Walia, Jaspreet; Hämmäinen, Heikki; Kilkki, Matti; Yrjölä, Seppo

5G network slicing strategies for a smart factory

Published in:
Computers in Industry

DOI:
10.1016/j.compind.2019.07.006

Published: 06/08/2019

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Walia, J., Hämmäinen, H., Kilkki, M., & Yrjölä, S. (2019). 5G network slicing strategies for a smart factory. *Computers in Industry*, *111*, 108-120. https://doi.org/10.1016/j.compind.2019.07.006

5G Network Slicing Strategies for a Smart Factory

Jaspreet Singh Walia[a], Heikki Hämmäinen[a], Kalevi Kilkki[a], Seppo Yrjölä[b]

[a] Department of Communications and Networking, Aalto University, Espoo, Finland, firstname.lastname@aalto.fi

[b] Nokia, Oulu, Finland, seppo.yrjola@nokia.com

Abstract Factories become increasingly dependent on network connectivity. The next generation of mobile communications, 5G, will enable better flexibility and service quality through network slicing. Network slicing is a means of creating logically separated use case specific virtual networks over the same physical network. However, there is a lack of techno-economic research related to management of network slices. Network slice management needs to take into account the multiple network domains, business actors and value networks involved in a vertical such as smart factories. The key for network slices to succeed where other resource reservation and quality of service technologies have previously failed is with well-defined and feasible management models and strategies. In this paper, we focus on network slice management and strategies for a smart factory. We study a state-of-the-art electronics assembly factory in Finland to find existing need for network slicing and missing capabilities to support smart factory use cases. Next, we define use case specific network slices and develop a network slice management model based on 5G specifications. The model allows for distribution of network functions between business actors over multiple network domains. The value network analysis method is utilized to develop alternative configurations that constitute the network slicing strategies facilitated by the model. Factory managers can decide on the most suitable strategy based on traditional factors such as make or buy, security, and level of automation. The strategies also differ in their technical applicability to different use cases. A feasibility study reveals the strategic differences from factory, local network operator and large mobile network operator perspectives.

Keywords 5G, micro-operator, Industry 4.0, network slicing, smart factory, value network

Corresponding Author

Jaspreet Singh Walia, jaspreet.walia@aalto.fi

Department of Communications and Networking

Aalto University

Konemiehentie 2, Espoo, Finland

1 Introduction

Virtualization, especially in local networks, has been extensively utilized in businesses due to the existence of multiple user and application groups with different requirements from the network. The need for virtual isolation in factory networks becomes evident due to different traffic types, volumes and patterns that arise from different sources accessing the same network. To this end, Virtual Local Area Networks (VLANs) are implemented to create multiple isolated virtual networks on the same infrastructure [1]. Further, different use cases and applications will require different network resources. However, networks typically operate with best effort service, in which all traffic shares the same network, and there is no prioritization or resource allocation per use case. Several procedures exist for implementing Quality of Service (QoS), majorly involving Differentiated Services (DiffServ) and Integrated Services (IntServ) architectures. These procedures promise better QoS but have been complicated and costly to implement [2]. As a result, to avoid complex implementations for QoS, network providers often overprovision the network to be able to provide sufficiently high quality services based on peak traffic estimates. This can be suitable for predictable networks but as the number of applications and users increases, overprovisioned networks no longer stay overprovisioned. Thus, a mechanism that is more scalable, and is easy to implement and manage becomes necessary. Further, due to limitations in current wireless networks, factory automation is limited to closed local wired networks.

IEEE based wireless networks such as Wi-Fi, have their limitations concerning mobile devices and machinery that require mobility, high reliability and low latency communications. 5G is expected to meet these communication requirements. Where the wide area services are predominantly served by traditional Mobile Network Operators (MNOs), bringing 5G inside a factory and providing factory specific services, implies the requirement of a local 5G network operator, such as Micro-Operator (uO) [3], [4]. A uO is a local 5G network operator (small entrant or existing multi-national service provider), taking up local network operation role, thus being responsible for deployment and management of the network infrastructure and provisioning of use case specific services. Additionally, an existing actor such as a service provider, machine vendor, network equipment vendor, venue owner or the factory itself can also take up the local network operation role.

The local 5G network will operate either over locally licensed, shared or leased spectrum. The 3.5 GHz spectrum band, which is suitable for both small cell and macro cell deployments, has been auctioned to existing MNOs in Finland [5]. The 28 GHz band is expected to be auctioned in the future to fulfill additional local capacity requirements in high-density areas and indoor hotspots [6], [7]. Thus, a local network operator can currently utilize 3.5 GHz band by sharing or leasing from the MNOs and in the future utilize the 28 GHz locally licensed band.

The future smart factory environment will comprise of a myriad of services accessing the same network with different requirements. For example, voice and video services require continuity, manufacturing processes and Augmented Reality (AR) services require higher reliability and low latencies, and Wireless Sensor Networks (WSN) services require higher connection densities with sporadic transmissions. Many more use cases and applications will be incorporated inside a factory to enhance both technical and business efficiencies [8]. Through virtualization in the 5G architecture, use case specific services can be provided through respective network slices [9]. Network slices can exist in multiple network domains managed by one or multiple network operators. With multiple operators for catering to local and wide area requirements, there is a need for an efficient network slice management model. These multiple operators will be able to exercise different levels of exposure of network resources with the factory and between themselves. Such multi-operator, multi-level interaction will lead to different network slicing strategies, with each of these being feasible for supporting a certain type of use cases.

The paper addresses two main research questions:

- What is the network slice management model for a smart factory in a multi-operator environment?
- What are the different network slicing strategies and their feasibility for a smart factory?

The paper is structured as follows. Chapter 2 investigates the current virtualization in factory networks, candidate slices, missing technology capabilities and business limitations by studying a state-of-the-art electronics assembly factory located in Finland. Chapter 3 defines different smart factory use case groups based on communications service requirements and service flows over different network domains. Chapter 4 studies network slicing architecture based on 5G specifications and related work. Chapter 5 defines end-to-end network slices and develops a network slice management model to support smart factory use cases. Further, chapter 6 explores the possible options for interworking between local and wide area networks and develops three network slicing strategies using alternative value network configurations. Chapter 7 discusses the feasibility and applicability of different strategies to studied use cases, followed by conclusions in chapter 8.

2 State of the Art: Case Finland

For transitioning to smart factories, it is crucial to study the current network in a state of the art electronics assembly factory in Finland, hereinafter referred to as the 'case factory'. The case factory helps to formulate the existing use cases as slice candidates and find missing capabilities required for the development of smart factories.

In the case factory network, VLANs are utilized for virtualization and creating isolated logical networks on the same physical network. A VLAN identifier is used to distinguish between the different VLANs. It is possible to isolate different applications and user groups as separate VLANs so they do not interfere with each other's traffic and performance. The network gets shared in a dedicated manner such that some ports along the routing can be assigned to a particular VLAN. There is typically no dynamic sharing between VLANs. There is no individual session reservations and the dedicated resources are usually allocated based on traffic patterns and peak traffic estimates. However, VLANs can be complemented with some QoS technologies such as IntServ and DiffServ.

The IntServ architecture specifies guaranteed QoS requested by applications using the Resource Reservation Protocol (RSVP) to reserve resources from a network [10]. This requires all the routers to implement IntServ and each application requests reservations individually. This architecture is suitable for small networks but lacks scalability due to the fact that it cannot aggregate individual reserved sessions into a common class [11]. This can be solved with a multi-layer approach by defining some aggregation regions and assigning aggregator and de-aggregator roles to ingress and egress routers. The complexity of implementation and scalability to large service provider networks has been an obstacle for IntServ.

The DiffServ architecture specifies prioritized QoS by marking packets with a 6 bit Differentiated Services Code Point (DSCP) according to the type of service [12]. Applications or users send the packets without reserving any resources and the network classifies them into service classes. This way only aggregated flows are considered without any knowledge of individual connections [2]. DiffServ implementations have been utilized in VLANs to prioritize the packet flow on an aggregate level. As there is no explicit individual service level defined, DiffServ resembles best effort but with prioritization.

The existing major QoS mechanisms lack scalability and flexibility and are complex and costly to implement. As a result, these are often skipped and peak traffic estimates are used for overprovisioning, and a best effort service is implemented. Overprovisioning is suitable for predictable traffic networks but as the number of user devices increases and new applications are added, overprovisioned networks cannot stay overprovisioned, and further capacity increments can be costly and inefficient.

The case factory network follows a flat backbone network, using a single switch to connect multiple network areas to the company's private cloud. Interior gateway protocol such as Open Shortest Path First (OSPF) is utilized in the local area network. The different departments in the internal network are separated from the outside network and are connected to the company's private cloud through a firewall. The devices and traffic in each of these network areas are logically isolated from each other for independent management. Within each network area there exist multiple VLANs to connect different set of users, devices and applications. In this study, we focus on the factory floor part of the network. The factory floor VLANs are secured with a firewall and connected through two switches that also act as routers implemented in an active-passive configuration for fault tolerance (added redundancy) with one switch active at a time. Isolation and security of factory critical data and reliability of communication are currently of the utmost importance for factory networks. The factory VLANs can communicate with the company's private cloud but to eliminate cybersecurity concerns there is no connection with the public/wide area network or third parties.

The factory floor network runs VLANs to separate five broad use cases and applications namely, test network, logistics management, personnel handheld devices, multiple production lines and multiple product testing lines. Currently, these use cases are separated for independent management and dimensioned for the number of devices to be connected. As the use cases evolve, their communication service requirements become more specific and as more use cases are added there will be more diverse needs to be satisfied. These broad use cases being natural candidates for network slices, can be grouped with specific smart factory use cases depending on their communication service requirements.

Apart from virtualization, factories usually employ a strategy for deployment and management of networks based on the following factors:

- Make or buy (setting up or outsourcing): A factory can decide either to make, that is, deploy and manage the network themselves or to buy services from a third party. This decision is based on technical and investment capabilities.
- Security (Physical and cyber): A factory can decide to isolate some or all processes and data due to physical and cyber security reasons. This directly effects deployment and management of network infrastructure, virtualization and involved business actors.
- Level of Automation: The current level of automation and future approach to automation dictates the type of communication technology and equipment to be used.

From a strategy point of view, the Case factory has an isolated network to eliminate security concerns and outsources its connectivity requirements and management to an Information Technology (IT) company. The Case factory is depending on future wireless networks, such as 5G to enhance the level of automation. The factory has multiple departments and user groups such as, factory floor, corporate office, and IT management. The case factory network has some missing capabilities and business limitations to support smart factory use cases:

- Reliable wireless infrastructure: Critical and real-time applications require high reliability and have been limited to closed local wired networks. This also limits the possibilities in mobility, scalability and flexibility.
- Service quality: QoS mechanisms are usually skipped to reduce complexity, costs of implementation and management. This limits the flexibility in use case specific services.
- Future scalability: Factory networks have been quite predictable in the past and overprovisioning or peak traffic based provisioning is typically cheaper and still effective to avoid congestion and provide high quality. Addition of new use cases and possible unpredictable traffic scenarios require significant updating of the network.
- Support for diverse device types and traffic: Massive Internet of Things (mIoT) will produce microburst type of data from a massive number of sources. Video analytics/AR will require high bandwidths and high reliability. Best effort service is not enough to support diverse requirements.
- Limited mobility: Mobility has been quite limited in the past and needs better management. Local wired networks limit physical mobility and current wireless networks provide low reliability for handovers between access points.
- Limited business opportunities: There are no Virtual Private Networks (VPNs) for third-party involvement and thus limiting the possibility for remote maintenance, monitoring by machine vendors, leased factory premises and factory within factory opportunities.

3 Smart Factory

Smart factory, Industry 4.0 and factories of the future commonly refer to the same concept and are a crucial building block for innovation and the upcoming fourth industrial revolution. The machines and sensor devices will produce vast amounts of data which can be used to improve the efficiency of factory processes with system-wide feedback and coordination [13]. Additionally, a hierarchical architecture with an emphasis on multi-field cooperation to enable virtualization and configurability in smart factories is needed [14]. Thus, smart factory concept is a culmination of manufacturing technologies, Internet of Things (IoT), virtualization, cloud computing, big data and context-aware services to enhance factory processes. The main driving force behind a smart factory is the added value through flexible automation and improvement in the efficiency of factory processes.

3.1 Use Cases in a Smart Factory

3GPP has categorized factory use cases into five broad categories; Factory Automation, Process Automation, Human-Machine Interaction (HMI) and Production IT, Logistics and Warehousing, and Monitoring and Maintenance [15]. These categories are broken down into use case specific communication requirements and service flows in a factory environment.

3.1.1 Communication Service Requirements

There exist variations in use case specific requirements pointing to the need for separate logical networks for independent services, management and scalability. The communication requirements for smart factory use cases [8], [15], [16] are provided in Table 1. These use cases are grouped into Use Case Groups (UCGs) depending on the operation area and requirement of wide area network. The existing VLANs in the case factory can be grouped into UCG1 that does not require wide area network. Each UCG requires defining a slice type in terms of network functions placement in different network domains.

Table 1 Communications Requirements for Smart Factory Use Cases

Use Case	Latency	Data Volume	Data Rate	Density	Mobility	Operation Area	Wide Area Network	Current Solutions	UCG
Motion Control	<1 ms	Less than KB	Low	High	Low or stationary	Indoor	Not required	Industrial Ethernet, VLANs	**UCG1**
Control to Control	<10 ms	Less than KB	Low	High	Low or stationary	Indoor	Not required	Industrial Ethernet, VLANs	
Augmented Reality, Human Machine Interaction	<50 ms	High	High	Low	<10 Km/h	Indoor	Not required unless remote support	Handheld devices operated over Wi-Fi, Industrial Ethernet, VLANs (Low Reliability). AR not available.	
Mobile Robots	Variable, <1 ms, <500 ms	Variable	>10 Mbps	Low	<20 m/s	Indoor and outdoor	May be required	Not available	**UCG2**
Massive Wireless Sensor Networks	Condition monitoring (<10 ms), Interval, event based (<1 s)	Less than KB	Low	High	Low or stationary	Indoor and outdoor	May be required	Industrial Ethernet, VLANs	
Process Automation	<10 ms	Less than KB	Low	High	Low or stationary, mobile (30 Km/h)	Indoor and onsite outdoor	Not required (indoor), may be required (monitoring and management)	Industrial Ethernet, VLANs	
Remote Access and maintenance	Typically, Non-real time	Less than KB	Low	Peer to peer, Machine to machine	Low or Stationary	Indoor and multisite	Required	Typically not implemented but possible on small scale with Industrial Ethernet and VPNs	**UCG3**

Inbound logistics	Vehicle(<10 ms)
	Inventory(<1 s)
		Less than KB	Low	Medium	<30 Km/h	Indoor and outdoor	Required	Long Range (LoRa), Industrial Ethernet, VLANs (Low Reliability)	

Wide area fleet maintenance	Relaxed (~30 min delay upload)	Less than KB	Low	Medium	Variable	Outdoor	Required	LoRa	

Use Case	Latency	Data Volume	Data Rate	Density	Mobility	Operation Area	Wide Area Network	Current Solutions	UCG
Factory within Factory (modular factories)	Use cases involved, response(<1s), Configuration/ reconfiguration (<3 s)	Depends on involved use cases				Indoor and outdoor	Required	Not available	

3.1.2 Communication Service Flows

The provisioning of the network slices for each use case depends not only on the service requirements but also on the communication service flow and interactions between devices, local network, wide area network and cloud as described further.

UCG1:

Controllers (motion control, control to control) in factory send both cyclic and non-cyclic data, and can have real time or non-real time requirements for closed-loop control applications. These are currently handled by wired Industrial Ethernet technologies, such as Process Field Net (PROFINET), Controller Area Network (CAN), and separately operated using VLANs. Abrasion between connectors for moving parts, addition of new sensors, actuators and controllers can be made simple with wireless communication. 5G provides a promising approach but still must support integration with existing systems. Motion control and control-to-control communications are handled indoors and do not require wide area network access and in fact, it is critical that they are isolated from wide area networks.

Human-Machine Interaction involves factory personnel using mobile handheld devices and other stationary computer panels to manage processes and production flows. *Augmented Reality* devices can also be used to visualize such data as an overlay on personnel's AR glasses point of view. HMI, and augmented reality will not require interaction with wide area network unless remote support is needed.

UCG2:

Mobile Robots are programmable machines for multiple operations and can be remotely controlled or can be Automated Guided Vehicles (AGV). Mobile robots can communicate data for processes, video, collision avoidance and communicate with other mobile robots and machinery. There can be a central guidance system located inside a factory to monitor and guide the robots. Mobile robots can be traveling indoors or outdoors within factory premises and may require wide area network access.

Massive WSN deploy a huge number of sensors which are typically wired or wirelessly connected to local sensor gateways which are further connected to the local server or edge cloud for data collection and analysis. These can be deployed indoors as well as outdoors and may require interaction with wide area network.

Process automation for continuous measurements, decisions and inventory management will not require interaction with wide area network unless remote management is required.

UCG3:

Remote Access and Maintenance use case is currently absent as factory networks are isolated due to security concerns. It can be useful to remotely access machine data either locally, between multiple sites or from a faraway location to provide assistance. Event-driven data collected on the state of machines can be used for predictive maintenance to alarm personnel of a possible maintenance requirement. Possible security concerns for factory's vulnerable data and machines must be handled with only authorizing selected remote personnel and devices to connect to the factory network. This use case will require wide area network access when remote faraway access is required.

Inbound Logistics and *Wide Area Fleet Maintenance* will require wide area network access. Some logistics device might require dual subscription for accessing wide area and local network as logistics vehicles will be roaming from one factory site to another picking up and delivering goods. For example, a User Equipment (UE) in a delivery truck will establish a connection with the visited factory's local network while still being connected to the home factory over the wide area network.

Factory within Factory (FwF) involves modular factory operation and will require at least remote request, configuration and reconfiguration and thus require wide area network access over a secure network slice. Factory within factory use case implies modularization through virtualization of factory facilities, to virtually separate multiple tenants, who can then utilize and operate the same physical factory site.

3.2 Challenges to Future Network Operation

The service requirements and service flows in smart factory use cases pose some challenges to future network operation:

- Integration and Compatibility: The future technologies need to be compatible with existing infrastructure and sensor systems.
- Roaming and Dual subscription: Connected mobile robots, vehicles and other devices will require roaming and dual subscription to be supported by different networks in visited and home factory scenario.
- Multi-tenancy: Future networks will be required to support multiple tenants in the smart factory ecosystem.
- Lifetime: The industrial machines can have lifetimes of 10-20 years; thus, longevity, availability, flexibility and scalability of future networks will be very important.
- Security and Interoperability: As new use cases are added, the isolated factory networks should be updated with support for interoperability with wide area networks and roaming scenarios. Moreover, some critical use cases that require isolated operation must stay isolated.
- Diverse use cases: The use cases will require seamless services over different sized service areas (indoor, outdoor, wide area) and different communication requirements for different use cases within factory.
- Isolation: Physical or virtual separation is required for isolation and independent management of critical, non-critical and delay sensitive data.

The integration and compatibility with current networks will depend on the backward compatibility of the 5G network equipment, and the lifetime of networks depends on network equipment vendors and the deployment by operators, the other challenges can be met with well-defined network slices. To this end, network slicing for a smart factory will require management over multiple network domains and multiple operators to flexibly deploy future networks, implement isolation, security and establish interoperability between local and wide area networks. Network slicing not only provides a better means of network management but, also a means to expand business opportunities with different network slice configurations enabling new business models [17]. Justifiable business needs for network slices exist in a smart factory, and a network slice management model is needed based on the 5G specifications.

4 Specifications and related work

The ongoing research in smart factories has emphasized on the importance of upcoming enhancements in communication technologies [18], [19]. Thus, the dependability of communication technology is crucial for smart factory use cases [15]. In addition, the myriad of use cases with different communication service requirements, that will exist in the future lay the foundational need for virtualization, isolation and independent management of use cases through network slicing.

4.1 5G Network Slicing

Several standards organizations and other commercial organizations have contributed towards network slicing. NGMN proposed a three-layer model for network slices, namely the service instance layer, the network slice instance layer and the resources layer, and also proposes that network slices can be built from resources belonging to different domains [20], [21]. The work by ETSI on Network Functions Virtualization (NFV) and its relation to network slices has shown that network slice instances can contain one or more network slice subnet instances [22]. 3GPP is responsible for 5G architecture specifications and has defined three types of network slices; enhanced mobile broadband, mIoT and ultra-reliable low latency communications [9]. 3GPP has also defined the required network functions for slice selection and management.

In 3GPP defined 5G architecture [9], the UE connects to the Access Network (AN), which establishes a connection with the Access and Mobility Management Function (AMF) in the Core Network (CN), responsible for access control and mobility management. Then the session management and User Plane Function (UPF) selection is accomplished by the Session Management Function (SMF). UPF management in 5G is similar to user plane management in Control and User Plane Separation (CUPS) in 4G Evolved Packet Core (EPC) [23]. With the flexibility offered by 5G architecture, multiple SMFs and UPFs can be selected for a UE with multiple sessions. The Policy Control Function (PCF) performs policy control related to QoS, mobility and session management. The Authentication Server Function (AUSF) performs subscriber authentication based on the subscription data stored in User Data Management (UDM). The Network Repository Function (NRF) allows the network functions to request and discover the required functions based on their required capabilities and services. Further, the Network Exposure Function (NEF) enables exposure between network functions internally and externally with external applications.

A Network Slice Instance (NSI) consists of required Network Slice Subnet Instances (NSSIs), which in turn consist of the required Network Functions (NFs). These subnets can belong to different domains of the network. The Network Slice Selection Function (NSSF) performs network slice selection. Network slices are identified by Network Slice Selection Assistance Information (NSSAI) signaled by the UE. Based on the signaled NSSAI, the AMF signals the NSSF to select the required network slice. The various network functions, broadly the User Plane (UP) and Control Plane (CP) functions can be flexibly deployed based on communication requirements and resource levels. Further, network slices can be dynamically created, configured, and managed based on the communication requirements.

4.2 Network Slice Management

To be able to create, configure, and manage network slices based on the requested services, there needs to be translation of communication requirements into network slice and subnet requirements. Here translation means the conversion of high-level communication service and service flow requirements into network slice and subnet requirements, specifically in terms of the required network functions, their optimal placement, allocation of available resources and routing.

As there will be multiple slices, customers, business actors, there also need to be separate management functions. Virtual network function management and orchestration require utilizing the concepts of Software Defined Networking (SDN) and NFV [24]–[26]. 3GPP has defined three management functions for network slicing, namely, Communication Service Management Function (CSMF), Network Slice Management Function (NSMF) and Network Slice Subnet Management Function (NSSMF) [27]. These functions follow a consumer-provider type of relationship as shown in Figure 1.

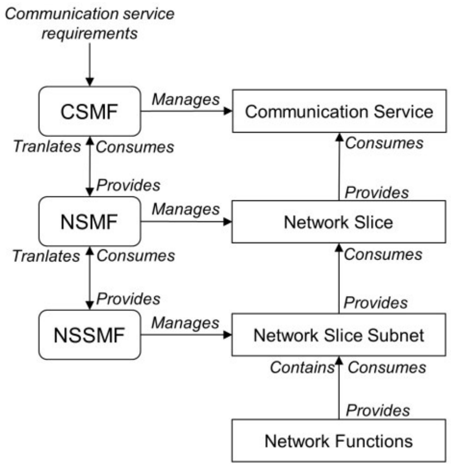

Figure 1. 3GPP Network Slice Management Functions for Network Slicing

The CSMF is responsible for the translation of communication requirements to network slice requirements and communicate these requirements with the NSMF. The NSMF is responsible for management and orchestration of network slice instances and for the translation of network slice requirements to network slice subnet requirements. The NSMF communicates these requirements with the NSSMF. The NSSMF is responsible for management and orchestration of network slice subnet instances and communicating with NSMF. The NSSIs are created by allocating the required network functions from different network domains. The NSIs for a particular use case are created by chaining the required NSSIs. The created NSI can then be selected by the NSSF and provided to the requesting UE. A slice instance can be defined for the UEs belonging to a use case. For use cases belonging to a UCG, a slice type can be defined in terms of network functions from different network domains. The network slices within each slice type can then be dimensioned based on the required network resource levels per use case.

5 Network Slices for a Smart Factory

Several industry verticals will require their use case specific network slices which share the same underlying physical network. The network will be horizontally sliced, which means the network functions from each of the network domains (access, edge, core, application/data) will be dynamically allocated to respective slices. These slices will be use case specific and multiple of these use case specific slices will be required for each vertical. Thus, network slicing for a vertical refers to network slices designed for the use cases or use case groups of a specific vertical. The horizontal and vertical aspects of network slicing are summarized in Table 2.

Table 2 Vertical and Horizontal Aspects of Network Slicing

Characteristics	**Vertical**	**Horizontal**
Objective	To create use case specific slices for verticals.	To slice the end-to-end network to take advantage from the flexibility and modularity of virtualization
Usage	Specific vertical requirements.	Similar services in different customer segments.
Constituents	Within the vertical, there can be multiple slices for different services.	Multiple similar slices for similar services.
Example in factory context	Factory slices; consisting of slices for logistics, WSN, self-driving vehicles/robots.	Consumer & factory IoT
Enable	Physical and virtual nodes for specific vertical networks.	Virtualization with distributed computing, storage, networking.

An end-to-end sliced network takes advantage from flexibility and modularity of virtualization to distribute computing, storage, networking in different network domains. Multiple use cases can have network slices similar in terms of similarly placed and allocated network functions and resources.

5.1 Use Case Specific End-to-End Network Slices

The use cases within each use case group have similar service flow and interactions with the local and wide area network. The network slices for each of the use cases in a use case group are defined by similar network functions placements and thus have similar subnet requirements from different network domains. Thus, broadly three slice types can be defined, while the total number of network slices depends on the number of involved use cases. Further, each network slice can be dimensioned based on the required network resource levels. The end-to-end slices for a smart factory consist of use case specific slices from a horizontally sliced network with similar subnet requirements as shown in Figure 2.

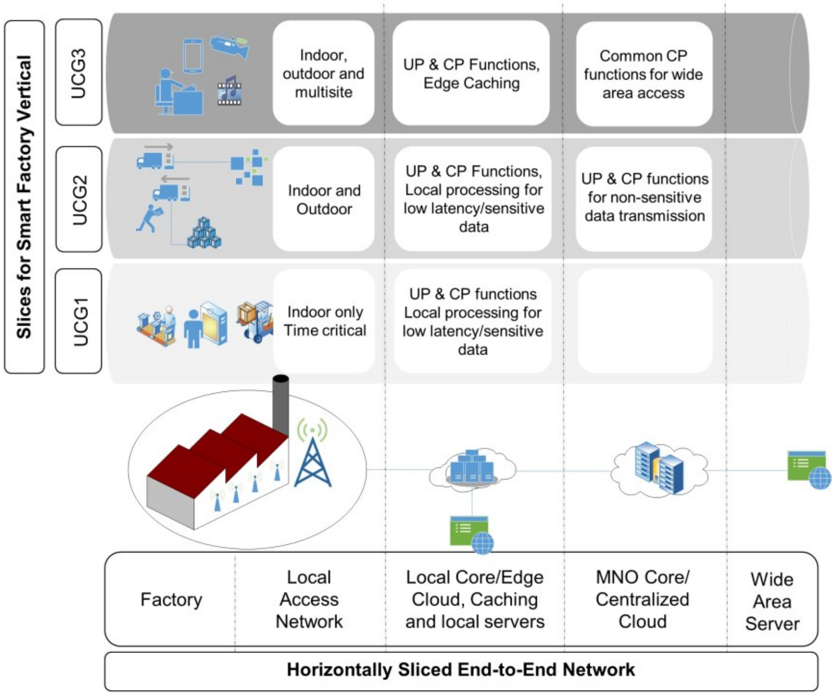
Slices for Smart Factory Vertical
UCG3
UCG2
UCG1
Indoor, outdoor and multisite
UP & CP Functions, Edge Caching
Common CP functions for wide area access
Indoor and Outdoor
UP & CP Functions, Local processing for low latency/sensitive data
UP & CP functions for non-sensitive data transmission
Indoor only Time critical
UP & CP functions Local processing for low latency/sensitive data
Factory
Local Access Network
Local Core/Edge Cloud, Caching and local servers
MNO Core/ Centralized Cloud
Wide Area Server
Horizontally Sliced End-to-End Network

Figure 2. End-to-End 5G Network Slices for a Smart Factory (Use case specific slices within a smart vertical from a horizontally sliced e2e network)

The different domains of the network can be flexibly utilized depending on the required network functions and level of resources. For critical low latency services, the processing can be located at the local server or the edge cloud. For less demanding services, a centralized server can be utilized. The placement of UP and CP functions in the local core can be used to achieve a local breakout of data for local processing, low latency, and maintaining complete isolation for sensitive data as depicted for UCG 1 and UCG2. Some services will also require access to MNO's wide area network. The placement of UP and CP functions in the centralized MNO core can be used to provide roaming support and interworking between the local and wide area networks for UCG2 and UCG3. Such grouping can be made bigger or smaller depending on the number and orthogonality of use cases. The number of network slices belonging to the three slice types will depend on the number of involved use cases.

5.2 Network Slice Management Model

The network slice management model will consist of CSMF, NSMF and NSSMF network functions. These functions can be flexibly deployed in different network domains, being allocated to one or be shared among multiple business actors. The local operator will be responsible for translating the factory's high-level communication service requirements into end-to-end network slice requirements using CSMF and establishing communication between CSMF and NSMF. The local operator will be responsible to translate the slice requirements to subnet requirements using NSMF and establishing communication between the NSMF and NSSMF. The local operator uses the NSSMF function to instantiate the required NSSIs by selecting the required NFs from different network domains. Then it uses NSMF function to instantiate the NSIs by selecting the required NSSIs and then CSMF function to manage the communication services provided as use case specific slices to the factory. These functions follow a provider-consumer relationship and thus the NSSIs provided by the NSSMF are consumed by the NSMF to create end-to-end NSIs, which are in turn consumed by the CSMF to provide the communication service. The proposed network slice management model for a smart factory in a multi-operator environment is shown in Figure 3.

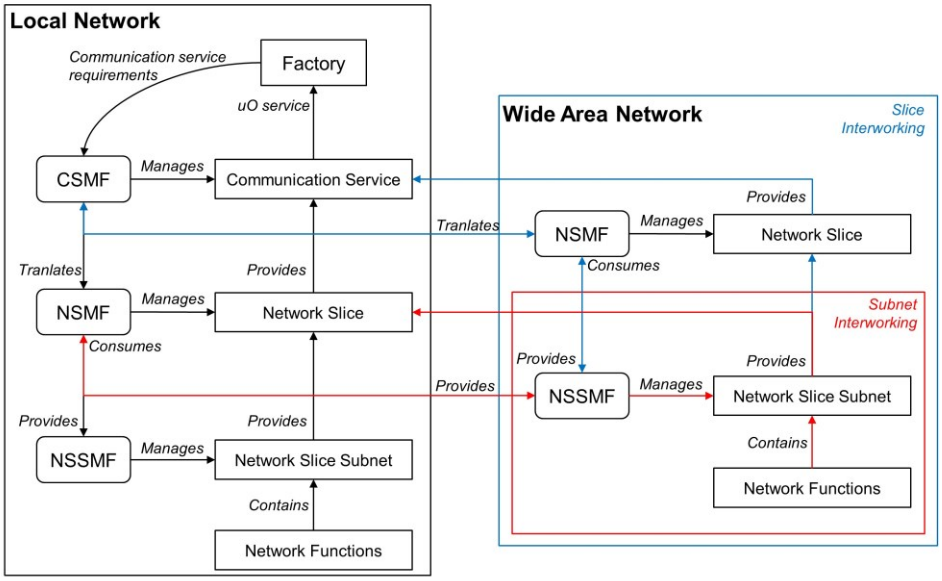

Figure 3. Network slice management model for a smart factory in a multi-operator environment

The management procedure also applies to an MNO providing slices to its customers. The difference being the local operator's network functions constitute the local network for a specific vertical while MNO's network functions constitute the wide area network. The local and wide area networks can interwork for providing network slices either at the subnet level or at the slice level. Interworking at subnet level implies that communication service is requested from the local operator, who provides the required slices that contain the required local and MNO subnets. Interworking at slice level implies that the communication service is requested from both local operator and MNO, and each provides their respective slice. These options will depend on the factory's expertise and use case specific requirements. The factory can be provided with some level of control over the CSMF to monitor and request changes in the service. An advanced customer factory that demands independent control over the slice configuration and management could take up more independent control over CSMF. Additionally, these options can be assumed with the factory taking up the local network operation. This model consists of multiple levels of interactions between technical components and business actors. This multi-level, multi-operator slice management model allows for the possibility of different network slicing strategies, analyzed using the value network analysis method.

6 Network Slicing Strategies

The Case factory has an isolated network and outsourced IT management, with limited business flexibility. Further enhancing the level of automation for diverse use cases and expansion of business opportunities is possible with 5G network slicing. As different use case groups can be involved with multiple levels of interactions between technical components and stakeholders, different strategies can be feasible for different use cases. As described in chapter 3.2, we have grouped use cases into three groups for testing technical applicability. The method used for studying the strategies is described further.

6.1 Value Network Analysis Method

The Value Network Analysis (VNA) method developed in [28], is used to design alternate Value Network Configurations (VNCs) and the notation used is shown in Figure 4. In this method firstly, the technical architecture is studied to find the possible options and the required technical components. The required business actors are assigned respective business roles over the technical components. The technical components are connected via technical interfaces and the business actors are connected via business interfaces. The business interfaces depict the means of value exchange between actors. Different possible technical components, interfaces and assignment of roles leads to alternative VNCs.

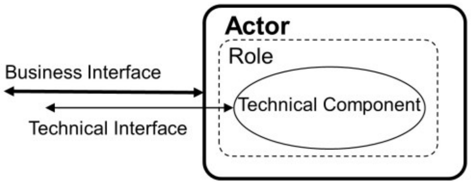

Figure 4. Value Network Configuration notation [28]

Each VNC is driven by a business actor that takes up majority of the roles and acquires the maximum value in terms of services, control over the network and its revenue sources. The feasibility of each VNC depends on the required services and the costs and benefits for the involved business actors. A local network operator is better suited to satisfy local use case specific communication requirements [29]. In this paper, we focus on local operator as the main service driver for developing a network slicing strategy for smart factories and investigate the possible interworking with MNOs.

The local network can be deployed with or without interworking with the wide area network. It is possible that some factories will want to deploy, operate and manage the network themselves (make instead of buy). In that case, the business roles of local network operation can be assumed to be taken up by the factory itself. Additionally, existing service providers, machines vendors, network equipment vendors, and venue owners can take up the role of local network operation. To avoid redundancy in describing the VNCs, only the local operator is assumed to take up such roles. Further, it is possible to distinguish between a basic and an advanced factory, depending on their network management capabilities. Additionally, service providers such as machine vendors can also be assumed to be slice consumers and will be able to provide their services, such as remote maintenance, over the factory's respective network slices provided by the local operator. The network slice management model is explored using VNA method to formulate three alternative network slicing strategies for a smart factory.

6.2 Non-interworking Strategy

The local operator is responsible for translating communication service requirements into network slice requirements, creating the required network slice subnets and providing service-specific network slice. The factory makes the request based on its service requirements to the local operator. There is no interworking as there is no interface between the local and wide area operators. The local operator is responsible for network slice management via CSMF, NSMF and NSSMF, over the technical components of service, slice and subnets respectively. The local operator can provide some level of capabilities to the customer over the CSMF function to monitor and manage communication service. However, the local operator is mostly responsible for the CSMF function. Based on the level of control over the CSMF and exposed capabilities, it can be possible for the customer to monitor and request changes if needed.

The local operator derives the network slice subnet requirements from the network slice requirements, creates the required NSSIs, and associates these to the NSIs. Based on the subnet related requirements the NSSIs will be created, configured, used, reconfigured, shared among NSIs. The business roles and network slice management functions are listed in Table 3.

Table 3 Business actors, roles and network slice management functions (Non-interworking)

Business Actor	Business Role Description	3GPP Network Slice Management Functions		
		CSMF	NSMF	NSSMF
Factory	Consumes communication service and has capability to monitor, manage and request the service	x		
Local Operator	Provides communication service, network slices and network slice subnets to factory and requested network slice subnets to third-party SPs	x	x	x

The factory applies low management effort for a limited control (monitoring and requesting only) and outsources the network operation and management of its closed indoor network to the local operator. The factory only needs one business interface (SLA) with the local operator, as shown in Figure 5. A closed indoor network and absence of wide area support mean limited opportunities for use cases such as wide area fleet maintenance and logistics, multisite communication, roaming, remote maintenance, third-party services and FwF.

From factory managers perspective this VNC illustrates the strategy for a fully isolated type of factory; buying connectivity services for an isolated network with limited opportunities for automation and business. From the local operator's perspective, this strategy allows it to exercise full control over the network and acquire connectivity and services related revenues.

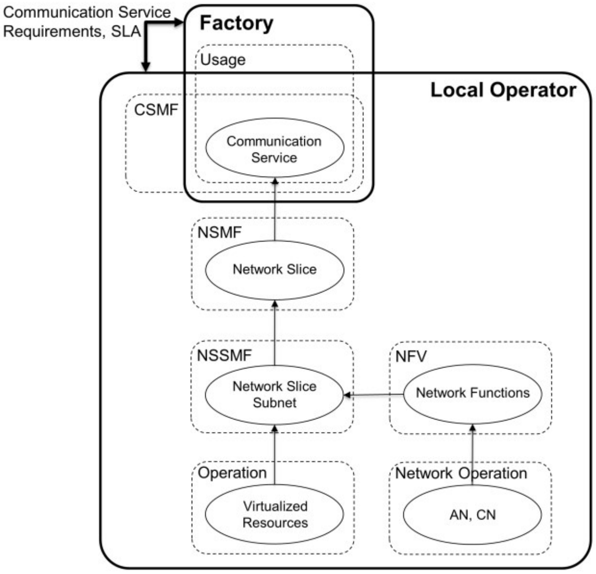

Figure 5. Non-Interworking Strategy

6.3 Subnet Interworking Strategy

The provisioning needs of the factory in this VNC include configuring the slices with local and wide area resources for accessing faraway servers, remote monitoring, roaming, multisite operation, and wide area fleet maintenance. The local operator's procedure of network slice provisioning and management with the local network resources, and the communication service requirements, request and monitoring for the factory resembles the local operator only VNC. Additionally, in this VNC, shown in Figure 6, the local operator can also provision the slices with wide area resources from MNOs. The local operator and MNOs will have a sharing contract and there must exist an interface between the local operator and MNOs to share resources. The factory still only has one contract with the local operator who provisions the slice with local operator subnets and MNO subnets. Additionally, local operator's NSMF must support multiple slice subnet instances from local operator and MNO, and support them as a single slice to provide communication service to the customer. The business roles and network slice management functions are listed in Table 4.

Table 4 Business actors, roles and network slice management functions (Subnet Interworking)

Business Actor	Business Role Description	3GPP Network Slice Management Functions		
		CSMF	NSMF	NSSMF
Factory	Consumes communication service and has capability to monitor, manage and request the service from local operator.	x		

Business Actor	Business Role Description	3GPP Network Slice Management Functions		
		CSMF	NSMF	NSSMF
Local Operator	Provides communication service, network slices and network slice subnets and also requests the required network slice subnets from the MNO	x	x	x
MNO	Provides the network slice subnets requested by the local operator.			x

Additionally, third party SPs can be part of the service provisioning and based on the requested resources the local operator will provide connectivity to the SPs. For example, a machine provider can remotely monitor the status of a machine and provide remote assistance and predictive maintenance. In this case, the local network's firewall must allow some applications and remote SPs to communicate.

The factory applies medium management effort for a limited control (monitoring, requesting and partial agreed upon management exposure) and outsources the network operation and management for all local and wide area requirements to the local operator.

From factory managers perspective this VNC illustrates the strategy for a local isolated network type of factory with the possibility for local and wide area interoperability for certain use cases; buying connectivity services and management with better opportunities for automation and business. This VNC is suitable for factories with multisite operation via a single contract with the local operator. From the local operator's perspective, this strategy allows full control over the local network and agreed upon control over MNO's shared resources. The local operator acquires the connectivity and services related revenues and shares part of the revenue with the MNO based on the share and usage of resources. From MNO's perspective, this strategy allows it to utilize its resources better and open new revenue opportunities.

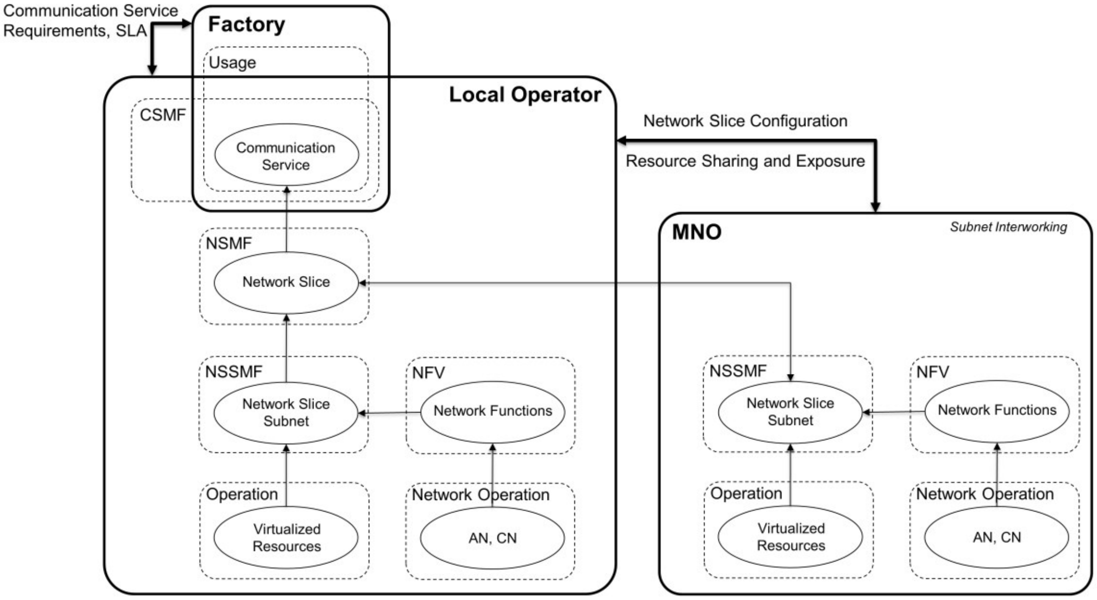

Figure 6. Subnet Interworking Strategy

6.4 Slice Interworking Strategy

The provisioning needs of the factory in this VNC include access to wide area services similar to subnet interworking but also include independent requesting of slices from local and wide area network and support for dual subscription. The network slice provisioning and management over both the local and wide area network, differs from the previous VNC, as the interface at the network slice level. The communication service provisioning in this VNC includes local operator slice and wide area MNO slice as shown in Figure 7. Thus, local operator and MNO interface with the factory, both providing own network slice as part of the service and enable roaming. This enables the factory to have dual subscription for home and visited factory scenarios. Factory can also buy a separate factory broadband slice from MNOs and the MNOs can extend their coverage indoors. The access to machine data still needs to pass through the factory's firewall for allowed applications and SPs. The customer factory takes full control of the CSMF, which must support multiple network slices. The business actors, roles and network slice management functions are listed in Table 5.

Table 5. Business actors, roles and network slice management functions (Slice Interworking)

Business Actor	Business Role Description	3GPP Network Slice Management Functions		
		CSMF	NSMF	NSSMF
Factory	Consumes communication service. Monitors and manages the service. Requests the required network slices from local operator and MNO.	x		
Local Operator	Provides requested network slices and network slice subnets.		x	x
MNO	Provides requested network slices and network slice subnets.		x	x

The factory applies high management effort for control over the communication service (monitoring, requesting and managing through CSMF) and outsources local network operation to the local operator. From factory managers perspective this VNC illustrates the strategy for a local isolated network type of factory with wide area access for certain use cases; buying connectivity but self-managing the communication service to have better control over automation and business. This VNC is suitable for factories with multisite operation with multiple national and international logistics operations and requirements of multi-tenancy. From local operator's and MNO's perspective, this strategy allows for control over their respective network and resources. Both acquire revenues by having contracts with the smart factory for connectivity but the service tailoring is managed by the smart factory.

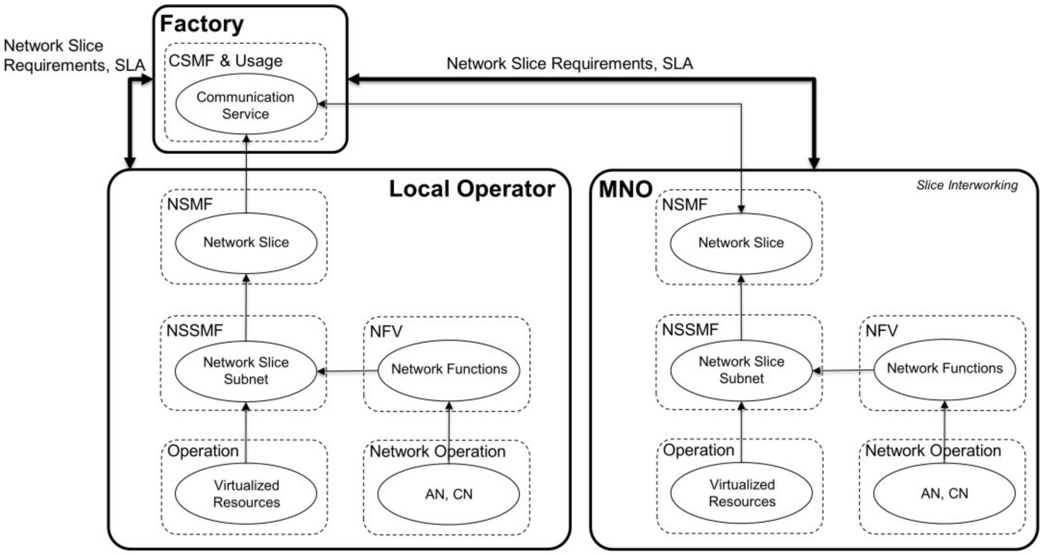

Figure 7. Slice Interworking Strategy

7 Feasibility Study

Different network slicing strategies for a factory are possible based on possible interworking options in network slice management model. Factory managers can decide on the choice of strategy for their communication network based on traditional approaches of make or buy, security and level of automation. Additionally, one network slicing strategy can be more feasible over the other, depending on the type of factory, service types, operation area, QoS, isolation requirements, number of contracts, network expenses and level of management efforts by different actors.

A Feasibility study involves studying different characteristics of considered alternatives, to find the costs and benefits for involved stakeholders and supported use cases. The feasibility of the three strategies, their main characteristics and costs and benefits to different business actors, and technical applicability to use case groups were studied and summarized in Table 6.

Table 6. Network Slicing Strategies and Feasibility

Characteristics	Non-interworking	Subnet Interworking	Slice Interworking
Communication service	local operator slice = local operator subnets	local operator slice = local operator subnets + wide area MNO subnets	local operator slice + wide area MNO slice
Interworking	Not Available	At network slice subnet level	At network slice level
Type of factory	Isolated	Multi-site	Multi-site, visited and home factory scenario
MNO service availability	Not Available	Through the local operator for inter-site and wide area	Indoor, inter-site and wide area
Level of exposure to factory	Low	Medium	High
Level of exposure between operators	Not available	High	Low
Third-party involvement	Low	Medium	High
Factory management effort	Low	Medium	High
Operator management effort	High	Medium	Low
Number of contracts	Single	Single	Multiple
Factory expenses	Low	Medium	High
Operator expenses	High	Medium	Low
Operator control	High	Medium	Low
Technical Applicability			
UCG1	x	x	x
UCG2		x	x
UCG3			x

In the non-interworking strategy, low level of exposure of network resources limits third-party involvement and MNO service availability. Whereas, in this strategy, the factory's effort and expenses for network management will be low through a single contract. In the subnet interworking strategy, there is a medium level of exposure to the factory while a high level of exposure between the operators. This enables third-party involvement and MNO service availability through a single contract with the local network operator. In the slice interworking strategy, the level of exposure to the factory is high while the level of exposure between the operators is low. This enables third-party involvement, MNO service availability and independent slice configurability, through multiple contracts.

The choice of strategy can have implications on the overall network virtualization in smart factories. The non-interworking strategy is suitable for a factory with isolated operation and limited third-party involvement. The subnet interworking strategy is suitable for a factory with local isolated network but with possibilities for wide area access for certain use cases and inter-site communication. The slice interworking strategy is suitable for factories who require more management control over their services, configuration and management of the slices, and control over the local and wide area service independently. In each of the strategies, the level of exposure of network resources varies between the factory and operators, and between interworking operators. A smart factory can take the role of local network operation (make instead of buy) based on its technical expertise, and to utilize more than one strategy depending on support multiple use case groups.

Based on the possible interworking in each of the strategies, the UCG1 is supported by all three strategies, UCG2 is supported by either subnet or slice interworking strategies and UCG3 is supported by slice interworking strategy. The factory managers can find the most feasible strategy based on this feasibility study, the suitability of each strategy for the type of factory and the technical applicability to support involved use cases.

8 Conclusions

Many smart factory use cases will have more stringent communication service requirements than current technologies can fulfill. Moreover, there will be a need to bridge the gap between the local and wide area networks. 5G will bring lower latency, more capacity, higher speed, and higher reliability compared to current wide area 4G and local area Wi-Fi. The virtualization in 5G enables flexibility in managing network resources. Further, network slicing will be a secure and effective way of provisioning and managing different use cases through logically separated networks over the same physical network. Typically, large MNOs operating over the wide area provide best effort service for all use cases. A local operator is better suited to provide local use case specific needs for a smart factory.

The studied state-of-the-art electronics assembly factory possesses an existing need for logically isolated networks. However, there are some missing capabilities to support smart factory use cases. The smart factory use cases can be grouped into three use case groups based on their communication requirements and service flows over different network domains. Network slices were defined for these use cases in terms of optimal network functions placement over multiple network domains, namely, local network, edge, wide area network and central cloud.

Our network slice management model allows distribution of functions between business actors based on the 5G network architecture. Three alternative network slicing strategies were developed based on the possible options for interworking between the local and wide area networks. The three strategies differ in terms of the applicability to different use cases, the number of contracts and other costs and benefits to involved business actors. The strategies have implications on the implementation of virtualization to support smart factory use cases. Factory managers could then decide on the most feasible strategy for their factory.

The non-interworking strategy is feasible for a smart factory with isolated operation, only consisting of use cases not requiring wide area access. The subnet interworking strategy is most feasible for a smart factory that includes use cases requiring wide area access with a single contract and medium management effort. The slice interworking strategy will be most feasible for a smart factory that demands more control over the slice configuration and management. It is possible for a smart factory to be responsible for the installation, operation and management of the network itself (making instead of buying). Further, a smart factory can utilize more than one strategy, for different use cases and thus, have the corresponding type of contracts with involved business actors.

Acknowledgements This work was supported by Business Finland in the uO5G project (grant no. 7438/31/2016) and the 5G VIIMA project (grant no. 6430/31/2018).

References

[1] “IEEE 802.1: 802.1Q - Virtual LANs.” [Online]. Available: http://www.ieee802.org/1/pages/802.1Q.html. [Accessed: 30-Jul-2018].

[2] M. Luoma, M. Ilvesmaeki, and M. Peuhkuri, “Source characteristics for traffic classification in differentiated services type of networks,” 1999, vol. 3842, pp. 25–36.

[3] M. Matinmikko, M. Latva-aho, P. Ahokangas, S. Yrjölä, and T. Koivumäki, “Micro Operators to Boost Local Service Delivery in 5G,” *Wirel. Pers. Commun.*, vol. 95, no. 1, pp. 69–82, Jul. 2017.

[4] J. S. Walia, H. Hämmäinen, and M. Matinmikko, “5G Micro-operators for the future campus: A techno-economic study,” in *2017 Internet of Things Business Models, Users, and Networks*, 2017, pp. 1–8.

[5] “State nets €77m in 5G frequencies auction | Yle Uutiset | yle.fi,” 02-Oct-2018.

[6] ITU News, “Finland’s vision for 5G development,” 05-Jul-2018.

[7] Aetha Consulting, “National positions and developments in the 26GHz band,” 2018.

[8] 3GPP, “TS 22.104 V16.1.0 Service requirements for cyber-physical control applications in vertical domains,” 2019.

[9] 3GPP, “TS 23.501 v15.2.0 System Architecture for the 5G System,” 2018.

[10] D. Clark, R. Braden, and S. Shenker, “RFC 1633 Integrated Services in the Internet Architecture: an Overview,” 1994.

[11] B. Davie, F. Baker, and C. Iturralde, “RFC 3175 Aggregation of RSVP for IPv4 and IPv6 Reservations,” 2001.

[12] K. Nichols, D. L. Black, S. Blake, and F. Baker, “RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” 1998.

[13] S. Wang, D. Li, and C. Zhang, “Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination,” *Comput. Networks*, vol. 101, pp. 158–168, Jun. 2016.

[14] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, “Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges,” *IEEE Access*, vol. 6, pp. 6505–6519, 2018.

[15] 3GPP, “TR 22.804 V16.1.0 Study on Communication for Automation in Vertical domains (CAV),” 2018.

[16] 5G-PPP, “5G and Factories of the Future-White paper,” 2015.

[17] I. Badmus, M. Matinmikko-Blue, J. S. Walia, and T. Taleb, “Network Slice Instantiation for 5G Micro-Operator Deployment Scenario,” in *European Conference on Networks and Communications (EuCNC)*, 2019.

[18] E. Hofmann and M. Rüsch, “Industry 4.0 and the current status as well as future prospects on logistics,” *Comput. Ind.*, vol. 89, pp. 23–34, Aug. 2017.

[19] R. F. Babiceanu and R. Seker, “Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook,” *Comput. Ind.*, vol. 81, pp. 128–137, Sep. 2016.

[20] NGMN Alliance, “NGMN - Description of Network Slicing Concept.” 2016.

[21] NGMN Alliance, “NGMN - 5G End-to-End Architecture Framework v2.0.” 2018.

[22] ETSI, “ETSI GR NFV-EVE 012 v3.1.1 Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework,” 2017.

[23] 3GPP, “TS 29.244 v15.2.0 Interface between Control Plane and the User Plane Nodes,” 2018.

[24] J. Miao *et al.*, “Zero-touch Network and Service Management-Introductory White Paper,” 2017.

[25] H. Flinck, C. Sartori, A. Andrianov, C. Mannweiler, and N. Sprecher, “Network Slicing Management and Orchestration,” 2017.

[26] ETSI, “ETSI GS NFV-IFA 010 - V3.1.1 - Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Functional requirements specification,” 2018.

[27] 3GPP, “TR28.801 V15.1.0 Study on management and orchestration of network slicing for next generation network.”

[28] T. Casey, T. Smura, and A. Sorri, “Value Network Configurations in wireless local area access,” in *2010 9th Conference of Telecommunication, Media and Internet*, 2010, pp. 1–9.

[29] J. S. Walia, H. Hammainen, and H. Flinck, “Future scenarios and value network configurations for industrial 5G,” in *2017 8th International Conference on the Network of the Future (NOF)*, 2017, pp. 79–84.