Network-Aware Availability Modeling of an End-to-End NFV-enabled Service

Besmir Tola, *Member, IEEE,* Gianfranco Nencioni, and Bjarne E. Helvik, *Life Senior Member, IEEE*

***Abstract*—Network Function Virtualization (NFV) represents a key shift in nowadays network service provisioning by entailing higher flexibility, elasticity, and programmability of network services. Dependability is one of the main aspects that need to be investigated and tackled in order to profitably use NFV in the future. The main objective of this paper is to propose a comprehensive approach to estimate the end-to-end NFV-deployed service availability and present a quantitative assessment of the network factors that affect the availability of the service provided by an NFV architecture. To achieve this goal, we adopted a two-level availability model where i) the low level considers the network topology structure and NFV connectivity requirements through the definition of the system structure function based on minimal-cut sets and ii) the higher level examines dynamics and failure modes of network and NFV elements through stochastic activity networks. By using the proposed model, we have carried out an extensive sensitivity analysis to identify the impact on the service availability of the different service elements involved in the delivery, and their deployment across the network. The results highlight the significant impact that network nodes have on the end-to-end network service. Less robust network nodes may reduce the availability of an NFV-enabled service by more than one order of magnitude even though NFV elements like VNFs or MANO are provided with redundancy. Moreover, the results show that adopting an SDN-integrated network degrades the service availability and increases the vulnerability of the network service to SDN controllers unless adequately protected.**

***Index Terms*—NFV, Software-defined Networking, Service Function Chaining, Availability Modeling, SAN Models.**

I. Introduction

NETWORK Function Virtualisation (NFV) has drained significant attention from the research community due to its promising benefits in network manageability, cost efficiency, and reduced time to market of new and more specialized network services. Through the use of virtualization and paradigms like cloud computing, it decouples network function software from expensive purpose-built hardware and runs them as software deployed on Commercial Off-The-Shelf (COTS) hardware [1]. As such, NFV provides the necessary flexibility to enable agile, cost-effective, and on-demand service delivery model in conjunction with automated management.

According to the European Telecommunications Standards Institute (ETSI) [1], the high-level NFV architectural framework consists of three main blocks which include: i) Virtualised Network Functions (VNFs), ii) NFV Infrastructure (NFVI) and iii) NFV Management and Orchestration (MANO) block. The latter comprises the NFV Orchestrator (NFVO), VNF Manager (VNFM) and Virtualised Infrastructure Manager (VIM) where the communication among the functional blocks is enabled through well-defined reference points.

The VNF is the software implementation of a network function and it is executed on the NFVI, which encompasses a set of diverse physical resources and their virtualization software. The NFVI may be distributed on geographically distinct locations, called NFVI Point of Presences (NFVI-PoPs), and the related resources (e.g. compute, storage and network) are managed and controlled by one or more VIMs. The VNFM is the entity responsible for the lifecycle management (e.g. instantiation, scaling, termination, healing , and monitoring) of one or more VNF instances. Moreover, the NFVO is in charge of the orchestration and management of NFVI resources across multiple VIMs and the lifecycle management of network services. The NFVO and VNFM work jointly to ensure that the network services and their corresponding VNFs meet the service quality requirements specified in a Service Level Agreement (SLA), e.g., throughput, latency and reliability [2].

In order to be fully beneficial, the success of NFV is tightly coupled with several challenges that need to be addressed, where service *dependability*, as the ability to deliver a service that can justifiably be trusted [3], represents a major concern [4], [5], [6]. In addition, the upcoming 5G cellular system, for which NFV represents an essential enabling technology [4], envisions very demanding usage scenarios like Ultra Reliable and Low Latency Communications (URLLC). A URLLC service expects that the underlying infrastructure is able to provide more than fine-nines availability being translated into less than 5 minutes of downtime per year. Therefore, it becomes important to assess and quantify the dependability of NFV-enabled services.

Evaluation of system dependability (reliability, availability, etc.) is commonly achieved through analytic and numerical methods [7]. In its specification regarding end-to-end reliability [2], ETSI provides several guidelines for modeling and estimating NFV service reliability and availability. They stress out that a correct reliability/availability estimation should incorporate all the service elements and components involved in the end-to-end delivery. The supporting infrastructure, both computing and transport network, and the inter-dependencies with the software providing the service, i.e., VNFs, are required to be taken into account when estimating the reliability or availability of the service. On the other hand, they present rather simple models consisting of series and/or parallel combinations of reliability block diagrams, hence, failing to capture failure/repair dynamics of service elements and their constituent components.

A number of previous works have quantified the availability of NFV-oriented services, either in "general" terms or by selecting specific NFV service use cases [8], [9],

[10]. Nevertheless, none of these works have performed an exhaustive assessment of NFV service availability since they lack key service elements like physical network links or forwarding/routing devices which are essential networking elements inter-connecting VNFs composing a service chain. Thus, as emphasized by ETSI as well, we found that incorporating the network and the topological dependencies remains a preliminary endeavor for a correct and complete end-to-end NFV service dependability assessment. This served as primary motivation for our contribution in this paper. In addition, NFV and Software-defined networking (SDN) are increasingly becoming co-dependent since the later brings the necessary flexibility in managing network resources for composing network functions into higher-level services [11]. Therefore, it is important to assess the network service dependability also for SDN-integrated NFV-based services. This further motivates our investigation and research contribution.

Availability, as the probability that service will be provided when needed, is regarded as the most important dependability attribute in networks [12]. As specified in [12], service availability is considered of major importance to end users and it has to be defined in a clear and concise way in the SLA. Thus, in this work we focus on the availability of end-to-end NFV-enabled services. To this end, the objective of this paper is to provide an approach for a more accurate prediction of the availability of NFV-based services than the current state of the art by both taking into account the structural properties of the underlying physical network, computing and storage infrastructure, and the dynamic behavior of network elements and functions.

In this paper, we present a two-level availability model where i) the lower level consists of the structural analysis based on minimal-cut sets which are derived by the network connectivity requirements for ensuring an end-to-end network service, and ii) the higher level is composed of the availability models, based on stochastic activity network (SAN), of the network and NFV elements that are needed to provide an NFV-based service. The two levels are merged by applying the *inclusion-exclusion principle*. Moreover, we perform a quantitative assessment and sensitivity analysis from which we are able to identify the main critical parameters in the deployment of the NFV elements that influence the overall service robustness. By identifying such parameters, we gain insights that could be exploited for designing and operating an NFV-based network service such that high-grade availability requirements are to be met.

The remainder of the paper is organized as follows. In Section II, we discuss the relevant studies regarding NFV dependability. Section III introduces the service elements composing an end-to-end NFV-based service and the related dependability challenges. In Section IV, a representative network topology is introduced together with a set of VNF, NFVI-PoP, and MANO configuration cases. The objective of this is twofold, to give a reference for the discussion of structural modelling in the next section and to serve as a basis for the numerical studies at the end of the paper. As indicated, in Section V, the two-level model used to evaluate the end-to-end service availability is presented. Discussion of the numerical results of the sensitivity analysis in regard to the most critical parameters is presented in Section VI. Finally, Section VII summarises the paper by highlighting the most important conclusions.

II. Related Work

There are several methodologies that dependability studies have used to develop analytic models for quantifying system dependability. A thorough introduction may be found in [7]. For a better understanding of the different techniques utilized in the related work, we briefly summarize the most common methodologies.

Analytic dependability models typically fall into three categories: i) Non-state-space models, ii) State-space models, and iii) Hierarchical models.

Typical non-state-space models include Reliability Block Diagrams (RBD), Fault-trees (FT), and Reliability Graphs (RG). RBDs and FTs are used to represent the logical structure of a system, with respect to how availability of system components impacts the overall system availability.

State-space models are used to model complex interactions and behaviors within a system. A variety of state-space modeling techniques have been used in previous works. They span from Markov-based models like discrete/continuous-time Markov chains (D/CTMC) to semi-Markov Processes. When a reward function is associated with the chain, for the evaluation of a certain metric, they are known as Markov reward models (MRM). Other representatives of state-space models, which are more human intuitive, include Petri-net (PN)-based models like stochastic-Petri nets (SPN) and generalized-SPN (GSPN). When a reward rate is associated with the net, it is a stochastic reward net (SRN). An additional of PNs are stochastic activity networks (SANs).

Hierarchical models are multi-level models where higher levels are frequently non-state space models and lower levels are typically state-space models which are more suitable for capturing individual complex behavior. A common feature of multi-level models, which makes them more useful in comparison to state space models, is the limitation of state-space explosion when dealing with large and complex systems.

Server virtualization represents a key enabling technology in NFV [13]. The authors of [14], [15] laid the groundwork of availability modeling involving virtualized systems. They use a two-level hierarchical model, composed of CTMC and FT, to represent and compare virtualized and non-virtualized server systems. Through a parametic sensitivity analysis, they were able to identify the parameters deserving more attention for improving the availability and the capacity oriented availability, i.e., performability, of the system. However, due to the nature of CTMCs, complex systems may have to deal with a state space explosion which represents an important drawback. Kim *et al.* [16] exploits Stochastic Reward Nets, an extension of Petri nets, to overcome this drawback. They extend the work in [14] by proposing a scalable model which is able to incorporate more failure and recovery behaviors involved in virtualized server systems, and include features like virtual machine live migrations and high availability.

Surprisingly, only a few works propose and quantitatively assess an NFV-based network service availability.

In [8], the authors present an availability model of a virtualized Evolved Packet Core, as an NFV use case, by using SANs. They assess the system availability through discrete-event simulation and identify the most relevant criteria to account for by service providers in order to meet a certain availability level. In addition, they model events like catastrophic failures as such events may represent a serious threat to the overall system availability.

A two-level hierarchical availability model of a network service in NFV architectures has been proposed in [17]. By aggregating RBDs (higher level) and SRNs (lower level), they evaluate the steady-state availability and perform a sensitivity analysis to determine the most critical parameters influencing the network service availability. Similarly, in [18], they extend such analysis by including the VIM functionality, as the entity responsible for the management of the network service, into the RBD. Their main findings indicate that a relatively small increment of hypervisor or VNF software failure intensity has a marginal effect on the service availability. In addition, they identify the most appropriate redundancy configuration in terms of additional replicas for providing fine-nines availability. The same authors model and assess the availability of an NFV-oriented IP multimedia subsystem (IMS) [9]. Exploiting the same modeling technique, consisting of a hierarchical model composed of RBD and SRN, they assess the availability of a containerized IMS and perform a sensitivity analysis on failure and repair rate of some of the IMS components. In addition, they identify the best k-out-of-n redundancy configuration for each elements of the IMS such that a five-nine availability is reached.

In a more recent study [10], a composed availability model of an NFV service, based on SANs, is proposed. Each VNF, composing the network service, is considered as a load-sharing cluster and the authors propose separate models for various redundancy mechanisms called Availability Modes. Through a sensitivity analysis, they investigate the effects of cluster provisioning and recovery strategies for each mode aiming at finding the most appropriate configuration providing the highest level of service availability.

The contribution of this work compared to the related studies differs in several points that aim at filling the current gap when estimating end-to-end NFV-based service availability. None of the previous works has considered the effects of the underlying physical network and its intrinsic topological dependencies emerging from the network connectivity requirements. In addition, the related works provide insights regarding a limited set of failure parameters associated with NFV elements and do not consider the impact of the failure dynamics of networking devices on the service availability. Instead, in this proposed approach, the network structural analysis allows evaluating the impact of the network connectivity in provisioning a highly dependable network service. Moreover, the dynamic models of the NFV-based service elements permit to identify the critical failure parameters, within the network and NFV elements, that impact the end-to-end service availability. Furthermore, this contribution can be seen by service operators as a starting point for developing a decision support tool in designing and operating fault tolerance and redundancy strategies to fulfill the resilience requirements of carrier-grade services. To the best of our knowledge, this approach is the first model to incorporate the impact of the transport network in an NFV-oriented service.

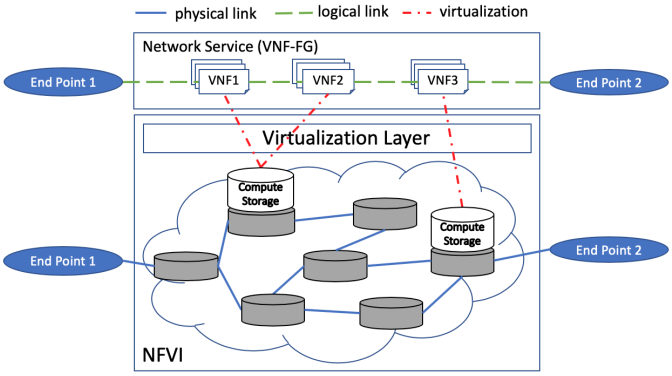


Fig. 1. Delivery of an end-to-end NFV-based service.

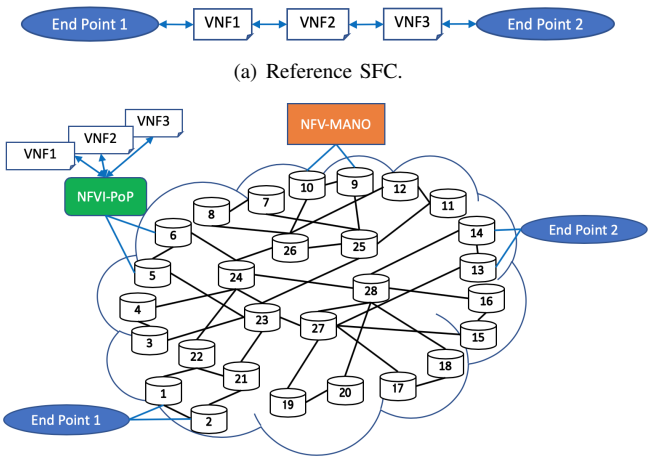
III. Dependability of an NFV-based Service

In NFV, a network service can be visualized architecturally as a forwarding graph of (virtual and physical) network functions supported and interconnected by the underlying network infrastructure. According to ETSI [1], a VNF Forwarding Graph (VNF-FG) defines the composition of VNFs, providing an NFV-enabled service and their relative sequence for traffic to traverse. Similarly, the Internet Engineering Task Force (IETF) specifies a Service Function Chaining (SFC) as "the definition and instantiation of an ordered set of service functions and subsequent steering of traffic through them" [19]. In the NFV context, both nomenclatures refer to the same thing, hence, hereafter we will refer to an SFC as the composition of an ordered set of VNFs providing a service. Thus, the delivery of an end-to-end service, illustrated in Figure 1, where both end points are customers of the NFV architecture, comprises several network functions, which are mutually connected in parallel or in series, to construct a network service graph in the form of a SFC. The service is implemented and operated through an interaction of the SFC, realizing the service, and the MANO, which acts as the manager of the service lifecycle.

The underlying network contributes to the behavior of the higher-level service which in turn can be regarded as a combination of the behavior of its constituent functional elements [1]. Thus, the delivery of a network service needs to be estimated based on the following functional elements:

- ingress and egress *end points*;
- physical and virtual *network functions* that constitute the SFC between the end points;
- *supporting infrastructure* (e.g., compute and storage nodes) that runs the VNFs;
- *networking devices* that allow the interconnection of the network functions.

From a dependability perspective, a network service could be potentially threatened by the failure of any of these elements. The transition to NFV deployments introduces additional challenges that service providers need to account for. As identified by ETSI [20], a typical challenge resides in



(a) Reference SFC.

(b) Reference NFV deployment.

Fig. 2. Network topology and NFV service deployment.

the dependency among VNFs, the virtualization layer, and the hardware infrastructure. By decoupling the software from hardware, the VNFs are not aware of the underlying hardware. Henceforth, a failure on the physical infrastructure may cause a service outage in case several VNFs share the same hardware, as opposed to physical network functions where the hardware is dedicated to a specific function. In addition, the virtualization layer introduces an additional failure source. The hypervisor itself may be prone to software failures which may affect a large part of the software infrastructure. Moreover, the NFVI will rely on extensive use of commercial off-the-shelf (COTS) servers which are usually more error-prone compared to specialized hardware implementing legacy network functions [5]. As a result, dependability may potentially represent a key threat to the success of NFV architectures and ETSI has streamlined specific reports in regard to reliability models, capabilities, and requirements [2], [20], [21].

IV. Network Topology and Case Studies

The reference SFC that will be considered in our assessment is depicted in Figure 2(a) and is composed of three VNFs. The SFC will be deployed in a real world-wide backbone network [22] which is composed of 28 nodes and 40 links, as illustrated in Figure 2(b). Note that only the network topology had been adopted from a real backbone network and the NFV deployment together with its relative redundancy configuration will be subject of investigation.

The location of the end points 1 and 2 will be fixed in all the evaluations, whereas the location and the redundancy of the NFV elements (VNF, NFVI-PoP, MANO) will change during the evaluations. Initially, the scenario where all the three VNFs are deployed into the same NFVI-PoP, referred to as the *Reference* case, is considered. In this scenario, both NFVI-PoP and MANO are placed in the edge part of the network. Afterward, the cases where the VNFs are deployed into two and three separate NFVI-PoPs (denoted *2 NFVI-PoPs* and *3 NFVI-PoPs*, respectively), placed in the edge, are investigated.

Note the representation of NFVI-PoPs and VNFs. The NFVI-PoP represents a physical entity and includes the physical resources and the software for managing the resources. The VNF represents the virtual resources and the software function that is using the resources. One or multiple VNFs are running on a NFVI-PoP. Given this assumption, the arrowed lines that connect the VNFs to the NFVI-PoP are virtual connections which we assume to be fault-free. Therefore, they are not considered as links in the structural analysis. In addition, we regard the SFC availability from the network operator's customer interface. Hence, we consider the end points and their connecting links outside the scope of the NFV-service availability evaluation. Lastly, we do not optimize the placement of NFVI-PoPs or VNFs across the network, since such problems fall outside the scope of this paper and regard challenges associated with resource allocation where service availability can be treated as an objective function or constraint, as investigated in works like [23], [24] and the references therein. Nonetheless, to acquire further insights, in addition to the *Reference* case, we evaluate the service unavailability even when the NFV elements are directly connected to the network nodes having a higher betweenness centrality, i.e., the core nodes of the backbone network. We refer to this deployment as the *Core* case and present the results of both redundant and non-redundant configurations in the numerical evaluation (Section VI-F).

Moreover, an integration with Software-Defined Networking (SDN) can be also considered. SDN consists in the separation of the control and data planes and the logical centralisation of the control plane in the SDN controller. In this case, several deployment strategies can be considered. As identified by [11], there are several use cases for SDN integration with NFV. Some of the Proof of Concepts (PoCs) regard the SDN controller merged within the VIM functionality as part of the MANO entity, whereas others consider the SDN controller as part of the NFVI or as a virtualised entity similar to a VNF. In this paper, we assume that the SDN functionality is part of the VIM entity but their location placement are geographically separated, as would the case when the NFV-based service provider and the network operator are two distinct entities.

Furthermore, a *redundant deployment* can be considered in order to provide a resilient service. In this case, the MANO, which is a logically-centralized entity, can be physically split or duplicated in different geographical areas. The VNFs, which are logical entities running on geographically-distributed computing centers, can be split or duplicated in the same (local) computing center or in other (remote) computing centers. Similarly, when an SDN-integrated architecture is considered, the SDN controller can be duplicated into separate locations in order to provide redundancy.

Figure 3 depicts the case study when a redundant deployment is considered. When only the MANO is redundant, the *Reference* deployment is considered but the dash-dot MANO element represents the MANO redundant unit which is denoted as *MANO redundant*. Similarly, in case the VNFs (and the NFVI-PoPs) are the only elements having redundant units they are denoted as *VNF redundant*. In case all the NFV elements are redundant, the deployment, denoted as *All redundant*, represent the case of fully redundant NFV service. When an SDN-integrated network is assumed, the SC node denotes the SDN controller and the relative dash-dot element represent the

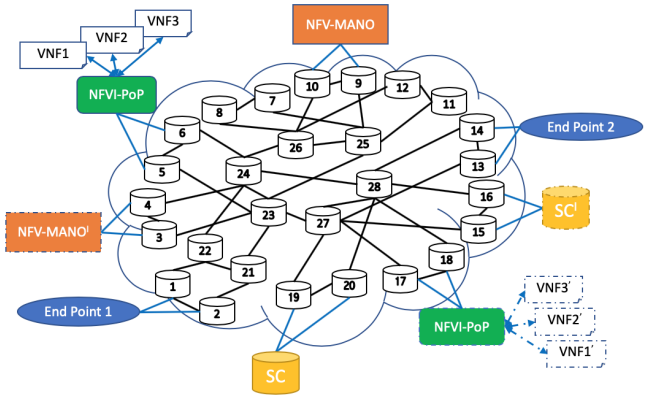


Fig. 3. SDN-integrated NFV redundant deployment.

redundant unit.

V. NFV-based Service Availability Modelling

In this section, we introduce the two-level model used to evaluate the availability of an NFV-based network service. Specifically, we regard the availability in terms of the steady-state availability, hereafter simply referred to as availability. The modeling approach consists of two levels:

- *Structural* model of the network topology and NFV deployment;
- *Dynamic* models of NFV-based service elements.

The two-level approach seeks to depict a large-scale NFV infrastructure that is deployed on top of network and computing infrastructures. The structural model assesses the network connectivity required to deliver an end-to-end NFV-based service by means of an SFC where the VNFs are running on computing centers distributed on the network infrastructure. For the structural model, reliability block diagram, fault trees, or structure functions expressed as minimal-cut or -path sets can be used (see Section V-A). The dynamic models characterize the potential failure causes of the elements needed to deliver an end-to-end NFV-based service. For the dynamic models, Markov model, Stochastic Petri nets, or extensions of the later can be used (see Section V-B).

In the following subsections, we introduce our approach through the case studies presented in Section IV which include the reference SFC that constitutes the NFV-based service. First, we present the connectivity requirements for providing an end-to-end NFV-enabled service and based on them the structure functions for each case study and minimal-cut sets are computed. Second, we introduce simple SAN models that characterize the failure dynamic behavior of the network and NFV elements. Finally, we show how to combine the two levels and evaluate the end-to-end service availability.

A. Structural Model

Structural models are an attractive technique for performing system dependability assessment [25]. Key dependability properties can be extracted from the structure function. Consider a system with n subsystems. Each subsystem can have two possible states: working and failed. As a result, the state of each i subsystem is given by a binary variable x_i, where $x_i = 1$

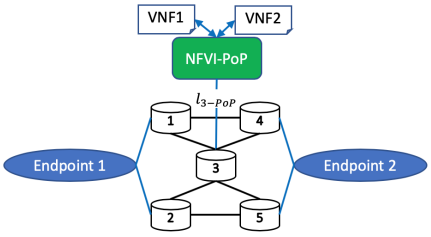


Fig. 4. Showcase for the structural analysis.

if the subsystem is working and $x_i = 0$ if the subsystem is failed. Hence, the state vector of the overall system is:

$$\mathbf{x} = (x_1, x_2, ..., x_n)$$

and the system operational mode can be described by the following binary function:

$$\Phi(\mathbf{x}) = \Phi(x_1, x_2, ..., x_n)$$

which is defined as the structure function and corresponds to a logical Boolean function that expresses the system mode, i.e., working or not. As a boolean function, it can be represented in one of the two canonical forms, the *Minimal sum-of-products form* (I^{st}-canonical form) or *Minimal product-of-sums form* (II^{nd}-canonical form). From these forms, we can extract dependability properties namely path and cut sets. The definition of the connectivity requirements will determine the most critical elements involved in an end-to-end network service and by means of the structural analysis, either based on *minimal-path sets* or *minimal-cut sets* [25], we are able to identify such elements. In this paper, we make use of *minimal-cut sets* and the following definitions apply:

Definition 1 (Cut set): A set of structure components that by failing ensures that the structure is failed.

Definition 2 (Minimal-cut set): A cut set of a structure that cannot be reduced without loosing status as a cut set.

Definition 3 (Structure function): Each max-term of the structure function expressed in a minimal product-of-sum form corresponds to a minimal-cut set.

To better illustrate, Figure 4 depicts a small system structure with five network nodes and a chain of two VNFs deployed in one NFVI-PoP. For simplicity, let us assume that the links connecting the network nodes do not fail. Let us consider a working service as a "flow" moving from endpoint 1, receive service from the VNFs, to endpoint 2. Note that the requirement of the flow being able to receive service from the VNFs defines a specific connectivity requirement that will influence the structure function. If the system has failed, the flow is prevented from being served and reaching the destination. The system is considered to be working if there exists a set of functioning components that permits the flow to be served by the VNFs and reach the destination.

From *Definition 1*, the cut sets of the structure are all the possible combinations of the components such that their simultaneous failure ensures that the system is in a failed state. Such cut sets are $\{VNF_1\}$, $\{VNF_2\}$, $\{NFVI\text{-}PoP\}$, $\{l_{3-PoP}\}$, $\{3\}, \{1,2\}, \{4,5\}, \{1,3,5\}, \{2,3,4\}, \{1, l_{3-PoP}, 4\}, \{1,2,VNF_1\}$, etc. Applying *Definition 2*, we can identify those sets that are strictly required to fail, i.e., minimal, such that the system

is failed. The statement "cannot be reduced" implies that if we remove one or more components from a minimal cut set, the set is no longer a cut set. Henceforth, the minimal-cut sets are only $\{l_{3-PoP}\}$, $\{VNF_1\}$, $\{VNF_2\}$, $\{NFVI\text{-}PoP\}$, $\{3\},\{1,2\},\{4,5\}$ and the structure function, in the form of *minimal product-of-sums*, is defined as:

$$\Phi(\mathbf{x}) = x_{VNF_1} \cdot x_{VNF_2} \cdot x_{NFVI-PoP} \cdot x_{l_{3-PoP}} \cdot x_3 \cdot (x_1 + x_2) \cdot (x_4 + x_5)$$

which aligns with *Definition 3*. In other words, the structure function identifies those system elements that being unavailable cause a system unavailability.

The adoption of an NFV architecture will change the way network services are provisioned compared to legacy networks by including more flexibility, automation, and agile orchestration. The key features of the new service delivery paradigm are the following: "centralisation" of the control logic into the MANO; "remotisation" of the network functions; "sharing" of the computing resource; geographical "distribution" of the computing centers. These features lead to an increase in the network connectivity requirements for provisioning a network service that can be summarized as follows:

- *MANO – end points connectivity:* The end point must be able to connect with the MANO in order to trigger the service provisioning.
- *MANO – VNF connectivity:* The MANO must be able to connect with the VNFs composing the SFC in order to orchestrate and manage the lifecycle of the VNFs.
- *SFC connectivity:* The ordered connectivity of the VNFs (and the end points) composing the SFC must be assured.

The first two connectivity requirements are related to the *control plane* in NFV and concern the necessary requirements of service request acceptance and management and orchestration of VNFs. Whereas, the last requirement regards the *data plane* layer and the correct service composition.

In case an SDN integrated network is considered, further connectivity requirements need to be included.

- **MANO – SDN controller connectivity**
  The peer-to-peer communication between the MANO and the SDN controller must be guaranteed in order to allow the request of the network resources for composing the SFC.
- **SDN controller – network nodes connectivity**
  The SDN controller must be able to connect with the network nodes that compose the paths among the elements in the SFC.

Furthermore, for a redundant deployment, the above connectivity requirements need to be modified accordingly, e.g., the requirement can be relaxed by ensuring the connectivity to at least one of the redundant elements.

For all the examined NFV deployments, their connectivity requirements are very important in establishing, through the structure function, the most critical elements in the delivery of a network service. For example, the requirement of ensuring an ordered connectivity of the VNFs, i.e., the SFC, is reflected in the structure function by imposing this condition when finding all the paths that include an ordered sequence of the VNFs. Accordingly, for each NFV deployment, this requirement will be embedded into the structure function from which we derive the relative minimal-cut sets. For further details on the structure function analysis, the reader may refer to [7], [25].

B. Dynamic Models

The second part of the two-level model consists of the dynamic models of network and NFV elements. To establish these models, Stochastic Activity Network (SAN) formalism is used. This enables detailed performance, dependability, or performability models to be defined in a comprehensive manner [26].

SANs are stochastic extentions of Petri Nets consisting of four primitives: *places*, *activities*, *input gates*, and *output gates*. Places are graphically represented as circles and contain a certain number of tokens which represent the *marking* of the place. The set of all place markings represent the state of the modeled system. Activities are action that take a certain amount of time to complete. They impact the system performance and can be *timed* (thick vertical lines) or *instantaneous* (thin vertical lines). A timed activity has a distribution function associated with its duration and can have distribution case probabilities used to model uncertainty associated with activity completion. The case probabilities are graphically represented as small circles on the right of the activities. Upon completion, an activity fires and enables token movements from places connected by incoming arcs to places connected by outgoing arcs. This way a system state update occurs and tokens are moved from one place to another by redefining the places markings. Input and output gates define marking changes that occur when an activity completes. Different from output gates, the input gates are also able to control the enabling of activity completion, i.e., firing. The models presented below are defined in the Möbius software tool [27].

Dynamic models are defined for the following elements:

- Network elements:
  - Connecting links;
  - IP router (*traditional network case*);
  - SDN switch (*SDN case*);
  - SDN controller (*SDN case*);
- NFV elements:
  - NFVI-PoP;
  - VNF;
  - MANO.

It is an objective that these models should be simple, yet sufficient. More complex and comprehensive models can be realized, but in this paper, we preferred to use models that enable us to apprehend the essential features of the system and emphasize the necessary details of the elements while keeping the complexity low since our focus is to evaluate the impact of networking on NFV-based service provisioning.

SAN models of network elements (for both SDN and traditional network) have been already proposed [28] and we will use the same models.

The NFVI comprises several geographical locations, and the transport network providing connectivity between these locations is considered as part of the whole infrastructure. A specific geographic location is where an NFVI-PoP (e.g., a

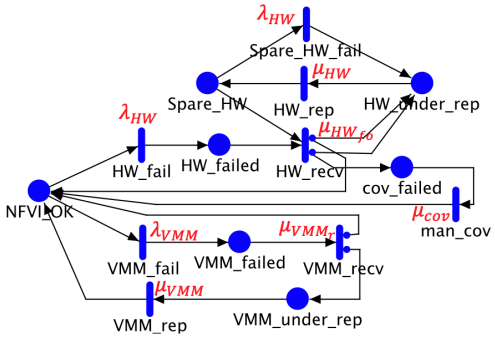


Fig. 5. SAN model of an NFVI-PoP.

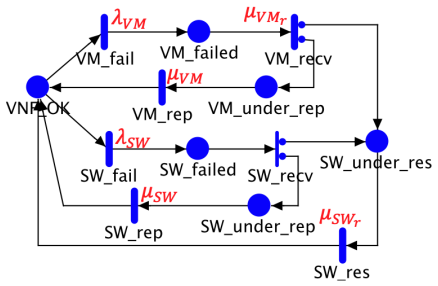


Fig. 6. SAN model of a VNF.

data center) is located and where a number of NFVI-Nodes reside. NFVI-Nodes are a group of physical devices that provide the necessary (computing, storage, and networking) resources needed by the VNF execution environment. Without any loss of generality and to keep a low complexity, we will consider NFVI-PoP and NFVI-Node as a single entity.

In modeling the VNF system, the choice of the virtualization technology used, i.e., hypervisor- or container-based, can determine the model. We believe that from a dependability perspective, the hypervisor-based technology represents a more advantageous choice due to, among others, stronger isolation between virtual and the physical machine or a higher fault detection coverage compared to containers, as shown by studies like [29]. Hence, in our model we assume a hypervisor-based technology and from a VNF perspective and depending on the deployment strategy, the VNF itself may have different failure sources. For example, when two or more VNFs are deployed in a single NFVI-PoP, the failure of the physical or hypervisor level represent a common cause failure for the different VNFs deployed on the same node. As such, we split the failure causes of the VNFs into those related to the underlying infrastructure which may represent a common failure mode for several VNFs, i.e., NFVI-PoP, and those representing the failure of the VNF itself which include the Virtual Machine (VM) and the VNF software.

1) NFVI-PoP: The SAN model of the NFVI-PoP is depicted in Figure 5. In the model we focus on the two main components that constitute the NFVI-Node which may cause a failure on the physical level, i.e., hardware and the Virtualisation-layer software infrastructure, otherwise called Virtual Machine Manager (VMM) or hypervisor. The model is composed of the following places:

- *NFVI_OK* corresponds to the fully working state of the system and is initialized with 1 token;
- *HW_failed* is populated with one token in case a failure of hardware level (memory, disk, I/O, storage etc.) is experienced, 0 otherwise;
- *HW_under_rep* represents the state where the failed hardware undergoes a repair process;
- *Spare_HW* represents the redundant hardware infrastructure ready to take over in case a hardware failure is experienced and it is initialised with one token;
- *cov_failed* represents the state where the hardware failover is unsuccessful and thus, manual intervention is required to bring the hardware up;
- *VMM_failed* represents the state when the virtualization software is failed.
- *VMM_under_rep* represents the state where the VMM undergoes a hard repair process, i.e., applying a fix/patch or software update;

Similarly to many related work and studies performing availability modeling and analysis, see for example [8], [9], [17], [18], we assume that timed activities follow an exponential distribution. The places in the model are connected by means of the following timed activities:

- *HW_fail* and *HW_repair* represent the hardware failure and recovery events with rates λ_{HW} and μ_{HW}, respectively;
- *Spare_HW_fail* represents the redundant hardware failure event with rate λ_{HW};
- *HW_recv* represents the hardware failover event with rate and $\mu_{\text{HW}_{\text{fo}}}$. There are two cases, with probability C_{fo} the failover procedure is successful where one token, fetched from *Spare_HW*, is moved to *NFVI_OK* and another one is placed in *HW_under_repair* in order to repair the failed hardware unit. Whereas with probability $1 - C_{\text{fo}}$ the failover is unsuccessful and one token is placed in *HW_under_repair* and another is moved back to *HW_failed* for a new failover procedure;
- *man_cov* represents a manual coverage intervention executing a hard recovery, with rate μ_{cov}, when an unsuccessful hardware failover is experienced;
- *VMM_recv* represents the recovery process of the virtualization software with rate $\mu_{\text{VMM}_{\text{r}}}$. It consists in a simple software reboot process and there are two cases, with probability C_{vmm} a simple reboot successfully recovers the failure and with probability $1 - C_{\text{vmm}}$ the reboot is not successful therefore a hard repair is needed. In both cases, a token is moved from *VMM_failed* to *NFVI_OK* or *VMM_under_rep*, respectively.
- *VMM_fail* and *VMM_rep* represent the failure and hard repair process of the visualization software with rate λ_{VMM} and μ_{VMM}, accordingly.

2) VNF: Figure 6 illustrates the SAN model of a VNF. The model considers failures on the VM and VNF software components. Once a VM failure is evidenced, the recovery undergoes a simple restart where with probability C_{VM} the restart successfully recovers the failure and with probability $1 - C_{\text{VM}}$ a hard repair (patching or fixing) is needed. If the VM restart is successful, the system undergoes a VNF software restart (*SW_res*) to fully recover. Similarly, if a VNF software

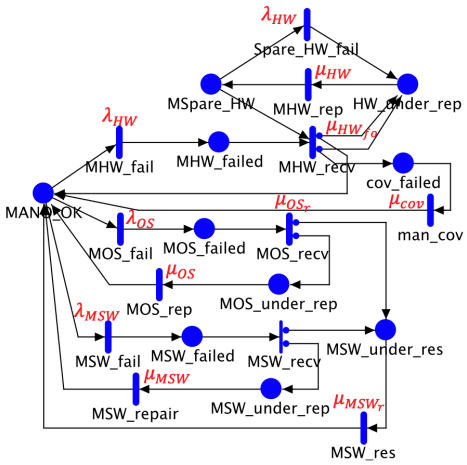


Fig. 7. SAN model of a MANO.

is experienced, with probability C_{SW} the VNF software restart successfully recovers the failure and with probability $1 - C_{\text{VM}}$ a software fixing is needed (*SW_rep*).

The model is composed of the following places:

- *VNF_OK* represents the fully working state of the system and is initialized with one token;
- *VM_failed* and *SW_failed* correspond to the states in which the VM or VNF software are failed. They are populated with one token in case a failure is experienced, 0 otherwise;
- *VM_under_rep* and *SW_under_rep* represent the states where the VM and VNF software undergoes a hard repair process, accordingly.
- *SW_under_res* corresponds to the state in which the VNF software undergoes a simple software restart action.

The VNF is failed if there are no tokens in *VNF_OK*. The following negative exponentially distributed timed activities connect the places of the model:

- *VM_fail* and *VM_rep* represent the VM failure and hard repair events with rates λ_{VM} and μ_{VM}, respectively;
- *SW_fail* and *SW_rep* represents the failure and hard repair events of the VNF software with rate λ_{SW} and μ_{SW}, respectively.s
- *VM_recv* represents the recovery process of the VM with rate μ_{VM_r}. It consists in a simple VM reset process and there are two cases, with probability C_{vm} a simple reset successfully recovers the failure and with probability $1-C_{\text{vm}}$ the reset is not successful therefore a hard repair is needed. In both cases, a token is moved from *VM_failed* to *SW_under_res* or *VM_under_rep*, respectively. Note that, in case the VM reset is successful there is a need to perform a VNF software restart to bring the system up. With nowadays technologies, these action times are comparable thus the need to include a VNF software restart becomes significant.
- *SW_recv* is an instantaneous activity which only models the software simple restart coverage. With probability C_{sw}, a simple software restart recovers the software failure and with $1 - C_{\text{sw}}$ a hard software repair is needed.

TABLE I
MODEL PARAMETERS FOR THE NFVI-POP, VNF AND MANO WITH THEIR RESPECTIVE NUMERICAL VALUES USED IN THE CASE STUDIES.

Intensity	Time	Description [Mean time to]
$1/\lambda_{\text{HW}} = 6$	months	next hardware failure
$1/\mu_{\text{HW}} = 2$	hours	hardware repair
$1/\mu_{\text{HW}_{\text{fo}}} = 3$	minutes	hardware failover
$1/\mu_{\text{cov}} = 30$	minutes	manual coverage
$1/\lambda_{\text{VMM}} = 4$	months	next VMM failure
$1/\mu_{\text{VMM}} = 1$	hour	VMM hard repair
$1/\mu_{\text{VMM}_\text{r}} = 1$	minute	VMM reboot
$1/\lambda_{\text{VM}} = 3$	months	next VM failure
$1/\mu_{\text{VM}} = 1$	hour	VM hard repair
$1/\mu_{\text{VM}_\text{r}} = 30$	seconds	VM reset
$1/\lambda_{\text{OS}} = 2$	months	OS failure
$1/\mu_{\text{OS}} = 1$	hour	OS hard repair
$1/\mu_{\text{OS}_\text{r}} = 1$	min	OS reboot
$1/\lambda_{\text{SW}} = 2$	weeks	next VNF software failure
$1/\mu_{\text{SW}} = 30$	minutes	VNF software hard repair
$1/\mu_{\text{SW}_\text{r}} = 15$	seconds	VNF software restart
$1/\lambda_{\text{MSW}} = 1$	month	next MANO software failure
$1/\mu_{\text{MSW}} = 30$	minutes	MANO software hard repair
$1/\mu_{\text{MSW}_\text{r}} = 30$	seconds	MANO software restart
$C_{\text{fo}} = 0.95$		failover coverage factor
$C_{\text{VMM}} = 0.9$		VMM reboot coverage factor
$C_{\text{VM}} = 0.9$		VM reset coverage factor
$C_{\text{OS}} = 0.9$		OS reboot coverage factor
$C_{\text{SW}} = 0.8$		VNF software restart coverage factor
$C_{\text{MSW}} = 0.85$		MANO software restart coverage factor

3) MANO: There are several differing MANO designs and the authors of [30] review some of them. We decided to represent a high-level architecture of a widely referenced open source solution, namely Open Baton [31]. A common deployment involves a high volume server running its own Operating System (OS), e.g., Linux based kernel OS, and the installation of the various MANO components software packages. However, for simplicity and with no loss of generality, we consider the MANO software as a single entity where the failure of any of its subcomponents causes a system failure.

As depicted in Figure 7, on the hardware level, the MANO model is identical to the NFVI-PoP. On the software level, the model is similar to the VNF model having the OS and the MANO software components instead of the VM and the VNF software, respectively. The MANO is considered unavailable when there are no tokens in *MANO_OK* place. Due to these similarities, a detailed description is omitted.

A set of numerical values regarding failure and repair intensities and coverage probabilities, retrieved from previous literature [9], [15], [16], [28], are presented in Table I. These are hereafter referred to as baseline parameters.

C. End-to-end Service Availability by Level Merging

The remaining step is to evaluate the end-to-end service availability by merging the structure function and minimal-cut sets from Section V-A with the individual elements availability computed using the SAN models in Section V-B. In particular, since we make use of minimal-cut sets, we consider system unavailability.

Imposing the connectivity requirements for a correct service delivery, identified in Section V-A, and expressing the structure function in the form of *minimal product-of-sums* we obtain all the possible sets of service elements (network and

NFV), i.e., minimal-cut sets, who's failure will generate a service outage. As a result, if at least one of these sets is unavailable, the service will be unavailable. Therefore, the service unavailability will be given by the probability of the union of these sets. Note that the structure function does not regard any particular routing mechanism since it considers all the available paths satisfying the connectivity requirements. In addition, even though the logical service chains are the same for the different case studies, they represent different physical topologies of the chain. Such differences are reflected by having a distinct structure function for each of the case studies we investigate.

In order to merge the two levels, we make use of the *inclusion-exclusion principle*, which is a probabilistic technique to obtain the elements in a union of finite sets. Using the inclusion-exclusion principle on the structure function we can define the service unavailability as the probability of the union of all minimal-cut sets.

$$U_{NS} = P\left(\bigcup_{i=1}^{n} C_i\right) = \sum_{k=1}^{n}(-1)^{k-1} \sum_{0\neq I\subseteq[n],|I|=k} P\left(\bigcap_{i\in I} C_i\right)$$

where $C_1, C_2, ..., C_n$ are the minimal-cut sets and $P(C_i)$ is the probability of set C_i.

To compute the probability of the intersection of minimal-cut sets we just need to know the unavailability of the individual elements composing the minimal-cut set, since in the structural analysis we assume that the failures of these elements are independent. As a result, the probability of the intersection is given by the product of the probabilities of minimal-cut sets which in turn are given by the product of the probabilities of the single elements belonging to the set. In our case, such probabilities represent the elements unavailability and we compute them by using the proposed SAN models defined in Section V-B.

For assessing the service unavailability of each case study, we select the minimal-cut sets with cardinality lower than five as principal-cut sets, because the probability of the intersection of minimal-cut sets with higher cardinality becomes negligible in comparison to the principle-cut sets. This is because almost all the probability mass is in the principle sets when elements unavailabilities are relatively small, i.e., order of 10^{-3} or smaller, as shown in our investigation (refer to Section VI). In this case, $P(C_1) \sim 10^{-3}$, $P(C_2) \sim 10^{-6}$, $P(C_3) \sim 10^{-9}$, and so forth. Therefore, the probabilities of the intersection of minimal-cut sets with cardinality higher than five will have a negligible effect. In addition, also the probability of intersection of higher cardinality minimal-cut sets with the probability of the principle-cut sets will be much smaller than the probability of the principle-cut sets.

Table II presents the distribution of the principal-cut sets for each case study. Observing the first three case studies, i.e., deploying the VNFs into different NFVI-PoPs, there is an increase of the principal-cut sets for each cardinality when spreading the VNF deployment into multiple NFVI-PoPs. In addition, for the same deployments, when an SDN-integrated network is considered, there is a further increase of the cut sets. On the other hand, the addition of redundancy decreases the number of minimal-cut sets for the smaller cardinalities, i.e., C_1 and C_2, and increases those with cardinality 3 and 4. We explore the impact of this increase in more details in the following analysis.

TABLE II
DISTRIBUTION OF MINIMAL-CUT SET FOR THE FIRST FOUR CARDINALITIES OVER THE DIFFERENT NFV DEPLOYMENTS.

	C_1	C_2	C_3	C_4	Sum (Total*)
Reference	5	63	16	0	84 (18,097,984)
2 NFVI-PoPs	6	74	20	0	100 (23,969,350)
3 NFVI-PoPs	7	85	24	0	116 (29,957,966)
SDN Reference	6	74	20	0	100 (19,727,900)
SDN 2 NFVI-PoPs	7	85	24	0	116 (24,947,306)
SDN 3 NFVI-PoPs	8	96	28	0	132 (30,557,922)
MANO redundant	4	45	50	161	260 (24,017,754)
VNF redundant	1	55	122	261	439 (73,600,881)
All redundant	0	35	122	414	571 (107,254,823)
SDN All redundant	0	43	122	415	580 (122,878,786)

*Over all C_i

VI. NUMERICAL EVALUATION

In this section, we present the numerical analysis that has been carried out to evaluate the NFV deployment across the network for different scenarios, i.e., VNF deployment locations, and the different levels of redundancy adopted by the NFV elements. The goal of our analysis is to investigate the effects of varying both elements unavailability and element's component failure intensities on the end-to-end NFV service, given the various NFV deployment case studies, NFV and network elements, and the variation of elements unavailability and element's component failure intensities. First, we identify the critical elements, involved in the service delivery, that mainly affect the end-to-end service availability. Afterward, we delve into the element's components aiming at identifying the critical ones which mostly impact the service unavailability.

Möbius [27] is a powerful software tool for system modeling and analysis as it offers formalism-independent solvers for the system evaluation of certain measures of interest, e.g. element unavailability. One type of solver integrated in the tool is a Discrete-Event Simulator (DES) [32]. The simulator allows the modeler to choose a variety of simulation execution parameters such as type of random generator, random seed, maximum/minimum batches, or simulation result accuracy through confidence intervals etc. In addition, it offers high flexibility in running multiple simulations at once which are very useful in case a multitude of scenarios are investigated. We use this simulator to derive the element's unavailability by solving the element's SAN models presented in Section V-B.

In this study, each element's baseline unavailability, presented in Table III, is derived through simulations of the individual *dynamic* SAN models with 95% confidence interval by utilizing the baseline parameters. As previously specified, we have assumed that the timed activities, having mean rates presented in Table I, follow an exponential distribution. In fact, as soon as the repair process is extremely short compared to the mean time between failures, their mean will dominate the impact on the element availability and the effects of the actual recovery distributions are marginal. We verified this "insensitivity" by evaluating the NFV elements with

TABLE III
ELEMENT'S BASELINE AVAILABILITY.

	Availability	Unavailability	95% Confidence Interval
Link	0.999911	$8.89 \cdot 10^{-5}$	+/- $1.34 \cdot 10^{-5}$
IP Router	0.9924	$7.55 \cdot 10^{-3}$	+/- $5.06 \cdot 10^{-4}$
SDN Switch	0.9970	$2.98 \cdot 10^{-3}$	+/- $5.33 \cdot 10^{-4}$
SDN Controller	0.99897	$1.02 \cdot 10^{-3}$	+/- $7.57 \cdot 10^{-4}$
VNF	0.99950	$4.94 \cdot 10^{-4}$	+/- $6.37 \cdot 10^{-4}$
MANO	0.99983	$1.68 \cdot 10^{-4}$	+/- $3.46 \cdot 10^{-5}$
NFVI-PoP	0.999951	$4.84 \cdot 10^{-5}$	+/- $1.85 \cdot 10^{-5}$

deterministic recovery processes and the their unavailability variation is almost none compared to the exponential case.

To evaluate the impact that variation of a certain element unavailability has on the end-to-end service unavailability, we use a scaling factor α_x for $x \in \{$Link, Router, MANO, NFVI-PoP, VNF, Switch, and SDN controller$\}$, which affects the baseline unavailability of the elements. Simulations have been carried out by considering a scaling factor α_x that varies within a range spanning: $\alpha_x \in \{10^{-i}\}$ for $i = -3, ..., 1$. For each simulation, we vary α_x while keeping the rest of the element's unavailability equal to their baseline values. To illustrate, for $\alpha_x = 1$ the x element unavailability equals its baseline unavailability and when $\alpha_x = 10$, the unavailability is increased by one order of magnitude, and vice-versa for $10^{-1}, 10^{-2}, 10^{-3}$. $\alpha_x = 1$ is what we consider the most likely value of these parameters which are computed by solving the relative SANs with failure and repair parameters retrieved from previous literature (refer to Table I). However, since there is an ongoing evolution of both hardware and software technologies, it is important to study the effects on the sensitivity of these parameters with the used potential range due to changes in technology. Therefore, the scaling factor range is introduced to capture this evolution and is intended to represent the foreseeable changes in the near years to come.

For presenting the results, we are looking at a 4-dimensional problem where one dimension is represented by the NFV deployments (see Table II), another one identifies the elements (network and NFV elements), another determines the range of the scaling factor, and the last one expresses the end-to-end service unavailability as a function of the previous three. Therefore, a compact and easily comparable representation of this is achieved by using pie-like polar plots which are divided into different sectors representing the various deployments. In each sector, the angle and radius show the service elements and service unavailability due to element's unavailability/component failure intensity variation imposed by the scaling factor, respectively.

A. Impact of element's availability

In this subsection, the effects of varying the unavailability of the network and VNF elements on the end-to-end network service are investigated. In addition, we compare the unavailability of an NFV-based service in the case of assuming a fault-free network.

Figure 8 shows the end-to-end network service unavailability when varying the scaling factor α_x for the cases when the SFC is deployed into a single, multiple or separate NFVI-PoPs,

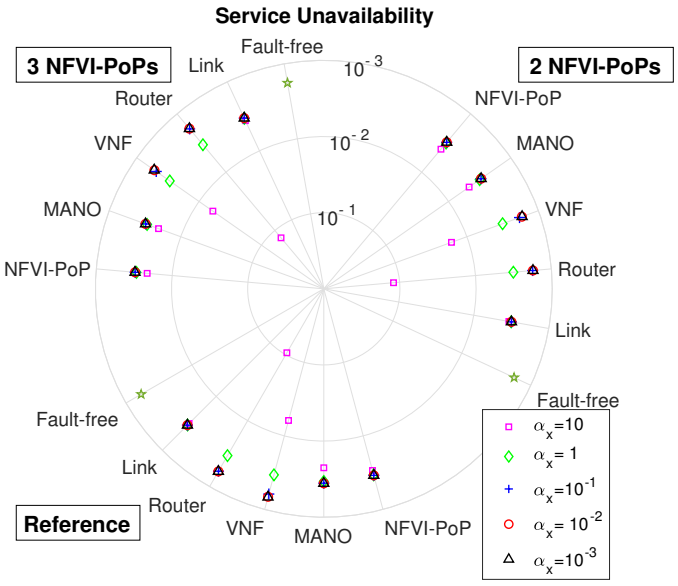


Fig. 8. Service unavailability of the three NFV deployments when varying element unavailability factor α_x.

and for the case when both links and IP routers are fault-free. Note that in this case, we consider a traditional network and not yet an SDN-integrated network. In the following, unless otherwise specified, all the case studies refer to a traditional network (TN).

An immediate observation is that the elements unavailability variation produces the same trends for all the three deployment cases. For the *Reference* deployment, given the baseline unavailabilities, the service unavailability reaches $2.9 \cdot 10^{-3}$. Any variation of link unavailability, either decreasing or increasing, does not significantly affect the service unavailability. On the contrary, the router unavailability may greatly impact the service unavailability. In particular, we observe that when the routers become less robust, i.e., $\alpha_{Router} = 10$, the service unavailability increases by more than one order of magnitude. On the other hand, when the router unavailability is reduced even by just one order of magnitude, the service unavailability is reduced to an extent that it approaches the fault-free network service unavailability ($1.71 \cdot 10^{-3}$ vs. $1.69 \cdot 10^{-3}$).

Regarding the NFV elements, the first observation we make is that for the MANO and NFVI-PoP, a decrease of their unavailability does not produce a noteworthy reduction of the service unavailability. The opposite is valid for the VNF where its unavailability reduction halves the service unavailability, i.e., from $2.9 \cdot 10^{-3}$ to $1.4 \cdot 10^{-3}$. In addition, we note that increasing the VNF unavailability by one order of magnitude, is accompanied with five times higher service unavailability. This can be explained by the fact that VNFs are three critical elements where the failure of any one of them produces a service outage. As a result, we can deduct that the VNF may play an important role in achieving both higher or lower service availability. Common to both network and NFV elements, decreasing their availability further, i.e., from 10^{-1} to 10^{-3}, does not bring an additional service unavailability reduction. In summary, the IP routers and VNFs represent the most critical network and NFV elements, respectively.

B. Impact of number of NFVI-PoPs

Deploying the VNFs, composing the SFC, into multiple or even separate NFVI-PoPs would definitively increase the path carrying service flows as they need to traverse more network elements. Accordingly, there would be an increase in the likelihood that more element's failures may impact the service availability. As a result, the system will be more vulnerable to failure events as highlighted by the increase of the principal-cut sets, presented in Table II, when the number of NFVI-PoPs hosting the SFC increases. Therefore, one can expect that service availability may be significantly deteriorated if for any reason the VNFs need to be geographically distributed. Surprisingly, spreading the VNFs into more or even completely separate NFVI-PoPs is followed with a very slight unavailability deterioration (in the order of 10^{-4}). More specifically, for the baseline element availabilities, employing two and three NFVI-PoPs results in a service unavailability of $3.17307 \cdot 10^{-3}$ and $3.39255 \cdot 10^{-3}$, respectively, versus $2.95355 \cdot 10^{-3}$ of the *Reference* case. The same difference is evidenced when varying the element's availabilities. The rationale behind is that despite the distribution of the VNFs into separate PoPs increases the low cardinality sets, the service availability is relatively insensitive to the VNF distribution in multiple NFVI-PoPs because in this case there is a higher number of available paths connecting the VNFs. The low cardinality sets are important but the high connectivity captured by the structure function and the associated flexibility in routing makes the placement effect insignificant. However, the outcome represent a good input to network administrators, as in cases an operator has to distribute the VNFs due to specific needs like resource shortages, the service availability will not be significantly affected. Note that there is an implicit premise that the network elements are homogeneous, i.e., have the same availability, and the presented outcome is also subject to the specific setting and network topology. In case a sparser network is considered the outcome may be otherwise.

To sum up, the splitting of the service chain into multiple NFVI-PoPs has a small effect on the unavailability due to an increase of the available paths connecting the splitted VNFs.

C. Impact of redundancy

In this subsection, we evaluate the impact of the redundancy of the NFV elements. To this end, we investigate the cases when only the MANO, the VNFs and when all the NFV elements are redundant, respectively.

In Figure 9, we illustrate the sensitivity analysis only for $\alpha_x = \{10^{-1}, 1, 10\}$, as for lower values there is not a significant variation. Deploying a redundant MANO decreases the service unavailability but the decrease is not significant (order of 10^{-4}). However, a redundant MANO provides adequate protection when the MANO unavailability increases, as opposed to the *Reference* case. Since the VNFs and routers are not protected with redundancy, an increase of their unavailability greatly affects the service by one and two orders of magnitude, respectively. In case only the VNFs are provided with redundancy, the service unavailability is further decreased reaching $1.1 \cdot 10^{-3}$ and it is sufficiently shielded against VNF

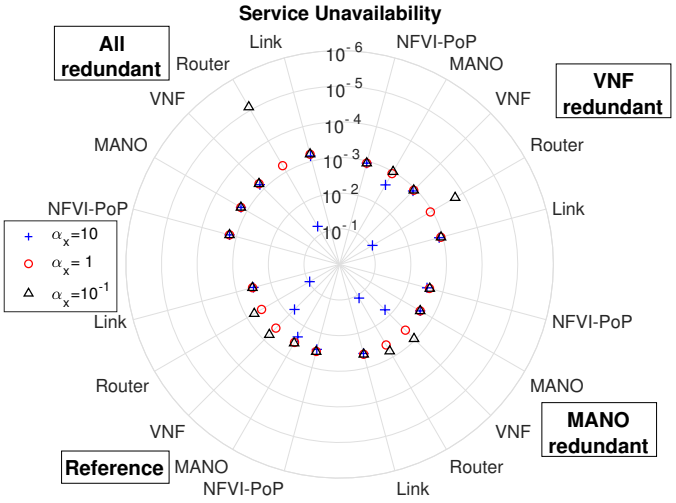


Fig. 9. Service unavailability for varying element unavailability factor α_x when considering NFV redundant elements.

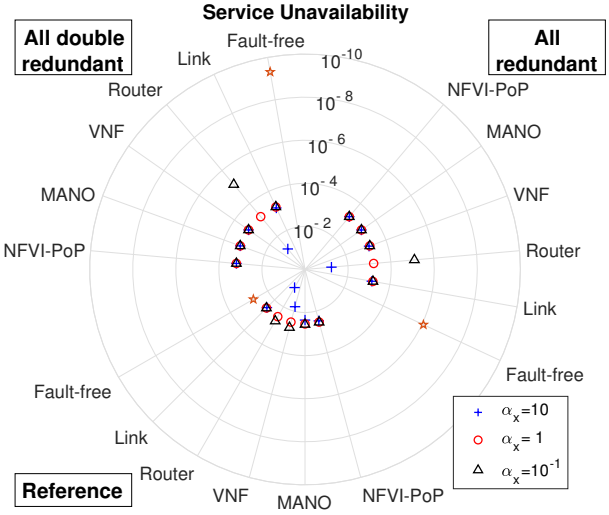


Fig. 10. Service unavailability for varying element unavailability factor α_x when considering single and double redundant NFV elements.

unavailability increments. Similarly, when all NFV elements are redundant, the service unavailability is further reduced compared to the previous two cases reaching a value of $6.3 \cdot 10^{-4}$. In this case, an increase of the VNF, NFVI-PoP or MANO unavailability does not impact the service unavailability as the redundant units provide an adequate protection. However, their unavailability reduction gives no effect at all.

Interestingly, the router may both greatly increase and reduce the end-to-end unavailability. A more robust IP router allows achieving a $7.09 \cdot 10^{-6}$ unavailability which represents target values expected by highly available NFV services, i.e., 5-nines availability [2], [5]. Moreover, we evaluate the case even when double redundancy, i.e., double VNFs, NFVI-PoPs and MANO, is deployed. Figure 10 shows the comparison of the sensitivity analysis for this deployment. We evidence that the additional unavailability reduction is rather negligible when a double redundant deployment is considered, i.e., an order of 10^{-5}. Curiously, very low service unavailability values are achieved only when the network elements are fault-free.

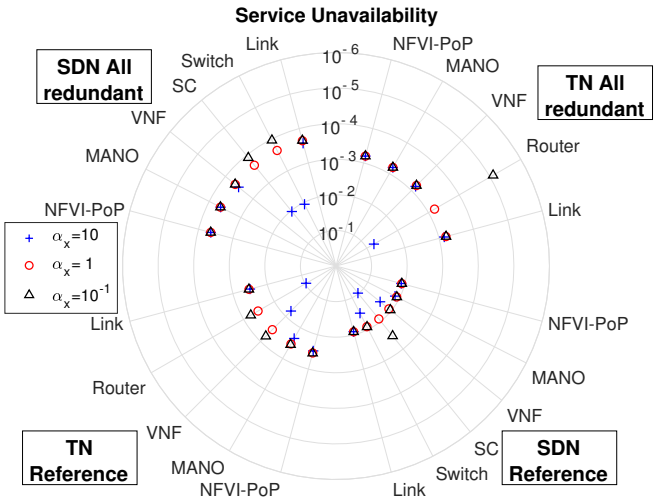


Fig. 11. Service unavailability of the traditional vs. SDN-integrated network for varying element unavailability factor α_x.

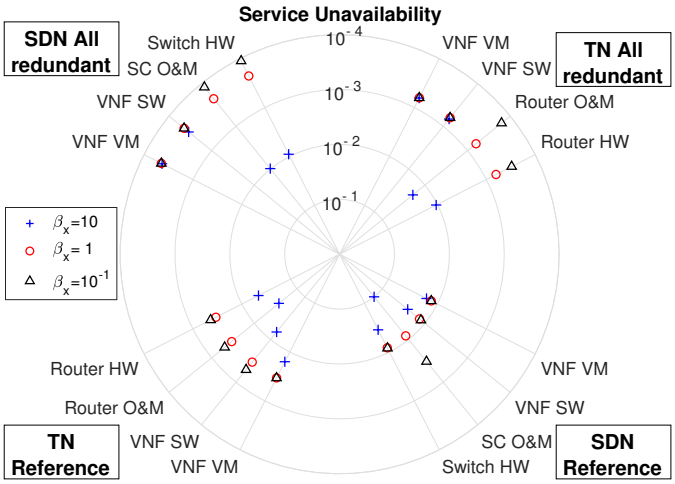


Fig. 12. Service unavailability of the traditional vs. SDN integrated networks for varying element's component failure intensity factor β_x.

Therefore, employing double redundant NFV elements does not produce compelling benefits unless the network elements are 'perfect'.

To summarize, for achieving five-nines availability, in addition to replicated NFV elements, the routers resiliency needs to be better than the nominal values used in this study.

D. Impact of SDN

When integrating an SDN network, there is an increase in the network connectivity requirements, presented previously in Section V-A, which is translated in an increase of the principle minimal cut-sets (refer to Table II). By having more principal-cut set, the SDN-integrated NFV service is expected to be more vulnerable in terms of service unavailability.

Figure 11 shows a comparison of the traditional and SDN-integrated network for the *Reference* and redundant deployments. As expected, the SDN-integrated service unavailability is higher compared to the traditional deployment. Specifically, for the *Reference* deployment, the SDN service unavailability reaches $1.2 \cdot 10^{-2}$ vs. $2.9 \cdot 10^{-3}$ of the TN case. This result is primarily due to the increased connectivity requirements imposed by the control plane of the SDN network.

Another observation regards the impact of the network nodes, i.e., routers or switches. For all the deployments, the robustness of the router is more relevant for the TN case than the switch for the SDN deployment. In the SDN case, it is the SC that has an impact magnitude similar to the routers for the TN case, thus representing the most crucial elements in an SDN-integrated network. Specifically, the increase/decrease of the scaling factor for the SC is accompanied with an increase/decrease of almost one order of magnitude of the service unavailability.

Surprisingly, when a redundant deployment is considered, the baseline service unavailability is three times less than the TN case. This result might look unexpected as it is the opposite compared to the non-redundant deployments, however, it is explained by the fact that the SC, being a critical component, is provided with redundancy which further decreases the baseline service unavailability. Nevertheless, an increasing SC unavailability may seriously degrade the service unavailability despite it makes use of a redundant unit. As a result, adopting a less robust SC may hinder the advantages created by the redundancy. Moreover, a similar trend is observed for the switches. An increasing switch unavailability is accompanied with more than one order of magnitude of service availability reduction. Differently, their unavailability reduction brings only a small service unavailability reduction. The opposite happens with the TN case, as a router unavailability reduction contributes to up to two orders of magnitude service unavailability drop. In brief, the SDN controller represents a critical element which may deteriorate the end-to-end service availability.

E. Impact of element's component failure intensity

In addition to the impact of the element's unavailability, we investigate the impact of each element components on the overall service unavailability. To this end, we investigate the impact of their relative failure intensities, presented in Table I. We use a scaling factor β_x for $x \in \{\text{HW}, \text{SW}, \text{O\&M}, \text{etc.}\}$, which affects the intensities of the relative element components, e.g., hardware, β_{HW}, software, β_{SW} or operation and management (O&M) etc. Simulations have been carried out by considering a scaling factor β_x that varies within a range spanning: $\beta_x \in \{10^{-i}\}$ for $i = -1, 0, 1$. For each simulation, we vary β_x while keeping the rest of the parameters as defined in Table I. Note that intensity variations are done one at a time.

Driven by the previous results, we present the sensitivity analysis of only the noteworthy components of the most critical elements, i.e., IP routers, VNFs, SDN switches, and SDN controller. Figure 12 shows the end-to-end service unavailability when varying the scaling factor of the most relevant failure intensities of those elements, for the TN and SDN *Reference* deployments with and without redundant elements.

For the non-redundant deployments, the largest impact on the service unavailability is due to the router and SC O&M failure intensity increments and such impact is similar for both TN and SDN deployments. On the other hand, when the O&M failure intensity decreases, a much larger relative gain is obtained by the SC compared to routers. The VNF software

TABLE IV
DISTRIBUTION OF PRINCIPAL-CUT SETS FOR THE DIFFERENT NFV ELEMENT PLACEMENTS AND THEIR RELATIVE SERVICE UNAVAILABILITY.

	C_1	C_2	C_3	C_4	Service Unavailability*	Reduction %
Reference	5	63	16	0	$2.953 \cdot 10^{-3}$	
Core	5	39	8	0	$2.443 \cdot 10^{-3}$	17.27%
SDN Reference	6	74	20	0	$1.218 \cdot 10^{-2}$	
SDN Core	6	50	8	0	$1.210 \cdot 10^{-2}$	0.65%
All redundant	0	35	122	414	$6.332 \cdot 10^{-4}$	
All redundant Core	0	35	73	97	$6.310 \cdot 10^{-4}$	0.34%
SDN All redundant	0	43	122	415	$2.264 \cdot 10^{-4}$	
SDN All redundant Core	0	43	69	122	$2.260 \cdot 10^{-4}$	0.17%

*Calculated with the element's baseline unavailabilities

presents a larger impact compared to the VNF VM component and such gain is slightly more pronounced for the TN case. This result is somehow expected since the VNF software failure intensity is much smaller than the VM intensity, while a reduction of the software intensity, i.e., $\beta_{\text{VNF}_{\text{SW}}} = 10^{-1}$, does not give a significant effect.

Regarding the redundant deployments, similarly to the previous outcomes, any increase on the VNF components failure intensity is suppressed by the redundancy protection. On the other hand, despite the SC is provided with redundancy, a higher O&M failure intensity may considerably degrade the service unavailability by more than one order of magnitude. Similarly, the SDN switch hardware system may play an important role in the overall service availability.

To summarize, for the traditional network, the hardware and O&M systems of routers represent critical components that may greatly impact the service availability. In an SDN network, the SC O&M software and switch hardware may have the largest impact on the end-to-end service availability.

F. Impact of NFV element placement

So far we have considered a presumably worst-case deployment where the NFV elements are placed on the edge of the backbone network. However, one might argue that the placement of the NFVI-PoPs, MANO and SDN controller, may significantly impact the service availability. To shed light on this, we examine the case where NFV elements, with and without redundancy, are deployed in the network nodes having the highest betweenness centrality [33]. These nodes are $\{23, ..., 28\}$ and represent the set of nodes that have the highest number of times they appear in the shortest path of any two other nodes. Figure 13 illustrates the TN and SDN-enabled NFV deployments for both redundant and non-redundant cases. A similar placement may be driven by the need of an operator to limit the service delay and/or the eventual additional path stretch due to the failover on the redundant element. The same notation, representing the previous use cases, followed by *Core* is used to identify the cases where the NFV elements are placed in the core nodes. To illustrate, *Core* represents the case of a traditional network with no redundant NFV elements and VNFs are running in the same NFVI-PoP. The MANO and the NFVI-PoP are connected to central nodes as depicted in Figure 13 (solid contour).

Table IV presents the distribution of the principal-cut sets for both the *Reference* and *Core* deployments together with their respective service unavailabilities. Observing the

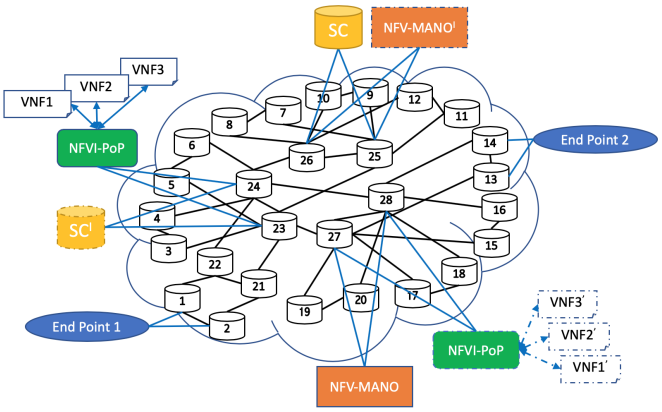


Fig. 13. SDN-integrated NFV deployments with NFVI-PoPs, MANO and SDN controller placed in the nodes with the highest betweenness centrality.

principal-cut sets for the non-redundant configurations, the *Core* deployments present a significant decrease in the number of minimal-cut sets of high cardinality suggesting that the service will be less vulnerable compared to the *Reference* cases. Despite this reduction, a minor decrease is achieved only for the TN deployment where the service unavailability is 17% less than the *Reference* deployment. This is because, given the element's baseline availabilities, on the *inclusion-exclusion principle*, the most impactful principal-cut sets, i.e., C_1, are not changed and the contributions from the other cardinalities are much smaller. In the SDN-enabled case, the service reduction is almost none and this can be explained by the fact that the SDN controller, being a crucial element, is still present in first cardinality sets which mostly impact the service unavailability. A similar trend is evidenced for the redundant cases where despite the principal-cut sets are more than halved, the service unavailability reduction is rather insignificant as a result of the fact that the lower cardinality sets C_2 remain unchanged. In addition to the *Core* deployment, we examined also the case where the MANO, PoP and SC are attached to the same two networking nodes having the highest betweenness centrality, i.e., nodes 23 and 24. We noticed that even in this deployment, the availability increase is not significant. Specifically, the unavailability is $1.208 \cdot 10^{-2}$ vs. $1.21 \cdot 10^{-2}$ of the *SDN Core*. This result is further evidence that it is the SC which brings a significant effect on the service availability regardless of the placement. To conclude, the placement of the NFVI-PoPs, MANO and SDN controller has a minimal effect on the overall service availability for the non-redundant architecture and almost none for the redundant architecture.

VII. CONCLUDING REMARKS

A comprehensive approach for the evaluation of end-to-end NFV-based service availability has been proposed. Through the formalized *two-level* availability model, we are able to capture both network topology structural dependencies and failure dynamics of the individual elements involved in the end-to-end service delivery. In addition, an extensive sensitivity analysis, for several case studies including traditional and SDN-integrated networks, aiming at identifying the main

critical elements has been carried out. The main outcomes include the following:

- in case a traditional network is employed, the most impactful elements are represented by the IP routers and VNFs composing the SFC. Adopting less robust routers and VNFs, compared to their baseline availabilities, may reduce the end-to-end service availability up to two orders of magnitude. Despite a small gain is obtained for more available routers and VNFs, adopting much more available routers and VNFs does not gain accordingly;
- deploying the VNFs into multiple or separate NFVI-PoPs does not significantly affect the service unavailability. In addition, the placement of the NFVI-PoPs, MANO and SDN controller does not reflect a remarkable impact;
- applying redundancy to NFV elements further decreases the service unavailability and brings adequate protection to any eventual increase of their unavailabilities. In addition, when such elements are redundant, making use of more robust router devices allows the service to reach target values like 5-nines availability;
- compared to a traditional network, an SDN-integrated solution brings additional challenges reflected in lower service availability. In an SDN network, the SDN controller is the most critical element which could even inhibit the advantages brought by the redundancy of the NFV elements. On the other hand, adopting a redundant SDN controller further decreases the service unavailability compared to a traditional network with redundant NFV elements;
- from an element's component perspective, the service is mostly affected by the router hardware and O&M failure intensity variations for both redundant and non-redundant NFV element deployments. Similarly, for an SDN-integrated network, high intensity of SC O&M software and switch hardware failures may significantly degrade the service unavailability.

To summarize, deploying redundant NFV elements like VNFs, MANO, and NFVI-PoPs contributes in lower service unavailability but network elements like IP routers may either severely degrade or significantly increase the overall service availability. Therefore, if 5-nines target figures are to be expected, in addition to NFV redundant elements, more reliable router hardware and O&M software architectures need to be employed.

REFERENCES

[1] G. N. ETSI, "Network Functions Virtualisation (NFV): Architectural Framework," *ETSI GS NFV*, vol. 2, no. 2, p. V1, 2013.

[2] ETSI, "Reliability; Report on Models and Features for E2E Reliability," ETSI, Tech. Rep. GS REL 003 v1.1.2, 2016-07.

[3] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.

[4] N.-I. ETSI, "Network Functions Virtualisation (NFV); Network Operator Perspectives on NFV priorities for 5G," Tech. Rep., 2017.

[5] B. Han, V. Gopalakrishnan, G. Kathirvel, and A. Shaikh, "On the resiliency of virtual network functions," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 152–157, 2017.

[6] R. Mijumbi *et al.*, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, 2016.

[7] K. S. Trivedi and A. Bobbio, *Reliability and availability engineering: modeling, analysis, and applications*. Cambridge Univ. Press, 2017.

[8] A. Gonzalez *et al.*, "Service availability in the NFV virtualized evolved packet core," in *GLOBECOM, 2015 IEEE*. IEEE, 2015, pp. 1–6.

[9] M. Di Mauro *et al.*, "Ip multimedia subsystem in an nfv environment: availability evaluation and sensitivity analysis," in *2018 IEEE NFV-SDN*. IEEE, 2018, pp. 1–6.

[10] B. Tola, G. Nencioni, B. E. Helvik, and Y. Jiang, "Modeling and evaluating nfv-enabled network services under different availability modes," in *2019 15th International Conference on the Design of Reliable Communication Networks (DRCN)*, March 2019, pp. 1–5.

[11] N. ETSI, "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework," Tech. Rep., 2015.

[12] ITU-T E.860 (06/02), "Framework of a service level agreement," 2002.

[13] ETSI, "Network Functions Virtualisation, An Introduction, Benefits, Enablers, Challenges & Call for Action," *White Paper*, no. 1, pp. 1–16, 2012.

[14] D. S. Kim, F. Machida, and K. S. Trivedi, "Availability modeling and analysis of a virtualized system," in *Dependable Computing, 2009. PRDC'09. 15th IEEE Pacific Rim International Symposium on*. IEEE, 2009, pp. 365–371.

[15] R. d. S. Matos *et al.*, "Sensitivity analysis of server virtualized system availability," *IEEE Transactions on Reliability*, vol. 61, no. 4, pp. 994–1006, 2012.

[16] D. S. Kim *et al.*, "Availability modeling and analysis of a virtualized system using stochastic reward nets," in *Computer and Information Technology (CIT), 2016 IEEE International Conference on*. IEEE, 2016, pp. 210–218.

[17] M. Di Mauro *et al.*, "Service function chaining deployed in an NFV environment: An availability modeling," in *2017 IEEE CSCN*. IEEE, 2017, pp. 42–47.

[18] ——, "Availability modeling and evaluation of a network service deployed via NFV," in *International Tyrrhenian Workshop on Digital Communication*. Springer, 2017, pp. 31–44.

[19] J. M. Halpern and C. Pignataro, "Service Function Chaining (SFC) Architecture," RFC 7665, Oct. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc7665.txt

[20] I. N. ETSI, "ETSI GS NFV-REL 001 v1. 1.1: Network Functions Virtualisation (NFV); Resiliency Requirements," 2015.

[21] ——, "ETSI GR NFV-REL 007 v1.1.2: Network Function Virtualisation (NFV); Reliability; Report on the resilience of NFV-MANO critical capabilities," 2017.

[22] G. Nencioni *et al.*, "Availability modelling of software-defined backbone networks," in *DNS Workshop, 2016 46th Annual IEEE/IFIP International Conference on*. IEEE, 2016, pp. 105–112.

[23] P. Vizarreta *et al.*, "Qos-driven function placement reducing expenditures in NFV deployments," in *Communications (ICC), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1–7.

[24] H. Zhu and C. Huang, "Availability-aware mobile edge application placement in 5G networks," in *IEEE GLOBECOM*, 2017, pp. 1–6.

[25] M. Rausand and A. Høyland, *System reliability theory: models, statistical methods, and applications*. John Wiley & Sons, 2004, vol. 396.

[26] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: Formal definitions and concepts," in *Lectures on Formal Methods and Performance Analysis*, ser. Lecture Notes in Computer Science, vol. 2090. Springer, 2001, pp. 315–343.

[27] "Möbius: Model-based environment for validation of system reliability, availability, security and performance," "https://www.mobius.illinois.edu", Accessed: 2019-03-31.

[28] G. Nencioni, B. E. Helvik, and P. E. Heegaard, "Including failure correlation in availability modeling of a software-defined backbone network," *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1032–1045, Dec 2017.

[29] D. Cotroneo, L. De Simone, and R. Natella, "NFV-bench: A dependability benchmark for network function virtualization systems," *IEEE Trans. on Network and Service Management*, vol. 14, no. 4, pp. 934–948, 2017.

[30] N. F. S. de Sousa, D. A. L. Perez, R. V. Rosa, M. A. Santos, and C. E. Rothenberg, "Network service orchestration: A survey," *Computer Communications*, vol. 142-143, pp. 69 – 94, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366418309502

[31] "Open Baton: An open source reference implementation of the ETSI NFV MANO specification," "http://openbaton.github.io", Accessed: 2019-03-31.

[32] A. L. Williamson, "Discrete event simulation in the mobius modeling framework," Master's thesis, University of Illinois at Urbana-Champaign, 1998.

[33] L. C. Freeman, “A set of measures of centrality based on betweenness,” *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977. [Online]. Available: http://www.jstor.org/stable/3033543

Besmir Tola received the M.Sc. degree in Electronics and Telecommunication Engineering from the University of Siena (Italy) in 2014. In autumn 2015, he joined the IIK department at the Norwegian University of Science and Technology (NTNU) as a Ph.D. candidate in Telematics. In 2016 and 2018, he was a visiting researcher at the Nokia Bell Labs in Stuttgart (Germany), and UNINETT (Norwegian National Research and Education Network Operator), respectively, where he worked on dependability modeling and failure data processing, and analysis of cloud computing infrastructures and services. His current research interests include performance and dependability analysis of Cloud Computing, SDN, and NFV architectures.

Gianfranco Nencioni received the M.Sc. degree in Telecommunication Engineering and the Ph.D. degree in Information Engineering from the University of Pisa, Italy, in 2008 and 2012, respectively. In 2011, he was a visiting Ph.D. student with the Computer Laboratory, University of Cambridge, U.K. He was a Post-Doctoral Fellow with the University of Pisa from 2012 to 2015 and the Norwegian University of Science and Technology, Norway, from 2015 to 2018. He is an Associate Professor with the University of Stavanger, Norway, from 2018. His research activity regards modelling and optimization in emerging networking technologies (e.g., SDN, NFV, 5G, Network Slicing). His past research activity has been focused on energy-aware routing and design in both wired and wireless networks and on dependability of SDN and NFV.

Bjarne E. Helvik (1952) received his Siv.ing. degree (MSc in technology) from the Norwegian Institute of Technology (NTH), Trondheim, Norway in 1975. He was awarded the degree Dr. Techn. from NTH in 1982. He has since 1997 been Professor at the Norwegian University of Science and Technology (NTNU), the Department of Telematics and Department of information Security and Communication Technology. In the period 2009 – 2017, he has been Vice Dean with responsibility for research at the Faculty of Information Technology and Electrical Engineering at NTNU. He has previously held various positions at ELAB and SINTEF Telecom and Informatics. In the period 1988-1997 he was appointed as Adjunct Professor at the Department of Computer Engineering and Telematics at NTH.

His field of interests includes QoS, dependability modelling, measurements, analysis and simulation, fault-tolerant computing systems and survivable networks, as well as related system architectural issues. His current research is on ensuring dependability in services provided by multi-domain, virtualised ICT systems, with activities focusing on 5G and SmartGrids.