The Isolation Concept in the 5G Network Slicing

Andres J. Gonzalez*, Jose Ordonez-Lucena†, Bjarne E. Helvik‡, Gianfranco Nencioni§,
Min Xie*, Diego R. Lopez† Pål Grønsund*
*Telenor Research, Telenor ASA; †Telefónica I+D – CTIO;
‡NTNU – Norwegian University of Science and Technology, Norway; §University of Stavanger, Norway

***Abstract*—The fifth generation (5G) of cellular networks shall host a number of tenants and provide services tailored to meet a wide range of requirements in terms of performance, dependability and security. Network slicing will be a key enabler, by assigning dedicated resources and functionalities to meet such requirements, where the isolation between slices, i.e., that a slice may operate without interference from other slices, becomes a core issue. The objective of this paper is to give a thorough insight into the isolation concept, discuss the challenges involved in providing it, and outline the means available to provide various levels of isolation. Fundamental concepts that can be used in further work to build an isolation solution tailored to specific needs. This paper defines important concepts such as the Provider Management, the Tenant Management, and the Means of Isolation in the context of the Isolation Dimensions. The conclusion of the study is that dealing with isolation between slices needs extensions in state of the art on the mentioned concepts, and in how to tailor the isolation to meet the needs in a cost-efficiency manner.**

I. Introduction

5G is distinguished from 4G not only in the improved performance, but also in the shift towards a programmable multi-service platform, to serve a wide variety of use cases brought up by vertical industries, with highly different requirements, in a common infrastructure. To this end, network slicing is introduced to enable multiple logical networks to concurrently run on top of a common network infrastructure. Based on proper design and optimization, various network slices are instantiated and deployed on specialized end-to-end (E2E) network partitions to provide the services requested by the vertical customers. The corresponding instances (E2E logical networks) are called *Network Slice Instances* (NSIs) [1].

All NSIs need to operate independently as if they are separated networks. The property that a NSI operates without any influence of other NSIs utilizing the same infrastructure is referred to as *isolation*. Isolation is a capital yet challenging requirement for supporting network slicing in 5G. Performance degradation, failures, or security breaches may propagate from the original NSI to other NSIs. Violation of isolation significantly complicates service assurance, due to the difficulty in identifying the root causes of a NSI problem under the influence of others. Although the importance of isolation is well recognized, most of existing works either omit its implications, address it from very specific angles, i.e., on Radio Access Network (RAN) [2], or on Datacenter Networks [3], or describe it generally as one property to achieve network slicing [4], [5], [6].

One of the first steps to address isolation in a more detailed way from a Network Slicing perspective is provided in [7]. There, isolation was studied, providing an initial perspective and challenges on the wireless and Software-Defined Networking (SDN) domains, security, and a brief overview of management issues. In [8] isolation in 5G is studied from the point of view of prioritization. Furthermore, [9] makes an analysis of the management issues related to slice isolation, proposing a definition of isolation parameters and the design of a suitable Management and Orchestration system. Finally, [10] analyses performance impact of different resource sharing settings in Network Slicing. To the best of our knowledge, there is no work in the literature that addresses isolation holistically, considering: i) the resources, network and management domains and the related means of isolation; ii) the provider and tenant management role in isolation; iii) the isolation dimensions, and its associated challenges.

This article provides a thorough study of the isolation concept in network slicing, and it aims to answer three key questions: *What* is isolation, *How* can isolation be realized (Means of Isolation), and *Why* is isolation so important (Isolation Dimensions). The objective is to provide the fundamental concepts to build in further works, architectural solutions that fit the specific isolation needs of use cases. This paper discusses the isolation mechanisms in key slice network domains (Radio, Core and Transport), and it analyzes isolation from the perspectives of two actors, the network slice *provider* who deploys, provisions, and operates NSIs; and the network slice *tenant* who orders, rents and consumes NSI(s) from the provider [1]. Finally, isolation is analyzed in three dimensions, *performance*, *dependability*, and *security*, to have a better overview about the tenant requirements.

The remaining of this article is as follows. First, Section II presents the isolation concept, using as reference the 5G-VINNI architecture, which today has four running facilities that operate network slicing [11] (*What*). Then, the means of isolation are described in Section III (*How*), followed by a description of the Isolation Dimensions in Section IV (*Why*). Finally, some concluding remarks are provided.

II. Isolation: concept and principles

This paper defines *isolation as the property that services in a slice may operate without any direct or indirect influence from activities in other slices, and unsolicited influence of the infrastructure providers.*

In order to provide the right context, this paper uses the 5G-VINNI reference architecture presented in Figure 1 [11], since it has been used for real implementation of 5G and Network Slicing in the framework of the EU-H2020-ICT-17-2017 5G-VINNI project.

978-1-7281-4355-2/20/$31.00 ©2020 IEEE

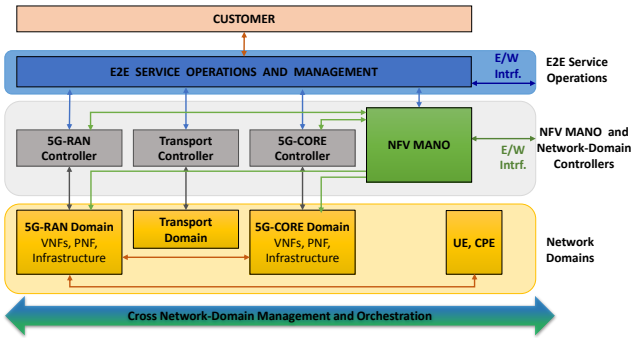

Figure 1: 5G-VINNI Reference Architecture

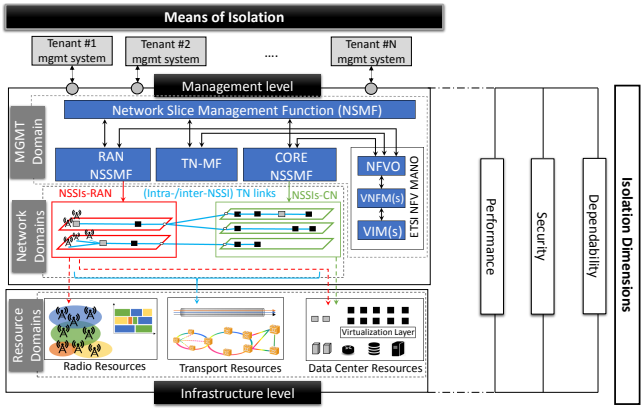

Figure 2: Isolation Dimensions in Network Slicing

The architecture is E2E oriented, spanning all network domains, including RAN, Core Network (CN), and Transport Network (TN). On one hand, RAN and CN domains provide Network Slice Subnet Instances (NSSIs) (not-E2E) that can be flexibly combined to define different NSIs. On the other hand, TN allows defining virtual links to provide connectivity across all the components building the different NSIs, including backhaul links connecting NSSIs-RAN with NSSIs-CN and any other link that could be needed to enforce intra-NSSI connectivity. In the lower layer of Figure 1 are infrastructure and the Network Domains composed by the Transport network, the radio equipment, and the Network Functions (NFs) that can be Virtual (VNFs) or Physical (PNFs) in the 5G Radio Access Network (RAN) and 5G Core. Above, the Network Domains are the NFV-Management and Orchestration (MANO) and the respective controllers of each domain. NFV-MANO is focused on virtualization-specific tasks (i.e., management at the virtualized resource level), while domain controllers focus on non-virtualization-related operations (i.e. management at the application level). The NFV-MANO is responsible for managing VNFs, combine them in order to set up one or more network services, and for life cycle management such as instantiation, scaling, updating, and terminating VNFs and Network Services (NSs). The Domain Controllers at the RAN and Core are in charge of managing the different NFs at the application level (independently of their deployment), and in general to provide control of all the non-virtualization-related operations. They can be associated with the 3GPP Network Slice Subnet Management Function (NSSMFs). The Domain Controllers at the transport include components such as SDN controllers or Multi-Protocol Label Switching (MPLS) management and control components. The E2E service operations and management level is in charge of coordinating the different domain controllers and the network services provisioned by the NFVO, in order to have an harmonic service across RAN, transport and Core, in addition to provide the resources needed for interacting with the request of the customers.

The fact that NSIs have to be isolated is one of the main challenges that network slicing brings. Isolation in network slicing is a multi-faceted problem, with multiple dimensions that need to be carefully addressed. In order to better understand the implications on the tenant requirements, isolation in slicing must be analyzed from three dimensions: performance, security, and dependability (see Fig. 2). Isolation in terms of *performance* ensures that service Key Performance Indicators (KPIs) are always met on each NSI, regardless of congestion or load surges occurring in the rest of NSIs. Isolation in terms of *security* ensures that any type of intentional attack occurring in one NSI must not have an impact on any other NSIs. This means that each NSI shall have appropriate mechanisms preventing unauthorized entities to have read and write access to NSI-specific configuration/management/accounting information, and be able to record any of these attempts. Finally, isolation in terms of *dependability* ensures that faults originated in one NSI must be confined to that NSI, thus preventing their propagation across slice boundaries. These faults can be of different types, including development, integration, or physical faults. While the first two find their root cause at design-time, the latter stemming from hardware failures occurring at run-time. The mentioned dimensions need to be considered when designing solutions to keep intended isolation among NSIs. These solutions need to be developed and integrated at two levels: infrastructure level (lower part of Fig. 2) and management level (upper part of Fig. 2).

On the one hand, solutions at the infrastructure level may leverage mechanisms providing means to split underlying infrastructure resources into a set of partitioned resources that can be later allocated across the RAN, CN and TN domains in such manner that the resulting NSIs can behave with isolation guarantees. These resource partitioning mechanisms are defined per resource domain, including radio resource domain (e.g., RF carriers arranged into flexible time-frequency resource grids), transport resource domain (e.g., multi-technology, connectivity links) and data center resource domain (e.g., compute, storage, and networking nodes) where Core and potentially RAN (if Cloud-RAN) VNFs are deployed. How these resource domains provision network domains is shown in Fig. 2.

On the other hand, to achieve isolation among NSIs at the management level, both policy-based orchestration algorithms and mechanisms enabling multi-tenancy support must be defined at the participant management blocks. As seen in Figure 2, these blocks can be 3GPP-specific Network Slice Management Function (NSMF) which is the one with an E2E view that coordinates all the domains

below, and Network Slice Subnet Management Function (NSSMFs) which are focused on specific domains. Also, non-3GPP (NFV-MANO and TN Management Function TN-MF). There are two different types of management that are important for the realization of slicing. First the *Provider Management* that is in charge of implementing the appropriate allocation and partition of resources across the network domains, and the E2E composition of those split resources to obtain the required NSIs. Second, the *Tenant Management* which allows the control of the specific resources defined in the slice, in such a manner, each tenant may be able to operate its provided NSI(s) with independence. Different tenants shall be provided with separate management spaces, each defining the (performance, configuration, lifecycle, fault) management capabilities that the tenant's management blocks can consume. This means that NSI operation is governed by both, the tenant management and the provider management.

III. Means of Isolation

The mechanisms used to achieve isolation in network slicing are based on the split of resources at the different network domains, and the management needed in order to coordinate them. Here, these two perspectives are analyzed.

A. Split and Isolation of Resources

This section describes some of the general principles used to split and isolate network resources, and some examples on how they can be achieved at the different network domains, as summarized in Figure 3.

General Means of Isolation. All network domains are built on top of physical resources such as servers, antennas, fibers, etc. First, some tenants may demand entire physical resources (*Physical Isolation*), since it may be the best way to guarantee complete isolation. Second, physical resources split, where the new sub-components are still well delimited physical entities (*Physical Resource Splitting*), e.g., frequency band divided in sub carriers. This offers high isolation, but the components and actions needed for such split reduce the isolation level. Third, isolation at the logical level, with three possibilities. i) The capacity of the new logical components are clearly delimited (*Logical - Capacity Delimitation*), e.g., radio Physical Resource Blocks (PRBs) or Multiprotocol Label Switching Traffic Engineering (MPLS-TE). ii) The new logical components can be differentiated by prioritization (*Logical - Prioritization*), e.g., Differentiated Services (DiffServ), or Radio Access Bearer (RAB) admission control. iii.) Finally, when delimitation or prioritization are not considered (*Simple Logical Isolation*), e.g., VLAN tagging. In conclusion, splitting is made by a system common to all the resulting resources, and hence it represents a central threat for the security, performance and dependability isolation.

The Radio Domain may be composed of different radio access technologies (RATs), usually differentiated by frequency, modulation, coding, etc. Tenants may demand *isolation at the RAT level*. Dedicated and *isolated antennas* in some specific areas can be also a tenant demand. Third the *isolation at and entire frequency band*, or the *isolation at the carriers* obtained by the division of the frequency bands. Carriers can be divided in time and frequency resources offering the possibility to provide *isolation at the PRBs*. Interference is a big threat for isolation in RAN, therefore in the PBR approach, complementary approaches such as inter-cell-interference-coordination (ICIC) are needed (PRB with ICIC), as was studied and described in [2]. However, interference avoidance is an open challenge that needs further investigation. Finally, there *Admission Control*, where a RAB can be admitted or not.

The Transport Domain can provide complete isolation by provisioning dedicated fibers. This is feasible but very expensive. Therefore, physical splitting (e.g., in time or frequency) can be used. For instance, in optical networks, where full lambdas can be isolated (Wavelength Division Multiplexing, WDM), or Time Division Multiplexing (TDM) techniques by assigning specific time slots to specific slices. The previous techniques are known as *hard isolation*. At the opposite, there are *soft isolation* solutions that rely on the simple separation of traffic delivery such as simple MPLS or VLAN tagging. These mechanisms offer separation, but not isolation performance guarantees. The design of intermediate solutions between hard and soft isolation may be classified in two: *i.)* Link layer (L1.5/L2) technologies such as Flex Ethernet (FlexE), dedicated queuing, Time Sensitive Networking (TSN). *ii.)* Network layer technologies such as MPLS-TE, Deterministic Networking (DetNet), Segment Routing (SR).

The Datacenter Domain. In a big scale, the use of different datacenters is a common policy that has been used to enhance dependability and security, and to cope with different regulations. Zones is also a big scale concept that can be used to achieve better security and dependability isolation. The terms availability zone and security zone are common in today's clouds, and for network slicing the principles will remain similar. Virtual resources result from the abstraction of the underlying commodity hardware, allowing the instantiation of different VNFs. However, the fact that they run on a common hardware brings potential risks on isolation. To avoid this, two different approaches can be followed: (i) VNFs from different slices are executed on separate compute nodes; (ii) VNFs from different slices can be executed on a shared compute nodes. The first approach provides the most isolated environments, as performance decrease and hardware failures only affects the slice functions it accommodates. The second approach allows a more efficient resource usage, at the cost of introducing new factors that can result in the loss of isolation. Finally, there are separated OSs (VM approach), or shared OSs (Docker approach).

B. Management of Isolated Resources and E2E coordination

One important concept illustrated in Figure 4 is the *shared part*. Based on the previous sections on split and isolation of resources, it is clear that there are different mechanisms that provide a wider or narrower shared resources (e.g., the shared part of virtual machines may be a physical server, which is narrower than the shared part of containers, where the OS is also shared). Therefore, the grey blocks in Figure 4 are abstract representations of the shared

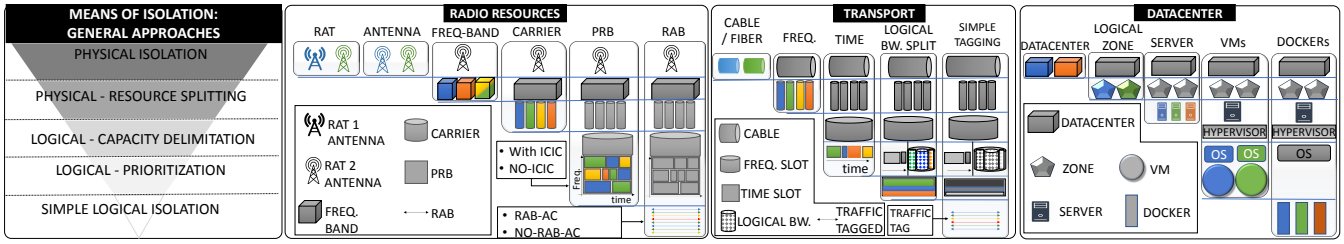

Figure 3: Means of Isolation at the Resource Domains

part, where usually, the smaller it is, the higher the level of isolation provided. For illustrating the concept of isolation at the management and orchestration level is important to distinguish between two different kinds of managers. First *the provider-manager*, who is in charge of administrating the shared part (See Figure 4), taking care of resource split management, and coordination of integration points to have a harmonized end to end perspective. It can be also defined as the isolation and slices creation enabler. Second the *tenant-managers*, who are in charge of administrating the functions running inside a specific slice, with its respective resources assigned.

Isolation at the management and orchestration is based on the concept of multitenancy (e.g., multitenancy in OSM, ONAP, etc). In that sense, each tenant should have an exclusive administration of the end-to-end slice and the network domains controllers that compound it, such as datacenter, RAN and transport. By default, there is a master tenant user (usually called administrator and operated by the slice provider), who can manage and orchestrate all tenants. See for instance Tenant A and B in Figure 4. However, specific tenants may demand rigorous access to its tenant-management components, even excluding the provider as such. This is illustrated in Figure 4 as Tenant C and D, being Tenant D a special illustration of the case when customer may demand to have the related management entities inside the tenant premises (e.g., customer offices). However, the implementation of such case is still an open challenge. The differences of the tenant managers A and B with C and D may represent also different levels of isolation at the tenant-management.

The framework presented here attempts to provide a generic and complete vision of the variables to consider for the isolation at the management and orchestration level. Multitenancy at the VIM and NFVO level is something that is given in today solutions. On the other hand, specific multitenancy options at the RAN, transport and Core controllers, as well as the E2E level require further study, being this proposal a reference and motivation to elaborate further on this regard.

IV. Isolation Dimensions

This section deals with the isolation aspects that have most impact on end customers. It contains an analysis of the mechanisms, risks and challenges of isolation, in the context of dependability, security and performance,

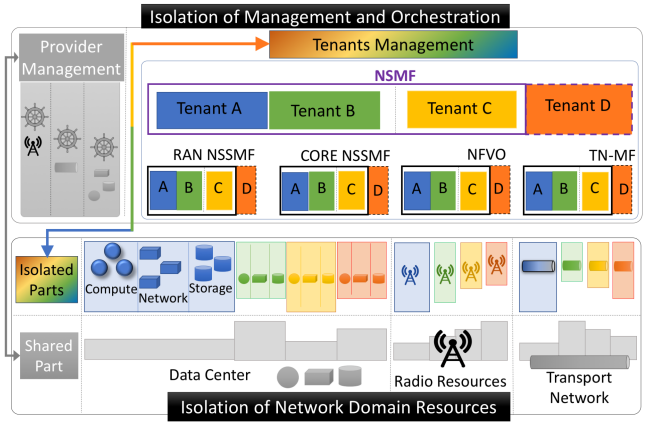

Figure 4: Management and Orchestration Means of Isolation

A. Performance

The concatenation of all the resources designated at the different network domains will compound the slice. In terms of performance, it is important to assess first each domain-part separately (throughput, latency, jitter, etc) in order to avoid any performance bottleneck at any part of the chain. In addition, the holistic end-to-end slice needs to consider pre-test from and E2E perspective, considering the integration points on each network domain, e.g., the RAN and Transport Domains are usually concatenated via a Cell Site Routes, which in principle is a single shared physically device whose capacity should be dimensioned accordingly. One of the challenges on fulfilling the expected performance of a NSI is the fact that each time a split mechanism is used, it usually has a negative impact on the performance. For instance, the additional physical components and software routines needed to provide physical/logical isolation will increase the delay on the information processing through the system. Finally, from the management point of view it is important to have routines that verify the integrity of resource assignment tasks [12], i.e., the resources allocated by the provider-management are according to what was planned. In addition, networks are dynamic entities which may constantly change, therefore any new setting should be properly planned, e.g., guarantee enough resources in order to maintain the required performance, in case of failure recovery.

B. Security

Regarding security, a service must be immune to attacks from any adversary attempting to distort its functionality or features, i,e,. *protection*. There are many global approaches to counterattack those scenarios, however concerning slice isolation is required that attacks against a specific slice must be confined to such slice, thus preventing their propagation [13]. For this, the higher the level of isolation the better, i.e., the shared part illustrated in Figure 4 should be as small as possible. This represents an open challenge since the shared part usually can not be avoided, which represents additional focus in the attesting [14] of hardware and software in the provider-management as well as the components used for integration between network domains. Another important aspect is to guarantee that no data from any actor in a given slice is accessed by any unauthorized party, i.e., *privacy*. For this, first the security attestation of the provider and tenant management are crucial [15]. In addition, it is important to follow standard policies on each tenant-manager, such as the use of robust key management mechanisms, secure connections, where not only the identity, but also the status of the communicating parties are securely established, and finally the use of mechanisms to prevent data leakage. Finally, to enforce proper authentication, authorization and accounting at the tenant-management is crucial. Where in addition the traceability of the activity of different tenants has a high relevance.

C. Dependability

A significant threat to dependability in network slicing is failure propagation. Therefore, each isolated part needs to be designed to avoid it at the hardware and software level [13]. Also, in case of failure, complete redundancy of each isolated resource needs to be planned and provided, which may be challenging due to the costs that this may imply. In addition, integration points between network domains are not getting enough attention today, and they may represent a single points of failure if not planned properly. Radio interference has been always one of the big threats for dependability in all radio systems, and in a Network Slice environment this is not the exception. Finally, management has crucial importance to guarantee the dependability of a NSI. On one hand, tenant managers should be properly isolated to interfere with operation from other tenants. On the other hand, mis-configuration at the provider and tenant manager must be avoided by the implementation of integrity check routines [12].

V. Concluding remarks

This paper points out the need to be more specific in the definition of isolation, so it may i) be dealt with in SLAs, ii) be assigned specific KPIs and iii) be addressed in system design and dimensioning. There is a number of mechanisms available to provide isolation, but there are also a range of threats and challenges to achieve it. Best understood are the mechanisms for resource sharing that assure different levels of isolation with respect to performance impairments. There is, however, no thorough study on how these may be used to achieve a targeted end-to-end performance, dependability and security. Dealing with these kind of threats may have significant implication on the system design and/or quality assurance of the elements in the network. Management is salient in isolation, it ensures the use of appropriate mechanisms to provide resources and at the same time ensures the intended level of end-to-end isolation. In summary, provided isolation is demanding. Dealing with this property should be address in initial architecture and design phase, and not be considered as a feature to be added afterwards.

Acknowledgment

Work partially supported by the European Community through the 5G-VINNI project (grant no. 815279) within the H2020-ICT-17-2017 research and innovation program.

References

[1] 3GPP, "TR28.801: Study on management and orchestration of network slicing for next generation network (Release 15) ," 2018.

[2] O. Sallent, J. Perez-Romero, R. Ferrus, and R. Agusti, "On Radio Access Network Slicing from a Radio Resource Management perspective," *IEEE Wireless Communications*, 2017.

[3] V. Del Piccolo, A. Amamou, K. Haddadou, and G. Pujolle, "A Survey of Network Isolation Solutions for Multi-Tenant Data Centers," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, 2016.

[4] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network Slicing and Softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys Tutorials*, 2018.

[5] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, 2017.

[6] A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, 2020.

[7] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J. Wary, "On end-to-end approach for slice isolation in 5G networks. fundamental challenges," in *Federated Conference on Computer Science and Information Systems*, 2017.

[8] M. Jiang, M. Condoluci, and T. Mahmoodi, "Network Slicing management prioritization in 5G mobile systems," in *European Wireless 2016; 22th European Wireless Conference*, 2016, pp. 1–6.

[9] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J. Wary, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP Journal on Information Security*, 2018.

[10] C. Marquez, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Pérez, "Resource sharing efficiency in network slicing," *IEEE Transactions on Network and Service Management*, vol. 16, Sep. 2019.

[11] D. Warren *et al.*, "5G-VINNI deliverable D1.1 – design of infrastructure architecture and subsystems," December 2018. [Online]. Available: https://doi.org/10.5281/zenodo.2668754

[12] A. Gonzalez, G. Nencioni, A. Kamisiński, B. E. Helvik, and P. Heegaard, "Dependability of the NFV Orchestrator: State of the art and research challenges," *IEEE Communications Surveys Tutorials*, 2018.

[13] I. Tumer *et al.*, "Integrated design-stage failure analysis of software-driven hardware systems," *IEEE Transactions on Computers*, 2011.

[14] T. Zhang and R. B. Lee, "CloudMonatt: An architecture for security health monitoring and attestation of virtual machines in cloud computing," *SIGARCH Comput. Archit. News*, 2015.

[15] E. NFV, "ETSI GS NFV-SEC 014 NFV Security; Security Specification for MANO Components and Reference points," April 2018.