5G network lifecycle they play a role, and
5. A particular definition, which stakeholder owns (initially as well as during the lifecycle) and which stakeholder governs a certain element.

Although the previously outlined aspects could already define a certain operator model, not all implications can be derived easily or are obvious to the stakeholders. For example, governance of a certain element could imply that this element needs to be at a certain location (e.g. the edge cloud must be at the Enterprise site such that the Enterprise can have full governance). Another example is that the fact that certain elements are located at different locations imposes limitations with respect to governance, access to an element by a stakeholder, IT security, and many others. In light of these considerations, the following additional information is required to judge the applicability and practicability of operator models:

1. Competencies for each private 5G network lifecycle task, which is required by the responsible stakeholder(s), and
2. The possible locations of elements, especially 5G-related elements (i.e. deployment models).

The subsequent sections shall explore some possible settings (or possibilities for concrete operator models) by presenting, in a generic way, the interrelationship between the dimensions, e.g. in a number of tables. With respect to the private 5G network lifecycle, the different required competencies are explored, as well. While Section 3.2 introduces the possibilities of locations with respect to each element, Section 4 explores the interdependence between operator models and deployment models more elaborately.

3.2 Governance & Ownership of Elements

Table 4 shows the interrelationship between 5G and non-5G elements, and ownership, stakeholder and governance, resulting in a matrix answering the question "Which potential stakeholder owns and governs with elements". It is important to note that each entry represents a list of possible stakeholders, which also implies that, for a particular element, the owning stakeholder can be different from the governing stakeholder. For example, 5G Core functions (e.g. UDM, AUSF, SMF, AMF, UPF, and NEF) are developed by the network equipment vendor (NEV) or service provider (SP), but they can be deployed and governed by the MNO, the service provider or even the enterprise (E). Another example is that the government (G) usually owns the spectrum, but the spectrum is generally used and managed by the MNO, the service provider and/or the enterprise. Furthermore, the initial owner of the MEC platform is either the MNO, a network equipment vendor or a service provider, while the owning and governing stakeholders are the MNO, service provider or the enterprise. Nevertheless, initial ownership, owning stakeholder, and governing stakeholder of some elements can be the same for some elements, such as the control plane data or user plane data. This interrelationship can help enterprises know the cooperative partners who can assist in building and managing the private 5G network, and, of course, explore concerns and requirements regarding certain stakeholders owning and governing particular elements.

Table 4 : Ownership and Governance over Elements.

Element Type	Element	Initial Ownership	Owning stakeholder	Governing stakeholder
5G	Core (UDM, AUSF, SMF, AMF, UPF, NEF)	NEV, SP	MNO, SP, E	MNO, SP, E
	Transport network	MNO/FNO	MNO, SP, E	MNO, FNO, SP
	RAN (DU, CU)	NEV	MNO, SP, E	MNO, SP, E
	SIM	MNO	MNO, SP, E	MNO, SP, E
	5G OAM System	NEV, SP	MNO, SP, E	MNO, SP, E
	Spectrum	G	G, MNO, SP, E	G, MNO, SP, E
	Control Plane Data	E, SP, MNO	E, SP, MNO	E, SP
Non-5G	Application	E, SP	E, SP	E, SP
	MEC Platform	MNO, NEV, SP	MNO, SP, E	MNO, SP, E
	User Plane Data	E	E	E
	WAN Infrastructure	MNO, 3WO, E, 3EC	MNO, 3WO, E, 3EC	MNO, 3WO, E, 3EC
	Shop floor	E	E	E
	Shop floor plan	E	E	E
	Enterprise Network IT	E	E, SP, 3EC	E
	Third-party cloud platform	CP	CP, SP	CP, SP
	Enterprise OAM System	E	E	E
	Enterprise Personnel and/or End Device Database	E	E	E

3.3 Possible Locations of Elements

Elements and 5G elements in particular can be placed at different locations, which has a number of implications with respect to stakeholders being able to operate and manage the system, IT security as data has to be sent over geographically distributed networks, and others. In light of private 5G networks, a number of different locations has to be considered. They are depicted in Figure 5, which also illustrates that some of the sites are farther away (in logical and/or geographical terms) from the end user or end device.

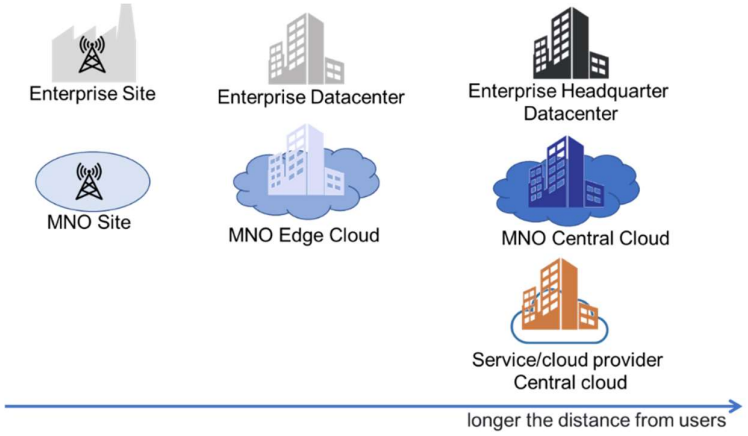

Figure 5: Different Locations of Elements for the Private 5G Network.

1. **Enterprise site**, which is the physical location including the infrastructure on enterprise premises, where the 5G end devices are installed, either inside the factory or a plant.
2. **Enterprise datacenter**, which is a datacenter infrastructure owned and governed by the enterprise, either logically or physically separated from the IT infrastructure at the enterprise site, which means that it can possibly be located off-site. An enterprise can have multiple such enterprise data centers and more than one enterprise site can be connected to the enterprise data center.
3. **Enterprise headquarter datacenter**, which is a datacenter infrastructure owned and governed by the enterprise.
4. **MNO site**, which is the area, where the MNO builds the base stations. This area can be equivalent to the enterprise site in case of a dedicated indoor deployment inside a factory, but it can also be a separate location, for example, if the private network shares the outdoor RAN of the MNO.
5. **MNO edge cloud**, which is a small-localized datacenter infrastructure owned and governed by an MNO.
6. **MNO central cloud**, which is a (partially) public cloud infrastructure owned and governed by an MNO.
7. **Service/cloud provider central cloud**, which is a (partially) public cloud infrastructure owned and governed by a third-party service/cloud provider.

Table 5 shows the possible locations for each of the elements. For example, the 5G Core functions AMF and AUSF can be located as virtualized software functions in the enterprise datacenter, enterprise headquarter datacenter, the service/cloud provider central cloud, the MNO central cloud or the MNO edge cloud. They can be close to the enterprise site, so that the registration and authentication information can be accomplished inside the enterprise IT infrastructure. Alternatively, the AMF and AUSF are placed in the off-premise, i.e. the MNO central cloud, and the registration and authentication procedures are carried through the remote core network. RAN-DU and RAN-CU can be deployed in an enterprise site, or MNO

site depending on deployment models. RAN-DU and RAN-CU can also be deployed according to distance from users, which depends on the performance requirements of the use cases. Another example is the MEC platform, which can to be located at the enterprise site, the enterprise datacenter, the MNO site, or the MNO edge cloud. The location of the MEC platform is also determined according to the requirements of the applications and IT security. The options shown can help enterprises understand the scale of deployment and the implications of the locations of elements in their private 5G networks.

While, from a technical perspective and thanks to the flexible service-based architecture of the 5G System, each and every single element can flexibly allocated to another location, some limitations and interdependencies occur, nevertheless. For example, routing of control and user plane data depends on the location of the respective 5G functions and the co-location of multiple functions actually depends on the concrete setup of a multi-site deployment. Since the different locations are owned and governed by different stakeholders, which are likely to employ varying security concepts, a large number of concerns and requirements actually emerge from the different deployment options and the associated implications on operator models. Hence, a large share of concerns and requirements, which are explained in Section 5, are referring to the different constellations outlined here.

Table 5 : Elements and their Locations, (X)' means technically possible but less likely.

Element Type	Element	Enterprise Site	Enterprise Datacenter	Enterprise HQ Datacenter	MNO Site	MNO Edge Cloud	MNO Central Cloud	SP / CP Central Cloud
5G	Core-UDM	(X)	X	X		(X)	X	X
	Core-AUSF	(X)	X	X		(X)	X	X
	Core-SMF	(X)	X	X		(X)	X	X
	Core-AMF	(X)	X	X		(X)	X	X
	Core-UPF	(X)	X	X		(X)	X	X
	Core-NEF	(X)	X	X		(X)	X	X
	Transport Network	X	X	X	X	X	X	X
	RAN-DU	X	X	X	X			
	RAN-CU	X	X	X	X			
	SIM	X			X			
	5G OAM System		X	X			X	X
	Spectrum	X			X			
	Control Plane Data	X	X	X	X	X	X	X
Non-5G	Application	X	X	(X)		X		
	MEC Platform	X	X		X	X		
	User Plane Data	X	X	X	X	X	X	X
	WAN Infrastructure	X	X	X	X	X	X	X
	Shop floor	X						
	Shop floor plan	X						
	Enterprise Network IT	X	X	X				
	Third-party cloud platform							X
	Enterprise OAM System	(X)	X	X				

	Enterprise Personnel and/or End Device Database		X	X				

3.4 Required Competencies for Private 5G Network Lifecycle Tasks

Because the lifecycle of a private 5G network involves a large number of tasks and related responsibilities and because an operator model essentially assigns them to the different stakeholders, many concerns can arise simply from the fact that very diverse competencies and expertise is necessary. The following explanations attempt to illustrate this clearly.

For example, the architecture and system definition task (see Task A-3), is to define the network architecture according to the specified use case requirements. This requires expertise as network architect with advanced knowledge of 3GPP 5G capabilities and existing solutions. The network architect can select and design the best feasible architectures and systems for the enterprise, which also requires knowledge about existing solutions regarding network slicing, enterprise-dedicated base stations, and core networks, independent networks, and many other applications. Furthermore, the core network development task (B-3) is to configure and install the 5G Core network. In order to configure parameters and install the network functions of the core network, it is necessary to have an in-depth understanding of 5GC network functions, protocols, cloud environments (such as Docker, Kubernetes), and networking solutions. Understanding protocols used between various network functions and virtual environments based on the existing solutions, helps manage, plan, and deploy the 5GC. Another example is the deployment and planning task (C-2). This task includes planning of the site, network component deployment, and discussion for all partners. The site planning action requires shop floor owners to discuss assembly line planning, access point layout, equipment arrangement, and site surveys with enterprises. The network component deployment action is affected by the networking type (such as wireless or wired) and the deployment plan of network components, so enterprises have to consider intranet architecture and restrictions and discuss these network requirements with professional network partners. The discussion action requires close conversations between all corporate partners and technical staff of enterprises for proposing the most feasible deployment plan on the shop floor. So enterprises and partners need to have network technology, 5G component knowledge, and workshop planning capabilities to complete this task by using the above three actions.

An elaborate list of detailed descriptions and required competencies and expertise for each lifecycle task is provided in the Annex of this document (Section 7). In general, the private 5G network lifecycle requires a minimum number of different stakeholders to cover all the expertise requirements in a proper manner, while maintaining low complexity of interactions and organizational effort, when this number grows.

3.5 Elements Touched During Private 5G Network Lifecycle

Most of the required competencies and expertise for each tasks originates from the specific element, on which the task is carried out or for which it is used or required (in general “touched”). Therefore, it is important to specify and analyze which 5G and non-5 G elements are affected by, touched by, or required for a certain task during the lifecycle of a network.

For example, end-to-end functional testing of deployment phase (D-6) is a very important step because it can show the stability, safety, and availability of the function. Availability is related to the transmission capacity of the 5G network and the cooperation of applications on the MEC platform, such as data transmission on the 5G network and data processing of applications on the MEC platform. Enterprises and MEC platform owners must consider stability and security, such as SIM card management, limits of MEC platform operational capacity, and long-term operation of the OAM system. Therefore, end-to-end functional testing is related to network

elements related to stability, security, and availability. Another example is the following. Deployment of new applications of operation phase (E-3) is the most basic and important task. This task can be used to update or modify the functions of applications belonging to enterprises, and these applications are usually deployed on the MEC platform. Therefore, MEC platform owners must consider the standard procedures for changing applications, and enterprises must consider the stability and security of applications deployed on the MEC platform. For the above reasons, the enterprise and MEC platform owners must be responsible for this task together. Furthermore, management of applications efficiency (F-5) is an important task for enterprises. Since some enterprise applications are used in precision industries, they cannot allow any efficiency problems. Those applications are usually deployed on the MEC platform and belong to enterprises. Therefore, both enterprises and MEC platform holders must be responsible for the efficiency of the application. Enterprises are responsible for application efficiency, and MEC platform owners are responsible for the efficiency of data transmission and MEC platform.

An elaborate list of elements touched during each of the private 5G network lifecycle tasks is provided in the Annex (Section 8).

3.6 Possible Acting Stakeholders for Private 5G Network Lifecycle Tasks

What already became obvious is that the different private 5G network lifecycle tasks require diverse requirements that can only be covered by multiple interacting stakeholders. Table 6 shows potentially acting (but not necessarily owning/governing) stakeholders for each of the lifecycle tasks. It also illustrates which stakeholder might require interaction during particular tasks.

For example, during the upgrade phase, negotiation with governing stakeholders (G-2) is an essential step for all partners. Enterprises, service providers and MNOs have to announce upgrade messages to all stakeholders that will be affected. Each of them must evaluate the extent of the impact of updating and give an updating report to, for example, the enterprise. Enterprises have to evaluate these reports to consider a feasible negotiation solution, then enterprises and other stakeholders can evaluate the feasible negotiation solution and come up with an executable solution. Another example is the monitoring task (H-2), which provides a real-time monitoring service of the system for stakeholders. But monitoring parameters must be provided by each stakeholder of various fields because the individual partners know, which parameters need to be monitored and how to verify that the values of parameters are correct in their field of expertise. Therefore, each stakeholder will contribute their expertise to maintain the stability, efficiency, and safety of the system. Also the teardown phase is of importance here. Deletion of subscriber data (I-2) is an important operation for enterprises, because enterprises need to confirm the necessary data has been backed up and the data of the MEC platform has been deleted. Therefore, MEC platform owners need to assist enterprises in deleting the data of enterprises on MEC platforms. If necessary, MEC platform owners also need to help enterprises transfer the required data to the target database. The data of applications also need to be performed above operations, so enterprises and service providers have to delete and transfer the data of applications together. When the application data processing is completed, this task is also completed.

Summarizing, each task requires diverse expertise that can be brought in by a number of stakeholders. Nevertheless, this alone can cause stakeholders raising some concerns, for example, regarding sharing information, cost and complexity implications if additional stakeholders need to be involved.

Table 6 : Lifecycle Tasks and Possibly Involved Stakeholders.

Task	MNO	SP	E	NEV	CP	3SI	3NP	3WO	G	3EC	PS
A-1	X	X	X	X	X	X	X	X	X	X	X
A-2	X	X	X	X	X	X	X			X	
A-3	X	X	X		X	X	X			X	
A-4	X	X	X		X	X	X	X		X	
A-5	X	X	X		X	X	X			X	
A-6	X	X	X	X	X	X	X			X	X
B-1	X	X	X	X	X	X		X		X	
B-2	X	X	X	X	X					X	
B-3	X	X	X	X	X						
B-4	X		X	X			X	X			
B-5	X	X	X		X	X				X	
B-6	X	X	X	X	X					X	
C-1	X	X	X	X			X		X		
C-3	X	X	X	X	X	X		X			
D-1	X	X	X	X	X	X	X	X		X	X
D-2	X	X	X	X	X	X	X			X	
D-3	X	X	X	X	X	X				X	
D-4	X	X	X	X		X				X	
D-5	X	X	X								
D-6	X	X	X	X	X	X	X	X		X	
D-7	X	X	X	X	X	X	X	X		X	
D-8	X	X	X			X			X	X	
D-9	X	X	X	X	X	X					
E-1	X	X	X	X	X					x	
E-2	X	X	X								
E-3	X	X	X		X	X				x	

Task	MNO	SP	E	NEV	CP	3SI	3NP	3WO	G	3EC	PS
F-1	X	X	X								
F-2	X	X	X		X						
F-3	X	X	X		X						
F-4	X	X	X				X				
F-5	X	X	X		X						
F-6	X	X	X	X	X						
G-1	X	X	X		X						
G-2	X	X	X	X	X	X				x	
G-3	X	X	X		X	X	X	X			
G-4	X	X	X	X	X	X					
G-5	X	X	X	X	X	X	X	X		X	
G-6	X	X	X	X	X	X	X	X		X	
G-7	X	X	X		X	X					
H-1	X	X	X	X						X	
H-2	X	X	X	X	X		X			X	
H-3	X	X	X	X	X	X	X	X		X	
I-1	X	X	X	X	X					X	
I-2	X	X	X		X					X	
I-3	X	X	X		X					X	
I-4	X	X	X	X	X	X				X	
I-5	X	X	X	X	X	X		X		X	X

4 Interdependence between Operator and Deployment Models

According to the private 5G network architectures defined in WP2 (D2.1), the 5G CONNI project considers four models: fully private, MVNO, hybrid and MNO's private core network. The objective of this section is to explain how a deployment model could have an impact on the feasibility of an operator model. Each operator model has its peculiarities and restrictions. Besides the MNO's private core network model, the rest of them include an enterprise core network.

The deployment strategy of private 5G networks can deploy single operator model or multiple operator models based on coverage and KPI requirements or some constraints imposed by the regulators. For example, the enterprise can deploy either a fully private model or MNO's private model. The enterprise may also deploy both MVNO model and Hybrid model at different sites. While some enterprise sites use MNO RAN network for wireless data transmission, some other enterprise sites construct its dedicated RAN network for better wireless coverage or capacity demand. Another example is a global enterprise, which may also deploy both fully private model and MVNO model at different sites. While the enterprise private core network is located at the enterprise headquarters, some branches may not be able to setup its dedicated RAN network regarding the ownership of spectrum or the regulations per country. Those enterprise branches may deploy a MVNO model instead.

Each 5G-related element can be physically and logically "located" at different systems, platforms or locations. The different locations that could be taken into account for distributing the elements are listed in Table 5. In the following subsections, we consider the relationship to governance and ownership of such 5G-related elements and implications such a placement of a 5G-related element at a location can have on the possible owning and governing stakeholders.

4.1 Impact of 5G-related Element Locations on Ownership and Governance

This section describes the relationship of 5G elements at the location of enterprise, SP, CP, and MNO regarding control, governance and ownership.

4.1.1 Enterprise domains

The enterprise domain locations include enterprise data center, enterprise headquarter data center and enterprise site. When the enterprise deploys a multi-site private 5G network, the location of the enterprise private 5G core network can be the enterprise headquarter data center for centralized management.

4.1.1.1 Relationship to governance and ownership

The possible deployment locations of 5G Elements defined in Table 2 will impact the ownership and governance on the different stakeholders involved in private 5G network. Having 5G elements at enterprise locations excludes certain stakeholders as governing or owning entities as shown in Table 7. For example, when an enterprise deploys a fully private 5G network and the enterprise owns its dedicated 5G Core and RAN at the enterprise location, the MNO and SP possibly have no ownership and governance to the 5G elements.

Table 7 : Relationship to governance and ownership in enterprise domains

Enterprise Location	5G Element	No Ownership Stakeholders	No Governance Stakeholders
Enterprise Datacenter	Core-UDM / Core-AUSF / Core-NEF	MNO, SP	
	Core-SMF / Core-AMF / Core-UPF / Transport Network / 5G OAM System	SP	
	Control Plane Data	SP, MNO, CP	
Enterprise Site	RAN-DU / RAN-CU	MNO, SP	
	Transport Network	MNO, SP	
	Spectrum	MNO, SP	
	SIM	SP	

4.1.1.2 Relationship to the stakeholders that act on the element

The possible deployment locations of 5G-related elements will impact the relevant tasks of the different stakeholders involved in a private 5G network. The relevant tasks from network deployment to eventually tearing it down have been depicted in previous Figure 2 and Figure 3. A summary of having 5G-related elements at enterprise locations possibly excluding certain stakeholders task responsibilities is provided in Table 8.

Table 8 : Relationship to the stakeholders that act on the element in enterprise domains

Enterprise Location	5G Element	No Task Action Stakeholders
Enterprise Datacenter	Core-UDM / Core-AUSF / Core-NEF	3NP, 3WO, G
	Core-SMF / Core-AMF	3WO, G
	Core-UPF	CP, G
	Transport Network	SP, CP, 3NP, G
	5G OAM System	CP, 3NP, G
	Control Plane Data	NEV, CP, 3NP, 3WO, G
Enterprise Site	RAN-DU/ RAN-CU	SP, CP, 3WO, G
	Transport Network	SP, CP, 3NP, G
	Spectrum	SP, CP, 3WO
	SIM	NEV, CP, 3WO, G

4.1.2 Service provider domains

The service provider domains locations include service/cloud provider central cloud. Service/cloud provider central cloud, which is a (partially) public cloud infrastructure owned and governed by a third-party service/cloud provider.

4.1.2.1 Relationship to governance and ownership

The possible deployment locations of 5G Element will impact the ownership and governance of the different stakeholders involved in private 5G network. Having 5G elements at SP / CP central cloud locations possibly excludes certain stakeholders as governing or owning entities as shown in Table 9**Erreur ! Source du renvoi introuvable.**. For example, when the service provider deploys enterprise 5G network in conjunction with the public network, the enterprise 5G CN is owned and governed by service provider, the MNO and SP have no ownership and governance to the 5G elements.

Table 9: Relationship to governance and ownership in service provider domains

Location	5G Element	No Ownership Stakeholders	No Governance Stakeholders
SP / CP central cloud	Core-UDM / Core-AUSF / Core-NEF / Core-SMF / Core-AMF / Core-UPF	MNO, E	
	Transport Network	E	
	Control Plane Data	E, MNO, CP	

4.1.2.2 Relationship to the stakeholders that act on the element

The possible deployment locations of 5G-related elements will impact the relevant tasks of the different stakeholders involved in a private 5G network. The relevant tasks from network deployment to eventually tearing it down have depicted in previous Figure 2 and Figure 3. A summary of having 5G-related elements at SP / CP central cloud locations possibly excluding certain stakeholders task responsibilities is provided in Table 10.

Table 10 : Relationship to the stakeholders that act on the element in service provider domains

Location	5G Element	No Task Action Stakeholders
SP / CP central cloud	Core-UDM / Core-AUSF / Core-NEF	3NP, 3WO ,G
	Core-SMF / Core-AMF	3WO, G
	Core-UPF	CP, G
	Transport Network	MNO, E, 3NP, G
	5G OAM System	MNO, E, CP, 3NP, G
	Control Plane Data	MNO, E, NEV, CP, 3SI, 3NP, 3WO, G

4.1.3 MNO domains

The MNO domain locations include MNO edge cloud, MNO central cloud and MNO site. The MNO edge cloud is a small localized datacenter infrastructure owned and governed by an

MNO. The MNO central cloud is a (partially) public cloud infrastructure also owned and governed by an MNO.

4.1.3.1 Relationship to governance and ownership

The possible deployment locations of 5G Element will impact the ownership and governance on the different stakeholders involved in private 5G network. Having 5G elements at MNO domain locations possibly excludes certain stakeholders as governing or owning entities, as shown in Table 11. For example, when an MNO deploys a private 5G network in an MNO central cloud, the private 5G Core is owned and governed by MNO, the enterprise and SP have no ownership and governance to the 5G elements.

Table 11 : Relationship to governance and ownership in MNO domains

MNO Location	5G Element	No Ownership Stakeholders	No Governance Stakeholders
MNO Edge Cloud	Core-UDM / Core-AUSF / Core-NEF	MNO, SP	
	Core-SMF / Core-AMF / Core-UPF / RAN-CU / Transport Network / 5G OAM System	E, SP	
	Control Plane Data	E, SP, CP	
MNO Central Cloud	Core-UDM / Core-AUSF / Core-NEF Core-SMF / Core-AMF Core-UPF Transport Network 5G OAM System	E, SP	
MNO Site	RAN-DU / RAN-CU / Transport Network /Spectrum	E, SP	

4.1.3.2 Relationship to the stakeholders that act on the element

The possible deployment locations of 5G-related elements will impact the relevant tasks of the different stakeholders involved in private 5G network. The relevant tasks from network deployment to eventually tearing it down have depicted in previous Figure 2 and Figure 3. A summary of having 5G-related elements at MNO locations possibly excluding certain stakeholders task responsibilities is provided in Table 12**Erreur ! Source du renvoi introuvable.**. For example, when the 5G Core-UPF is located at MNO edge cloud, the involved stakeholder to carry out relevant tasks could be enterprise, service provider, MNO, 3rd-party SI, 3rd-party NP and 3rd-party WAN operator.

Table 12: Relationship to the stakeholders that act on the element in MNO domains

MNO Location	5G Element	No Task Action Stakeholders

MNO Edge Cloud	Core-UDM / Core-AUSF / Core-SMF / Core-AMF	E, CP, 3NP, 3WO, G
	Core-UPF	CP, G, G
	Core-NEF	E, CP, 3SI, 3NP, 3WO, G
	Transport Network	SP, E, CP, 3NP, G
	5G OAM System	E, CP, 3NP, G
	Control Plane Data	SP, E, NEV, CP, 3SI, 3NP, 3WO, G
	RAN-CU	SP, E, CP, 3WO, G
MNO Central Cloud	Core-UDM / Core-AUSF / Core-SMF / Core-AMF	E, CP, 3NP, 3WO, G
	Core-UPF	CP, G
	Core-NEF	E, CP, 3SI, 3NP, 3WO, G
	Transport Network	SP, E, CP, 3NP, G
	5G OAM System	E, CP, 3NP, G
	Control Plane Data	SP, E, NEV, CP, 3SI, 3NP, 3WO, G
MNO Site @ Base Station	Transport Network	SP, E, CP, 3NP, G
	RAN-DU/ RAN-CU	SP, E, CP, 3WO, G
	SIM	E, NEV, CP, 3WO, G
MNO Site @ edge site	Spectrum	SP, E, CP, 3WO

4.2 Considerations on Operator Models Mapping to Architectures

In this subsection, we discuss the impact of mapping operator models to an architecture. The mapping from an architecture or deployment model to an operator model will be done in the final report on private 5G network architecture and operator models (D2.2) of WP2.

The ownership of elements plays a central role for the mapping of operator models to the architecture. The easiest case is when the enterprise owns elements from the user devices to the applications. In this case, the enterprise will have access to the RAN elements, the transport networks, and the core network. In this case, the USIM cards belong to the enterprise. It is the same if the enterprise deploys its own core network and applications but the RAN is shared and connected to both the MNO and enterprise's core networks. The USIM cards still belong to the enterprise. But in a hybrid model where the enterprise owns its radio and core network, the enterprise user can access both the MNO network and the private network under some roaming agreements. In the extreme case, in the MNO's private network, the enterprise owns its application where 5G elements and USIM cards are owned by MNO. Depending on the mapping, users must register or subscribe to both private network and MNO network or only to a private network.

The governance (i.e. management and orchestration) and the required competencies must also be taken into consideration when the operator models are mapped. The enterprise could need specialized telecoms engineers to setup and maintain its own elements whereas third parties will mainly need system integration team and MNO will govern elements.

Some considerations must also be done on spectrum allocation. The private 5G network can use licensed spectrum with the permission of the MNO license owner or government authorized private spectrum or unlicensed band.

Finally, before selecting an operator model mapping to an architecture, we should also consider some KPIs. The latency depends on the data path in a certain operator model. In fact, the traffic can be sent to private edge servers only or to both the cloud server and edge server and these servers can be physically or logically located on-site, in local data center or in cloud center. Considerations about security are also important and highly depend on the data path and control path in a certain operator model.

5 Concerns and Requirements Regarding Operator Models

After having explored the fundamentals of operator models and, thereby, making this new field accessible, this section lists and explains concerns that can be raised by all the relevant stakeholders. As explained in Section 3.1, an operator model is defined by sets of stakeholders, tasks and elements, as well as by the information, which stakeholder is involved in a certain task and which stakeholder owns and governs elements, in particular 5G elements. In contrast, a deployment model (or architecture) specifies, at which location certain elements are installed. As both aspects (operator and deployment models) go hand-in-hand, the location of 5G elements need also explicit consideration for the identification of concerns and requirements regarding operator models. In fact, certain deployment models can imply aspects of operator models and vice versa, as outlined in the previous section. Figure 6 illustrates, on a high level, how a stakeholder raises concerns (and associated requirements and their criticality). Concerns can arise on each interface between the dimensions but also for an entire operator model construct. They can be related to the dimension itself, or they are related to another aspect, such as an IT security concept, which is not an explicit part of an operator model.

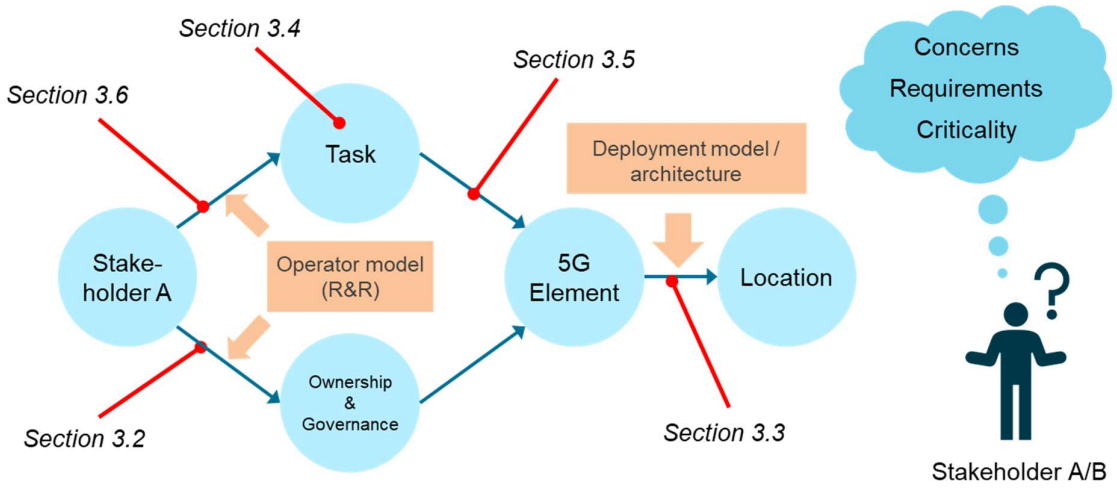

Figure 6: Concerns and Requirements by a Stakeholder Regarding an Operator Model.

In general, concerns can be grouped into a number of categories and sub-categories. The categories that are found with the model above are: Confidentiality, integrity and availability; Access to and control of elements; Private 5G Network Lifecycle; Regulations; and Applicability and practicability. They are shown in Figure 7 along with their sub-categories, which themselves contain the actual concerns and requirements.

While the different concerns and requirements are explained in the subsequent sections, they are also listed in a more structured way in the Annex (Section 9) along with an evaluation of their importance.

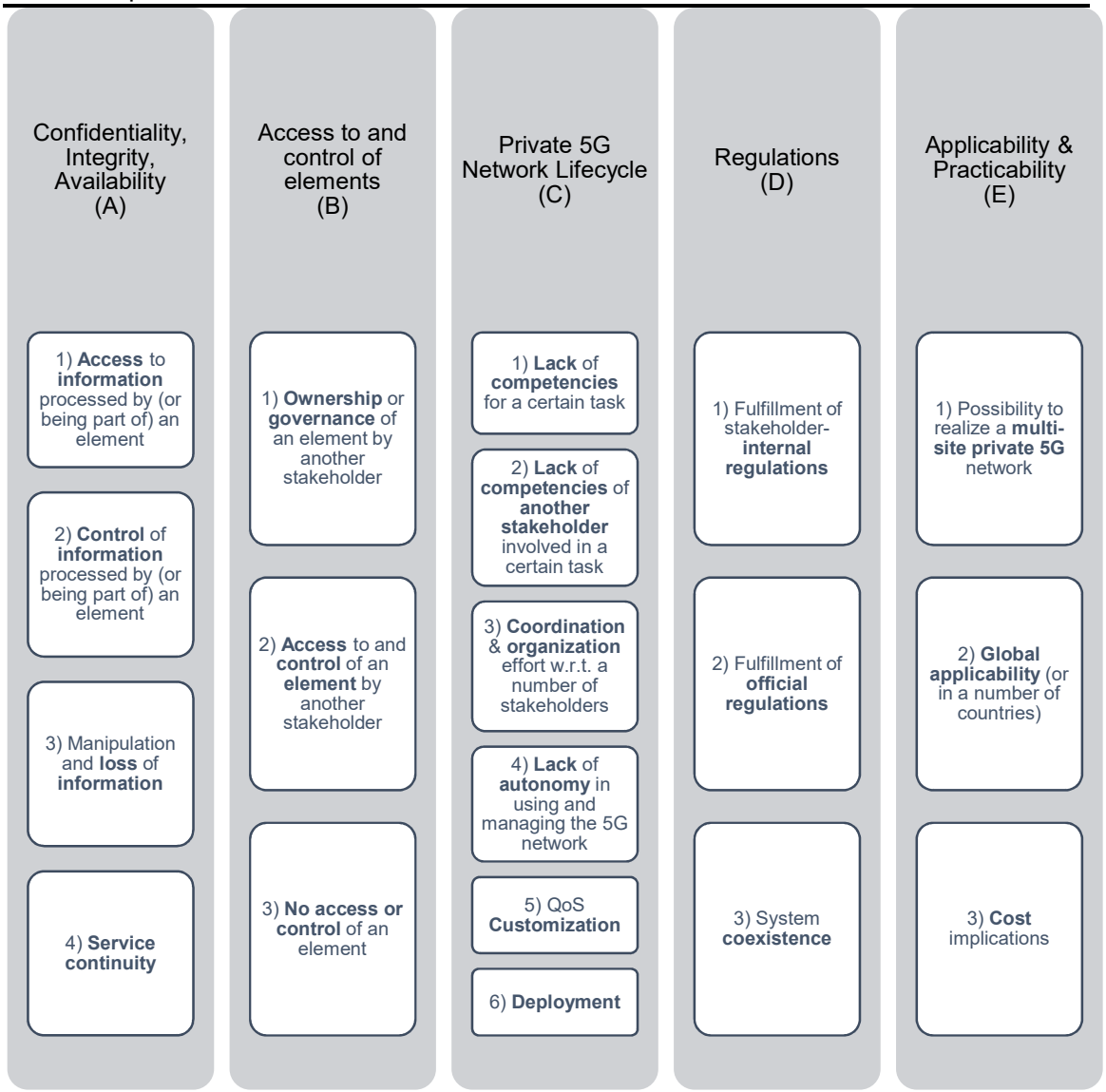

Figure 7: Categories for Concerns Regarding Operator Models

5.1 Concerns Regarding Confidentiality, Integrity and Availability

Confidentiality, integrity and availability of information are the three main pillars regarding IT security, and in particular important to any enterprise that uses a private 5G network, for example, in manufacturing. Here, any information, such as production process data, needs appropriate protection, which is even more important if any other stakeholder is involved in the operation of underlying IT infrastructure. Hence, this section explores the concerns and requirements regarding operator models in the context of information security.

5.1.1 Access to information processed by or being part of an element

Due to its modularity, the 5G System allows for a flexible distribution of network functions, which are responsible for both, control and data plane. The ability to access or even actually accessing information processed by such an element can raise concerns for another stakeholder, in particular, for the enterprise. Also, other information that needs to be accessed and used during the design and deployment phases of the private 5G network lifecycle that is of importance to any stakeholder needs to be considered.

Accessing and exploiting user plane data that is owned by the enterprise through another party can cause considerable damage to the enterprise. Therefore, a certain operator model must ensure that any third party does not have the technical ability to access user plane data (e.g. routed by the UPF) for confidentiality reasons. If another party manages the UPF, it must be technically or by contract ensured that user plane data is not accessible by that third party. In this regard, encryption of user plane data plays a significant role. Depending on the deployment and operator model, stakeholders other than the owner of user plane data or even attackers could get access to a 5G element, which is involved in network-driven encryption/decryption (such as a gNB), and exploit vulnerabilities. Therefore, a certain operator model should ensure that any third party cannot have access to an element (5G or non-5G), which is involved in decrypt/encrypt processes, in particular, if no application layer or other end-to-end encryption can be employed, for example, for URLLC applications. Another concern with respect to confidentiality and integrity is the usage of an off-premise MEC platform, which is not owned or governed by the enterprise. In particular, access to an application running on such a platform or information processed by that application by an attacker can cause substantial damage to an enterprise. Therefore, for a certain operator model, no other party or tenant shall have the technical ability to access the Enterprise's application on the MEC platform or information processed by that application. Other concerns regarding operator models are related to operation and management of the private 5G network. For instance, a management system, such as the operations support system (OSS) requires access to information from another system, for example, owned and governed by the enterprise. Such systems could, for example, be enterprise personnel and/or end device data bases. Because such information is highly sensitive, an operator model must ensure that there is no or only necessary/essential access to information of an enterprise personnel and/or end device data base by any other third party and that the highest security standards are employed. This is even more important if open architectures are employed to provide functionalities for end-to-end management systems with global applicability. Furthermore, the design and deployment phases require access to elements or sensitive information of element that also could raise concerns. One example is that access to the shop floor and shop floor plan can already be seen as critical by a manufacturing enterprise, such that access shall be restricted only to authorized non-enterprise stakeholders.

5.1.2 Control of information processed by or being part of an element

Control of information and also control over how information is processed in terms of security measures are two other important aspects, which play a role in terms of concerns and requirements regarding operator models.

For example, in an MNO-operated model, the local network security concept of an enterprise needs to be modified or aligned with the one of the MNO, such that it could potentially weakened. Here, the enterprise and the operator need to analyze possible infrastructure vulnerabilities and attack vectors that could occur with a chosen architecture and define measures to avoid them. Also, the effectiveness needs to be checked by frequent intrusion checks. In addition, the design of an architecture (or deployment model) that results from an operator model and the measures outlined above have to be carried out in a manner, such that they are future-proof, when it comes to adding different use cases. In fact, another concern in this regard is that the requirements to protect critical data transported via an infrastructure operated by a third-party can't be fulfilled for each application. Therefore, analysis must be carried out whether current and future use case requirements can be fulfilled by a certain operator model (that implies an architecture/deployment model). SLAs can be contractual measures in this respect. One specific aspect here and with respect to IT security is the following. Encryption keys for confidentiality and integrity protection are used and processed

by a number of different 5G elements, including the gNB, AMF, AUSF, and UDM. A strong concern by the enterprise is that such keys are not directly accessible, manageable and controllable by the enterprise, in particular, if the UDM is governed by the MNO. Hence, in an MNO-operated model, the UDM and encryption keys shall ideally be accessible and governed by the enterprise.

5.1.3 Manipulation and loss of information

Not only access to sensitive information by another party or attacker but also its manipulation or loss can cause considerable damage to the owner of the data. Hence, stakeholders need to consider such concerns when designing an operator model, too.

In general, there may be a concern that vulnerabilities in one stakeholder's security concept can lead to attacks in other stakeholder networks, which can apply for a number of stakeholders including the enterprise, a service provider, or the MNO. Thus, for operator models, in which different security concepts are in place for the different stakeholder, vulnerabilities in one stakeholder's security concept need to be identified and mitigated, e.g., through vulnerability tests and potential redesign of the security concepts, if necessary. Similar to the access of sensitive information, data manipulation through intrusion attacks, especially in the case where a third-party operates the 5G network, are of large concern pre-dominantly by the enterprise. Proper network design and architectures shall be possible with a certain operator model, such that intrusion attacks are prevented; otherwise, contractual agreements shall be put in place. Another concern is that network and storage events are not fully under control by the enterprise in case another stakeholder is involved in the operator model, which leads to data being lost or corrupted. As a consequence, for operator models that imply a certain architecture/deployment model, data loss and corruption must be prevented, e.g. through appropriate redundancy concepts. Finally, an operator model needs to specify policies and processes in order to handle such events, which includes tracking mechanisms for the manipulation and loss of information. Here, such events need to be recorded by components and elements, which can send corresponding notifications to appropriate personnel.

5.1.4 Service continuity

Availability not only refers to information but also a service; in this case, the connectivity service of the private 5G network. Such concerns are considered by the enterprise, the service provider and the MNO likewise.

Interruption due to failures of the system are general concerns by the user and the provider of the service. In such a case, the stakeholder needs to find the source of interruption quickly, which requires status reports by other stakeholders, as well as, a hotline or quick response team. Another measure in this regard is that the MNO and/or network equipment vendors setup network redundancy plans, which ensure that there are no single points of failure, i.e., components whose failure would otherwise cause the shutdown or unavailability of the entire communications system. Finally, MNOs, service providers and other stakeholders require software or hardware updates of individual system components (5G elements). Such situations can lead to unwanted unavailability of the service, either because redundancy concepts fail during system updates or because such planned maintenance is not well aligned among the stakeholders. Here, system redundancy and appropriate maintenance schedules are important requirements.

5.2 Access to and Control of Elements

Because deployment and operator models are intertwined, another group of concerns and requirements are related to the aspects of access to and control of elements, be it 5G elements or non-5G elements. In contrast to access to and availability of information, this group is

specifically related to the interactions (and restrictions thereof) of stakeholders involved in certain lifecycle tasks with corresponding elements. Such concerns are then usually raised because other stakeholders are involved in certain tasks or by the fact that there is only limited access to and control of elements.

5.2.1 Ownership or governance of an elements by another stakeholder

This category includes concerns and requirements of one stakeholder related to the ownership and governance of particular elements by another stakeholder. They are also partly related to IT security, (unallowed) access, maintenance and extensibility of the system.

The two most important concerns regarding ownership and governance are the following. Ownership and governance over the spectrum by the enterprise could raise concerns regarding the proper handling of the spectrum, e.g., in terms of interference management, especially in the case of spectrum sub-licensing from the MNO. As a consequence, for any operator model, governance and responsibility about the spectrum shall ideally be taken by an appropriate stakeholder and/or by having the required competencies/expertise. The other aspect is that ownership and governance of the MEC platform and a third-party cloud (e.g. for the application and the 5G Core functions) by a service provider raises concerns for the enterprise regarding confidentiality and integrity of the processed information and the applications that run on those platforms. Hence, in an ideal case, the enterprise has governance over the cloud/MEC platforms, or parts of them, to ensure confidentiality and integrity of the application and the information processed by the application. Another important concern relates access and service availability. Depending on the location of certain elements, stakeholders have less control in case of physical damage of 5G elements due to vandalism, accidents, or premises outages (air conditioning, power, etc.). An operator model must therefore ensure that unallowed access to third-party equipment is restricted and that environmental conditions are closely monitored. In this regard, another concern is that, e.g., an enterprise, cannot counteract quickly enough in case of outages, etc., when it has no governance over certain elements. As a result, the MNO and/or service provider needs to provide means for the enterprise to monitor network health status information, for example, through appropriate monitoring dashboards or APIs towards elements. Finally, stakeholders and the enterprise in particular, want to carry out certain management tasks without requiring to interact with other stakeholders. In this regard, limited extensibility concerning use cases and the number of end devices is a major concern. For an MNO-operated model, the MNO should guarantee means for the enterprise to carry out such tasks by himself/herself. For instance, this could be achieved by providing SIM card provisioning tools along with UDM user provision interfaces to enlarge the UE pool.

5.2.2 Concerns of a stakeholder regarding the access to and control of an element located at a certain location by another stakeholder

Another set of concerns and requirements arises from the fact that stakeholders have access to certain elements, which might not be preferred by another stakeholder.

In particular, a major concern arises for the MNO and service providers, which have 5G components installed at the enterprise's premises. For any such operator model, uncontrolled physical access or compromising components shall be prevented, e.g. though components being mounted in access controlled areas/cabinets. In close relation to this, involved stakeholders (MNO, service provider, enterprise, etc.) are required to establish reasonable authority control to avoid wrong access by unrelated personnel.

5.2.3 No access to or control of an element located at a certain location

While there might be some concerns by a stakeholder regarding another stakeholder accessing elements, concerns regarding only limited or no access at all are more severe as they are more related to emergency/outage cases or necessary remote access/maintenance.

Limited access is a concern shared by different stakeholders. On the one hand, MNOs or service providers cannot carry out emergency maintenance on premise 24/7 in the case when the premises are closed or access is restricted. An appropriate operator model shall implement a proper emergency maintenance plan with a 24/7 field service concept. On the other hand, enterprise personnel wants to carry out urgent maintenance tasks by himself/herself, even if 5G elements, such as the RAN RU, DU or CU, or the I-UPF are not directly accessible by an enterprise as they are governed by the MNO. Here, an operator model requires a plan to enable such tasks for the enterprise, e.g., through providing shutdown and restart procedure manuals to the enterprise. Concerns regarding limited remote access can also be raised by multiple stakeholders. Firstly, the MNO or service provider raises concerns if there is no appropriate or only restricted access to 5G elements including the transport network, when they are located at a location owned by the enterprise. As a result, the enterprise shall provide sufficient access to 5G elements to the SP or MNO considering the risks associated. This can, for example, be accomplished by setting up MPLS VPN connections with firewall and network quarantine policies. Secondly, remote access to stakeholder's equipment can be interrupted because of failure in the transport environment. As a consequence, the impact of failure shall be minimized, e.g. through implementing an out-of-band management concept. The third aspect relates, again, to the management of the MEC platform (or parts of it) through the enterprise, while the platform is not located on the enterprise's premises. Specific concerns in this regard are limited accessibility in general, lack of being able to manage the platform and the risk of low integrity (of data and the application). Hence, a requirement could be that the MEC platform shall be well accessible by the enterprise for management purposes, even it is located off-premise and owned by another stakeholder. In general, stakeholders are required to work together, e.g. by making clear location access requirements and defining appropriate interfaces to access elements.

5.3 Private 5G Network Lifecycle

Private 5G networks offer new business opportunities and allow the coexistence of multiple stakeholders on their infrastructure in order to be tailored to the specific needs of the enterprise. It is not always easy to manage the private 5G network lifecycle and even less when the requirements are very specific. Operator models must allocate the roles and the responsibilities to the stakeholders in each task according to their competencies, must provide them enough autonomy to accomplish their action, must organize each task and coordinate each stakeholder. In this section, we focus on concerns and requirements related to multiple stakeholders' ecosystem and to tasks realization.

5.3.1 Lack of competencies for a certain task

This category includes concerns and requirements of one stakeholder to carry out a certain task by himself. For the enterprise, the efficient management of the private 5G network is essential and the issue of required competencies and outsourcing remains crucial. The Enterprise might not have required competencies for the following tasks:

- Network architect with advanced knowledge of 5G capabilities and existing solutions,
- Network designer dimensioning of the communication system,
- RF expert with instrument knowledge for experiment,

- Solution architect and developers to specify and develop each component of the end-to-end private 5G network,
- Radio planning and RF experts adapting and configuring the solution for the deployment in the specific site,
- Network operators managing the access, monitoring / analyzing the network statics and repairing network anomalies.

For any operator model, certain tasks require specialized competencies. The enterprise can build up expertise or can involve other stakeholders with limited amount of effort and at low cost. For example, If the stakeholder's first level support is not familiar with local 5G set up, the enterprise can elaborate and improve operating concept based on contracts with the service provider and can train his personnel.

Finally, network designers have to understand the specific context of the 5G private network and the network regulations of enterprises since they need to design the network architecture under these specifications. Thus, the network architects of enterprises must explain network configuration principles and restrictions to network designers.

5.3.2 Lack of competencies of another stakeholder

This category includes concerns and requirements about another stakeholder not having the required competencies to carry out a certain task. If the outsourcing service provider cannot prove its know-how or carry out a task, the different stakeholder must interact with each other and make some trade off during the private 5G network lifecycle.

In the use cases and requirements analysis (A-2), the expertise knowledge of the enterprise can affect the analysis accuracy. Thus, the enterprise can explain his expertise knowledge to partners and can train his personnel for improving the analysis accuracy of use cases and requirements. If Enterprise is involved in the private 5G lifecycle, the MNO or the service provider can raise concerns regarding the proper O&M of the Enterprise, especially regarding liability and can provide their support for certain tasks. In this case, the total number of stakeholders and coordination effort need to be minimized. If some specialized features, once implemented have decreasing or missing support, the enterprise must ensure that specialized features of a private 5G network solution shall be supported during the entire private 5G network lifecycle. Moreover, some stakeholder demands can lead to decrease in MNO's/service provider's standards and automation procedures. Thus, a compromise between fulfilling a stakeholder's (especially the enterprise's) demands and keeping up the MNO's/service provider's standards and automation procedures shall be found for a certain operator model.

5.3.3 Coordination and organization effort

The main concern in the private 5G network lifecycle is about coordination and organization of the effort with respect to the number of stakeholders. The flexibility of the private 5G network enables the customized network deployment by several stakeholders. It establishes a relationship of trust between stakeholder competencies.

During the phases A-D, a larger number of stakeholders need to be involved, potentially causing delays, many iterations in finding a solution and architecture that is appropriate. Coordination effort shall be minimized and activities shall be bundled within a small group of stakeholders avoiding delay and excessive iterations on finding a solution. Long delays can also happened for configuration, fault management and upgrades, when another stakeholder (service provider or MNO) is less responsive, potentially causing damage to the enterprise. The responsiveness is essential in case of breakdown or hacking. An operator model shall enable fast and low-effort updates, upgrades, configuration and fixing of problems, potentially

through a fast acting group of engineers (provided by a certain stakeholder). Some delays are due to deficiencies in operation concept that impede effective fault management, planned maintenance and upgrades. For any operator model, work and interaction between the stakeholders must be coordinated well and proper operation concepts need to be established.

The communication must be the pillar of the coordination. If communications between stakeholders are restricted and don't consider emergency requirements, dedicated communication channels between stakeholders need to be installed and high availability shall be ensured to consider emergency cases (e.g. fast recovering from network failure). When partners have similar expertise and offer different opinions, task leader needs to compromise those opinions of partners. The task leader can make a pros and cons list of partner's opinions to clarify the full impact of tasks and verify their correctness. Finally, the task leader needs to decide the most feasible way.

5.3.4 Lack of autonomy in using and managing the 5G network

Some concerns are related to the lack of autonomy in using and managing the 5G network. Without a well-defined trust and governance model, responsibilities and liabilities are unclear. The coordinator has to clearly define the role and the scope of each stakeholder in order to easily identify the contact and the responsible. No clear (or lean) network demarcation between Enterprise and MNO/SP could lead to huge effort to fulfill requirements of the enterprise (i.e. provide respective network services). The demarcation must be done on 5G elements but also on non 5G related elements. For example, the MEC platform can be managed by the MNO, the enterprise, a cloud provider or a another third-party but user data in the MEC platform will involve confidentiality issues. The MEC platform holder needs to clarify the authority of user data and relevant regulations with users (i.e., user data needs to be clearly defined who has the right to access and use).

5.3.5 QoS customization

The flexibility of the private 5G architecture enables customized network deployment and the support of heterogeneous use cases with different requirements. This flexibility makes the network deployment more challenging. For the QoS customization, each stakeholder must exchange specific requests and requirements and some configuration option shall be available. If the QoS parameters in the PCF function for each user / applications / network-slice are managed by the MNO, the enterprise shall have access ability to configure customization of the QoS parameters. If the application has specific requirements, which do not fit in SP's standard solution and has not been implemented, the owner of the application shall have enough impact to influence the evolution/extension of the standard private 5G/compute solution, such that increasing requirements are fulfilled. If the features and solutions to fulfill application requirements will not be implemented, the stakeholder, who requires the features and solutions with respect to the 5G network, which are essential for additional use cases, shall have enough impact to get the features or solutions.

5.3.6 Deployment issues

Some concerns are related to the availability of non-5G elements to realize a deployment. If the deployment is limited by power supply, room space, cooling or transport connection, enterprises shall provide existing or deploy new infrastructure related to power supply, cooling or WLAN infrastructure.

5.4 Regulations

Regulation must adopt a harmonized approach that facilitates support for the deployment of a private 5G network by all stakeholders (stakeholder-internally, officially).

Internally, different enterprises can have different security requirements for private data or resources. These enterprises can discuss how to find a compromise between each other's security requirements to decide the most feasible security solutions. Each enterprise can explain the requirements of safety regulations and knowledge of international standards. Then, enterprises exchange opinions with each other to integrate similar and different parts into the most feasible security solution. Moreover, some coexistence concerns can appear. For example, the enterprise must coordinate and plan solution deployment and check their compatibilities. If the enterprise 5G services have separate VLANs with enterprise-internal networks, additional routers to exchange data with 5G services and existing enterprise system can solve the problem.

Regarding the spectrum regulation, the government manages the spectrum and provides enterprises with spectrum leasing services. Therefore, companies in different countries/regions may use different spectrums to work and must follow their regulations. Enterprises may require local partners (such as MNO, E, or 3EC) for spectrum planning, and companies may also understand the regulations and apply for spectrum from the government.

In order to fulfill official regulations, an enterprise might have concerns regarding the proper handling of spectrum, especially in terms of appropriate interference management towards adjacent (private) networks. The owning and governing stakeholder regarding the spectrum shall have the technical means and the competencies to avoid improper handling of the spectrum.

5.5 Applicability and Practicability

For enterprises with multiple sites distributed across several countries, the global applicability and the practicability of the operator model is an important group of concerns. 5G offers a flexible, modular and programmable system architecture enabling a large range of deployment scenarios. Nevertheless, multi-site deployments need interoperability, interconnection or shared models/components to mutualize the cost, and this sometimes under different regulations, laws and architectures.

5.5.1 Multi-site private 5G network

Although the concept of private 5G networks opens new opportunities, there are still a few remaining concerns regarding multi-site private 5G networks in terms of interoperability, interconnection, shared models and components.

The enterprise that has many sites might raise concerns regarding increased complexity of managing a multitude of different operator models, which can be a burden regarding monitoring and managing the networks at the different sites. The enterprise needs comprehensive view on implemented 5G networks in different locations, perhaps across multiple countries, based on the same or a similar operator model. This is particularly important if, for example, users may want to setup multiple PDN sessions to different DNN by UPF located at different sites. Core-SMF may have UPF selection policies for user to setup PDU sessions at multiple DNN with multiple I-UPF. In a multi-site private 5G network, enterprises may consider the transmission security and efficiency of private data. Then, enterprises can consider international standard safety regulations, NEV hardware function limitations and MNO service types to find the most feasible solution.

Finally, concerning the mobility continuity within multi-site (i.e. handover), the RAN equipment vendors or service providers should configure suitable radio parameters and setup Xn or N2 interface handover for mobility continuity.

5.5.2 Global applicability

Some concerns of a stakeholder are related to the global applicability of the same operator model or at least the capability to apply the same operator model in a large number of countries. Multi-site deployments under different regulations, laws and architectures must be carefully planned and designed. The operator model may have different laws and regulations in different countries/regions. A globally acting enterprise's concern could be that different official regulations or ecosystems across countries lead to the situation that private 5G networks cannot be deployed, as the resulting operator models do not comply with the enterprise requirements. At design level, the global applicability of an operator model shall be ensured, which is largely independent of the variety of regulations per country and the enterprise's requirements in this regard (e.g. regarding ownership of spectrum). Before applying the operator model, enterprises may need to learn about the operator model regulations in various countries/regions or find local partners (such as MNO, third-party enterprises, cloud providers, or service providers) to provide operator model deployment plans.

Concerning the private 5G network architecture, if sites use different operator models (e.g., site A uses an MVNO-operated model whereas site B a hybrid-operated model for better coverage or capacity requirements), the enterprise may setup an additional RAN network if MNO RAN network is not capable of enterprise services.

5.5.3 Cost implications

A major group of concerns of a stakeholder influencing operator models will be the cost that implies each specificity, performance requirement, coverage extension or additional support. An enterprise's concern might be increased costs for a technical solution (architecture or deployment model) that is implied by a certain operator model (without alternatives, e.g. due to lack of local spectrum). Thus, single operator models require a number of different deployment and architecture options that are cost-attractive in light of the enterprise's technical requirements. Moreover, an enterprise might have concerns regarding high costs associated with SLAs regarding QoS provisioning. The operator model shall provide high QoS provisioning and associated SLAs at reasonable costs. The radio coverage of RAN will also affect the cost and transmission capability, two of which are inversely proportional. Therefore, a good feasible solution needs to balance the cost and transmission capability. Enterprises can obtain radio service through local partners (such as an MNO, a service provider, a third-party network planner, or a network equipment provider), and using this information to make a good feasible solution. Finally, 24/7 field service for emergency maintenance can be costly. For any operator model, 24/7 field service shall be provided with reasonable costs.

6 Criticality of Aspects and Evaluation Template

This section finally assesses the concerns and requirements that have been collected in the previous section and provides a template for the evaluation of concrete operator models, which will be used in WP 2.

6.1 Criticality of Aspects Regarding Operator Models

In order to identify the most important aspects for an in-depth evaluation of operator models, the collected requirements are regrouped again to form a set of evaluation criteria. The aspects partly follow the categorization of the corresponding concerns and are provided in Table 13. For each of the aspects, the table collects the corresponding concerns with indices in Annex III (Section 9), the number of concerns per aspect and the sum of the ratings. Here, each requirement has been rated according to its expected importance on a scale between 1 and 5, with 1 being “least important” and 5 being “most important”. Finally, a criticality index is provided for each aspect, which is calculated as the sum rating normalized to the sum rating averaged over all aspects.

Table 13: Criticality of Aspects for the Evaluation of Operator Models.

Aspect		Corresponding concerns (see Annex 3)	Number of requirements (Total / E / MNO / SP)	Sum rating (see Annex 3)	Criticality Index
A1	Wrong or missing access to elements by a stakeholder	B-2.1 – B-3.7	**9** / 8 / 8 / 7	34	**1.89**
A2	Interoperability of security systems and alignment of security concepts	A-2.1 – A-3.4	**7** / 7 / 2 / 2	26	**1.44**
A3	Lack of expertise to carry out lifecycle tasks	C-1.1 – C-2.4	**7** / 4 / 5 / 4	25	**1.39**
A4	Confidentiality, integrity, availability of data	A-1.1 – A-1.6	**6** / 6 / 1 / 1	24	**1.33**
A5	Autonomy of stakeholder	C-4.1 – C5.4	**7** / 6 / 7 / 5	22	**1.22**
A6	Ownership of and governance over elements by another stakeholder	B-1.1 – B-1.6	**6** / 5 / 5 / 5	20	**1.11**
A7	Coordination effort	C-3.1 – C-3.5	**5** / 5 / 3 / 3	15	**0.83**
A8	Multi-site setups	E-1.1 – E-1.4	**4** / 4 / 3 / 3	15	**0.83**
A9	Costs	E-3.1 – E-3.4	**4** / 4 / 1 / 1	14	**0.78**
A10	Service availability and continuity	A-4.1 – A-4.3	**3** / 3 / 3 / 3	12	**0.67**
A11	Global applicability	E-2.1 – E-2.3	**3** / 3 / 2 / 2	10	**0.56**
A12	Regulation	D-1.1 – D-2.2	**3** / 3 / 2 / 1	9	**0.5**
A13	Deployment and system coexistence	D-3.1 – D-3.2, C-6.1	**3** / 3 / 1 / 2	9	**0.5**

		Total: **67** / 61 / 43 / 39	Avg: 18	Avg: 1.0

From the analysis of all 67 concerns and requirements and the subsequent rating and regrouping, it becomes clear that an operator model should be designed in a manner that concerns regarding wrong or missing access to elements (5G elements in particular) by certain stakeholders are addressed. Furthermore, an operator model (and the related deployment model and architecture) needs to ensure interoperability of security systems and the alignment of security concepts of different stakeholders, most importantly the ones of the enterprise and the MNO or service provider. Two other important aspects of an appropriate operator model are that it needs to consider the potential lack of expertise required by stakeholders to carry out private 5G network lifecycle tasks, while at the same time it should ensure autonomy of stakeholders – two seemingly contradictory aspects. Moreover, confidentiality, integrity and availability of sensitive data is important. Finally, the analysis also reveals that aspects around global applicability of an operator model, regulations, and deployment and system coexistence issues are less critical in comparison.

6.2 Evaluation of an Operator Model

Table 13 also shows the number of concerns per stakeholder, in particular by the enterprise (E), the mobile network operator (MNO) and the service provider (SP). It becomes obvious from the numbers that these three stakeholders are the most relevant ones. Therefore, an operator model should be evaluated from each of these perspectives considering only those requirements that are of importance to the concrete stakeholder. In addition, rating, X, needs to be considered as a weighting factor to prioritize one requirement over the other.

The requirements collected are very diverse. They range from technical ones to organizational ones and also include rather general requirements, which can be fulfilled by different means. In this regard, the following general possibilities exist to fulfill any requirement:

1. **Inherent:** A requirement can be inherently fulfilled by an operator model. This means that no additional effort is required, such that this is the best possible option.
2. **Technical feature:** If a requirement is not inherently fulfilled by an operator model, it can still be fulfilled by a particular deployment strategy, an architecture setting or any other technical feature. Typically, some additional effort is necessary to implement certain features, which typically apply to technical challenges arising from the requirement.
3. **Contract**: If a requirement is not inherently fulfilled by an operator model and if there are no technical solutions that ensure it, there still exists the possibility to employ contractual agreements between involved stakeholders.
4. **Not fulfilled**: If neither the operator model itself, nor technical or contractual solutions can be used to fulfill a requirement, it is considered to be not fulfilled.

The four categories above suggest a decreasing preference from “inherent” to “technical feature” to “contract” to “not fulfilled”. In order to account for this, a factor F is introduced, which takes the values from 2, 1.5, 1 and 0, respectively.

Table 14 provides the evaluation template for operator models. Per operator model, a dedicated template is used for each of the stakeholders. The template includes the requirement IDs (see Annex 3) for each of the aspects described in Table 13, the rating X for the individual requirement and options, how the requirement can be fulfilled according to the categorization above. Then, each requirement is given a score, which is the product of X and F, essentially jointly reflecting the importance of the requirement and the ease of fulfilling it. In the next step, the requirement-specific scores are summed up to reflect, how well an operator model fits a certain stakeholder with respect to a particular aspect. Finally, the total score is

again the sum over the aspect-specific scores, indicating the overall fit of an operator model to a stakeholder.

Table 14: Evaluation Template for Operator Models.

<Operator Model>		***<Stakeholder>***		***<Total Score>/<Max Score>***	
Aspect A1	**Wrong or missing access to elements by a stakeholder**				
Require-ment	**Rating** X	**Inherent** $(F = 2)$	**Technical feature** $(F = 1.5)$	**Contract** $(F = 1)$	**Score** $(F \cdot X)$
B-2.1	3	✓			6
…	…	…	…	…	…
				Total Score A1 / Max Score A1	*<Total score per aspect> / <Max score per aspect>*
Aspect A2	**Interoperability of security systems and alignment of security concepts**				
Require-ment	**Rating** X	**Inherent** $(F = 2)$	**Technical feature** $(F = 1.5)$	**Contract** $(F = 1)$	**Score** $(F \cdot X)$
A-2.1	4			✓	4
…	…	…	…	…	…
				Total Score A2 / Max Score A2	*<Total score per aspect> / <Max score per aspect>*
…	**…**				
…	…	…	…	…	…

7 Annex 1: Lifecycle Description and Required Competencies

Task	Description	Required Competencies
A-1	Identify technical requirements on the system based and on the business needs (e.g., collect the requirements of 5G networks, shop floor information and enterprise network architecture.)	Knowledge of technical business skills.
A-2	Define some use cases and corresponding requirements.	Knowledge of technical requirements and demand analysis (e.g., instructive discussion with enterprise technicians).
A-3	Define the network architecture according to the use case and the requirement.	Knowledge of 3GPP 5G capability and existing solutions.
A-4	Dimension the communication system in terms of network efficacy (i.e. data rate, bandwidth, and throughput), radio frequency specification (i.e. frequency band selection), radio coverage, network capacity (i.e. number of devices), data availability and security.	Knowledge of 3GPP 5G capability and existing solutions.
A-5	Define system specifications according to the enterprise's requirement.	Knowledge of 3GPP 5G capability and existing solutions.
A-6	Realize measurement campaign, experiment with labs platform to validate the architecture choice	RF experts with instrument knowledge (e.g., measurement activities, laboratory platform experiments).
B-1	Consider network service specification and core network elements software requirements to choose appropriate elements.(e.g., for hardware, GPU, CPU, Ethernet speed and storage. For software, NFV K8S platform or OpenStack platform)	Solution architect in 5G and known each component capacity and hardware set
B-2	Install and configure MEC parameters. Choose which types (UPF/ bump-in-the-wire) to setup. Consider applications running on MEC platform.	Knowledge of 5GC network entities, protocols, cloud environments (such as Docker, Kubernetes), and network solutions in 5G MEC space
B-3	Install and configure core network parameters.	Understanding of 5GC network entities, protocols, cloud environments (such as Docker, Kubernetes), and network solutions.
B-4	Install and configure RAN parameters.	Knowledge of network solutions in 5G RAN space and design/implementation.
B-5	Install and configure application parameters.	Network solutions in application space.
B-6	Use APIs of the core network to get information and integrate with their applications.	Knowledge of core network APIs.
C-1	Define on-site Radio Planning service requirements including ability deployment (e.g., users traffic model, coverage, and capacity) and radio design deployment (e.g., radio unit location, antenna radiation direction, and tilt angle.)	Expert in outdoor gNB site identification and site survey, site planning, link budget preparation and access network resource planning/optimization operations.
C-2	Plan the deployment with enterprise's technical staff. In the site, it includes site surveys, power, equipment space planning and the placement of access points. For networking, it takes into	Ability to carry out wireless network system end-to-end network design and 5G components.

Task	Description	Required Competencies
	account enterprise's intranet architecture and restrictions.	
C-3	Consider deployment models and IP address planning (such as network equipment, applications, and OAM). Setup the firewall and VPN between MNO elements and Enterprise elements. (e.g., the MNO RAN needs to setup a VPN connection to Private 5G CN – AMF on MNO network. The UPF, located in the factory, has to setup VPN connection to Private 5G CN – SMF on probably broadband network.)	Experience in IP networking (e.g., LAN/WAN networking architecture, firewall and VPN setup) and in IP Routing (i.e. routing and CCNA or CCNP license)
D-1	Deploy and install 5G private network hardware, packaging and space reservation, interface with IT network, connection with IT power supply.	Experience of onsite radio network construction and provisioning hardware engineering
D-2	Configure radio network parameters (e.g., frequency, bandwidth, Output Power, TAC, eNB ID and MME IP). Configure Private network router (e.g., network VLAN TAG, UnTAG, IP usage, Enterprise network routing policies.) Build on-site radio network (e.g., RRU, Synchronization Clock Source, Ethernet cable layout, Electricity.) Install and configure MEC/ Core network software including HA.	Understanding RF configuration and cloud platform. Experience in IP-based platforms and IP networks. Proficient in Linux operation and management such as wireless base station equipment, core network, MEC and application operation/installation.
D-3	Integrate applications, traffic routing, and applications running on the MEC platform.	Experience in network integration for VNF (virtualized network function), application operation and MEC operations.
D-4	Integrate enterprise's OAM system monitoring the continuous operation of product line and equipment on the shop floor like CNC, AGV. Couple 5G network management system with a production management system	Experience with integrating with enterprise systems (e.g., databases, ERP systems, and factory automation systems). Knowledge of Enterprise's OAM system and 5G components operation/maintenance.
D-5	Configure user profile both in USIM cards and in core network.	Knowledge of 5G Core-UDM operation and the provision tool to grant UDM provision authorization.
D-6	Validate the end-to-end functional test, ensuring the network connection and application function.	Understanding applications, 5G core, 5G MEC, 5G RAN, and experience in 5G 3GPP function test planning, execution and classification.
D-7	Validate private network end-to-end performance, ensuring reaching service requirements.	Understanding applications, 5G core, 5G MEC, 5G RAN, and defining system test cases and automated execution to ensure performance requirements.
D-8	Apply for government supervision unit using private network spectrum. The government will send someone to verify.	Understanding the laws, government regulations, executive orders, agency rules and democratic political procedures in order to collect information and fill out application forms.
D-9	Monitor private network performance in terms of efficacy (i.e. utilization of traffic and elements), monitoring (i.e. health check and periodic performance report) and error handling (i.e. alarm notification and fault management)	Understanding the operation and maintenance of 5G components. Experience in network technology (server, switch or device configuration), key network protocols, tunneling technology, switching and routing.
E-1	Monitor network anomalies, UE health status, network performance over time per UE, security mechanisms (i.e. confidentiality and integrity protection), spectrum usage, networking	Understanding 5G RAN, Core, MEC . Experience in application's operation/maintenance (i.e., monitor and analyze statistical data to develop improvement plans)

Task	Description	Required Competencies
	capabilities, guaranteed performance and supported services. Verify that outage protection is activated and failover and redundancy concepts are ready.	
E-2	Register UE and assign network slice to UE. Add/edit subscriber profile and application subscriptions on the Core-UDM.	Knowledge of using the provision tool to grant UDM provision authorization.
E-3	Deploy new application when a new application or service is available via the 5G system. Register applications to network and update subscriber's data.	Knowledge of new applications and MEC platform to deploy the new applications.
F-1	Order and deploy SIM card, eSIM, etc. Create backup of subscriber profiles and recover subscriber profiles. Retrieve subscriber management log files.	Knowledge of 5G Core-UDM operation.
F-2	Check CPU, memory, disk and bandwidth usage of MEC platform.	Knowledge of MEC capacity related hardware resource.
F-3	Check CPU, memory, disk usage of Core network and software licenses (number of UEs or IoTs).	Understanding of 5G core network operation, and optimization and related capacity hardware resource.
F-4	Check spectrum and radio resource usage.	Understanding of NR theory and practical experience. Understanding of hardware resources related to RAN capacity
F-5	Check CPU, memory, disk usage of applications and limitation characteristic of applications.	Knowledge of application capacity related hardware resource.
F-6	Modify and revoke management, configuration and monitoring access rights. Assign priorities to end devices, device groups and services	Knowledge of Core-UDM operation and OAM operation.
G-1	Announce the upgrade event ensuring related personnel know the effect of equipment of production line.	Knowledge of 5G network including RAN, Core, MEC platform and transport network.
G-2	Develop the upgrade planning.	Knowledge of effect of upgrade 5G components ensuring continuous operation.
G-3	Switch to the redundant system and ensure continuous operation.	Knowledge of 5G Core, MEC and base station operation.
G-4	Update the software of core, radio, and MEC.	Knowledge of operation, installation and upgrade process of RAN, core network, and MEC platform.
G-5	Validate the end-to-end functional test, ensuring the network connection and application function.	Understanding applications, 5G core, 5G MEC, 5G RAN, and experience in 5G 3GPP function test planning, execution and classification.
G-6	Validate private network end-to-end performance, ensuring reaching service requirements.	Understanding applications, 5G core, 5G MEC, 5G RAN, and defining system test cases and automated execution to ensure performance requirements.
G-7	Switch to the active system and ensure continuous operation.	Knowledge of 5G Core, MEC and base station operation.
H-1	Collect the logs from equipment export and automatically check by OAM system. (if available, the OAM system sends SMS or e-mail alarm.)	Knowledge of system logs performance counters and data of 5G RAN, Core, MEC and applications.
H-2	Check network performance reports regularly to optimize private network KPIs by possible adjustments like RRU expansion if necessary.	Knowledge of operation and maintenance of 5G RAN, Core, MEC and applications
H-3	Use technical methods to find the problem and fix the problem.	Knowledge of operation/maintenance capabilities of 5G RAN, Core, MEC and applications, and

Task	Description	Required Competencies
		analyzing technical issues and verifying error repairs.
I-1	Disconnect existing system such as enterprise's OAM system, production management system, and equipment on the shop floor like CNC, AGV.	Knowledge of enterprise's OAM system and 5G components operation and maintenance
I-2	Delete subscriber profile and deboard/deregister UE on the Core-UDM.	Knowledge of using the provision tool to grant UDM provision authorization.
I-3	Disconnect the applications and equipment of production line.	Knowledge of applications and MEC platform to undeploy the applications.
I-4	Uninstall/remove the software of 5G RAN, Core, MEC platform and applications.	Knowledge of 5G Core, MEC and base station operation.
I-5	Remove 5G private network hardware and disconnect the IT power supply	Experience of onsite network construction and provisioning hardware engineering

8 Annex 2: Elements Touched During Private 5G Network Lifecycle

Task	Core-UDM	Core-AUSF	Core-SMF	Core-AMF	Core-UPF	Core-NEF	Transport Network	RAN-DU	RAN-CU	SIM	5G OAM System	Spectrum	Control Plane Data	Application	MEC Platform	User Plane Data	WAN Infrastructure	Shop floor	Shop Floor Plan	Enterprise IT network	Third-party cloud platform	Enterprise OAM System	Enterprise Database	Power Supply
A-1	X	X	X	X	X		X	X		X	X	X		X	X		X	X	X	X	X	X	X	
A-2	X	X	X	X	X		X	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
A-3	X	X	X	X	X		X	X	X	X	X	X		X	X		X	X	X	X	X	X	X	
A-4	X	X	X	X	X		X	X	X	X	X	X			X		X		X	X	X	X		
A-5	X	X	X	X	X			X	X	X	X	X		X	X					X	X	X	X	X
A-6	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	
B-1	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X	X	X	X			
B-2							X				X			X	X		X			X	X		X	
B-3	X	X	X	X	X	X	X				X				X		X			X	X	X	X	
B-4								X	X	X	X	X			X		X			X				
B-5							X							X	X		X			X	X		X	
B-6	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X			X	X	X	X	
C-1							X	X	X	X	X	X					X	X	X	X		X		
C-2	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X	X	X	X	X	X	
C-3	X	X	X	X	X	X	X	X	X		X			X	X		X			X	X	X		
D-1	X	X	X	X	X	X	X	X	X		X				X		X	X						X
D-2	X	X	X	X	X	X		X	X				X		X				X					
D-3	X									X			X	X	X	X			X	X	X		X	
D-4	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	
D-5	X									X			X							X			X	
D-6	X	X	X	X	X		X	X		X		X	X	X	X	X	X			X	X	X	X	
D-7	X	X	X	X	X		X	X		X		X	X	X	X	X	X			X	X	X	X	
D-8	X	X	X	X	X	X	X	X	X	X		X		X	X			X						
D-9	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	
E-1	X	X	X	X	X		X	X	X				X	X	X	X				X	X	X		
E-2	X									X			X							X			X	
E-3	X									X			X	X	X	X			X	X	X		X	
F-1										X														
F-2														X	X									
F-3	X	X	X	X	X	X																		
F-4								X	X			X												
F-5														X	X	X				X	X			

Task	Core-UDM	Core-AUSF	Core-SMF	Core-AMF	Core-UPF	Core-NEF	Transport Network	RAN-DU	RAN-CU	SIM	5G OAM System	Spectrum	Control Plane Data	Application	MEC Platform	User Plane Data	WAN Infrastructure	Shop floor	Shop Floor Plan	Enterprise IT network	Third-party cloud platform	Enterprise OAM System	Enterprise Database	Power Supply
F-6	X	X	X	X	X	X	X				X		X	X	X	X	X			X	X	X	X	
G-1											X			X						X		X		
G-2	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X		X	X	X	X	X	
G-3	X	X	X	X	X	X	X	X	X				X	X	X	X	X			X	X	X		
G-4	X	X	X	X	X	X	X	X	X				X	X	X	X				X	X	X		
G-5	X	X	X	X	X		X	X		X		X	X	X	X	X	X			X	X	X	X	
G-6	X	X	X	X	X		X	X		X		X	X	X	X	X	X			X	X	X	X	
G-7	X	X	X	X	X	X	X	X	X				X	X	X	X	X			X	X	X		
H-1	X	X	X	X	X		X	X	X				X		X		X							
H-2	X	X	X	X	X		X	X	X				X	X	X	X				X	X	X		
H-3	X	X	X	X	X		X	X	X				X	X	X	X				X	X	X		
I-1	X	X	X	X	X	X	X	X	X		X			X	X		X	X	X	X	X	X	X	
I-2	X									X										X	X		X	
I-3	X									X				X	X				X	X	X		X	
I-4	X	X	X	X	X	X		X	X						X									
I-5	X	X	X	X	X	X	X	X	X		X				X		X	X						

9 Annex 3: Concerns of and Requirements by Stakeholders

9.1 Confidentiality, Integrity and Availability

A-1	Concerns of a stakeholder regarding the access to information processed by or being part of an element by another stakeholder			
	Concern	**Stakeholder**	**Derived requirement**	**Rating**
A-1.1	A third party is able to access user plane data of the Enterprise causing considerable damage to the Enterprise.	E	For a certain operator model, any third party should not have the technical ability to access user plane data (e.g. routed by the UPF) for confidentiality reasons. If another party manages the UPF, it must be technically or by contract ensured that user plane data is not accessible by that third party.	5
A-1.2	Access to 5G elements that do not have a continuous encryption chain (i.e. end-to-end encryption) by another party is a concern regarding confidentiality (especially in a shared RAN scenario).	E	For a certain operator model, any third party shall not have access to an element (5G or non-5G), which does not provide a continuous encryption (e.g. decrypt/encrypt on a network element if no application layer or other end-to-end encryption can be employed).	4
A-1.3	Access to an application running in an off-premise MEC platform or information processed by that application is a concern from a confidentiality and integrity point of view.	E	For a certain operator model, no other party or tenant shall have the technical ability to access the Enterprise's application on the MEC platform or information processed by that application.	4
A-1.4	Access to the shop floor and the shop floor plan (information) by another party can cause concerns in terms of confidentiality, e.g. if there is critical production.	E	For any operator model, access to the shop floor and shop floor information shall be restricted to authorized non-Enterprise stakeholders.	3
A-1.5	Information contained in and processed by an Enterprise personnel and/or end device data base is highly sensitive. (different countries have also different regulations regarding privacy)	E	For any operator model, there shall be no or only necessary/essential access to information of an enterprise personnel and/or end device data base by any other third party and the highest security standards need to be employed.	4
A-1.6	Global availability of functionalities for end to end management	E, MNO, SP	Provide an open architecture. This brings security issues and opportunity for attacks	4

A-2	Concerns of a stakeholder regarding the control of information processed by or being part of an element by another stakeholder			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
A-2.1	Requirements to protect critical data transported via an infrastructure operated by a third-party can't be fulfilled for each application	E	Analysis must be carried out whether current and future use case requirements can be fulfilled by a certain operator model (that implies an architecture/deployment model). SLAs can be contractual measures in this respect.	4
A-2.2	Local network security, i.e. that of the Enterprise, can depend on	E	Enterprise and operator analyze possible infrastructure vulnerability	4

	security concepts of the MNO/SP, and can therefore be weakened by them		and attack vectors and define measures to avoid these. Verify effectiveness by frequent intrusion checks	
A-2.3	Encryption keys that are managed in the UDM are not directly accessible by an Enterprise if the UDM is governed by the MNO and located at the MNO central or edge cloud.	E	For an MNO operated model, the UDM and encryption keys shall be accessible and governed by the enterprise	4

A-3	**Concerns of a stakeholder regarding the manipulation or loss of information processed by or being part of an element**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
A-3.1	Data is lost or corrupted because of network, storage events that are not or not fully under control by the Enterprise	E	For operator models that imply a certain architecture/deployment model, data loss and corruption must be prevented, e.g. through appropriate redundancy concepts.	4
A-3.2	Intrusion attacks, especially in the case where a third-party operates the 5G network, are of large concern	E	Proper network design and architectures shall be possible with a certain operator model, such that intrusion attacks are prevented. Otherwise, contractual agreements shall be put in place.	4
A-3.3	Vulnerabilities in one stakeholder's security concept leads to attacks in other stakeholder networks	E, SP, MNO	For operator models, in which different security concepts are in place for the different stakeholder, vulnerabilities in one stakeholder's security concept need to be identified and mitigated, e.g. through vulnerability tests and redesign if necessary	3
A-3.4	Manipulation or loss of information needs a tracking mechanism.	MNO, SP, E	Manipulation or loss of information must be recorded by the component and the elements send notifications.	3

A-4	**Concerns of a stakeholder regarding service continuity (zero time service interruption)**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
A-4.1	The enterprise can quickly find the source of interruption	MNO, SP, E	Every stakeholder needs to report their status and provide a hotline or response team	4
A-4.2	The stakeholder needs to update some elements	MNO, SP, E	Define maintenance schedule minimizing the impact on regular operation	3
A-4.3	The network elements failure may bring down an entire private network.	MNO, SP, E	Network Elements Vendors need to setup network redundancy plan.	5

9.2 Access to and Control of Elements

B-1	Concerns of a stakeholder regarding the ownership or governance of an element by another stakeholder			
	Concern	**Stakeholder**	**Derived requirement**	**Rating**
B-1.1	Ownership and governance over the spectrum by the Enterprise could raise concerns regarding the proper handling of the spectrum (e.g. interference management), e.g. in the case of spectrum sub-licensing.	E, MNO, SP	Governance and responsibility about the spectrum shall ideally be taken by an appropriate stakeholder and/or by having the required competencies.	3
B-1.2	Ownership and governance of the MEC platform and third-party cloud (e.g. for the application and the 5G Core functions) by a SP can raise concerns for the Enterprise regarding confidentiality and integrity of the processed information and the applications that run on those platforms.	E	For any operator mode, ideally, the Enterprise has governance over the cloud/MEC platforms, or parts of them, to ensure confidentiality and integrity of the application and the information processed by the application.	4
B-1.3	Unallowed physical access or compromising MNO's or SP's 5G components built on- premise by the Enterprise	MNO, SP	For any operator mode, uncontrolled physical access or compromising components shall be prevented, e.g. though components being mounted in access controlled areas/cabinets	3
B-1.4	Physical damage of 5G components because of vandalism, accidents, on premise outage (climate control, power …)	MNO, SP, E	Hosting colocation takes appropriate measures to restrict unallowed access to third party equipment and monitors and adjusts climate and power	3
B-1.5	The enterprise can quickly find the problem of the private 5G network.	MNO, SP, E	Every stakeholder needs monitoring dashboards or APIs of elements for the enterprise.	3
B-1.6	The enterprise with increased number of users.	MNO, SP, E	For an MNO operated model, the MNO shall provide SIM card provisioning tool and provision parameters along with UDM user provision interfaces to enlarge UE pool. Under the premise that RAN and Core capacity is sufficient.	4

B-2	Concerns of a stakeholder regarding the access to and control of an element located at a certain location by another stakeholder, e.g. for management purposes			
	Concern	**Stakeholder**	**Derived requirement**	**Rating**
B-2.1	Management of MEC platform (or part of it) by the Enterprise while the platform is off-premise might raise concerns regarding accessibility, and management by the SP or MNO might raise concerns regarding integrity and proper management.	E	For any operator model, the MEC platform shall be well accessible by the Enterprise for management purposes, even it is located off-premise and owned by another stakeholder.	3
B-2.2	Elements are the wrong accessed by unrelated personnel and then cause system problems.	MNO, SP, E	Stakeholders need to establish reasonable authority control to avoid wrong access by unrelated personnel.	4

B-3	Concerns of a stakeholder regarding having no access to or control of an element located at a certain location, e.g. for management purposes			
	Concern	**Stakeholder**	**Derived requirement**	**Rating**
B-3.1	No appropriate or only restricted access to 5G elements by the SP or MNO, when elements are located at a location owned by the Enterprise	MNO or SP	For a third-party operator model, the Enterprise shall provide sufficient access to 5G elements to the SP or MNO considering the risks associated.	4
B-3.2	Stakeholder can't do emergency maintenance on premise 24/7 because premise is closed or access to it is limited	MNO, SP, E	For a third-party operator model, 24/7 emergency maintenance service shall be possible, e.g. through a 24/7 field service concept	4
B-3.3	Remote access to stakeholder's equipment is interrupted because of failure in the transport environment	MNO, SP, E	Remote access to stakeholder's equipment shall be ensured and the impact of failure shall be minimized, e.g. through implementing an out-of-band management concept.	4
B-3.4	The operation of the personnel can not find the source of the problem.	MNO, SP, E	Enterprises must make clear location access requirements and it shall be included in a global architecture	3
B-3.5	The transport network to establish secure N2 and N3 connections are controlled by the Enterprise.	MNO, E	Enterprise may setup MPLS VPN with firewall and network quarantine policies. MNO may acquire access authority to specific network elements are located at enterprise sites for maintenance and management.	4
B-3.6	The RAN(RU/DU/CU) and I-UPF are not directly accessible by an Enterprise that are governed by the MNO and located at the Enterprise sites.	MNO, SP, E	For an MNO operated model, the MNO shall provide 5G elements like the RAN network, I-UPF, transport network shutdown and restart procedure manuals when the Enterprise encounter annual maintenance or power outage.	5
B-3.7	Not all features are accessible. For example, when the system was design, some internal functionalities were not intended to be used by external stakeholder. Thus, no interface was defined.	MNO, SP, E	Stakeholders must jointly define their interfaces	3

9.3 Private 5G Network Lifecycle

C-1	Concerns of a stakeholder to not have the required competencies to carry out a certain task by himself/herself			
	Concern	**Stakeholder**	**Derived requirement**	**Rating**
C-1.1	Enterprise might not have required competencies for the following tasks (most relevant ones): A-3, A-4, A-6, B-1 to B-4, B-6, C-1, D-2, E-1, E-2, F-1, F-4, F-6, G-2, H-3	E	For any operator model, certain tasks requires competencies, such that other stakeholders need to be involved but with limited amount of effort (coordination) and at low cost; or build up expertise (e.g. A-3, A-4, A-6, B-1 to B-4, B-6, C-1, D-2, E-1, E-2, F-1, F-4, F-6, G-2, H-3)	5

C-1.2	Stakeholder's first level support is not familiar with local 5G set up	E, SP, MNO	Operation concept: Enterprise elaborates and improves operating concept based on contracts with SP and trains personnel	3
C-1.3	Network designers have to understand the network regulations of enterprises since they need to design the network architecture under these specifications.	E, 3NP, MNO	The network architects of enterprises must explain network configuration principles and restrictions to network designers.	4

C-2	**Concerns of a stakeholder about another stakeholder not having the required competencies to carry out a certain task**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
C-2.1	If Enterprise is involved in the private 5G lifecycle, MNO or SP can raise concerns regarding the proper O&M of the Enterprise, especially regarding liability	SP or MNO	When the Enterprise is involved during the private 5G network lifecycle, support by the MNO/SP is required with carrying out certain tasks during the private 5G network lifecycle, while total number of stakeholders and coordination effort need to be minimized.	4
C-2.2	Decreasing or missing support for specialized features, which have once been implemented	E	For any operator model, support for specialized features of a private 5G network solution shall be ensured during the entire private 5G network lifecycle	3
C-2.3	Stakeholder demands leads to decrease in MNO's/SP's standards and automation procedures	MNO, SP	A compromise between fulfilling a stakeholder's (especially the Enterprise's) demands and keeping up the MNO's/SP's standards and automation procedures shall be found for a certain operator model.	3
C-2.4	The use cases and requirements analysis come from the enterprise, so these requirements include the expertise knowledge of the enterprise. This knowledge will affect the analysis accuracy of use cases and requirements.	MNO, SP, CP, 3SI, 3NP, 3EC	Enterprises can explain the expertise knowledge of the enterprise to partners for improving the analysis accuracy of use cases and requirements.	3

C-3	**Concerns of a stakeholder about coordination/organization effort regarding a number of other stakeholders involved in certain tasks**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
C-3.1	During the phases A-D, a larger number of stakeholders need to be involved, potentially causing delays, many iterations in finding a solution and architecture that is appropriate	E	During phases A-D of the private 5G lifecycle, coordination effort shall be minimized and activities shall be bundled within a small group of stakeholders avoiding delay and excessive iterations on finding a solution.	3
C-3.2	Long delays for configuration, fault management and upgrades, when another stakeholder (SP or MNO) is less responsive, potentially causing	E	An operator model shall enable fast and low-effort updates, upgrades, config and fixing of problems, potentially through a fast acting group of engineers	4

	damage to the Enterprise due to downtime or the like		(provided by a certain stakeholder).	
C-3.3	Deficits in operation concept impedes effective fault management, planned maintenance and upgrades	E, SP, MNO	For any operator model, work and interaction between the stakeholders must be coordinated well and proper operation concepts need to be established	3
C-3.4	Communication between stakeholders is restricted and doesn't consider emergency requirements	E, SP, MNO	For any operator model, dedicated communication channels between stakeholders need to be installed and high availability shall be ensured to consider emergency cases (e.g. fast recovering from network failure).	3
C-3.5	When partners have similar expertise and offer different opinions, task leader needs to compromise those opinions of partners.	MNO, SP, E, CP, 3SI, 3NP, 3WO, 3EC	The task leader can make a pros and cons list of partner's opinions to clarify the full impact of tasks and verify their correctness. Finally, the task leader needs to decide the most feasible way.	2

C-4	**Concerns of a stakeholder regarding his/her autonomy in using and managing the private 5G network**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
C-4.1	No clear (or lean) network demarcation between Enterprise and MNO/SP possible, leading to huge effort to fulfill requirements of Enterprise (i.e. provide respective network services)	MNO, SP	For any operator mode, demarcations between an MNO's/SP's network and that of the Enterprise shall be clear and lean, while the Enterprise's requirements can be fulfilled	3
C-4.2	In a 5G private network, the MEC platform can be managed by MNO, E, CP or 3EC. But user data in the MEC platform will involve confidentiality issues, so user data needs to be clearly defined who has the right to access and use.	MNO, E, CP, 3EC	The MEC platform holder needs to clarify the authority of user data and relevant regulations with users.	3
C-4.3	Without a well-defined trust and governance model, unclear responsibilities and liabilities	E, SP, MNO	Clearly define the role and scope of each stakeholder	4

C-5	**Concerns of a stakeholder about QoS customization**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
C-5.1	QoS Customization	MNO, SP, E	Each stakeholder must exchange specific requests and requirements and some configuration option shall be available	3
C-5.2	The QoS parameters in PCF for each user / applications / network-slice are managed by MNO.	MNO, E	Enterprise shall have access ability to configure customization of the QoS parameters.	3
C-5.3	Features and solution to fulfill application requirements will not be implemented	E, MNO, SP	For any operator model, the stakeholder, who requires the features and solutions with respect to the 5G network, which are essential for additional use	3

			cases, shall have enough impact to get the features or solutions	
C-5.4	Application has specific requirements which do not fit in SP's standard solution and will not be implemented	E, MNO, SP	For any operator model, the owner of the application shall have enough impact to influence the evolution/extension of the standard private 5G/compute solution, such that increasing requirements are fulfilled.	3

C-6	**Concerns of a stakeholder about deployment**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
C-6.1	Limitation of power supply, room space, cooling, transport connection	MNO, SP, E	Enterprises shall provide existing or deploy new power supply, cooling or transport connection	3

9.4 Regulations

D-1	**Concerns of a stakeholder to fulfill stakeholder-internal regulations**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
D-1.1	Different enterprises have different security requirements for private data or resources. Enterprises can discuss how to compromise each other's security requirements to decide the most feasible security solutions.	MNO, SP, E,NEV,CP, 3SI, 3NP, 3WO, 3EC	Each enterprises explains the requirements of safety regulations and knowledge of international standards. Then, enterprises exchange opinions with each other to integrate similar and different parts into the most feasible security solution.	3

D-2	**Concerns of a stakeholder to fulfill official regulations (e.g. with respect to spectrum)**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
D-2.1	An Enterprise might have concerns regarding the proper handling of spectrum, especially in terms of appropriate interference management towards adjacent (private) networks	E	For any operator model, the owning and governing stakeholder regarding the spectrum shall have the technical means and the competencies to avoid improper handling of the spectrum	3
D-2.2	The government manages the spectrum and provides enterprises with spectrum leasing services. Therefore, companies in different countries/regions may use different spectrums to work and must follow their regulations.	E, MNO, 3EC	Enterprises may require local partners (such as MNO, E, or 3EC) for spectrum planning, and companies may also understand the regulations and apply for spectrum from the government.	3

D-3	**Concerns of a stakeholder about system coexistence**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**

D-3.1	Coexistence with existing system (intra or inter)	E, SP	Enterprises must coordinate and plan solution deployment and check their compatibilities	3
D-3.2	The Enterprise 5G Services may have separate VLAN with Enterprise internal network.	E	Additional routers to exchange data with 5G services and existing enterprise system can solve the problem.	3

9.5 Applicability and Practicability

E-1	**Concerns of a stakeholder regarding the possibility to realize a multi-site private 5G network**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
E-1.1	The Enterprise that has many sites might raise concerns regarding increased complexity of managing a multitude of different operator models, which can be a burden regarding monitoring and managing the networks at the different sites	E	For any operator model, the Enterprise needs comprehensive view on implemented 5G networks in different locations, perhaps across multiple countries, based on the same or a similar operator model	4
E-1.2	In a multi-site private 5G network, enterprises may consider the transmission security and efficiency of private data.	E, MNO, CP, SP, 3EC, NEV	Enterprises can consider international standard safety regulations, NEV hardware function limitations and MNO service types to find the most feasible solution.	4
E-1.3	The mobility continuity within multi-site like handover.	E, MNO, SP, NEV	The RAN equipment vendors or SP should configure suitable radio parameters and setup Xn or N2 interface Handover for mobility continuity.	4
E-1.4	User who wants to setup multiple PDN sessions to different DNN by UPF located at different sites.	E, MNO, SP	Core-SMF may have UPF selection policies for user to setup PDU sessions at multiple DNN with multiple I-UPF.	3

E-2	**Concerns of a stakeholder to not be able to apply the same operator model globally or, at least, in a larger number of countries**			
Concern		**Stakeholder**	**Derived requirement**	**Rating**
E-2.1	A globally acting Enterprise's concern could be that different official regulations or ecosystems across countries lead to the situation that private 5G network cannot be deployed, as the resulting operator models do not comply with the Enterprises requirements	E	Global applicability of an operator model shall be ensured, which is largely independent of the variety of regulations per country and the Enterprise's requirements in this regard (e.g. regarding ownership of spectrum)	4
E-2.2	The operator model may have different laws and regulations in different countries/regions. Before applying the operator model, enterprises must follow the laws of the country.	E, MNO, CP, SP, 3EC	Enterprises may need to learn about the operator model regulations in various countries/regions or find local partners (such as MNO, 3EC, CP, or SP) to provide operator model deployment plans.	3
E-2.3	Enterprise site A may use MVNO operated model where site B may use Hybrid operated model for	E, MNO, SP	Enterprise may setup additional RAN network if MNO RAN network	3

	better coverage or capacity requirements.		is not capable of Enterprise services.	

E-3	Concerns of a stakeholder about cost implications for a certain operator model			
	Concern	**Stakeholder**	**Derived requirement**	**Rating**
E-3.1	An Enterprise's concern might be increased costs for a technical solution (architecture or deployment model) that is implied by a certain operator model (without alternatives, e.g. due to lack of local spectrum)	E	Single operator models require a number of different deployment and architecture options that are cost-attractive in light of the Enterprise's technical requirements	4
E-3.2	24/7 field service for emergency maintenance can be costly	E	For any operator model, 24/7 field service shall be provided with reasonable costs	3
E-3.3	An Enterprise might have concerns regarding high costs associated with SLAs regarding QoS provisioning	E	An operator model shall provide high QoS provisioning and associated SLAs at reasonable costs.	4
E-3.4	The radio coverage of RAN will affect the cost and transmission capability, two of which are inversely proportional. Therefore, a good feasible solution needs to balance the cost and transmission capability.	E, MNO, NEV, SP	Enterprises can obtain radio service through local partners (such as MNO, SP, 3NP, or NEV), and using this information to make a good feasible solution.	3