CampusOS Whitepaper 2

Operating Models for Open and Modular 5G Campus Networks

CampusOS

Supported by:
Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag

Authors

Bahr, Michael	Siemens AG
Besslich, Robert	Siemens AG
Blümle, Sascha	YUMA Technologie GmbH
Götz, Dario	atesio GmbH
Hupfeld, Sibylle	Deutsche Telekom AG
Klaus, Harald	Deutsche Telekom AG
Pabst, Tobias	Universität Leipzig, ICCAS
Richter, Stefan	MUGLER SE
Schröder, Bernd	brown-iposs GmbH
Seidel, Martin	akquinet GmbH
Tammen, Matthias	RPTU
Weishaupt, Guido	Deutsche Telekom AG
Zeiger, Florian	Siemens AG

Table of Contents

List of Acronyms 4

1. Introduction 5
- a) Scope 5
- b) Definitions 6

2. Value chains for open and modular campus networks 7
- a) Value chains in exemplary use-cases 8
- b) Generic value chain for open and modular campus networks 15

3. Operating models 19
- a) Operating model framework and lifecycle of network operation 19
- b) Challenges 23
- c) Types of operating models 32

4. Task oriented guidance for hybrid operating models 38
- a) In-house vs. external evaluation scheme 46

5. Conclusion 47

6. Appendix 48
- a) Definitions 48
- b) Identified roles for network operation 51
- c) Identified roles for medical use cases 54

Contact 58

List of Acronyms

CAGR	Compound Annual Growth Rate
COTS	Commercial of the Shelf
CU	Centralized Unit
DAS	Distributed Antenna System
DU	Distributed Unit
E2E	End-to-End
EMC	Electromagnetic Compatibility
IT	Information Technology
HW	Hardware
LAN	Local Area Network
M&O	Maintenance and Operation
MANO	Management and Network Orchestration
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
MORAN	Multi Operator Radio Access Network
NW	Network
OT	Operational Technology
PLMN	Public Land Mobile Network
PoC	Proof of Concept
R&D	Research and Development
RACI	Responsible, Accountable, Consulted, Informed (Method to assign different classes of involvement)
RAN	Radio Access Network
RF	Radio Frequency
RFQ	Request for Quotation
RIC	RAN Intelligent Controller
RT	Realtime
RU	Radio Unit
SBB	Solution Building Block
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprises
SMO	Service Management and Orchestration
SW	Software
TP	German: Teilprojekt (similar to Work package)
USP	Unique Selling Proposition
VNF	Virtual Network Function
WAN	Wide Area Network

1. Introduction

a) Scope

The advent of 5G technology promises a fundamental improvement in connectivity, delivering ultra-low latency and massive connectivity to support demanding applications. Private 5G networks - we call them 5G campus networks – enable industries to harness the potential of cellular connectivity within their own dedicated environments. But as enterprises look to deploy these networks, they are faced with several operating model choices, each with its own set of benefits and complexities. Open and modular architectures and modules of 5G networks may give a high flexibility for combining and deploying 5G private networks at reliable costs without running into the danger of a vendor lock-in.

When navigating through the landscape of 5G campus networks, you can see that very different value chains emerge due to the different complexities. From infrastructure providers to service integrators and application developers, the ecosystem is diverse and requires stakeholders to carefully orchestrate collaboration and alignment to achieve desired outcomes. As we believe in the immense potential for innovation and efficiency gains of open and modular solutions for 5G campus networks, this white paper aims to provide some understanding and guidance for selecting the most appropriate operating model for your purpose. By understanding the nuances, we believe that by collaborating across the value chain and investing in the required competencies, organizations can unlock the full potential of 5G technology in their respective domains.

We discuss the different value chains for four use cases to illustrate the versatility of 5G campus networks: Industry 4.0, agriculture, medicine, and crane operations. In our Industry 4.0 scenario, we examine the case of a 5G campus network as an enabling complement to an Industry 4.0 vendor's main product. For an agricultural application of weed control, we discuss three very different approaches to providing 5G coverage: through a fully local service, through a mobile operator slice in a public network, and finally through a neutral host approach to temporarily extend public 5G coverage where 5G is needed. In the medical case, we are looking for 5G to support clinical ser-vices such as surgery and patient monitoring, as well as internal communications. Finally, a private 5G network will be used while deploying giant cranes in logistic environments such as ports.

When it comes to operating models, organizations can choose from self-operated, fully managed, or hybrid approaches. A self-operated model gives the organization full control and customization, while a fully managed model outsources network operations to a third-party provider. Hybrid models offer a blend of both, allowing organizations to benefit from external expertise while retaining strategic control. Regardless of the operating model chosen, the lifecycle of a 5G network follows a structured trajectory that includes design, planning, construction, optimization, and periodic reassessment. Each phase presents unique challenges, ranging from spectrum allocation and infrastructure deployment to performance optimization. Security must be considered at every stage.

This is discussed in Teletrust's recent guideline[1] and will not be discussed in depth here, although it needs to be considered at every step.

To effectively address these challenges, organizations need to cultivate a diverse set of competencies that include technical expertise, regulatory compliance, vendor management, and strategic planning. By providing a decision guidance framework, we hope to help organizations evaluate trade-offs, prioritize investments, mitigate risks, and find their individual operating model throughout their 5G campus network journey.

b) Definitions

The term "operating models" for a 5G campus network discriminates between the distributions of responsibilities regarding the tasks to be mastered over the lifecycle of a 5G campus network between a business case owner and external parties.

In established public land mobile networks (PLMN), the mobile network is the major business asset of the mobile network operator (MNO), and its operation is a core competence of the MNO. Most responsibilities are with the MNOs and historically just a few tasks are outsourced to external parties.

In contrast to that, 5G campus networks often are supplemental to the actual core business of a business case owner. But to run a 5G campus network himself the business case owner is expected to have relevant expertise to operate a radio network. In industrial use cases, 5G campus networks are expected to provide a wide range of different services with demanding requirements regarding network performance and tight integration into individual business information technology (IT) and operational technology (OT) that may require specialized expertise both in terms of network operation and domain knowledge for the use case. In these cases, it may be beneficial to pass responsibilities for parts of network operation to external parties leading to more complex operating models.

The term "value chain" for a 5G campus network generally describes the progression of activities and relevant interactions between different parties that are required to support the network's complete lifecycle.

The following Table 1 provides a short overview of notions that frequently appear in the subsequent sections of this document. More elaborate descriptions of these terms can be found in the appendix.

Table 1: Definitions of specific terms used in this document

Term	Short Definition
Task	A task describes a set of activities and related responsibilities.
Role	A role is a collection of responsibilities related to a set of tasks.
Actor	An actor takes on roles and bears the corresponding responsibilities.
Stakeholder	A stakeholder is a person, group, or organization affected by and/or interested in the campus network.
Value Chain	A value chain is the progression of value creating activities in the lifecycle of a 5G network.
Operating Model	An operating model describes the distribution of roles across all relevant actors.

2. Value chains for open and modular campus networks

Methodology to describe value chains

In this section, the underlying economic relationships between the value creation for the product or service „disaggregated and modular campus network" and the functional areas involved (the roles) are shown. Added value is generated at every level of the roles involved. The result of this value creation is hardware, software and/or a service (activity/task) which, in the sum of its individual components, comprises the campus network. It generates a certain economic value (added value) compared to its input factors. The visual representation of all roles with the associated value and financial flows creates the value chain, which comprises the totality of all roles involved in the process of value creation.

The aim of the following chapters is to use a case study approach to illustrate the value-added relationships of the roles involved for selected sectors. In doing so, it generates an understanding of the market structure and its mechanisms in the industrial application areas of campus networks. Each scenario represents only one of several conceivable interlinking of roles. To visualize the value chains, a distinction is made between three types of relationships: service flows in the form of hardware, software, or activities/tasks (marked in blue), information flows in the form of data or knowledge (marked in yellow), and money flows (marked in black). All roles are defined in the Appendix.

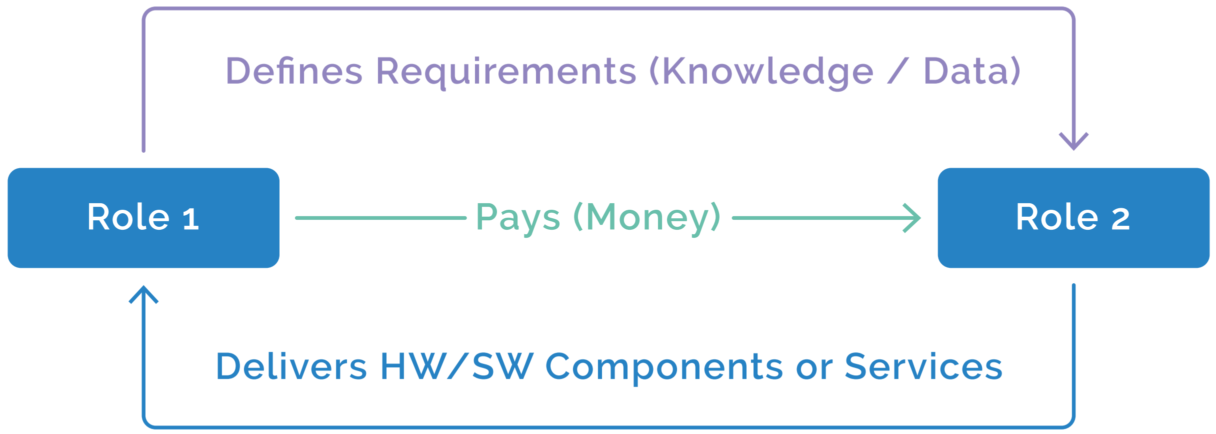

Figure 1: Representation of value chains through roles and flows

1 [opposite, p. 6] Bundesverband IT-Sicherheit e.V. (TeleTrust) 2024: „Handreichung 5G Campusnetze", https://www.teletrust.de/publikationen/broschueren/5g-campusnetze/

a) Value chains in exemplary use-cases

CampusOS – Industry 4.0 and mobile systems
This use case study covers scenarios in factories, logistic facilities, or similar where a product is manufactured or stored. The Industry 4.0 factories are using 5G campus networks in their industrial communication and for digitalization. The connected industrial automation devices and mobile systems have high demands on low latency, availability, and determinism. Also, safety functionality often relies on proper operation of the communication system, thus emphasizing the complexity of the communication system lifecycle, including the application requirements of low latency and high availability for the communication system. This use case study represents a single supplier-customer relationship by using a monolithic system where the 5G system is an integral part of a solution.

The main roles in this value chain are the Business Case Owner, responsible for manufacturing the product (e.g. a large machine) and the Product/Service Provider, responsible for providing the logistics or production facilities as a solution. Additional coordination is necessary with manufacturers of 3rd party products that are going to be integrated into the production facilities or logistics solution as subsystems by the System Integrator Product. However, the complexity of the logistics and production facilities and their defined production processes makes various other roles necessary. A large amount of information for the system design is required. Several involved implementation partners (System Integration, System Integration 5G system) rely on this information and offer their integration services. The communication system is usually not in the technical responsibility of the Product/Service Provider and is considered as a self-contained subsystem of the logistics and production facilities. However, the communication system is part of the business model and will be operated by the plant owner or an Operator 5G System. Without an efficient and functioning communication network with high availability, the logistics and production facilities would not be feasible in this form. And precisely because communication is an essential value proposition in industrial automation, manufacturing of products, logistics as well as in providing solutions for logistics and production systems, the implementation of the communication network into the logistics and production solutions should be an integral part of the process. Accordingly, the value chain is directly impacted by the performance and quality of the communication.

The value chain as compiled in Figure 2 considers a specific use case scenario, where a product/service provider delivers a complete, monolithic production or logistics solution to the business case owner. The solution includes a 5G campus network for the industrial communication, customized to the use case and its application requirements

In the beginning, the overall design is agreed and the requirements for productivity and availability are clarified based, for instance, on different technological opportunities and concepts or on available tenders and proposals. A system layout is drawn up and any interfaces to other suppliers of plant components are coordinated. Due to the complexity of the system and potential local, regional, or national requirements, the installation and launch is carried out with sub-suppliers, who execute the required steps under the instruction of the Product/Service Provider. An active exchange with Regulatory Approval and Licensing is needed to meet the respective (potentially multinational) legal requirements. The installation of a large and complex system may take several months during which extensive coordination takes place. After a successful launch, the logistics and production system is handed over to the Business Case Owner. The value chain graph in Figure 2 shows the possibility for several actors (e.g., Operator 5G System). In the case of smaller plants, it is also possible that all these roles are exclusively in the hands of the Business Case Owner. This would correspond to a merging of the individual roles in the end.

Not only the installation but also the operation of such a system is challenging. There are different entities responsible for the operation as well as for the monitoring. The 5G campus network must provide high availability as it is used for operation of critical systems of the product. While the operation corresponds to a normal value creation process between Business Case Owner and Operator 5G System, the monitoring of the logistics and production system is interesting in terms of value creation in several aspects. On the one hand, monitoring the effects on operation can be used for parameter optimization, on the other hand, the areas of maintenance and improvement of the logistics and production system are supported with important data. All involved manufacturers of parts of the logistics and production system can receive extensive information about the operating conditions of their sub-systems via specific services. Continuous improvement of the logistics and production processes and facilities is the result.

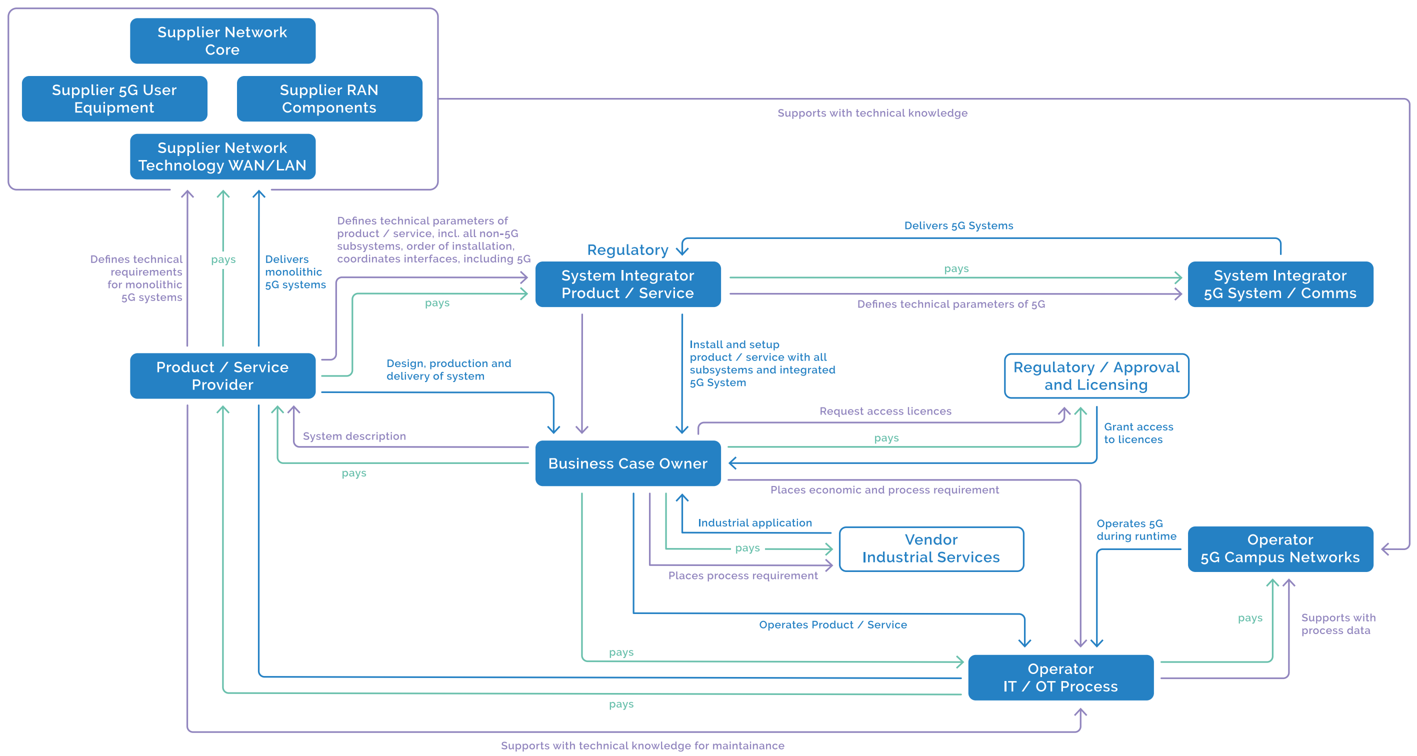

Figure 2: Value Chain Case Study – Industry 4.0 and mobile systems

CampusOS – Agriculture with temporary 5G coverage

This case study examined in the main project from three different angles, Nomadic Node, Virtual Slice and Neutral Host. The differences between them are described below, but all of them describe a scenario of weed control. This is done by using a drone and a spraying robot. A drone is equipped with a camera and will automatically fly over the field, taking aerial photos of the plants. These are transmitted over the 5G connection to a local edge cloud, where the images are analysed and the weeds are detected. This requires a high data rate for photo transmission and low latency to be able to control the drone if needed. Based on the positions of the weeds an optimal path is calculated and transmitted to the spraying robot. The spraying robot then drives along the planned path and distributes the spraying agent specifically to the weeds.

With the nomadic node, a private radio network is brought to the required location for a short time using a vehicle and put into operation for a short period. The advantage of this realization is that it can be used where no, or insufficient public mobile network coverage is available. A licence for local spectrum in this area is usually required.

However, if public mobile network coverage is available, the implementation around the virtual slice can be considered. A slice of the public mobile network is made available exclusively to the weed control services. Using a public mobile network offers the advantage that the drone can also fly over public space. The neutral host is a special case. By the introduction of an intermediate operator, a „neutral host", a local radio network extension of public networks is provided even if a direct connection to the public network is not possible or insufficient. The temporary and non-stationary demands of local 5G network coverage are fulfilled by nomadic RAN nodes controlled and steered by the intermediate operator. It is not using the private spectrum but is using – in cooperation with an MNO – an MNO-frequency band. Authentication and user-contract for (e)SIMs are the MNOs responsibilities with the Multi-Operator-Core-Network (MOCN)-approach, while the service is provided by the intermediate operator. Independent deployments of independent local networks at different sites – rented to different clients (e.g. farmers) – are possible.

In the following graphic (Figure 3) and text regarding the value chain we focus on the neutral host realization only. In the neutral host (for small and medium-sized applicants from agriculture and forestry) scenario the use case owner is representing a farmer of a small or medium-sized farm. Typically, these farms are too small to run their own private network due to a lack of resources. To enable them to run state-of-the-art technology in general and interwork also with agriculture contractors in particular – as it is usually happening in harvesting campaigns – 5G local networks must be brought to their fields in a temporary manner. An independent „intermediate 5G operator" is providing nomadic RAN nodes and takes over all organizational duties.These 5G nomadic RAN nodes are providing 5G coverage „on behalf of MNOs", meaning these nodes are advertising MNC/MCC-combinations of MNOs and forwarding all traffic to the corresponding MNO.

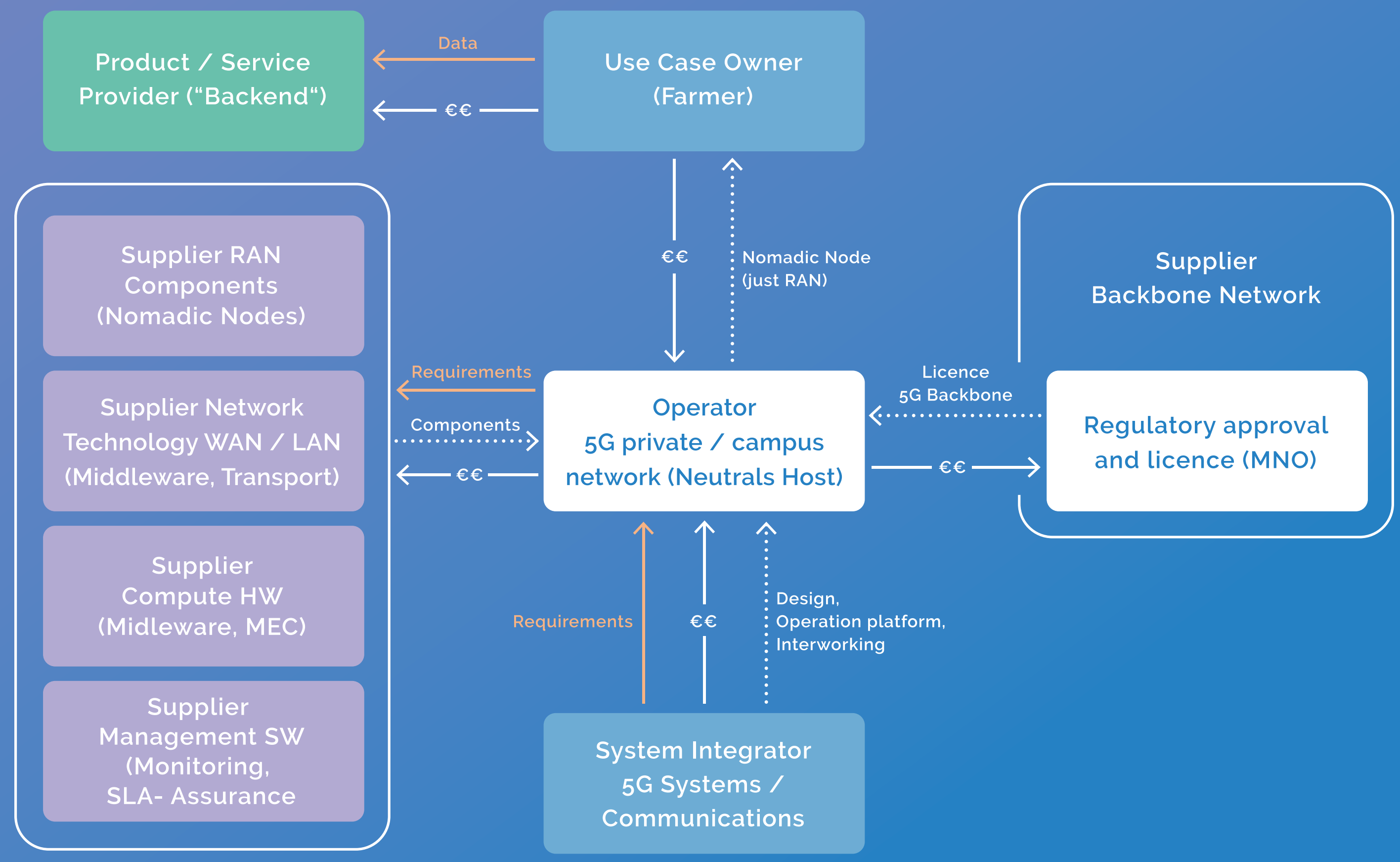

Figure 3: Value chain for the neutral host case for agriculture

By using Multi-Operator-Core-Network (MOCN) functionality this is done for all involved MNOs at the same time and at the same frequency. Therefore, this intermediate operator is called the „Neutral Host". It needs the allowance of the MNOs to advertise their MNC/MCC[2] combinations as well as using a 5G frequency which is licensed to them. Furthermore, a MNO's 5G network may be used as a backbone, and network slicing may be used in this backhauling approach to ensure quality and availability of services. The intermedi-ate operator itself might be rather an association of the agriculture section, like the "Maschinenring". Their interest is to provide services to the farmers, they are less experienced in network services and appreciate therefore the help of system integrators, also for running the intermediate network operations and to build and provide proper nomadic RAN nodes. These nodes are not set-ting up a fully autonomous 5G network, instead they are providing the connectivity to MNO's 5G cores via an intermediate compute center at the neutral host provider. Local mobile edge compu-ting (MEC) services nevertheless may be provided at the nomadic RAN nodes as well as at the neu-tral host's operation site. Anyhow the provision of applications is not a native part of this operator model. In this regard the plant owner (farmer) is on an application-level interacting with the prod-uct service providers (product service 3rd party) only, while the neutral host operator is an infra-structure-as-a-service provider, that is transparent to these two.

2 MNC/MCC Mobile Network Code / Mobile Country Code. A technical number combination to identify the 5G network.

KliNet5G – 5G Services used in hospital

5G campus networks in a hospital improve the wireless interconnection between personal and equipment and can be used for

a) Interconnecting staff,
b) Connecting IT-equipment, IT-systems, smart as well as medical devices and sensors,
c) Improving wireless device management and
d) Providing Internet access for guests and patients.

In order to support those use cases, close communication and coordination between the departments of IT, medical engineering, construction and various medical clinics is necessary. Some hospitals have a communications department, which would also be involved. This study has two focus points:

a) the identification of typical roles (in German hospitals)
b) independence from size, distribution, or economic situation of a hospital

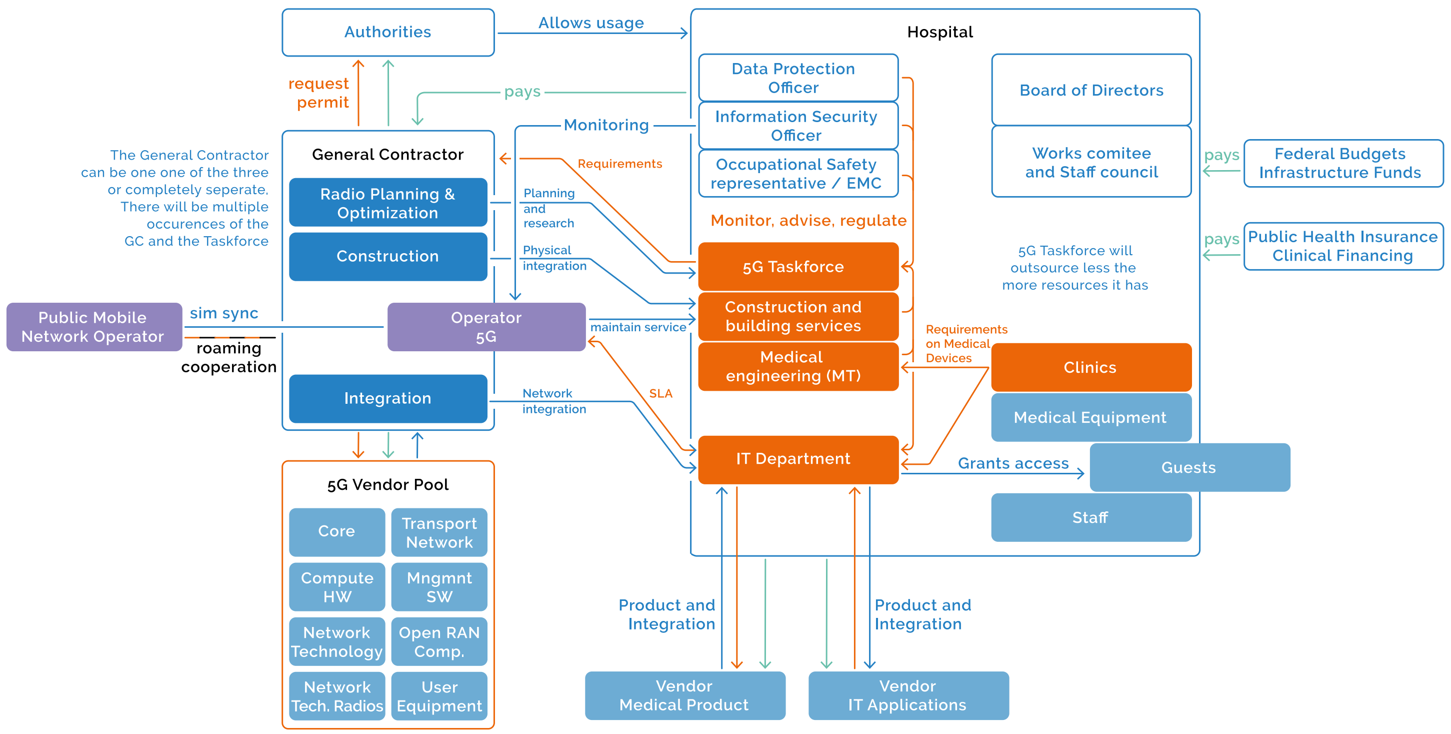

Figure 4: Value Chain 5G Services use in Hospital.

5G campus network offers the possibility for a more modular and flexible network than current network technologies. At the same time, it can support a wider range of use cases than current clinical networks. A campus network can provide a local area network based on mobile radio. This enables the staff to call, exchange mails and messages, share files and access IT systems over a local wireless network. The scope limited to the campus makes it more resilient, provides increased data protection and is better controllable. A 5G network has further advantages to support wireless interconnectivity of medical devices. Currently, medical devices can be connected to networks via ethernet or Wi-Fi. However, most devices which are using these networks do not use them for critical functions. Mainly because those technologies have limited support for safety and are not reliable enough. A 5G campus network offers network qualities that are comparable to proprietary solutions using cables and thus offering the first real chance for network critical functions. Besides communication 5G will offer new features in the future. For example, enhanced support for localization, enabling robust tracking of devices which will improve fleet and device management.

The hospital landscape in Germany is very heterogeneous in terms of clinic size, spatial distribution, and financial resources. Despite that, this study aimed to identify roles that can be applied to every clinic as 5G supports such a wide range of use cases. Because of the involvement of several different departments, hospitals need a coordinated strategy of communication with the various 5G vendors and stakeholders. In most cases, on the 5G vendor side a general contractor will be used who possesses appropriate 5G knowledge and who designs service level agreements (SLAs) for the clinic. On the clinic side, a task force consisting of representatives of the individual departments must be formed (this task force can be under the lead of one department or the hospital management). With this structure, the setup and continuous development of the network should be considered as a project that requires personal, financial, and technical resources. After the initial installation and setup phase, continuous network monitoring and network maintenance is required as well as the expansion of the network due to changing requirements. A detailed description of the roles is in appendix 6.b).

The availability of the network for medical devices needs to be critical high (>99,5%) while for other communication a high availability (>98%) is sufficient. The operation of the 5G network is strongly connected to the IT and medical technologies departments. The hospital may use the extensibility of the open RAN architecture to integrate different vendor technologies between waves of retrofitting. Within this example the 5G network is being operated partly from the hospital. For legal and security reasons the network belongs to the hospital and the hospital controls the basic functionality. For advanced tasks, for example radio optimization, it relies on external service provider as this requires highly specific domain knowledge and skilled staff.

5G++FlexiCell — 5G systems for quality assurance

This use case describes the implementation of a 5G campus network at a global manufacturer of mobile and crawler cranes. High data rates are required to transfer firmware for the vehicles during the test setup at the crane acceptance site, as the firmware has grown to a total size of 10 GB. In addition, a transparent channel into the manufacturer's corporate network is required via this 5G network, which supports the possibility of addressing and providing virtual subnets. For this purpose, a connection unit (UE) is temporarily positioned in the crane.

A portable computer, a label printer, and the vehicle itself are connected to the connection unit. Another use case for the 5G campus network is the allocation of eSIM to external companies when accessing the factory premises, which should enable various accesses to the Internet or internal subnets depending on requirements. The manufacturer is also considering whether mobile data collection devices with 5G resources that are already in operation should be converted from their current use in the existing Wi-Fi network to access via 5G.

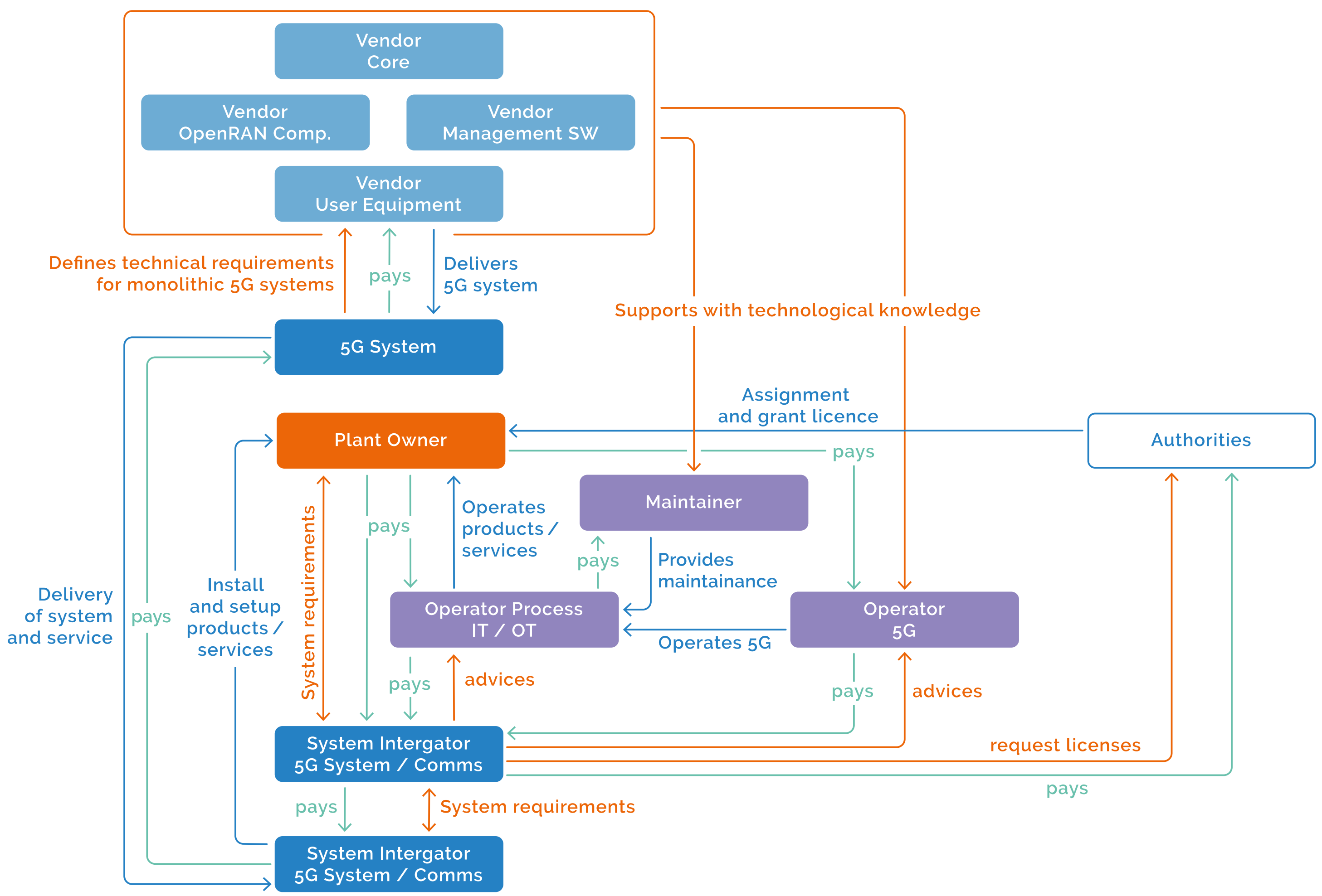

Figure 5: Value chain FlexiCell – 5G campus network as part of production and quality control.

The license holder of the 5G network is the manufacturer who operates an IT department which is responsible for the operational management of the network in terms of hardware and software administration. Another organization of the license holder, a central company-wide IT department, operates the 5G network. A system integrator supports the IT department for the setup of the 5G network and advises on necessary configuration changes, e.g. due to legal changes. This system integrator obtains advice from manufacturers and upstream suppliers regarding the selection of necessary components and their configuration. The manufacturers of the components provide technical expertise for the support of the hardware and software of the 5G components to a service administration and an instance that takes care of the maintenance of the systems.

b) Generic value chain for open and modular campus networks

The generic value chain for open and modular 5G campus networks considers all products (hardware and software) to operate a network as well as all necessary services to plan, deploy, operate, and optimize the system until its end of life.

Based on previous research, a first attempt was undertaken to build a general value chain for 5G campus networks. Value creating activities for all different flavors of private 5G networks can be assigned to seven main segments among the entire lifecycle as shown in Figure 6.

1. Devices and Components
2. Connectivity and Network
3. Platform enablers
4. Applications

Comprises hardware and software products and permissions of an open 5G private network from an E2E-perspective.

5. System Planning
6. System Integration
7. Operations and Maintenance

Comprises E2E-services for open 5G private networks among the entire lifecycle.

Segment	**Devices / Components**	**System Planning**	**System Integration**	**Connectivity / Network**	**Plattform enablers**	**Applications**	**Operations & Maintainance**
Description	All required Hardware components	Physical and logical design and planning of the network	Construction and setup of the NW and integration into existing en-terprise systems	All SW-, HW-based private network elements (Architecture, Standards, etc	Software Soluti-ons with Interface to Applications	Applications to be supported by the network	Operations and Extension of the network and applications
Elements	Servers	Network Design	Enterprise & OT Integration	Spectrum	Private Cloud	Application Development	Technical Support
	Switches	IT Security Analysis	Network Integration	Core Network	Edge Cloud	Content / service Development	Expansion & Optimization
	Edge-Devices	Radio Network Planning	Text & Verification	Connectivity Management	Public Cloud	Backend	Monitoring & quality
	Routers	Infrastructure Planning	Civil Works	CU / DU / RU			
	Sensors	(regulatory) approvals		Security	Security		
	SIM-cards	Technology consulting		OSS / NMS	Triple AAA		
				Licence			
				Backbone			

Figure 6: Generic value chain approach for campus networks

First, the required hardware components need to be analyzed and sourced. This ranges from radios over routers to servers. In the second step the system needs to be planned, which includes the physical and logical high-level and low-level design as well as fixing the technology to use and obtaining regulatory approvals. Once the system is planned the system integration can take place. The new 5G campus network needs to be integrated with existing hardware and software structures. Furthermore, the hardware needs to be installed and setup. The next step of the generic value chain focuses on the technological part of the 5G campus network and does not necessarily need to be exactly at this place in the value chain. It addresses the network architecture, security measures, licensing, how the core is deployed and many more technical features. In a next step, the generic value chain adds platform enablers, which build the interface to new software applications that can run on the 5G campus network. With that platform in place, applications can be installed and the benefits of the 5G campus network can be leveraged. Applications may range from support functions that help maintain the system to 3rd party providers offering services.

Once the 5G campus network is operational, various support functions need to be implemented to ensure that the system is running. These functions can range from classical support and monitoring to expansion and optimization of the system.

3. Operating models

a) Operating model framework and lifecycle of network operation

Motivated by the different approaches for the development of business models (Osterwalder & Pigneur, 2010)[3] or operator models (Campbell, et al., 2017)[4] found in practice and literature, and following on from the definition of operating models, a framework model for the description of operating models for open and modular campus networks is proposed. Such a framework shall help to understand the technological and regulatory specifics and the groundbreaking character of 5G campus networks. The framework was developed with the intent to not only depict a single exemplary operating model for a specific company, but to express the wide range of possibly conceivable content-related operating model designs and implementation options.

The operating model framework therefore contains different thematic areas that the authors believe are particularly relevant for describing operating models for campus networks with open modular architectures. This is intended to provide potential users and operators of campus networks with assistance and guidance in precisely specifying their individual operating models, which are likely to be found as hybrid operating models.

The following section and Figure 2 describes the seven thematic areas – *lifecycle tasks, resources, expertise, solution building blocks, service level agreements, contract model, right of property* – of the operating models are described below, which are clustered into an organizational-process layer (lifecycle tasks and resources), a competency layer (expertise), a technological layer (solution building blocks and service level agreements) and a business layer (contract model and right of property/ ownership):

3 Osterwalder, Alexander; Pigneur, Yves: Business Model Generation, John Wiley & Sons, 2010.

4 Campbell, Andrew; Gutierrez, Mikel; Lancelott, Mark: Operating Model Canvas: Aligning Operations and Organization With Strategy, Vam Haren Publishing, 2017.

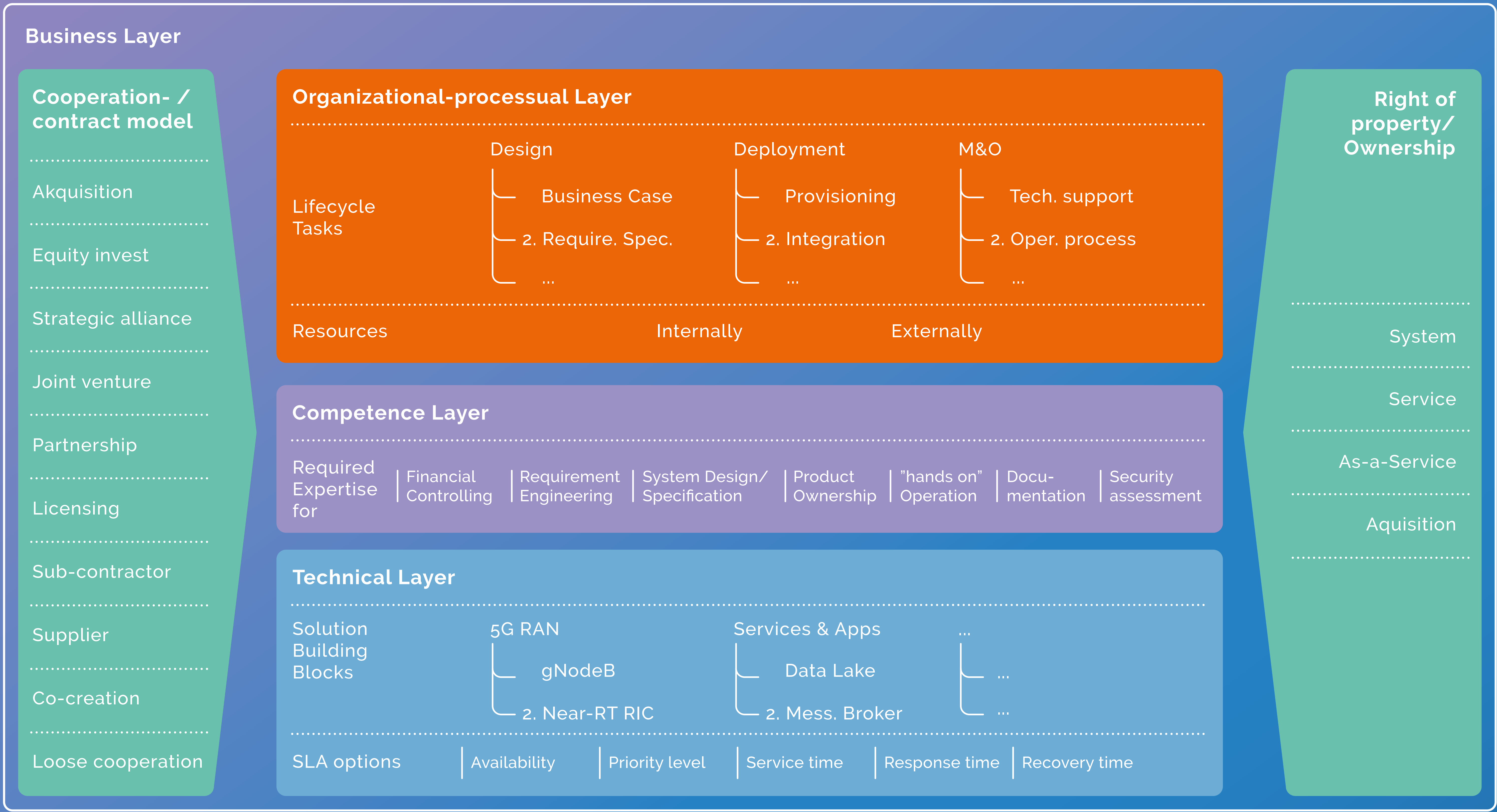

Figure 2: Operating model framework for open and modular campus networks

Lifecycle tasks

At first glance, an operating model in a very narrow understanding might only focus on the operating phase of the campus network, i.e. from commissioning onwards. However, this does not go far enough and must also be considered in the context of the upstream life cycle phases. For example, an operator model that includes a functional specification from the business case owner[5], who demands a certain network quality with specified parameters, differs greatly from an operating model in which concrete specifications are given for the solution. In the former case, the planning and design of the campus network is transferred to the provider and not provided by the business case owner. This example, among others, illustrates the need to consider the entire life cycle and the associated tasks in the course of an operating model.

Expertise and Resources

As the fulfilment of the tasks within the lifecycle is associated with general, but also highly specialized tasks, the business case owner must evaluate which competencies the respective tasks require and which of these tasks can be fulfilled by themselves, make sense to acquire this competence or must be outsourced to an external partner. The assessment of competencies and the division of tasks between the available internal and external resources is therefore a central aspect of this analytical work.

Solution Building Blocks and Service Level Agreements

Beside the organizational and competence-related thematic areas there are also technological elements that describe technical implementation variants of modular campus networks as an end-to-end solution. This is based on the building block catalogue in the form of the Solution Building Blocks (SBB), which are planned to be published until the end of the CampusOS project. The operational phase of the campus network (M&O phase) requires a specification regarding the service level agreement agreed with an internal or external partner, which defines fixed options for the rectification of faults for different fault types / priorities.

Cooperation model and right of property

There are also thematic areas that can be assigned to a type of business layer and permeate the aforementioned thematic areas at all levels. On the one hand, this includes the contractual basis that constitutes the cooperation between the companies involved, in particular the business case owner and its most important (external) roles. Such cooperation or contract models are described in detail in the literature. On the other hand, the business layer also includes the ownership rights/right of property of the 5G campus network itself, which can be transferred from the provider to the business case owner in the form of hardware (HW) and software (SW) components, for example, by means of a purchase agreement. Furthermore, temporary use in the form of licensing (especially for SW components) is conceivable or the complete provision of the campus network as a service model, without the user / business case owner receiving ownership of the campus network, instead being granted an exclusive or limited right to use the infrastructure (as-a-service).

5 A description of the role of a business case owner and other relevant roles is provided in section 4.b)).

Both thematic areas, cooperation models and right of property, are linked to very individual decisions on the part of the companies, which are based on strategic decisions, for example. In addition, the literature already provides relevant descriptions of the underlying models. For these reasons, there is no detailed consideration of both thematic areas in this deliverable.

The methodological tools which are part of this approach are based on a, RACI matrix for lifecycle tasks and on a catalogue of competencies. These serve as suggestions for decision-making for the assessment of internal or external processing of tasks.

b) Challenges

In the following section focus is set on highly relevant challenges, categorized as „highly critical" regarding risk assessment. The respective challenge is associated with high potential for damage and high probability of occurrence resp. negative effects. These include, for example, system failures, security criteria, or potential cost increase.

Significant differences for certain case studies (concerning an industry or application) are explained separately. In addition, the lifecycle phase impacted by each identified challenge is indicated.

Across all case studies, the following pattern regarding the most critical challenges can be recognized: On the one hand the HW/SW complexity of an open modular campus network increases significantly versus an established monolithic integrated campus network: The number of components and interfaces increases; some functions may be hosted on a local dedicated server, others in a (public) cloud. On the other hand, the burden of ensuring E2E functionality moves away from the network equipment provider to an internal or external system integrator. Therefore, it is a highly critical and challenging requirement that the system integrator builds up the capabilities to design and deploy an open system that meets the requirements defined by the specialized IT and OT systems.

The diversification of responsibilities is another critical challenge. If there is a single vendor that delivers all HW/SW components, a service provider can rely on vendor support in case of component malfunction. Also, the service provider can enter into back-to-back agreements with the vendor to guarantee service levels and KPIs (e.g., E2E network availability or critical fault clearance time). With a multivendor approach, this is no longer the case: A system integrator 5G must step in to guarantee E2E functionality of the multivendor system; an operator 5G must step in to guarantee E2E service levels. These aspects will become even more critical the more 5G campus networks are used not just for tests and trials but for critical processes in industry, healthcare, or other vertical domains.

As the benefits of open campus networks described above are obviously at least partly offset by additional costs for system integration, testing and more complex day-to-day operations, one of the most critical requirements – especially for deployments within the industry – is the clear demonstration of the financial viability: In the end, the plant owner has to be convinced that an open modular campus network is the best solution to meet his operational and financial targets. Otherwise, the plant owner will choose an alternative approach, be it a 5G campus network with an established monolithic integrated architecture or a completely different solution (e.g., Wi-Fi or cable).

Security appears to be a very special case. In general, security is of course a highly critical issue for all case studies, even though the impact of potential security breaches varies significantly across the case studies, from temporary service interruptions to significantly more severe scenarios. However, it is difficult to differentiate between highly and moderately critical security requirements as the weakest link in a security chain defines the overall vulnerability of a network. Again, the main responsibility to design a secure E2E solution lies with the system integrator 5G.

This chapter gives a summary of the most relevant challenges, derived from NGMN project "ODiN 2.0"[6] and requirements given by the CampusOS case studies for disaggregated campus networks. Following the ODiN 2.0 publication , the challenges are grouped into 17 categories, with each challenge being assessed as either "mandatory", "optional" or "not applicable" according to the definitions given in Table 2.

Relevance	Remark
Mandatory	From a case study perspective, these challenges demand additional effort (technical complexity, cost, time, resources/manpower). The criterion is essential for the use case.
Optional	From a case study perspective, these challenges do not necessarily demand additional effort (technical complexity, cost, time, resources/manpower). The criterion is dispensable for the use case.
Not applicable	Not applicable, no need for action

Table 2: Relevance for the assessment of challenges

6 ODiN – Operating Disaggregated Networks, 2022, v2.0, NGMN Alliance, https://www.ngmn.org/wp-content/uploads/NGMN_ODiN_v2.0.pdf

Supply chain and procurement process handling

Procurement is an important element of the supply chain. It includes ordering, buying, or leasing of HW/SW components and services. Minimizing cost is one important aspect of improving the procurement processes. It is vital to identify suppliers that provide the needed quality of HW/SW and services and have the capacity to deliver reliably, with a track record of doing so. Especially within open modular campus networks these capabilities are essential and more cost and time consuming than in traditional implementations.

Procurement processes vary greatly depending on each company's structure and needs, but generally include the following steps:

1. Identify which goods and services the company needs
2. Submit purchase request
3. Assess and select vendors
4. Negotiate price and terms
5. Create a purchase order
6. Receive and inspect the delivered goods
7. Conduct three-way matching
8. Approve the invoice and arrange payment
9. Record keeping

In the context of disaggregated systems, the increased number of suppliers is a challenge for procurement, since more time and cost are needed in the plan/design phase. Request for Information (RFI)/Request for Proposal (RFP) process will take more time and resources as more comprehensive scanning of the market is necessary. The documentation of the solution design and the preparation for the functional specification will take more time, as the interfaces and processes need to be described for every single component.
In general, the increased complexity of the system requires additional resources on each stage of the campus network lifecycle. During the design and deployment phase of the future solution design, procurement will need to handle RFI/RFP for HW/SW components. In this environment it is essential to have market knowledge and the time to carry out procurement processes. The process may be supported by consultants. During the maintenance & optimization phase – if the operator of the 5G system does not have sufficient knowledge or resources – procurement should onboard additional capacities to close the gap. On the owner/use case side, when it comes to testing and acceptance test of the system, there are additional resources needed, not only for testing, but also for documentation and going live activities.

Monitoring the market and searching for standardized HW/SW components, taking care of necessary conformity declarations, and clarifying all this with the business will take time and additional effort. This means that a higher diversity of software and / or hardware components requires more resources. Licensing schemes need to be established with multiple vendors.

Setting up an open modular campus network leads to a diversification of responsibilities. Because within disaggregated systems there is more than one partner involved, a clear description of the responsibilities, internal and external, must be defined. This definition must be part of the contract between the business partners. Service Management is the driver in the operation phase and must guarantee that all stakeholders are in the loop.

In addition to the increase in variables in purchase and delivery, there is the challenge of handling different kinds of Service Level Agreements (SLAs). The definition of SLAs is made in cooperation with Service Management and, if necessary, with other stakeholders. The goal is to standardize these SLAs for all vendors and suppliers to have the same KPIs for monitoring and reporting in place. This task is time-consuming and may benefit from external resources to speed up the process.

System integration process handling

System integration is one of the biggest challenges in adopting disaggregation. There are many possible functional split options between SW components as well as HW/SW splits due to virtualization. Many potential solutions and solution providers need to be considered for the provision of these components. The resulting key challenges extend to all lifecycle phases of an open modular campus network.

System integration challenges in the context of open modular campus networks are not necessarily due to challenges in integrating the campus network into the existing company network infrastructures. However, open interfaces require special attention for the implementation of a security concept[7]. Rather, the challenges arise because several subcomponents – in the sense of a multi-vendor setup – need to be orchestrated into a functional overall E2E solution that meets the operator's requirements (e.g. in terms of performance, reliability, ease of use). The mix and match of components, as formulated as a mission of the O-RAN Alliance, is not yet possible in a way of "plug and play". Therefore, system integration is associated with increased effort, and may result in higher costs than the integration of single vendor solutions. To provide a disaggregated system that meets customers' requirements, system integration must make sure that test cases are always provided for the integration of partial solutions as well as for the E2E overall solution, and proof of interoperability should be provided by testing under real conditions.

Shift of tasks and responsibilities means an allocation from a single vendor (of an established monolithic integrated E2E system) to at least two or a larger number of vendors for subcomponents. In this context it must be ensured that no tasks are lost and, in the best case, that there is no overlap between the various companies and roles involved. The requirement to provide a functional overall system, and thus also the overall responsibility, cannot be provided solely by a vendor. This responsibility must be taken on by the purchaser itself or by a third party.

The above aspects show that stakeholders must interact with a larger number of organizational interfaces (companies, people, roles), which can lead to increased efforts for coordination and alignment. The number of technical interfaces, on the other hand, depends on the amount of disaggregation and is predetermined by the final planned network design. Even with two vendors, the number of technical interfaces can be complex, since interfaces from the HW/SW split and SW interfaces to underlying operating systems must be considered. The interfaces must therefore be developed coherently from each vendor/supplier of the overall system. In the second step the defined interface specifications and the implemented interfaces to the involved partners must be documented. Subsequent vendors are asked to contribute actively to the interoperability testing, i.e., especially in a multi-vendor setup.

Cost handling

Cost handling is one aspect of the planning process. The expected costs must be considered. In the context of 5G campus networks, there are different models for this ranging from acquisition to operating costs. To select the appropriate model, business plans are created in advance to compare them with each other and to align them with the business.

Disaggregation promotes competition to provide cheaper equipment, but also to adjust pricing models.

One challenge that can arise from disaggregation is the increased intrusion effort and associated costs. The multitude of possible combinations leads to more and more know-how, which the integrator must bring along and get paid for. Therefore, the increased cost must be offset by benefits. The added value of this solution must be demonstrated in advance.
This leads to the second challenge. If the equipment makes production more efficient and the total cost of operation (TCO) can be reduced as a result, the additional costs can be worthwhile. This must be considered when creating business plans.

7 see e.g. https://www.teletrust.de/publikationen/broschueren/5g-campusnetze/ for more details on security concepts in 5G campus networks

Handling of competence development and training

The promise of disaggregation is that somehow components would become available and could be combined into running systems that reduce network operators' dependency on established vendors. However, it becomes clear that this shift requires a whole new set of skills. Both the operators and the vendors need to communicate and understand requirements more deeply than was originally expected. Rather more than less engineering knowledge is needed when hardware and software components from various vendors are combined into one network. Such setups require operators to deeply understand issues of functionality, compatibility, interoperability, dimensioning, interfaces, and more. Since – depending on the setup – either the system integrator or the network operator is the one having the complete picture of the network, having technical competence available becomes a key requirement to being able to design, operate, optimize, and adapt the setup.

In addition to the operator having to ensure technical competence development and training, the same is true for the vendor. No longer are vendors able to sell their solutions "as is", but they are faced with a growing number of, sometimes fragmented, solutions and components within the ecosystem, as well as system architectures that their customers are already working with. Therefore, vendors must keep a good understanding of the commercial and technical landscape, of any APIs and standards, their own position inside the ecosystem, as well as of their customer's actual requirements. This no longer allows a mindset of a vendor selling a specific product, but rather one of a vendor positioning himself inside an ecosystem and dynamically developing and adapting solutions.

The importance of a third stakeholder becomes apparent: the system integrator. Given the technical understanding needed to combine disaggregated HW/SW components and make them meet customer's needs, it seems sensible to have a role permanently established that keeps learning about technologies, trends, and solutions, and can match players within the ecosystem as well as design and operate systems.

As in the other challenges, the need for training technical skills increases with the level of complexity, be it in the number of HW/SW components and settings or in the number of stakeholders involved.

Responsibility control

The disaggregation of 5G campus networks goes along with a considerable loss of E2E responsibility: In case components from several vendors are combined and malfunctions occur, it may be unclear who is responsible and able to solve this issue. This is particularly the case if the defect is due to nonconforming interworking of these components.

The constellation that components from different vendors are used within one network is not uncommon, even in conventional network architectures. To give an example, MNOs that execute a multi-vendor strategy typically combine RAN and core systems from different vendors in their public networks. In such constellations the number of different vendors is very limited. Usually, these vendors are contractually obliged to ensure the interoperability of their components with the components of the other network equipment providers. Therefore, MNOs have been able to outsource the task to solve interoperability issues to their network equipment providers.

In open modular campus networks, however, the situation is hugely more complex: The number of components, potentially coming from different vendors and of potential vendors, might be much higher than in such conventional public network scenarios. In addition, it is reasonable to assume that such specialized vendors for open campus network components will have significantly less engineering resources than the established network equipment providers that supply public network markets globally; it will be extremely challenging for these vendors for open networks to solve interoperability issues with any other component for any other vendor.

Asset management

Economic business models and companies basically require lean and manageable processes and a clear assessment of their operated systems and the resulting expenses within the lifecycle to be able to handle and measure their business accordingly. Previous communication models were easy to measure in this respect, as they were either less complex technologies (e.g., Wi-Fi) or combined systems from a single vendor. The new disaggregation of 5G campus networks, as considered here, leads to completely new conditions. There are significantly more players, who can have completely different ideas on their system handling (costs, lifecycle, etc.). In the end, suitable measures and contracts must ensure that longterm trouble-free and cost-optimized operation is possible.

It is essential that the approach and the individual contracts are tailored to the final operating model. It must be avoided in any case that gaps in system availability or unexpected cost elements arise. One risk in the asset management of a final communications project based on an open modular campus network is the number of possible subcomponents and partners. This can lead to inhomogeneities in terms of runtimes, technological evolution, availability, and maintainability. It must therefore be clarified by the operator of the business model whether the necessary transparency, if the internal know-how is lacking, can only be ensured by purchasing possible external resources (for example in the form of a 5G provider). This usually leads to additional costs in operation but can contribute to building up the necessary know-how for future business ventures.

Fundamentally necessary steps for successful asset management for disaggregated communication assets are:

- The standardization of cost models and payment periods.
- Clear software and license models and contracts.
- Coordination of possible update cycles for hardware and software in relation to further technological development and external regulations.
- Ensuring uniform and coordinated maintenance cycles for all involved components.
- Valid lifecycle planning of the whole system.

Service, management, and orchestration

The increased flexibility in network design through disaggregation comes with an increase in complexity. The Open RAN architecture introduces a variety of new interfaces that management solutions need to comply with. Networks are increasingly expected to comprise of a heterogeneous landscape of both physical and virtualized network functions.

Network management and orchestration is concerned with making efficient use of network and compute infrastructure, monitoring network state and performance, fault handling, and supporting agile onboarding of new network services. With the increase in network complexity and the diversity of its interfaces, the integration of network management and orchestration solutions poses additional challenges compared to traditional network architectures.

Network disaggregation opens the market for management solutions, allowing smaller vendors to develop specialized solutions. While this offers chances for increased competition on the market, a broader ecosystem, and the acceleration of innovation, it also means that new and more diverse tools by potentially multiple vendors need to be handled. New competence for E2E service management regarding both technical and organizational topics needs to be acquired. This entails spending additional resources on proper training for the required tools and training regarding the management of all parts of the network as well as the application in general.

Specifically in the context of open modular campus networks, the size and complexity of the network infrastructure may vary strongly, depending on the use case. For smaller-sized networks, it can be assumed that the full feature-set and capabilities of fully-fledged network management and orchestration systems may not be required, relaxing the challenges to some extent.

A frequency usage license is required from the regulatory authority, in Germany from the Federal Network Agency (BNetzA), to operate a private 5G network in the range of 3.7 to 3.8 GHz (5G band n78). The license conditions for this band specify that it is only valid in a predefined area and that only local fixed deployments are allowed. This is typically not suitable for nomadic use cases. In the position paper „Needs for nomadic networks“ summarizes current problems. The position paper is an argumentation aid for technical and regulatory solutions towards the BNetzA as regulatory authority responsible for the approval of radio networks in Germany.

After evaluation by the BNetzA and thematic detailing in a joint workshop, the following results are written down as framework conditions for nomadic networks for emergency services:

- There is currently no solution for real ad-hoc operations and there is no solution in sight, at least in the area of campus network frequencies.
- However, the problem is generally understood, and solutions will continue to be sought.
- There are other options for less time-critical operations.

It is therefore necessary to complement the current spectrum usage conditions with an adequate approach for nomadic networks in the future.

c) Types of operating models

Network operation as fully self-operated

There are generally two motivations for self-operated and customized 5G campus networks. On the one hand, many companies want a communication network that matches the internal structure and access requirements of their own IT landscape in every respect, so that it can be seamlessly operated and maintained in accordance with their own policies to ensure maximum security. On the other hand, large companies, in particular, want to incorporate the communications factor into the development of their structure (e.g. smart factory) or their products and therefore require unrestricted access to the communications resource.

In the development scenario, self-operated 5G campus networks will therefore give companies full control over their network infrastructure. They can adapt the network to their specific needs, optimizing the performance and security of their applications, without having to seek support (from the external operator) if the parameters or configuration of the network need to be changed. The development department is directly „hands on" and responsible for the system. In this case, the SLAs for disaster recovery or operational figures are not in place or are at a basic level to rebuild the system if the development department is unable to do so.
In the case of manufacturing networks, as mentioned above, in some cases the ‚product' is a ‚golden nugget' and the manufacturer has decided that no process or other task can be operated by a third party. This is partly for security and intellectual property reasons, but also because internal production processes can be so complex and sensitive that the slightest disruption can result in significant costs. A so-called monolithic system of some kind is required to ensure that the operational behavior, once set, is guaranteed under all circumstances. Design, deployment and maintenance & operations (roles within the case studies) are carried out internally and therefore all SLAs are an internal responsibility.

Reasons for self-operated 5G campus networks:

1. Security, Intellectual Property, Performance and Privacy: In sensitive industries such as healthcare, manufacturing, and finance, maintaining data security and privacy is paramount. Self-operated 5G networks provide a higher degree of control and isolation, reducing the risk of data breaches and cyberattacks.
2. IoT Integration: 5G networks are well-suited for accommodating a vast number of IoT devices. Self-operated networks enable organizations to better manage and integrate IoT devices into their operations.
3. Reduced Operating Costs: While the initial investment in building and operating a self-operated 5G campus network can be significant, it may lead to long-term cost savings, as organizations won't have to rely on external providers for network services.
4. Future-Proofed: Self-operated 5G networks provide flexibility and adaptability to evolving technology and business needs, making them a future-proof solution.
5. Competitive Advantage: Having a robust, self-operated 5G network can give organizations a competitive advantage in terms of innovation, efficiency, and responsiveness.
6. Vertical-Specific Use Cases: Various industries, including manufacturing, healthcare, education, and logistics, have specific use cases that benefit from the deployment of self-operated 5G networks. These use cases often require tailored solutions, and they are designed to tackle diverse use case requirements and ensure proper Key Performance Indicator (KPI) fulfillment, which is crucial for industrial applications like intralogistics in Industry 4.0, connected mobility, agriculture, and more.

In summary, the main drivers for self-operated 5G campus networks are the need for organizations to have greater control, customization, security, and reliability in their network infrastructure. This is especially important in industries where security, intellectual property, and the ability to handle a large number of devices and data-intensive applications are critical.

Network operation as a service

„As a service" operation for 5G campus networks can be applied to „fully private networks" as described in the previous subsection or to networks that are deployed and operated in cooperation with a Mobile Network Operator (MNO). In 3GPP[8] these two cases are referred to SNPN (Stand-alone Non-Public-Networks) and PNI-NPN (Public Network Integrated Non-Public-Network). Both networks can be implemented with very different deployments as discussed in (Board, 2022)[9]. In the following we first discuss the PNI-NPN case and subsequently the SNPN case.

8 3GPP: Non-Public Networks (NPN), Dec 2022, https://www.3gpp.org/technologies/npn

9 5G PPP Technology Board: Non-Public-Networks – State of the art and way forward, Nov 2022, https://5g-ppp.eu/wp-content/uploads/2022/11/WhitePaperNPN_MasterCopy_V1.pdf

MNO-integrated 5G Campus network (PNI-NPN)

An industrial company can have its own 5G campus network, which is nevertheless integrated in an MNO's network and managed by them, a so-called PNI-NPN. The business owner has the flexibility to design various aspects of the network according to its specific requirements. Depending on the needs, the business case owner can decide to use his own private licensed frequencies or the frequencies assigned to the MNO.

Sharing a portion of the mobile operator's spectrum through a dedicated „slice" is another option. The exclusive private infrastructure offers the business owner more control, while a slice of the public network may be more cost effective.

Setting specific requirements, e.g. on network operation, for the MNO is another key aspect. The business owner defines specific quality requirements for the services and requests that the provider meets them. This includes providing the required Quality of Service (QoS) for different services to ensure optimal performance. Depending on the capabilities and offers of the provider both parties may negotiate an SLA (Service Level Agreement) as a part of their mutual contract.

The provider may give access to various tools to the business owner for effective management of the 5G network. These include monitoring tools, APIs (Application Programming Interfaces) and SLA (Service Level Agreement) agreements for various fault levels. These tools enable detailed monitoring, control and optimization of the network according to the business owner's requirements, but always only limited within the boundaries agreed between the provider and the business owner. In particular, even in this case, the business owner must spend some internal effort and has responsibility to adjust the network performance according to the before mentioned capabilities. Overall, management by an MNO allows the customization of a 5G campus network according to the specific needs of a business owner, ensuring flexibility, control and optimization.

Private 5G Campus Network (SNPN) managed by a 3rd party

An external service provider can be commissioned to implement the 5G Campus Network for a business owner. This network comprises various key elements, including the 5G RAN (Radio Access Network), the 5G User Plane, the 5G Control Plane, subscriber management and application management. These components can be provided as a complete solution or some parts by one or more specialized providers, with the business owner selecting the service providers and suppliers according to its own preferences.

The design of the private network is based on the business owner's specific design requirements. This allows customized solutions that are precisely tailored to individual needs and requirements. Service providers and vendors are also selected according to the requirements and standards of the business owner to ensure that the implementation meets the highest quality and performance standards.

The network is set up by a system integrator who specializes in the integration of various technologies and components. This integrator is responsible for seamlessly integrating the various network elements and ensuring smooth operation. The maintenance of the 5G campus network can either be carried out by the system integrator or by the business owner's staff itself, depending on the preferred operating models and resources. If so, it is already a hybrid version of an operating model, and is discussed in the following subsection, and allows the business owner a lot of flexibility to retain control of the maintenance process or rely on the integrator's expertise to ensure optimal performance and availability.

Network operation as hybrid models

Between these two poles of purely self-operated and purely third-party managed campus networks there is a continuum of operating models with some degree of shared tasks between the parties involved.

On the one hand, e.g., even private networks with dedicated on-site components may have some form of vendor or operator involvement. The most common 5G systems for private networks have a cloud-based network management, which is realized on a cloud system operated by the vendor. In addition, debugging of software code or solving hardware malfunctions can typically only be done by the vendor.

On the other hand, e. g. even in the case of a purely virtual campus network, the plant owner will typically execute some day-to-day tasks himself without involvement of the network operator, e. g. managing SIM cards and devices or monitoring the network status and KPIs.

For the sake of clarity, the following considerations apply to hybrid operating models with substantial tasks shared between the parties involved, while models with one party only fulfilling minor tasks are considered as "self-operated" or "as a service". There can be many drivers for choosing a hybrid model, including both architectural and business requirements. This is discussed in the following points.

Hybrid operating models as a consequence of architectural choices

In general, the more components of a network are shared, e.g., in form of a fully or partially shared 5G core on a public cloud or a RAN shared with the public network, the less degrees of freedom to choose a specific operational model are available. Therefore, the choice of a specific architecture will impact the choice of the operational model and vice versa.

This becomes even more relevant in the case of open and modular campus networks, which offer an even broader scope of architectural options with virtualized and cloudified components. For example, the CU of an Open RAN system and the control plane of a 5G core may be realized in a public cloud, while latency-critical functions are realized on-premises, with the former components being third-party operated and the latter being self-operated or third party operated.

Hybrid operating models as a result of business decisions

Hybrid operating models may be the result of a deliberate business decision, as they may combine advantages of self-operated and third-party operated networks.

Operating a campus network comprises one-time tasks, in particular in the planning and deployments phase, and recurring tasks in the operations/maintenance phase. Typically, the one-time tasks require highly specialized skills and deep system know-how, e. g. radio planning and system integration. In many cases, it appears to be an attractive option to build up know-how primarily for the recurring routine tasks while outsourcing one-time and occasional tasks to a third party with highly specialized know-how. This may e. g. lead to an operating model with a third party responsible for design and deployment, while the own organization takes over responsibility after the hand-over of the fully implemented and tested system from this third party. In the operational phase, the external operator only performs few tasks with an impact on the overall functionality of the system, e.g. yearly software updates, while day-to-day tasks are performed by the own organization.

Hybrid models may also be an attractive choice when the use case is very demanding with respect to operational aspects. To realize minimum fault clearance time at acceptable costs, a model can be implemented with own mid-skilled 24/7 resources and local spare parts, supported remotely by a highly skilled specialist from a third-party service provider.

Concerns about hybrid operating models

Hybrid operating models also come with disadvantages, which may or may not outweigh the advantages described above.

1. It will be necessary to provide some own resources for the tasks done by the own organization. For small implementations with a limited number of devices, this might be seen as not economical. Companies without a large IT unit may prefer to focus on their core competencies and not to build up resources for an enabling function.
2. In case tasks are shared between the own organization and a third party, it is difficult to assign an end-to-end responsibility for maintaining operational service levels.
3. The communication between the internal and the external team must be organized, which may cause additional complexity. E.g. a joint ticketing system needs to be set up.

Market insights

As the CampusOS network tracker[10] shows, currently the most common operational model with tasks distributed between the own organization and a third party is „*design and deployment by third-party; operations/maintenance by own organization*". More complex models with distributed tasks within the lifecycle phases have not been identified.

10 The Campus network tracker collects information on currently existing 5G campus networks in Germany based on publicly available sources. More information is given in section 3.3 of the report "Monitoring: Campusnetze": https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/5G_Campusnetze/20240212_monitoring_campusnetze_qt4.pdf

4. Task oriented guidance for hybrid operating models

Required tasks and competencies to design, deploy, and run a 5G private network

As mentioned above, the lifecycle of a 5G campus network is characterized by different phases. These are design, deployment, maintenance, and optimization (M&O), and finally rebuild. Within the first three phases in particular, several tasks need to be performed. For each of these tasks, the business owner must decide whether it will be performed by its own staff („in-house") or by a third party („external" or „outsourced"). From the case studies, we learned that these decisions could vary widely. In fact, the two poles – all tasks being fulfilled in-house, or all tasks outsourced – represent only special variants of a hybrid model when viewed from a „task-oriented" perspective. Most operating models are therefore a mixture, as discussed already in the previous sections.

In addition, executing a task needs specific competencies, independently if it is done by own staff or by subcontractors. The subsequent table describes these competencies in two variants. While the first variant directly relates to the „doing", a second variant is looking at the „managing" (or validating) of the execution of the task. „Doing" means here, that the tasks for designing, building, and operating a 5G campus network are executed with a sufficient and suitable quality by people who (at least should) have the ability and experience to do so. Obviously also the validation of the execution of a task is required by the business owner if the execution itself is outsourced to a third party, such as an external subcontractor or an internal department. If a business owner is not able to cope or organize these competencies a 5G campus network might not be a good choice.

Table 3: Tasks to design, deploy, and run a 5G campus network and competencies required to execute or to validate these tasks.

Decision point	Lifecycle phase	Task description	Competencies required for task execution	Competencies required for evaluation
Business case evolution/ evaluation	Design	Evaluate business case resp. develop of business model and prepare application for frequency spectrum at regulatory (BNetzA) and other authorities (LBO)	Business knowledge to model the business case, to specify its goals, and to align them with the overall business strategy, including a high-level understanding of the use case and financial expertise for the development of a business model. Basic technical expertise for the application of frequency spectrum, e.g., demand in bandwidth as a relation to throughput, antenna parameters and radio planning. The responsibility for this activity cannot be delegated	Business management, financial controlling, and availability of all the assumptions and the corresponding KPIs that were used to develop the business model, as well as access to data for periodical assessment. The application for a radio frequency range must be done by the business case owner and therefore, expertise in the application process is mandatory, including legal and technical competencies for checking plausibility.
Requirements and specifications	Design	Find out customer's needs and requirements and define functional specifications. Plan application and open modular 5G network components accordingly and in compliance with industry standards, technical guidelines and regulatory requirements. Prepare frequency application and do further planning for 5G system in terms of approval law (e. g. building law, BNetzA) and for the application (e. g. ascent permit drone, machinery directive). Define requirements for application and 5G system accordingly (on your own, with business, with external consultants, or with contractors). Define acceptance criteria for the application and the 5G system (on your own, with business, with external consultants, or with contractors).	Project management expertise is required, including high-level understanding of business and technical application, as well as and networking aspects for requirements analysis. High-level knowledge of the application from end-to-end perspective (incl. requirements) is needed to design the application, infrastructure, and network architecture. Knowledge of industry standards and guidelines is needed to ensure compliance of the design. 5G architecture and system engineering knowledge is needed for planning the radio network (e.g., RF and capacity planning, interfaces, dimensioning, access, placement, cabling, and housing), including related legal and regulatory requirements.	Project management knowledge with a good technical understanding to check completeness of requirements specification and system design. Strong technical expertise (incl. economics) to ensure compliance with industry standards, adherence to regulatory requirements and alignment of architecture and customer's specification. Expertise in communication network planning, network dimensioning, radio coverage planning, data traffic models, and RF-propagation models are required for a proper check of technical plausibility of the design. Legal plausibility checks require expertise in different legal domains (e.g., local RF regulations, building & construction, workplace).
Procurement	Design	Prepare RFQ (incl. KPI and SLA specifications) and carry out procurement process	Break down specifications to trades and lots (in German: Gewerke), to create RFQ documents, to define and run RFQ processes, incl. knowledge of payment and warranty conditions. Deep understanding of the business needs to evaluate the results.	Legal knowledge and knowledge of the business rules and processes to ensure compliance to the RFQ and procurement decisions and processes. Completeness of RFQ has to be ensured by prior validation.
Acceptance evaluation	Design	Prepare RFQ (incl. KPI and SLA specifications) and carry out procurement process	Break down specifications to trades and lots (in German: Gewerke), to create RFQ documents, to define and run RFQ processes, incl. knowledge of payment and warranty conditions. Deep understanding of the business needs to evaluate the results.	Legal knowledge and knowledge of the business rules and processes to ensure compliance to the RFQ and procurement decisions and processes. Completeness of RFQ has to be ensured by prior validation.
Acceptance evaluation	Design	Application and 5G system is handed over. Acceptance criteria (incl. regulatory requirements) for 5G system are fulfilled and documented.	Diligence, prudence as well as some skills in technical writing for the preparation of the planning documentation for receiving permits. Receiving the permit might come with some conditions, which needs to be turned into technical guidance to internal and external staff. Good understanding of the processes related to all systems, including both application and 5G system, are necessary for the handover of the application and 5G system. Good communication skills support the writing of precise and comprehensive documentation	High-level competencies in the domains of 5G systems and application for verification and approval of design decisions and to give the "ready to deploy" go-ahead. The latter is the final step in the design phase and might not be delegated to 3rd parties. Project management skills with a clear technical background for preparing the milestone report with approval checklist and hand over document.
Integration of 5G network and business applications	Deployment	Set up 5G network according to customer's specification in compliance with applicable industry standards, directives and legal resp. regulatory requirements resp. integrate 5G system into existing customer environment. Deploy/provide customer interface for maintenance and optimization. . . .	Application domain and 5G systems expertise to provision the 5G system and application according to the specifications of the design phase and regulations (incl. relevant industry standards). Good relationships to business owner and communication make it easier to consider and integrate its specifications. . . .	Approval and acceptance of the installation according to the design and requirements from the design phase according to specifications from design phase - no specialized competences required. Technical knowledge of the application, 5G system, and customer environment to review and accept interface and system tests. . . .

Decision point	Lifecycle phase	Task description	Competencies required for task execution	Competencies required for evaluation
		Ensure compatibility of each single component through interoperable interfaces and through proof of test cases, e.g. interfaces for manage-ment of components or to other Open RAN com-ponents (as O-RU, O-DU, O-CU), interfaces to Core NW, NW Technology, n-RT-RIC / non-RT-RIC, SMO, and to user equipment. Train and educate different target groups on relevant func-tionality, usage, and operation.	Integration and system engineering, including hands-on and trouble-shooting experience (incl. broad knowledge of the 5G system, application, customer environment, and interfaces) for the integra-tion. Comprehensive 5G system and testing expertise for in-depth testing of the 5G system components and their interfaces (incl. configuration, LAN networks, Open RAN, and RF), as well as systematic software testing. Deep knowledge and proper training skills on the 5G system to run training and education.	High-level understanding of 5G systems and knowledge of the interfaces to review and accept functionality, compatibi-lity and performance. Organization of training on operating the 5G system and assessment of provided content and training quality.
Testing	Deployment	Test and proof all functionalities according to requirements	Software and system testing spanning from test design to test execution and lastly test reporting, incl. sufficient knowledge of the system-under-test.	Technical understanding to review, approve, and accept test specification.
Acceptance evaluation	Design	Prepare RFQ (incl. KPI and SLA specifications) and carry out procurement process	Break down specifications to trades and lots (in German: Ge-werke), to create RFQ documents, to define and run RFQ pro-cesses, incl. knowledge of payment and warranty conditions. Deep understanding of the business needs to evaluate the results.	Legal knowledge and knowledge of the busi-ness rules and processes to ensure compliance to the RFQ and procure-ment decisions and processes. Completeness of RFQ has to be ensured by prior validation.
Acceptance evaluation	Design	Application and 5G system is handed over. Acceptance criteria (incl. regulatory requirements) for 5G system are fulfilled and documented.	Diligence, prudence as well as some skills in technical writing for the preparation of the planning documentation for recei-ving permits. Receiving the permit might come with some conditions, which needs to be turned into technical guidance to internal and external staff. Good understanding of the processes related to all systems, including both application and 5G system, are necessary for the handover of the application and 5G system. Good com-munication skills support the writing of precise and compre-hensive documentation.	High-level competencies in the domains of 5G systems and application for verification and approval of design decisions and to give the "ready to deploy" go-ahead. The latter is the final step in the design phase and might not be delegated to 3rd parties. Project management skills with a clear technical back-ground for preparing the milestone report with approval checklist and hand over document.
Integration of 5G network and business applications	Deployment	Set up 5G network according to customer's specification in compliance with applicable industry standards, directives and legal resp. regulatory requirements resp. integrate 5G system into existing customer environment. Deploy/provi-de customer interface for maintenance and optimi-zation. Ensure compatibility of each single component through interoperable interfaces and through proof of test cases, e.g. interfaces for management of components or to other Open RAN components (as O-RU, O-DU, O-CU), interfaces to Core NW, NW Technology, n-RT-RIC / non-RT-RIC, SMO, and to user equipment. Train and educate different target groups on relevant func-tionality, usage, and operation.	Application domain and 5G systems expertise to provision the 5G system and application according to the specifications of the design phase and regulations (incl. relevant industry standards). Good relationships to business owner and communication make it easier to consider and integrate its specifications. Integration and system engineering, including hands-on and trouble-shooting experience (incl. broad knowledge of the 5G system, application, customer environment, and interfaces) for the integration. Comprehensive 5G system and testing expertise for in-depth testing of the 5G system components and their interfaces (incl. configuration, LAN networks, Open RAN, and RF), as well as systematic software testing. Deep knowledge and proper training skills on the 5G system to run training and education.	Approval and acceptance of the installation according to the design and requirements from the design phase according to specifications from design phase - no specialized compe-tences required. Technical knowledge of the application, 5G system, and customer environment to review and accept interface and system tests. High-level understanding of 5G systems and knowledge of the interfaces to review and accept functionality, compatibi-lity and performance. Organization of training on operating the 5G system and assessment of provided content and training quality.
Testing	Deployment	Test and proof all functionalities according to requirements	Software and system testing spanning from test design to test execution and lastly test reporting, incl. sufficient knowledge of the system-under-test.	Technical understanding to review, approve, and accept test specification.

Table 3: continuation of previous page

Decision point	Lifecycle phase	Task description	Competencies required for task execution	Competencies required for evaluation
Operational issues (incl. (e)SIM man-agement, orchestra-tion, HW and SW releases)	Maintenance & Optimiza-tion	Define responsibilities and implement operational proces-ses. Orchestrate automation of the entire network (e.g., configu-ration adjustment, transmission powers, virtual architectu-re). Define and set up processes for SIM card management, HW and SW release management (e.g., provision of SW patches and optional feature enhancements).	Automation of orchestration, incl. provision of tools / inter-faces for automation of workflows and processes for hand-ling all „every day" jobs (includes de-tecting failures (FCAPS functionalities), KPI handling / reporting, etc.) Engineering tasks like updates (hot fixes), software license handling, replacement of components, E2E network, etc. need to be managed - typically a task of skilled IT staff. Tools for management of SIM/eSIM, AAA processes, and cre-dentials need to be integrated with exist-ing access manage-ment tools. Awareness and technical understanding for (cyber-)security issues, certificate management and handling. The operator must know the telecommunications laws and be able to assess and represent them regarding its network properties and operational services. This also includes compli-ance with regulations to protect privacy, but also the environ-ment as well as health and safety of workers.	High-level knowledge on service process management to prepare and accept an operational handbook summarizing the settings of the provision of the technical support. A general understanding of the whole network is required to verify that the orchestration satisfies the requirements and legal and regulatory constraints. Authentication and configuration management is key to the security concept of any en-terprise IT and therefore needs proper integration with the 5G system. System engineering incl. update management is part of net-work operation and needs „hands on" experience in system integration and management. Since legal responsibility can never be sub-contracted the business owner has to be aware of all legal implications. This might need legal support by lawyers and experts.
Support	Maintenance & Optimiza-tion	Provide technical support as 1st, 2nd or 3rd level for both, application and subcomponents (also for fulfilment of the SLA for defined KPIs; if necessary, patch management, in-cident mgmt., fault clearance). Provide interfaces to BSS, OSS and other support systems. Provide technical tools for service request management system for MACD/S (Move, Add, Change, Delete/Service).	Technical support is typically structured in a hierarchical way and is used with specialized systems and processes (ticket tools e.g.): 1st level - identify the area of support and to fix easier issues by a structured, pre-defined way. 2nd level - more expertise and good knowledge on problem analysis in all parts of the 5G system (core, transport, components, air interface, as well as applications), also incl. process know-how on those areas the 5G system is used for. 3rd level - deep un-derstanding with focus on the components themselves, incl. SW debugging skills. Technical knowledge as well as a deep business and use case understanding of interfaces to company IT systems like ERP or CSM. Service request tooling and business and administrative pro-cess understanding is required - for the operation of MACD (Move, Add, Change, Delete/Service) it is essential to provide technical tools for their support by a kind of ticket handling (e.g., via Remedy, ServiceNow, JIRA).	Good understanding of service management KPIs (response times, severity, ...), as well as tool implementation details for the service process documentation. A high-level understanding of all involved systems to vali-date the necessary interfaces with respect to functionality, compatibility, and performance. Limited technical and process insights to receive informa-tion on the provisioned tools and service request process and accept them.
Support issues (1st / 2nd / 3rd level, troubleshooting, ...)	Maintenance & Optimiza-tion	Ensure that E2E monitoring and reporting is set up and running; troubleshooting tools for root cause analysis are in place and used. In case: Know and claim warranty for the provided network solution.	Analytical skills, technical as well as economical know-how, incl. knowledge on different interfaces with their special capa-bilities to define KPIs and to create reports. Capability for root cause analysis within the tool sets requires trained engineers with a lot of technical expertise for trouble-shooting. Deep engineering skills for network solutions are required to guarantee correct operation of a de-ployed 5G network.	A high-level understanding of technical aspects to unders-tand and confirm the selected technical KPIs and monitoring methodology as well as to subsequently check and accept monitoring reports. In-depth knowledge of the financial aspects tied to the sys-tem is required to define, monitor, and report these KPIs. High-level knowledge of the 5G system, application, and support systems are sufficient to accept reports of root cause analysis and approve actions that are necessary. Skilled and trained persons with a good technical as well as economical background with good understanding about the capabilities and performances of the 5G system in the actual integration environment to assess warranty cases.

a) In-house vs. external evaluation scheme

As outlined in the previous section, several tasks are required to decide on a 5G campus network and to design, plan, build and operate it. Some of these tasks will or must be performed by the business owner itself („in-house"), some will have to be performed by third parties (other providers or other business units within the same company). A hybrid operating model is the sum of these decisions. In the evaluation scheme presented below, the business owner can use the aforementioned guiding questions to decide whether to outsource this task to a third party. Such an assignment is always associated with (internal or external) cost accounting, so it is also immediately clear what funds may need to be made available for.

Along the tasks listed in the table in the previous subsection the business owner should go through the following questions for each task individually. Not every question is always applicable, but it is usually necessary to weigh up the various criteria before deciding whether to take on a task yourself or outsource it. While designing and implementing the network many further questions may arise, like they are described in TeleTrusT's guideline (s. above) on security in 5G campus networks.

Basic questions guiding to your decisions:

- Do I have the time / resources / budget / skills to do this myself?
- Are there central guidelines in the company that need to be taken into account?
- How important is the protection of intellectual property in this task?
- Do certain regulatory requirements have to be met? Am I in a position to do this?
- Do I have an overview of the technical and financial offerings on the market?
- Which SLAs / KPIs are relevant? How can these be measured and checked?
- Do I have / do I need interchangeability of manufacturers / providers?
- Do I want to integrate into an existing system?
- Am I in a position to support continuous further development of the technology and
- surrounding system?
- Am I dependent on future functional enhancements?

By answering these questions (and maybe further ones found as relevant) the business owner can evaluate the previous listed tasks regarding his preference to keep it in-house or provide it to external partners.

5. Conclusion

The exploration into operating models for open and modular campus networks shows the complexities and opportunities of 5G technologies. Through comprehensive study of use cases, the research illuminated the value chains, operational hurdles, and the array of operational frameworks necessary to navigate the evolving landscape of campus networks.

This approach was used for an analysis of organizational and functional requirements for operation of open modular campus networks and several challenges within the decision process finding a proper operating model were identified. The complete lifecycle of a campus network was investigated and challenges with different complexity and impact were identified.

A key result of this research is the development of a comprehensive operating model framework tailored for open and modular campus networks. This framework encompasses organizational processes, competency layers, technological configurations, and business considerations. It serves as a guidance for stakeholders to design, deploy, and maintain 5G private networks, accommodating a spectrum from fully self-operated models to hybrid and third-party managed solutions.

This work also provides detailed task-oriented guidance for designing, deploying, and running a 5G private network. This encompasses from the evolution of business cases through procurement and deployment to maintenance and optimization. It highlights the importance of balancing in-house capabilities with external expertise, ensuring flexibility, control, and optimization of network operations.

Overall, the transition to open modular campus networks presents a transformative opportunity for industries to leverage 5G technologies tailored to their specific operational needs. The challenges identified require developing competencies, managing costs effectively, ensuring seamless integration, and operating diverse system components. The proposed operating model framework and the task-oriented guidance offer a structured approach to navigate these complexities. As 5G technologies continue to evolve, these findings provide a foundational understanding for stakeholders to be successful in the emerging landscape of modular and open campus networks.

6. Appendix

a) Definitions

The following section describes terms that are frequently used in this document to describe different realizations of operating models and value chains and achieve a better understanding of how they are constituted.

Task

A task describes a set of activities that need to be performed during the lifecycle of a 5G campus network. The activities making up a task come with corresponding requirements for their completion such as efforts, related costs, required rights, expertise, and capabilities and potentially other requirements. Usually, activities related to the same task are technically closely related and performed by the same actor. Each task can be attributed to a phase of the network's lifecycle such that the lifecycle phases form a natural grouping for the tasks.

The notion of a task helps to unify the view on the activities appearing in various use cases by providing an abstraction that shall be usable across use cases. For instance, the activities related to performing radio planning in an industrial factory setting may be different from those in an agricultural setting, but the task of „radio planning" is valid in both settings.

A task describes a set of activities and related responsibilities.

Role

A role describes a collection of responsibilities in the lifecycle of a 5G campus network. The responsibilities can often be described in terms of relations towards relevant tasks. For instance, a role may be responsible for performing the work for achieving a task or it may be accountable for its successful completion. In other cases, the role may be responsible for providing support towards the task's completion or shall be kept informed about its progress and status. Roles are assumed by actors that then take the related responsibilities onto them.

The notion of a role serves to reduce the overall complexity of describing an operating model. This is achieved by aggregating multiple tasks into those that are technically related and usually performed by the same actors as they may be analyzed together. At that level of abstraction, a role describes „what needs to be done" with the corresponding responsibilities, rights, and requirements.

A role is a collection of responsibilities related to a set of tasks.

Actor

An actor is a person, group, or organization that affects the 5G campus network by assuming one or more roles and taking the corresponding responsibilities. In this way an actor may be accountable for the successful completion of a certain set of tasks, may gain responsibility for achieving their successful completion, shall provide consulting support or needs to be kept informed on their progress. In particular, the actor needs to fulfil all relevant requirements for living up to the responsibilities pertaining to the associated tasks (e.g., efforts, expertise and capabilities, related costs, and rights).

It is to be expected that the number of different actors involved in the operation of an open modular 5G campus network /system is higher than in the operation of a proprietary monolithic system due to the diversity of the hardware components and vendors to be managed and also due to the special requirements on network performance in industrial use cases and the need for tight integration into business IT/OT, among others.

In contrast to the role itself, the actor represents „who is responsible for it to be done" but not "what needs to be done".

An actor assumes roles and takes corresponding responsibilities.

Stakeholder

A stakeholder is a person, group, or organization that is affected by the campus network, interested in it, or able to affect it. While the notion of a stakeholder is closely related to that of an actor as both describe parties that may affect the operation of the network, they differ in what they are supposed to express. The actor is supposed to capture information about the activities to be carried out together with corresponding responsibilities. The stakeholder on the other hand shall focus on the perspective on what interests the involved parties have in the lifecycle of 5G campus networks, what influence they can exert, and how their attitude towards it is.

A stakeholder is a person, group, or organization affected by and/or interested in the campus network.

Value chain

A value chain for 5G open modular campus networks is the progression of value creating activities and the provision of hardware and software components that provide the end customer (business case owner) with an end-to-end solution. Each activity is associated with specific roles – performed to support all phases of the network's lifecycle. It shall help in exposing business relationships between various stakeholders in order to explore different technical deployment options.

A generic value chain for open 5G campus networks considers all products (hardware and software) to operate a network as well as all necessary services to plan, deploy, operate, and optimize the system until end of life.

A value chain is the progression of value creating activities in the lifecycle of a 5G network.

Operating model

With the above notions of tasks, roles, and actors at hand, the term "operating model" describes how the roles that are relevant for the operation of a 5G campus network are distributed and aggregated among the relevant actors. This entails which tasks each actor is responsible for and in which lifecycle phases of the network he is responsible for. Also, which efforts are involved, which expertise, capabilities, and rights are required to be present with the actors to be able to fulfill their respective roles.

The description of a concrete operating model for 5G campus networks shall ensure to consider the following items:

1. Different phases within the lifecycle of campus networks
2. Differentiation between stakeholders, actors, and roles
3. End-to-end perspective
4. Network elements and their locations
5. Association of tasks with roles
6. Differentiation of ownership and administration/management

Many different possible realizations of operating models for 5G campus networks are possible, ranging from „full self-operation" by the business case owner via hybrid models with responsibilities both in the hands of the business owner as well as external parties to operation as a „fully managed service" by an external party.

An operating model describes the distribution of roles across all relevant actors.

b) Identified roles for network operation

Table 4: Identified roles for the operation of campus networks

Role	Description
Product / Service Provider	Represents the provision of a service / product which is made possible by using a 5G campus network solution (the 5G campus network solution is inherent part of the overall solution).
System Integration Product / Service	Commissioning (including planning aspects) and implementation of the application into the IT-/OT-environment.
System Integration 5G Systems / Communications	Commissioning (including planning aspects) and implementation of the 5G campus network solution into the IT-/OT-environment.
Business Case Owner	Owns the business case and provides requirements, spatial, technical, and regulatory conditions to implement the 5G campus network solution and its extensions (including licensed spectrum). The entity pays for the provision and is a beneficiary of the advantages achieved by the 5G network campus network solution (e.g. higher efficiency).
Use Case Owner / Works Manager	Is the entity which is responsible for the process. He is responsible for a use case that is covered by the 5G campus network solution (e.g., can be a higher-level organization entity or an end user).
Operator 5G Private Campus Network	Operates in a facility (for a facility) a 5G private campus network according to the specifications, including all support levels and maintenance.
Operator IT	Operates the IT system of a facility according to the requirements, including all support levels and maintenance.
Operator OT / Process	Operates the process / OT system of a facility according to the requirements, including all support levels and maintenance.
Compute Provider	Provides cloud services (e.g., computing power for RAN & Core SW, control, analytics, etc.) alternatively or complementary to the Internal IT/OT.
Regulatory Approval and Licensing	Legal approver which is responsible for granting authorizations (e.g. frequency allocation, building permission, drone ascent license).
Supplier Industrial Service Apps	Provides OT software components and interfaces for industrial services (e.g., data lake and data connectors).
Supplier Management SW	Provides software components and interfaces for management services (e.g., industrial network management, SMO/MANO, nonRT-RIC, rApps).

Role	Description
Supplier Business Service Apps	Provides IT software components and interfaces for Business Service Applications (e.g., Industrial Control Process with requirements for the system).
Supplier RAN Components	Provides individual SW and / or HW components of the 5G campus network (e.g. CU/O-CU, DU/O-DU, nearRT-RIC, xApps).
Supplier Network Core	Provides software entities (e.g. core network components, VNF) for the 5G campus network solution.
Supplier Compute HW	Provides compute HW components (typically COTS-based: server blades, HW accelerators, etc.).
Supplier Network Technology WAN/LAN	Supplies network components (routers, switches, cables, ...).
Supplier Network Technology Radio	Provides RF components (RU and antennas; e.g., DAS or Small Cells / full gNodeB).
Supplier Backbone Network	Provides access to an external network (e.g., fibre cable, microwave, a slice in an MNOs public 5G network). External could be private or public but is not part of the 5G network solution.
Supplier 5G User Equipment	Provides the devices (e.g., drone/agv with M2.Module) which are connected to the 5G campus network solution for the application.
5G Network App Platform Provider	Provider of a PaaS infrastructure, which takes the marketing of tested, certified & approved solutions of the xApps & rApps as its central task.
Civil Works (Building Network Infrastructure)	Contract partner of the „initiator/landlord" who provides standard services for network installation.
Data Protection	Ensures compliance with legal and company-specific rules and requirements related to data protection for the planning, operation and use of the 5G campus network solution (e.g. Protection of users' / administrators' personal data).
Information Security	Ensures compliance with legal and company-specific rules and requirements related to information security for the planning, operation, and use of the 5G campus network solution to achieve protection goals, e.g., confidentiality, availability and integrity.

Role	Description
Occupational Safety	Ensures compliance with legal and company-specific rules and requirements related to electromagnetic compatibility (EMC) for the planning, operation, and use of the 5G campus network solution (e.g., Occupational health and safety; Protection of machines and equipment related to external immunity).
Works Council	Ensures the interests of employees. - Approval of new technology and tools - Laws and collective agreements are observed. - Employees' views regarding improving the workplace are monitored, e.g., implementation of new technology (like radio emissions). - Monitoring of security @ the job

Identified roles for medical use cases

Table 5: Specific roles of a medical 5G private network

Role	Description
5G-Taskforce	A dedicated team assigned to the 5G project aimed at establishing 5G connectivity, encompassing representatives from all impacted departments to serve as a coordinating interface for both external and internal end users. Some clinics also historically have a telecommunications department that takes on this role.
Construction and building services	This department handles the physical modifications needed, such as laying cables and installing cooling systems. It might operate independently from the clinic itself.
Medical Engineering Dept. (MT)	Manages all aspects of medical devices and software, from procurement to error handling, working closely with the IT Department to define necessary performance parameters based on clinic use cases.
IT Department	Oversees the administration of networks, devices, and software, ensuring these meet the operational parameters set jointly with the MT Department.
Clinics and medical devices	Clinics, such as radiology and dental offices, are the main users of the network, setting requirements for medical devices to support high-level communication protocols like HL7/FHIR, DICOM, or IEEE 11703 SDC. The Operations and Maintenance Team (OMT) purchases 5G-enabled medical devices from vendors based on these needs. IT then authorizes these devices for network use. Future expectations include patients bringing personal medical devices, like smart insulin pumps, requiring clinics to develop strategies for secure integration and connectivity to maintain network safety.
Staff and Guests	Staff and guests require network access for their personal devices, necessitating broad connectivity solutions.
Public health insurance	Does the financing of all costs that can be mapped to a specific treatment
Government	Does the financing of all costs for new infrastructure or specific technological projects.
Board of directors	Specifies overall strategic direction, decides on financial expenses and project realization. Is involved in the steering committee, controlling the overall project direction.
Data protection officer	Overseeing all activities related to the handling of personal data for patients, staff, and trial participants. It includes the authority to veto any procedures that could compromise data protection standards and involves ensuring compliance with legal and regulatory requirements related to data protection.
Information Security Officer	Oversees the management of health and personal data transfer, storage, and access, ensuring the clinic's data security and IT safety. It grants the authority to veto any actions that could jeopardize data security standards and is responsible for confirming compliance with IT safety and security guidelines, such as ISO/IEC 27001.
Occupational safety representative / EMC	This role is focused on safeguarding individuals and devices from potential harm, specifically targeting protection against electromagnetic radiation in the given context.
Vendor Medical Product	This entity is responsible for designing, producing, and distributing Medical Technology (MT) products, which may include hardware or software, such as defibrillators, medical imaging devices, or tumor decision support software. It is crucial for this entity to guarantee that these products comply with the clinic's network requirements and adhere to relevant federal laws, like DIN EN 60601 and the Medical Devices Act (MPG).
Vendor IT Application	This entity focuses on designing, implementing, and selling IT products, which may be hardware or software, including applications, drivers, and mobile apps such as network switches or web-based patient portals. It must ensure that these products are compatible with a clinic's network requirements and comply with federal laws and regulatory guidelines.
Mobile Radio General Contractor (GC) (Pool)	Oversees the comprehensive organization, coordination, and execution of the 5G project, including managing all related sub-projects and subcontractors. They are responsible for risk management, ensuring adherence to schedules, budgets, and quality standards, and bear liability for any issues arising during the project. Additionally, they serve as the primary point of communication with the customer, regularly updating them on project progress and facilitating clear communication among all involved parties to meet customer requirements.

Role	Description
Mobile Radio Construction	Involves the setup, installation, and management of the 5G system's hardware and infrastructure, including core servers, radio access network (RAN) hardware, network equipment, cabling, power supply, and air conditioning. Optional tasks may include constructing steel supports for antennas.
Mobile Radio Integration	This role focuses on the deployment and configuration of software for the 5G system and network technology, including the setup and integration of core software, RAN software, and network software.
Mobile Radio Planning & Optimization	This role entails the design and configuration of the overall 5G system, includ-ing parameterization of the 5G RAN and core, as well as acquiring licenses for 5G campus networks.

Contact

Coordinators

Prof. Dr. Slawomir Stanczak
Head of Wireless Communications and Networks Department
Fraunhofer-Institut HHI

Prof. Dr. Thomas Magedanz
Director of Business Unit NGNI
Fraunhofer FOKUS

Address

Fraunhofer Heinrich-Hertz-Institut, HHI
Einsteinufer 37
D–10587 Berlin

Web campus-os.io
E-mail info@campus-os.org

CampusOS

Supported by:
Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag