Private 5G Networks for Connected Industries

Deliverable D2.2

Final Report on Private 5G Network Architecture and Operator Models

Co-funded by the Horizon 2020 programme
of the European Union in collaboration with Taiwan

Date of Delivery: 30.09.2021
Project Start Date: 01.10.2019 **Duration:** 36 Months

Document Information

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

Document Number:	D2.2
Document Title:	Final Report on Private 5G Network Architecture and Operator Models
Editor:	Sven Wittig (HHI)
Authors:	Sven Wittig (HHI) Henrik Klessig (BOSCH) Nicola di Pietro (ATH) Marco Centenaro (ATH) Daniele Munaretto (ATH) Kuan-Yi Chih (ITRI) Jack Shi-Jie Luo (ITRI) Cheng-Yi Chien (CHT) Jiun-Cheng Huang (CHT) Yueh-Feng Li (CHT) Ling-Chih Kao (CHT) Isaku Chu (III)
Dissemination Level:	Public
Contractual Date of Delivery:	30.09.2021
Work Package	WP2
File Name:	861459-5G CONNI-D2.2-Final Report on Private 5G Network Architecture and Operator Models-v1.0.docx

Revision History

Version	Date	Comment
0.1	23.09.2021	Consolidation of individual chapters
0.2	27.09.2021	Updated authors list Completed Introduction and Executive Summary
0.3	28.09.2021	Update authors list Editorial changes Modifications to Sections 5.2, 6.2.1
1.0	30.09.2021	Version for submission

Executive Summary

The present deliverable D2.2 concludes the work carried out as part of Work Package 2 “Private 5G Networks: Architecture & Operator Models” and documents its results as of the second reporting period. Simultaneously, it marks the overall conclusion of conceptual level work within the 5G CONNI project, drawing heavily on preparatory results achieved in this Work Package as well as in Work Package 1 “Use Cases & Requirements”.

The preceding deliverable D2.1 described four different main architectural models for private 5G networks on which the discussion found in this document further elaborates. To provide an initial indication of a particular deployment model’s suitability for specific enterprises’ needs, a SWOT analysis incorporating the different stakeholder views represented in the 5G CONNI consortium yields a qualitative judgement. In a second step, a much more elaborate evaluation is presented based on the outcomes of WP1 as documented in D1.2. This document defines a comprehensive framework for description and systematic evaluation of private 5G operator models, which is applied to the four models under consideration.

In extension to the industrial application use cases of D1.1, a number of use cases for site interconnectivity between geographically dispersed parts of a private 5G network are discussed as may arise in large, internationally distributed enterprises.

All these considerations finally lead to the definition of the overall high level architecture of the 5G CONNI end-to-end demonstration system, the detailed implementation of which is now underway in Work Package 5.

Table of Contents

List of Figures

List of Acronyms

5G CONNI	5G for Connected Industries
5GC	5G Core
5QI	5G QoS Identifier
AF	Application function
API	Application programming interface
AUSF	Authentication Server Function
BBU	Baseband unit
CAPEX	Capital expenditure
CN	Core network
CP	Control plane
C-RAN	Centralized (or Cloud) Radio Access Network
CU	Central Unit
DN	Data network
DPI	Deep packet inspection
D-RAN	Distributed Radio Access Network
DU	Distributed Unit
E2E	End-to-end
IMSI	International mobile subscriber identity
MAC	Medium Access Control
MEC	Mobile edge computing
MIMO	Multiple Input Multiple Output
MNO	Mobile network operator
MVNO	Mobile virtual network operator
NF	Network function
O-RAN	Open Radio Access Network
PHY	Physical layer
QoS	Quality of service
RAN	Radio Access Network
RU	Radio Unit
SLA	Service level agreement
SP	Service provider
SWOT	Strengths, weaknesses, opportunities, threats
UDM	Unified Data Management
UE	User equipment
UP	User plane
UPF	User plane function
USIM	Universal subscriber identity module
VPN	Virtual private network

1 Introduction

A central aspect of the 5G CONNI approach to industrial wireless networking is the notion of private 5G networks. While these networks will built upon the technologies developed over the past years of 5G system research and standardization in areas such as radio access, core and transport networks as well as edge and cloud computing, they bring along a shift in the traditional ownership and governance structures of mobile radio networks dominated by monolithic operator organizations. With more stakeholders involved in the deployment, operation and usage of the network and each network component possibly owned and governed by a different party with its own business model, private 5G networks open up a larger space of possible deployment and architectural options. These options directly influence a multitude of factors that may guide an enterprises choice for one of them. The more prominent among them are the associated costs, confidentiality and security issues and organizational effort. In the design of an industrial private 5G network, it is therefore prudent to carry out an analysis of different architectural choices with respect to these factors first.

Work Package 2 has previously discussed the primary components of a private 5G system and different models of ownership and governance, as well as different stakeholders' interactions with them. This lead to a definition of four archetypal architecture options, which serve as the basis for the continued discussion presented in the document at hand. Its focus lies in a detailed evaluation of the presented models and the implications of architectural choices.

Concluding the conceptual work of Work Packages 1 & 2, this document presents the overall high-level architecture of the 5G CONNI end-to-end demonstration system, the detailed implementation of which is now underway in Work Package 5.

1.1 Scope

This deliverable is a result of Work Package 2 "Private 5G Networks: Architecture & Operator Models" and further details the discussion of different system architecture options suitable for private 5G networks in industrial applications. The results presented here constitute a continuation of work, both from Work Package 1 "Use Cases & Requirements" as well as Work Package 2. Its focus lies on an in-depth evaluation of the presented deployment and operator models, which lead to the definition of an overall high-level system architecture for the international 5G CONNI end-to-end industrial 5G demonstrator. In addition to the individual industrial application use cases presented in D1.1, a number of use cases for globally distributed interconnected multi-site private 5G networks is discussed.

1.2 Structure

This document is structured as follows: Elaborating on the four architecture options described in D2.1, Section 2 first presents a SWOT analysis for each of them. To motivate the further discussion of an internationally connected demonstration network, Section 3 presents five additional use cases beyond the applications of D1.1 that arise and justify that type of deployment. Section 4 then presents the applied methodology and summarized results from a systematic in-depth evaluation of operator models based upon the four architecture options. A short discussion on the implications of different network functional splits, especially in the radio access part, in Section 5 concludes the conceptual considerations that finally lead to the overall 5G CONNI demo system architecture presented in Section 6.

2 SWOT Analysis of Architecture Options

The concept of operator models described and discussed in detail in the context of Work Package 1 (cf. D1.2) lends a comprehensive logical framework for the description of and analysis of private 5G deployments across their entire lifecycle. With the developed evaluation methodology, it creates a powerful tool for the assessment and choice of a suitable model for a given application. However, its high level of detail makes it useful for comprehensive evaluation as is presented in Sec. 4.

The four network architecture options laid out in D2.1 offer a narrower view on operator models, focusing specifically on 5G system related aspects and thus a viable entry point for a more in-depth discussion. To elucidate their specific key characteristics and lay the foundation for the choice of architecture, a SWOT (strength, weaknesses, opportunities, threats) analysis of the four options has been conducted. With the involved 5G CONNI partners representing different stakeholders' perspectives, the consolidated analysis gives a balanced initial view.

2.1 Fully Private Infrastructure

The Fully Private Infrastructure architecture considered here is described in Sec. 3.1 of D2.1.

Table 1: Fully Private Infrastructure - SWOT matrix

	Internal		
Positive	**Strengths** • Tight integration between RAN equipment and CN infrastructure • High resilience (all NFs are on premise) • Higher level of security/confidentiality because CP, UP and MP do not leave the site (isolation) • Possible integration into existing IT • Exclusive access, no resource sharing • Full control of QoS • Full control by the user, i.e. enterprise (ownership and governance) • High flexibility in deployment	**Weaknesses** • Likely to be more costly compared to other options (high CAPEX) • Lack of integration with the public RAN • No off-site connectivity/service continuity • Lack of scalability for large/distributed enterprises • Governance and responsibilities for the user/enterprise require 5G domain knowledge, which itself can be costly to be built up and maintain • If operated as managed service by an MNO/service provider probably more costly • High deployment complexity • Higher maintenance complexity and effort	**Negative**
	Opportunities • Tighter integration with applications/services (e.g. direct access to network status) • Greater flexibility for future innovations in application • Solutions might become more tailored to the needs of an enterprise/factory in the long run, which might decrease cost and effort for the end user • Flexible adaption of the 5G system to the enterprise's specific requirements.	**Threats** • Prohibitively large upfront investments • Unflexible/unsuitable vendor pricing and/or support models • Weaker position for MNO roaming agreements • Availability and cost of regulated resources (i.e. spectrum, IMSIs) • Decreasing support by possibly involved MNO/service provider for very specific modifications	
	External		

Observations

The Fully Private Infrastructure option is expected to offer tight integration with the application and the highest level of control. It is most suited for insular deployments and requires a high commitment of resources if implemented.

2.2 MVNO Model

The Mobile Virtual Network Operator (MVNO) architecture considered here is described in Sec. 3.2 of D2.1.

Table 2: MVNO model - SWOT matrix

	Internal	
Positive	**Strengths** • Less costly than fully private solution • Off-site mobility/service continuity possible • Low impact on IT infrastructure • Enterprise largely does not have to care about radio deployment and operation • Security/Confidentiality of the user plane data through local UPF • Low maintenance complexity • Low deployment complexity	**Weaknesses** • Relies on availability of sufficient RAN infrastructure • QoS guarantees only through SLAs if the MNOs RAN is used • Security threats if RAN is not owned/governed by enterprise • Exposure of IT infrastructure to third parties • Some governance concerns if third-party SPs are involved and govern elements such as the (edge) cloud • Lower flexibility in meeting specific requirements
	Opportunities • Scalability for larger enterprises • Provide network services to third parties (intra-enterprise) • Probably a good solution for outdoor use cases (coverage of outdoor plant areas) • Outsourcing of day-to-day RAN operations to specialized providers • Combination of multiple RAN operators	**Threats** • Control plane data outside of enterprise network exposes vulnerability to malicious external actors • Disruption of shared public infrastructure • Dependence on MNO RAN strategy might limit future extensions or upgrades • MNO might need to consider multiple different enterprise SLAs and consumer QoS requirements at the same site possibly increasing complexity • Reluctance of MNO to enter MNVO agreement due to lack of expertise
	External	

Observations

The MVNO option, obviating the need for a private RAN, is expected to lower the commitment on behalf of the enterprise at the expense of reduced control over network operation and offered services. It offers scalable services within the bounds of a MNOs network to enterprises with less stringent overall requirements.

2.3 Hybrid Model

The Hybrid Model architecture considered here is described in Sec. 3.3 of D2.1.

Table 3: Hybrid model - SWOT matrix

	Internal	
Positive	**Strengths** • Extreme deployment flexibility, with configurable split options • Interoperability with the public network possible → off-site mobility, service continuity • Combines characteristics of Private & MVNO models • In general higher security/confidentiality because the enterprise is free to choose between private or MNO RAN and UP does not leave the site • Full control over QoS	**Weaknesses** • Potential for high costs (investment & recurring) • Highest level of complexity • Still security threats without control of the MNO RAN by the enterprise • Confidentiality contingent on transport ownership • Additional 5G domain knowledge required by the enterprise to manage RAN • Failures on the connectivity towards the CP NFs may leave the edge sites without their controlling entities • Effort for UE and RAN authentication of both private and public core
	Opportunities • Various edge deployments can be managed by a unique control center, while still preserving UP data privacy • Rapid and affordable business rollout • Offering tailored services for first (inter-enterprise) and third parties (intra-enterprise) • Scalability to different market and legal environments (e.g. w.r.t. spectrum regulation) • This model could be considered as part of a long-term transitional strategy from MVNO towards fully private model.	**Threats** • Full privacy (comprising CP data) requires the ownership of the transport network • Transport network reliability may impact the control center effectiveness • Many parties involved in continuous long-term operation • Dependence on MNO RAN strategy might limit future extensions or upgrades • Possible interoperability issues between the enterprise core and a multitude of MNO RANs (across vendors, countries) • Ability to reach roaming agreement with MNOs
	External	Negative

Observations

The Hybrid Model is expected to offer the highest degree of flexibility in satisfying a diverse set of possibly conflicting individual applications' requirements at the expense of high overall complexity. It still requires higher resource commitment on behalf of the enterprise, which, however, may be gradually scaled.

2.4 MNO's Private Core Network

The MNO's Private Core Network model considered here is described in Sec. 3.4 of D2.1.

Table 4: MNO's private core network - SWOT matrix

	Internal		
Positive	**Strengths** • Lowest cost among presented options • Low commitment by enterprise • Global connectivity and service continuity are easily achieved • Low deployment and maintenance complexity • Higher operational security for using operator's security strategy	**Weaknesses** • Highest degree of security threats as confidential data (e.g. CP, MP) leaves the site • Full dependence on MNO/vendor strategy • Neither governance nor control over any of the elements by the enterprise, therefore full dependence on MNO and corresponding SLAs • Applications run on devices with third-party access/governance • Bump-in-the-wire MEC seems to requires DPI, which is critical from a performance/security perspective • Integration with enterprise IT mgmt systems complicated or even not possible • Breakout into local network can be complicated (I-UPF not necessarily on premise) • Low flexibility in choice of security mechanisms because USIM credentials are always required. • Low flexibility due to MNO involvement • Probably fewer solutions tailored to enterprise needs • Scalability outside of MNO's business area	Negative
	Opportunities • Entry-level solution for technology adoption • For multi-site setups, UP does not necessarily leave 3GPP network for some use cases, which might bring additional benefits (e.g. authentication, security, etc.) • The enterprises mainly focus on the operation of edge computing systems and applications. • Deployment of dedicated RAN by MNO for improved QoS	**Threats** • Network demarcation between enterprise IT and MNO IT needs proper alignment, which might results in non-optimal compromises • Full dependence on MNO/service provider business model and strategy for long term operation (lock-in effect) • Insufficient service area • High cost for MNO, potentially low interest	
	External		

Observations

The MNO's private core network model is expected to provide private 5G services with the lowest commitment on behalf of the enterprise. Low control over the network is expected to result in conflicts with enterprise-specific requirements.

3 Inter-site Use Cases

Discussion of use cases for 5G connectivity in the industrial manufacturing context is mostly focused on applications at the network edge, which in themselves do not necessarily warrant large-scale network deployments. In Work Package 1, a number of innovative use cases have been selected for demonstration within the project, which might very well be addressed by compact, insular 5G deployments. However, the unique cross-regional composition of the 5G CONNI consortium enables to shift the view to global enterprise operations. Thus, in extension of D1.1, this section presents five additional use cases for a larger, inter-site private 5G network connecting multiple geographically disconnected but operationally associated sites.

In this context, we discern two types of inter-site communication:

- Intra-enterprise: Both sites within the 5G network belong to the same enterprise, i.e. are subject to common governance.
- Inter-enterprise: Both sites within the 5G network belong to different but associated enterprises, i.e. they are subject to governance by different entities.

3.1 IS-1: Cross-border, intra-enterprise monitoring

Relevant for: Single multi-business, multi-factory enterprises

Description: More often than not, large enterprises have more than one site. Such sites include corporate headquarters, office buildings and, for the industrial sector, manufacturing sites or plants, and they are interconnected with specific sets of IT rules and regulations in mind. Manufacturing sites in particular can exchange information among each other in a secure way. Depending on the specific use case, such information can be process data that help improve production processes across sites or other information that should be centrally gathered. Additional information that is shared among different interconnected sites including corporate or division headquarters is data with respect to production efficiency, material consumption or overall equipment efficiency. Besides this, IT systems including communication infrastructures are often centrally managed by IT experts for the sake of lower complexity and low management effort. In regard to private 5G networks, 5G management and 5G Core functionalities then ideally remain at a central location and where use case requirements are met.

Implication on architecture: Therefore, such a scenario would call for a solution, in which the 5G Core is installed at division or corporate headquarters, managed either by company-internal experts or an external MNO or solution provider.

3.2 IS-2: Cross-border, intra-enterprise or inter-enterprise shipping of production assets or production lines

Relevant for: Single multi-business unit, multi-factory enterprises and multiple interconnected enterprises

Description: Production assets, such as robots, machines, tools or work piece carriers, are actively used in production over several years until they are replaced by other components. Nevertheless, those assets are reused at different locations, either in plants of the same enterprise or of different enterprises. Usually, after their productive years machines and production lines are disassembled, shipped to the other location and then re-assembled to produce similar or other goods. Here, it would be beneficial to retain wireless configurations, such as subscriber and QoS profiles, that are actually tailored to the specific production line

but in case the production line is re-assembled at a new location, the subscriber profiles can actually remain active along with the configuration of the network, e.g. in terms of network slices. In such a case a unified 5G management or even 5G core would be preferred, so that the production assets work the same way at the new location as at the old one, while manual re-configuration of the wireless system including the UEs is minimized.

Implication on architecture: Favorable solutions in this scenario would require the 5G Core be located within the enterprise domain for central management or in a central cloud with unified management across multiple companies. Alternatively, multiple interconnected private 5G Cores can also be possible, which share a common user profile data base.

3.3 IS-3: Intra-enterprise or inter-enterprise lineside delivery and tracking on logistics routes

Relevant for: Single multi-business unit, multi-factory enterprises and multiple interconnected enterprises

Description: Inbound and intra-logistics are important aspects of all factories, where ideally automated processes for tracking and registration of all kinds of assets and materials are applied. Here, 5G networks will play a crucial role regarding positioning and identification of connected UEs in different factories, either of the same enterprise or of different ones, and also on logistics routes in between them. While private networks cover the area within and around factories, the public 5G network provides connectivity and tracking possibilities on logistics routes. In addition to localization of assets and goods, this avoids manual inbound registration processes and leads to minimal human intervention or use of other technologies such as RFID gates.

Implication on architecture: For this scenario, sensitive user and position data needs to be securely exchanged between the end devices in the respective private networks, but also over the public network. Here, roaming architectures and private communications are important ingredients in such a constellation.

3.4 IS-4: Remote commissioning of machines, etc.

Relevant for: Single multi-business unit, multi-factory enterprises and multiple interconnected enterprises

Description: 5G-interconnected plants and enterprises enable new opportunities for machine builders, process engineers and similar experts through innovative connectivity applications. Here, experts can remotely and securely log into machines and other assets, configure them and optimize production processes, for instance. This is not only a flexible approach but can also save effort and costs for the required personnel.

Implication on architecture: Usage of remote access, maintenance, commissioning and other services require private and highly secured connections between the expert and the single machine. Communication needs to be, at least logically, isolated from other communication streams or data flows.

3.5 IS-5: Remote expert support for process diagnosis

Relevant for: multiple interconnected enterprises

Description: Deploying manufacturing sites overseas has been a common practice for companies that aim to reduce cost on production and logistics. Collaboration of engineers from various location and transfer expertise to production sites calls for a lot of traveling cost. With the pandemic of COVID 19, things get worse as almost all international traveling has been shot down. 5G technology brings new opportunity to resolve the above difficulty as we can link engineers with digital twins and interact with each other via cutting edge AR/VR technology to provide immersive environment so that they can design, plan, and troubleshooting in the same virtual factory. By doing so experts from enterprise headquarters can support manufacturing sites all around the world and

1. Reduce traveling cost for collaboration
2. Quickly deploy new manufacturing sites while keeping the core technology within enterprise and provide necessary support by using digital twins in the cloud computing platform.

Implication on architecture: Given the physical distance constraints between BOSCH and IMTC, latency critical scenarios will be demonstrated locally rather than inter-continental. In addition, the digital twin information, remote instructions and live video will be exchanged between two sites. To this end, the highly secured VPN connectivity or UPF chaining is required.

4 Evaluation of Operator Models

The evaluation of private 5G network operator models is not trivial, as many different aspects, or dimensions, have to be considered. The amount and diversity of these dimensions, as well as the large number of different concerns and requirements necessitate a systematic approach to assess the models in light of the different aspects and from the viewpoints of various stakeholders. To this end, an operator model evaluation template has been designed in Work Package 1 and documented in the 5G CONNI D1.2. Section 4.1 reiterates on the methodology chosen by the 5G CONNI consortium to explore this topic. Section 4.2 provides some general insights and results based on the evaluation, while Section 4.3 details results specifically for each model. Finally, Section 4.4 attempts at giving a relative comparison of the model including conclusions.

4.1 Methodology

Work Package 1 has resulted in a broad yet deep understanding of the different dimensions of operator models, which include network lifecycle tasks, (network) elements and their locations and involved stakeholders. From this exploratory work, a large number of concerns and requirements have been devised (see Annex 1 in D1.2), which resulted in 13 different aspects rated according to their criticality (cf. Section 6.1 in D1.2).

ID	Concern	Requirement	Evaluation: How is the requirement fulfilled? Select one option, please. Architecture/operator model: Fully Private Model Stakeholder perspective: Enterprise				Comment (Please provide a very short explanation of your choice)
			Inherently fulfilled by operator model.	If not inherently fulfilled, fulfilled by technical feature?	If neither fulfilled inherently nor by technical feature, fulfilled by contract between stakeholders ?	Cannot be fulfilled at all.	
A1	Wrong or missing access to elements by a stakeholder						
B-2.1	Management of MEC platform (or part of it) by the Enterprise while the platform is off-premise might raise concerns regarding accessibility, and management by the SP or MNO might raise concerns regarding integrity and proper management.	For any operator model, the MEC platform shall be well accessible by the Enterprise for management purposes, even it is located off-premise and owned by another stakeholder.	☐	☐	☐	☐	
B-2.2	Elements are the wrong accessed by unrelated personnel and then cause system problems.	Stakeholders need to establish reasonable authority control to avoid wrong access by unrelated personnel.	☐	☐	☐	☐	
B-3.2	Stakeholder can't do emergency maintenance on premise 24/7 because premise is closed or access to it is limited	For a third-party operator model, 24/7 emergency maintenance service shall be possible, e.g. through a 24/7 field service concept	☐	☐	☐	☐	
B-3.3	Remote access to stakeholder's equipment is interrupted because of failure in the transport environment	Remote access to stakeholder's equipment shall be ensured and the impact of failure shall be minimized, e.g. through implementing an out-of-band management concept.	☐	☐	☐	☐	
B-3.4	The operation of the personnel can not find the source of the problem.	Enterprises must make clear location access requirements and it shall be included in a global architecture	☐	☐	☐	☐	

Figure 1: Short Extract of the Operator Model Evalation Template Used in this Assessment.

The operator model evaluation template (cf. Section 6.2 in D1.2) takes every requirement associated with the different aspects and asks for a multiplier that indicates how well a

requirement is fulfilled by a certain operator model from the viewpoint of a stakeholder. The factor is chosen according to four different categories: 1) The requirement is inherently fulfilled by the operator model under consideration, 2) The requirement necessitates additional technical features with the operator model, 3) If technical features are insufficient or not available, contractual means need to be put in place between two or more stakeholders, or 4) The requirement cannot be fulfilled with the operator model, even not with additional technical features or contracts.

The templates have been circulated within the 5G CONNI consortium and the partners have given each requirement a rating according to the method explained above. In addition, each partner was asked for a short yet appropriate reasoning for the chosen option to gain more detailed insights.

Finally, the results were cross-reviewed by other partners to check for meaningfulness.

4.2 General Results

In general, each of the four different architecture models can address the stakeholders' requirements in a particular way, i.e. they are either inherently fulfilled by the model, by additional technical features, by contractual agreements between at least two stakeholders (if technical features are not available) or they cannot be fulfilled. Some insights with respect to a number of requirement groups and to what extent they are fulfilled by the four different models are explained subsequently.

One group of requirements pertain to “Wrong or missing access to elements by a stakeholder” (aspect A1), e.g. remote access to stakeholder's equipment shall be ensured and the impact of network element failure shall be minimized. In general, fulfilling this group of requirements is less of a problem, when fewer stakeholders are involved in management and operation tasks. For instance, this is the case for the fully private model, where the enterprise retains full control over each and every element, or where the MNO has full control, e.g. in the hybrid and MNO models. Remote access to network elements can be accomplished through standard tools, but if maintenance needs to be carried out locally, access must be guaranteed by the enterprise, which requires bilateral contractual agreements.

Additional requirements emerge from the aspect of “Interoperability of security systems and alignment of security concepts” (A2). This is of major concern of the party that wants to integrate the private 5G network into the local IT infrastructure, i.e. the enterprise. One example is that the UDM and encryption keys shall be accessible and governed by the enterprise. In principle, there are no dependencies between MNO or SP security concepts and that of the enterprise in the fully private model. In fact, private 5G can be securely integrated as needed. Obviously, the MNO might prefer the MNO model as this is the one that requires least IT integration efforts.

For models, where many different stakeholders are involved, “Lack of expertise to carry out certain network lifecycle tasks” (A3) might be a main problem. In particular, this applies for the enterprise, which generally might lack competencies regarding cellular network management, which includes handling of the spectrum. Here, the enterprise might prefer an MNO- or SP-operated model, such as the hybrid, MVNO or MNO model. Of course, since MNOs and SPs bring in the right expertise, there might be only a few requirements towards the enterprise depending on tasks that could be transferred to the enterprise.

In terms of “Confidentiality, integrity and availability of data” (A4), the fully private model may be the clearly preferred model by an enterprise, whereas for the MNO model most requirements can only be fulfilled by contract between the parties, which specify to handle events of data breach, system unavailability, etc. with different kinds of service level

agreements. One such requirement is that for confidentiality reasons the UPF shall not be accessible by any other third party in case of unencrypted data transfer.

Because fewer other stakeholders are involved in the MNO and hybrid models, they are clearly preferred by an MNO in terms of “Stakeholder autonomy” (A5). While QoS guarantees can be given by technical features through the MNO/SP in their view, the enterprise might want to prefer contracts that would also ensure appropriate QoS beyond today's known use cases. On the contrary, the fully private model might be preferred by the enterprise, where the latter can directly negotiate the network features and QoS guarantees with the network vendor.

Other requirements also emerge from concerns related to “Ownership of and governance over elements by another stakeholder” (A6), e.g. easy expansion of UE base. While in many cases this might require additional technical features of extension of the wireless network and compute capacity (technical features), the enterprise might require dedicated capacity expansion plans, which are solved through contractual means.

Also related to some of the already mentioned requirements above, further ones belong to reducing “Coordination effort” (A7), “Multi-site setup support” (A8), “Costs” (A9), “Service availability” (A10), “Continuity” (A11), “Regulation” (A12) as well as “Global applicability” (A13). In summary, all four models have advantages and disadvantages in light of the different requirements of the stakeholders. While not all requirements are inherently fulfilled by the models, most of them can be addressed by additional technical or contractual means. Ultimately, the fully private model might be the one to be considered by (large) enterprises, while MNOs and SPs can quite flexibly apply technical solutions solving most of the challenges of private 5G networks and their operation. Here, the hybrid, MNO and MVNO models can play a significant role. Lastly, the actual choice then depends on balancing all the relevant aspects including security, autonomy, costs and global applicability.

4.3 Model-Specific Results

Apart from the general results, some interesting insights and conclusions can be drawn from more deeply analyzing model-specific scorings and explanations given from the perspective of the various stakeholders. In this regard, the following paragraphs shall provide some helpful additional information and explanations, while the quantitative results can be found in Annex I.

4.3.1 Fully Private Model

One of the truly novel architectures is the fully private model (cf. Section 3.1 of D2.1), which can be entirely isolated from other, public networks in terms of user traffic. Standalone Non-Public Networks (SNPNs) are the corresponding private network type in 3GPP. SNPNs provide performance (latency) and privacy benefits to dedicated services of enterprises at the cost of increased expenses, as most of the components are owned and governed by the enterprise, incl. the 5G Core and the radio access network. This also means that most of the responsibilities are with the enterprise, including network planning and roll-out. Although SNPNs are not integrated with public networks, they can still realize a local data breakout through the locally deployed UPF into the enterprise network and the Internet, as well.

4.3.1.1 Enterprise’s Perspective

The fully private model generally received high scores from the enterprise’s perspective. Only with respect to the aspects “Lack of expertise to carry out lifecycle tasks” (A3), “Global applicability” (A11) and “Regulation” (A13), other models have higher scores, which is a natural consequence of the facts that not all enterprises might be prepared to carry out specific 5G network management tasks and that, especially for international enterprises, operation concepts need to be aligned with local regulations (e.g. in terms of usage of spectrum) and owning or governing spectrum might not be allowed at all. On the other hand, the fully private

model is superior to other models, in particular with respect to “Confidentiality, integrity, availability of data” (A4), “Autonomy of stakeholder” (i.e. enterprise, A5), “Coordination effort” (A7) and “Service availability and continuity” (A10). This is not surprising because A4 and A10 are specific design elements of the fully private model and the main reasons to tailor the 5G network architecture to relief such enterprise concerns.

4.3.1.2 MNO’s Perspective

From an MNO’s perspective, the fully private model provides some advantages, especially regarding “Interoperability of security systems and alignment of security concepts” (A2), “Confidentiality, integrity and availability of data” (A4), “Service availability and continuity” (A10), and “Deployment and system coexistence” (A13). In regard to aspects A2 and A4, the usage of open architectures and dedicated firewalls are sufficient means to protect user data of the enterprise, and the FPM allows for dedicated development and integration of appropriate security mechanisms on a single end user basis. In light of aspects A10 and A13, since ownership/governance is with the enterprise, there is a clear separation of responsibilities between the stakeholders. In this regard, well-defined processes in large enterprises are already designed and in place to handle issues regarding service availability and deployment and system coexistence. Hence, the FPM often inherently fulfills the associated requirements. On the other hand, “Ownership of and governance over elements by another stakeholder” (A6), “Coordination effort” (A7), and “Multi-site setups” (A8) received lower scores. If there are interactions between the enterprise and an MNO, e.g. in terms of spectrum or connectivity towards the public network, then some technical solutions or contractual agreements are necessary.

4.3.1.3 Service Provider’s Perspective

For the service provider, the fully private model has some benefits, too. The aspects “Interoperability of security systems and alignment of security concepts” (A2), “Confidentiality, integrity and availability of data” (A4), and “Costs” (A9) received higher scores. From an SP perspective, alignment and on security concepts and data security, can be achieved through dedicated security solutions that are chosen or developed during the solution design phase. In contrast, the fully private model has also some disadvantages regarding “Wrong or missing access to elements by a stakeholder” (A1), “Ownership of and governance over elements by another stakeholder” (A6), and “Service availability and continuity” (A10). General concerns regarding aspect A1 need to be addressed by contractual means, when a SP accesses elements owned by another stakeholder, in particular the enterprise. When it comes to spectrum handling and monitoring of elements owned by another stakeholder (A6), technical features (monitoring tools) and contractual solutions (spectrum licensing) need to be taken into consideration. Also, if the SP takes over responsibilities (regarding A10) in case the Enterprise wants to outsource some activity (perhaps because of not being able to provide the required competencies by itself), contractual SLAs need to be put in place.

4.3.2 MVNO Model

In the MVNO model, the Enterprise owns almost every dimension except for the RAN and the transport network. While the RAN is shared and connected to both the MNO and the private CN. The radio network is accessible to Enterprise, MNO and SP. Moreover, the transport network and OAM network are governed by several parties. Involving multiple stakeholders that lead to a higher risk of control over the MVNO network. Furthermore, the transport network and OAM network are directly connected to the site's IT infrastructure and the Enterprise and MNO CN. In order to protect user data, signaling data, operation data, and management data, security concepts and IT integration efforts are critical concerns in the MVNO model to all involved stakeholders. The MNVO model has several advantages in comparison with other operation models in “Costs” (A9), “Global applicability” (A12) and “Regulation” (A13) due to

international enterprises can cooperate with local MNOs where local MNOs obtain the sublicensing spectrum that is inherently fulfilled with the respect to above aspects.

4.3.2.1 Enterprise's Perspective

From the point of view of the enterprise, the MVNO model generally received low scores to the aspects that concern the "Security concepts", "Network Maintenance and Network Management" and the "Coordination effort". The aspects related to "Security concepts" like "Wrong or missing access to elements by a stakeholder" (A1), "Interoperability of security systems and alignment of security concepts" (A2), "Confidentiality, integrity and availability of data" (A4) can only rely on contractual agreements and SLAs granted by the involved parties to establish secured inter-connections in MVNO shared RAN network. Other aspects relate to "Network Maintenance and Network Management" like "Lack of technical expertise to carry out lifecycle tasks" (A3), "Autonomy of stakeholder" (A5), "Governance over elements by another stakeholder" (A6) and "Service availability and continuity" (A10). The shared RAN network management responsibility and network maintenance plans include 24/7 field service, quick service response time, redundancy plan must be carried out by contractual agreements and adequate SLAs with MNO and SP. Because the MVNO model requires coordination and interoperation effort among stakeholders to handle shared RAN network, transport network and OAM network. This explains the low scores enterprise has received because of high dependency on external stakeholders. Indeed, this model is preferred by enterprises for the aspect of "Costs" (A9), "Global applicability" (A11) and "Regulation" (A12). The contractual agreements with different countries local MNOs to obtain spectrum and shared RAN network elements to fulfill the local regulations (e.g., in terms of usage of spectrum) is a feasible solution to international enterprises.

4.3.2.2 MNO's Perspective

From the point of view of the MNO, the MVNO model received high scores in the following aspects "Ownership of and governance over elements by another stakeholder" (A6), "Multi-site setups" (A8), Costs (A9), "Regulation" (A12). MNO plays an important role in MVNO in shared RAN network and spectrum for ownership and governance. Since MNO is almost inherently fulfilled with the above aspects. The other concerns regarding access RAN network monitoring interfaces and the establishment of security channels with Enterprise and SP shall be regulated by contracts. Similar to 4.3.2.1 Enterprise's perspective in MVNO model, aspects regarding "Security concepts", "Network Maintenance and Network Management" and the "Coordination effort" involve multiple parties that require contracts and adequate SLAs to ensure data security, emergency maintenance, RAN functions upgrade for extension of features, etc. The aspect of "Interoperability of security systems" (A2) within Enterprise, MNO, and SP, technical means e.g., jointly defining security algorithms and intrusion checks could fulfill each stakeholders' requirements. Shared RAN QoS customization has a great impact on network performance. It can be enforced via technical features that must comply with MNO design specifications. In consequence, "Cost" (A9) for QoS customization is a concern MNO for additional supports that requires contractual agreements with Enterprises.

4.3.2.3 Service Provider's Perspective

From the point of view of the SP, the MVNO model generally received medium scores in all aspects. This can be explained because SP plays a 3rd party role in all operation models. From the aspect of "Lack of technical expertise to carry out lifecycle tasks" (A2), enterprises can outsource operations training and maintenance to SP's support teams to relieve enterprise concerns. Contractual agreements and adequate SLAs between Enterprise, MNO and SPs are required to tackle the concerns of "Security concepts", "Network Maintenance and Network Management" and the "Coordination effort" described in previous 4.3.2.1 and 4.3.2.2.

Contractual agreements for the division of responsibilities and appropriate supportive services are the main point to SP in the MVNO model.

4.3.3 Hybrid Model

As described in Section 3.3 of D2.1, the Hybrid model defined by 5G CONNI can be seen as a combination of the Fully Private and MVNO models. Architecturally, it is characterized by the deployment of the control plane core NFs at a central location (either a datacenter owned by the enterprise or an external cloud belonging to a service provider), whereas UPFs are distributed, generally with one UPF placed at each different site. This, together with privately owned RAN and MEC platforms, combines for the enterprise the advantages of the Fully Private model with the benefits of having a centralized control center that oversees the connectivity of a plurality of distinct sites within the same private network. As such, it is a suitable model for many of the requirements of 5G CONNI's use cases (cf. D1.1), even if it entails a possibly more complex network management for the owner of the private network. In the following, we are reporting some interesting conclusions yielded by the evaluation of the Hybrid model, from the perspective of the three main stakeholders: the enterprise, the MNO, and the service providers.

4.3.3.1 Enterprise's Perspective

From the point of view of the enterprise, the Hybrid model has received the highest scores for the aspects defined in D1.2 that concern "Deployment and system coexistence" (A13) and "Service availability and continuity" (A10). The latter is particularly interesting when compared to the scores assigned to the same category in the evaluation of the other models. Indeed, the fact that in the Hybrid model the enterprise has the maximum control over the network explains the high score in category A10, close to the (slightly higher) score obtained by the Fully Private model and tangibly higher than the score of the other two models, in which the enterprise is more dependent on the other stakeholders for the networking services. The lowest scores of the Hybrid model, instead, are given by the enterprise to the aspects that concern the "Coordination effort" among stakeholders (A7) and the "Lack of expertise to carry out lifecycle tasks" (A3). This can be explained because the Hybrid model requires an important coordination and interoperation effort among stakeholders to handle a more complex architectural setup, and, at the same time, requires the enterprise to acquire specific advanced competences to operate and manage its own private network, without depending for this on external stakeholders.

4.3.3.2 MNO's Perspective

The Hybrid model turns out to be the "least favorite" model for MNOs, when we look at the average scores over all the considered aspects. More precisely, the Hybrid model receives strictly lower scores compared to all the other models in the following aspects: "Ownership of and governance over elements by another stakeholder" (A6), "Multi-site setups" (A8), "Costs" (A9), A10, "Global applicability" (A11), "Regulation" (A12). This is due to several concurrent reasons, distinct for the various considered aspects. Nonetheless, a general observation can qualitatively explain this trend: the Hybrid model has the least favorable tradeoff for the MNO between the interoperation effort among the stakeholders and the control/access capability of the network elements. Indeed, in the Hybrid model the MNO plays the role of a "supporting partner" for the overall networking activity of the enterprise: it does not have the same central role as in the MNO and MVNO models (because of the independence acquired by the enterprise at the core and RAN level), but it still must guarantee connectivity support for roaming in a non-trivial inter-site network architecture. The result is a more complex and penalizing interoperation with the other stakeholders for what concerns the model evaluation.

4.3.3.3 Service Provider's Perspective

Finally, from the point of view of the service provider, given the "third-party" role that such a stakeholder plays in all operator models, the evaluation shows that several aspects are equivalently critical and not highly differentiated compared to the other models. At the same time, there is no aspect for which the Hybrid model strictly turns out to be the most critical. On the contrary, for a few aspects, namely the A8 and A11 categories, the service provider is the stakeholder that inherently brings (or substantially contributes to) the solutions to the possible criticalities. For these reasons, the Hybrid model proves to be the most fitting to the role of a service provider.

4.3.4 MNO's Private Core Network

For MNO's private core network model as described in section 3.4 in D2.1, the operator has lots of effort on this model because it provides most of the network components such as spectrum, RAN, core, and transport network. This model can be used with end-to-end network slice technology, so that the core network and RAN resources can be separated to different enterprises. As the data flows in local sites, there are two kinds of architecture being discussed. One is using I-UPFs between the PDU session anchor UPF (PSA UPF) and the NG-RAN may be used to support the data flow local breakout, which uses the N3 tunnel connecting with NG-RAN node and via N6 interface connecting with public service at edge or local site. The bump-in-the-wire mode consists of dedicated RANs, on-premise MEC, and a core network built by the operator. The USIM cards also belong to the MNO. It is convenient to use the same USIM card between private and public networks. The applications of enterprises are deployed on-premise MEC. Because the RAN is connected to MNO's core network, operators assist enterprises in deploying the MEC and connecting to their internal applications. This architecture distinguishes internal and external areas of the enterprise through dedicated base stations. However, both architectures can significantly reduce the cost of construction and maintenance no matter if you use UPF or Bump-in-the-wire edge break out option.

4.3.4.1 Enterprise's Perspective

From the point of view of the enterprise, the MNO mode basically only has to prepare their own applications and the service requirements demanded by use cases in the enterprise's intra network. The score of "Lack of expertise to carry out lifecycle tasks" (A3), "Global applicability" (A11), "Regulation" (A12) and "Deployment and system coexistence" (A13) are unsurprisingly high with the enterprise's view. For this division of responsibilities, the enterprise and operators may have to discuss the in-formation shared mechanism across enterprises and operators for the network OAM system. In contrast, the enterprise and operators have to pay attention to clarify the authority of monitoring systems and provide the fault management functions, then discuss what specifications operators would plan to build in enterprises for supporting those services. Thus, there are lower scores in "Interoperability of security systems and alignment of security concepts" (A2), "Autonomy of stakeholder" (A5) and "Service availability and continuity" (A10) items.

4.3.4.2 MNO's Perspective

The MNO Model will be the most suitable network architecture for mobile network operators without a doubt by getting the high control of the whole end-to-end network system, especially the security domain and multi-site scenario. Thus, the "Interoperability of security systems and alignment of security concepts"(A2) and "Multi-site setups"(A8) almost get the full credit due to the experienced telecom system integrity service. As the stakeholder consistency in MNO is relatively simple with other architectures, both of the "Wrong or missing access to elements by a stakeholder"(A1) and "Autonomy of stakeholder"(A5) getting high support from operators apparently. On the other hand, from an operator perspective there will not be much effort in

"Deployment and system coexistence"(A7) and "Coordination effort"(A13) domain when planning and building the MNO network module.

4.3.4.3 Service Provider's Perspective

From the point of view of the service provider, the MNO model turns out to be the least favorite model due to lack of flexible network planning adjustments to support the specific customized applications and services. It even didn't get any score when evaluating the "Cost"(A9) and "Global applicability"(A11) issues. Besides, the SP also didn't think that the MNO module can support the "Multi-site setups"(A8), "Service availability and continuity"(A10) and "Deployment and system coexistence"(A13) as a result of the operator controlling the whole system deployment. Moreover, the additional requirement of network architecture adjustment for application and service might bring the extra cost and time to get the agreement with operators. The only benefit for SP to consider about MNO mode is the "Interoperability of security systems and alignment of security concepts"(A2) and "Confidentiality, integrity, availability of data"(A4) due to the mastery of data security and integrity.

4.4 Comparison and Conclusion

The overall scores are provided in Table 5. It is important to note that the numbers give a rough indication. Differences in the second digit after the decimal point can be rather disregarded for a comparative analysis between the different models. Also, it is important to compare only between different models from one single stakeholder perspective and to not mix the different perspectives for the reason that the concerns and requirements vary among the different stakeholders.

Table 5: Summary of total scores (normalized, see D1.2) for the different operator models and from different stakeholder views.

	FPM	Hyb	MVNO	MNO
E	0.83	0.67	0.70	0.69
MNO	0.79	0.70	0.77	0.76
SP	0.48	0.65	0.62	0.43

Some general conclusions can be drawn for each of the different stakeholders:

The investigated operator models are related to new business models, where all the involved partners play new roles compared to the past. This brings opportunities of new revenues but also organizational and operational complexities that need to be properly addressed. The concerns and challenges upon which our evaluation was based, can be seen as business opportunities for new actors in the market, while, for each aspect, the order of the four models is different from a different stakeholder perspective, so that coordination effort is essential when building and operating the private 5G network where multiple stakeholders are involved.

The Enterprise has tangible interests, highlighted by our evaluation, in investing in its own private network towards the fully private model. For this, it does not only have to purchase and install new equipment, but it must train or hire experienced staff for the network operation and maintenance towards autonomy and efficiency. Nevertheless, this model can be operated entirely independently in terms of resources and can be more convenient in management and meets the requirements of enterprises flexibly.

Alternatively, SPs come into play. Especially (but not exclusively) in the Hybrid and MVNO models, a SP's business can be to provide solution and consultancy to the new technical and

interoperability challenges that characterize the new operator models. As competitors to MNOs, SPs can act as integrators of complementary solutions, network installers, equipment vendors, and consultants for non-ordinary operations. In general, SPs can address all concerns where technical solutions are needed.

MNOs have a lot of resources, including RAN, core cloud, edge cloud, transport network, etc., to be competent in various operator models. However, they may want to develop independent branches of their business dedicated to private networks, to facilitate the adoption of the models in which they play a role. Studying and designing efficient and cost-effective technical and contractual solutions to the investigated concerns is key, and MNOs are typically big enough players to guarantee this. At the same time, they may lack the flexibility and adaptability of specialized SPs.

Security (of both the digital and physical infrastructure and premises) is key and needs to adapt to the new business models. This requires novel technical solutions and adapted contractual agreements for all the investigated operator models.

5 5G Network Functions – Splits & Scalability

One of the disruptive principles guiding the design of the 5G system is a further functional disaggregation and modularization while simultaneously defining standardized interfaces between the individual components of the system. This greatly expands the design space for the implementation of 5G system components and allows for more effective optimization towards specific use cases or deployment scenarios. Disaggregation is especially novel in the radio access part of the network, fueled by initiatives such as the O-RAN alliance.

As already discussed in the context of operator models and high-level network architecture options (cf. D2.1, Sections 2 and 4), partitioning of network functions between stakeholders and locations has considerable impact on the suitability of a deployment model with respect to an enterprise's requirements. Furthermore, it will influence the cost structure of the private 5G network as well as requirements towards supporting infrastructure that is required at the site of deployment.

A key characteristic of the disaggregated network architecture is the possibility for virtualization of networks functions. While this architectural approach has been consequently applied to 5G core networks, it is increasingly applied to the radio access network, moving more and more parts of the radio protocol stack to software. This has far-reaching consequences for overall network design, scalability and consequently, cost.

Thus, in this section, we briefly review the disaggregated network architecture as standardized in 3GPP Rel. 15 and its implications for private 5G network deployments.

5.1 Radio Access Network

Figure 2 shows the disaggregated radio access network architecture as defined by 3GPP Rel. 15 [38.401], highlighting the components of the gNB in orange color and the interfacing core network function in blue.

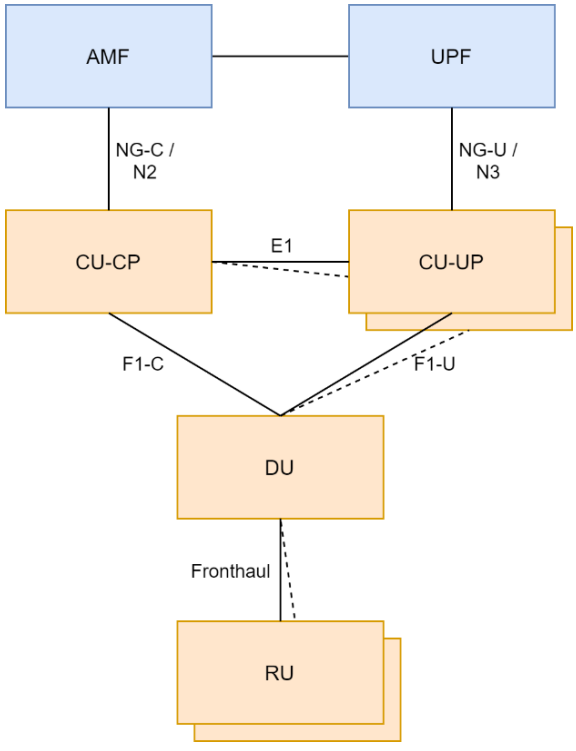

Figure 2: Disaggregated RAN Architecture

In this model, the gNB is decomposed into three main components:

- **Central Unit (CU)** responsible for backhaul connectivity towards the core network, AS and signaling protocol handling and higher layer radio protocol processing, including integrity protection and encryption of user plane data. The CU may be further split into a control plane (CU-CP) and a user-plane part operating independently and interfacing via the standardized E1 interface.
- **Distributed Unit (DU)** responsible for most real time Layer 1 (PHY) and Layer 2 (MAC) processing, including radio signal processing and channel coding.
- **Radio Unit (RU)** acting purely as a transmission and reception point for RF signal, implementing only lowest PHY layer operations in hardware.

5.1.1 Deployment Models

Resulting from the RAN functional split, three different main deployment models have emerged, characterized by their level of aggregation.

5.1.1.1 Aggregated gNB / Small Cell

The Small Cell represents the highest degree of integration, aggregating all three RAN components in a single physical node. With a form-factor and performance comparable to enterprise-grade Wireless LAN access points, these nodes are commonly built on a highly integrated hardware platform such as, for example, Qualcomm's FSM or NXP's Layerscape Access. Due to limited RF and processing resources, a small cell's capacity is typically limited in terms of simultaneously connected UEs and aggregated throughput.

Scalability Implications

The small cell poses the minimal requirements towards infrastructure among the three RAN deployment models in which it is comparable to enterprise-grade wireless LAN systems. Especially for indoor deployments, it still requires packet timing capability on the transport network (see 5.1.2). Due to its high level of integration, it creates the least CAPEX among the RAN models. Together with its comparably low capacity, this makes it most suited for small to medium scale deployments in terms of coverage area and number of UEs, where the infrastructure overhead incurred by the other models may be prohibitive. Capacity scaling of the deployment may be achieved by addition of nodes as far as radio interference planning permits.

5.1.1.2 Distributed RAN (D-RAN)

The distributed RAN model represents currently most prevalent deployment model in which CU and DU are aggregated in a single physical node, the baseband unit (BBU), which in turn serves a larger number of RUs and logical cells.

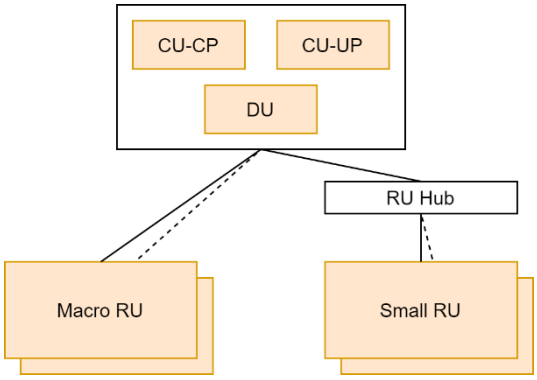

Figure 3: Distributed RAN deployment model

The baseband unit is typically built on dedicated proprietary hardware, offering the highest achievable capacity in terms of simultaneously connected UEs and aggregate throughput. Radio Units may range from high power types capable of serving large coverage areas, possibly incorporating massive MIMO techniques involving large numbers of RF transmit-receive chains, to distributed smaller types more suited to indoor deployments, often employing a hub-and-spoke fronthaul topology as depicted in Figure 3.

Scalability Implications

The high capacity of specialized D-RAN hardware makes it most suited to medium to large-scale deployments, with a single BBU being capable of serving a large number of UEs and a larger number of transmission-reception points, i.e., RUs. Typical BBU designs allow for limited scaling in hardware capacity. The proprietary nature of this model makes it susceptible to a vendor lock-in effect offering little to no interoperability with third-party RAN components beyond the standardized external interfaces. CAPEX and OPEX depend strongly upon vendor pricing models, which at the time of writing are still mostly tailored to large scale MNOs. Whereas a singled BBU might serve a typical industrial deployment site, limitations of the fronthaul interface prevent it from serving larger, potentially geographically disconnected deployments.

5.1.1.3 Centralized / Cloud RAN (C-RAN)

The centralized or cloud RAN model offers the full level of disaggregation as specified by the 3GPP standard. By isolating gNB sub-components, it offers the greatest potential for virtualization and thus scalability. Since the CU performs mostly networking functions it is the most natural component for virtualized deployments, possibly co-located with the corresponding core network functions. For deployment with strict requirements concerning user plane data, hybrid deployments with centralized control plane and edge-terminated user plane are possible. The DU in this deployment may also be virtualized, however, due to its heavy signal processing workload it typically still relies on specialized accelerator hardware limiting it to specially equipped, designated DU compute nodes. In addition, due to a limited number of RUs served by each DU and strict requirements on the fronthaul transport network, DU deployments are limited close to the network edge.

Scalability Implications

Generally speaking, the C-RAN deployment model offers the greatest degree of deployment flexibility, but also incurs the highest infrastructure overhead for relying on general purpose compute resources. While the CU may be fully virtualized and thus easily centralized and scaled, hardware requirements of DU and RU limit the potential for virtualization. This architecture is adopted by the O-RAN alliance specification [ORAN], further augmenting the 3GPP specification by additional interfaces, including but not limited to, standardized OAM and fronthaul. This creates the opportunity for vendor-neutral, interoperable deployments where individual parts of the RAN may be acquired from different sources. Due to its reliance on powerful compute infrastructure, this approach is mostly suited for medium to large-scale deployments. It is most useful and efficient where synergies with existing datacenter infrastructure may be leveraged.

5.1.2 Transport network requirements

In disaggregated RAN deployments, special attention needs to be paid to the requirements put on the transport network by the interfaces between the different RAN network functions. While the mid- (F1) and backhaul (NG/N2/N3) interfaces requirements are largely dictated by aggregate throughput which may be satisfied by contemporary datacenter and enterprise network environments offering 10/25 GbE connectivity, the fronthaul interface's requirements

for connecting DU and RU are more demanding. In the following, we refer to the O-RAN Alliance specified Open Fronthaul interface as the de-facto standard [O-RAN.WG4.CUS.0]. It builds upon the eCPRI specification using Ethernet transport. Depending on RU size and supported bandwidth, up to two 25 GbE links may be required between DU and RU with a typical small indoor RU requiring 10 GbE connectivity. However, due to protocol timing requirements and synchronized TDD operation across the network, strict timing requirements are put on the fronthaul transport network. Typical delay budgets limit the feasible length for fronthaul links to 5km, which may further be reduced by processing delays introduced by additional network nodes along the path [PER19].

Due to synchronization requirements, all RAN deployment models require a common global time source, typically provided by a global navigation satellite system (GNSS). In outdoor deployments, gNB nodes may synchronize directly utilizing using dedicated GNSS timing receivers. However, use of packet timing technologies such as IEEE 1588 (PTP) or SyncE is becoming the norm and for indoor deployments is a strict requirement. It follows, that in any case as soon as an architecture option or deployment model with dedicated or indoor RAN is chosen, a timing aware network infrastructure in compliance with telecom standards family ITU-T G.8275 for fronthaul transport has to be erected.

5.2 Core Network

On the core network side, virtualization is the key for scalability, and it is the catalyst for automation of the network management and orchestration from a scalability point of view.

Referring to the architectural setups investigated by the project (cf. D1.2), on the one hand fully on-site networks have the advantage of being tailored to the exact need of the facility and users that they serve, without looking for a one-size-good-for-all hardware and software deployment. On the other hand, a hybrid core network is ideal for scalability over several sites, also in geographical locations that are far from one another: a company that builds a new site can quickly and effectively deploy in it an edge node and connect it to the centralized control plane to make it part of the same private network.

Furthermore, hybrid solutions that exploit private or public cloud resources can leverage the cloud's native resources and solutions that are dedicated to scalability. Both vertical and horizontal scaling are "infrastructural" over the cloud, and, from the IT point of view, the management and orchestration of the core network resources is dealt with by the cloud infrastructure provider, not necessarily by the network owner/provider. A public-cloud-based solution moves the burden of IT management from the company itself to an external professional.

So, combining the hybrid and fully on-site solutions within the same network as is done at the two European sites of the 5G CONNI demonstration system (see also Section 6) allows a perfect combination of independence and scalability over sites.

The four architecture options for private 5G networks discussed in Sec. 3 of D2.1 and analyzed in detail in Sections 2 and 4 of the present document reflect different core network deployment and governance models, the cost implications of which are discussed in D2.1.

6 5G CONNI Demo System Architecture

In this section, we recall the main architectural features of the demonstrative setups that are being developed within the activities of WP5. Then, we discuss how the specific architectural choices answer the use case requirements, and how they are related to the SWOT analysis and the operator model evaluation presented in the previous sections.

6.1 Architectural Design

6.1.1 European setup

The European setup, represented in Figure 4, is conceived to provide 5G connectivity to three different sites, located in different geographical areas: a company's headquarters (HQ), physically represented by some offices at HHI; a manufacturing site of the same company, represented by one of BOSCH's factories; and a central cloud.

The proposed design is made of two interconnected CN deployments.

The first is *hybrid*, in the sense that the control plane functions are instantiated at the cloud whereas the user plane resides at the enterprise's HQ, collocated with the Radio Access Network (RAN).

The second, instead, is *fully on-site*. The choice to have a replica of the CN deployed at the factory allows to maintain local the factory's data traffic with security benefits and, not less importantly, to enable edge computing at the local edge servers. Moreover, the network function redundancy that follows from this architecture, guarantees business continuity even in case of malfunctions of one of the two CNs. A complete description of the European setup and of its hardware and software components is available in D5.1.

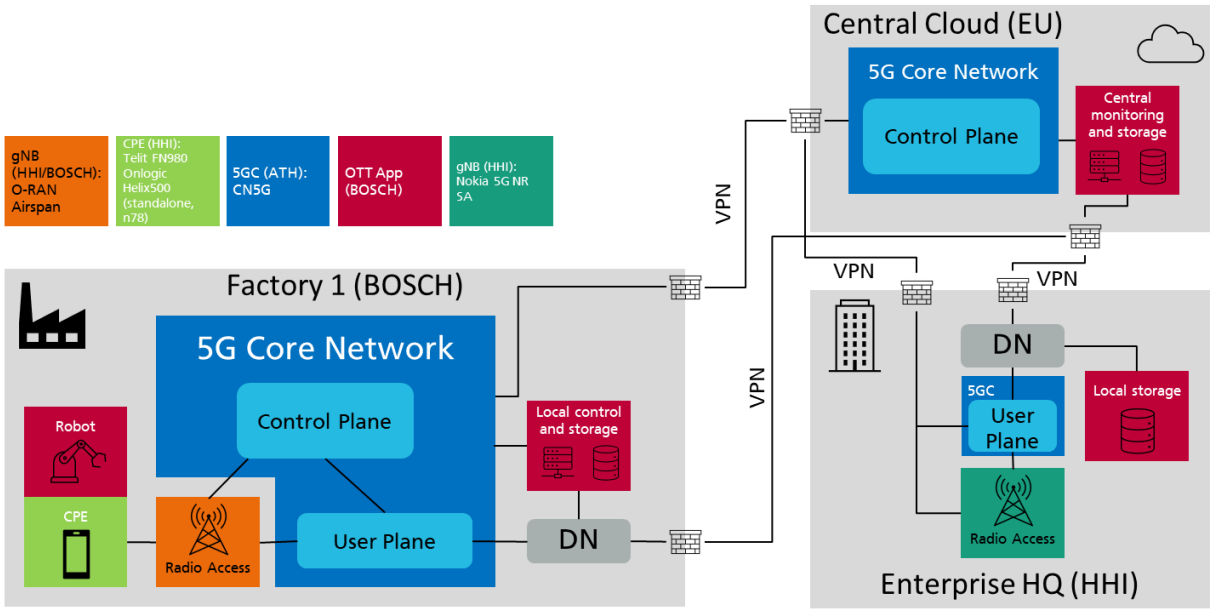

Figure 4: The European demo setup.

6.1.2 Taiwanese setup

The 5G network logical architecture is illustrated in Figure 5, where two main sites are interconnected:

1. The facility at ITRI that represents an enterprise's data center.

2. The pilot production site (ITRI's IMTC, Intelligent Machinery Technology Center) that represents the enterprise's manufacturing site. It involves a machine room to host most of the network elements and a metal workshop.

The proposed setup moves control plane functions of the 5G core towards enterprise data center, while the user-plane traffic will be terminated on the premises for delay-critical services or forwarded to the enterprise data center for monitoring purposes. The MEC platform is deployed at the IMTC and transparently integrated between the base station and 5G core without signaling connections, which requires little re-configuration of the 5G system. In addition, all network functions are located inside the logical perimeter of the enterprise, data privacy and security are fully supported with the demo setup. A detailed description of the Taiwanese setup and associated hardware and software components is available in D5.1.

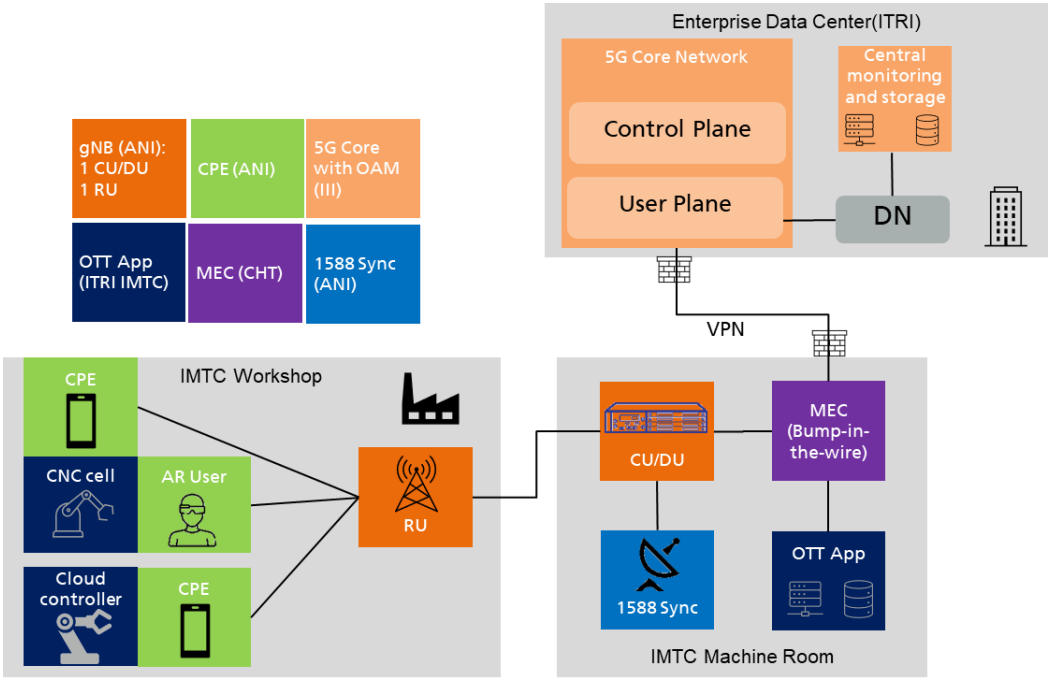

Figure 5: The Taiwanese demo setup.

6.1.3 End-to-end setup

The end-to-end setup, pictured in Figure 6, is designed to unify into a single framework the European and Taiwanese network architectures. As such, the setup constitutes a prototype of intercontinental company network deployment that interconnects two independent local private networks to satisfy the requirements of the inter-site use cases presented in Section 3.

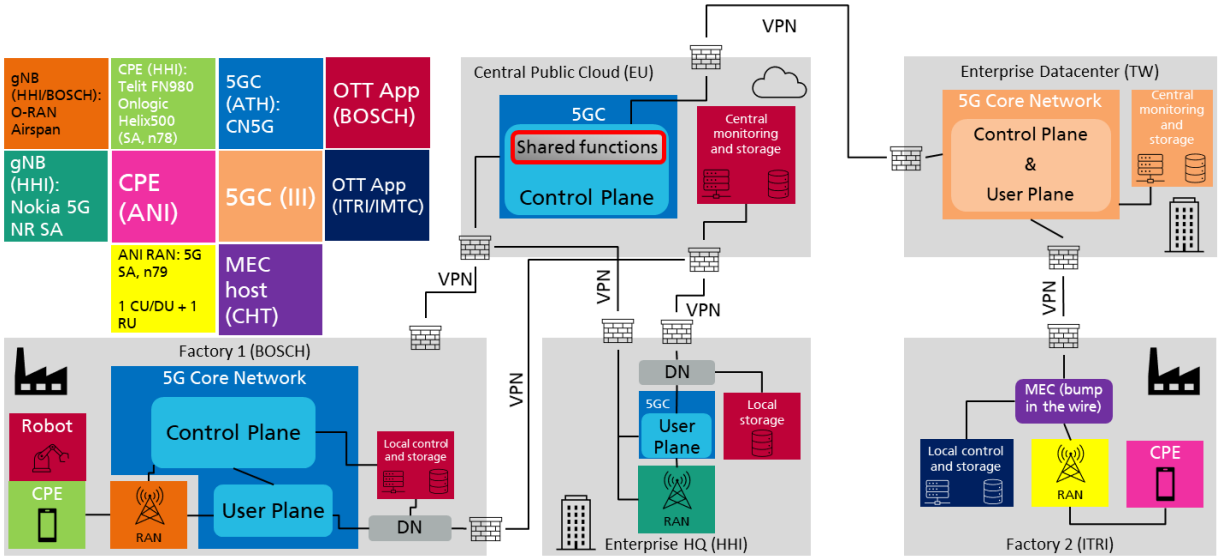

Figure 6: The end-to-end Euro-Taiwanese setup.

Such interconnection is obtained by sharing the authentication and user data management functions at the central 5GC deployed at the central cloud. This minimizes the IT and network configuration effort whenever, for instance, some company assets are shipped from one continental site to the other and need to be rapidly and easily put in play. More details on the end-to-end demo architecture are provided in D5.1 and the results of the experimentation over such a demonstrative setup will be reported in D5.2 and D5.3.

6.2 How the System Architecture Supports the Targeted Features

Three use cases that are planned to be implemented at the 5G CONNI demo sites were described and specified in the 5G CONNI deliverable D1.1 of WP1. Each of these use cases entails a number of functional (13) as well as non-functional (14) requirements, systematically documented in D1.1. Many of them are essential to the realization of the use case, in particular in the demo setups. In addition, 61 functional requirements exist that go beyond the demo use cases and relate to the theme of private 5G networks rather than the use cases. In D1.1, they were categorized into eight different groups, including requirements related to subscriber and identity management, cyber-security, etc. Those requirements that are related to the architecture design are discussed in Section 6.2.1.

In addition, there are concerns and requirements regarding operator models, which have been thoroughly analyzed in the 5G CONNI Deliverable D1.2. Section 6.2.2 discusses how these requirements are addressed by the chosen architecture, also in relation with the SWOT analysis of Section 2 and the evaluation of the operator models of Section 4.

6.2.1 Requirements That Have Influenced the Architecture Design

In the following table, we recall from D1.1 the functional requirements that are relevant for the three selected use cases. Moreover, we highlight which of such requirements were particularly relevant for the architectural design of the 5G CONNI demonstrational testbeds.

Table 6: Use Case Functional Requirements and Relevance for Architecture Design.

FR-ID	Functional requirement	Relevant for architecture design?	Motivation
FR-1	Mobility management	X	• Both local setups allow local mobility within a location (a factory or the HQ). • The EU setup allows mobility between the factory and the HQ with minimum reconfiguration effort. • The end-to-end design addresses the case of a UE that can connect to both the European and the Taiwanese networks with minimal configuration effort.
FR-2	Energy efficiency		
FR-3	End-to-end QoS	X	• All network elements (CPE, gNB, MEC, Core) have to support QoS following 3GPP specifications. 5GC can provide multiple QoS rules per DNN through 5QI, and the gNB and UE will consider the setting to apply the end-to-end QoS support. • Local breakout and the UPF deployed at the edge allow for end-to-end QoS management at the factory.
FR-4	Network capability exposure	X	The AF at the factory of the EU testbed exploits the network exposure capabilities for controlling the feedback loop (for instance, via monitoring of the performance metrics).
FR-5	Priority, QoS and policy control	X	5GC and UE will be able to decide proper QoS rule, and MEC supports data traffic transmission priority according QoS
FR-6	Time synchronization		
FR-7	Localization service		
FR-8	Context-aware network	X	The AF at the factory of the EU testbed exploits the network exposure capabilities for controlling the feedback loop (for instance, via monitoring of the performance metrics).
FR-9	Real-time end-to-end QoS monitoring	X	• Where fully private model is adopted, the degree of

			compliance regarding E2E QoS monitoring is high. • Where 5G elements are deployed across different places (Enterprise, edge site, HQ, core cloud), APIs must be provided for monitoring the overall system.
FR-10	5G LAN-type service support / Layer-2 LAN switching capability support / Ethernet transport services		
FR-11	Proximity services		
FR-12	Secure remote access	X	• Remote authority management and control is related to stakeholders, so secure remote access is relevant for the architecture. • Secure remote access is typically supported via VPN. • The fully on-site deployment for remote access ensures that security management and control can be fully controlled on the enterprise side.
FR-13	Edge computing	X	• Enabled by default with the adopted architecture, typically because the user plane and the destination DN are on site • Supported via either bump-in-the-wire or distributed UPF configuration.

Furthermore, similarly to above, we include in the following table the list of non-functional requirements.

Table 7: Use Case Non-Functional Requirements and Relevance for Architecture Design.

NFR-ID	KPI	Relevant for architecture design?	Motivation
NFR-1	Service bitrate	X	The fully on-site and the hybrid (with localized UPF) deployments guarantee a higher service bitrate, thanks to the dedicated RAN and the full localization of the traffic for latency-critical applications.
NFR-2	Communication area		

NFR-3	Connection density		
NFR-4	Area traffic capacity		
NFR-5	UE speed		
NFR-6	Positioning accuracy		
NFR-7	Positioning latency		
NFR-8	Motion-to-photon latency	X	The low communication delays enabled by the deployment of the UPF at the edge in the fully on-site and hybrid setups guarantee that the motion-to-photon latency requirement imposed by the AR/VR use case is respected.
NFR-9	End-to-end latency	X	The fully on-site and the hybrid (with localized UPF) deployments support low end-to-end latencies whenever needed.
NFR-10	Transfer interval	X	The fully on-site and the hybrid (with localized UPF) deployments guarantees shorter transfer intervals for specific applications running at the edge.
NFR-11	Transmission time	X	The fully on-site and the hybrid (with localized UPF) deployments reduce transmission times for specific applications running at the edge.
NFR-12	Survival time	X	Fully on-site functions, both in an independent only on-site deployment and in a redundant mixed on-site/hybrid deployment, allow for shorter tolerable survival times, thus increasing service resilience.
NFR-13	Message size		
NFR-14	Video latency	X	The fully on-site and the hybrid (with localized UPF) deployments support low communication latencies.

Beyond the use case requirements, 19 goals for a reasonable deployment of a private 5G network should be considered, where each of the goals falls into one of following eight categories (see D1.1, Section 5). The following table points out the categories of goals that were relevant for the demo's architectural choices.

Table 8: Deployment Goals Categories and Relevance for Architecture Design.

CAT-ID	Category of Goals	Relevant for architecture design?	Motivation

C1	Subscriber and identity management	X	Shared AUSF/UDM is adopted to logically connect the continental sites, thus making a unique architecture in which subscribers can relocate between the sites easily.
C2	Cyber-security	X	Fully on-site deployment and VPN connections support the cyber security.
C3	Monitoring and alerting	X	Supported by the APIs exposed by the network locally on-site.
C4	Slice and network management	X	All network elements support Priority, QoS and policy control. 5GC and UE will be able to decide proper QoS rule, and MEC supports data traffic transmission priority according QoS.
C5	Service availability	X	Service availability is maximized at the EU factory (via on-site deployment).
C6	Access control		
C7	Voice services		
C8	Charging		

6.2.2 Reasoning from the Perspective of the Operator Model Evaluation

Besides targeting to satisfy the requirements and categories of goals recalled above, the 5G CONNI demo system architecture was designed considering the SWOT analysis reported in Section 2 and the evaluation of the related operator models summarized in Section 4. Namely, the EU, TW, and E2E setups emerge as a synthesis of such investigations with the concrete business and technological interests of the partners of the consortium.

As recalled in Section 6.1.1, the network architecture of the EU side of the E2E demo is the result of the combination of two operator models: the *fully private* and the *hybrid*. This choice is the consequence of several concurrent factors. First of all, it meets the overall goal of the project of fostering the adoption by companies of their own private networks, giving them "maximum" control of such resources. Telecommunication networks become in this way *infrastructural* to the companies themselves in the same way as physical facilities and IT networks already are nowadays, thus yielding new business models, production flows, and management/operation strategies. From this perspective, the fully private option meets the enterprise's preferences and interests highlighted by our operator model evaluation. For instance, the aspect that the enterprise retains control over most or all network elements (in terms of ownership and governance) leads to less complex processes during the entire network lifecycle, as well as higher data security levels, irrespective of the fact that this might require acquiring additional competencies regarding network operations, etc. As we also saw in Section 2, preferences by an enterprise are justified by this model's high resilience, degree of physical and cyber security, and compatibility with the stringent requirements imposed by latency-critical applications.

Now, the choice of a fully private core network and RAN deployment at a company may be somehow drastic, and therefore it needs to be evaluated case by case whether its strengths and opportunities entirely justify it. Thus, 5G CONNI's EU demo includes also a hybrid

architectural setup, which contributes to represent a more realistic scenario that mitigates the potential weaknesses of a pure fully on-site model. Such weaknesses are, for example, distributed and replicated, and hence costly control plane functions (while for the hybrid model, network functions run in a centralized manner), and less required competencies for the enterprise, when operated by an MNO or SP. At the same time, it is the most suitable deployment for a company made of multiple branches and sites, with different facilities for different business tasks. Such a hybrid architectural configuration endows the setup with further flexibility, scalability, and streamlined management of the multi-site networking operations, as put in evidence by the SWOT analysis. Finally, it is not a coincidence that the consortium has chosen to focus on and implement the two models that reduce to the minimum the role of MNOs[1]. In part – and very pragmatically – this is due to the absence of an MNO among the European partners of the project. Yet, more importantly, this supports the intention of the project to showcase how private networks open the field to new business models and roles for enterprises and service providers like RAN and core network providers and integrators, independently from the classical role that mobile operators have played so far.

Like the 5G CONNI's EU demo side network architecture, the Taiwanese demo side also deploys the network architecture of two operator models: the fully private and the hybrid. The TW site owns and governs network as a network vendor that inherently takes full control of the whole network. The TW site fully private network is performed by professional 5G personnel to carry out lifecycle tasks for network operations. It obtains spectrum license from government authorization to acquire certain frequency range different from commercial frequency. The dedicated private wireless network expansion can be achieved to satisfy the demands. The TW site also deploys hybrid model of the edge cloud in the factory that adopts Bump-in-the-wire MEC to support edge computing technique. The 5G Core Network and its control plane is separately located at Enterprise Data Center (ITRI) including OAM for network management. The transport network between Enterprise Data Center and the factory machine room is set up by the premium Ethernet leased line with guaranteed transmission rates, standard telecom QoS management, and SLA assurance. The hybrid operator model enable time-critical user-plane traffic like robot platform control is directly processed by local MEC edge server to shorten the latency. For some production statistic data, that are transported via dedicated Ethernet-over-SDH circuit to the Enterprise Data Center not only for monitoring production efficiency but also to ensure data privacy.

The fully private and the hybrid operation models in Taiwan side do not involve stakeholders like MNO and SP. The fully private operation model brings several strengths to higher flexibility in deployment, exclusive access without resource sharing, flexible adaption to the enterprise's specific requirements like service bitrates, and full control over the 5G private network. The MEC server in the hybrid model offers the benefits of multi-site extension capability and confidential data to remain locally on-site. To fulfill the requirements of cyber security and secure remote access, the transport network in Taiwan side utilizes VPN connections over the premium ethernet leased line. The enterprise data center can be remote access through a secured connection for full remote control and monitor the whole 5G network.

Finally, but not less importantly, notice that the E2E setup that spans across the EU and Taiwan is another instance of a hybrid operator model and network architecture. As such, it has the same features and advantages highlighted for the EU hybrid setup, made even more valuable by the peculiar geographic characteristics of such scenario, that connects facilities situated in two different continents into a single networking framework. 5G CONNI's E2E

[1] In particular, notice that the hybrid configuration of the EU testbed does not leverage the support of an external MNO, as allowed in principle by the most general definition of a hybrid model (cf. D2.1).

testbed was conceived to push the concept of private network towards unexplored applicative and operational fields. This requires the adoption of the most flexible and adaptable network architecture, the hybrid one, as shown by the SWOT analysis and the operator model evaluation.

7 References

[D1.1] “Report on Use Cases & Requirements,” 5G CONNI, Deliverable D1.1, 01.07.2020.

[D1.2] “Report on Relevant Requirements and Concerns Regarding Suitable Operator Models,” 5G CONNI, Deliverable D1.2, 31.12.2020.

[D2.1] “Intermediate Report on Private 5G Network Architecture,” 5G CONNI, Deliverable D2.1, 04.09.2020.

[D5.1] “E2E In Lab System Integration Report,” 5G CONNI, Deliverable D5.1, 30.06.2021.

[38.401] *NG-RAN; Architecture description,* 3GPP TS 38.401, V15.6.0, June 2019.

[ORAN] *O-RAN Architecture Description,* O-RAN Alliance TS O-RAN.WG1.O-RAN-Architecture-Description-v04.00, V04.00, March 2021.

[O-RAN.WG4.CUS.0] *Control, User and Synchronization Plane Specification,* O-RAN Alliance TS O-RAN.WG4.CUS.0, V06.00, March 2021.

[PER19] G. Otero Pérez, D. Larrabeiti López and J. A. Hernández, "5G New Radio Fronthaul Network Design for eCPRI-IEEE 802.1CM and Extreme Latency Percentiles," in *IEEE Access*, vol. 7, pp. 82218-82230, 2019, doi: 10.1109/ACCESS.2019.2923020.

Annex I: Quantitative Ratings of Operator Models

Table 9: Scores for different aspects and operator models from the perspective of the enterprise.

Aspect	Rating			
	FPM	Hyb	MVNO	MNO
A1	0.88	0.62	0.64	0.68
A2	0.81	0.67	0.63	0.56
A3	0.67	0.57	0.57	0.83
A4	0.91	0.74	0.74	0.66
A5	0.92	0.66	0.66	0.46
A6	0.84	0.75	0.75	0.63
A7	1.00	0.50	0.70	0.70
A8	0.75	0.62	0.75	0.75
A9	0.75	0.75	0.64	0.75
A10	0.90	0.81	0.58	0.58
A11	0.65	0.65	0.93	1.00
A12	0.67	0.67	0.92	0.92
A13	0.83	0.83	0.83	0.83

Table 10: Scores for different aspects and operator models from the perspective of the MNO.

Aspect	Rating			
	FPM	Hyb	MVNO	MNO
A1	0.85	0.85	0.78	0.82
A2	0.88	0.88	0.75	1.00
A3	0.81	0.75	0.65	0.63
A4	1.00	0.75	0.75	0.75
A5	0.86	0.86	0.67	0.80
A6	0.69	0.59	0.91	0.72
A7	0.66	0.50	0.50	0.50
A8	0.57	0.50	1.00	0.91
A9	0.75	0.50	1.00	1.00
A10	0.83	0.50	0.71	0.71
A11	0.75	0.50	0.63	0.75
A12	0.63	0.50	1.00	0.75
A13	1.00	1.00	1.00	0.50

Table 11: Scores for different aspects and operator models from the perspective of the service provider.

Aspect	Rating			
	FPM	Hyb	MVNO	MNO
A1	0.36	0.51	0.51	0.44
A2	0.75	0.75	0.75	0.75
A3	0.56	0.56	0.56	0.44
A4	0.75	0.75	0.75	0.75
A5	0.59	0.59	0.59	0.59
A6	0.52	0.66	0.75	0.42
A7	0.59	0.59	0.59	0.59
A8	0.00	1.00	1.00	0.27
A9	0.75	0.75	0.00	0.00
A10	0.60	0.71	0.71	0.29
A11	0.50	1.00	0.50	0.00
A12	0.50	0.50	0.50	0.50
A13	0.38	0.38	0.38	0.38