Advanced Techno-Economic Modeling of Industrial 5G Non-Public Networks

Jyrki Penttinen
Alphacore Inc.
Tempe, AZ, USA
email: jyrki.penttinen@outlook.com

Jari Collin
Telia Company
Helsinki, Finland
email: jari.collin@telia.com

Jarkko Pellikka
Nokia
Helsinki, Finland
email: jarkko.pellikka@nokia.com

***Abstract*— Non-Public Networks (NPNs), commonly referred to as Private Networks, are emerging as a pivotal component in commercial deployments across a wide range of industrial verticals, offering tailored connectivity solutions that meet specific operational needs. The development of NPNs is being spearheaded by the 3rd Generation Partnership Project (3GPP), with current models spanning multiple generations of mobile communication technology. This paper provides a review of the state-of-the-art standardized NPN solutions, with a particular focus on Fifth Generation (5G) mobile communications and critically evaluates their suitability for industrial applications identifying gaps in the existing NPN models that need to be addressed to fully realize their potential. Using selected industrial use cases, the paper explores the practical implications of deploying NPNs, analyzing key factors such as network performance, reliability, and security that are crucial for Industrial IoT (IIoT) scenarios. Furthermore, the paper assesses the key techno-economic considerations involved in NPN model selection, providing a framework for evaluating the cost-effectiveness and scalability of NPN solutions in industrial contexts. This paper offers insights and proposes base modeling and further evolved methodologies for optimizing the deployment and management of NPNs to support the growing needs of the industrial ecosystem.**

Keywords—NPN; private network; 5G deployment modeling; NPN optimization; network planning.

I. INTRODUCTION

A Non-Public Network (NPN), referred also to as Private Network, provides network services in isolated environment. It can be based on cellular networks or other wireless technologies, and it does not depend on numbering of regulated Public Land Mobile Networks (PLMN). Building upon previously published research [1] and the posterior advances of private networks, this paper explores the feasibility of NPN for serving industrial 5G applications. In addition to the assessment of available information from the standardization and field in general, this paper expands and deepens our originally presented model that helps select feasible private network model implementation considering specific requirements and needs of the users.

5G NPN refers to a 3GPP cellular system to deliver its capabilities for NPN use cases, such as businesses and municipalities. The 5G NPN can reside partially or completely in physical premises of an organization using it, e.g., within a factory or campus area, so that an external entity separate from a Mobile Network Operator (MNO) assumes the responsibilities of the isolated part offering its services to a limited group. NPN does not typically allow inbound roamers, although the NPN users may have roaming capabilities to use other PLMNs.

The benefits of NPN deployment include the possibility to control the Quality of Service (QoS) and protection by isolation. NPN service can include voice connectivity in defined geographical areas, or it can focus on Internet of Things (IoT) and respective industrial applications; today, there are many test projects and commercial setups involving industrial devices [2].

This paper explores the applicability of NPNs for Industrial 5G applications. “Industrial 5G” refers to Industrial Internet of Things (IIoT) with real-time data of networked sensors, assets, objects, and people, 5G network, and edge computing enabling ultra-reliable, low-latency, and high-bandwidth communication.

The presented model aims to provide means to evaluate the feasibility of available private network deployment options considering key requirements of use cases of interest, and it supports techno-economic assessment considering realities of various network deployment scenarios.

This paper introduces standardization of private network landscape in Section II and summarizes the key architectures of the available 3GPP models in Section III. Section IV discusses private network deployment models including 3GPP and other relevant options highlighting their key aspects. Section V summarizes the most important benefits and drawbacks of the presented private network variants, comparing their suitability in different scenarios. Section VI presents how techno-economic modeling can be applied in the selection of the most feasible variants based on key cost items related to Radio Access Network (RAN), Core Network (CN), Trasport Network (TN), and respective Capital Expenditure (CAPEX) and Operational Expenditure (OPEX) items. Section VII presents our further developed model, and Section VIII summarizes the findings.

II. STANDARDIZATION

Private networks can be formed by a variety of technologies. The 3rd Generation Partnership Project (3GPP) has designed technical architecture specifications that build upon mobile network technologies, and industry bodies complement the effort through deployment guidelines.

A. 3GPP

3GPP has designed 4G and 5G NPN specifications in Release 16 providing enablers for 5G IoT, including IIoT [3] [4]. The areas include Time Sensitive Networking (TSN), NPN, and Local Area Network (LAN) type services. Release 17 evolve these capabilities further defining NPN in the Technical Specifications TS 23.251 (architecture and functional description of network sharing) [5], TS 22.104 (service requirements for cyber-physical control applications in vertical domains) [6], and TS 23.501 (5G system architecture) [7].

As stated in [8], Release 18 studied a set of features to evolve NPN. These study items include solutions for the support of non-3GPP access such as Wireless LAN (WLAN), support of mobility between Standalone NPNs, (SNPNs) without a need for new network selection, and means to provide access to local services such as enablement of localized service provider that can interact with NPN for local services.

Also, clarified specifications for charging aspects were noted important because, although no complex charging functions are needed for use cases involving internal SNPN communications, interaction between external entities may require support for more complete charging models.

As the NPN ecosystem evolves, a variety of new use cases and scenarios arise including, e.g., interaction involving one or more SNPNs, Public Network Integrated NPNs (PNI-NPNs), and MNO networks, and this expanding environment requires adequate solutions for a fluent charging. Release 18 has identified also the need for further enhancement of security and management of NPNs including end-to-end communications through radio and core networks, as well as capability exposure management for NPN variants.

As a result, the 3GPP Release 18 specified functions for the support: 1) of mobility between equivalent SNPNs, 2) for trusted and untrusted non-3GPP access for SNPN, 3) for connecting devices that lack support for 5G Core Non-Access Stratum (NAS) signaling over non-3GPP access to SNPN, and 4) for localized services during limited time within limited area. The Release 18 use cases focus largely on scenarios involving generic public in, e.g., campus, exposition, stadium, and concert venues. [9]

B. Industry Bodies

The 5G-ACIA (5G Alliance for Connected Industries and Automation) summarizes industrial IoT deployment scenarios for 5G NPNs based on 3GPP-defined 5G NPN [10]. It presents deployment models to complement their architectural design.

Also, GSMA (GSM Association) considers NPN, and their guidelines provide overview to deploy 5G industry campus NPN by 3GPP definition, which is one of the key 5G concepts to support “to business” models [11].

III. 5G NPN STANDARD ARCHITECTURES

As per the 3GPP Release 16 definitions, an NPN enables deployment of 5G System (5GS) for private use. The NPN can be deployed as a SNPN or PNI-NPN variant. An NPN operator manages SNPN without relying on the functions of a PLMN, whereas PNI-NPN deployment depends on those [12].

Figure 1 depicts NPN variants as interpreted from [11], [10].

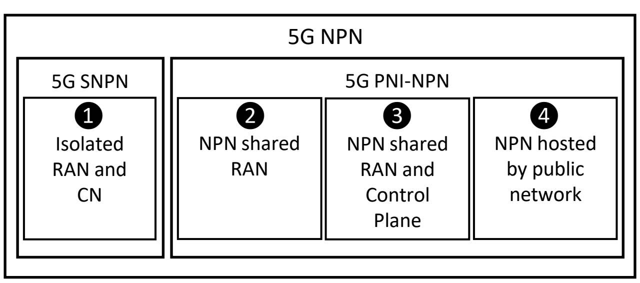

Figure 1 3GPP and 5G-ACIA NPN variants

A. SNPN

The SNPN uses combined PLMN Identifier (PLMN ID) and Network Identifier (NID). 5G User Equipment (UE) supporting SNPN can attach to it based on 5G Subscription Permanent Identifier (SUPI) and credentials. The RAN of SNPN broadcasts the combined PLMN ID and NID in the System Broadcast Information (SBI) signaling and supports network selection and re-selection, load and access control, and barring. The NIDs can be self-assigned individually to the SNPN NIDs upon its deployment.

The active NIDs may not be unique, but they use different numbering space than the other scenario, coordinated NID-assignment, that can have either 1) globally unique NID-assignment independent of the respective PLMN ID, or 2) globally unique NID/PLMN ID combination.

B. PNI-NPN

The PNI-NPN uses PLMN ID whereas Closed Access Group Identity (CAG ID) indicates the CAG -enabled 5G radio cells. Within a PLMN, a CAG cell can broadcast one or more CAG IDs, in which case PLMN ID is the base for the network selection and reselection whereas the network uses CAG ID for the cell selection and re-selection, as well as for the control for letting only CAG-enabled UEs access the network.

C. Implementation Aspects

As depicted in Figure 1, these two options result in practical scenarios of isolated deployment of standalone non-public network (1) or non-public network in conjunction with public networks. The latter breaks down into three scenarios including the Industrial and IoT environment: shared RAN (2); shared RAN and Control Plane (CP) (3); and NPN hosted by the public network (4) [10].

- SNPN: the NPN is separated from the public network, and all network functions reside inside the organization’s premises. The possible communication between the NPN and the public network takes place via a firewall, e.g., through Non-3GPP Interworking Function (N3IWF).
- Shared radio access network: the NPN and public network share part of the radio access network as per the 3GPP TS 23.251. Communication stays within NPN in this model.
- Shared RAN and CP: the NPN and the public network share the RAN for the defined premises while the public network does the network control tasks, the NPN traffic remaining within the premises. Network Slice (NS) or 3GPP Access Point Name (APN) can realize this case.
- PLMN-hosted NPN: the enterprise is served by a 5G NS.

IV. NPN DEPLOYMENT MODELS

A. Standalone NPN

Figure 2 depicts the principle of SNPN as interpreted from [10] [13]. In this scenario, the User Plane Function (UPF) works as a data router to connect Multi-access Edge Cloud (MEC) and possible LAN. The RAN manages the connectivity of 5G gNB (Next Generation NodeB) and UE of the SNPN users on licensed or unlicensed band. 5G Core (5GC) houses the NFs including Unified Data Management (UDM) of user credentials.

In this model, Network Functions (NFs) reside within the operational area of related entity, e.g., factory, the SNPN being isolated network from the PLMN, allowing the communication between the PLMN and NPN through an optional firewall which isolates the NPN. In this way, Operational Technology (OT) company can operate the NPN and its services, including the NPN IDs to provide additional PLMN services in the NPN coverage area, NPN-subscribers to roam the public networks, and public networks' subscribers to roam the NPN depending on roaming agreement. NPN users may also have dual subscription for PLMN use.

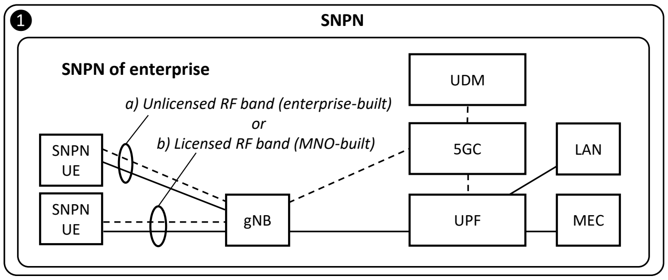

Figure 2 Principle of a SNPN

An example of the NPN 5G deployment on IIoT scenarios is the interconnection with TSN as per 3GPP TS 24.519 [14]. TSN is a set of new open standards that provide deterministic, reliable, high-bandwidth, low-latency communication [15].

The standalone private network can be built in various ways: by dedicated Service Level Assurance (SLA), local PLMN, PLMN by dedicated proportion of operator's licensed spectrum, or by SNPN using unlicensed or private spectrum. Each deployment model has its pros and cons. As an example, licensed spectrum is one of the most expensive single items in the commercial network. Feasible way to set up this type of network is to construct mm-Wave radio access points in a limited enterprise area and virtualized cloud core functions in nearby edge, one option being a broker managing the NPN [16].

B. Shared RAN

Shared RAN involves NPN and PLMN with certain part of its RAN for joint use whereas other network functions remain separated. Figure 3 depicts the principle of this model showing the connectivity of the NPN RAN to PLMN core while the own core network of the NPN is isolated from the external world as interpreted from [10], [11], and [17].

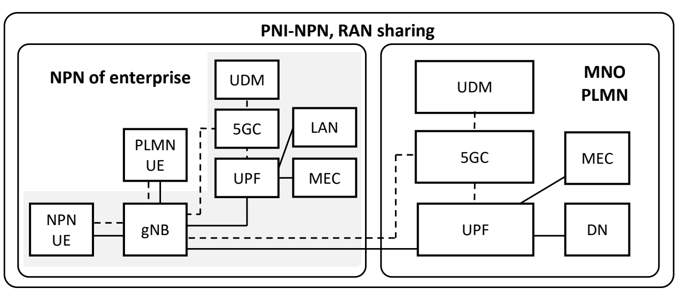

Figure 3 Shared RAN NPN deployment; the grey area indicates the private network slice that forms the NPN

In this deployment model, NPN traffic stays internal and within the logical, defined area, such as factory premises.

The 3GPP TS 23.251 details the network sharing model in its architectural and functional description and scenarios for network sharing usable also in NPN environment, which are Gateway Core Network (GWCN) and Multi-Operator Core Network (MOCN) [5].

C. Shared RAN and Control Plane

As depicted in Figure 4, interpreted from [10], [11], and [17], in this deployment, both NPN and PLMN share the RAN within defined business area premises and PLMN takes care of the control plane so that the internal NPN traffic stays always within the logical network related to the business. NS is one way to set up this scenario creating logically independent networks within a shared physical infrastructure. The isolation of the private network portion is possible by using unique NS identifiers. Using 3GPP-defined APN is another method to implement this scenario. In this case, the APN indicates the target network with opportunity to differentiate traffic.

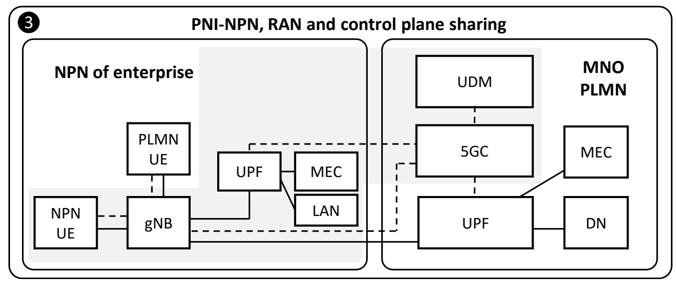

Figure 4 Deployment for shared RAN with control plane; the grey area indicates the private network slice that forms the NPN.

In the shared RAN scenario with shared Control Plane, the PLMN hosts the NPN so that the devices are a subset of PLMN subscribers. This arrangement eases the contractual aspects of PLMN and NPN operators, and the NPN devices can connect, apart from the NPN itself, also to the PLMN services and roaming. The NPN services may connect to PLMN services, which require optional interface between the NPN and PLMN services, so NPN devices can connect to NPN services via the PLMN if the device is located outside of the NPN coverage and still within the PLMN. Logically, if the NPN devices can access the PLMN services, this interface is not needed.

In Shared RAN and Control Plane deployment models, a particularly important evolution is the use of Local Breakout (LBO) architectures, where the UPF and selected application services are deployed locally within or near the enterprise premises while the Control Plane remains integrated with the MNO's infrastructure. This arrangement creates a practical balance between fully isolated SNPNs and fully outsourced public-network-hosted solutions. The enterprise benefits from reduced infrastructure ownership complexity because mobility management, authentication, orchestration, and subscriber control can remain under the operator's domain, while latency-sensitive industrial traffic is processed locally without traversing distant transport and core network paths. This is especially important for Ultra-Reliable Low-Latency Communications (URLLC) use cases such as robotic automation, autonomous vehicles, motion control, machine vision, and TSN integration.

The LBO also improves deterministic performance, data sovereignty, operational resilience, and cybersecurity isolation while still allowing efficient integration with public network services, roaming, and cloud-native management platforms.

D. PLMN-Hosted NPN

In this case, as depicted in Figure 5 and interpreted from [10], [11], [17], both the PLMN and NPN traffic are external to the business area.

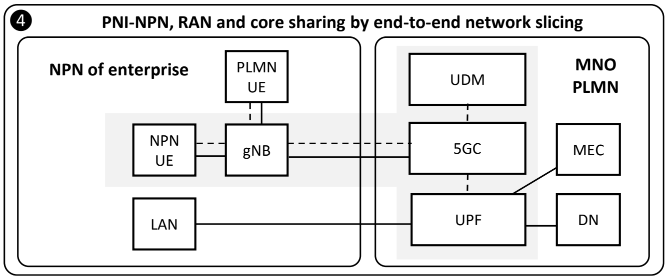

Figure 5 PLMN-hosted NPN; the grey area indicates the private network slice that forms the NPN

This scenario is facilitated by network virtualization and cloudification. It means that these traffic flows are served by different networks, and the NPN subscribers are in fact public network subscribers. The NPN-PLMN roaming implementation is straightforward as the traffic routes via the PLMN.

E. Private Network on Network Slice

Although the differentiation between certain user types is possible in 4G networks, it is limited to techniques, such as the isolation of services in a common infrastructure; the means for this include APN Routing, MOCN, and Dedicated Core Network (DECOR) [18]. Built upon Service Based Architecture (SBA), which enables the use of common hardware that executes the NFs as instances, 5G has been designed to support also network slicing with respective QoS assurance.

In this manner, the Network Slice Provider (NSP) can offer suitable characteristics within their different NSs fulfilling variety of different requirements for their subscribed verticals, also in NPN environment. NS provides means to differentiate the network resources and performance figures that can create also new business models. As an example, an operator can offer their customers gold, silver, and bronze categories, each having their personalized NS price and QoS levels [19]. The NSP can be either MNO or 3rd party. Technically, the NSP could be also enterprise taken their skillset suffices to manage slices.

In NS-based NPN, it is important to adequately interpret the end-user requirements. GSMA provides guidelines for NS setup based on requirements [20], and clarifies how the requirements can be captured from the vertical field [19].

NSs are not yet used widely in commercial Standalone (SA) 5G networks, despite the statistics indicating steady growth and about 25% use base in 5G by 2025 [21]. Furthermore, the optimal NS functionality in practice, especially in the end-to-end scenarios, might require still further development to cope with the impacts of real-world non-idealities in synchronization, near real-time orchestration, and overall management of the slices.

F. Open RAN as a Private Network

Open RAN refers to the overall movement of the telecom industry to disaggregate hardware and software to create respective open interfaces in between [22]. O-RAN Alliance publishes RAN specifications, releases open software for the RAN, and supports O-RAN Alliance members in integration and implementation testing. O-RAN Alliance works on open, interoperable interfaces, RAN virtualization, and big data enabled RAN intelligence [22] [23].

Open RAN may offer feasible small-scale, isolated shared RAN network deployment options also as NPNs. The concept is still evolving, though, and may not provide optimal techno-economic solutions quite soon; nevertheless, as the technology matures, Open RAN may offer competitive 4G and 5G NPN variants.

G. Legacy Network as a Service

Increasing number of incumbent MNOs have switched off their 2G and/or 3G legacy mobile communications networks or are aiming to sunset them soon. Nevertheless, there will remain scenarios involving IoT and voice services via legacy systems, especially in developing markets. According to GSMA statistics, the 2G and 3G systems combined still more than 20% of the global footprint in 2025 [21]. This can be a niche opportunity to manage part of this lessening infrastructure on the remaining spectrum, maintaining a minimum feasible type of infrastructure for IoT and other 2G/3G services via private networks for verticals needing only low capacity.

H. Local and Fixed Wireless Access (FWA)

The LTE-WLAN Aggregation (LWA) as per 3GPP Release 13 allows mobile device configuring on simultaneous LTE and Wi-Fi links [24]. 5G can work also in parallel with non-3GPP access to comply with a light-weight private networks' need. 3GPP Release 15 defines N3IWF allowing Wi-Fi access points delivered through 5G infrastructure as Wi-Fi hotspots or Fixed Wireless Access (FWA).

Release 16 defines further a Residential Gateway (RG) to interconnect end-users' devices via trusted access points. These gateways complement the N3IWF.

FWA can provide solutions to variety of use cases, such as tethering and Mobile Broadband (MBB), best effort FWA, and speed-based QoS [25]. Reflecting these use cases, the FWA could serve as a small-scale home office solution, too, with quick and economic deployment without need for optic fiber.

I. Non-3GPP Wireless Private Network

Technically, it is possible to set up a simple private network using any wireless access beyond the 3GPP specifications on unlicensed, shared spectrum. An example of this is a Wi-Fi hotspot network using common applications within the network providing Over the Top (OTT) voice and messaging. Also, Low Power Wide Area Networks (LPWANs) can provide a feasible communications channel to many IIoT use cases.

V. CONSIDERATIONS OF SCENARIOS

The feasibility of each NPN deployment depends on the foreseen use cases. As an example, the roaming requirements impact the needed coverage and mobility of the end-users of the NPN. This is one of the examples that can dictate the selection between Standalone and PLMN-assisted scenarios.

A. SNSP Deployment

The main aspects of the previously presented deployment models for SNPN scenarios are summarized in the following list, with statements on their suitability for selected use cases.

5G SNPN. An OT operates the NPN and its services behind a firewall independently. This solution provides good level for security isolation, e.g., to IIoT applications as data is not exposed externally. Optional PLMN interconnectivity can be realized via firewall. The operation and management of SNPN requires sufficient level of skillset from OT company. The solution provides an opportunity to build a very secure environment, but it can turn out to be more expensive than only partially owned, or completely outsourced network.

5G SNPN with SLA. The agreed SLA level impacts the business case in this model, so, the higher the SLA, more costly the CAPEX and OPEX are due to, e.g., active-active network mode and reliability of, e.g., 99.999% as per 3GPP Release 15 URLLC performance, or up to 99.9999% as per Release 16 performance for, e.g., TSN interconnectivity to serve critical IIoT applications.

PLMN with local infrastructure. This is a special case of PLMN that isolates part of the infrastructure and spectrum for sole use by private network devices in limited geographical areas. It can be set up technically, e.g., by barring access from others than specifically defined set of subscribers.

PLMN on part of MNO's licensed spectrum. Spectrum is typically very expensive investment for the license holder, so dedicating part of it needs to be designed carefully applying techno-economic optimization to adequately balance the cost and expected quality.

SA NPN on unlicensed spectrum. The RAN deployment and RAN business case are light in this scenario as there is no license fee involved. Nevertheless, the QoS cannot be ensured due to load of shared spectrum with possible other users.

B. PNI-NPN Deployment

The following list summarizes key aspects of this model.

NPN shared RAN. NPN and PLMN share part of the RAN, but the NPN communications stay within the defined premises. 3GPP defines well the technical RAN sharing options that can be applied in this model.

NPN shared RAN and CP. The NPN and PLMN share the RAN for the defined premises while the PLMN has network control and the NPN traffic remains within the defined premises. Network slicing serves this model as per 3GPP specifications, complemented by industry forums' guidelines for slice template setup. Alternatively, the setup can be based on APN.

NPN hosted by public network. PLMN and NPN traffic are external to the business area in this scenario so that these traffic flows are served by different networks, and the NPN subscribers are effectively public network subscribers.

C. Pros and Cons of Deployment Models

a) SNPN

Pros: Access for customization, independent controlling; high security by full isolation; RAN functions are within reduced geographical area favoring low-latency applications.

Cons: Deployment cost; expertise required for deployment. Dedicated network for sole enterprise includes the cost of the whole system in the geographic area.

b) Shared RAN

Pros: Optimizes RAN infrastructure costs while the internal data remains within the NPN infrastructure providing good protection; PLMN RAN connectivity serves for delivering the data meant for outside of the NPN as per need. Within the NPN, part of the base stations can be connected to PLMN according to the RAN sharing agreement between the PLMN and NPN operators while the rest can be kept internal. Licensed spectrum copes interferences; deployment less expensive compared to SNPN; uses typically local functions favoring low-latency applications.

Cons: External interferences can be higher than in SNPN, and the overall control of the network is less independent; need for local expertise, although less than in SNSP.

c) Shared RAN and CP

Pros: Licensed spectrum for controlled interferences; lower deployment expenses compared to SNPN and PNI-NPN; SLA can be applied between the NPN and public network.

Cons: Less independent from public networks; latency typically higher than in SNSP and PNI-NPN deployments; some local expertise required.

d) Hosted solution (Network Slicing by NSP/MNO)

Pros: Facilitated by NSP, no need for local expertise; fast to set up and adjust based on expressed requirements.

Cons: Less control for adjustments as the NS is managed by the NSP; technology not yet final, practical deployments require SA 5G network that are not yet many in markets.

e) Open RAN as an NPN service

Pros: The cost can be low; easy to set up by provider; can be hosted as "light-weight" 5G SNPN or NPI-NSN.

Cons: technology is still evolving and the realistic products for Open RAN -based NPN can take time.

f) 5G FWA (home office use case)

Pros: Customer Premises Equipment (CPE) easy to install; replaces fixed cabling.

Cons: use case adequate in a home office environment but limited for larger enterprise NPN use.

g) Non-5G-based solutions (Wi-Fi hotspots)

Pros: Wi-Fi hotspot deployment is rather straightforward within an enterprise area. The radio coverage does not require license, and it can also be extended to reach any Wi-Fi device external to the enterprise premises.

Cons: Low security, limited mobility, and lack of QoS.

h) LPWAN

Pros: Many options available basing on both cellular and non-cellular radio technologies. Cellular-based LPWANs are services integrated to system, easy to deploy.

Cons: Non-3GPP-based LPWANs have varying security and protection levels, and they require a separate infrastructure.

VI. Techno-economic optimization modeling

A. Current Deployment Models

Each NPN deployment model has its advantages and disadvantages. Understanding the requirements of the use cases and applying tecno-economic optimization assessment that considers the key variables, the selection of the most adequate deployment model will benefit favorable business.

In the selection of the deployment model, the task is to understand the realistic needs of the final users of the NPN access, performance, security aspects, mobility, capacity, QoS, and other key factors, and how they can be served by applying cost-efficient technical solutions. It is important to understand also the changing requirements in the foreseen future because along with the evolution of the environment, originally selected, initially optimal model, can turn out to be less optimal in longer term.

As described in [19], related to NS scenarios, the collection of the verticals' requirements can be done via practical means to interpret the needs of the end-users. From the operators' perspective, this can be somewhat challenging task as the verticals may often express their requirements using non-standard terminology or are not able to formulate the actual requirements.

The methodology in [19], despite its original focus on the assessment of vertical requirements for forming NS templates, can be useful to be extended to cover additional aspects the other NPN deployment models. This methodology suits to interpret practical vertical needs based on the foreseen use cases, and to form technical requirements that can be finally be mapped to represent input parameters for the NPN modeling, whether it is about tailored 5G NS template for which the GSMA PRD NG.116 serves as a base, more "traditional" standalone NPN setup, or shared network model.

The aim of the requirement list is to ensure a common understanding of the environment and to set the expectations also for service level.

B. Base Techno-Economic Optimization

The assumption of the modeling is that the NPN is a business between an entity capable of deploying adequate wireless network (such as MNO, NSP, network equipment vendor, or system integrator) and an enterprise desiring to facilitate the mobile communications for their end-users via Industry IoT applications (such as port or energy company monitoring and controlling their workflow via intelligent sensor network).

The model for the selection of the most adequate NPN deployment option can build upon modular elements, which are:

1: *Interpretation* of the enterprise and end-user needs (e.g., via survey) to form technical requirements statement as a base for the input parameters; e.g., capacity (number of expected users/devices), coverage, QoS, need for roaming/local-only utilization; and services (IoT, voice, other).

2: *Business aspects* assessment (understanding possibility for investment in terms of CAPEX and OPEX; flexibility for initial and longer-term investments).

3: *Forecast* of near-future and longer-term outlook for the possible need for expansion of the network, capacity, and evolving QoS (which is important to avoid investing to multiple types of NPN as the requirements evolve).

4: *Any other relevant information* on the deployment aspects.

The assessment of the feasibility of the deployment options relevant to the scenario under evaluation can be carried out based on these results in a comparative manner. The base for the economic assessment is the cost for enterprise in terms of the CAPEX (initial deployment and forecasted posterior need for new infrastructure investments) and OPEX (yearly cost that is required to operate NPN).

The cost estimate of each scenario presented in the NPN Deployment Models Section considers the key attributes, such as area of deployment, device number (total expense x_d), and radio performance indicators, which together result in the required bandwidth and number of radio cells, and finally in the total cost of cells x_{gnb}. As an example, in very high data rate scenario requiring large indoor and outdoor NPN, the number of mm-Wave small cells, each resulting in, e.g., 80-100 m cell range, can be in order of dozens per km^2. Other attributes consider the cost of transmission network x_{tn}, and spectrum x_s.

For the core network, the cost includes the licenses and other cost items to activate the needed network functions NF x_{nf}. Cost of the needed applications / services x_a refers to the support of, e.g., voice service (that requires either own or outsourced IMS core for integrated Voice over New Radio) and IoT service license, and Location Based Service (LBS) deployment. Roaming and interconnectivity cost x_r is related to the agreements with national and international networks.

The cost x_v of other variable items can include, e.g., the actual installation of RAN, TN, CN equipment or cloud / edge environment, including antenna systems, base station shields, cabling, and any other expense that is required to set up an NPN for enterprise.

For the estimate of yearly operating costs y, the same main components as presented in CAPEX analysis generate expenses, such as licensing fees and electricity consumption, whereas an additional item to be considered in operations is the maintenance cost y_m. The resulting Equations for the initial costs (1) and operating costs (2) are thus:

$$CAPEX = x_{gnb} + x_{tn} + x_s + x_a + x_d + x_v + x_r + \sum_{nf1}^{nfn} x_{nf} \quad (1)$$

$$OPEX = y_m + y_{gnb} + y_{tn} + y_s + y_a + y_d + y_v + y_r + \sum_{nf1}^{nfn} y_{nf} \quad (2)$$

In this base techno-economic assessment, the resulting graphs turn out to be linear over time, providing a simplified manner to form an estimated CAPEX and OPEX behavior as a function of time. It should be noted, though, that the variables in Equations (1) and (2) can have non-linear inter-dependencies in practice; as an example, the volume discount of the number of radio cells can also lower the relative cost of core software and cloud feature licensing. This scenario will be discussed in Section VII, Further Developed Model.

The assessment presented hereby results in a statement of the suitability of deployment scenarios to indicate their level of compliance with the requirements. This method can be visualized in terms of the total cost per area as a function of time, considering attributes of interest, such as maximum supported device number or maximum data rate.

The method serves thus to estimate the rough level of initial and longer-term cost of deployment models under evaluation. Most importantly, the model indicates if the initially most cost-efficient option might turn out to be less optimal in longer run.

C. Return on Investment

The described modeling can be extended to estimate Return on Investment (RoI) of private network, including the business of MNO, enterprise, or 3rd party.

The RoI depends on the deployment and operational costs, share of ownership of private network components (hardware, software) versus outsourced items (e.g., 5G core that runs in virtualized environment served by cloud provider) in different deployment scenarios of interest, the generated savings compared to reference deployment scenario (as an example, enterprise can compare MNO-operated scenario against completely or partially enterprise-owned network), as well as potential earnings for different stakeholders.

As an example, enterprise managing completely or partially owned private network, either on shared or own spectrum, could allow also additional users to roam into that network for a fee that depends on the data consumption or time.

Although the pricing of network components is business between the vendors and customers and thus largely non-public information, it can be assumed that large entities investing to either own network infrastructure or outsourced solutions to provide the private network services to the end-users, may benefit from lower costs due to scale of economies compared to smaller entities.

Nevertheless, the private network ecosystem is expected to grow significantly at present, so it can thus also be assumed that small and medium sized entities could reach fortified position for own network component price negotiation in their private network market, which also can impact positively on the pricing models.

D. *Expectations of the Modeling*

As can be seen from Equations 1 and 2, the selected items result in a linear presentation of initial and operating costs. That said, the Equations represent snapshots of scenarios, and each parameter value may have either linear or non-linear behavior as a function of time, number of components, etc. As an example, the expense related to gNB can be either fixed per the number of gNBs, or there could be a volume-based discount granted by the vendor as a function of the number of gNBs.

As can be expected, the values of the cost items in Equations 1 and 2 depend on the markets, vendor pricing strategies, competitive landscape, and many more variables, so the further analysis of scenarios would be merely speculative without the availability of concrete parameter values. Nevertheless, an example of potential possible behavior can be presented by testing different scenarios and cost estimates of the parameters to understand the business impact in short, mid, and long-term operation of a private network.

The scenarios can be divided into following categories for the assessment of the total cost of a network, that a) is completely owned, partially owned, or completely outsourced ownership; b) uses licensed, shared, or unlicensed spectrum; c) has no roaming (completely isolated), or has inbound roaming, outbound roaming, or bilateral roaming.

To complement the evaluation, additional criteria can be assessed, too, for validating the level of compliance for end-user requirements such as QoS, latency, maximum and average data rate, reliability, etc. The level of compliance of different scenarios can be compared by using numeric values and their weights of importance.

Let us assume an enterprise desires to compare the techno-economic feasibility of a) completely own and isolated small-scale (10 mm-Wave gNBs), 5G network (SNPN) that is based on unlicensed 5 GHz spectrum and 5GC NFs on cloud, with b) MNO-operated private network that is based on an NS dedicated to the enterprise with gNBs that are already partially deployed for PLMN users in the area complemented by five additional, enterprise-owned indoor mm-Wave small cells that are located in the enterprise's operational premises.

Based on these assumptions, Figure 6 depicts theoretical example of the relevant key expense behavior over time using the parameters of Equation 1 and 2 and certain estimated values so that they are normalized having the SNPN CAPEX as the reference at year 0.

In this example, the assessment considers a relatively modest base of 50 mid category user smart devices, with 20% yearly renewal rate.

A considerable cost item in the SNPN deployment can be the price of the radio base stations (gNB). It should be noted that this item may vary largely and it depends on the business models applied between selected network vendor and enterprise customer, as well as the final set of quality, functional, capacity, and performance requirements.

Although the 3GPP technical specifications set the reference for the minimum viable performance, for example the level of radio and core network quality needs to be dimensioned based on the desired key performance indicators that may vary based on, e.g., on the criticality of the served area.

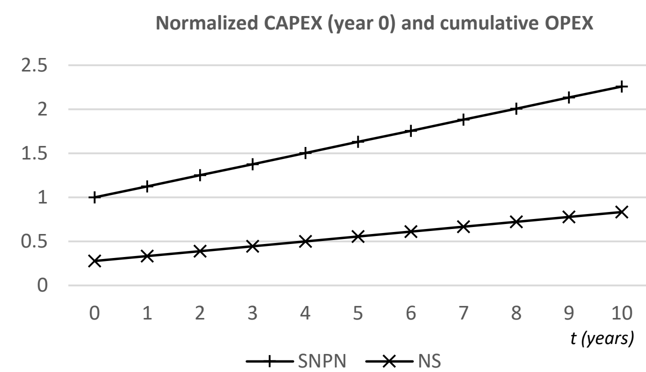

Figure 6 Example of the model's outcome comparing SNPN (reference) and NS deployment scenarios

In the highest quality service provisioning scenarios, a licensed spectrum is important, but at the same time, depending on the national regulation and type of license agreements, the license fees may represent a major cost item.

As the SNPN in this initial base assessment uses unlicensed spectrum, the analysis assumes there are no related fees in the use cases or the results presented in Figure 6.

Another cost item for an enterprise-owned and operated SNPN is the transmission from gNB to the rest of the network. Its significance depends on the respective provider and cost models. It can be assumed that this cost item is not of concern in completely outsourced NS deployment model.

As can be seen from Figure 6, the initial cost of completely own network of enterprise can be considerably higher than a subscription to MNO's NS-based service to form a private network due to required investments on the infrastructure. In this scenario, the OPEX of the SNPN adds up faster, too, compared to the dedicated MNO NS due to need for maintenance and licensing expenses of the own network.

VII. Further Developed Model

The original techno-economic assessment presented in the conference version of this work provided a high-level framework for comparing different NPN deployment options using simplified CAPEX and OPEX representations [1].

Although this approach served as a baseline for illustrating the economic differences between deployment models, in practical industrial deployments, the behavior of private network costs, reflecting operational requirements, is considerably more complex than what purely linear models can adequately describe.

A. New Aspects of the Model

Industrial 5G deployments evolve over time. The operational environment may change, e.g., due to increasing numbers of connected devices, evolving QoS and other performance and functional requirements, software modernization, expansion of edge computing resources, changes in energy pricing, and increasing cybersecurity requirements. The deployment costs may exhibit nonlinear behavior, too.

As an example, the unit cost of radio access equipment may decrease due to economies of scale or customer-specific discounts over time and bulk orders, while maintenance aspects may vary disproportionately as the network expands. Equally, virtualization and cloud-native architecture models may initially reduce infrastructure investments but introduce recurring operational costs that can grow over time as per traffic and computational demand.

For these reasons, the presented enhanced model aims to extend the original framework into a dynamic lifecycle-oriented techno-economic model, which can reflect realistic operational behavior of industrial 5G NPNs. The updated model includes weighted multi-criteria assessment and takes better into account nonlinear parameter dependencies, deployment specialization coefficients, technology renewal cycles, and time-dependent operational growth functions. The resulting framework enables comparative evaluation of different deployment scenarios, including SNPNs, PNI-NPNs, NS deployments, Open RAN implementations, and hybrid ownership models.

The objective of the new model is still to identify the lowest-cost deployment alternative considering technical requirements, but considering more detailed operational constraints, scalability expectations, and long-term economic sustainability.

B. Lifecycle Modeling

The enhanced model presented hereby evaluates the Total Cost of Ownership (TCO) of a private network deployment over a selected operational lifetime. The model considers both initial investments and operational costs while discounting future expenditures to present value using a configurable discount rate. The lifecycle cost model can be expressed as:

$$TCO(t) = CAPEX(t) + \sum_{i=1}^{t} \frac{OPEX(i)}{(1+r)^i} \tag{3}$$

where $TCO(t)$ represents cumulative lifecycle cost at year t, $CAPEX(t)$ denotes cumulative infrastructure investments up to time t, $OPEX(i)$ represents yearly operational expenditures, and r is the discount rate reflecting the time value of money.

The lifecycle-oriented TCO formulation used in the model applies discounted cash flow principles to represent the economic value of future expenditures in present-value terms. The denominator term $(1+r)^2$ represents the discounting factor applied to future operational expenditures occurring at year i. The purpose of this term is to account for the time value of money, based on the principle in techno-economic assessment, financial analysis, and infrastructure investment planning [26].

The rationale behind the denominator is that a monetary amount spent in the future does not have the same economic value as the same amount spent today. Capital available today can potentially be invested elsewhere to generate returns, while future expenditures are economically worth less when converted into present-value terms. Thus, future operational costs must be discounted back to the reference year to compare investment alternatives consistently over long operational periods.

The estimation of discounted lifecycle costing is important because industrial private networks can be expected to be long-term strategic investments whose economic feasibility depends on initial infrastructure expenses and recurring operational and modernization costs over several years. In practical industrial deployments, it is not uncommon that a deployment model with lower initial CAPEX may ultimately become more expensive due to, e.g., increasing operational complexity, subscription-based service costs, or software licensing fees.

The enhanced model separates the overall lifecycle behavior into interacting categories including infrastructure deployment costs, operational costs, network growth dynamics, technology refresh cycles, QoS-driven scaling effects, and deployment-specific specialization factors.

C. Enhanced CAPEX Modeling

The original model represented the CAPEX as a sum of infrastructure-related cost components. The new, enhanced framework still preserves this modular structure with additional functional dependencies and deployment-specific parameters. The total CAPEX is represented now as:

$$\begin{aligned} &CAPEX(t) \\ &= C_{RAN}(t) + C_{CN}(t) + C_{TN}(t) + C_S(t) + C_A(t) \\ &+ C_I(t) + C_{SEC}(t) + C_{EDGE}(t) \end{aligned} \tag{4}$$

The model separates the investment items into radio access network costs (RAN), core network infrastructure (CN), transport network deployment (TN), spectrum-related costs (S), application platforms (A), installation and integration expenses (I), security infrastructure (SEC), and edge computing resources (EDGE). This categorization reflects the fact that industrial private networks can be assumed to become increasingly dependent on distributed cloud-native architectures and edge computing systems in addition to traditional radio infrastructure.

In modern industrial deployments, edge computing and security systems may represent, in fact, a substantial share of overall investment due to the need for low-latency processing, deterministic industrial communications, cybersecurity hardening, and local analytics capabilities.

The model also enables differentiation between fully enterprise-owned deployments, partially shared infrastructures, and outsourced service-based implementations. In practice, these deployment alternatives differ in how investments are distributed between local infrastructure, subscription-based services, and cloud-native operational environments.

D. Radio Access Network Cost Behavior

The RAN remains one of the most significant contributors to the total infrastructure investment of industrial 5G private networks. However, the behavior of the cost of the RAN is not linear in practical deployments. The enhanced model represents the RAN investment as:

$$C_{RAN}(t) = N_{gNB}(t) \cdot P_{gNB} \cdot D_v(N_{gNB}) \cdot S_{QoS} \cdot S_f \quad (5)$$

where the cost depends on the number of deployed radio cells (N_{gNB}), the average unit price of each gNB (P_{gNB}), a nonlinear volume discount function D_v, a QoS multiplier S_{QoS}, and a frequency-dependent deployment coefficient S_f.

The inclusion of the nonlinear volume discount function reflects realistic procurement behavior. In large deployments, vendors may provide reduced relative unit pricing due to economies of scale, framework agreements, software bundling, and shared deployment costs, and this behavior can be modeled using the following equation:

$$D_v(N_{gNB}) = N^{-\alpha} \quad (6)$$

where the coefficient α reflects the magnitude of the volume-based cost reduction. The coefficient α represents the strength of the economies-of-scale effect associated with increasing deployment volume. The purpose of this coefficient is to model the realistic observation that the relative unit cost of infrastructure components decreases as the number of deployed radio nodes increases due to factors such as bulk procurement, shared installation resources, standardized deployment processes, centralized management efficiencies, and vendor discount structures.

In practice, when $\alpha=0$, no volume discount exists and the deployment behaves linearly. When $\alpha>0$, the effective unit cost decreases progressively with deployment size, whereas larger values of α correspond to stronger economies of scale. As an example of this behavior, a small industrial deployment of, say, five indoor gNBs may require largely manual installation, custom integration, and individually licensed software, whereas a deployment involving hundreds of gNBs may benefit from framework agreements, automated provisioning, shared transport infrastructure, optimized logistics, and lower per-unit software licensing costs.

This means that the total RAN cost does not scale linearly with the number of deployed cells, even though the absolute infrastructure investment continues to increase. The nonlinear coefficient is especially relevant in industrial 5G deployments because dense private networks may require large numbers of small cells, cloud-native orchestration enables centralized scaling efficiencies, and industrial campuses may reuse shared infrastructure components such as transport, edge computing, and security systems. This coefficient is thus selected because the use of power-law scaling to model economies of scale is well established in engineering economics and infrastructure cost modeling and can be found in well-established references [27].

The QoS multiplier models the impact of reliability and latency requirements on infrastructure costs. In critical industrial environments, such as automated manufacturing, mining, and port automation, the network may require, e.g., redundant radio coverage, active-active operation, and hardened resilience mechanisms, which means that the respectively implemented infrastructure can become more expensive compared to best-effort connectivity solutions.

In a similar fashion, the frequency bands impact deployment economics. Millimeter-wave deployments may provide very high capacity and low latency but require significantly much more dense radio deployments due to limited propagation characteristics, whereas lower-frequency deployments may reduce the required number of cells but provide lower overall throughput capacity.

E. Core Network and Virtualization Scaling

The economic behavior of the 5GC infrastructure differs from traditional hardware-centric deployments because cloud-native architecture models allow dynamic scaling of NFs. The enhanced model expresses the core network cost as:

$$C_{CORE}(t) = (C_{NF} + C_{LIC}) \cdot U(t)^{\beta} \quad (7)$$

where the cost depends on the infrastructure supporting the network functions (*NF*), software licensing (*LIC*) expenses, and the scaling behavior associated with the number of users *U* (that is, connected devices).

This formulation allows modeling of elastic and non-elastic deployment behaviors. In lightweight, cloud-native deployment scenarios, the scaling exponent β may remain below unity because virtualization enables efficient resource pooling and dynamic orchestration, whereas in highly isolated industrial private networks, the operational complexity and infrastructure cost may increase faster than the number of users or devices because strict reliability and security requirements often require duplicated network functions, geographically or logically separated resources, dedicated security domains, failover mechanisms, and increasingly complex orchestration and lifecycle management systems.

The model also reflects the growing importance of software licensing and orchestration platforms in modern private network deployments. While virtualization may reduce initial hardware investments, software-driven infrastructure can involve recurring operational cost items that evolve dynamically according to traffic growth and computational demand.

F. Transport Network and Edge Computing

Transport infrastructure plays a central role in industrial private networks because ultra-reliable and low-latency communication require deterministic transport characteristics. The transport network cost can be modeled as:

$$C_{TN}(t) = L_{fiber} \cdot P_{fiber} + N_{link} \cdot P_{mw} \quad (8)$$

where the total cost depends on deployed fiber infrastructure and microwave transport links. The first part of the Equation represents the total cost of deployed fiber-optic infrastructure, where L_{fiber} is the total length of the deployed fiber transport network (in m or km), and P_{fiber} is the unit deployment cost of fiber per distance unit, including expenses such as trenching, cabling, connectors, installation labor, permits, and optical transmission equipment.

The second part of the Equation represents the cost of microwave-based transport links, where N_{link} is the number of microwave transport links deployed in the network, and P_{mw} is the average cost per microwave link, including antennas, radios, mounting infrastructure, alignment, and installation. Together, these two terms model the total transport network investment required to interconnect radio access nodes, edge computing platforms, and core network functions using either fiber-based or wireless backhaul infrastructure, or a combination of both.

The model supports different transport architectures including fully fiberized industrial campuses, microwave-based industrial deployments, hybrid transport systems, and shared operator transport infrastructures.

Edge computing infrastructure is represented separately because industrial applications increasingly rely on localized processing for deterministic operation, artificial intelligence, analytics, digital twins, and operational automation. The edge computing investment is represented as:

$$C_{EDGE}(t) = N_{edge} \cdot P_{edge} \cdot S_{latency} \tag{9}$$

where the latency multiplier reflects the increasing complexity of ultra-low-latency processing environments.

G. Dynamic Operational Expenditure

Operational expenditures are time-dependent and exhibit nonlinear growth behavior during the operational lifetime of practical private industrial networks. The yearly operational expenditure can be modeled as:

$$OPEX(t) = O_{energy}(t) + O_{maint}(t) + O_{license}(t) + O_{cloud}(t) + O_{satff}(t) + O_{security}(t) + O_{roaming}(t) \tag{10}$$

This formulation captures the operational impact of energy consumption, maintenance, software licensing, cloud resource utilization, staffing requirements, security operations, and roaming-related expenses. Unlike static models, the enhanced framework assumes that these operational components evolve dynamically over time. As an example, cloud-related costs may increase due to growing AI workloads and expanding edge analytics, while staffing costs may increase due to operational complexity and cybersecurity requirements.

H. Energy Consumption and Traffic Growth

Energy consumption has become an increasingly important economic factor in private industrial networks, particularly as radio densification, edge computing, and AI-driven analytics continue to expand. The model represents energy-related operational cost items in the following way:

$$O_{energy}(t) = E_0 \cdot (1 + g_T)^t \cdot P_e(t) \tag{11}$$

where the operational energy cost depends on the baseline energy consumption (E_0), yearly (t) traffic growth (g_T), and the evolving electricity price P_e. The term $(1+g_T)^t$ represents the compounded growth of network traffic and computational load over time. The reasoning for this term is because industrial private networks can experience progressive expansion, and the formulation reflects the reality that industrial network traffic rarely remains constant during the lifecycle of deployment.

As enterprises continue their digital transformation, the number of connected devices, autonomous systems, sensors, and edge applications typically increases significantly over time. Furthermore, energy consumption does not scale linearly because increased traffic often requires additional radio processing, computational resources, and cooling capacity. For example, if yearly traffic growth is 20% (i.e., g_T = 0.20), then after the first year, the term results in $(1+0.20)^1=1.20$, and after the third year $(1+0.20)^3=1.728$, meaning the traffic-related energy demand has increased by approximately 72.8% compared to the initial deployment year.

I. Maintenance Growth and Technology Refresh Cycles

Industrial network infrastructures are subject to technology evolution and aging effects throughout their operational lifetime. The respective maintenance cost can be represented as:

$$O_{maint}(t) = M_0 \cdot (1 + \gamma t) \tag{12}$$

where the M_0 is the baseline yearly maintenance cost at the beginning of operation, and coefficient γ models the increasing operational complexity and maintenance burden associated with aging infrastructure, and t is the operational time in years.

In addition to gradual maintenance escalation, industrial private networks periodically require modernization investment related to, e.g., hardware replacement, migration to newer 3GPP releases, cybersecurity upgrades, AI-assisted optimization platforms, and edge computing expansion. Equation (12) thus assumes that maintenance expenses increase progressively due to factors such as, hardware aging, increasing failure probability, software patching requirements, and other issues that increase over time.

It should be noted that the expression is linear with time because many maintenance-related operational costs tend to increase approximately gradually during the normal operational lifetime before major modernization or replacement occurs.

As an example, if the baseline maintenance cost is USD 100,000/year, and the aging coefficient is γ=0.08, then after the first year, the term results in $(1+0.08\cdot 1)=1.08$, and after the fifth year, it is $(1+0.08\cdot 5)=1.40$ meaning the yearly maintenance cost has increased by 40% compared to the initial operational year.

Thus, the term models the lifecycle behavior in which older industrial network infrastructure generally need progressively greater operational effort and maintenance expenditure over time. The model captures these reinvestment events using discrete refresh cycles:

$$C_{refresh}(t) = \begin{cases} R_f, & t \in T_r \\ 0, & otherwise \end{cases} \tag{13}$$

This reflects the realistic lifecycle behavior of industrial deployments where significant reinvestments may occur every several years.

J. Weighted Multi-Criteria Suitability Assessment

It can be reasoned that pure cost optimization alone is insufficient for industrial NPN deployment decisions because many industrial environments prioritize factors such as reliability, security, isolation, and operational control. For this reason, the enhanced framework introduces weighted multi-criteria assessment. The overall suitability score is:

$$S = \sum_{i=1}^{n} w_i \cdot p_i \quad (14)$$

where each criterion has relative importance weight and a normalized performance score. The evaluated criteria may include, e.g., latency, reliability, security, isolation, scalability, mobility, roaming support, energy efficiency, operational flexibility, and regulatory compliance.

In this equation, S represents the total suitability score of the deployment scenario, w_i represents the importance weight assigned to a specific evaluation criterion, p_i represents the normalized performance score of that criterion, and n is the total number of evaluated criteria.

The principle of the equation is that each of the selected criterion contributes to the final suitability score according to how important the criterion is for the enterprise, and how well the evaluated deployment fulfills that requirement. Typical criteria may include latency, reliability, security, and scalability, among other selected criteria.

This approach allows comparison of deployment scenarios from a broader industrial perspective. As an example, SNPN deployment may provide superior isolation and security, whereas a network slicing solution may provide lower initial investment and better scalability. The weighting mechanism enables the model to adapt to different industrial verticals whose priorities may differ significantly depending on the operational environment.

TABLE I presents an example of the weighting, assuming an industrial enterprise, which evaluates a private network deployment using three criteria.

TABLE I. EXAMPLE OF WEIGHTING

Criterion	Weight w_i	Performance p_i
Security	0.5	0.9
Latency	0.5	0.8
Cost Efficiency	0.2	0.6

The resulting suitability score becomes $S = (0.5 \times 0.9) + (0.3 \times 0.8) + 0.2 \times 0.6) = 0.45 + 0.24 + 0.12 = 0.81$. Thus, the deployment of this example has a suitability score of 0.81 on a normalized scale between 0 and 1. This behavior allows different industrial verticals to prioritize their most important requirements. For example, a factory automation environment may assign high weight to latency and reliability, whereas an energy utility may prioritize security and resilience, and a logistics deployment may emphasize scalability and mobility.

K. Dynamic Evolution of Enterprise Requirements

The enhanced model assumes that industrial digitalization evolves continuously during the operational lifetime of the network. The number of connected devices is modeled as:

$$N_d(t) = N_0 \cdot e^{\lambda t} \quad (15)$$

where the exponential growth coefficient reflects the pace of industrial automation and digital transformation. This approach reflects realistic industrial evolution trends involving increasing sensor density, autonomous robotics, AI-driven analytics, digital twins, and machine-to-machine communication. As deployment evolves, the respectively increased traffic volume, demand for computing, orchestration complexity, and exposure to cybersecurity create secondary impacts throughout the techno-economic model.

In this Equation, $N_d(t)$ is the number of connected devices at time t, N_0 is the initial number of devices, λ is the digitalization growth coefficient, t is time in years, and e is the base of the natural logarithm. The exponential term reflects that industrial device growth can be assumed to accelerate over time rather than increase linearly. As enterprises adopt more automation, AI-assisted monitoring, robotics, digital twins, and Industrial IoT services, the number of connected endpoints may expand rapidly.

As an example, let us assume that an industrial campus initially deploys 1,000 connected devices in such a way that the yearly digitalization growth coefficient is λ=0.18 and the enterprise expands automation continuously. The device growth becomes:

$$N_d(0) = 1000 \cdot e^{0.180} = 1{,}000$$

$$N_d(3) = 1000 \cdot e^{0.180 \cdot 3} = 1{,}716$$

$$N_d(5) = 1000 \cdot e^{0.180 \cdot 5} = 2{,}460$$

As can be seen, in this scenario, the deployment has grown to approximately 1,716 devices after 3 years, and after 5 years, the deployment reaches approximately 2,460 devices.

It can be assumed that this type of behavior is realistic in industrial environments where additional sensors are gradually deployed, autonomous systems increase, AI-driven analytics expand, production monitoring becomes more granular, and operational systems become increasingly interconnected.

L. Practical Implementation in Excel

The developed Excel-based implementation enables practical evaluation of industrial private network deployment scenarios by allowing users to modify parameter values dynamically and visualize the resulting lifecycle cost behavior. The implementation includes configurable input parameters for deployment architecture, number of users and devices, traffic growth, SLA level, gNB pricing, spectrum costs, cloud elasticity, maintenance escalation, technology refresh cycles, and discount rate.

The resulting calculations generate yearly CAPEX, OPEX, cumulative lifecycle cost, and discounted TCO curves based on the input parameters. This implementation enables comparative evaluation of deployment alternatives and supports sensitivity analysis of key techno-economic variables under realistic industrial deployment assumptions.

It should be noted that the most realistic analysis requires valid commercial values of devices and solutions. Nevertheless, based on a high-level estimate of the input values can provide useful examples of the output. Figure 7 presents such a theoretic assessment for cumulative discounted TCO, and Figure 8 for annual OPEX. The presented curves are normalized setting the SNPN Discounted TCO as the common reference (value 1). In these cases, the basic assumptions are the following: discount rate 8.0% annual; inflation 2.5% annual, device base 50 in year 0, device annual growth 0.2, traffic base per device 0.5, traffic annual growth 0.12. It should be noted that the assessment uses assumptions for the base unit CAPEX and annual OPEX values through best effort estimate covering user devices, gNB units, transmission, spectrum, core network (NFs), applications and services, roaming and interconnect, installation, as well as maintenance and variable cost items.

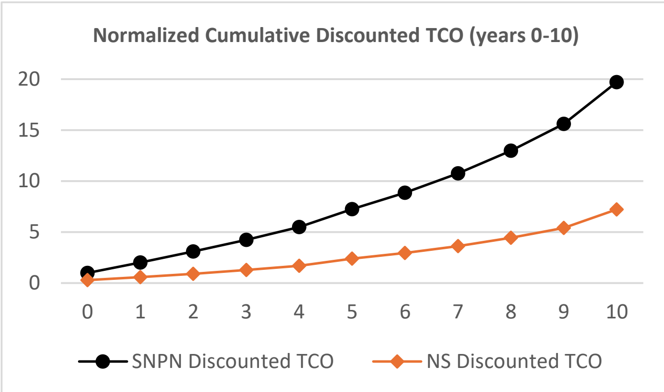

Figure 7. Example of the evolved model's outcome comparing SNPN (reference=1) and NS deployment TCO over 10 years

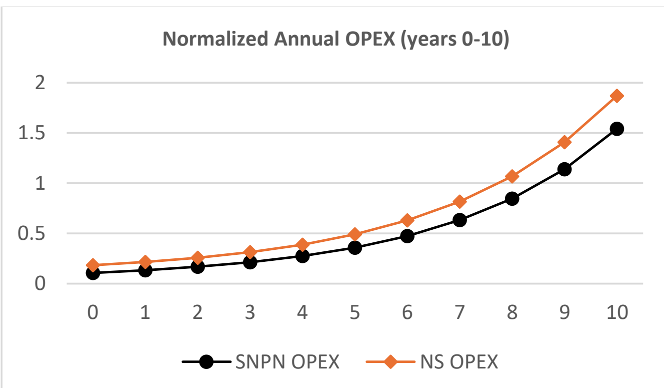

Figure 8. Example of the evolved model's outcome comparing SNPN and NS deployment Annual OPEX over 10 years; the presented values are normalized (the reference is the initial SNPN TCO)

As can be seen from Figure 7 and Figure 8, in this specific scenario, the TCO of SNPN deployment increases faster over time than deploying NS. Nevertheless, the OPEX of the NS deployment model grows faster than the SNPN deployment with the selected parameter values. In this scenario, the NS deployment remains less expensive throughout the lifecycle, but it is possible that the lowest initial investment in some other deployment scenario may turn out to be more expensive over time.

VIII. Summary and Future Work Opportunities

An NPN can serve many verticals and their use cases in a more optimal way than PLMN may be able to, to comply with special requirements for, e.g., hardened security by isolation, or high flexibility for network settings adjustment, for which the pros and cons of enterprise-owned vs. operators' components need to be evaluated. There are variety of deployment and ownership models, so the assessment of the scenarios prior to business decisions for the most feasible deployment and ownership model is beneficial.

The presented method provides the enterprise with a tool to estimate the cost difference of deployment models of interest over time and to assess whether certain variants are acceptable for deployment regardless of projected, potentially higher cost to balance the key requirements of the enterprise considering, e.g., the level of independent network control and security.

This paper presents means for the assessment of the techno-economic feasibility of NPN models and examples of the applicability through base and evolved variants of the models. For the model to perform adequately, insights into realistic OPEX and CAPEX values of the parameters are important. Thus, feedback from NPN proof of concepts and trials serve to calibrate this modeling and helps identify and focus on the evaluation of the most essential cost items.

Private networks are becoming reality, and they provide a functional base for many verticals and use cases to cope with special requirements. Stakeholders considering deployment and use of private networks benefit from adequate platform. As this study shows, even a relatively simple model can support the ecosystem to better understand the differences of the business cases related to a variety of private network models.

Abbreviations

3GPP, 3rd Generation Partnership Project
5GC, 5G Core
5GS, 5G System
ACIA, Alliance for Connected Industries and Automation
APN, Access Point Name
CAG, Closed Access Group
CAPEX, Capital Expenditure
CN, Core Network
CP, Control Plane
DECOR, Dedicated Core Network
gNB, Next Generation NodeB
GSMA, GSM Association
GWCN, Gateway Core Network
ID, Identifier
IIoT, Industrial Internet of Things
IoT, Internet of Things
LAN, Local Area Network
LBS, Location Based Service
LBO, Local Breakout
LPWAN, Low Power Wide Area Network
LWA, LTE-WLAN Aggregation
MBB, Mobile Broadband
MEC, Multi-access Edge Cloud
MNO, Mobile Network Operator
MOCN, Multi-Operator Core Network
N3IWF, Non-3GPP Interworking Function
NAS, Non-Access Stratum
NF, Network Function
NID, Network Identifier
NPN, Non-Public Network
NS, Network Slice
NSP, Network Slice Provider
OPEX, Operational Expenditure
OT, Operational Technology
OTT, Over the Top
PLMN, Public Land Mobile Network
PNI, Public Network Integrated

QoS, Quality of Service
RAN, Radio Access Network
RG, Residential Gateway
SA, Standalone
SBA, Service Based Architecture
SBI, System Broadcast Information
SLA, Service Level Assurance
SNPN, Standalone NPN
SUPI, Subscription Permanent Identifier
TCO, Total Cost of Ownership
TN, Trasport Network
TS, Technical Specification
TSN, Time Sensitive Networking
UDM, Unified Data Management
UE, User Equipment
UPF, User Plane Function
URRLC, Ultra-Reliable Low-Latency Communications
WLAN, Wireless LAN

References

[1] J. T. J. Penttinen, "On Techno-Economic Optimization of Non-Public Networks for Industrial 5G Applications," in *The Nineteenth Advanced International Conference on Telecommunications (AICT), June 26-30, 2023*, Nice, France, 2023.

[2] GSMA, "Internet of Things," GSMA, 15 December 2020. [Online]. Available: https://www.gsma.com/iot/manufacturing/private-networks/private-networks/. [Accessed 18 May 2026].

[3] 3GPP, "TR 23.700-20: Study on enhanced support of Industrial Internet of Things (IIoT) in the 5G System (5GS)," 3GPP, 2021.

[4] 3GPP, "TS 23.502: Procedures for the 5G System (5GS)," 3GPP, 2026.

[5] 3GPP, "3GPP TS 23.251 Network Sharing; Architecture and functional description (Release 17)," 3GPP, March 2022.

[6] 3GPP, "TS 22.104: Service requirements for cyber-physical control applications in vertical domains," 3GPP, 2024.

[7] 3GPP, "TS 23.501: System architecture for the 5G System (5GS), Stage 2," 3GPP, 2026.

[8] D. Kim, "Non-Public Networks (NPN)," 3GPP, 15 December 2022. [Online]. Available: https://www.3gpp.org/technologies/npn. [Accessed 18 May 2026].

[9] 5G-ACIA, "NPNs for Industrial Scenarios," 5G-ACIA, 20 March 2024. [Online]. Available: https://5g-acia.org/whitepapers/npns-for-industrial-scenarios/. [Accessed 18 May 2026].

[10] 5GACIA, "5G Non-Public Networks for Industrial Scenarios," 5GACIA, July 2019.

[11] GSMA, "5G industry campus network deployment guideline," 10 November 2020. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.123-v1.0.pdf. [Accessed 18 May 2026].

[12] D. Chandramouli, "5G for Industry 4.0," 13 May 2020. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/tsn-v-lan. [Accessed 18 May 2026].

[13] H. J. Son, "7 Deployment Scenarios of Private 5G Networks," NetManias, 21 October 2019. [Online]. Available: https://www.netmanias.com/en/?m=view&id=blog&no=14500. [Accessed 18 May 2026].

[14] 3GPP, "TS 24.519: Time-Sensitive Networking (TSN) Application Function (AF) to Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NW-TT) protocol aspects," 3GPP, 2021.

[15] 5G-ACIA, "Integration of 5G with Time-Sensitive Networking for Industrial Communications," 5G-ACIA, 2021. [Online]. Available: https://5g-acia.org/whitepapers/integration-of-5g-with-time-sensitive-networking-for-industrial-communications/. [Accessed 18 May 2026].

[16] Syniverse, "Managing the Complexities of Connectivity for Enterprises and Operators," Syniverse, 24 March 2022. [Online]. Available: https://www.syniverse.com/blog/connectivity/managing-the-complexities-of-connectivity-for-enterprises-and-operators/. [Accessed 18 May 2026].

[17] M. Dryjański, "Private 5G Networks – Technology, Architecture, and Deployment," Rimedo Labs, 4 January 2021. [Online]. Available: https://rimedolabs.com/blog/private-5g-networks-technology-architecture-and-deployment/. [Accessed 18 May 2026].

[18] Samsung, "Technical whitepaper: network slicing," Samsung, 2020.

[19] GSMA, "Network Slicing: North America's Perspective V1.0," GSMA, 3 August 2021. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.130-White-Paper-Network-Slicing-NA-Perspective-1.pdf. [Accessed 18 May 2026].

[20] GSMA, "Generic Network Slice Template V 7.0," GSMA, 17 June 2022. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v7.0.pdf. [Accessed 18 May 2026].

[21] GSMA, "Mobile economy report 2026," GSMA, February 2026. [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2026/02/The-Mobile-Economy-2026.pdf. [Accessed 18 May 2026].

[22] M. Shelton, "Open RAN Terminology," Parallel Wireless, 20 April 2020. [Online]. Available: https://www.parallelwireless.com/open-ran-terminology-understanding-the-difference-between-open-ran-openran-oran-and-more/. [Accessed 18 May 2026].

[23] O-RAN Alliance, "O-RAN: Towards an Open and Smart RAN," O-RAN Alliance, October 2018.

[24] Intel, "LTE-WLAN Aggregation (LWA): Benefits and Deployment Considerations," Intel, 2016. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/lte-wlan-aggregation-deployment-paper.pdf. [Accessed 18 May 2026].

[25] Ericsson, "Fixed Wireless Access handbook 2023 edition," 2022. [Online]. Available: https://www.ericsson.com/en/fixed-wireless-access. [Accessed 18 May 2026].

[26] W. Sullivan, E. Wicks and C. Koelling, Engineering Economy, 16th Edition, Pearson, 2014.

[27] H. Lee and C. Tang, "Modeling the Costs and Benefits of Delayed Product Differentiation," *Management Science,* vol. 43, no. 1, pp. 40-53, 1997.