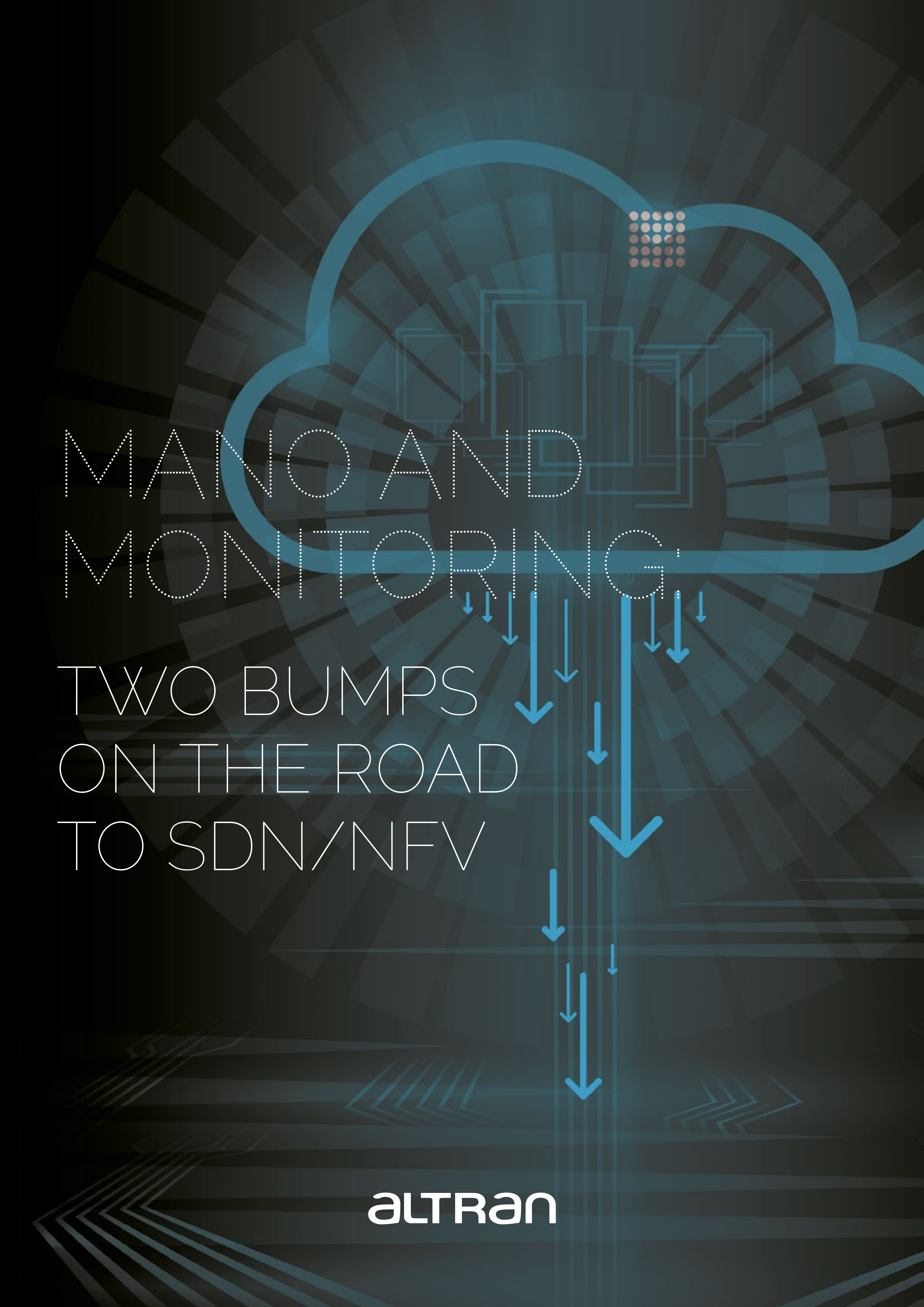

MANO AND MONITORING: TWO BUMPS ON THE ROAD TO SDN/NFV

TABLE OF CONTENT

EXECUTIVE SUMMARY

Network Virtualization and Software-Defined Networking implementations depend on functional and trustworthy Management, Orchestration and Performance Monitoring solutions in order to take full advantage of the benefits they offer.

NFV Management and Orchestration (MANO) is the stack formed by three major elements: NFV Orchestrator (NFVO), VNF Manager (VNFM) and Virtualized Infrastructure Manager (VIM). MANO is key when it comes to deploying different Network Services. This explains why all Communication Service Providers (CSPs) were waiting for the rapid completion of the different MANO standards which only happened in Q3 2016.

In terms of implementation, MANO relies on two main choices: pure Open Source approaches and the commercial deployment of MANO stacks provided by vendors. We think that it is worth taking a look at both options considering the CSP requirements, the problems to solve and the deployment maturity. In this document, we describe the following proposals, under the two mentioned options:

- Open Source solutions: OSM (Open Source MANO) which is one of the most important Open Source initiatives, ONAP (Open Network Automation Platform), and Cloudify MANO.
- Vendors' proprietary solutions: the Ericsson proprietary MANO solution called ECM (Ericsson Cloud Manager) and Nokia's MANO proprietary implementation called CloudBand among others.

Moreover, the NFV/SDN inherent multi-layer infrastructure requires an evolved monitoring approach relying on the following 4 key aspects: Multilayer (covering all layers), Multivendor, Real-Time Analytics capability and end-to-end Active service monitoring. The dependencies among all entities from the multiple layers have to be well defined within the interlayer data model.

INTRODUCTION

The ETSI (European Telecommunications Standards Institute) started to work on Network Function Virtualization (NFV) standards (architecture, interfaces, etc.) at the end of 2012. However, the final version of the standard release 2, including in particular Management and Orchestration (MANO) was only delivered in September 2016. During this three-year period, Communication Services Providers (CSPs) were only performing proofs of concept or trials to assess the capabilities of NFV and the different pre-solutions available.

Orchestration is key when it comes to deploying different Network Services, each made up of a group of VNFs (Virtual Network Functions) running in the same common NFV Infrastructure (NFVI). For this system to be operational, providing the end user the expected performance, everything must be monitored and alarmed in a seamless way, making it possible to detect pitfalls before they happen.

This paper intends to delve deeper into these two crucial topics, MANO and Performance Monitoring Solutions, providing the reader with some key aspects to have in mind before thinking of any complex NFV deployment.

1 MANO KEY CHALLENGES

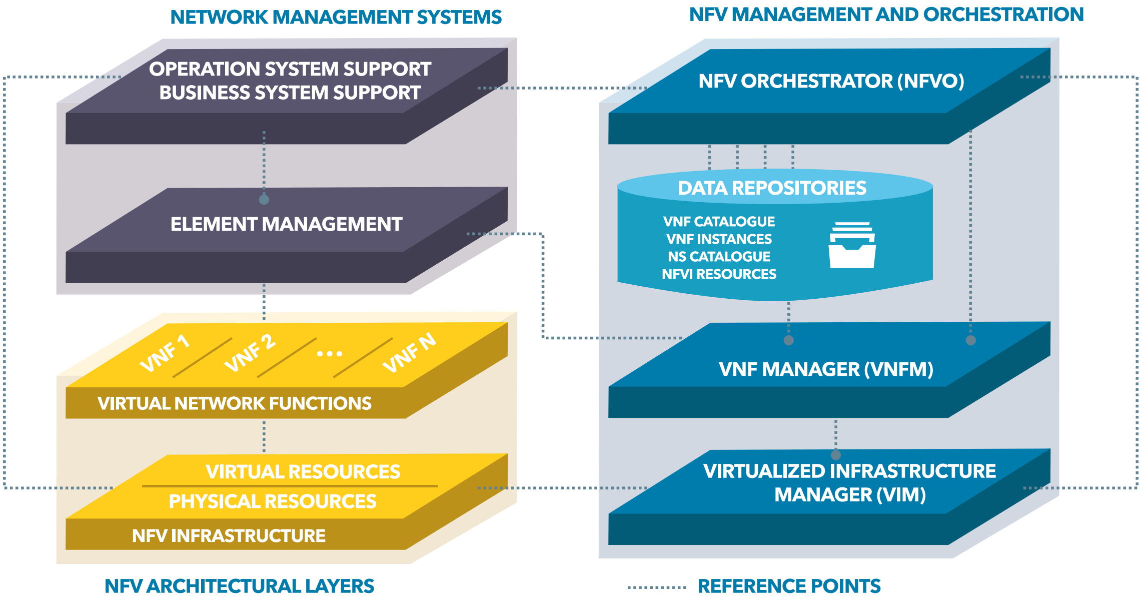

FIG. 1:
NFV LAYER ORGANIZATION

As described in figure 1, the **NFV MANO** is the stack formed by **three major components**:

→ **NFV ORCHESTRATOR (NFVO):** designed to cover two main functionalities, Service Orchestration (SO) and Resource Orchestration (RO).

→ **VNF MANAGER (VNFM):** there can be a generic VNFM able to manage several VNFs, or particular VNFMs dedicated to managing only certain VNFs. VNF lifecycle is to be managed by this component.

→ **VIRTUALIZED INFRASTRUCTURE MANAGER (VIM):** this is the component that manages the entire virtualized infrastructure (computing, storage, and network resources). It is responsible for allocating and releasing the NFVI resources, as well as for access control security policies.

While MANO is a crucial stack to enhance an NFV deployment, it has **two main challenges** that are closely related:

1) INTEROPERABILITY:
A MANO stack should provide the NFVO, a generic VNFM and the possibility of incorporating specific VNFMs from the different NFV vendors. Several approaches have been taken to implement these MANO stacks, both commercial and Open Source, but reaching the objective still seems quite far off.

2) TO COVER BOTH SERVICE ORCHESTRATION AND RESOURCE ORCHESTRATION FROM THE NFVO:

• Resource Orchestration is a responsibility shared between the NFVO, the VNFM and the VIM. The resulting lack of clear fixed boundaries may lead to different standardized implementations that are not compatible among themselves. Thus, as the implementation is quite open, compatibility is not guaranteed.

• Service Orchestration: NFVO is responsible for providing deployment-specific configuration information, issuing requests to the VIM in order to allocate resources needed for the connectivity of Network Services. How this network services are defined and how they are implemented within the NFVO is a key topic.

2 MANO IMPLEMENTATION SCENARIO

For proper deployment, pure Open Source approaches do not seem to be the best option, since there is a lot of work to be carried out. On the other hand, commercial deployment of MANO stacks provided by vendors may impose a new "vendor lock-in" on Communication Service Providers (CSPs), which is something this NFV ecosystem was intended to avoid.

So, what is the best option? We think that it is worth taking a look at both options, understanding Open Source approaches and the exact stage of development of each product. The first possible step is an analysis of the network services and network functions the CSP wants to deploy in NFV, followed by an assessment of which products on the market are most interoperable, most open and least bound by a vendor full stack, while featuring compatibility with different VIMS, easy integration of VNFMs developed by competitors, and so on. Then, once the deployment is live, problems that arise should also be shared with the Open Source community so developments can progress faster, leading to product maturity; at that time migration should be analyzed and planned carefully.

3 CURRENT IMPLEMENTATION APPROACHES

Nowadays, Telco providers are starting to turn to MANO solutions for their NFV deployments. In the MANO space we can find several Open Source proposals and other relevant solutions developed by vendors. Some of these implementations are identified and described below (non-exhaustive list).

→ **OSM (OPEN SOURCE MANO)** is one of the most important Open Source initiatives to highlight. It is an Open Source Management and Orchestration (MANO) stack aligned with ETSI NFV Information Models. OSM offers and automates service orchestration to simplify the NFV life cycle. Some of the key features offered by OSM are related to EPA (Enhanced Platform Awareness)-based resource allocation capabilities, which enables high-performance VNF deployments with lower Total Cost of Ownership (TCO) for the operator. OSM also provides multi-site support to automate service delivery across multiple sites and underlay network management functionalities. The SDN controllers and VIMs supported in the second release of OSM are ODL (OpenDaylight), ONOS (Open Network Operating System) and Floodlight from the SDN perspective, as well as OpenStack, Vmware vCloud Director and AWS (Amazon Web Services) as VIMs.

→ **ONAP (OPEN NETWORK AUTOMATION PLATFORM)** is an Open Source MANO solution that comes from the merger of AT&T's ECOMP and the OPEN-O projects. ONAP provides capabilities for design, creation, orchestration monitoring and cycle management of VNFs and SDN solutions. ONAP provides all these services in a dynamic and real-time cloud environment in addition to different graphic design and monitoring tools.

→ **CLOUDIFY MANO** is an Open Source solution with a TOSCA-based cloud orchestration framework that can be leveraged as both the NFVO and G-VNFM in the context of the ETSI MANO architecture. It is able to interact with multiple VIMs, containers, and even external and non-virtualized infrastructure and devices, OSS and BSS, since it enables communication with any northbound or southbound APIs. Currently, Cloudify supports OpenStack, vCloud VMWare, Azure Cloud Stack, SoftLayer and AWS as VIMs and ODL, OpenContrail and ONOS as SDN controllers.

→ **THE ERICSSON PROPRIETARY MANO** solution is called **ECM** (Ericsson Cloud Manager). It provides management and orchestration of the VNF life cycle management, which depending on the use case, can substitute or complement parts of the OSS VNFM functionality. The ECM also allows orchestration and management of network services and cloud resources like storage, networking and virtual machines. This MANO solution offers on-boarding and instantiation of virtual applications using the Open Virtualization Format (OVF) package standard, capabilities of integrating with SDN for L3 VPN connectivity, service chaining of functions and infrastructure and VNF monitoring (fault and performance management).

→ **NOKIA'S MANO** proprietary implementation is called **CloudBand** and is an ETSI NFV MANO system with commercially proven reliability, automation, repeatability and security. It is flexibly deployed for any combination of NFV Infrastructure / Virtualized Infrastructure Manager (NFVI / VIM), generic VNF Manager (VNFM-g), and NFV Orchestrator, and serves VNFs from Nokia and other suppliers. It is also the cloud management system for the Nokia Government Cloud Enablement Platform.

Commercial implementations may not be as ambitious as the open models in terms of features or functionalities covered, but they are ready to be used in a real environment. As MANO is key in a NFV implementation, it is not rare to observe some carriers that are taking both approaches: first, using a commercial MANO stack to go to market in the short term, but at the same time evaluating and even participating in open source MANO initiatives to adapt them as soon as they are sufficiently mature.

4 THE NEED FOR A MONITORING SOLUTION

The NFV/SDN inherent multi-layer infrastructure requires an evolved monitoring approach relying on the following key aspects:

→ **MULTILAYER:** i.e. covering all layers (from bottom to top)

- Data center Hardware and Software computing infrastructure, software-defined storage and networking infrastructure
- Virtualization layer over cloud platforms and software-defined network platforms
- Virtualized telecom infrastructure (virtual network functions and network service chains)
- End user telecom services

→ **MULTIVENDOR:** In silo-shaped legacy infrastructure, the monitoring is a "built-in" feature in the element management applications belonging to a single vendor and confined to its own Hardware and Software. In NFV/SDN, all the virtual network functions and chains as elements from different vendors have to be monitored as virtual elements hosted by a shared cloud platform in a shared physical infrastructure.

→ **REAL-TIME ANALYTICS CAPABILITY:** i.e. it must be able to correlate data from all the layers involved to understand the root-cause analysis in case of a problem occurring in the top layers (end user services or network services or network functions) correlating data from top (service- or function-related) and from bottom (infrastructure-related) layers.

→ **END-TO-END ACTIVE SERVICE MONITORING:** i.e. it should possibly use active monitoring by continuous testing for end user service layers, also relying on service activation automated testing systems used during automated deployment by NFV orchestrator.

5 MONITORING SOLUTION BUILDING BLOCKS

Below is a schematic view of data sources, measurements to collect and detect possible problem for each layer.

Data source	Measurements to collect	Problem triggers
End-to-end service layer		
• Service level Active probes • Passive probes within network service chains	• Voice, Web, Video QoS/QoE KPIs • Traffic volumes per content type (Internet, Voice, Video) • Internet traffic volumes per source • Video traffic volumes per content	• KPI "acceptable quality" thresholds • Traffic volume degradations compared to historical profiles
E2E Service orchestration	• Service Lifecycle Events and Triggered Actions • Service inventory	• Service Lifecycle Alarms (Service unavailable, recovery action failures)
Virtual Network Functions & virtualization layer		
• Vendor-specific Element managers collecting application and OS data from their agents and VNF applications • VNF Agents/Proxies or CLI scripts at VM level (only for system resources	• Virtual System resources usage (CPU, Disk, RAM) by VNF application process • Virtual System level KPIs, Alarms, Events, Configuration	• System blackout • Application Process blackout • Resource Usage thresholds Alarms, • Unexpected events • Inconsistent VNF configuration
Infrastructure orchestration VNF Managers	• Virtual Infrastructure lifecycle events and triggered actions • Virtual Infrastructure inventory • VNF lifecycle events and triggered actions • VNF inventory	Infrastructure and VNF Alarms (Resources unavailable, recovery action failures)
Compute workload active probes	Processing KPIs, RAM R/W KPIs I/O KPIs, Disk R/W KPIs	Percentage of operations above correctness and timing thresholds
VIM telemetry data (e.g. Openstack Telemetry) collected by agents/ proxies	• Virtual resources consumption per VM • Cloud system resources usage, system level and application level KPIs, alarms, events, configuration • VM and VN inventory	• Node blackout • Application process blackout • Resource Usage thresholds Alarms, • Unexpected events • Inconsistent SDN configuration (model, policies.)
DC Network, DC-SDN & SD-WAN layer		
SDN telemetry data	• sFlow, NetFlow, IPFIX traffic-related • BGP-LS/BMP • Application-aware routing • Policy usage • Network resources usage • SDN resources inventory	• Traffic blackout • Routing blackout • Unwanted routing for a an application destination/source • Network Policy no longer available • Security policy violations • Network resource usage above threshold
SNMP agents or CLI scripts at switch fabric and Gateway/Provider Edge(PE) level	• Physical system measurements, physical network system resource usage, system & network level KPIs, alarms, events, configuration • Network Inventory	• Environment conditions beyond sustainability for physical systems • Switch HW fault • Switch configuration fault
Data Center Physical Compute and Storage Systems		
• IPMI data at HW level to DCIM platform (or via cloud telemetry) • SDS telemetry data	• Physical systems measurements (temperature, power) • Physical computing, storage system resource usage, system level KPIs, alarms, events, configuration • Software-defined storage resource usage • SDS inventory • Physical systems inventory	• Environment conditions beyond sustainability for physical systems • Compute server blackout • Storage system blackout • SDS application fault • Storage resource usage above threshold

The dependencies among the layer entities have to be well defined within the **interlayer data model** which is the foundation of the overall service assurance platform collecting all above measurement data and performing all real-time analysis and anomaly detection, as well as root-cause analysis and impact analysis in an automated fashion. Figure 2 below describes those blocks and monitoring flows in the Telco cloud assurance architecture.

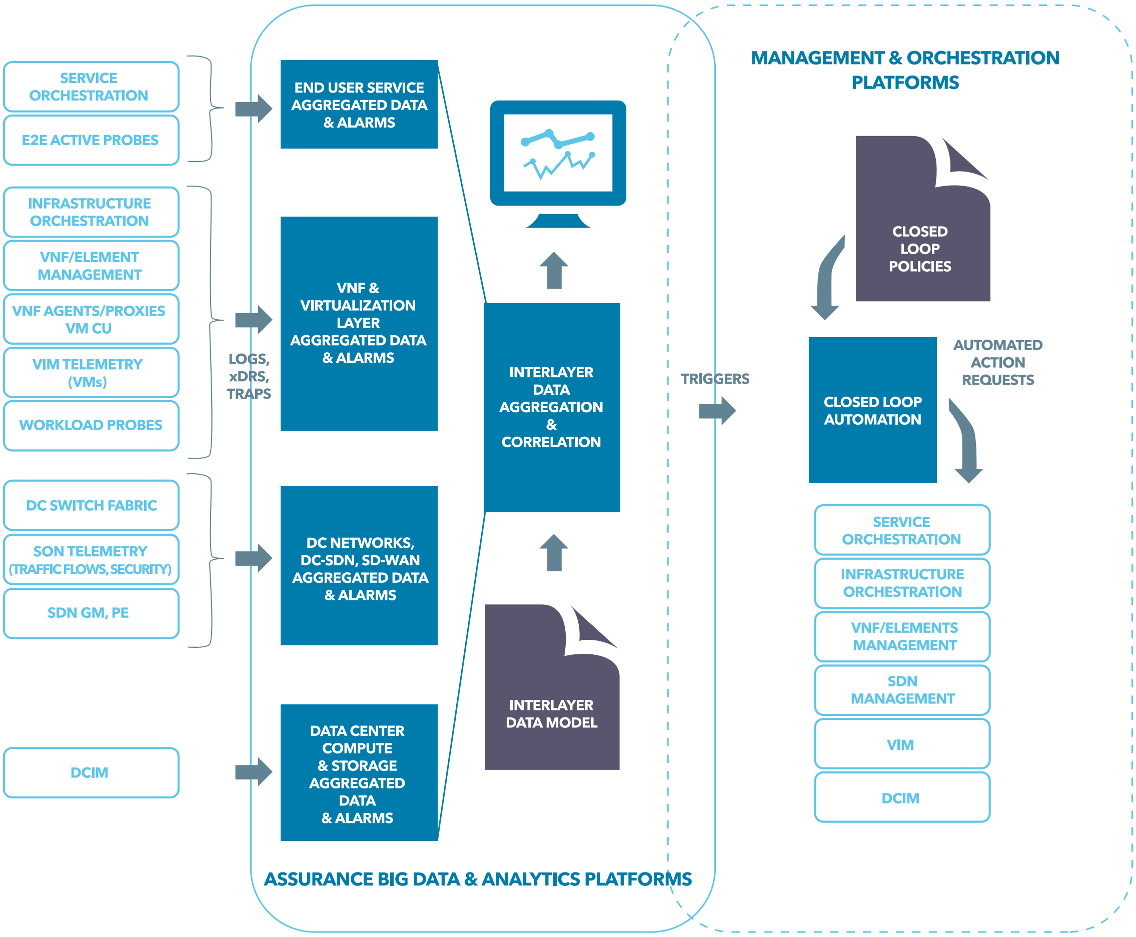
SERVICE ORCHESTRATION
E2E ACTIVE PROBES
INFRASTRUCTURE ORCHESTRATION
VNF/ELEMENT MANAGEMENT
VNF AGENTS/PROXIES VM CU
VIM TELEMETRY (VMs)
WORKLOAD PROBES
DC SWITCH FABRIC
SON TELEMETRY (TRAFFIC FLOWS, SECURITY)
SDN GM, PE
DCIM
LOGS, xDRS, TRAPS
END USER SERVICE AGGREGATED DATA & ALARMS
VNF & VIRTUALIZATION LAYER AGGREGATED DATA & ALARMS
DC NETWORKS, DC-SDN, SD-WAN AGGREGATED DATA & ALARMS
DATA CENTER COMPUTE & STORAGE AGGREGATED DATA & ALARMS
INTERLAYER DATA AGGREGATION & CORRELATION
INTERLAYER DATA MODEL
ASSURANCE BIG DATA & ANALYTICS PLATFORMS
TRIGGERS
MANAGEMENT & ORCHESTRATION PLATFORMS
CLOSED LOOP POLICIES
CLOSED LOOP AUTOMATION
AUTOMATED ACTION REQUESTS
SERVICE ORCHESTRATION
INFRASTRUCTURE ORCHESTRATION
VNF/ELEMENTS MANAGEMENT
SDN MANAGEMENT
VIM
DCIM

FIG. 2:
TELCO CLOUD OVERALL MONITORING MODEL

ABOUT ALTRAN AND SDN/NFV

Altran is an international group and global leader in innovation and high-tech engineering consulting. It has been leading and designing the early integration of SDN and NFV in operator networks, covering the entire lifecycle from helping identify key capabilities unlocked by SDN/NFV, which are table-stakes for large-scale topologies, to the design and validation of solutions. The related offering is managed by the **Altran World Class Center (WCC) Advanced Networks** which covers the full engineering value chain, i.e. from development/design to testing, validation and transition to operations.

The Altran value proposition leverages WCC Advanced Networks SDN/NFV LAB capabilities that would complement the SDN/NFV offering with the availability of a multi-VIM/SDN environment including SDN controllers to allow for custom developments, MANO & Service Chaining solution testing, validation and benchmarking, NFV/SDN pre-production trials and POCs implementation for Vendors.

ABOUT ALTRAN

As a global leader in Engineering and R&D services (ER&D), Altran offers its clients a new way to innovate by developing the products and services of tomorrow. Altran works alongside its clients on every link in the value chain of their project, from conception to industrialization. For over thirty years, the Group has provided its expertise to key players in the Aerospace, Automotive, Defence, Energy, Finance, Life Sciences, Railway, and Telecoms sectors, among others. In 2016, the Altran group generated revenues of €2.120bn. With a headcount of more than 30,000 employees, Altran is present in more than 20 countries.

CONTACT US

For more information please contact **wcc.advanced-networks@altran.com**

MANO AND MONITORING:

two bumps on the road
to SDN/NFV

altran