NFV and OPNFV

Stanislav Guerassimov
Betreuer: Edwin Cordeiro, Lukas Schwaighofer
Seminar Innovative Internettechnologien und Mobilkommunikation SS2016
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: s.guerassimov@in.tum.de

ABSTRACT

The demand for flexible and economically viable cloud computing and virtualization technologies is continuously increasing. In this paper we discuss how Network Function Virtualization (NFV) enables simplified network function management and other benefits and challenges that it brings. We also note major NFV standardization efforts, while describing OPNFV in depth. Further, this paper introduces a couple of use-cases for NFV, such as deployment alongside SDN in a datacenter and even deployment in industrial automation systems. We also provide a collection of analyses of existing pilot implementations of NFV. As a result, this paper should provide the reader with an up-to-date state of network function virtualization technologies.

Keywords

NFV OPNFV network function virtualization

1. INTRODUCTION

Virtualization technologies have become a big subject over the recent years. Commodity hardware has become more powerful, thus allowing flexibility in IT operations as well as significant economical benefits. The growing demand to data size and processing speed, as well as the ability to scale in order to accommodate new demands for those parameters has been treated with virtualization technologies. The result was scalable cloud architectures. Network inflexibility has become a bottleneck for those growing demands. So it simply made sense to apply the same approaches to the network.

In order to avoid confusion we will address several terminological questions. From a formal perspective, virtualization can have a lot of different meanings. In the context of network and datacenter operations virtualization means the ability to run several full operating system on a software platform as if they were running on several distinct hardware platforms. Virtualization in networking historically meant multiplexing several network flows over a shared physical link, something often referred as a tunnel. Technically, this means the virtualization of layers 1-3 of the OSI model. NFV on the other hand virtualizes layer 4-7.

The overall concept of NFV should become more clear as the next section explores it in depth, together with technical aspects and challenges. Section 2.2 presents various attempts at standardization of NFV implementations. A particular standardization effort, OPNFV, is analyzed in section 3, along with existing OPNFV versions, projects and architecture. The reader will become familiarized with theoretical concept designs for NFV, including NFV in the datacenter and even in industrial automation systems in section 4, as well as with existing industry implementations of NFV in section 5.

2. NFV

Unlike server virtualization, network virtualization is not a mature technology that is widely adapted.

Network virtualization has the same goals as server virtualization. Analogous to those technologies, NFV should allow the network and it's functions to appear to hosts as a real physical ones. This should allow network engineers to deploy previously physical networking devices as software applications. Examples include firewalls, routers, switches, loadbalancers, WAN optimizers, IP Multimedia Subsystems (IMS), Evolved Packet Cores (EPC) and Deep Packet Inspection (DPI). The network architecture itself will change, as all devices are now running on a single hardware environment. Figure 1 provides a basic overview, which shows how hardware functions are transformed into virtualized network functions (VNF). In the next section we will discuss various advantages and challenges of NFV.

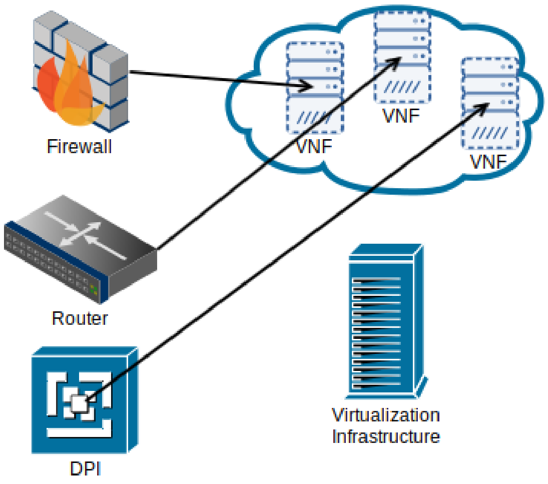

Figure 1: NFV concept

doi: 10.2313/NET-2016-09-1_08

2.1 Technical aspects

The concept of NFV introduces numerous benefits to network operations. Arguably, only by utilizing NFV we can achieve the full benefits of OS virtualization, since physical networks bottleneck the capabilities of the former.

The hardware liberation that NFV brings changes several aspects about network operations. The first is the cost of hardware. Function consolidation reduces the amount of required running hardware for high availability. Previously a common proper practice was to purchase spare hardware units for each working unit. The amount of devices standing by can now be reduced. This will also reduce energy consumption, a benefit inherited from virtualization of operating systems. It could be reduced by minimizing the amount of online hardware thanks to consolidation.

Hardware costs are also reduced because specialized devices are replaced by commodity of the shelf (COTS) hardware. This also means that network engineers become decoupled from vendor solutions. There is no need to relearn new hardware, no need to wait for a vendor to implement a new feature or suffer price extortion from network equipment producers.

NFV also lowers the network industry barrier to smaller companies and open source communities, so that they can also develop network solutions. Since network technologies are now software based the amount of competition among vendors increases. Smaller vendors that were unable to enter the market, due to the impossibility of launching their own hardware production lines, can now have a competitive edge against large network technology giants, for example by offering customers specialized solutions.

NFV can reduce the complexity of testing new network functions. Building a test environment becomes easier than before, since deploying a new virtual machine is significantly easier than purchasing new hardware. Another aspect is the benefits functions provided by virtualization bring, for example snapshotting makes it easier to test new settings with the ability to quickly revert to the last stable configuration. When it comes to launching those functions, the process will no longer entail purchasing new networking hardware, main and spare, provisioning space for that hardware, power sources, temperature control.

Another important aspect is security. By replacing network devices with virtualized applications, the risk of unauthorized hardware access becomes close to impossible, which alleviates a renown network security attack vector.

It is necessary to notice, that even though we often mention security as a technical advantage of all virtualization technologies, this fact remains to be a highly debated topic. While making a step forward in terms of security, at the same time we make two steps backward. Even without going into detail, simply the increase of the code base that implements virtualization gives a larger attack surface for malicious intents. Existing NFV security approaches recommend applying corresponding hardening techniques to each separate security domain of the virtualization scheme [4, page 20,22].

Another challenge that NFV introduces is performance. In the beginning of NFV development, hardware platforms were not completely ready for network virtualization. It turned out that virtualization poses a great amount of issues for network performance. It turned out that transferring packets from the physical connection to the virtual guest required a significant increase of the amount CPU interrupts. This created a major bottleneck for all virtual network function implementations.

Vendors have reacted to these problems, for example Intel has introduced technologies such as Virtual Machine Device Queues VMDq and Single Root Input/Output Virtualization (SR-IOV). VMDq allows each virtual machine to recieve network messages on it's own queue, removing the necessary interupts of the hypervisor CPU [10]. SR-IOV allows the NIC to provide seperate resources, such as memory space and a transmit and receive queue, directly to a VM. According to Intel, this should allow VNF to achieve 10Gb on selected hardware [9].

These solutions are considered to be a compromise: the hypervisor bypassing techniques that are utilized by SR-IOV pose restrictions on the possibility to orchestrate network functions, since SR-IOV is dependent on hardware support.

Another challenge is the organizational aspect of NFV. NFV is a distinctly new concept in networking. In order to implement it, we must consider not only technical aspects, but also organizational issues. Not only must NFV users replace heaps of existing networking hardware with new commodity off the shelf hardware (COTS), but they should also reassess existing processes. Switching to a NFV environment is a serious investment which requires engagement from all departments - IT, marketing, top management, sales and R&D. While some telecommunication companies have began integrating NFV, the return of investment is not easy to estimate for a large amount of other companies. A reason for this is that simply virtualizing previously available hardware network functions is just a minor step towards becoming a cloud telecommunications provider, a step which brings practically little business value. A large percentage of companies call high level organizational issues their major roadblock for NFV [2].

Lack of a standard orchestration tool is also a major impediment. At the moment of writing the purposed effort to bring management and orchestration (MANO) to the NFV standard OPNFV is barely half an year old. This is expanded in the MANO section.

The fact that NFV allows COTS hardware to be used creates another challenge: vendors experience reluctance towards NFV. This is not really a technological issue of NFV in general, as much as a business model one. Large network equipment companies are not eager towards NFV development since it is very likely to damage their profits. Key problems are:

- NFV makes existing developed technologies that took years to develop obsolete
- NFV is a vendor agnostic technology that frees com-

- panies from proprietary lock-in. Companies have no incentive to achieve that.

As a result, it can be expected that equipment producers might try to develop their own version of NFV.

As mentioned earlier, hardware replacement is a burden even for the network owners. Companies have spent a great amount of money and years building their network systems. Replacing recent hardware and existing support contracts is not an attractive decision, especially while some companies are still struggling to get rid of their legacy network technologies.

2.2 NFV Standards

A major complaint among companies interested in NFV was the lack of guidance in the implementation of NFV [20]. Particularly the telecommunications industry has strict requirements for security, performance and reliability, therefore it is fair to state that the success of NFV relies on standards. Several institutes have been making efforts in the standardization of NFV.

2.2.1 *TM Forum*

TM Forum (formerly TeleManagement Forum) decided to consolidate their operations management expertise across their members in order to realize a "Zero-touch, Orchestration, Operations and Management" (ZOOM) strategy for NFV implementations. The ZOOM project is supposed to build a new clear architecture blueprint that will enable flexible and agile virtual network services [23]. TM Forum focuses on bringing together organizations interested in NFV to address various challenges of the technology, while working together with ETSI and other efforts. An example of such work groups are various Catalysts, which are "rapid fire, member-driven proof-of-concept projects which both inform and leverage TM Forum best practices and standards" [22].

2.2.2 *OASIS TOSCA / IETF YANG*

Developed by The Organization for the Advancement of Structured Information (OASIS), the Topology and Orchestration Specification for Cloud Applications (TOSCA) is a standard language built specifically for orchestration of different cloud based web services. The TOSCA NFV profile specifies a Network Functions Virtualisation (NFV) specific data model using TOSCA language [12]. Complementary with YANG, a data modeling language for the Network Configuration Protocol created by the IETF [7], TOSCA can be used to manage and deploy NFV in an automated manner, where YANG is responsible for configuration and TOSCA is used for the orchestration mechanism.

2.2.3 *Linux Foundation*

In September 2014 the Linux Foundation has founded OPNFV. The goal of the organization is to accelerate the development of NFV technology by developing an integrated open source ecosystem that includes existing open source software an allows new solutions to be developed with the participation of vendors [13].

3. OPNFV

It has been 2 years since the Open Platform for NFV Project (OPNFV) has began working, and has already delivered on two software versions and developed an expansive series of questions regarding requirements, architectures and use cases for NFV.

3.1 OPNFV versions

3.1.1 *OPNFV Arno*

8 Months since it's creation, OPNFV was ready to release the first software version called Arno. It's main elements featured the Linux based virtualization solution KVM as hypervisor environment and an OpenStack architecture with an OpenDaylight-based SDN controller. Key capabilities of OPNFV Arno included:

- the ability for the users to deploy NFVs on the platform to test their functionality and performance
- a continuous integration toolchain that allows projects to do automatic builds and verification as Open-Source components are developed independently.

It was expected that Arno would attract users to explore the platform and it's capabilities to satisfy their networking requirements, therefore accelerating NFV integration in the industry. [14]

3.1.2 *OPNFV Brahmaputra*

Brahmaputra is the second and latest version of OPNFV. According to Chris Price, technical steering committee chair of the project: "Building on the foundation of Arno, the OPNFV community worked tirelessly to integrate and combine components from multiple communities to deliver Brahmaputra, which brings end-to-end feature realization" [18]. Brahmaputra includes almost double the projects that Arno had and brings enhancements such as: layer 3 VPN management, initial support for IPv6, better fault detection and recovery, developements with Data Plane Development Kit (DPDK) for data plane performance boosts and improved infrastructure testing capabilites [18].

3.2 OPNFV projects

OPNFV manages activities in form of projects, created by the Technical Steering Committee. Each project has a team of commiters, which manages it and reviews contributions. As of writing, OPNFV has little over active 40 projects [15]. Many of these projects are critical for the success of NFV, for example OPNFV DPACC, that addresses the issues in data plane performance that where discussed in section 2. Describing every single one of them in detail is not within the scope of this paper, so only a couple would be described.

3.2.1 *OPNFV Doctor*

OPNFV Doctor is a project that maintains network function status awareness and uses a notification system to warn in changes of the statuses. The Doctor project is a key enabler of High-Availablity (HA) for network functions, since it can signal Virtual Network Function Managers to take recovery actions once a failure has accured [16].

3.2.2 OPNFV Prediction

The Prediction system consists of a data collector, a predictor and a management module. Tools such as OpenStack's Celiometer and Monasca are used for data collection and are interact with other tools such as Zabbix or Nagios. Prediction runs real-time analysis and applies machine learning techniques on the data provided by the collection tools and then sends notifications to the Virtual Network Function Managers that will act upon the notification [19].

3.2.3 OPNFV MANO

In 2015 the OPNFV has approved the MANO ”requirements for integration” founded by Telefónica, RIFT.io, Mirantis, Intel, and Canonical. Until that moment, OPNFV was limited to virtualized network function and accompanying lower layer management [17]. By including MANO, OPNFV now openly works on a full NFV reference implementation. According to industry representatives, the lack of a management and orchestration layer was a common reason that kept operators reluctant towards NFV.

3.3 OPNFV Architecture

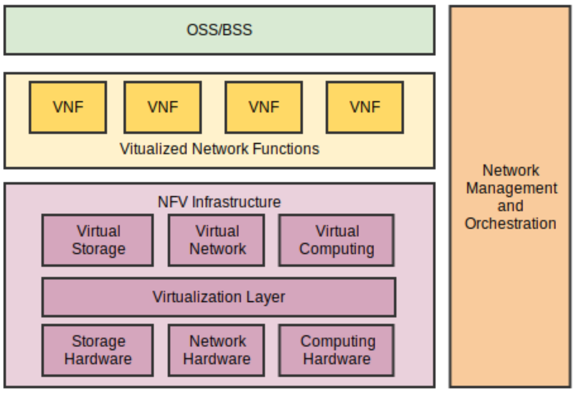

Figure 2: OPNFV architecture

The current top-level state of the OPNFV project structure is displayed on Figure 2 according to [15].

- Virtual Network Function
  Technically, a virtual machine (VM) or a group of VMs that realize the given Virtual Network Function (VNF). VNFs are controlled by the Element Management System.
- Network Function Virtualization Infrastructure (NFVI)
  The physical hardware that constitutes as the infrastructure of the network, their configurations. These include the servers, storage devices, virtual switches, hypervisors and others.
- NFV Management and orchestration
  The part that controls VNFs and the underlying infrastructure and their operations. The management component controls VNFs and the Orchestration controls the NFVI.
- Operations/Business support systems (OSS/BSS)
  Systems for monitoring, control, billing, provisioning, into which NFV are integrated either through MANO, or one by one through direct interfaces.

4. USE CASES

It is always important that any new technology does not remain to be a solution looking for a problem. NFV can be proven to be anything but that, by viewing it from several perspectives: helping cloud providers in datacenter management, helping Internet service providers by easing customer service and even bringing flexibility in factories of the future to a new level.

4.1 Datacenter network optimization

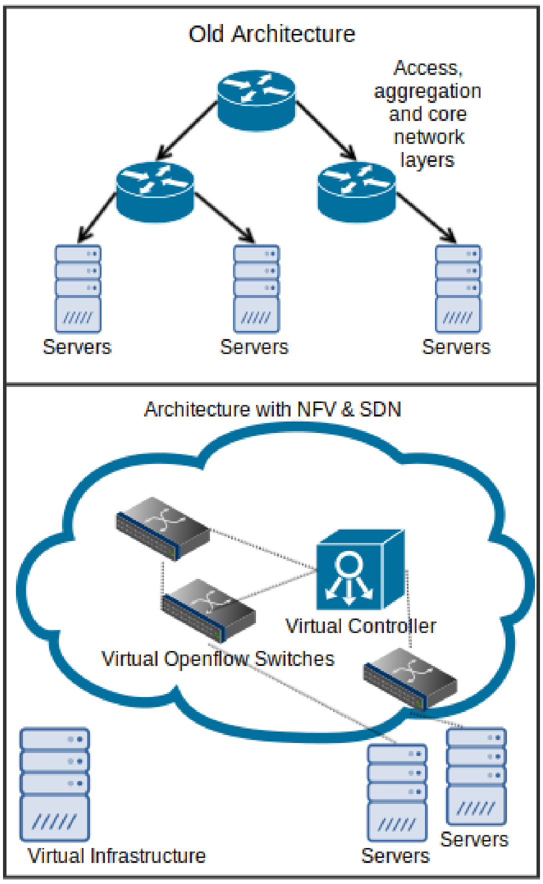
Old Architecture
Access, aggregation and core network layers
Servers
Servers
Servers
Architecture with NFV & SDN
Virtual Controller
Virtual Openflow Switches
Virtual Infrastructure
Servers
Servers

Figure 3: SDN and NFV in the datacenter

NFV pared with Software Defined Networks (SDN) can bring a new level of flexibility to modern datacenters. A rough explanation of SDN is that SDN is an effort to separate the control and data plane, while using a standardized and centralized controller. The controller manages forwarding rules in the data plane by sending messages to SDN switches. The currently popular implementation of SDN is a standard called OpenFlow. By uniting NFV and SDN in their datacenters, organizations can finally consolidate their regular systems operations with network operations, allowing more flexibility, scalability and availability. SDN simplifies the orchestration of virtual SDN switches by abstracting the configuration and those network functions all feature benefits of virtualization discussed in section 2. The SDN controller

doi: 10.2313/NET-2016-09-1_08

can also be virtualized. The concept comparing the old architecture and NFV/SDN one is illustrated on figure 3.

4.2 Customer Gateway Virtualization

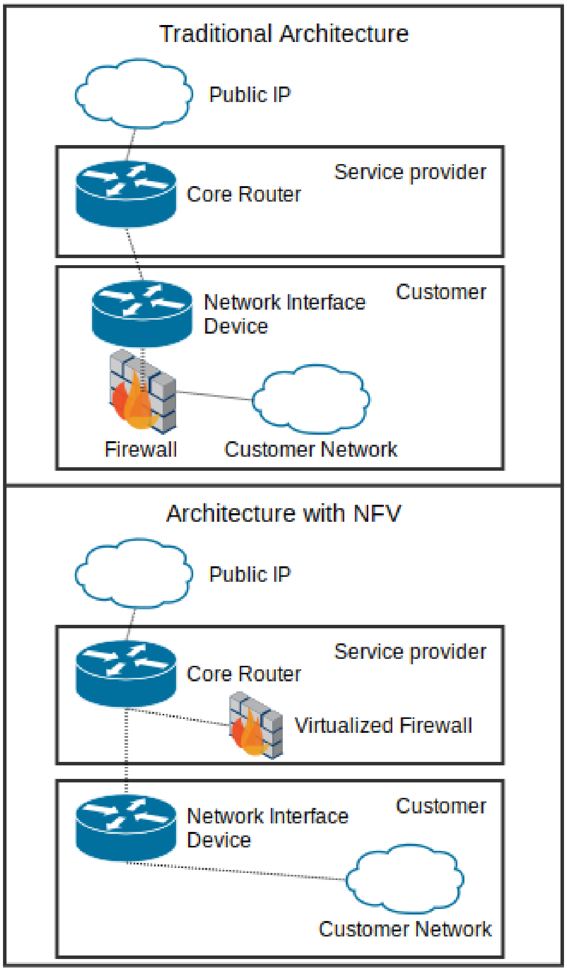

Figure 4: Deployment of a firewall

When a new customer connects to the network of an internet service provider (ISP), usually the ISP assists in hardware installation: either on site, or by providing device settings. Some customers would appreciate additional network services, such as firewalls, VPN support, and DDoS protection. Often the customers are small and medium businesses without an established IT team. The operation of supporting these setups is not a straightforward task, especially since the customer requirements for their network are hard to predict.

NFV can allow the ISP to provide the customer with a simple gateway device which will have all of the network function logic on the servers of the provider. Figure 4 illustrates an example of how a service such as a firewall can be deployed. Large organizations can also apply the same principle inside their corporate intranets to organizational units, while hosting the network functions in their own datacenter.

This will allow end users to rent a network service, while the ISP handles everything behind the curtains. Since deploying a new virtual network function is much faster than a piece of hardware at the users site, this brings a series of advantages: functions are deployed more quickly and have increased elasticity, meaning that functions can be deployed promptly at any time.

4.3 NFV for Industrial Systems

Industrial automation has been considered to be a conservative field, though various industries have already began adapting technologies from the IT world, including networking and virtualization.

In the last decades, controlling machines in industry automation and in Supervisory Control and Data Acquisition (SCADA) systems have begun using more and more technologies and standards which are built upon Ethernet and Internet technologies, instead of the usual CAN, Fieldbus and EtherCAT. For example, the Siemens SIMATIC S7-300 controller has support for the CP 343-1 Lean communcations processor, that add support of TCP/IP, UDP, and Ethernet to the controller. [21]

Industrial automation systems have been receiving new requirements such as adaptability and distribution. This has even led to IEC developing a new standard under the code 61499. The IEC 61499 standard provides the architecture, tools and rule of compliance for development of distributed and reconfigurable automation and systems [6]. The pharmaceutical industry is a great example of a field where quick reconfigurablity could give benefits - the product range changes quickly and the software logic behind production needs to changed often, much more often than the hardware.

An example of such an existing production system virtualization deployment is a New England Controls project in a pharamaceutical company Biogen [11]. The project was deemed to be a success. More similar proofs of concept show that this is just a beginning. Another example is a TM Forum Catalyst (discussed in section 2.2) called Smart Industrial Manufacturing which explores a concept ”Robot As a Service”, where multiple robot cells can be reconfigured through a hardware abstracted API. [24]

IEC 61499 introduces a number of principles that can appear to be analogous to those that exist in the virtualization scene, as well as NFV and even SDN. Control applications are distributed to control devices in a similar way how virtual machines are deployed to hypervisors. Some similarities could be drawn between the separation of data and event flow proposed by IEC 61499 and the data and control plane separation concept ingrained in SDN technologies. [6]

It is logical to assume that the next step would be to adopt network function virtualization in industrial components and systems, once manufacturers become more confident in the capability of virtualization technologies to meet their requirements. It is also fair to expect that a standardization effort will be crucial for the adoption of NFV, particularly requirements for real-time operation.

5. PROOF OF CONCEPTS

According to IHS, 82% companies have evaluated or deployed SDN in their networks, though the deployment scale remains very small. SDN is a more mature technology than NFV, though already 35 % of companies surveyed planned to deploy NFV in 2015 [8]. Looking in to existing deployments should give an idea how NFV is expanding in the industry.

5.1 CMCC in Shaanxi

In September 2015, China Mobile began a pilot deployment of a cloud-based network core. This started a period of NFV testing in live mobile networks in China. In this pilot project, Huawei, together with the Shaanxi Branch of China Mobile, performed a comprehensive set of verifications and a small-scale field trial of the cloud-based network [5]. Even though Shaanxi is only a small province of China, CMCC has about 24 million customers in the network, of which 6 million use LTE provided by 29 thousand LTE stations [1].

According to Huawei, "the trial was aimed at verifying the cloud-based networking, technical specifications, service capabilities, maintenance, and full lifecycle management, laying a solid foundation for large-scale trial and commercial use of cloud-based core networks in the future [5].

On December 10, 2015, China Mobile made the first VoLTE call over the pilot NFV-based network. This cloud-based VoLTE call demonstrated that the IMS system deployed in a multi-vendor hardware environment had successfully connected with a live network. Achieving this step was not possible without problems. Key issues encountered during the pilot project were [1]:

- High Equipment cost. Even though commodity hardware from multiple vendors could now be used, the purposed benefit of cost reduction didn't realize. Up to 600 servers were purchased, but due to organization problems average load stayed at about 20%.
- Slow Time to Market, up to 9 months
- High Servicing costs
- Consolidation organization problems, due to various departments owning hardware.

5.2 Orange Global Software-Defined WAN

ClearPath together with Orange and Intel demonstrated a joint proof of concept at the 2015 OPNFV summit that showed secure, distributed virtual Customer premise equipment, a concept discussed in section 4. According to Clearpath, their "NanoServices, open source VNFs, and containers significantly reduce vCPE costs for each end user" [3]. The report confirms that customer gateway virtualization, built according to the OPNFV reference implementation, is a viable NFV deployment.

6. CONCLUSION

In this paper, we have examined the novel technology of network function virtualization. NFV has been gaining an increasing amount of interest from the networking industry. Modern datacenters, cloud providers and telecommunication companies are processing ever-increasing data volumes, which makes network agility a most important goal. NFV is proven to be a key enabler of the demanded flexibility.

We have examined the concept of NFV and currently existing standards, including one particular standard, OPNFV, which was analyzed in greater detail. OPNFV has been making serious advances in building an effort to provide a much needed guidance in NFV implementation. An increasing amount of projects backed by large vendors induces the support that it is receiving from the interested industry members.

Current use cases and proof of concepts demonstrate that NFV brings it's benefits to existing and new networking models, such as operator networks and customer gateway virtualization. It's advantages could serve not only operators, but also industrial systems and data centers. We concluded that the standardization efforts will probably need to be developed further in order for NFV to enter new fields, such as the automation industry.

We observed that NFV still has certain challenges to go through. Key issues have to be addressed before NFV adaptation becomes more widespread. Nevertheless, we believe NFV is going to be one of the most revolutionary technologies for networking in the following decade and the development of standards like OPNFV is the key towards advancements in network function virtualization.

7. REFERENCES

[1] Aleksey Shalaginov. Operator SDN: Implementation Attempt (Operatorskie seti SDN: Opyt realizacii), 2016. https://shalaginov.com/2016/05/16/%d0%be%d0%bf%d0%b5%d1%80%d0%b0%d1%82%d0%be%d1%80%d1%81%d0%ba%d0%b8%d0%b5-%d1%81%d0%b5%d1%82%d0%b8-sdn-%d0%be%d0%bf%d1%8b%d1%82-%d1%80%d0%b5%d0%b0%d0%bb%d0%b8%d0%b7%d0%b0%d1%86%d0%b8%d0%b8/; last accessed on 2016/06/19.

[2] Dr. Jim Metzler, Ashton, Metzler and Associates. When Will NFV Cross the Chasm. http://ashtonmetzler.com/When%20will%20NFV%20Cross%20the%20Chasm.pdf; last accessed on 2016/06/19.

[3] Dustin Do. ClearPath teams up with Orange and Intel to enable secure managed services for the enterprise, 2015. http://www.clearpathnet.com/clearpath-teams-up-with-orange-and-intel-to-enable-secure-managed-services-for-the-enterprise/; last accessed on 2016/06/19.

[4] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal. Nfv: state of the art, challenges, and implementation in next generation mobile networks (vepc). *IEEE Network*, 28(6):18–26, Nov 2014.

[5] Huawei. NFV Has Entered the Fast Lane: Core Networks will be the First to Take a Stroll in the Clouds, 2016. http://www.huawei.com/en/mwc2016/topics/nfv-has-entered-the-fast-lane; last accessed on 2016/06/19.

[6] IEC. IEC 61499 - The New Standard In Automation.

http://www.iec61499.de/; last accessed on 2016/06/19.

[7] IETF, M. Bjorklund, Tail-f Systems. RFC6020, 2010. https://tools.ietf.org/html/rfc6020; last accessed on 2016/06/19.

[8] Infonetics Research. 35 Percent of Operators Surveyed Will Deploy NFV This Year, 2015. http://www.infonetics.com/pr/2015/NFV-Strategies-Survey-Highlights.asp; last accessed on 2016/06/19.

[9] Intel. PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology. https://www-ssl.intel.com/content/www/us/en/pci-express/pci-sig-sr-iov-primer-sr-iov-technology-paper.html; last accessed on 2016/06/19.

[10] Intel. Virtual Machine Device Queues. https://www-ssl.intel.com/content/www/us/en/ethernet-products/converged-network-adapters/io-acceleration-technology-vmdq.html; last accessed on 2016/06/19.

[11] Matthew Daniels, Michael Kalvaitis. Virtualized Infrastructure Leads to More Flexible Process Automation for Pharmaceutical Manufacturers, 2016. http://files.massbio.org/file/Virtualized-Infrastructure-Takes-Hold-at-Biogen.pdf; last accessed on 2016/06/19.

[12] OASIS. OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC, 2016. https://www.oasis-open.org/committees/tosca/; last accessed on 2016/06/19.

[13] ONF. https://www.opennetworking.org/about/onf-overview, 2016. https://www.opennetworking.org/about/onf-overview; last accessed on 2016/06/19.

[14] OPNFV. OPNFV Arno. https://www.opnfv.org/news-faq/press-release/2015/06/opnfv-delivers-open-source-software-enable-deployment-network; last accessed on 2016/07/20.

[15] OPNFV. OPNFV Wiki. https://wiki.opnfv.org/; last accessed on 2016/06/19.

[16] OPNFV. Doctor Wiki, 2016. https://wiki.opnfv.org/display/doctor/Doctor+Home; last accessed on 2016/06/19.

[17] OPNFV. MANO Wiki, 2016. https://wiki.opnfv.org/display/PROJ/OPNFV-OPEN-O; last accessed on 2016/06/19.

[18] OPNFV. OPNFV Delivers Second Release of Open Source Network Functions Virtualization Platform , 2016. https://www.opnfv.org/news-faq/press-release/2016/03/opnfv-delivers-second-release-open-source-network-functions; last accessed on 2016/06/19.

[19] OPNFV. Prediction Wiki, 2016. https://wiki.opnfv.org/display/prediction/Prediction; last accessed on 2016/06/19.

[20] Ray Le Maistre. Vodafone Demands More From NFV Vendors, 2016. http://www.lightreading.com/nfv/nfv-strategies/vodafone-demands-more-from-nfv-vendors/d/d-id/723690; last accessed on 2016/06/19.

[21] Siemens. CP 343-1 Lean. http://w3.siemens.com/mcms/industrial-communication/en/ie/system-interfacing/simatic-s7-sinumerik-o/s7-300/pages/cp343-1lean.aspx; last accessed on 2016/07/20.

[22] TM Forum. Catalyst Program. https://www.tmforum.org/collaboration/catalyst-program/; last accessed on 2016/06/19.

[23] TM Forum. ZOOM (Zero-Touch Orchestration Operations and Management). https://www.tmforum.org/zoom/; last accessed on 2016/06/19.

[24] Tony Poulos. Industrial manufacturing gears up for robots as a service, 2016. http://inform.tmforum.org/features-and-analysis/featured/2016/04/industrial-manufacturing-gears-up-for-robots-as-a-service/; last accessed on 2016/06/19.