Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Hanne Randal Vikre

Analysis of MANO design approaches with respect to dependability in a 5G isolated sliced environment.

Master's thesis in Communication Technology
Supervisor: Bjarne Emil Helvik
June 2020

NTNU
Norwegian University of Science and Technology

Hanne Randal Vikre

Analysis of MANO design approaches with respect to dependability in a 5G isolated sliced environment.

Master's thesis in Communication Technology
Supervisor: Bjarne Emil Helvik
June 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU

Kunnskap for en bedre verden

Title: Analysis of MANO design approaches with respect to dependability in a 5G isolated sliced environment.

Student: Hanne Randal Vikre

Problem description:

The fifth generation (5G) networks will be a significant innovative step for communication. An important element of 5G is network slicing, where multiple logical networks concurrently run on top of a common network infrastructure. Although the slices utilise the same physical infrastructure, each slice should be able to operate without any influence caused by activity in other slices. This is defined as the isolation property of the slice.

One of the benefits of 5G and network slicing is that each slice can be tailored to specific requirements. One aim is to be able to flexibly distribute the physical resources across the slices, ensuring better utilisation of network resources. A high level of slice isolation will demand more dedicated physical resources, reducing the flexibility of the system with regards to resource sharing between slices. On the other hand, a low level of isolation might reduce the operators ability to meet the reliability requirements of the slice.

The management and orchestration entity is responsible for the slicing and isolation between the slices. Many papers are based on the ETSI NFV-MANO architecture for management and orchestration. This architecture was developed by an ETSI working group, and there exist several papers which try to extend its features. Although efforts have been put into developing a management and orchestration system for 5G, it is still an open question how the final architecture of such a system will look like. One of the questions is whether the management and orchestration system should be flat or hierarchical. Different structures could have consequences for the dependability of the 5G network.

The aim of this master's thesis is to analyze how different approaches of designing distributed MANO can influence the dependability in a 5G isolated sliced environment. Qualitative methods will be used to identify the main dependability challenges of relevant topologies.

Responsible professor: Bjarne E. Helvik, IIK

Supervisor: Bjarne E. Helvik, IIK

Abstract

The fifth generation (5G) of mobile technology is envisioned to be a significant step in the evolution of communication technology. One of the important components of a well functioning sliced 5G system is its management and orchestration system. As 5G is expected to play an important role in several critical sectors, it is significant to explore potential dependability challenges such a system might have.

The aim of this thesis is to present the current state of the management and orchestration in 5G systems, and based on this perform an analysis of dependability challenges different architectural designs of the management and orchestration system might have. Two main categories of architectures were identified: the flat and the hierarchical. The analysis is qualitative and based on depends-upon graphs that have been developed after analysing multiple architectural proposals for 5G management and orchestration systems.

As a standardised architecture for 5G management and orchestration is still to be agreed upon, this paper serves as an initial step towards assessing dependability concerns through a qualitative analysis. Results from the analysis indicate that there are positive and negative consequences for both of the analysed architectures, and much will still be dependent on implementation choices. A hierarchical architecture might enable easier coordination both of resource utilisation and isolation capabilities as it has a central overarching orchestrator entity. On the other hand, this entity might become a potential single point of failure if it were to be mis-operated or unavailable. The flat architecture provides multiple such orchestrator entities and thus provides some redundancy. The coordination might be more challenging as several such entities need to cooperate. Suggestions for future work are provided in the final conclusion.

Sammendrag

Den femte generasjonen (5G) av mobilteknologi er tenkt å være et viktig steg i utviklingen av kommunikasjonsteknologi. En av de viktige komponentene i et velfungerende 5G-system er dets administrasjons og orkestreringssystem. Siden 5G forventes å ha en viktig rolle i flere kritiske sektorer, er det viktig å utforske potensielle pålitelighetsutfordringer et slikt system kan ha.

Målet med denne oppgaven er å presentere dagens situasjon for administrasjon og orkestrering i 5G-systemer. Basert på dette vil det utføres en analyse av pålitelighetsutfordringer forskjellige arkitekturelle design av administrasjons og orkestreringssystem kan ha. To hovedkategorier for arkitekturer ble identifisert: flat og hierarkisk. Analysen er kvalitativ og basert på depends-upon grafer som er utviklet etter analyse av flere arkitekturelle forslag for 5G administrasjons og orkestreringssystem.

Ettersom det fortsatt trenger å bli enighet om en standardisert arkitektur for 5G administrasjon og orkestrering, fungerer denne oppgaven som et første skritt mot å vurdere pålitelighetsutfordringer gjennom en kvalitativ analyse. Resultater fra analysen indikerer at det er positive og negative konsekvenser for begge de analyserte arkitekturene, og mye vil fremdeles være avhengig av implementeringsvalg. En hierarkisk arkitektur kan gi enklere koordinasjon av både ressursutnyttelse og isolasjonsevner ettersom den har en sentral overordnet orkestratorentitet. På den andre siden kan denne enheten potensielt bli et enkeltpunkt for feiling om den skulle operere feil eller bli utilgjengelig. Den flate arkitekturen har flere orkestratorenheter og kan dermed gi mer redundans. Koordinasjonen i en flat arkitektur kan vise seg å bli mer utfordrende ettersom flere slike entiteter må samarbeide. Forslag til fremtidig arbeid er inkludert i den endelige konklusjonen

Preface

This thesis serves as the final contribution to my Master of Science degree in Communication Technology at the Norwegian University of Science and Technology (NTNU).

First and foremost I would like to thank my supervisor Bjarne E. Helvik for the valuable help, guidance and support I have received throughout this semester.

I would also like to thank my family and friends for their support and encouragement during my five years in Trondheim.

Contents

List of Figures

List of Acronyms

3GPP Third Generation Partnership Project.

5GPPP 5G Infrastructure Public Private Partnership.

B2B Business to Business.

B2C Business to Customer.

BSS Business Support System.

dO Domain Orchestrator.

E2E End-to-End.

EMBB Enhanced Mobile Broadband.

EMS Element Management System.

ETSI European Telecommunications Standards Institute.

MANO Management and Orchestration.

MdO Multi-domain Orchestrator.

MMTC Massive Machine-Type Communications.

NF Network Function.

NFV Network Function Virtualisation.

NFVI NFV Infrastructure.

NFVO NFV Orchestrator.

NGMN Next Generation Mobile Networks.

OSS Operations Support System.

P2P Peer-to-Peer.

QoS Quality of Service.

SDN Software Defined Networking.

SLA Service Level Agreement.

TdC Technical Domain Controller.

URLLC Ultra-Reliable and Low-Latency Communication.

VIM Virtualised Infrastructure Manager.

VNF Virtualised Network Function.

VNFM VNF Manager.

Chapter 1
Introduction

This chapter seeks to provide a brief introduction of the motivation and objectives of the thesis. It also presents a short overview of the applied methodology. Lastly, the rest of the thesis is outlined.

1.1 Motivation

The fifth generation of mobile technology (5G) is currently under development, and will be a significant innovative step for communication. 5G will not only connect people, but also interconnect machines and devices. As described by the 5G Infrastructure Public Private Partnership (5G PPP) vision, 5G should support an optimised and more dynamic usage of all distributed resources [Par15]. This increased efficiency of the 5G infrastructure should also allow for substantial cost reductions. One of the important aspects of 5G is that it will be driven by software with a considerable dependence on emerging technologies like Network Functions Virtualisation (NFV) and Software Defined Networking (SDN).

The future 5G network is developed to be able to support very different requirements based on the need of the services running on the network. A way to achieve this is through the concept of network slicing. This entails that multiple logical networks concurrently run on top of a common network infrastructure. Each slice can be configured to cater the requirements of the services running on the slice. This could be essential for a future 5G network where a very high number of devices is expected to be connected. Although the number of use cases that can be provided by the network are many, there are three types of services commonly referred to in literature: Enhanced Mobile Broadband (EMBB), Massive Machine-Type Communications (MMTC) and Ultra-Reliable and Low Latency Communications (URLLC) [Gro17]. All three service types have a very different set of requirements and it would be difficult to define a common architecture ensuring that they are met. With network slicing, each slice could be tailored to the needs of the specific service provided.

Both dependability and isolation are fundamental concepts of a functioning 5G sliced network [All15]. The network is expected to deliver a service reliability higher than 99.999% [Par15], making it crucial to consider dependability from an early stage in the development. Although the slices utilise the same physical infrastructure, each slice should be able to reliably operate without any influence caused by activity in other slices. How to manage this while also ensuring optimal utilisation is a challenging task. It thus seems crucial that both dependability and isolation are considered when developing the new network.

The entity responsible for flexibly allocating the resources between the slices is the Management and Orchestration (MANO) system. The MANO system should be the contact point which translates the requests from the customers into actual network functions and slices [All15]. In order to provide dependable services, it is important to have a proper MANO system in place. There is a need for holistic orchestration so that each slice meets it's service requirements while it also efficiently utilises the available resources [FPEM17].

There seems to have been a limited focus on dependability concerns of 5G, and especially the MANO system, in research. The work that has been performed has mainly focused on availability in the space domain such as [BBZ19] and [ML17]. Others such as [GXG18] have looked at the dependability challenges in a sliced network, but from an overall view and not specifically the MANO entity. Their paper also highlights the need for further studies on the topic. There is thus a motivation to look further into these topics. It would be both interesting and useful to further explore dependability of the 5G MANO system, and look at it from the context of slicing and isolation. Different design approaches of a MANO system could possibly have consequences for the dependability of the 5G network. It can thus be interesting to explore the extent of such potential impacts.

1.2 Objectives

The main objective of this thesis is to identify how different architectural designs of a MANO system can influence the dependability of a 5G isolated sliced environment. This can be divided into three sub-objectives:

- To investigate the state of the art of the 5G MANO system in an isolated sliced network.
- To identify potential architectural designs of the 5G MANO system.
- To analyse dependability challenges of the identified architectures.

1.3 Methodology

The research methodology used in the thesis can be divided into two parts: literature study and analysis. Both will be briefly explained in this section.

1.3.1 Literature Study

The literature study serves as the foundation of the thesis. It has been an important part of the thesis to acquire new knowledge both for establishing the background knowledge of the thesis and to investigate the current state of the art of the MANO system in 5G networks. The study was a central part of identifying functionalities and dependability requirements of the MANO system. These could later be used in the analysis phase. The literature study was also an important part of identifying potential architectural designs of MANO. Papers have been evaluated in order to define the two distinct architectural options that stand out for a 5G MANO system.

A literature study is always subject to potential weaknesses. In this thesis work there is especially a concern when it comes to the selection and interpretation of papers regarding MANO architectural proposals. There is always a possibility of neglecting a paper that should have been included and misinterpreting the intent of the author of a publication. Striving for a trustworthy approach, some elements were adapted from [Kit04]. The systematic review methodology presented in this paper is a bit out of scope for this thesis, but contains some valuable elements. The primary academic search engines used to discover relevant sources were NTNU Oria and Google Scholar. Both can be used for finding academic resources across multiple platforms.

Some criteria were set prior to the selection of sources. As the field of management and orchestration in 5G is subject to rapid changes and developments, it became clear that the date of publication of the sources collected would be of great significance. Sources reviewed were published from 2015 to 2020. It was also decided that sources representing MANO architectures needed to support multi-domain orchestration to be considered relevant for this thesis.

1.3.2 Analysis

For this thesis, a qualitative approach was chosen over a quantitative approach. As there is still no clear consensus on a multi-domain management and orchestration system for 5G, it would be challenging to build relevant quantitative models with low uncertainty. By performing a qualitative analysis, we can gain insight and overview at an early stage.

A qualitative analysis was performed to evaluate the challenges of different MANO architectural designs to achieve dependability requirements. In this thesis depends-upon graphs were utilised to examine the relation between components of 5G MANO. Flavin Cristian introduced the depends-upon graphs in [Cri91] as a mean to understand fault-tolerant distributed systems. The graphs developed in the thesis were meant to serve as a comprehensible and visual support in understanding fault-tolerant MANO systems.

One of the uncertainties this approach faced was with the functionalities of each component within the MANO system. All system component functionalities have not been clearly defined yet, and thus it was necessary to make some assumptions. This could potentially impact the validity of the results. Further discussions on the limitations of the approach chosen can be found in Chapter 5.

1.4 Outline

The thesis has been structured into the following six chapters:

- Chapter 1 gives a short introduction to the motivation and objectives of the thesis. It also presents the applied methods.
- Chapter 2 presents the requisite background concepts and definitions for the thesis. This includes a brief introduction to network slicing, dependability, isolation, Network Function Virtualisation and Management and Orchestration in 5G networks.
- Chapter 3 examines various MANO architectural proposals from scientific papers. The chapter concludes with two abstract architectural options for management and orchestration systems.
- Chapter 4 contains an analysis of how the architectures identified in Chapter 3 may impact the dependability of the 5G sliced network. Potential depends-upon graphs are developed for both architectures before a more thorough analysis is performed.
- Chapter 5 presents a discussion on the findings in Chapter 4, comparing the two architectures. It also includes a discussion of the limitations faced by the chosen method of analysis.
- Chapter 6 concludes the thesis and proposes future areas of work.

Chapter 2
Background

The following chapter provides an introduction to the requisite background concepts and definitions related to 5G slicing, dependability, isolation, Network Function Virtualisation, Software Defined Networking and Management & Orchestration.

2.1 Network Slicing in 5G

Network slicing enables operators to concurrently run multiple logical networks on top of a common network infrastructure. The concept of 5G network slicing was first introduced by the Next Generation Mobile Network (NGNM) Alliance. According to NGNM, a 5G network slice is *composed of a collection of 5G network functions and specific RAT settings that are combined together for the specific use case or business model*[All15]. This means that the slice can span all domains of the 5G network forming a complete instantiated logical network. An example of 5G network slices can be seen in Figure 2.1. The slices are tailored to specific services from smartphones in Slice 1 to autonomous vehicles and massive IoT in Slice 2 and Slice 3 respectively. By dividing the network into separate slices, each slice can be configured to meet the individual needs of the customers. With such diverse services running on the network, the consequences of reduced dependability can vary greatly. For instance, it would be very inconvenient to have reduced availability in the smart phone slice, but it could have fatal consequences for vehicles connected to the autonomous vehicle slice requiring a highly reliable service.

Today, sharing details about one's own network is quite uncommon among the operators. The 5G network, however, calls for multi-operator business, service and resource coordination [HBT16]. There is thus a need for Service Level Agreements (SLA), which are mutual contracts which guarantee that the network will be delivering data using agreed network functions, capabilities and attributes [All15]. It will be important for the operators to fulfil the SLAs and provide dependable networks.

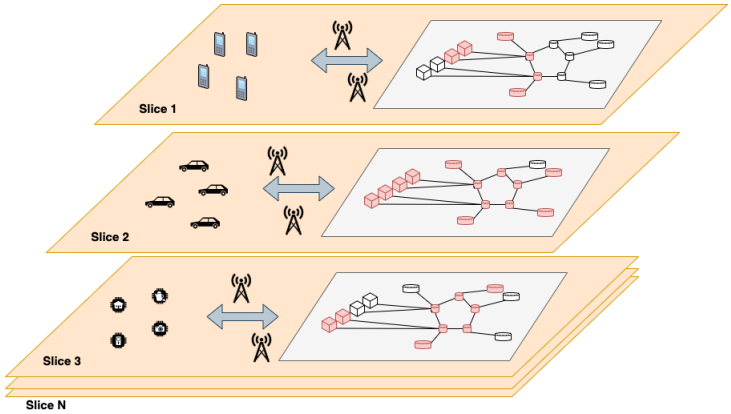


Figure 2.1: 5G network slices implemented on the same infrastructure for different use cases. Adapted from [All15].

2.1.1 Network Function Virtualisation (NFV)

One of the main enablers of 5G network slicing is Network Function Virtualisation(NFV). As described in [MSG+15], the main idea of NFV is the decoupling of physical network equipment from the functions that run on them. Hardware and software are not integrated in NFV, and can thus progress separately from each other. NFV also allows for dynamic network operations, where the operators can scale performance on demand.

Being one of the main components in network slicing, NFV is envisioned to be an important part of the 5G network. The European Telecommunications Standards Institute (ETSI) has lead the standardisation process of NFV technology through their NFV Industry Specification Group (NFV ISG). A significant result of this work is the definition of the ETSI NFV-MANO reference architectural framework as seen in Figure 2.2 [ETS14]. The high-level architecture is comprised of three main functional blocks: NFV Infrastructure (NFVI), Virtual Network Functions (VNFs) and the NFV Management and Orchestration (MANO) framework.

VNFs are software implementations of network functions deployed on virtual environments. NFVI is the environment in which VNFs are deployed. It consists of both hardware and software resources. The NFV MANO framework is responsible for the orchestration and lifecycle management of network services. It consists of three components:

– **NFV Orchestrator (NFVO)** is responsible for the lifecycle management of network services. It also performs resource orchestration across multiple VIMs.

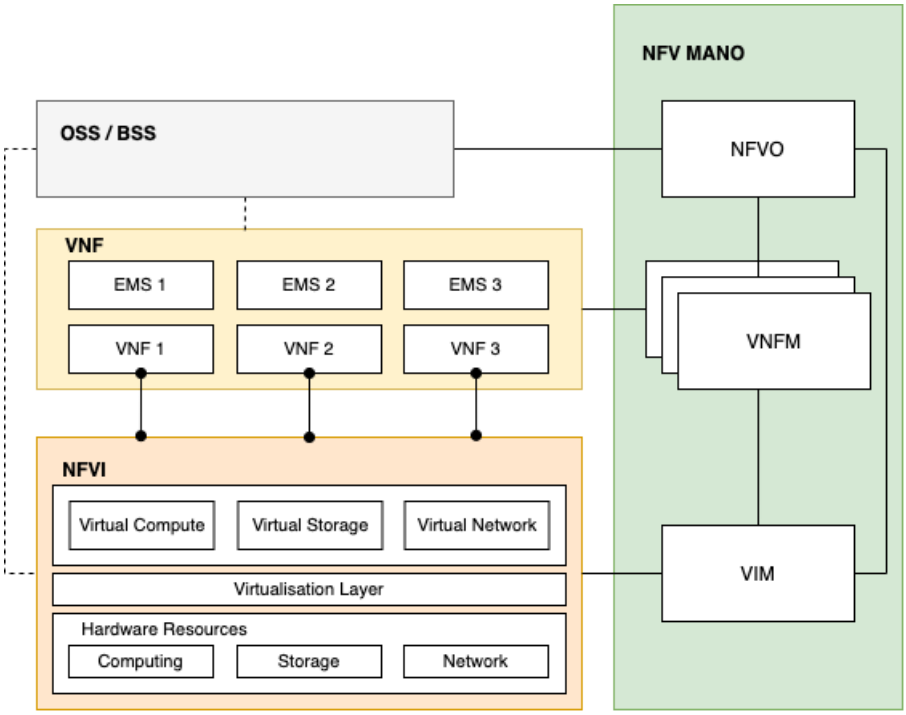


Figure 2.2: NFV Reference Architectural Framework adapted from [ETS14].

The NFVO is thus in close coordination with the VNFMs and the VIMs. The NFVO receives network performance metrics and analyses them to make sure requirements are satisfied.

- **VNF Manager (VNFM)** is responsible for lifecycle management of VNFs.
- **Virtualised Infrastructure Manager(VIM)** manages and controls the NFVI resources. It is responsible for performing resource allocation on behalf of the NFVO and VNFM, and collects information with regards to fault performance.

2.1.2 Software Defined Networking (SDN) and NFV

Another important technological enabler for 5G network slicing is Software Defined Networking (SDN). SDN is defined as the physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices [BAMH20]. By separating the forwarding logic from the network control plane, flexibility is provided with a global view of the entire network. The 5G network slicing

architecture is designed from the foundation of the NFV architecture, integrated with SDN [GXG18].

The integration of SDN and NFV is, however, not an easy task. In [OLAL+17], the authors analyse an ETSI tentative framework to integrate SDN within the reference NFV architecture. In this proposal, two SDN controllers are introduced:

- **Infrastructure SDN controller (IC)** arranges and manages underlying networking resources in order to provide necessary connectivity. The IC is managed by the VIM entity.
- **Tenant SDN controller (TC)** dynamically manages VNFs used to realise network services. It can either be represtented as one of the VNFs or as part of the Network Management System (NMS) which performs the general network management tasks.

2.1.3 Dependability

Dependability is a fundamental part of a functioning 5G sliced network. Guaranteeing dependability has to be a top priority, as 5G networks will be a critical infrastructure in many important sectors [GXG18]. According to NGNM [All15], the 5G network should enable 99.999% network availability. Other 5G advantages will be universal connectivity, extremely low latency, and high-speed data transfer.

The dependability of a system is, as defined by [ALRL04], *its ability to deliver a service that can justifiably be trusted.* The following threats, attributes and means are all adapted from [ALRL04].

There are several threats to a system:

- **Fault** is the hypothesised cause of an error.
- **Error** is the part of the system state that may lead to service failure.
- **Failure** is the event that occurs when the delivered service deviates from correct service.

The relationship between the concepts is as follows: A fault can cause an error, which might lead to a failure. For a system to be considered dependable, the following attributes need to be considered:

- **Availability** is the readiness for correct service.

- **Integrity** is the absence of improper system alterations.
- **Maintainability** is the ability to undergo modifications and repairs.
- **Reliability** is the continuity of correct service.
- **Safety** is the absence of catastrophic consequences on the users and the environment.

It is interesting to notice that addressing security to a large extent overlaps the goal of dependability. Security focuses on the attributes of confidentiality, integrity and availability. The security of a system also faces many of the same overlapping threats. The means to achieve a secure and dependable system can be grouped into four categories:

- **Fault prevention** means to prevent the occurrence or introduction of faults.
- **Fault tolerance** means to avoid service failures in the presence of faults.
- **Fault removal** means to reduce the number and severity of faults.
- **Fault forecasting** means to estimate the present number, the future incidence, and the likely consequences of faults.

2.1.4 Isolation

Isolation is an important aspect of network slicing. 5G network slices are expected to run concurrently on top of a shared infrastructure without affecting each other. A network slice can be fully or partly isolated from other slices, both logically and physically [All19]. It is important that a slice does not interfere with the traffic in other slices.

The common infrastructure is composed of resources that may be owned and managed by different administrative domains [ETS17]. The level of trust between these administrative domains can vary, and it is thus of significant importance to be able to ensure full mutual isolation among slices. This can mean that dedicated resources need to be used. This might, however, lead to inefficient network resource utilisation.

Different architectural proposals can have different implications for the isolation of slices. Full isolation of MANO of each slice makes it easier to guarantee resources and thus fulfil SLA and Quality of Service (QoS) requirements. On the other hand it gives less flexibility and control of the resources [NGG+18]. Less isolation and a global MANO view can lead to a better utilisation of resources as well as more flexibility with regard to failure handling.

2.2 Management and Orchestration in the 5G Network

Management and orchestration is a crucial part of establishing and functioning a sliced network. How best to structure the management and orchestration in the future 5G network has received significant attention. Despite this, there has yet to be agreed upon a common definition of 5G network slicing [RBM+19]. This also means that the relationship between the slicing system and the management and orchestration system is still not clearly defined. One of the challenges with orchestration in the 5G environment is that the slice-based services will need communication between different administrative and technological domains to be able to provide End-to-End (E2E) slices.

2.2.1 Single- and Multi-domain MANO

In a single domain, the orchestrator is responsible for and has full control of all services and resources within its domain. The scope of the single-domain orchestrator is limited to a specific technological and administrative domain. A multi-domain orchestrator is more complex, as information has to be exchanged across multiple technological and administrative domains. As described by [DJEG20] the 5G network infrastructure can be owned and managed by various administrative entities. Guaranteeing E2E service delivery is thus a difficult task, both because of the multiple administrative domains and the interaction between multiple heterogeneous technologies. Building a complete E2E 5G network will require merging together services by multiple technological and administrative domains. In a distributed management approach, multiple orchestrators work together to manage the system. There thus needs to be some sort of coordination between the orchestrators in order to ensure E2E services. The coordination between orchestrators needs to be optimal in order to offer a dependable network, as issues in one domain can affect the overall quality of service provided.

2.2.2 MANO Standardisation Efforts

Management and orchestration in 5G networks has received attention from several standardisation organisations. The 5GPPP summarises the efforts of the Third Generation Partnership Project (3GPP) and ETSI, combining the two views and deriving at a consensus meta architecture [RBM+19]. The work to combine the ETSI and 3GPP views is not over yet, and considerable effort is still necessary to put the views into perspective. One of these efforts was done in [ETS17] where there was a mapping between NFV and 3GPP network slicing concepts. In 3GPP work, a network slice contains one or more network slice subnets. A NFV Network Service can be regarded as a resource-centric view of a network slice, as long as the network slice contains at least one VNF. A network slice subnet instance can be shared by

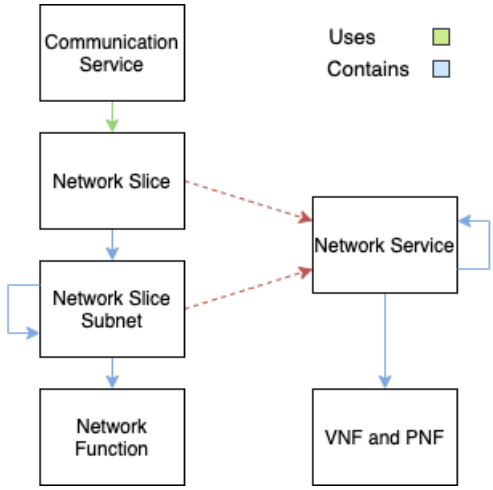


Figure 2.3: Mapping between 3GPP Network Slice (left) and ETSI VNF Network Service (right) adapted from [ETS17].

multiple network slice instances. The mapping between the 3GPP network slice and the ETSI VNF network service is visualised in Figure 2.3.

As stated in [RBM+19], the ETSI NFV components are typically still used at a high level in many architectural suggestions. The support for slices varies between architectures, with some of them incorporating slice management directly into the NFVO and some implementing a separate slice manager unit. The ETSI NFV-MANO framework is frequently used to orchestrate network services (NSs), but reaches limitations when it comes to management and orchestration of E2E slices [GXG18]. Many proposed architectures for MANO are thus based on the ETSI NFV-MANO components, but extends the architecture to achieve E2E support.

2.2.3 Functional Requirements

Through an analysis of industry and standardisation resources, [BAMH20] has identified requirements for an E2E 5G MANO system. The requirements include flexibility, customisation, simplification, exposure, elasticity, cloudification, legacy support, lifecycle management, automation, isolation and multi-domain and multi-tenant support.

Several standardisation organisations discuss the MANO entity's role with regards to 5G slicing [GPCM+16]. Many view it as a contact point between the tenant use case requests and the implementation of the actual slices. This entails life cycle management of the slices, including creation, update, deletion and operation of the

slice.

In general the MANO system is responsible for managing and orchestrating in three different levels of abstraction: The Service Level, the Network Function Level and the Infrastructure Level [FPEM17]. The terminology for each level differs between papers and organisations.

2.2.4 Dependability Requirements

In [GXG18], the authors aim to define policies that assure the dependability of the slicing architecture in 5G. One of the most fundamental aspects is avoiding Single Point-of-Failure of the MANO. Failure in one element should not produce unavailability of the whole MANO. Whether the components are stateless or stateful should also be considered, as stateful components will need special consideration with regards to synchronisation. Lastly, the MANO and the managed systems need to be designed in Failure-Independent Domains. This implies that a failure in one domain does not cause disturbances in another domain.

Chapter 3
Management and Orchestration Architectures

In this chapter, we analyse various MANO architectural proposals and map them into the two categories: hierarchical and flat. From the analysed proposals, an abstract architecture of these two categories is presented and explained.

3.1 Characterisation of MANO Architectural Proposals

There are several ways to characterise a management and orchestration system in a 5G sliced network. In such a network there needs to be a resource negotiation between the different administrative domains. In the scope of this thesis we will focus on the architectural aspect of this negotiation. In order to analyse how different architectural approaches can influence the dependability of the system, it is necessary to derive some differentiating characteristics. According to [ATS+18] and [RBM+19] there are two distinct options that stand out: The hierarchical and the flat architectures.

Hierarchical organisation

In a hierarchical model, the orchestrators are organised into two or more levels. While the base layer orchestrators work within their domains, the higher layer orchestrators are responsible for the service orchestration across multiple orchestrators at lower layers. Communication between orchestrators is vertical, with no communication between units on the same layer. The higher-level orchestrator is, as described by [ATS+18], capable of acquiring and negotiating resources from different underlying domains. It thus needs to have some sort of global view of the network. As noted by [RBM+19], a hierarchical approach seems to be quite popular in current discussions. There are, however, some concerns of scalability issues and how to ensure isolation. A hierarchical approach enables the direct application of the ETSI NFV-MANO system for a single domain [KNS+18], which can then be coordinated by an overarching entity.

[TASY19] proposes a multi-domain network slicing orchestration architecture

which can be classified as hierarchical. The architecture is presented in Figure 3.1. It introduces a Service Broker which obtains abstracted service capability information from the administrative domains. Through this a global view of the service support is created. The Service Broker communicates with the Multi-Domain Service Conductor Plane. This plane is in charge of service orchestration and management across federated resources. Its two main components are the Service Conductor and the Cross-domain Slice Coordinator. The Service Conductor decomposes a slice request toward different administrative domains and chooses the combination of domains to fulfil the slice request. The Cross-domain Slice Coordinator is instantiated by the Service Conductor. It monitors, manages and controls resources and serves as a mediator among federated resources compensating potential performance degradation by allocating and re-adjusting domain specific resources. The Cross-domain Slice Coordinator interacts with the Fully-Fledged Network Slice Orchestration Plane. This plane allocates internal domain resources for establishing a federated Network Slice Instance. It consists of four blocks: The Service Management, the Slice Life-Cycle Management, the Sub-domain Connectivity Control and the Sub-domain NFV MANO. The resources being controlled belong to the Sub-domain Infrastructure Plane which consists of all the physical and virtual infrastructure.

[KNE16] propose a multi-domain orchestration architecture for NFV as seen in Figure 3.2. The proposal also supports the concept of network slicing. The architecture includes a multi-domain orchestrator (MdO) entity which has the overall responsibility for the services offered as well as the coordination of resources in all of the available domains. The proposal follows an hierarchical organisation, with the MdO working from a higher level to organise the domain orchestrators on the lower level. There is no apparent communication between the domain orchestrators.

In [SMY+19], Sciancalepore et al. propose an architecture which extends the standard ETSI NFV MANO system as seen in Figure 3.3. The proposal is a multi-domain solution, which introduces coordination between the different MANO systems through an over-arching entity called the Inter-slice Resource Broker (ISRB). Independent MANO stacks are deployed on each single infrastructure domain and connected to the ISRB. From a technical perspective the ISRB should have a general view of the whole offered infrastructure within a single administrative domain. To make this possible from a business perspective, the various administrative domains need to reach an agreement.

The paper by Gonzalez et al. [GXG18] is not an architectural proposal. Nevertheless, it mentions how an E2E slice may consist of several network services that are being orchestrated by NFV-MANO. It is thus necessary with an additional E2E Orchestrator (E2EO) which connects to all domain orchestrators. Such an E2EO would be responsible for both intra-slice E2E management and inter-slice

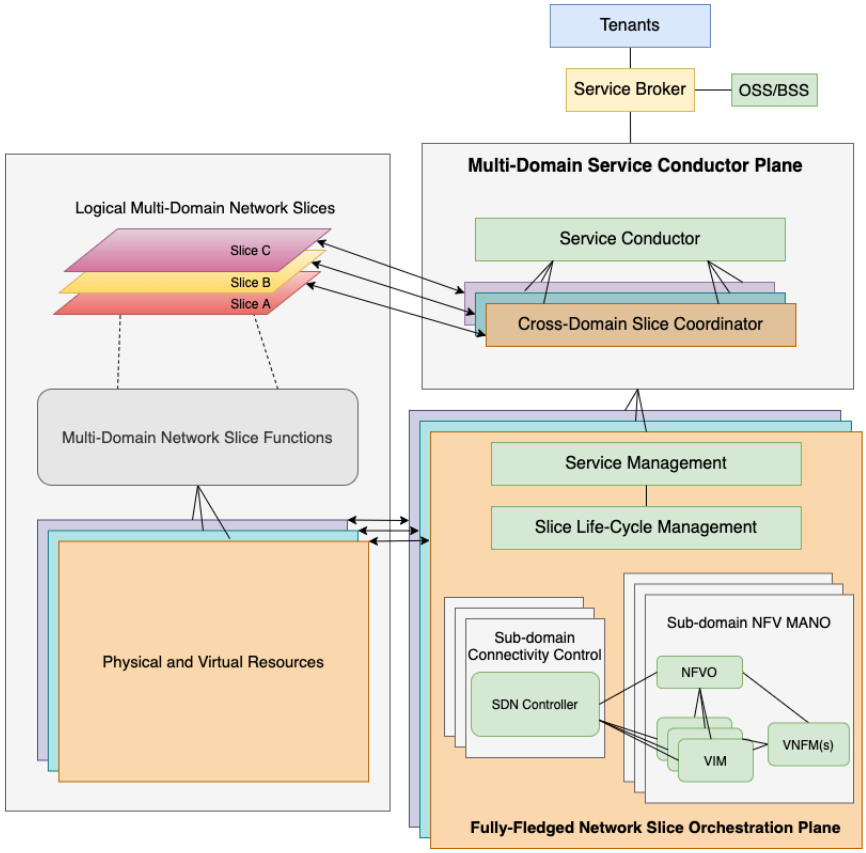


Figure 3.1: Taleb et al. proposed multi-domain network slicing orchestration architecture. Adapted from [TASY19].

management. The E2EO would thus provide multi-domain management support as seen in Figure 3.4 through an hierarchical organisation with the E2EO orchestrating from the top layer.

The 5G!Pagoda project leverages the ETSI NFV architecture in their architectural proposal [AKB+17] which can be seen in Figure 3.5. The architecture consists of domain-specific slice orchestrators that are bound together by a multi-domain slice orchestrator (MdO) which is responsible for the E2E management. The MdO communicates with the domain-specific slice orchestrators to be able to create cross-domain slices with resources allocated in each of the administrative domains. Within each administrative domain there can be different technological domains that are orchestrated by their own Resource Orchestrator (RO). On top of the technology specific ROs, there is an administrative domain RO which aggregate all the resources

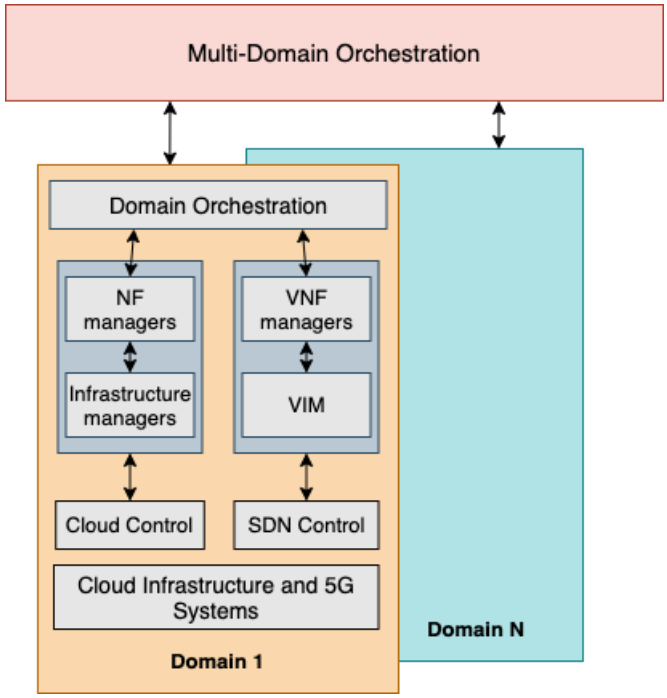


Figure 3.2: Katsalis et al. multi-domain orchestration architecture proposal adapted from [KNE16].

and make the network resources transparent to the domain-specific slice orchestrator. The proposed architecture follows a hierarchical approach, with the higher level MdO coordinating between the different administrative domains.

Flat organisation

Flat organisation uses horizontal peer to peer (P2P) communication between orchestrators. There is no central actor all the orchestrators have to go through in order to communicate and share resources. Instead the orchestrators from different domains are directly linked. Providers are free to request resources and services from each other.

As a part of the 5GEx project, Guerzoni et al. [GVPC+17] present a reference architectural framework for E2E management and orchestration in multi-domain environments. The architecture extends the concept of the ETSI NFV architecture and is split into three layers: the resource domain layer, the single domain orchestration layer and the multi-domain orchestration layer. In Figure 3.6 we see that the lower layer resources are exposed to the single domain orchestration layer. In

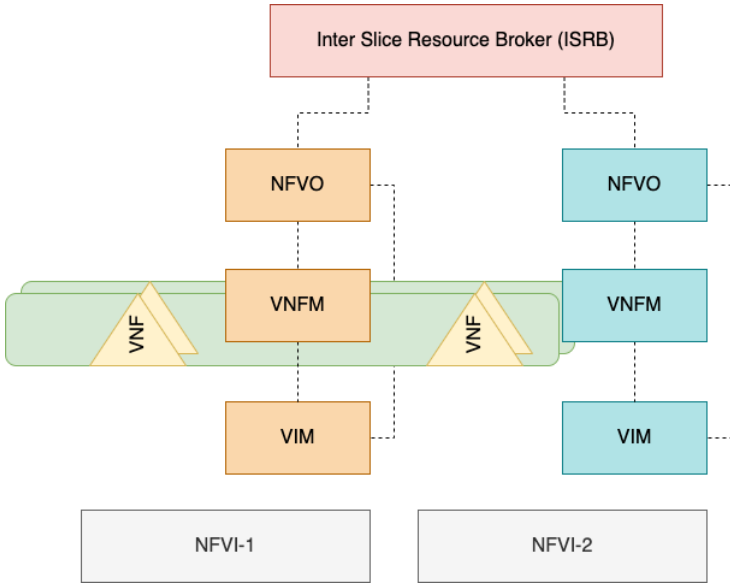


Figure 3.3: Sciancalepore et al. proposal for multi-domain MANO architecture. Adapted from [SMY+19].

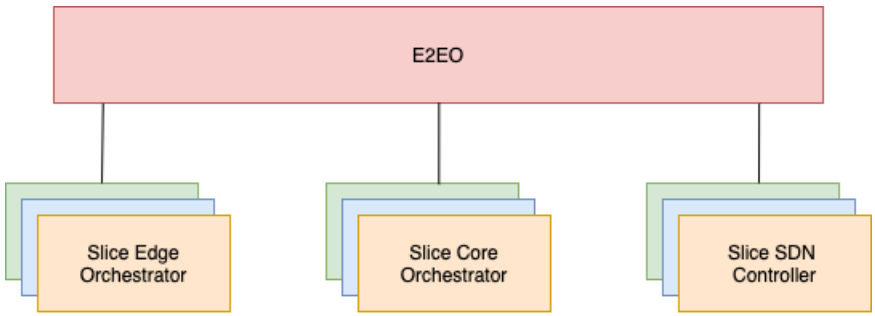


Figure 3.4: E2EO hierarchically connected to domain orchestrators. Figure adapted from [GXG18].

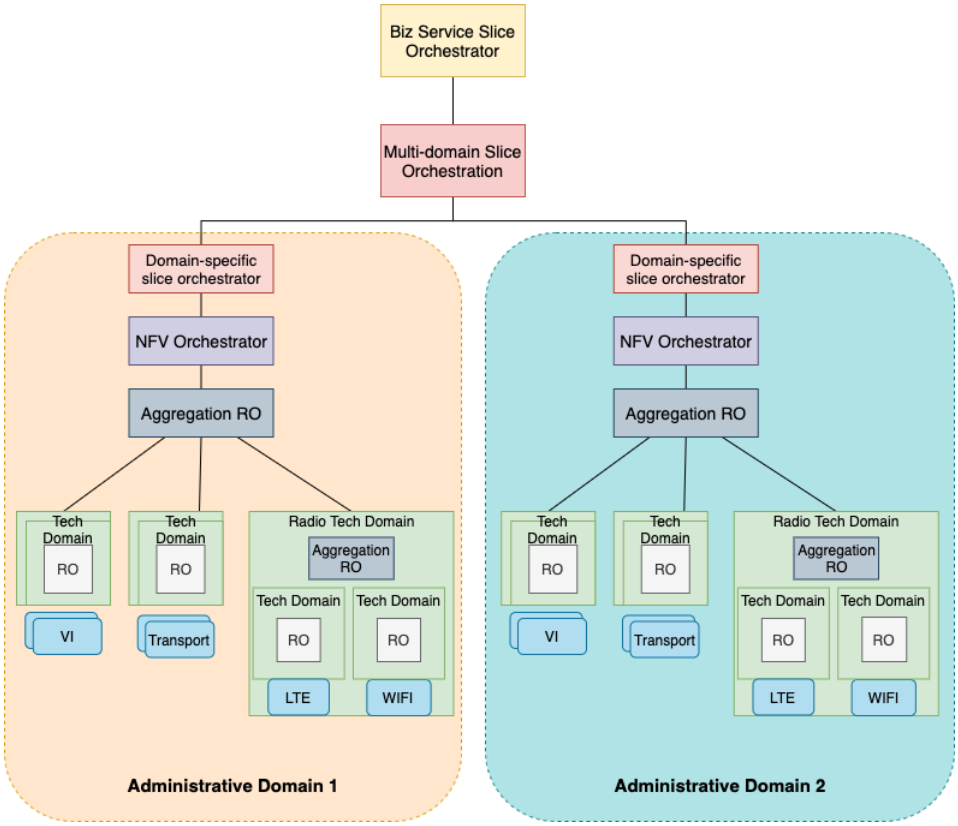


Figure 3.5: Afolabi et al. 5G!Pagoda architectural proposal adapted from [AKB+17].

this middle layer, there are domain specific orchestrators which perform resource and service orchestration of specific domains. According to the architecture, domain orchestrators within the same administrative domain can communicate amongst each other as well as with the top layer multi-domain orchestrators. It is the multi-domain orchestrator that communicates with the customer through a business to customer (B2C) interface. The multi-domain orchestrators are also connected to other multi-domain orchestrators through a business-to-business (B2B) interface which enables orchestration across administrative domains. The MdO should have an updated view of the underlying infrastructure exposed by domain orchestrators and by other MdOs. This view should be abstract and limited. Each MdO is responsible for controlling the abstract resources in its own administrative domain, but resources can be shared through communication between the MdOs of different administrative domains.

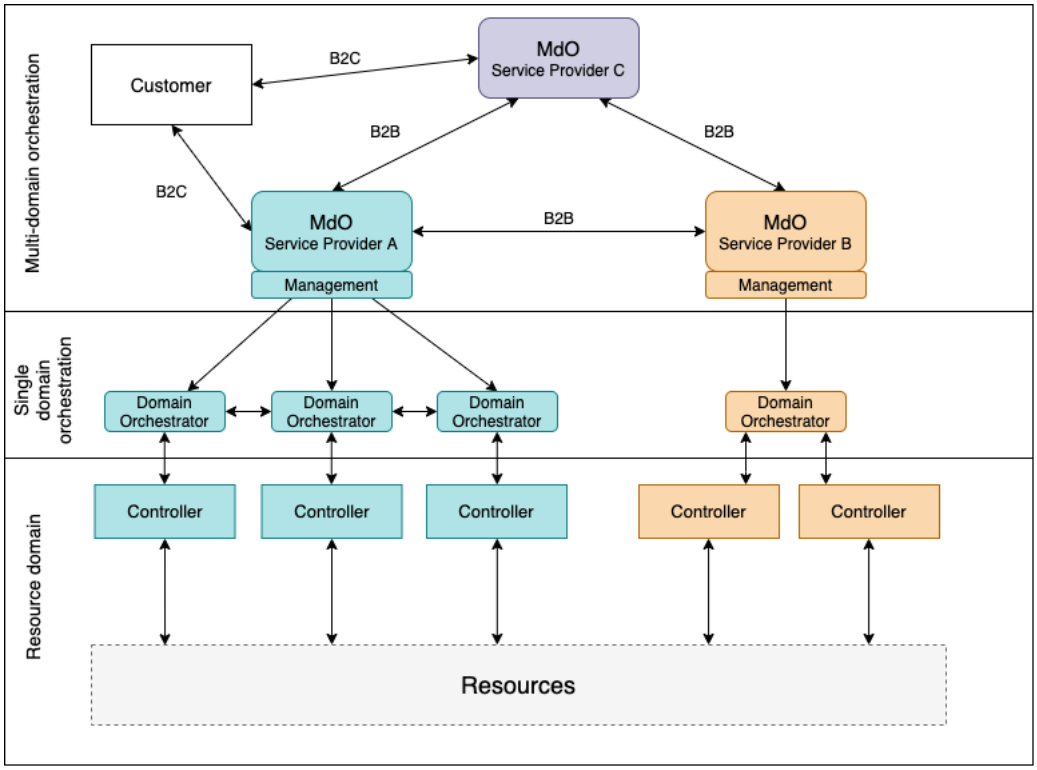


Figure 3.6: Guerzoni et al. reference architectural framework adapted from [GVPC+17].

3.2 Abstract MANO Architectures

As discussed in 3.1 there seems to be two distinct architectural options for a 5G management and orchestration system. After examining various papers, an abstract architecture of these two options was created. A proposal for the hierarchical MANO architecture can be seen in Figure 3.7 while the option for the flat architecture can be seen in Figure 3.8. Following is a short summary of the functionality of the different components that were included.

Common for both architectures is that there seems to be a need for a multi-domain orchestration component in order to provide E2E services. The Multi-domain Orchestrator (MdO) is responsible for managing the specific domain orchestrators (dO). These dO's control the specific Technical-domain Controllers (TdC) which manage the available resources. With a specific use case in mind, the tenant requests a service or slice. As mentioned in section 2.1, there needs to be a SLA in place

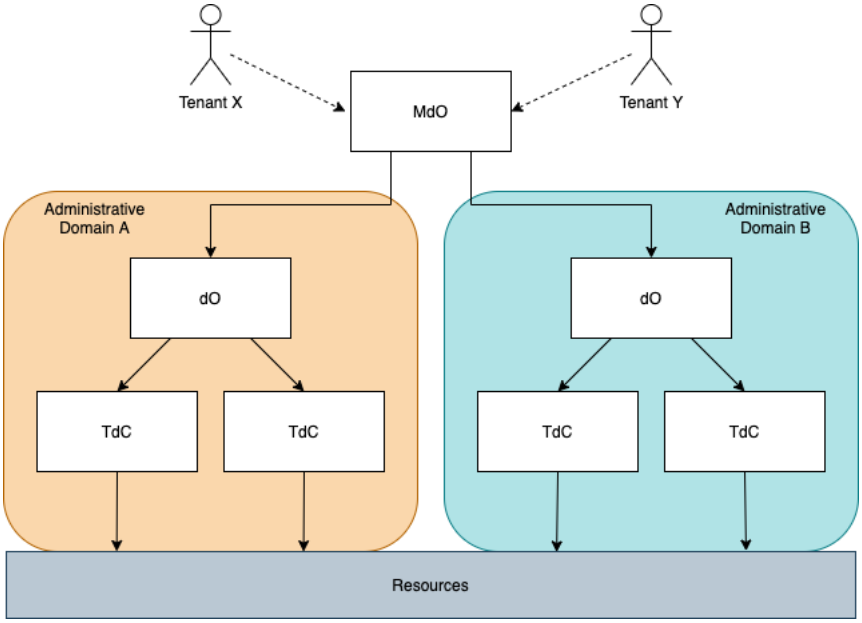


Figure 3.7: Abstraction of hierarchical multi-domain MANO architecture with two administrative domains.

between the tenant and operator. In order to implement the service according to the SLA, the request needs to be handled by a component that can provide E2E services: the MdO. As the resources needed to fulfil the tenants request might belong to multiple administrative domains, such an MdO might have both direct and indirect access to the dO's and TdC's which provide access to the resources. The characteristics and functionalities of the MdO is what differentiates the Hierarchical and Flat architectures. The MdO requests selected dO's to provide sub-slices, which together forms a complete slice. In this thesis it is assumed that the MdO possesses slice management abilities, as opposed to having a separate entity for this purpose.

The hierarchical model, which is seen in Figure 3.7, consists of several layers with an overarching MdO on top. It provides the tenant with the agreed services according to the SLA. The MdO can connect with dO's of all administrative domains in the network it has an agreement with. There are several possible views the MdO can have of the underlying network. It should have an overview of the capabilities of the underlying infrastructure, but whether this is very abstract or detailed can vary. Disclosing detailed information about an administrative domain can cause business implications, and this will be a part of the consideration.

The flat model is presented in Figure 3.8. The MdOs in this model communicate

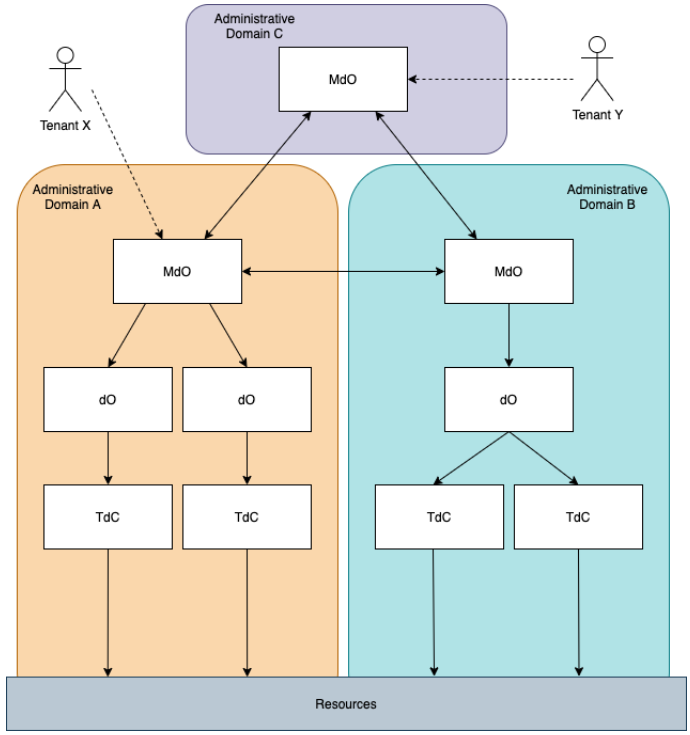


Figure 3.8: Abstraction of flat multi-domain MANO architecture with three administrative domains.

in a P2P fashion in order to fulfil the SLA between operator and tenant. The MdO of one administrative domain has full control of the resources within the same domain. In order to use resources from other domains, the MdO needs to request such resources from other MdOs. The MdO which provides the slice to the tenant does not necessarily need to own it's own infrastructure. As seen in Figure 3.8, the MdO of the Administrative Domain C can request resources from other MdO's to fulfil the SLA and provide the requested slice from the tenant.

Chapter 4
Analysis of Dependability Challenges

The following chapter presents an analysis on how the MANO architecture could affect the provisioning of a dependable 5G sliced network. This is done for both the hierarchical and flat architectures which were presented in the previous chapter. The chapter starts with developing potential depends-on graphs for each architecture before a more thorough analysis is performed based on these depends-on relations.

4.1 Depends-on Relations of the MANO Architectures

Depends-upon graphs can be used as a mean to understand fault-tolerant distributed systems. In this section proposals for depends-upon graphs for the hierarchical and flat architectures will be presented. In order to analyse the fault tolerance and dependability of a system it is necessary to introduce the building blocks the system consists of, and identify the failures that these can experience [Cri91]. A component X depends on a component Y if the correctness of X's behaviour depends on the correctness of Y's behaviour. X can then be denoted as a *user* of Y and Y as a *resource* of X. A resource can be dependent on another resource, so the names will be relative to the depends-on relation. This relation can be represented in an acyclic graph format where the arrows represent the depends-on relation. An example of such a graph related to the example of X and Y can be seen in Figure 4.1. In order to provide a dependable system the graph must be unidirectional and loop-free.

The different architectural proposals for MANO systems found in literature are presented with different entities, connections and levels of detail. The specific functionalities of all elements and their connection to other elements are also not fully described yet. It is thus still challenging to get a complete overview of how a MANO system will look like at a detailed level. In order to develop depends-upon graphs, it was thus necessary to summarise the roles of the entities included. Table 4.1 describes the different entities included in the graphs, their assumed role in the system and which other entities they might depend on:

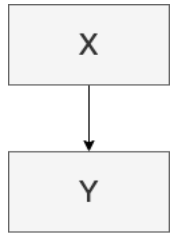


Figure 4.1: Example of a depends-on graph where user X depends on resource Y.

Table 4.1: Entities in a hierarchical and flat MANO system with functionalities and dependencies explained.

Entity	**Hierarchical: Role**	**Hierarchical: Depends-on**	**Flat: Role**	**Flat: Depends-on**
Service	Composed of interconnected VNFs from multiple domains. The service provided should be in accordance with the SLA agreed upon between tenant and operator.	Depends on the underlying VNFs of multiple administrative domains. Depends on a single MdO which coordinates between the domains.	Same as for hierarchical.	Depends on the underlying VNFs of multiple administrative domains. Depends on multiple MdOs belonging to different administrative domains, either directly or indirectly.

Continued on next page

Table 4.1 – *Continued from previous page*

Entity	**Hierarchical: Role**	**Hierarchical: Depends-on**	**Flat: Role**	**Flat: Depends-on**
MdO	Receives incoming slice requests. Coordinates between administrative domains. Collects abstracted service capability information regarding different administrative domains. Monitors, manages and controls.	Depends on other resources than it manages in order to prevent loop dependencies. Dependent on underlying dOs to give correct abstraction of underlying network in order to perform management correctly. Also dependent on dO in order to forward/enforce management decisions.	Receives incoming slice requests. Requests other MdOs for resources if needed to deliver service in accordance with SLA. Collects abstracted service and capability information both from other MdOs and its own underlying administrative domain.	Depends on other resources than it manages in order to prevent loop dependencies. Dependent on underlying dOs to give correct abstraction of underlying network in order to perform management correctly. Also dependent on dO in order to forward/enforce management decisions. The MdO which the service is dependent on (B2C relation to tenant) is dependent on other MdOs to ensure SLA's are met.

Continued on next page

Table 4.1 – *Continued from previous page*

Entity	**Hierarchical: Role**	**Hierarchical: Depends-on**	**Flat: Role**	**Flat: Depends-on**
dO	Orchestrates and manages within a single administrative domain based on decisions by the MdO. Allocates internal domain resources. Collects abstracted view of service and performance capabilities of underlying resources which it forwards to the MdO.	Dependent on the underlying NFVO in order to receive abstracted view of service and capability of underlying infrastructure. Also dependent on NFVO in order to implement management decisions.	Same as for hierarchical.	Same as for hierarchical.

Continued on next page

Table 4.1 – *Continued from previous page*

Entity	**Hierarchical: Role**	**Hierarchical: Depends-on**	**Flat: Role**	**Flat: Depends-on**
NFVO	Provides the dO with an abstracted view of the underlying infrastructure. Provides lifecycle management of network services based on provided capabilities. Coordinates the management of NFVI resources and VNFs through the VIM and VNFM respectively.	Dependent on correct information about available virtual resources from VIM/WIM and VNFMs. Also dependent on these to perform management of resources.	Same as for hierarchical.	Same as for hierarchical.
VNFM	Configuration and life cycle management of the VNFs within its domain. Allocates optimal amount of resources to particular VNFs in collaboration with the NFVO.	Dependent on NFVI resources which it can allocate to the VNFs.	Same as for hierarchical.	Same as for hierarchical.

Continued on next page

Table 4.1 – *Continued from previous page*

Entity	**Hierarchical: Role**	**Hierarchical: Depends-on**	**Flat: Role**	**Flat: Depends-on**
VNF	Implementation of a network function that can be deployed on a NFVI. Multiple VNFs are interconnected to form a fully-fledged network service.	Dependent on the NFVI resources it runs on. Dependent on the management of the VNFM for instantiation, modification and termination.	Same as for hierarchical.	Same as for hierarchical.
VIM/WIM	Controls and manages NFVI resources.	Dependent on the NFVI resources it is managing and the SDN controller.	Same as for hierarchical.	Same as for hierarchical.
SDN Controller	Sets up and manages underlying networking resources to provide required connectivity for communicating the VNFs. Can be both a part of the NFVI interacting with the VIM/WIM or and independent PNF entity linked with the NFVO.	Dependent on the NFVI resources.	Same as for hierarchical.	Same as for hierarchical.

Continued on next page

Table 4.1 – *Continued from previous page*

Entity	**Hierarchical: Role**	**Hierarchical: Depends-on**	**Flat: Role**	**Flat: Depends-on**
NFVI	HW and SW resources used to host and connect VNFs.	Not dependent on the other entities included.	Same as for hierarchical.	Same as for hierarchical.

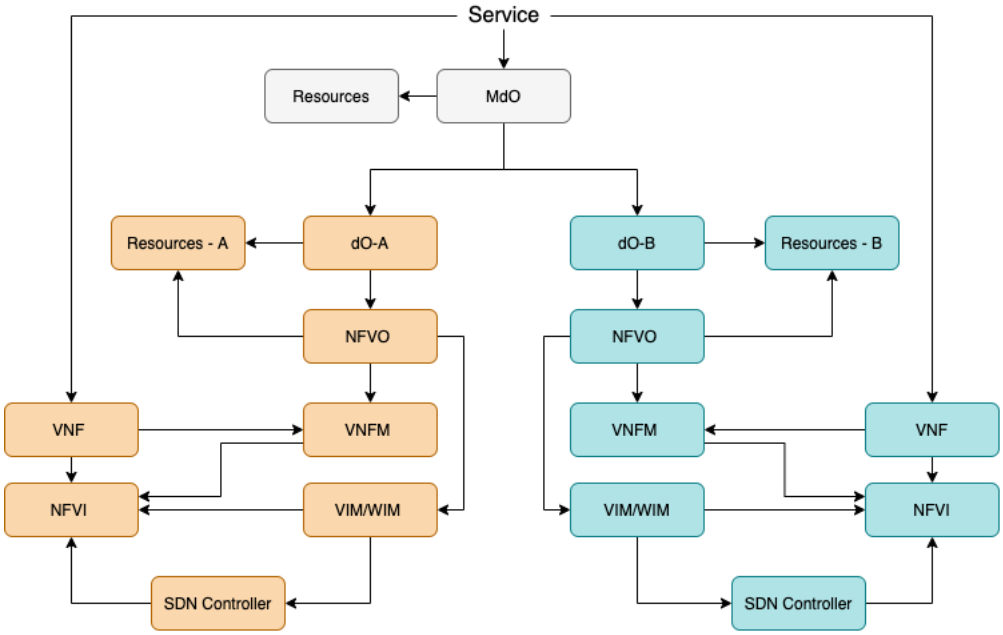


Figure 4.2: Depends-on graph attempting to present dependability between components in a multi-domain hierarchical MANO system with administrative domain A and B.

Figure 4.2 shows the proposed depends-on graph which attempts to present the dependability between components in a hierarchical MANO architecture. Two administrative domains are used to depict how the service might be built with resources from multiple administrative domains.

Both Figure 4.3 and 4.4 try to present depends-on relationships in a flat MANO architecture. In Figure 4.3 the tenant is separate from the operators. The business to customer connection is set between MdO-A and the tenant. MdO-A is responsible for requesting additional resources from MdO-B in a business to business connection. In 4.4 the tenant is both operator (with no infrastructure) and tenant. MdO-C does not have own infrastructure, but is dependent on MdO-A and MdO-B in order to provide services.

The depends-on graphs could have been extended to include more of the SDN control and physical functions. This was, however, considered as out of scope as the main focus of this thesis lies in the MdO and dO interactions. The rest of the thesis will thus focus on the MdO and dO as these are the entities that vary significantly between the two architectures.

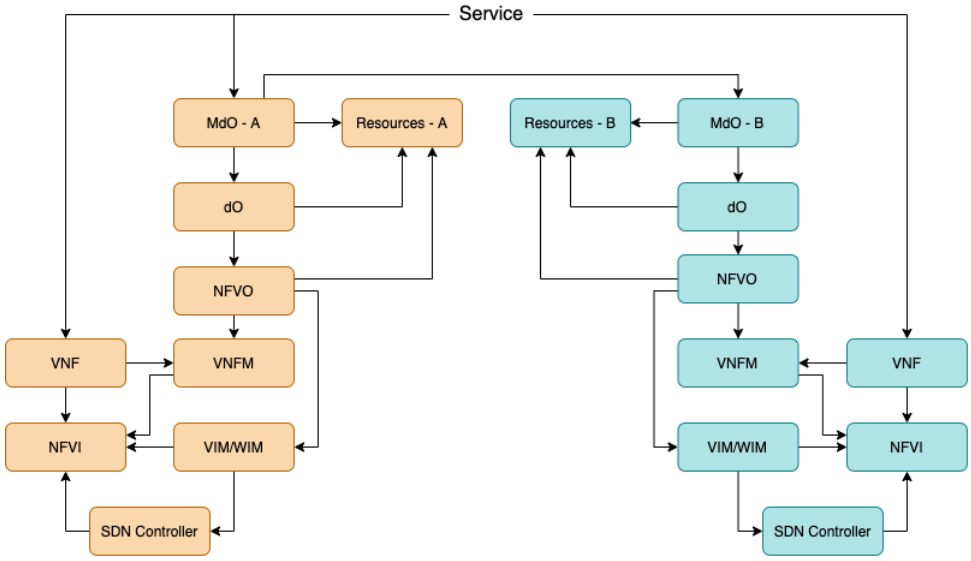


Figure 4.3: Depends-on graph proposal for flat multi-domain MANO architecture with two administrative domains.

The MdO and dO entities can be exposed to a set of threats. The source of these threats can be both random and malicious. These threats might lead to the failure of the entity and subsequently the failure of the MANO system. Failures, both random and caused by malicious actors, can lead to disruptive behaviour and unavailability. In the next sections we will focus on the following:

- Random faults causing mis-operations.
- Random faults causing unavailability.
- Malicious act causing mis-operations.
- Malicious act causing unavailability.

4.2 The Hierarchical

In order to deliver services in accordance with agreed SLAs, the hierarchical architecture is dependent on an overarching MdO which coordinates between the different administrative domains. If functioning properly, the MdO receives requests and coordinates between the underlying domains while it monitors and makes sure the resources are optimally utilised. The MdO is dependent on the underlying dOs. The

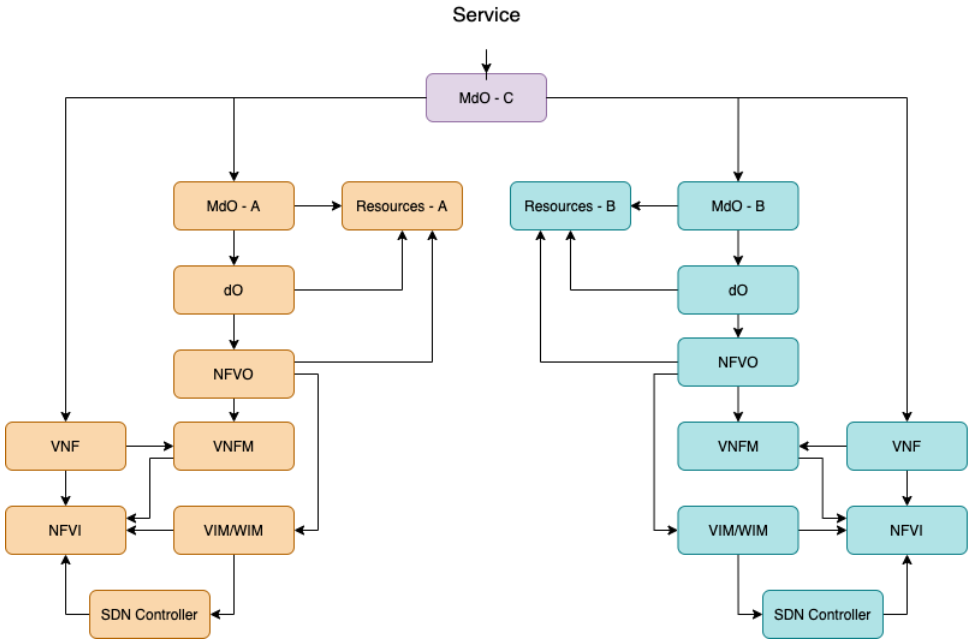


Figure 4.4: Depends-on graph proposal for flat multi-domain MANO architecture where domain C is acting as both tenant and operator.

dOs also have a management role, but it is restricted to a single administrative domain. The dO forwards abstracted information about the service capabilities of its domain to the MdO.

4.2.1 Failures

As a central unit with management and coordination responsibility for E2E services, the MdO emerges as a potential single point of failure in the hierarchical MANO architecture. The potential consequences of such a failure in the MdO depends on the type of failure, the nature of the services depending on the MdO and the criticality of such services.

Random faults and unavailability of the MdO

If the failure causes the MdO to become unavailable, the resulting effects would seemingly depend on the duration of the unavailability. Deployed slices would most likely continue to operate. However, in the absence of the MdO it would no longer be possible to deploy new E2E slices or adjust the resource utilisation of the deployed slices from an E2E perspective. The impact of this depends highly on what kind of

services are needed. If the service is quite stable, the unavailability of the MdO might not be too critical. For a slice that needs frequent adjustment, the consequences might be more severe. If there is an urgent need for a specific service and slice, the network will fail to meet this demand. Failure to meet tenant requests might have severe consequences depending on the services they are running, and possibly have further implications for the safety of the users. For instance, if a slice supporting autonomous vehicles needs urgent readjustments which the operators fail to provide, it might have dire consequences not only because the service is unavailable but because the safety of the users can be endangered. The MdO is also supposed to provide E2E optimised utilisation of resources. When it comes to resource utilisation, the consequences would depend on how long the MANO system is unavailable. One could anticipate a more severe outcome with a longer unavailability, which might impact a larger part of the network.

Malicious act and unavailability of the MdO

A malicious act causing unavailability of the MdO would seemingly have similar consequences as for random faults. In addition, the timing of the unavailability could potentially be fine tuned resulting in even greater consequences for the network.

Random faults and mis-operation of the MdO

Another type of failure that could affect the MdO would be mis-operations caused by random faults. Such a failure might be even more dramatic than unavailability and could potentially have catastrophic consequences. Mis-operations can also take longer to detect as it might not be as apparent as when the MdO is fully unavailable. The MdO has E2E control over multiple administrative domains and thus the consequences could potentially influence a large geographical area.

Malicious act and mis-operation of the MdO

Dependability and security are tightly linked concepts. If a malicious actor gets control over the MdO, that would mean that an attacker potentially has control of the management of the whole network. In contrast to random faults, the consequences of the mis-operations in this case would benefit the attacker and might thus be more severe. If the MdO carries out random mis-operations, the consequences might still be severe, but they would also to some extent be random. A malicious actor can spend more time on carrying out specific mis-operations resulting in their own benefit or the maximum destruction of the network. As 5G is expected to become a critical infrastructure as well as support other critical infrastructures, the outcome of an attack might be catastrophic. This would also make the MdO a tempting target for actors with malicious intentions. It can be potentially challenging to detect and implement countermeasures.

Random faults and unavailability of the dO

If the dOs experience faults in the form of unavailability, the effects would be somewhat restricted to that specific administrative domain. If one of the dOs is unavailable, the MdO has no control over the resources within that administrative domain. From a technical perspective, this could be solved by using resources from other administrative domains. The overall resources the MdO can use will be less, but it would then be able to use other dOs to fulfil the requests from the tenants. The MdO will have a continuous view of overall resources available in the different domains it has access to. From a business perspective it could be more complex, as it might not be as easy as just switching over to another domain depending on the business relationships between different tenants and operators.

One of the questions is also how autonomous the dOs will be without receiving instructions from the MdO. If they can perform local domain adjustments based on monitored values, the scenario might be better than if they are solely dependent on the MdO to perform any adjustments. This could also depend on the resource model chosen. If the resources are pre-allocated, there might be more flexibility for the dOs to handle certain issues on their own. On the other hand, if the resources are solely allocated on demand the need for a top coordinator might be continuous.

Malicious act and unavailability of the dO

A malicious actor causing the dO to become unavailable should have similar consequences as that of random faults. However, the dO can be specifically targeted and thus potentially cause disruptions to specific services of the threat actors choosing. The malicious actor can then target dOs which are a part of the E2E service chain of a critical service, making it more challenging for the MdO to secure the dependability of the service.

Random faults and mis-operation of the dO

If the dOs start to mis-operate, the consequences could be that the MdO receives the wrong information about resource utilisation and capabilities of the domain that specific dO governs over and might perform operations based on this. This could potentially have significant effects on the E2E management of the MdO, and in turn affect the service provisioning. The MdO will then have a wrong view of the state of the network. The dO can also mis-operate when it comes to the management actions it performs over its domain. This could then cause disruptions within that administrative domain.

Malicious act and mis-operation of the dO

A malicious actor can target specific dOs for mis-operation. The effects would seemingly be similar, but with a targeted approach the consequences might be more severe and critical services could be targeted specifically leading to more harm and destruction.

4.2.2 Isolation

Isolation in terms of dependability entails the prevention of faults propagating across slice boundaries. [TASY19] points to how the choice of which functions and resources to be shared or kept dedicated impacts the end-to-end performance and economic cost. Although isolation might enhance security and improve availability in a 5G sliced network, it can reduce the efficiency of resource utilisation. It is thus important to find an acceptable trade-off between the achieved isolation level and cost-efficiency. Isolation in the hierarchical architecture is two sided. At one hand the logically centralised MdO might make it easier to coordinate isolation policies between the different administrative domains from end to end. As described by Kotulski et al. [KNS+18], each domain has to guarantee proper isolation in order to provide an isolated E2E slice. At the other hand, the MdO entity itself might pose as a threat against isolation as it has a management role towards all domains. The MdO might also be better equipped to isolate faults and attacks to certain slices or domains as it has an overall view. The holistic view might also enable the MdO to faster gain control of the situation and restore network conditions.

4.2.3 Business

The hierarchical approach could be implemented in several ways. The MdO could have more or less information about the underlying domains, and the level of control it possesses can also be discussed. From a pure technical perspective, it might be tempting to envision a MdO with great knowledge about the underlying network which can perform effective and optimised management operations. From a business perspective this might be much harder to realise, as there is a reluctance among the operators to disclose too much information about their own networks. As described in [HBT16], this stems from the fear of losing competitive advantages as well as national security regulations in relation to the protection of information on critical infrastructure. This leads to the operators only sharing limited information. The authors conclude that a platform enabling mutual trust and cooperation will result in a sufficient benefit of information exchange, though not excessively. The reluctance to share information about underlying infrastructure could potentially cause implications for implementing a hierarchical MANO architecture. In countries such as Norway, where the state enforces distribution and competition in the communication sector, it could be challenging to obtain a central entity with overall control. An important

question would then be who should be in control of such an entity. Because of this, the information received by the MdO at the top of the hierarchy should be abstracted to what is necessary to coordinate E2E services. As briefly mentioned before, if the MdO could be implemented in such a way that it enabled mutual trust and cooperation between the operators, it might result in an overall benefit. Even with a limited view of the service capabilities of the underlying administrative domains, someone will still be in charge of the MdO. This might introduce further implications based on the relationship between different businesses.

In any scenario, it seems necessary to include proper SLAs both between the MdO and tenants as well as between the MdO and the dOs belonging to the different administrative domains. Some sort of agreement needs to be in place in order for the MdO to be aware of how to utilise the resources and which services to prioritise if the capabilities of the network is reduced. This could also be an interesting dilemma from a economic versus ethical viewpoint. Should for instance some services i.e autonomous vehicles or a Public Safety Network be prioritised automatically if the capacity is low.

4.3 The Flat

In a flat architecture the service depends on multiple MdOs, both directly and indirectly. These MdOs can communicate in a peer to peer fashion to obtain resources from each other. The MdOs can have underlying dOs and infrastructure it manages, or it can be borrowing such through other MdOs. As for the hierarchical architecture, failures can occur in multiple ways and might have different consequences depending on the criticality of the service the MdO is supposed to support. The MdOs in a flat architecture are dependent on other MdOs and dOs.

4.3.1 Failures

In the flat architecture the management and coordination responsibility for E2E services is distributed across several MdO entities. The potential consequences of failures of the MdO and dOs depends on the type of failure, the nature of the services depending on them and the criticality of such services.

Random faults and unavailability of the MdO

If the MdO which holds the business to customer connection with the tenant is unavailable it could have serious consequences. From a technical perspective the tenant might just request its services from a different MdO. This would entail that if MdO of administrative domain A is unavailable, tenant X which primarily is connected to MdO-A could connect to MdO-B of administrative domain B (assuming

it can provide the same type of resources) and still be able to provide its end users with an E2E connection. There could, however, be physical restrictions making the possibilities of an easy switch between MdOs more limited. It would also need to work from a business perspective. The tenant would then need redundant agreements with MdOs of other administrative domains in order to have a robust connection to the network both physically and virtually. Consequences would depend on how fast the new connection can be up and whether or not this new connection can fulfil the agreed SLA in the same way as the original MdO.

The MdO which is responsible for providing a service is dependent on both underlying dOs and other MdOs in order to fulfil tenant requests. If an arbitrary MdO is unavailable, the benefit of the flat architecture is that it does not introduce a single point of failure. If MdO-C is responsible to fulfil a tenant request and MdO-A is down, it can simply ask another MdO which has the same type of service capabilities as MdO-A. By splitting the architecture in multiple MdOs, there is a layer of redundancy added as long as multiple reachable MdOs can possess the same service capabilities.

Malicious act and unavailability of the MdO

A malicious actor can target specific MdOs, and potentially cause more harm than a random fault as more vulnerable and critical services could be targeted. There would, however, still likely be redundancy through other MdOs.

Random faults and mis-operation of the MdO

When it comes to mis-operations of the MdO which holds the B2C connection, it might be more difficult for the tenant to detect. In the case of known mis-operations, the same solution could be applied as for the unavailability scenario and the tenant can request services from a different MdO.

Arbitrary mis-operating MdOs could have significant consequences for the E2E provisioning. If the failure is detected, the MdO could be "cut out" of the network, and other MdOs could be used as a replacement. If not detected, the effects might propagate to other MdOs, resulting in a strained network. One could also consider if it would be easier to detect and prevent mis-operations by an MdO in a flat P2P system. There is not one single MdO which has a top responsibility, but rather several MdOs with a shared responsibility to make E2E connections work.

Malicious act and mis-operation of the MdO

The fact that several MdOs are in charge of E2E coordination, could enable some sort of checking mechanisms preventing that one malicious MdO gets full control

of everything. A malicious actor would be able to target more specifically, but it would likely still have similar consequences to random faults and mis-operations. If the attack is very sophisticated it might be more difficult to detect than randomly caused mis-operations.

Random faults and unavailability of the dO

If a dO is unavailable the problem would be restricted to a specific part of a single domain, and thus likely not affect the whole domain or multiple-domain connections. As long as another dO with the same capabilities exists either in the same administrative domain or in a different administrative domain, the request can still be met from a technical perspective.

Malicious act and unavailability of the dO

As for other scenarios, the consequences would most likely be similar to that of random unavailable dOs. However, a malicious actor has the capability of targeting specific dOs and choosing a specific timing which might increase the consequences.

Random faults and mis-operation of the dO

Mis-operating dOs could have effects on critical services, and if providing the MdO with incorrect information about service capabilities it might lead to larger issues. If the dO is blindly trusted by the MdO, mis-operations might go undetected and reduce the optimisation of resource utilisation.

Malicious act and mis-operation of the dO

A malicious actor might use a low level dO to provide incorrect information to the MdO. A dO of a flat architecture manages a very restricted part of a specific administrative domain, but the effects might nonetheless have an impact on the overall service provisioning if the MdOs act on this wrong information.

4.3.2 Isolation

As described by [KNS+18], isolation constitutes a set of properties chosen according to implementation needs. Achieving an appropriate level of isolation in a multi-domain environment, both including administrative and technological diversity, could be a challenge. This also includes security aspects, as there should be mechanisms in place to ensure attacks and faults in one domain or slice does not impact others. This could, potentially, be even more challenging in a flat architecture, as there would be no overarching central entity managing every domain. At the same time, there is no entity connecting all the elements together, and thus it might be easier to implement failure independent domains from an administrative perspective.

4.3.3 Business

From a business perspective, there will need to be agreements in the form of SLAs between tenants and operators. At the same time there would also be a need for a sort of agreement among the operators. There also needs to be some sort of exchange of capabilities between the MdOs in order to enable the cooperation and sharing of resources. The level of detail would probably be low as the operators would wish to keep information about their own networks as private as possible.

Chapter 5
Discussion

This chapter discusses the findings in the analysis of Chapter 4. The chapter includes a table summarising the highlights of the analysis. Based on this, there will be a discussion on the differences of the hierarchical and flat architectures with regards to dependability.

5.1 Discussion

A brief summary of the analysis in Chapter 4 can be found in Table 5.1. The following discussion will focus on the same elements as in the analysis: The failure of the MdO and dO, the isolation capabilities and the business implications of the two different architectures.

Table 5.1: Highlights from analysis chapter.

	Hierarchical	**Flat**
Failure of MdO	Potential single point of failure.	Multiple MdOs provide redundancy.
Failure of dO	Whole administrative domain impacted.	Part of administrative domain impacted.
Isolation	Might be easier to coordinate policies. Potentially introduces vulnerability through MdO.	Challenging to coordinate policies with P2P.
Business	Less control of own resources.	More control of own resources.

5.1.1 Comparing Failure of the MdO

The MdO entity is to a large extent what separates the hierarchical and flat architectures. The flat architecture MdO does, to some extent, support more redundancy than the hierarchical MdO when it comes to multi-domain E2E orchestration. In the flat architecture the tenants could potentially reconnect to other MdOs if it is unavailable or has been detected to mis-operate.

A malicious actor which gains control of a MdO in a hierarchical architecture seems to gain control of a larger part of the E2E management than that of the flat. It could also potentially be easier to detect mis-operations of a MdO in a flat architecture if such controls are implemented by the other MdOs.

5.1.2 Comparing Failure of the dO

The dO plays a different role in the two architectures. In the hierarchical, the dO serves as the only connection between the MdO and the administrative domain the dO belongs to. In contrast, the flat architecture can have several dOs within a domain, and the MdO serves as the connection between other MdOs and the administrative domain. A failure which leads to the dO being unavailable could thus isolate a whole administrative domain in the hierarchical architecture, while it could isolate part of the administrative domain in a flat architecture.

Mis-operations of a dO can have some of the same consequences in both architectures, dependent on how much trust and autonomy is put in each dO.

5.1.3 Comparing Isolation Capabilities

Isolation could be implemented in a different entity than the ones included in the architectures presented. Nevertheless, it can be interesting to look at how the two architectures capabilities would differ if such a responsibility was to be put in the MdO.

Faults should not propagate across slice boundaries nor across domains. For the hierarchical architecture, isolation might be viewed as easier to coordinate as there is a central MdO which could have the means to coordinate it both between domains and across slices. Such a MdO might also be more efficient when dealing with isolation issues with an overall view. The flat architecture on the other hand will need to achieve E2E isolation through P2P communication.

The MdO in the hierarchical architecture might introduce a vulnerability when it comes to isolation as potential faults might be transferred from one domain to the other through the MdO. This could, arguably, be less of a problem in the flat architecture.

5.1.4 Comparing Business Implications

From a business perspective, operators would wish to restrict the sharing of information about the underlying network in both architectures. This could, however, be easier in a flat architecture than in the hierarchical one.

Even with a very restrictive view of the network, the MdO in a hierarchical architecture would possess a certain level of power. This entity would also need to be owned by someone, which can cause implications with regards to business relationships. In the flat architecture each operator takes care of its own MdO. There needs to be collaboration between these entities in order to provide multi-domain services, but the operators might feel like they are left with more control of their own network with such an architectural solution.

5.1.5 Limitations

There are still a lot of open questions that need to be settled with regards to the MANO of 5G networks. This introduces a lot of uncertainties in a discussion, and subsequently a lot of the potential consequences discussed in Chapter 4 are to a large extent dependent on implementation details beyond this thesis. The functionality of each entity is also not fully defined, so the findings should also be looked at in light of this.

Such an analysis is also influenced by the individual skills of the researcher, and can to an extent be more influenced by personal biases than that of a quantitative approach. Although the qualitative analysis is subject to weaknesses, it is a starting point for assessing dependability in 5G MANO systems, and can shed a light on what steps can be taken in the future.

Chapter 6
Conclusion

6.1 Concluding Remarks

The MANO system is a significant part of the future 5G sliced network. The work presented in this thesis strives to be a step towards exploring dependability concerns regarding the 5G MANO system. In this work a background study of key 5G concepts and MANO architectures was conducted. We first presented several architectural proposals for 5G MANO which were examined and mapped into two promising categories for management and orchestration: The hierarchical architecture and the flat architecture.

We then analysed how the two different architectural designs identified can impact the dependability of an isolated 5G sliced network. A qualitative analysis was conducted based on developed depends-upon graphs of the two architectures. Results from the analysis indicate that both architectural options can have both positive and negative consequences for the dependability of the 5G network. This will likely also depend greatly on the implementation of the different entities and functionalities. A hierarchical architecture might enable easier coordination both of resource utilisation and isolation capabilities as it has a central overarching orchestrator entity. On the other hand, this entity might become a potential single point of failure if it were to be mis-operated or unavailable. It could also introduce a isolation vulnerability through the MdO entity. The flat architecture provides multiple such orchestrator entities and thus provides some redundancy. The coordination might be more challenging as several such entities need to cooperate. From a business perspective the flat approach might be more promising as it could reduce the need for sharing information about the network. The shortcomings in the MANO standardisation process for 5G systems provides some limitations to the results, and further work should be done to improve this.

6.2 Future Work

This thesis is intended to be an initial step towards assessing the dependability concerns of management and orchestration for 5G sliced networks. A potential next step for future work could be to undertake a quantitative analysis to assess dependability challenges. This would involve developing quantitative models to predict the impact of failures in the MANO system on the dependability of the 5G network.

Another suitable topic for future work could also be to analyse the dependability challenges of the MANO with a more detailed look at each of the components.

Lastly, a potential future approach could be to extend the scope and include more components of the network in the analysis.

References

[AKB+17] Ibrahim Afolabi, Adlen Ksentini, Miloud Bagaa, Tarik Taleb, Marius Corici, and Akihiro Nakao. Towards 5G network slicing over multiple-domains. *IEICE Transactions on Communications*, 100(11):1992–2006, 2017.

[All15] NGMN Alliance. 5G white paper. https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf, visited 2020-05-5, 2015.

[All19] NGMN Alliance. 5G network and service management including orchestration. https://www.ngmn.org/wp-content/uploads/Publications/2019/190312_5G_Network_and_Service_Management___including_Orchestration_3.14.0.pdf, visited 2020-05-5, 2019.

[ALRL04] 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*, 1:11–33, 2004.

[ATS+18] 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*, 20(3):2429–2453, 2018.

[BAMH20] Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi, and Andrew Hines. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167:106984, 2020.

[BBZ19] Yosra Benchaabene, Noureddine Boujnah, and Faouzi Zarai. Ultra Reliable Communication: Availability Analysis in 5G Cellular Networks. In *2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pages 96–102. IEEE, 2019.

[Cri91] Flavin Cristian. Understanding Fault-tolerant Distributed Systems. *Commun. ACM*, 34(2):56–78, 1991.

[DJEG20] Mouhamad Dieye, Wael Jaafar, Halima Elbiaze, and Roch Glitho. Market Driven Multi-domain Network Service Orchestration in 5G Networks. *IEEE Journal on Selected Areas in Communications*, 03 2020.

[ETS14] ETSI. ETSI GS NFV 002 V1.1.1(2013-10): Network Functions Virtualisation (NFV); Architectural Framework. Technical report, 2014. Also available as https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf, visited 2020-05-5.

[ETS17] ETSI. ETSI GR NFV-EVE 012 V3.1.1(2017-12): Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework. Technical report, 2017. Also available as https://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/012/03.01.01_60/gr_NFV-EVE012v030101p.pdf, visited 2020-05-5.

[FPEM17] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina. Network Slicing in 5G: Survey and Challenges. *IEEE Communications Magazine*, 55(5):94–100, 2017.

[GPCM+16] Riccardo Guerzoni, David Perez-Caparros, Paolo Monti, Giovanni Giuliani, Javier Melian, and Gergely Biczók. Multi-domain orchestration and management of software defined infrastructures: A bottom-up approach. 2016.

[Gro17] IETF Network Working Group. Network Slicing Architecture. Technical report, 2017. Also available as https://tools.ietf.org/id/draft-geng-netslices-architecture-01.html, visited 2020-05-6.

[GVPC+17] Riccardo Guerzoni, Ishan Vaishnavi, David Perez Caparros, Alex Galis, Francesco Tusa, Paolo Monti, Andrea Sganbelluri, Gergely Biczók, Balasz Sonkoly, Laszlo Toka, et al. Analysis of end-to-end multi-domain management and orchestration frameworks for software defined infrastructures: an architectural survey. *Transactions on Emerging Telecommunications Technologies*, 28(4):e3103, 2017.

[GXG18] Andres J Gonzalez, Min Xie, and Pål Grønsund. Network Slicing Architecture and Dependability. In *International Conference on Mobile, Secure, and Programmable Networking*, pages 207–223. Springer, 2018.

[HBT16] Poul E Heegaard, Gergely Biczok, and Laszlo Toka. Sharing is power: Incentives for information exchange in multi-operator service delivery. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2016.

[Kit04] Barbara Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.

[KNE16] Kostas Katsalis, Navid Nikaein, and Andy Edmonds. Multi-domain orchestration for NFV: Challenges and research directions. In *2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*, pages 189–195. IEEE, 2016.

[KNS+18] Zbigniew Kotulski, Tomasz Wojciech Nowak, Mariusz Sepczuk, Marcin Tunia, Rafal Artych, Krzysztof Bocianiak, Tomasz Osko, and Jean-Philippe Wary. Towards constructive approach to end-to-end slice isolation in 5G networks. *EURASIP Journal on Information Security*, 2018(1):2, 2018.

[ML17] HV Kalpanie Mendis and Frank Y Li. Achieving ultra reliable communication in 5G networks: A dependability perspective availability analysis in the space domain. *IEEE Communications Letters*, 21(9):2057–2060, 2017.

[MSG+15] Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, and Raouf Boutaba. Network function virtualization: State-of-the-art and research challenges. *IEEE Communications surveys & tutorials*, 18(1):236–262, 2015.

[NGG+18] Gianfranco Nencioni, Rosario G Garroppo, Andres J Gonzalez, Bjarne E Helvik, and Gregorio Procissi. Orchestration and control in software-defined 5G networks: Research challenges. *Wireless communications and mobile computing*, 2018, 2018.

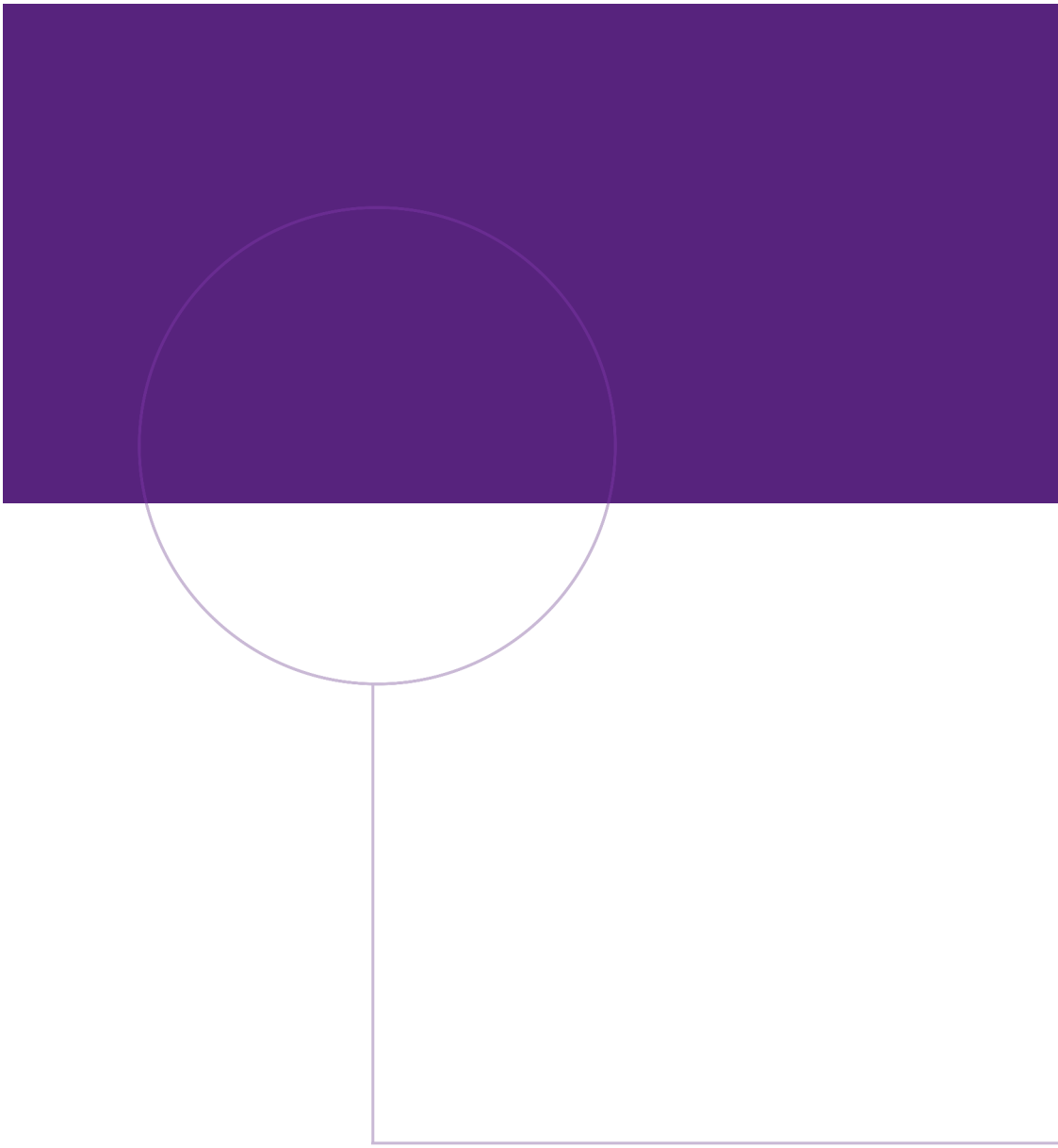
[OLAL+17] Jose Ordonez-Lucena, Pablo Ameigeiras, Diego Lopez, Juan J Ramos-Munoz, Javier Lorca, and Jesus Folgueira. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine*, 55(5):80–87, 2017.

[Par15] The 5G Infrastructure Public Private Partnership. 5G Vision. https://5g-ppp.eu/wp-content/uploads/2015/11/Vision-brochure.pdf, visited 2020-05-5, 2015.

[RBM+19] Simone Redana, Ömer Bulakci, Christian Mannweiler, Laurent Gallo, Apostolos Kousaridas, David Navrátil, Anna Tzanakaki, Jesús Gutiérrez, Holger Karl, Peer Hasselmeyer, Anastasius Gavras, Stephanie Parker, and Edward Mutafungwa. 5G PPP Architecture Working Group - View on 5G Architecture, Version 3.0. https://doi.org/10.5281/zenodo.3265031, visited 2020-05-5, June 2019.

[SMY+19] Vincenzo Sciancalepore, Christian Mannweiler, Faqir Zarrar Yousaf, Pablo Serrano, Marco Gramaglia, Julie Bradford, and Ignacio Labrador Pavón. A Future-Proof Architecture for Management and Orchestration of Multi-Domain NextGen Networks. *IEEE Access*, 7:79216–79232, 2019.

[TASY19] Tarik Taleb, Ibrahim Afolabi, Konstantinos Samdanis, and Faqir Zarrar Yousaf. On multi-domain network slicing orchestration architecture and federated resource control. *IEEE Network*, 33(5):242–252, 2019.



NTNU

Norwegian University of
Science and Technology