5G Americas Whitepaper

THE STATUS OF OPEN SOURCE FOR 5G

FEBRUARY 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"5G" and "open source" are by far two of the hottest topics in the telecom industry over the past few years. Mobile operators worldwide are pioneering these technologies by leading the standards organizations and establishing, funding and contributing to community-driven projects. Mobile operators also have begun deploying the solutions produced by these projects to demonstrate the real-world benefits of 5G and open source. Security is also an important consideration when moving to open source. The pros and cons of security need to be fully understood by any entity moving to open source.

5G system architecture has been defined, but many of these initial deployments are expected to have the interoperability challenges that 3G and 4G faced. However, 5G system architecture gives mobile operators more openness than previous generations. Operators will need to take advantage of open source principles in order to stay, or become, competitive in the marketplace.

This 5G Americas white paper provides an overview of 5G architecture, with a focus on its applications of open source principles. It also explores how this combination will benefit mobile operators and their customers.

1. INTRODUCTION

3GPP Release 15 defines the 5G system architecture. A key component is Service-Based Architecture (SBA), which enables modularization of network functions and aligns well with the Network Function Virtualization (NFV) and Software-Defined Network (SDN) principles. Together, these provide agility and flexibility in terms of resource placement and efficient resource utilization, reducing time-to-market for new services and thus helping operators stay or get competitive. Efficient processes also are required for rapid development and deployment of software, while keeping up with the stringent service performance requirements.

Over the course of the past couple of decades, many open source projects have been highly successful. Large global developer communities have been solving various technical challenges that the telecom industry has faced, and constant release of the solutions keep the security and feature/functionality at pace with the needs of end users.

This paper discusses the applicability of the open source on 3GPP Release 15-defined 5G system architecture. It covers key aspects such as:

- **Open Source Model**
  - Provides different license types and importance of governance models
  - Compares similarities and differences between the standards and open source models
- **5G Architecture**
  - Gives a high-level overview of the 5G system architecture per 3GPP Release 15
- **Open Source Applicability in 5G**
  - Discusses the opportunities in open sourcing key areas of the 5G system architectures and network infrastructure
  - References existing open source efforts in the respective areas

2. OPEN SOURCE (OS) MODEL

In actuality, open source existed in the beginning of the computing industry, as the original computer operating software and compilers in the 1950s and 1960s were delivered as a part of hardware purchases without separate fees. At the time, source code, the human-readable form of software, was generally distributed with the software providing the ability to fix bugs or add new functions. Universities were early adopters of computing technology. Many of the modifications developed by universities were openly shared, in keeping with the academic principles of sharing knowledge, and organizations sprung up to facilitate sharing. As large-scale operating systems matured, fewer organizations allowed modifications to the operating software, and eventually such operating systems were closed to modification.

2.1 WHAT IS OPEN SOURCE?

The term “open source” refers to something people can share, modify and use via an openly available design. Open source, as applied to software, permits sharing via inspection, copying, learning, altering or distribution. Code or binary distribution may be permitted, depending upon the software license. Software licenses, which must be accepted by users, usually dictate how attribution of the work and the license are distributed with the software.

Software labelled as open source may be licensed under an Open Source Initiative (OSI)- approved license or a bespoke license that is developed by a project to meet the objectives of Open Source, while preserving compatibility with the project’s specific needs and policies. OSI-approved licenses follow the Open Source Definition (OSD), which provides 10 criteria[1] that must be met. Open source software can be used for any commercial purpose, but the copyright holder cannot restrict how it is used or who can use it. Open Source is a generally loose term, but for the purpose of this document we define Open Source as following the Open Source Definition.

Software alteration is permitted, but the license may require those alterations to be shared in some manner. “Copyleft”[2] licenses permit alteration (therefore, the creation of a derivative, under the condition that they use the same license as the original).[3] Although many copyleft licenses are open source, not all open source licenses are copyleft.[1] In such cases, the non-copyleft license permits software released under the original license to be used as a part of works that may be under different licenses. These licenses may even be proprietary (“non-open source” or “closed source”), which is controlled by the copyright holders of the combined work.

Some license types refer to a specific combination of sharing, modification and usage. For example, a “permissive” license is a term applied to one that grants freedom to use, alter and redistribute while permitting derivative works that may be proprietary. On the other hand, copyleft only affects how derivative works are licensed, and the original license may not follow a specific type.

Open source, as applied to hardware, refers to design specifications of a physical object that are licensed in a manner that the object and associated specification can be modified, studied, produced or distributed.

Section 2.1 is a heavily condensed version of the concepts presented at https://opensource.org/faq and https://opensource.com/resources/what-open-source.

[1] https://opensource.org/osd-annotated

[2] https://www.gnu.org/licenses/copyleft.en.html

[3] *What is "copyleft"? Is it the same as "open source"?* https://opensource.org/faq#osd. May 15, 2018.

2.2 GOVERNANCE MODELS MAKE A DIFFERENCE

The governance model in open source is one factor to be considered for new projects. The choice implications can be profound with regards to the adoption and continued need for contributions. While the licensing model for open source provides a legal framework, the governance model provides a social framework for collaboration. A good governance model must be well-defined and include documented rules for engagement, which is how decisions are made in order to nurture a healthy, long-term community.

Transparency is also extremely important as it helps the community understand how decisions are made and by whom. The leadership teams' constituency and its structure must be diverse to appeal to a broad group of stakeholders while avoiding tilting the balance toward specific business interests.

Depending on the projects' original intent, the seeding contributors and their strategic objectives, decisions can be made by appointed leads from specific organizations, elected ones on a merit-based criterion or a combination. A meritocracy-based governance is perceived as being more open and can encourage more participation, which in return will result in more opinions and potentially some overlapping code contributions that require consolidation/harmonization. This can translate into faster cycles, but it can also result in major architectural changes from the original seeding project. Some open source communities put the control in the hands of a commercial entity, while others are established around non-profit organizations that are vendor neutral.

There is no good or bad governance model for a specific project. The decision to choose one over the other has to do with finding the best tradeoff between control, process, agility and quality.

2.3 STANDARDS-BASED OPEN SOURCE VS. OPEN SOURCE IMPLEMENTATIONS

With the rise in popularity for open source projects, a common question regards the value of standards. Many people perceive open source as a competing force in the establishment of "de-facto" standards for various industries.

There are quite a few similarities between the standards and open source paradigms. Both have the objectives of increasing interoperability, reducing costs and facilitating the establishment of a healthy business ecosystem. The difference has to do with the method to achieve those goals.

Historically, standards have been developed using consensus-based collaboration in a process that required written documentation of the specific standard (for example, a specification, protocol, an Application Protocol Interface (API)). This is no different than open source projects, with the exception that for open source, contributions are in a form of running code.

Usually the collaboration process in standards is a very transparent one based on less transparent or even proprietary implementations. Open source projects can bring implementation transparency during the harmonization/standardization process, as well as after the finalization of a standard as a way to establish reference implementations.

Therefore, open source projects should be considered complementary to standards development, as a way to accelerate and improve the process of creating interoperable solutions. Figure 2.1 shows where standards and open source initiatives work together to benefit vendors, service providers and end users. Combined with automation tools, continuous testing and integration, as well as broad adoption of DevOps

within large organizations, this combination can be a powerful catalyst for innovation and rapid development.[4]

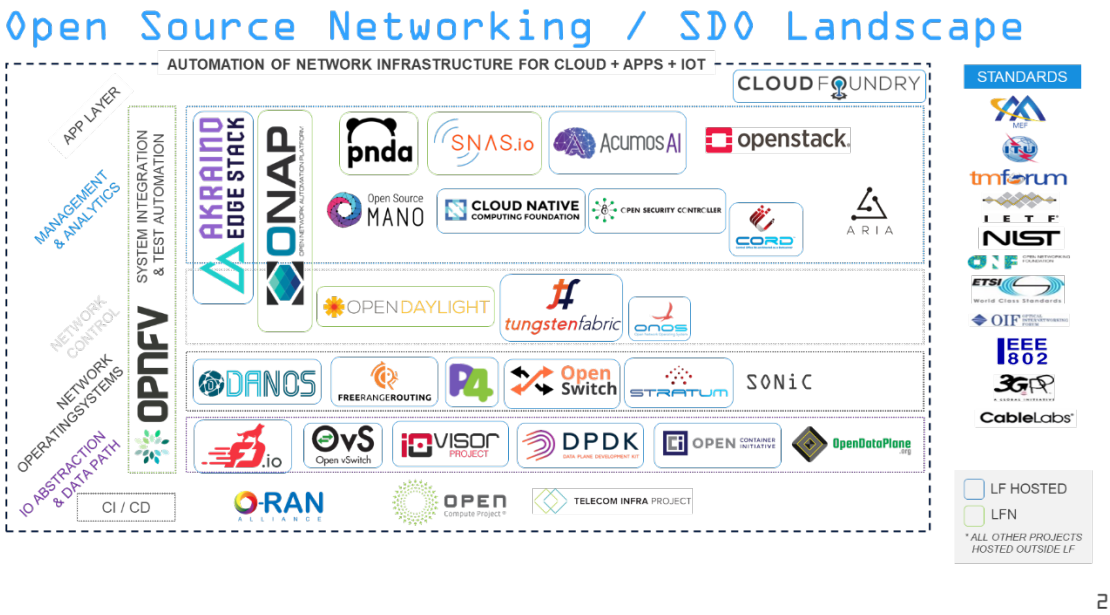

Figure 2.1. Open Source Projects and Standard Organizations[5].

3. 5G ARCHITECTURE

3GPP is the key industry body behind 5G technologies, but numerous other industry forums also have been developing 5G. O-RAN Alliance, an initiative formed in 2018 to drive openness and intelligence for the next generation wireless networks, is gaining traction in becoming the main forum focusing on open RAN architecture. Section 3 primarily references the work in 3GPP Release 15 and O-RAN initial architecture to describe the 5G system architecture.

3.1 5G CORE NETWORK

The trend towards the "softwarization" of telecommunication networks has been a major consideration in the development of 5G Next Generation Core (NGC) specifications. Following this trend, for the control plane in the 5G NGC, 3GPP decided to move away from traditional monolithic logical functions that used telecom-centric protocols to communicate by adopting an architecture that it defined as "service based." In this new Service-Based Architecture (SBA), the control plane is more modularized than the 4G Evolved Packet Core (EPC). These modules are called the network functions (NFs). Internally, the NFs comprise of one or more services that can be described as sub modules. Interaction between NFs is based on Service-Based Interfaces (SBIs) that are generally web services conforming to the Representational State Transfer (REST), or RESTful in nature.

Another aspect of the 5G architecture that brings it closer to "cloudification" and softwarization is the concept of network slicing. With this concept, it is now possible to virtualize the 5G core and run several

[4] https://www.researchgate.net/publication/275037585/download
[5] Source: Linux Foundation

logical instances of the 5G NGC in parallel, each instance being optimized to cater to, for example, certain customers, services or traffic types.

Prior to the start of 5G work in Release 14, the EPC had already separated the User Plane (UP) and Control Plane (CP) functions of the packet core. This concept of CP and UP separation, which is also aligned with SDN principles, was carried forward into 5G and used as a basis for the 5G system. Coupled with further modularization of the 5G control plane and introduction of concept of network slicing, 5G can be considered a much more flexible, scalable and adaptable mobile system compared to 4G.

Figure 3.1 shows the SBA as defined in 3GPP Release 15 with additional information about the NFs. More detailed information can be found in 3GPP TS 23.501.[6]

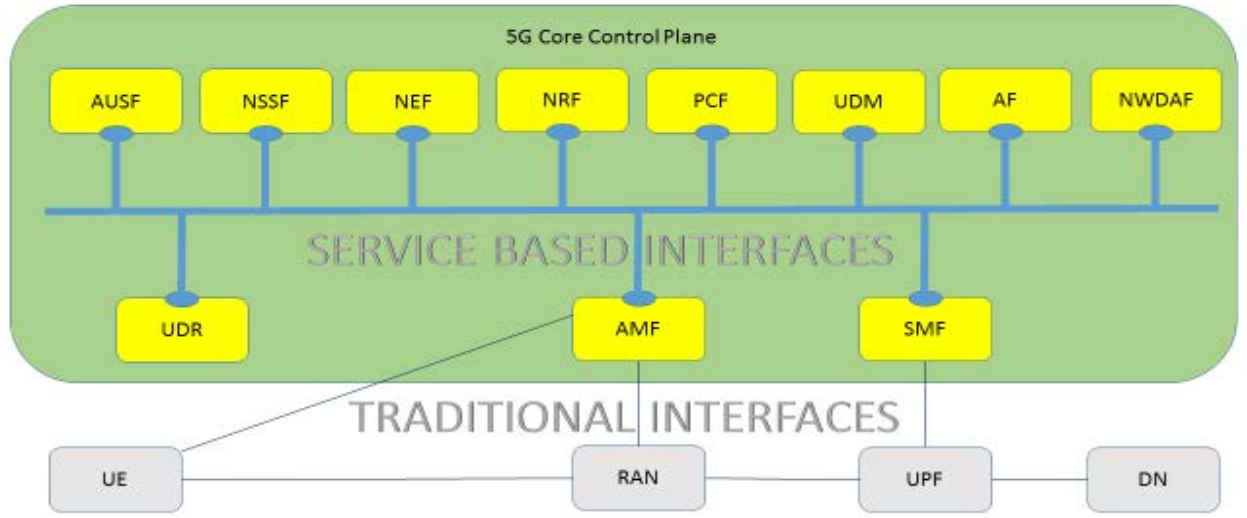

Figure 3.1. 5G NGC - Service Based Architecture.

3.1.1 CONTROL PLANE (CP)

Access and Mobility Management Function (AMF)

AMF is responsible for the termination of the Radio Access Network (RAN) CP interface, carries Non-Access Stratum or NAS signalling (therefore, communication between the User Equipment (UE) and Core) and terminates ciphering and integrity protection for communication over NAS. Some of its key functionalities include access authentication and authorization, mobility, reachability and connection management.

[6] 3GPP System Architecture for the 5G System.

Session Management Function (SMF)

The SMF is responsible for session-management-related functionalities including User Plane Function (UPF) tunnel maintenance and UE Internet Protocol (IP) address allocation. It also has roles in UPF functionality selection, in lawful intercept and in charging- and policy-related communication between the CP and UP.

Policy Control Function (PCF)

The PCF provides unified policy framework for use by the network operator. Among other inputs, it also makes use of subscriber data stored in the Unified Data Repository (UDR) and develops policy rules for the control plane that help manage network behaviour.

Network Exposure Function (NEF)

The NEF exposes capabilities and events from one NF to other NFs and to third parties. In the process, it stores and retrieves data in the UDR as needed. When third-party exposure is used, the Common API Framework (CAPIF) is also supported by the NEF to offer common sets of functionalities such as third-party authentication.

Network Repository Function (NRF)

The NRF maintains a list of available NF instances and the services that each NF supports. NRF may have such info at a slice level or at Public Land Mobile Network (PLMN) level. It is used by an NF instance for discovery of other NF instances where the requested service may reside. It can also be used in a roaming case.

Unified Data Management (UDM)

The UDM is responsible for functionalities such as generation of authentication credentials and for access authorization based on subscription. Located in the Home PLMN (HPLMN), the UDM uses UDR for storage and retrieval of information used in its transactions.

Authentication Server Function (AUSF)

The AUSF supports functionality associated with authentication of the UE.

Application Function (AF)

An AF is used to interact with the 3GPP Core Network Functions such as PCF for influencing network policies, or NEF for accessing network capabilities and events. An AF can be owned by the operator or a third party.

Unified Data Repository (UDR)

An UDR is a common repository for subscription data, policy data and exposure-related data. A UDR, and an NF accessing, it is assumed to be in the same PLMN.

Network Slice Selection Function (NSSF)

The NSSF is used primarily for selecting instances of slices that would be used to serve a UE based on the information provided by the UE. The NSSF gets slice-level congestion information from the Network Data Analytics Function (NWDAF0 that can help in load balancing across multiple slice instances.

Network Data Analytics Function (NWDAF)

NWDAF is an operator-managed network analytics function. In Release 15, NWDAF provides only slice-specific congestion-related information to the NSSF and PCF.

3.1.2 USER PLANE (UP)

User Plane Function (UPF)

The UPF acts as the mobility anchor point for user data and hence is the mobility tunnel's termination point. It provides user connectivity to external networks. Along with packet routing and forwarding, it also performs operator policy enforcement (for example, Quality of Service (QoS), packet marking) in the user plane, lawful intercept, and collection of charging-related data. Not all functionalities need to be supported in a UPF instance. Multiple UPF instances can be placed in the path of IP flow with different sets of functionalities.

3.2 5G RADIO NETWORK

The 5G radio network comes with several deployment scenarios. For the sake of simplicity, this section covers only the basic 5G radio network. For example, only New Radio (NR) is shown in Figure 3.3.3; various options of dual-connected mode, where both LTE and NR are deployed, are not provided; also note that an O-RAN[7] based architecture is being developed by a new alliance with participation from major service providers.

A key aspect of 5G RAN is to disaggregate eNB/gNB into multiple modules (DU, CU-CP, CU-UP, etc.), see figure 3.2 and define standard interfaces between them (e.g. New Open Front haul, A1-o (OAM), A1-c (control) E1, E2, F1 etc.) to support interoperability between various components coming from different vendors. This is being done by O-RAN in parallel to 3GPP. Additionally, separating control plane (CU-CP) and user plane (CU-UP) of new radio allows operator to implement advanced area optimization applications (e.g. per UE level optimization, Mobility management, radio connection management, load balancing, etc.). Ultimate goal is to allow operators to leverage open source community to implement best in class area optimizations applications in a vendor neutral CU-CP that is flexible enough to support plug-n-play optimization algorithms. Some of these concepts are being introduced to the larger community in 2019 and would require performance objectives to be tested and proven in follow-on work.

[7] https://www.o-ran.org/resources/

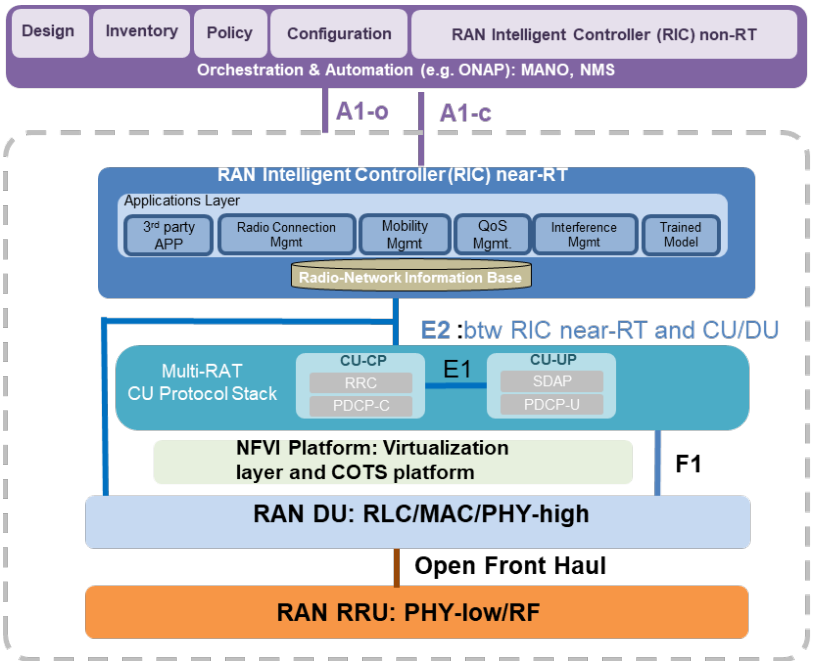

Figure 3.2. O-RAN Reference Architecture[8]

The primary functional element in a basic 5G radio network is the disaggregated element of gNB, CU-CP, which is a radio node responsible for connecting the UE to the 5G core. It terminates user and control plane traffic from a UE sent over the 5G air link. It then interfaces the control and user plane of the radio network to the 5G core. It also transparently passes signaling communication Non-Access Stratum (NAS) between the UE and the 5G core. A gNB can be further split into two sub modules.

gNB Central Unit (gNB-CU)

A gNB-CU is part of a gNB. It is a logical element that is home to higher layer radio protocols that can be placed in a more centralized manner. A gNB-CU controls the operation of one or more gNB-DUs and also communicates with other gNBs for tasks such as handovers. It has further CP and UP components as shown in Figure 3.2.

gNB Distributed Unit (gNB-DU):

A gNB-DU is part of a gNB. It is a logical element of home lower layer radio protocols that can be placed in a more distributed manner. One or more gNB-DUs are controlled by a gNB-CU.

As shown in Figure 3.3, a gNB-CU, along with one or more gNB-DUs, form a logical gNB. The interface connecting gNB-DU and gNB-CU is a point-to-point connection that carries both signaling and data traffic.

[8] https://www.o-ran.org/resources

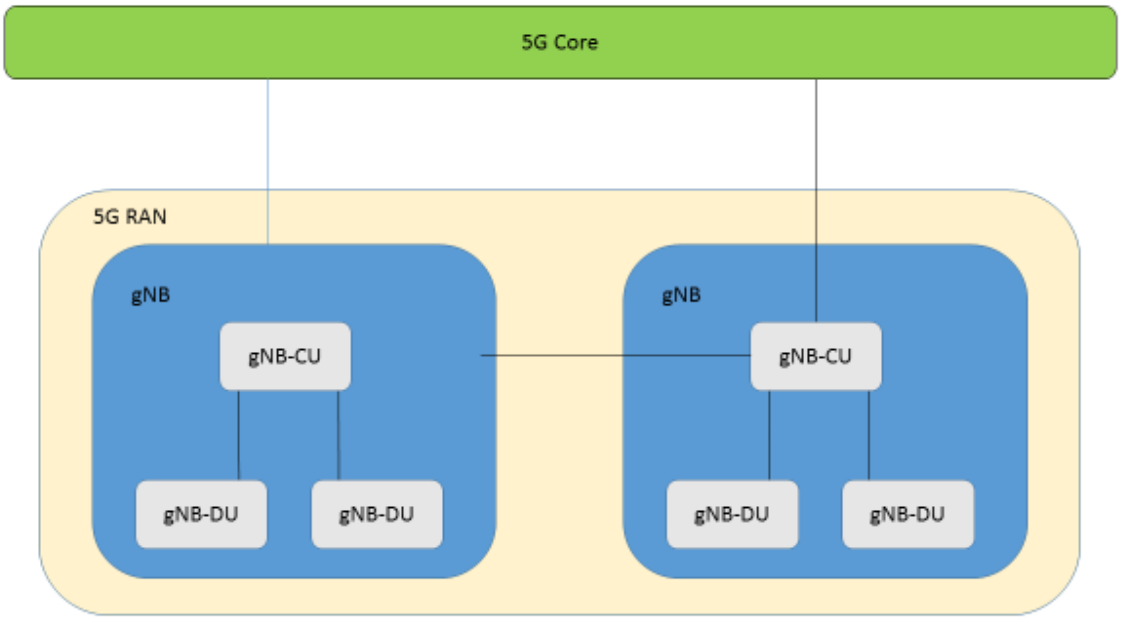

Figure 3.3. Simplified 5G Radio Network with NR.

3.3 CONVERGENCE – SUPPORT FOR NON-3GPP ACCESS

3GPP specifications have historically supported non-3GPP access types as part of 4G EPC. Examples of non-3GPP access types include Wi-Fi and wireline.

Traditionally, such support in 3GPP has been categorized into two types: untrusted and trusted. Untrusted can simply be described as an over-the-top model where it is assumed that local connectivity via non-3GPP access is available somehow and a secure tunnel is established between the UE and 3GPP network using 3GPP credentials.

For the untrusted model, 3GPP can develop solutions without external dependencies. In Release 15, as part of 5G work, only the untrusted model is supported. In Release 16, 3GPP is collaborating with the Broadband Forum to support the trusted model in 5G. Figure 3.4 shows a high-level architecture for the untrusted model that is supported in Release 15. Only key elements of the 5G core are shown. For example, a multi-access UE can be connected simultaneously to 5G NR and Wi-Fi/wireline. In this case, multiple data and signaling paths will exist from the UE.

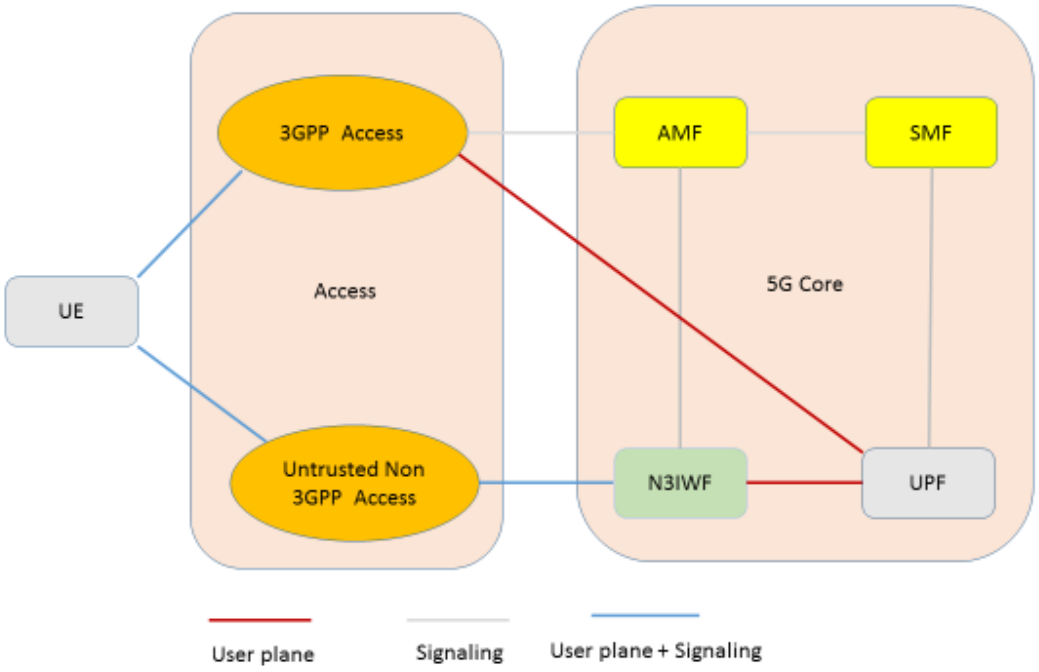

Figure 3.4. Support for Convergence in Release 15.

N3IWF

The key element of the untrusted access model is a new function named “Non-3GPP Inter-Working Function” (N3IWF). The UE uses N3IWF to connect to the 5G core over a non-3GPP access layer. N3IWF terminates the security tunnel from the UE side and terminates signaling and data plane from 5G core functional entities. The UE is assumed to support the 5G signaling plane (NAS). N3IWF carries both NAS and user plane data between the UE and 5G core functions.

4. OS APPLICABILITY IN 5G

With the emergence of network softwarization, open source software is going to be critical, as described in the following subsections, to 5G and will play an important role in the development of 5G networks. Open source projects have a global developer community for the task of solving technical challenges and expanding access to technical capabilities. The community model of open source development identifies and responds to user needs more rapidly than perhaps the traditional standards world. Open source could help operators find interoperable solutions, encourage innovation, improve quality and security and contribute to the community. The open source approach also helps vendors free up resources to pursue value-added products/services, improve quality and security and contribute to the community.

With the open source movement quickly gaining momentum, there are numerous open source projects across multiple domains of infrastructure, management, control, access and core. Determining the applicability of open source to an appropriate domain can be overwhelming.

Section 4 covers the aspects to be considered when determining the applicability of open source across different layers of the 5G network.

4.1 5G INFRASTRUCTURE

In order to provide massive amounts of bandwidth to a massive number of devices, there is a need to transform the network to be able to scale up and be agile while reducing cost. Network disaggregation with separation of user and control plane, separating out the network operating system from the underlying hardware, and use of general-purpose processing platforms is the key to creating networks that are massively scalable, agile and inexpensive.

Disaggregated hardware provides high performance at lower costs via approaches such as specialization of tasks (for example, servers designed for packet processing) or conformance to a common standard for commoditization. Some of the projects representing each approach are:

- **Open Compute Project (OCP)**, whose mission is "to apply the benefits of open source to hardware and rapidly increase the pace of innovation in, near and around the data center and beyond."[9] OCP's Telecom Working Group has developed the CG-OpenRack-19 specification. This specification offers telecom data center operators the benefits of open platform standards combined with the needed carrier-grade and environmental enhancements required for edge computing,[10] which will be one of the most important building blocks for successful 5G deployments.

- **Disaggregated Network Operating System (DANOS)** is an open and flexible alternative to traditional networking operating systems. DANOS will support a network operating system framework that leverages existing open source resources and complementary platforms such as switches and white box routers (note: the project is expected to be available in 2019).

- **P4** is an open-source initiative designed primarily to provide a declarative language for interacting with networking forwarding planes. P4 programs specify how a switch processes the packets. P4 controls silicon processor chips in network forwarding devices such as switches, routers and network interface cards.

- **O-RAN** alliance use two themes: "openness and intelligence" for the next generation wireless networks and beyond: "Building a more cost-effective, agile RAN requires openness. Open interfaces are essential to enable smaller vendors and operators to quickly introduce their own service" and "Intelligence— Networks will become increasingly complex with the advent of 5G, densification and richer and more demanding applications. To tame this complexity, we cannot use traditional human intensive means of deploying, optimizing and operating a network. Instead, networks must be self-driving, they should be able to leverage new learning-based technologies to automate operational network functions and reduce OPEX"

Leveraging open source is important for enabling a high-performance, flexible 5G user plane. There are various open-source networking initiatives—such as Data Plane Development Kit (DPDK), Vector Packet Processing (VPP), Fast Data Input/Output Project (FD.io), Mobile Central Office Re-architected as a Datacenter (M-CORD), National Ground Intelligence Center (NGIC) and Open Virtualized multilayer Switch (Open vSwitch or OVS) —that provide the necessary optimizations, bringing in the ability of the user plane to scale and handle increased throughput necessary for 5G use cases and services.

[9] http://www.opencompute.org/about/ocp-adoption.
[10] http://www.eenewseurope.com/news/open-compute-projects-first-carrier-grade-specs.

4.2 5G RADIO NETWORK

5G brings a diverse set of requirements and use cases, requiring an entirely new RAN architecture that is flexible, modular and supports open interfaces. The new RAN architecture needs to be operationally efficient and able to dynamically adapt to various, diverse requirements of 5G.

As shown in Figure 3.3.2 in the 3.2 5G Radio **Network** section, the Cloud-RAN (C-RAN)/Fronthaul Architecture separated the CUs also known as Baseband Units (BBUs) and the DUs also known as Remote Radio Heads or Units (RRHs or RRUs), with the CUs located at Central Offices (CO) or master cell sites while DUs are located at cell sites. These separately located units are connected via Common Public Radio Interface (CPRI) or gs 3.x. Until now, the main fronthaul standard was CPRI, which is outside the purview of 3GPP. Its successor, evolved CPRI (eCPRI), is implemented in a proprietary, non-interoperable manner. Also, O-RAN created a complete spec on Open Fronthaul Interface. Additionally, the C-RAN architecture is no longer able to handle the ultra-high radio speed, ultra-low latency and massive connectivity requirements of 5G. As part of the new RAN architecture, various functional splits have been proposed, each offering trade-offs such as reduced fronthaul capacity and higher latency. The key to effectively implementing the new RAN architecture with flexible splits and efficient fronthaul is the openness in its specification and implementation.

Such proprietary software and interfaces are often tied to the underlying hardware, which is a significant roadblock for openness. Enabling multi-vendor, best-of-breed flexibility in the RAN requires a move away from proprietary hardware to off-the-shelf, general-purpose processing platforms. Adoption of such commodity network hardware will require a reference design with standardized interfaces.

There are several industry forums such as O-RAN, Open RAN (ORAN) / Telecom Infra Project (TIP), which are focusing on decoupling the RAN control plane from the user plane, building a modular RAN software stack that uses commodity hardware and publishing open north- and south-bound interfaces. The challenge has been the lack of openness in the RAN architecture, which is being addressed with the specifications being defined by the ORAN group.

A RAN architecture with disaggregated software based on open specifications running on commodity hardware could allow operators to reduce complexity, innovate faster and significantly reduce deployment and operational costs. Hence adoption of this is most applicable for 5G RAN architecture. With well-established backing from the telecom industry, a growing community and an open hardware ecosystem in communities, such as the Open Compute Project (OCP) and O-RAN, the open specifications and implementations coming out of these forums are, over time, likely to see higher adoption and thus should be considered as applicable.

4.3 5G CORE NETWORK

The core network is a critical component, so it needs to be robust, highly resilient and high performance. 3GPP's Service-Based Architecture (SBA), has standardized the Network Functions (NFs), their procedures and the inclusion of NF sub-modules. Standards also define the APIs to be used by providing data model, protocol and format. However, there still exists lots of innovation and ongoing research in the open source community and within vendors to address specific problem areas or new ways of implementing specific interfaces. The following sections identify some ongoing open source initiatives in the control and user planes of the 5G core network.

4.3.1 CONTROL PLANE (CP)

Unlike previous generations, the 3GPP 5G system architecture is using open APIs referred to as Services Based Interfaces (SBIs). The communication over the SBI will need a services framework implementing a message communication bus that can support an efficient mechanism for synchronous communication between the NFs. Different mechanisms are needed for asynchronous data movement, such as transferring event notification, performance data, service availability and discovery.

As of now, this has been outside the purview of the standards. Web-scale companies have widely adopted microservices architecture; hence there is some open source software that provides a microservice message communication bus. Some of the open source implementation of a communication bus for synchronous communication are reverse proxies such as NGINX, High Availability Proxy (HAProxy) and Open Network Automation Platform's (ONAP) Micro-services Bus Project (MSB). Apache Kafka streams are also a possible implementation for asynchronous data movement enabling real-time data ingestion. This is important in the areas of analytics-based automation and service assurance, where real-time event monitoring becomes highly critical.

The Network Repository Function (NRF) will allow every network function to discover the services offered by other NFs. Open source implementations of Consul and others provide similar service registry and discovery mechanisms, which have been widely deployed by web-scale companies.

SBI and NEF have adopted the Open API Initiative, which defines a standard, language-agnostic interface to RESTful APIs. 3GPP has a study item on Common API Framework (CAPIF), which considers the common aspects of northbound APIs.

There are other industry forums, such as the OpenAirInterface Software Alliance (OSA), working on developing some of the 5G core network functions, which should be considered as applicable in 5G.

4.3.2 USER PLANE (UP)

SDN plays a vital role in customizing the user plane for diverse sets of the 5G services. There are various open source initiatives of SDN controllers, such as OpenDayLight, OpenContrail and Open Network Operating System (ONOS), that contain a collection of "pluggable" modules that can perform different network tasks. Some of the basic tasks include determining what devices are within the network, the capabilities of each, gathering network statistics, configuring routing rules for service chaining and enforcing security policies.

3GPP has defined Packet Forwarding Control Protocol (PFCP) as the native protocol to be used for controlling the user plane, which the SMF uses to perform the role of tenant SDN controller to configure appropriate enforcement policies into the UPF. Other open source protocols such as OpenFlow, Extensible Messaging and Presence Protocol (XMPP) and Network/Configuration (NetConf) could be used by the infrastructure SDN controller to configure the user plane with L0-L3/L4 routing aspects.

With the use of commodity hardware, the user plane no longer needs to rely on proprietary merchant silicon, which is not customizable. P4 is an open-source initiative that has projects such as P4 language and P4 runtime, which enable programmable forwarding plane and dynamic provisioning on merchant or open source silicon and software.

M-CORD is an open source reference solution for operators deploying 5G. It is built on the CORD infrastructure platform, which brings data center economics and cloud agility to operator networks. M-CORD

transforms the mobile network by disaggregating and virtualizing cellular network functions, as well as operator-specific services. M-CORD lays the foundation for 5G networks and services through support for disaggregated and virtualized EPC, end-to-end slicing from RAN to EPC, mobile edge computing and a programmable radio access network.

4.4 CONVERGENCE

The 5G industry vision goes beyond mobile, which is why 5G convergence in next-gen fixed and mobile cores will need to be addressed. Broadband Forum's Open Broadband and Open Broadband Labs are initiatives in developing specifications, open hardware and software platforms addressing the requirements of integrating fixed access with the 5G core.

CORD Forum's Virtual Optical Line Termination Hardware Abstraction (VOLTHA) project is working on the virtualized Optical Line Terminal (OLT), which will help accelerate time-to-market for new offerings such as fronthaul for 5G and services for business users. CORD also provides other virtualized NFs, which could enable faster integration of the fixed access into the 5G converged core via the N3IWF.

4.5 MANAGEMENT & CONTROL

Network Function Virtualization (NFV) and Software Defined Network (SDN) are the key technologies required to improve QoS with reduced capital expenditure (CAPEX), operating expenditure (OPEX) and energy consumption. RAN virtualization is a key enabler for 5G, providing flexibility, scalability and most importantly optimum resource usage. Running software payloads on virtual machines provisioned on general-purpose processing platforms enables the optimum usage of underlying network capacity and resources among deployments with varied traffic utilization. Virtualization benefits from low-cost, off-the-shelf hardware, while gaining greater agility in network management, service creation and provisioning.

The European Telecommunications Standards Institute (ETSI) aims to address the challenge of moving away from proprietary hardware in NFV by converging the telco and IT networks. It applies standard IT virtualization to consolidate network equipment types to standard high-volume servers, switches and storage. NFV is complementary to SDN and can be easily used to manage NFV deployments.

With web-scale companies adopting and deploying open source in general, there are already established agreements and implementation in management of virtualized resources. With the industry backing of the open source community in the cloud computing domain, and with success stories such as OpenStack, KVM, Hadoop, Docker and Kubernetes, use of open source is most applicable in the virtualization space.

Some additional areas to be considered as applicable for open source in the domain of management and control are:

- **Orchestration** of network services to provide expected agility in the telecom networks requires a way to define these services down to their atomic nature, physical and virtual resources. TOSCA, JuJu, YAML and YANG are modeling tools that enable modeling of applications (therefore, VNFs) and network services

- **Network Automation** enables automation by programmatically configuring and provisioning network connections. With disaggregated software, separate control and user planes, and distributed network functions, there is a need to automate the means of managing the control of the NFV infrastructure and also the VNFs running on that infrastructure. This will transform the network by making it operationally efficient and reduce OPEX

The key to efficient network automation is maximum openness without which integration is not possible. Without standard bodies focused on network automation, there is a need for adopting an open source approach. Some initiatives in this area that should be considered as applicable for 5G are ONAP, ZSM (Zero touch network & Service Management) and ENI (Experiential Network Intelligence)

- **Analytics** will also be key to network automation, as it allows closed-loop feedback for effective service assurance. This will allow the network to self-heal, self-optimize and self-organize, bringing operational efficiency to network management. Open source communities have significantly contributed to big data analytics projects that utilize many open source initiatives such as the SMACK (Spark, Mesos, Akka, Cassandra, Kafka) stack which has also seen wide adoption by web-scale companies. With the growing number of devices and data explosion in 5G networks, real-time analytics of disparate data will be necessary

- **DevOps** is a software engineering culture and practice that aims at unifying software development and software operation. The cloud-native approach is fundamental to 5G network functions/services and allows vendors and service providers to impose DevOps methods to automate the process of building, validating and deploying workloads into NFV environments. This enables service agility. Any open source efforts in this DevOps area are applicable for 5G

- **Testing Tools -** There are thousands of software and stress test tools, and a few hundred network test and simulation tools. By comparison, there are few such tools for testing telecom-specific protocols. It is more likely that support will be second hand through scripts that use other test tools. 5G NGC's use of Open API will allow many existing test tools to be leveraged

However, the use of Open API does not apply to all NGC interfaces in Release 15. Telecom providers cannot compromise the service interruptions despite the expected level of agility. Thus, it will be important for operators to split the responsibilities of continuous integration and deployment and the appropriate level of testing with their vendors. Open Platform NFC (OPNFV) is an open source platform for system integration and testing of various components developed by different open source communities.

4.6 SECURITY

There is an increased focus on security in 5G and open source software due to continuous evolving threat landscape and dynamically changing critical infrastructure that will carry massive amount of traffic to service multiple deployment options and use cases. With the recent data breaches and proliferation of state sponsored malware, it isn't surprising that open source is getting a lot of attention with security agencies trying to assess if the increased use of open source software is correlated with the spike in cyber-attacks globally.

Open source by definition provides transparency into the code logic so anybody can identify and exploit weaknesses by inspecting the code. While this can be perceived as a flaw, it is in fact one of the strengths of open source especially when is being used and contributed to broadly. Instead of relying on a small, closed group to fix security loopholes, the larger community of development users can spot, patch and update vulnerabilities. Continuous integration and testing tools, such as those most open source adopters employ, makes the patching process efficient and reduces the prolonged risk of exposure.

As new features and functionalities are constantly added to the original open source software stack, all software components along with platform code must have a clean baseline for continuous security and compliance validation. Operators, solution providers and open source communities will have to manage accurate inventories of open source software dependencies to mitigate the risk of code injection. This is a risk to any software; companies utilizing strong auditing and sourcing processing can minimize their exposure to attacks. Processes will have to be put in place to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open source.[11] Open source risk management will have to keep pace with all release cycles delivered at a rapid pace. The open source risk evaluation will need to integrate security planning and testing into the Continuous Integration/Continuous Deployment (CI/CD) pipeline, so that open source risk evaluation is performed in parallel with all other software delivery processes. For instance, static and dynamic code analysis should be part of the CI/CD process, which provide automated and early detection of security vulnerabilities.

With the adoption of open source in 5G, mobile operators have a menu of options to choose from to deploy new services; modify the service and give it another attempt, or simply scrap it without too great of an investment if it is not living up to its hype. However, the introduction of new services – whether they are short- or long-lived – may inherently bring in new security threats that have to be prevented and detected. Mobile operators have a chance to derive the security technology requirements, development and deployment strategies rather than being forced to choose from proprietary solution options. For instance, open source initiatives of SDN will facilitate prompt threat identification through a cycle of harvesting security intelligence from various network resources, states and flows. The SDN inherently supports reactive and proactive security monitoring, traffic analysis and enables incident response systems to provide continuous network security policy updates, network forensics, and Security-as-a-Service (SecaaS) insertion where and when it is needed. SecaaS can be deployed across the network – including edge and/or centralized functions of the core network architecture – due to global network visibility, whereas security systems such as firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS) can be used for specific traffic by updating the flow tables of SDN network elements. 5G inherently provides unique architecture options that introduces default isolation of networks such as the introduction of virtual network slices. However, network slicing could require specific security capabilities as not all virtual network slices are always created the same. Hence, the security of the network functions in 5G integrated with a security orchestrator in correspondence with the ETSI NFV architecture is paramount to creating a feedback loop mechanism that will need to consume and act accordingly on security faults, errors and alarms generated by various software and hardware systems to create a robust 'fail safe' environment that is capable of mitigating security attacks in real time and more importantly self-recover in the face of advanced persistent threats and system disasters.

A key goal of the collaborative telecom industry effort is to encourage implementation and growth of realizing the full potential of 5G working in tandem with the open source ecosystem. However, most of the work in the past was concentrated on the interworking of some of the 5G elements and open source capabilities with the aim to demonstrate them as viable technologies and to generate practical knowledge. Moving forward, it is important that the working standards and implementation activities include "security" as top of mind. The ongoing challenge will be the journey from technical feasibility of various 5G and open source technologies to ensuring security is embedded as part of the technological maturation.

Security tools for 5G and open source environments are still evolving. The security offerings have to include a mixture of centralized control and distributed and localized enforcement in the form of security services that can potentially be operated by the mobile operator's controller/orchestration infrastructure, allowing for better visibility and ultimate granularity in technology deployment and operations. 5G security must be

[11] *CSRIC Network Reliability and Security Risk Reduction Report,* https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0.

designed-in and not be an afterthought. Hence, a holistic approach to developing security in a 5G environment is required. Security controls need to be both horizontally and vertically distributed across the 5G environment to help enhance the end-to-end security posture. 5G transformation will occur. However, the level of its success will depend upon realizing the full potential of open source and making it securely deployable and operational.

4.7 SERVICES

Most of the industry backs open source efforts focused in the telecom infrastructure and access network area, but there have not been major open source efforts seen in the services space. A few open source IP Multimedia Subsystem (IMS)-related projects—such as Clearwater, Kamailio, rcsjta (RCS-e stack for Android with GSMA API) and OpenIMS (OS implementations of IMS Call Session Control Functions)—exist and provide end user services deployed in production. However, they will need modifications to support 5G as service-specific standards are defined.

[X]-as-a-service for cloud computing will become an important revenue generator for telecom operators. In addition to their own use for cloud management, OpenNebula-like cloud management software will be critical for operators to enable hosting third-party applications within their data centers. Meanwhile, customers will benefit from the open APIs and common API framework efforts focusing on traffic steering.

As we start seeing 5G progress into deployments, there are likely to be more open source efforts focused in the 5G services area, such as Multimedia Broadcast/Multicast Services (MBMS) and vehicle to everything (V2X).

4.8 CONSIDERATIONS FOR OPEN SOURCE APPLICABILITY

This section lists some additional general aspects to be considered while determining the applicability of open source.

Governance Model

The governance model as described in section 2.2 provides a social framework for collaboration. While determining the applicability of open source in 5G, it is important to look for an open source project with an effective governance model. An open source project with an effective governance model is one that balances the interests between volunteer contributors, corporate sponsors and users, and also provides the legal context in which the code is accepted from developers and released to the larger community.

Telecom infrastructure and applications/services have long lifetimes. As a result, open source communities that support and provide telecom infrastructure platforms and applications/services need a model that encourages and sustains themselves over these long-time frames.

In addition to providing newer functionalities, an effective governance model must focus and encourage improvements in areas of performance, reliability, security and interoperability, as all are critical for telecom infrastructure and applications/services.

In general, an effective governance model removes the technical barriers to participation, social barriers to participation and legal barriers to participation, which essentially lowers the barriers to collaboration and success of open source projects.

Licensing

With the increased use of open source software and direct contributions towards open source projects, companies are exposed to legal and business challenges related to the licensing terms. Generally speaking there are two major categories of open source licenses, as discussed in section 2.1:

- Copy-left such as General Public License (GPL) and Affero GPL (AGPL) require redistributed copies and derivative work to be under the same license

- Non-copy-left licenses such as Apache 2.0 and Massachusetts Institute of Technology (MIT) permit the incorporation of the code in software that is distributed under different licenses. Therefore, non-copy-left licenses are referred to as permissive licenses

One of the most overlooked areas in software development using open source is license compatibility. Just because code is under open source licensing doesn't mean they can be mixed or redistributed together. This caveat is particularly important with GPL and some permissive licenses.

Most well-established open source communities have policies and procedures in place to establish license compliance by identifying code origin, identify licenses and reduced risk. Companies have to establish automated license management procedures that constantly scan, analyze, approve and inventory open source software. To address this, GitHub has recently open sourced Licensed, a tool it's used internally to automate some of GitHub's open-source projects licensing process. While this is not a full license-compliance tool such as other commercial offerings, it still provides the developer with dependency-discovery automation in order to identify the most obvious licensing issues early on in a project.

OS Projects with Greater Community and Industry Support

An open source project is considered successful when companies deploy it. As a result, it is important for an open source project to have an engaged community and backing of telecom industry. An engaged community can immensely benefit open source by leading development and constantly improving technologies and solutions. For example, Linux or Apache Web Server are well established success stories of open source. A newer open source project such as OpenDaylight (ODL) is considered as a success due to ongoing evaluation activity being backed by world's largest carriers, web-scale companies, leading research institutions and increasingly global enterprises in the finance and retail sectors.

SDOs and specifications provide interoperability between the networks connecting users across the world, open source projects require validation based on interoperability. Hence industry alliances are important in a role in facilitating multi-party interoperability activities to demonstrate the viability of open source solutions in a variety of different contexts. For example, the OPNFV Verified Program (OVP) is an open source, community-driven initiative with mechanisms for validating and verifying NFV deployments based on open source NFV.

Convergence of Telecom and IT, with Open Source Benefiting from IT Industry Contribution

The web-scale internet companies have adopted disaggregation, deploying thousands of white box servers and switches running modern operating systems, open source software and automation at an unprecedented scale. This has allowed them to transform traditional IT data center infrastructure into a hyper scalable architecture, enabling them to deploy services with agility, more efficiently and cost effectively.

Web-scale IT is characterized by the use of open source software and commodity hardware to create infrastructure that can be completely controlled by software. These cloud computing principles being adopted in technologies such as NFV and SDN will benefit the telecom industry in the 5G era.

The web-scale architectures are already agile, born on the cloud and built on the new, faster principles that need to be adopted in order to build an agile mobile network. The web-scale delivery model is based on open source software, which supports continuous design, build, deploy and test. DevOps has made it possible for companies to develop infrastructure that responds quickly to change while remaining stable and reliable.

Open source software related to artificial intelligence, machine learning tools and real-time data ingestion developed by the IT industry will be applicable for the 5G world, where network automation becomes critical for operational efficiency.

Unlike previous network generations, 5G is expected to support a diverse set of use cases and be agile in-service delivery and efficient in network operations. Therefore, it is important to adopt the principles of the web-scale internet companies. NFV, SDN and automation are key enablers for 5G. Hence any open source project benefiting from the contribution of development done by web-scale companies should be considered as applicable.

Open Source Design

5G networks need to support diverse requirements and services. Thus, a focus of their design is on supporting disaggregated network functions that are modular, flexible, supporting extensible open interfaces and cloud native in all aspects. Open source must adopt and demonstrate these design principles in order to successfully integrate into telecom infrastructure and applications. This should be important criteria while determining the applicability of certain open source projects in 5G.

4.9 OPEN SOURCE EFFORTS

There are numerous open source projects related to 5G. This paper has discussed several of them. For a snapshot of the applicable open source project inventory, see Table 1. Open Source Efforts and References, in the Appendix.

5. CONCLUSION

Standards and open source both thrive to increase interoperability, reduce cost and establish business ecosystems. While standards are very transparent in collaboration and consensus, open source brings the transparency in implementation and modularization. Security is an important consideration when moving to open source. The pros and cons of security need to be fully understood by any entity moving to open source.

For those who look to participate in open source efforts, the structure of the project must weigh the optimum tradeoff between control, process and agility as well as attribution and distribution. An open source project process must adapt the best practices for vulnerability detection; security must be designed into both architecture and a continuous development process; and security will be amplified through openness. Solid support mechanisms must also be in place for the project.

Open source has been key to many recent advancements in high-performance and flexible packet processing, which is key to 5G use case and services. There are already a number of open source projects that are well into their product cycles, and more will be emerging as 5G network deployments start. Analysis performed in this paper suggests infrastructure (therefore, programmable forwarding plane, general-purpose processing platforms), management and control (therefore, automation, orchestration, analytics,

testing) are the key areas that, if open sourced, could benefit mobile operators the most in their 5G deployments.

Operators have different strategies for evolving their networks to 5G and each operator environment is different; there is no single open source effort that meets the needs of all operators; and network evolution cannot be prescribed to apply to all deployments.

As the focus of this paper is status of open source with respective to 5G, areas of discussion such as open source in a multivendor environment, challenges and strategies around integration of open source in different parts of the networks, and release management in the same environment were not covered. Lastly the issue of using code that may be exposed to the use of undisclosed patents and other undisclosed licenses.

Initial 5G deployments are expected to have the interoperability challenges similar to those that 3G and 4G faced. However, 5G system architecture gives mobile operators more openness than previous generations. Operators and OEMs may leverage open source principles in order to stay or become competitive in the marketplace.

This paper is intended to serve as a call to action for the 5G community of operators, solution providers and developers, to participate in the existing open source efforts applicable to 5G, or initiate new ones, in areas such as “Infrastructure” and “Management and Control” where the 5G ecosystem will likely benefit the most. Community involvement is important to help achieve critical backing of the projects, avoid one-off solutions from emerging, while enabling secure and reliable open source project outcomes to be productized with increased participation.

APPENDIX

A.1 APPLICABLE OPEN SOURCE EFFORT INVENTORY

Table 1 is not an exhaustive list but provides a snapshot of some open source efforts that are applicable in 5G.

Table 1. Open Source Efforts and References.

5G Network Area	Focus	Brief Description	Open Source Effort References
Infrastructure	Hardware	High performance at lower cost by programmability and specialization of tasks	Open Compute Project: https://www.opencompute.org P4: https://p4.org
Infrastructure	Networking	Fast rate packet processing by acceleration techniques	DPDK: http://dpdk.org VPP: https://fd.io
Infrastructure	Operating System	Enabling white box use in carrier grade networks	Linux: https://www.linuxfoundation.org/projects/linux/ Berkle Software Distribution: http://www.bsd.org Disaggregated Network Operating System: https://www.danosproject.org
Access Network	Radio	Implementing 4G LTE and 5G Radio Access Network for NodeB and/or User Equipment	openair5G: https://gitlab.eurecom.fr/oai/openairinterface5g/wikis/home O-RAN: https://www.o-ran.org/
Core Network	Wireless Core Network	Implementing 4G LTE EPC and 5G NGC	openairCN: https://gitlab.eurecom.fr/oai/openairinterface5g/wikis/home M-CORD NGIC: https://software.intel.com/en-us/articles/an-interactive-demo-of-the-next-generation-infrastructure-core-reference-implementation
Management & Control	Networking	Carrier grade packet processing and flow control	OpenDaylight: https://www.opendaylight.org ONOS: https://onosproject.org Open vSwitch: https://www.openvswitch.org M-CORD NGIC: https://software.intel.com/en-us/articles/an-interactive-demo-of-the-next-generation-infrastructure-core-reference-implementation FD.io: https://fd.io

Management & Control	Virtualization	Abstraction of general compute resources to be shared across multiple applications and logical networks	OpenStack: https://www.openstack.org Kubernetes: https://kubernetes.io Docker: https://www.docker.com
Management & Control	Orchestration	Frameworks for describing dynamic function and network deployment policies with specific performance characteristics	Open Source MANO (OSM): https://osm.etsi.org MEF Lifecycle Service Orchestration (LSO): XOS: https://www.opennetworking.org/xos/
Management & Control	Automation	Frameworks and middleware for enabling Orchestration and Management tools to configure general compute and networking components via virtualization layers	xRAN: http://www.xran.org ONAP: https://www.onap.org Ansible: https://www.ansible.com Terraform: https://www.terraform.io/
Management & Control	Modeling	Modeling tools and languages for defining function and network services for deployment used by Orchestration Frameworks	TOSCA: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca JuJu: http://jujucharms.com YAML: http://yaml.org YANG: https://tools.ietf.org/html/rfc6020
Management & Control	DevOps	Software development methods to automate process of building, validating and deploying workloads into NFV environments for service agility	Elasticsearch, Logstash, Kibana (ELK): https://www.elastic.co/elk-stack Consul: https://www.consul.io Etcd: https://coreos.com/etcd/ Jenkins: https://jenkins.io/ Puppet: https://puppet.com Chef: https://www.chef.io/chef/
Management & Control	Testing Tools		
Management & Control	Analytics	Data streaming protocols for continuous analysis of the service monitoring	Apache Kafka: https://kafka.apache.org/ Apache Spark: https://spark.apache.org/
Management & Control	AI	Framework for use of AI in Network	Automation https://www.acumos.org/
Management & Control	Edge Compute	Open source software for Edge	Computing https://www.akraino.org/
Security	Cybersecurity	Security framework for Virtual network infrastructures	SHIELD: https://torsec.github.io/shield-h2020/about/summary.html

A.2 GLOSSARY

3GPP	3rd Generation Partnership Project
AF	Application Function
AGPL	Affero GPL
AMF	Access and Mobility Management Function
API	Application Programming Interface
AUSF	Authentication Server Function
BBF	Broadband Forum
BBU	BaseBand Unit
C-RAN	Cloud RAN
CAPEX	Capital Expenditure
CAPIF	Common API Framework
CO	Central Office
CP	Control Plane
CPRI	Common Public Radio Interface
CU	Central Unit
DANOS	Disaggregated Network Operating System
DPDK	Data Plane Development Kit
DU	Distributed Unit
eCPRI	Evolved CPRI
ENI	Experiential Network Intelligence
EPC	Evolved Packet Core
FD.io	Fast Data Project Input/Output
GPL	General Public License
HAProxy	High Availability Proxy
HPLMN	Home PLMN
ICT	Information Communication Technology
IDS	Intrusion Detection Systems
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Prevention Systems
KVM	Kernel-based Virtual Machine
MBMS	Multimedia Broadcast/Multicast Services
M-CORD	Mobile Central Office Re-architected as Datacenter
MIT	Massachusetts Institute of Technology
MSB	Micro-services Bus Project
N3IWF	Non-3GPP Inter-Working Function
NAS	Non- Access Stratum

NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualization
NGC	Next Generation Core
NGIC	Next Generation Intelligent Core
NGINX	Open source HTTP server and reverse proxy
NR	New Radio
NRF	Network Repository Function
NRP	Network Repository Protocol
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
OAI	Open Air Interface
OCP	Open Compute Project
ODL	Open Daylight
ONAP	Open Network Automation Project
ONOS	Open Network Operating System
ORAN	Open Radio Access Network
O-RAN	Open RAN Alliance
OS	Open Source
OSD	Open Source Definition
OSI	Open Source Initiative
OVP	OPVN Verified Program
Open vSwitch/OVS	Open Virtual Multi-Layer Switch
PCF	Policy Control Function
PLMN	Public Land Mobile Network
RAN	Radio Access Network
REC	Radio Equipment Controller
REST	Representational State Transfer
RRH	Remote Radio Head
RRU	Remote Radio Unit
SBA	Service-Based Architecture
SBI	Service-Based Interface
SDN	Software-Defined Network
SDO	Standards Development Organization
SecaaS	Security-as-a-Service
SMF	Session Management Function
TIP	Telecom Infra Project
UDM	Unified Data Management
UDR	Unified Data Repository

UE	User Equipment
UP	User Plane
UPF	User Plane Function
V2X	Vehicle-to-Everything
VPP	Vector Packet Processing

ACKNOWLEDGEMENTS

The mission of 5G Americas is to advocate for and facilitate the advancement of 5G and the transformation of LTE networks throughout the Americas region. 5G Americas is invested in developing a connected wireless community for the many economic and social benefits this will bring to all those living in the region. 5G Americas' Board of Governors members include AT&T, Cable & Wireless, Cisco, CommScope, Ericsson, Intel, Kathrein, Mavenir, Nokia, Qualcomm Incorporated, Samsung, Shaw Communications Inc., Sprint, T-Mobile USA, Inc., Telefónica and WOM.

5G Americas would like to recognize the significant project leadership and important contributions of project co-leaders Lyle Bertz from Sprint and Bejoy Pankajakshan of Mavenir, as well as representatives from member companies on 5G Americas' Board of Governors who participated in the development of this white paper.

The contents of this document reflect the research, analysis, and conclusions of 5G Americas and may not necessarily represent the comprehensive opinions and individual viewpoints of each particular 5G Americas member company.