Ahmad Khalil, Benjamin Becker, Lisa Wernet, Ralf Kundel, Björn Richerzhagen, Tobias Meuser, and Ralf Steinmetz. *IEEE 19th International Conference on the Design of Reliable Communication Networks*

Dependability: Enablers in 5G Campus Networks for Industry 4.0

Ahmad Khalil*, Benjamin Becker*, Lisa Wernet*, Ralf Kundel*,
Björn Richerzhagen†, Tobias Meuser*, Ralf Steinmetz*
*Multimedia Communications Lab, Technical University of Darmstadt
{firstname.lastname}@kom.tu-darmstadt.de
†Siemens AG
bjoern.richerzhagen@siemens.com

***Abstract*—Modern smart factories, as envisioned by industry 4.0, are highly digitized, connected, and agile systems that monitor, control, and optimize the factory's efficiency and productivity by processing continuous data streams. Connectivity on the factory floor lays the foundation for these smart factories and, consequently, has a significant impact on the productivity of the whole system. Consequently, the factors influencing the dependability of a communication system need to be known and leveraged best to ensure the availability, reliability, maintainability, integrity, and safety of the system.**

In this paper, we focus on an analysis of Fifth-Generation (5G) campus networks and their dependability as prominent candidates for wireless connectivity in smart factories. We first provide an overview of modern smart factories and discuss the utilization of 5G networks in this context, followed by relevant background information on system dependability. We then discuss key factors influencing dependability in 5G campus networks and their architecture. Finally, we discuss open research challenges to enable 5G networks in various industrial applications.

***Index Terms*—Smart factory, Industry 4.0, 5G, Dependability**

I. Introduction

Modern smart factories represent highly digitized, cloud-connected, and agile systems that process continuous data streams to monitor, control, and improve the efficiency and productivity of the factory [1]. Smart factories are considered to be one of the most important aspects of the fourth industrial revolution (industry 4.0) [2], [3]. In industry 4.0, the underlying idea is that most components (like production machines or conveyor belts) are interconnected and able to exchange data in real-time, which facilitates efficient manufacturing and enables complex production processes. While the communication may be controlled centrally, the interaction between the different system components in the smart factory is decentralized by nature. This decentralized interaction between the components is considered to be a huge paradigm shift from the conventional fully centralized model [4]. In this paradigm, sensors are spread across the factory and continuously collect data from the production lines. Smart machines, robot arms, conveyor belts, inventories, and logistic vehicles can communicate with each other and have access to the data provided by the sensors.

978-1-5386-5541-2/18/$31.00 ©2018 IEEE

To fully realize the industry 4.0 vision, communication needs to meet the requirements of the respective industrial use cases, e.g., real-time constraints, bandwidth demands, availability and reliability, and support of fixed and mobile entities. In this paper, we focus on 5G systems as one candidate technology, especially for mobile entities and environments where utilizing wired connections might lead to an increased chance of failure [5]. 5G, especially with 3rd Generation Partnership Project (3GPP) releases 16 and 17, includes several technical enablers for low-latency and high-reliability communication, often referred to with the term Ultra-Reliable Low-Latency Communications (uRLLC), that specifically aim to address requirements from industrial use cases [6], [7]. In contrast to that, earlier generations of mobile networks, i.e., Third-Generation (3G) and Fourth-Generation (4G) mobile networks still in use today, focus on human-to-human communications and on human content consumption, generating large packets and a need for transmission of those packets with relatively high data transfer rates. While being suitable also for a number of industrial use cases, especially when it comes to outdoor coverage, 3G and 4G mobile networks do not address URLLC-related use cases [8].

In addition to supporting the respective performance requirements, 5G networks can operate as campus networks for industrial applications. This can be achieved either through dedicated local network infrastructure and spectrum, where available, or through means of virtualization and *slicing* within an operator's network. Combined with local or edge-based processing, this enables lower latency and potentially higher data rate, while at the same time allowing sensitive data to remain on-premise [9]. Of course, these options for the realization and placement of functional components of the 5G system and the resulting data and control flows have an impact on the dependability of the communication system. It is of tremendous importance to understand this impact on dependability within the respective industrial scenario.

The term dependability refers to the measure of the reliance that can be placed on the service delivered by a system, in our case, the network. Thus, it considers different attributes like reliability, availability, safety, maintainability, and integrity. In particular, the main contributions of this work can be summarized as follows:

- We highlight 5G network utilization approaches in modern smart factories.
- We discuss the critical factors influencing dependability in 5G campus networks.
- We derive open research challenges to enable 5G networks in various industrial applications, including smart factories.

The remainder of the paper is laid out as follows: In Section III, we provide background information on system dependability, followed by 5G networks and the 5G campus network architecture. In Sections V, VI, and VII, we highlight several research approaches to improve the 5G networks' dependability in diverse industrial applications before we conclude the paper.

II. System Dependability

The term dependability is used to describe the trust that can justifiably be placed in the service delivered by a system [10]. It describes the ability of a system to consistently deliver a service. Next to security and performance, dependability is one of three components of the trustworthiness of a system [11]. Dependability is still of high importance for current systems, in particular, where temporary failures are undesirable or can cause huge damage. In the following, we highlight the attributes of dependability, possible threats to dependability, and the means to handle these threats.

A. Dependability Attributes

Five attributes are often used to assess the dependability of a system: reliability, availability, safety, maintainability, and integrity [10], [12]. The first two attributes are often assigned a prominent role in the literature, while the others received less attention.

a) Reliability: Reliability describes the continuity of service and is declared as the probability that a system will invariably deliver the required service for a given time. In general, it is essential for applications that require continuous service over certain periods, such as teleconferencing or control applications.

b) Availability: The availability and reliability of a system are strongly related. This attribute is defined by the probability that a system is operational at a random point in time. In other words, availability is measured by the ratio of up-time to the total lifetime of the system. High availability is crucial for services that must be reachable most of the time. However, failures in communication systems cannot be prevented entirely.

c) Maintainability: Maintainability comprises two aspects: (i) In the case of a fault or failure, it describes the system's ability to be repaired quickly. (ii) In the non-failure case, maintainability also deals with system evolution, such as software updates or component replacement. Especially the last point is essential to ensure the safe operation of the system and prevent failures while manipulating the system.

d) Integrity: Integrity deals with preventing unauthorized manipulation of the system. Up-to-date software and hardware can help improve the integrity of a system. Preventing unauthorized manipulation is essential for a safe system.

e) Safety: Safety shifts the focus towards the prevention of catastrophic failures [13], such as the loss of human life or high property values. They should be prevented at all costs.

B. Threats

In addition to the attributes, possible threats play an essential role in analyzing dependability. Dependability threats can negatively affect the before-mentioned attributes. They include faults and errors, including cascading faults and errors [14].

Faults describe weaknesses in a system that can cause errors and include, for example, software bugs or insufficient defense mechanisms against external disturbances. Certain events can lead to these faults. Activated faults may cause **errors**, defined as deviations of one or more observable values from the correct value specified for them. Weaknesses and errors by themselves are not an issue for the use of a system as a whole and may remain undetected for long periods. As soon as the service provided by a system deviates from the desired expectation or specification, the system **fails**, leading to an interruption or limitation of the provided service.

C. Means

Understanding the threats and their relationship to the system under consideration is fundamental to analyzing possible means of building dependable systems. These **means** describe various techniques that can be used to increase the dependability of a system [10].

One mean to achieve this is to **prevent faults**, which is done by appropriate quality control techniques. Those include both the design and manufacturing of a system. Systems will never be able to avoid all faults from the outset.

As faults can never be prevented completely, **fault tolerance** is important, i.e., the ability of a system to tolerate a certain threshold of faults without failures occurring. One possibility for fault tolerance is the redundancy of essential components.

As fault tolerance has its limits, the third mean is the **treatment of active faults**. Active faults must be detected, diagnosed and corrected. Fault removal is thus important during the development time and the lifetime of a system.

The fourth mean is the **prediction of relevant faults** for the system and possibly resulting errors and failures. This last mean enables the design of targeted countermeasures, even before the fault occurs.

III. 5G Architecture

Every 5G network can be divided into two main parts: the Radio Access Network (RAN) and the core network (see Figure 1). There are two ways to realize current 5G networks: (a) **Non-standalone**, (b) **Standalone**. Non-standalone 5G networks build upon existing Long Term Evolution (LTE) networks for authentication and managing users, a so-called "anchor cell". To enable 5G non-standalone, a second connection

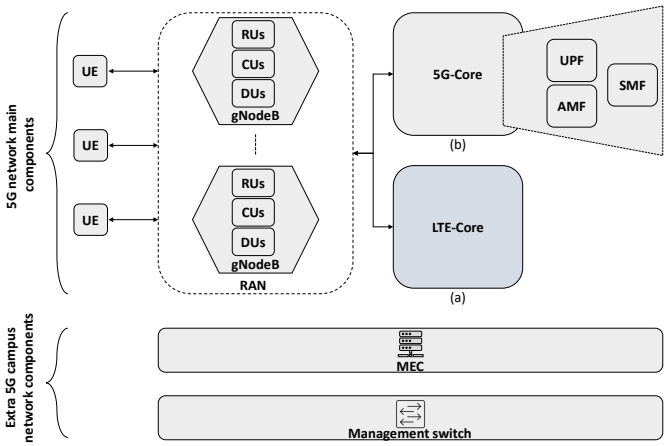

Fig. 1. Illustration of the main components of 5G networks at high level, together with additional components for 5G campus networks. (a) When connecting the RAN with the LTE-Core, this forms a non-Standalone 5G network. (b) When connecting the RAN with the 5G-Core, a 5G standalone network is formed.

is established between the User Equipment (UE), 5G-RAN and LTE-Core, providing higher total bandwidth for 5G-enabled UEs, but with limited functionality and performance compared to standalone networks. On the other hand, standalone 5G networks work without LTE anchor cells and provide all 5G network capabilities and services (e.g., end-to-end slicing). This can be achieved by directly connecting the RAN with the 5G-core.

As 5G networks are built upon the concept of Software Defined Networking (SDN), each 5G network can be split into two main components: the control plane and the data plane (or user plane).

In the following, we first provide details about both RAN and 5G-Core, and then introduce the 5G campus network architecture in more detail.

A. Radio Access Network

The main goal of RANs is to provide a connection between the UEs (e.g., mobile phones) and the 5G-core. The RAN can be represented with one or multiple gNodeBs, a 3GPP-compliant 5G-NR base station implementation. It is made up of separate network functions that implement 3GPP-compliant New Radio (NR) RAN protocols. As depicted in Figure 1, a gNodeB can be divided into multiple sub-functions such as Central Unit (CU), Distributed Unit (DU), and Radio Unit (RU), following the O-RAN terminology [15]. Further disaggregation models exist as well.

B. 5G-Core

The backbone part of every 5G network, and consists of a huge set of different components. In the following, we provide a short overview of the essential components 5G-core (see Figure 1). The first essential 5G-Core component is the User Plane Function (UPF). It works as a packet forwarder between the RAN and the data network and terminates all data tunnels for each UE device. For authenticating the different UEs, an Authentication Management Function (AMF) is required. To get authenticated, the UE sends an authentication request which gets forwarded through the RAN to the AMF. The AMF authenticates the UE by a defined handshake, and after successful authentication, a session can be established between the UE and data network through the RAN and core. For this, the Session Management Function (SMF) is involved, and responsible for managing all UEs data sessions in the UPF.

C. 5G Campus Network

5G campus networks can be realized in multiple topologies and operating models [16]. We are focusing on the setup of having completely separate, dedicated, and independent 5G campus networks which provide 5G connectivity inside the smart factory (see Figure 1).

Setting up, operating, and maintaining such systems should all be factored into cost estimates. Because all of the equipment must be purchased to begin with, the cost of setting up the network is the greatest under this operator model. Nevertheless, the operating expenses are typically constant, they should be proportional to the amount of communication. As a result, for operators with vast facilities, this operator model might be more cost-effective. Furthermore, the in-house operation model comes with a large set of advantages. For example, it achieves high levels of network security, as the complete network is managed inside the smart factory and it is less exposed to outside dangers. Moreover, this operating model is promising for long-term operability, more flexible and adaptable than the other operating models, more configurable for high availability, and best suits the highly time-sensitive applications [16].

However, some specific issues are related to the independent 5G campus networks. i.e., 5G networks operate at very high frequencies, which makes them more vulnerable to interference from physical obstacles such as walls or other structures. This can be particularly challenging in a campus network where there may be a large number of obstacles that can interfere with the 5G signal. Moreover, managing the campus network independently while maintaining high dependability levels requires supplying the network with the required hard/software for a long term. It is also essential to guarantee that the network is operated and maintained by well-trained staff. To reduce the setup, operational, and maintenance overhead, campus networks can be deployed in combination with public networks. 5G Alliance for Connected Industries and Automation (5G-ACIA) proposed several deployment scenarios that combine campus networks with public networks and compared their potential properties.

To this end, there are two additional components that can be considered in campus networks. The first component is the Multiaccess Edge Computing (MEC) as an optional component, which represents a platform that could run both core components (e.g., UPF) as well as RAN components. Depending on the operator model, MEC could be hosted and run entirely locally in the factory or within a private data center environment.

The second fundamental component of the 5G campus network is the management switch. The management switch provides connectivity between different gNodeBs and the network core. Moreover, it plays an essential role in detecting the failure cases of different 5G components (e.g., UPF). If required in some circumstances, the management switch forwards the packet between the different gNodeBs and another UPF running on MEC. In order to make the right forwarding decisions, it is essential for the management switch to consider metrics like the delay and the failure probability of the network.

D. Important Considerations for 5G Campus Networks

In the following, we assume that we have an in-house campus network operator model. Thus, all pieces of the architecture are managed locally. From Figure 1, each gNodeB has limited capacity. This gNodeB can fail to serve the connected UEs in high-load cases. However, these UEs can be big production machines or robot arms in smart factories. Thus, disconnecting them from the network could negatively affect production. To this end, and to make the network more robust, it is important to analyze the capacity of each gNodeB and calculate the number of gNodeBs required to install in each factory case. Moreover, some mission-critical UEs should be connected with more than one gNodeB (e.g., one primary gNodeB and other redundant gNodeBs), therewith the traffic gets forwarded to redundant gNodeB in case of primary gNodeB failure.

The management switch needs to have the ability to detect failures in different 5G components (e.g., UPF). After a successful failure detection, the management switch performs the intended fallback procedures. For example, in case of detecting a failing UPF, the management switch forwards the packet coming from and to gNodeBs accordingly to another UPF located in the MEC. It is thus very important to analyze the downtime for each component, which has to be considered from the management switch before initializing the fallback procedures.

To make the network more resilient, some 5G network components (e.g., UPF) should have ready-to-run instances in the MEC. This serves to handle the critical and high-priority traffic in case of in-house 5G network components failure. It is important to mention that it does take a short period (downtime threshold) from the management switch to start forwarding the traffic to the 5G component located in MEC instead of the failing in-house 5G component.

IV. 5G Campus Networks Dependability

5G network services can be split into three main categories namely massive Machine Type Communications (mMTC), enhanced Mobile BroadBand (eMBB), and uRLLC [17]. Each service category has different Quality of Service (QoS) requirements which have to be met. Depending on the industrial field, one or more of these network service types can be utilized. Smart factories mostly employ all service types [5] (Figure 2).

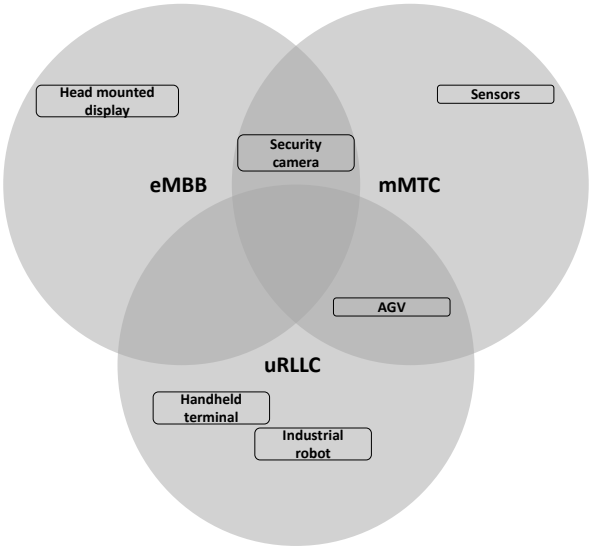

Fig. 2. 5G main service types with selected use cases in smart factories [5]

Therefore, mechanisms like network slicing can be utilized to boost the reliability of 5G campus networks [18]. Depending on the connectivity requirements of the different devices, slices can be created and configured to precisely meet those requirements (see Section V). For further increase in the network reliability, sophisticated decision-making systems can be used to provide load balancing, limit network slice failure, and provide other slices in the event of slice failure or overloading [19].

Mechanisms like network component redundancy can be used to improve the reliability and availability of 5G campus networks (see Section VI). For example, mission-critical UEs (e.g., Automated Guided Vehicle (AGV)), can be connected to multiple gNodeBs simultaneously (multi-connectivity), increasing the network availability for that components. Furthermore, redundant network components allow for scheduled repair without affecting service and hence increase network maintainability.

Moreover, to ensure a dependable 5G campus network, the traffic of existing applications and future applications should be estimated and modeled. The importance of traffic modeling in evaluating and designing the needed dependable communication network cannot be overstated (see Section VII).

One essential aspect of ensuring the safety of campus networks is by considering safety and security procedures from the beginning throughout the entire campus networks' life cycle [20].

In the end, to design and operate a dependable 5G campus network, we think that it is helpful to follow some of the well-known architecture principles and guidelines (like those provided by GAIA-X [21]). This gives us an intuition about the best network design and operational procedures which leads to dependable 5G campus networks.

V. Traffic isolation and slicing

The process of operating multiple logical networks in one physical network is called slicing. With slicing, network security can be enhanced by isolating the traffic of each slice, narrowing the attack surface. This makes it hard for the adversaries to dominate the network by preventing them from attacking the whole network surface. In general, slicing enables applying a dedicated QoS level for each slice, achieving better resource utilization over the network [22].

Moreover, slicing is the key enabler to satisfy the wide set of heterogeneous QoS requirements for different applications which require all 5G service types (mMTC, eMBB, and uRLLC). Although smart factories mostly employ all service types [5], the most critical applications, however, are the uRLLC applications. Applications from this category have strict latency and reliability requirements to ensure low latency and highly reliable communication. Slicing can facilitate fulfilling these requirements by introducing one dedicated uRLLC slice (or more), isolating the uRLLC applications' traffic from other applications' traffic.

The German federal ministry for economic affairs and energy provided four operator models which consider different slicing schemes for 5G campus networks [16].

As depicted in Figure 3, slicing in 5G networks is implemented in three different layers. The access layer is typically realized by the RAN, the transport layer, and the core layer. Each of these layers can involve several subslices. The Network Slice Manager (NSM) orchestrates the functionalities between the various subslices [23].
So far, many research studies have applied network slicing in industrial applications. To address complex problems, Jiang et al. [24] proposed a framework for dynamically integrating on-demand intelligence slices into 5G networks. Ginth et al. [25] introduced a dedicated deterministic traffic slice to deal with some network users' scheduling challenges.

Wijethilaka et al. [22] showed different slicing types applied in multiple industrial applications, like factory environment slice, remote machines operation, and remote maintenance slices. Both [22] and [26] highlighted the possibility of combining slicing with blockchain technology to build trust between the factories' machines.

To immediately react to the devices' failover cases, and to ensure efficient energy consumption, Wu et al. [27] provided multiple network slices for both critical missions and conditional monitoring. Wu et al. [28] demonstrated a practical slicing for a conditional monitoring scenario in the industrial Internet of Things (IoT) networks. They highlighted the efficiency gain when applying slicing compared with the classical network without implementing slicing. The use of programmable networking hardware provides new capabilities for in-band monitoring and immediate reaction to events [29].

Some of the industrial applications are served by multiple Network Service Providers (NSPs), which makes the end-to-end slicing more complicated. Theodorou et al. [30] proposed an approach for cross-domain slicing, introducing the *QoS-Orchestrator* that coordinates the different Network Service Provider (NSP) operations.

Considering both cyclic and switched industrial communication protocols, Kal et al. [31] presented efficient slicing methods. Moreover, they applied those methods on the network, serving the purpose of personalized medicine manufacturing use case, and conducted the end-to-end analysis.

In Table I, we summarized the related work that apply slicing in multiple industrial applications.

Although enabling network slicing can lead to a wide set of unavoidable benefits, it introduces, however, some design challenges [32]. As an example of such challenges, and due to the limitation in the available frequency radio spectrum, RAN slicing can quickly face some physical limitations. Furthermore, information sharing between different slices could lead to security issues.

So far, literature has been done on applying high-level slicing specifications for industrial applications. However, according to the authors' knowledge, the recent research has not handled the slicing of 5G campus networks in much detail.

VI. Software and Hardware Redundancy

Redundancy is a common mean to increase the dependability of systems. In 5G campus networks, the network infrastructure is often physically contained within a defined geographic area, such as a factory floor. This makes it easier to deploy redundant software and hardware components. Establishing redundant paths, usually, one active path and one passive path (to redirect traffic), improves the system's reliability and availability in the presence of a failure in the active path. Additionally, redundant network components offer the possibility of planned maintenance without service disruption and thus improve the network maintainability.

The 5G-core follows the paradigm of a Service Based Architecture (SBA) and consists of interconnected Virtual Network Functions (VNFs) [33]. Each VNF has its dedicated set of tasks and communicates with other network functions over defined interfaces. Depending on the individual requirements of the respective campus network, several instances of one specific network function may be either located on the same physical machine or deployed on several hardware entities. Redundancy allows traffic rerouting in the case of a failure of a VNF, a failing hardware component, or an interruption of a link between different entities. Gonzales et al. [34] presented the practical implementation of redundant VNFs at the edge in the context of uRLLC applications which ensures availability if the central core functions fail.

Besides those general possibilities to replicate VNFs of the 5G core, the 3GPP 5G specification in release 16 [35] introduces different concepts to increase the reliability of uRLLC applications by duplicating transmission paths in the user plane. While two of those concepts rely on redundant transmission between RAN and UPF, one concept is based on hardware redundancy. All components of the user plane, i.e., RAN and UPF, are replicated, and an UE establishes two separate connections, one to each RAN (dual-connectivity).

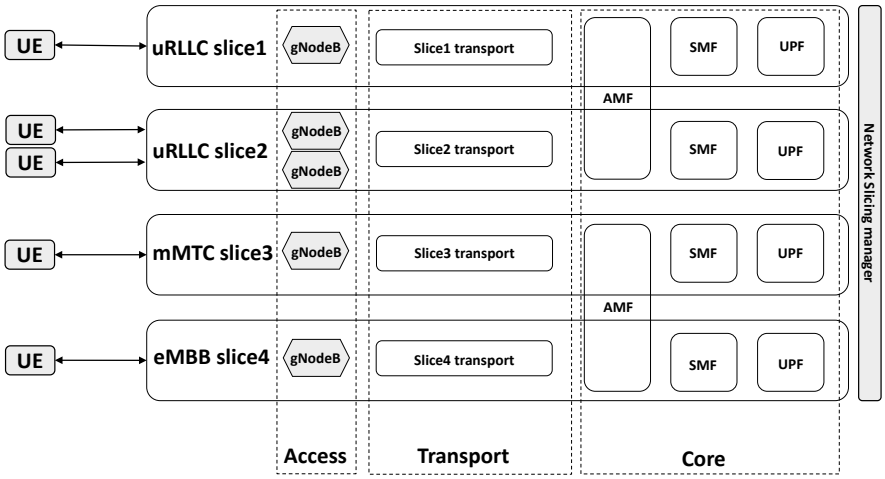

Fig. 3. Multiple slices in different network layers. NSM orchestrates the functionalities between the various slices in all layers [23].

Reference	Description	Use case	Dependability attribute(s)
[22]	Survey on slicing for multiple industrial applications.	Machines management, remote operation and monitoring	Reliability, safety, integrity
[22], [26]	Combining slicing with blockchain technology to build trust between the factories' machines.	Machine-to-machine trust	Safety, integrity
[24]	Framework for dynamically integrating on-demand intelligence slices into 5G networks.	On-demand intelligence tasks	Reliability, availability, safety
[25]	Dedicated deterministic traffic slice to deal with some of the network users' scheduling challenges.	Network users' scheduling	Reliability, availability
[27]	Multiple network slices for both critical missions and conditional monitoring.	Conditional monitoring	Safety
[28]	A practical slicing for conditional monitoring scenario in industrial IoT networks.	Conditional monitoring	Reliability, availability, safety
[30]	An approach for cross-domain slicing, introducing the *QoS-Orchestrator* which coordinated the different NSP operations.	Enable multiple NSP	Availability, maintainability
[31]	Efficient slicing methods, considering both cyclic and switched industrial communication protocols.	Personalized medicine manufacturing	Reliability, integrity

TABLE I
SUMMARY OF THE RELATED WORKS, THAT APPLY SLICING IN VARIOUS INDUSTRIAL APPLICATIONS.

Ganjalizadeh et al. [36] analyzed two adaptations of this dual-connectivity concept w.r.t. correlations in failures. These correlations are mainly caused due to similar environmental effects on redundant radio links. Thus, the positioning of redundant hardware can influence the reliability of the network. Sama et al. [37] expand the scope of network redundancy to application redundancy by connecting redundant UPFs with edge nodes for application servers. The 5G specification [35] also presents a dual-connectivity approach where the UE is simultaneously connected to a 5G Access Network (AN) and another non-3GPP AN. Choi and Kim [38] recommended improving the reliability of networks in smart factories by using this dual-connectivity approach with Wi-Fi as non-3GPP AN.

Although applying redundant network functions or paths is an inherent principle of 5G networks, only a few authors have been able to draw on systematic research into it. In addition, to the author's knowledge, additional requirements and mechanisms for efficient protocols that handle migration between Network Function Virtualization (NFV) replicas or redundant links are not considered. Further evaluation of actual implementations of the different redundancy mechanisms is required to determine if those mechanisms are suitable means for 5G campus networks.

VII. TRAFFIC MODELS

Smart factories vary in size, purposes, and communications network demands. For analyzing the 5G campus network dependability, it is pivotal to evaluate certain data sizes and traffic characteristics for each smart factory use case. This information about the data and the traffic is then used in modeling the traffic, generating a so-called traffic model. Traffic modeling is crucial to evaluate and design the required communication network.

Compared to the general 5G networks, 5G campus networks have a limited number of users and devices. This makes it easier to measure and monitor the traffic in 5G campus networks because the traffic is more predictable and easier to manage. In addition, 5G campus networks are typically designed for specific use cases, such as smart manufacturing or healthcare applications with specific traffic patterns and requirements. This means the network can be optimized and customized for the particular use case, which makes measuring and managing

the traffic easier. Overall, the limited scope and specific use cases of 5G campus networks make it easier to measure and manage traffic compared to general 5G networks, which cover larger areas and serve a broader range of applications and users.

The 5G-ACIA divided the traffic of industrial applications into two main types, **deterministic** and **non-deterministic** [6]. The deterministic traffic is generated when the applications exchange messages in specific time slots with an expected latency. According to 5G-ACIA, the main parameters used in formulating this traffic type are the *message size* and the *transfer interval*.

On the other hand, non-deterministic traffic does not define specific time slots for sending the application messages. Moreover, the application messages of this traffic type can extremely vary in their size. Parameters like *average data rate* and *peak data rate* are considered to formulate the non-deterministic traffic [6].

Depending on the use case, 5G campus networks can combine both the aforementioned traffic types. The expected traffic generated from all applications in the smart factory has to be modeled separately and then combined to assess the total data volume transferred over the communication network. Based on [39], [40], more parameters like *client mobility*, *retransmission*, and *endpoint traffic density* can also be considered while modeling the network traffic.

Building upon [6], Soós et al. [39] proposed a methodology for calculating industrial traffic in many use-cases. Their methodology considers measuring the existing network traffic and testing if the current network capabilities can handle new use-case requirements.

In the end, it is important to bear in mind that for assessing the required capabilities of the 5G campus network more factors have to be considered. Beside the traffic model, the campus network topology and the deployment scale are considered to be essential calculating aspects.

VIII. Conclusion

Most of the key network needs for modern smart factories, such as high availability, high reliability, ultra-low latency, and a large number of linked components can be met by the 5G and beyond mobile networks. This magnifies the need to investigate how dependable 5G networks are when used to offer connection in data-rich contexts like smart factories.

In this research, we investigated the dependability of 5G mobile networks in a number of industrial applications. With an emphasis on smart factories, we provided an overview of current smart factories and stressed the need to use 5G networks. Following that, we went through background information on system dependability, 5G networks, and the 5G campus network design. Finally, we presented and discussed some research work concerned with enhancing the dependability of 5G networks in different industrial applications, including smart factories.

Acknowledgement

This work has been co-funded by the German Research Foundation (DFG) within the Collaborative Research Center (CRC) 1053 MAKI, Siemens AG, and the LOEWE initiative (Hesse, Germany) within the emergenCITY center.

References

[1] N. Ilanković, A. Zelić, G. Miklós, and L. Szabó, "Smart factories - the product of industry 4.0," vol. 7, pp. 19–30, 09 2020.

[2] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & information systems engineering*, vol. 6, no. 4, pp. 239–242, 2014.

[3] L. S. Dalenogare, G. B. Benitez, N. F. Ayala, and A. G. Frank, "The expected contribution of industry 4.0 technologies for industrial performance," *International Journal of Production Economics*, vol. 204, pp. 383–394, 2018.

[4] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm," in *2014 IEEE international conference on industrial engineering and engineering management*. IEEE, 2014, pp. 697–701.

[5] G. Brown *et al.*, "Ultra-reliable low-latency 5g for industrial automation," *Technol. Rep. Qualcomm*, vol. 2, p. 52065394, 2018.

[6] 5G Alliance for Connected Industries and Automation, "A 5g traffic model for industrial use cases," Nov 2019.

[7] A. Khalil, T. Meuser, Y. Alkhalili, A. Fernández Anta, L. Staecker, R. Steinmetz *et al.*, "Situational collective perception: Adaptive and efficient collective perception in future vehicular systems," in *International Conference on Vehicle Technology and Intelligent Transport Systems*, 2022, pp. 346–352.

[8] Z. Temesvari, D. Maros, and P. Kadar, "Review of mobile communication and the 5g in manufacturing," *Procedia Manufacturing*, vol. 32, pp. 600–612, 01 2019.

[9] A. Y. Ding, E. Peltonen, T. Meuser, A. Aral, C. Becker, S. Dustdar, T. Hiessl, D. Kranzlmüller, M. Liyanage, S. Maghsudi, N. Mohan, J. Ott, J. S. Rellermeyer, S. Schulte, H. Schulzrinne, G. Solmaz, S. Tarkoma, B. Varghese, and L. Wolf, "Roadmap for edge ai: A dagstuhl perspective," *SIGCOMM Comput. Commun. Rev.*, vol. 52, no. 1, p. 28–33, mar 2022.

[10] A. Avizienis, J.-C. Laprie, and B. Randell, "Fundamental concepts of dependability," *Department of Computing Science Technical Report Series*, 2001.

[11] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[12] P. Mellor, "Failures, faults and changes in dependability measurement," *Information and Software Technology*, vol. 34, no. 10, pp. 640–654, 1992.

[13] D. Nicol, W. Sanders, and K. Trivedi, "Model-based evaluation: from dependability to security," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 48–65, 2004.

[14] J. C. Laprie, *Dependability: Basic Concepts and Terminology*. Vienna: Springer Vienna, 1992, pp. 3–245.

[15] R. Kundel, T. Meuser, T. Koppe, R. Hark, and R. Steinmetz, "User plane hardware acceleration in access networks: Experiences in offloading network functions in real 5g deployments." in *HICSS*, 2022, pp. 1–10.

[16] H. Angerer, M. Bahr, A. Bergmann, K. Drachsler, M. Fessler, M. Gergeleit, M. Janker, H. Klaus, J. Koppenborg, N. Marchenko *et al.*, "Guidelines for 5g campus networks–orientation for small and mediumsized businesses," 2020.

[17] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5g wireless network slicing for embb, urllc, and mmtc: A communication-theoretic view," *Ieee Access*, vol. 6, pp. 55 765–55 779, 2018.

[18] V. Petrov, M. A. Lema, M. Gapeyenko, K. Antonakoglou, D. Moltchanov, F. Sardis, A. Samuylov, S. Andreev, Y. Koucheryavy, and M. Dohler, "Achieving end-to-end reliability of mission-critical traffic in softwarized 5g networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 485–501, 2018.

[19] S. Khan, A. Hussain, S. Nazir, F. Khan, A. Oad, and M. Alshehr, "Efficient and reliable hybrid deep learning-enabled model for congestion control in 5g/6g networks," *Computer Communications*, vol. 182, 11 2021.

[20] M. Gundall, M. Strufe, H. D. Schotten, P. Rost, C. Markwart, R. Blunk, A. Neumann, J. Grießbach, M. Aleksy, and D. Wübben, "Introduction of a 5g-enabled architecture for the realization of industry 4.0 use cases," *IEEE Access*, vol. 9, pp. 25 508–25 521, 2021.

[21] Federal Ministry for Economic Affiars and Energy, "Gaia-x: Technical architecture," Jun 2020.

[22] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[23] R. Liu, X. Hai, S. Du, L. Zeng, J. Bai, and J. Liu, "Application of 5g network slicing technology in smart grid," in *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. IEEE, 2021, pp. 740–743.

[24] W. Jiang, S. D. Anton, and H. Dieter Schotten, "Intelligence slicing: A unified framework to integrate artificial intelligence into 5g networks," in *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2019, pp. 227–232.

[25] D. Ginthör, R. Guillaume, M. Schüngel, and H. D. Schotten, "5g ran slicing for deterministic traffic," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, 2021, pp. 1–6.

[26] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial internet of things: Architecture, advances and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462–2488, 2020.

[27] H. Wu, G. T. Nguyen, A. K. Chorppath, and F. Fitzek, "Network slicing for conditional monitoring in the industrial internet of things," *Transport*, vol. 2018, 2017.

[28] H. Wu, I. A. Tsokalo, D. Kuss, H. Salah, L. Pingel, and F. H.P. Fitzek, "Demonstration of network slicing for flexible conditional monitoring in industrial iot networks," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019, pp. 1–2.

[29] R. Kundel, F. Siegmund, R. Hark, A. Rizk, and B. Koldehofe, "Network testing utilizing programmable network hardware," *IEEE Communications Magazine*, vol. 60, no. 2, pp. 12–17, 2022.

[30] V. Theodorou, K. V. Katsaros, A. Roos, E. Sakic, and V. Kulkarni, "Cross-domain network slicing for industrial applications," in *2018 European Conference on Networks and Communications (EuCNC)*, 2018, pp. 209–213.

[31] A. E. Kalør, R. Guillaume, J. J. Nielsen, A. Mueller, and P. Popovski, "Network slicing in industry 4.0 applications: Abstraction methods and end-to-end analysis," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 12, pp. 5419–5427, 2018.

[32] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, "Network slicing to enable scalability and flexibility in 5g mobile networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, 2017.

[33] 3GPP, *Release 15 Description; Summary of Rel-15 Work Items*, 10 2019, version 15.0.0.

[34] A. J. Gonzalez, P. Grønsund, A. Dimitriadis, and D. Reshytnik, "Information security in a 5g facility: An implementation experience," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 425–430.

[35] 3GPP, *Release 16 Description; Summary of Rel-16 Work Items*, 01 2022, version 16.1.0.

[36] M. Ganjalizadeh, P. Di Marco, J. Kronander, J. Sachs, and M. Petrova, "Impact of correlated failures in 5g dual connectivity architectures for urllc applications," in *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[37] M. R. Sama, R. Guerzoni, W. Kiess, S. Thakolsri, and L. J. Jürjens, "Why is application reliability an issue for an ultra-reliable 6g network?" in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 568–573.

[38] Y.-i. Choi and J. H. Kim, "Reliable data transmission in 5g network using access traffic steering method," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 1034–1038.

[39] G. Soós, D. Ficzere, and P. Varga, "Investigating the network traffic of industry 4.0 applications–methodology and initial results," in *2020 16th International Conference on Network and Service Management (CNSM)*. IEEE, 2020, pp. 1–6.

[40] S. Gangakhedkar, H. Cao, A. R. Ali, K. Ganesan, M. Gharba, and J. Eichinger, "Use cases, requirements and challenges of 5g communication for industrial automation," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018, pp. 1–6.