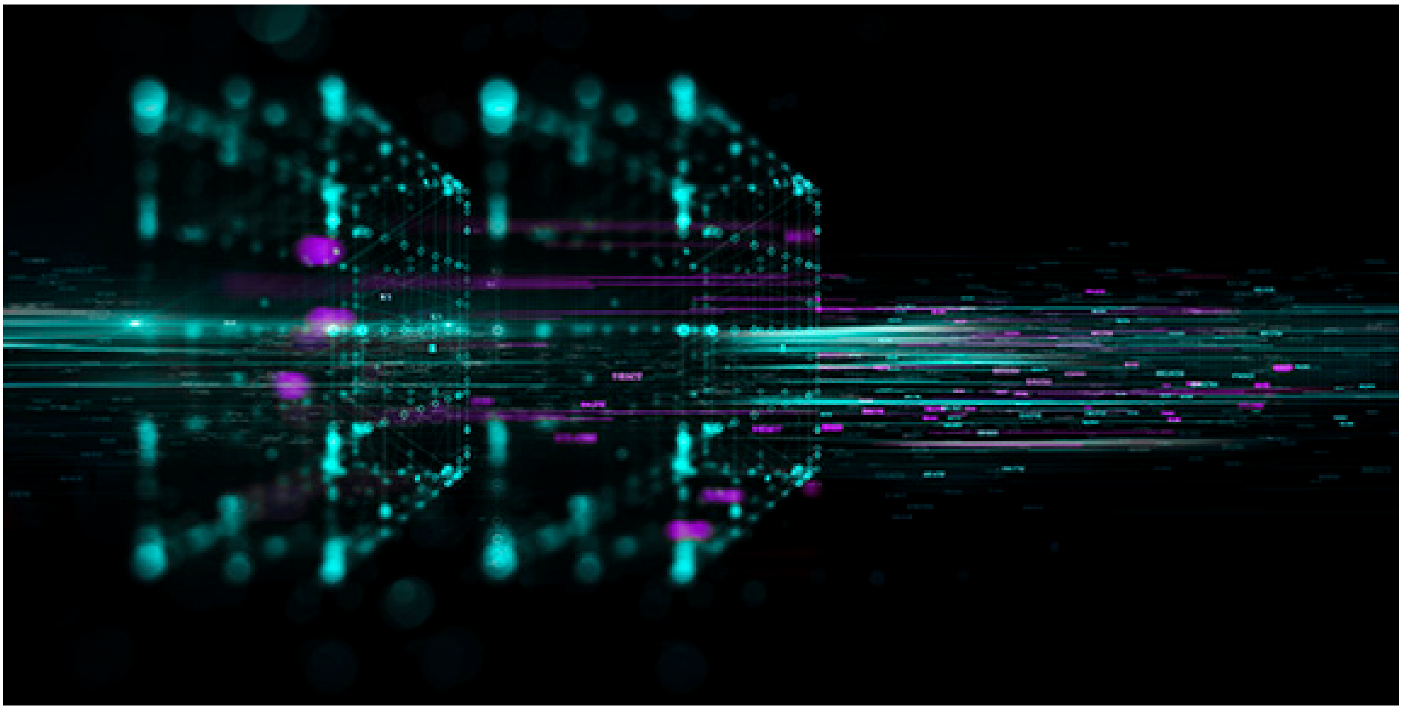
Risk mitigation while deploying 5G network infrastructure

Contents



Introduction

Historically, communications service providers (CSPs) have sourced their telco-grade network equipment from network equipment providers (NEPs). This meant that CSPs did not have much flexibility in choosing the vendors; however, CSPs' risk exposure was minimal as NEPs guaranteed that equipment deployed met stringent environmental and service-level agreement (SLA) requirements. Examples of environmental requirements are electromagnetic compatibility, electrical safety, shock, vibration, climatic, flammability, and energy efficiency. Examples of SLA requirements are latency, jitter, throughput, high availability, redundancy.

Network Functions Virtualization (NFV), prevalent in 5G networks where software is disaggregated from hardware and telecommunications workloads are deployed on IT-based infrastructure, promises lower cost and liberation from vendor lock-in. Also, NFV implies a shift in end-to-end validation responsibility from NEPs to system integrators or CSPs themselves. CSPs will therefore incur new risks for the end-to-end solution as elements are acquired and integrated independently. Also, deployed IT-based infrastructure needs to be telco-grade hardened in order to meet stringent environmental, SLA, and security requirements. The extensive use of IT infrastructure and the 5G network architecture also make the networks more vulnerable from a security standpoint.

As CSPs start deploying 5G, they will need to manage these new challenges. During this network transformation journey, they need a trusted partner that has unique capabilities to help them deploy NFV Infrastructure (NFVI) without incurring unwanted risks.

Risk mitigation and how HPE can help

Hewlett Packard Enterprise has developed a number of unique capabilities to mitigate risks that CSPs will incur during their 5G network transformation journey. These include:

- Secure infrastructure
- OS/driver tuning and performance benchmarking of telco workloads on HPE servers equipped with traditional and smart network interface cards (NICs) from leading vendors
- Telco compliance certification of HPE infrastructure
- HPE Telco Blueprints
- HPE Telco Software-Defined Infrastructure (SDI) Toolset

Secure infrastructure

HPE compute platforms have silicon root of trust technology that protects infrastructure throughout its lifecycle. This capability is quite unique because we design and develop our own custom HPE Integrated Lights Out (iLO) 5 chip. We also design and develop our own firmware. HPE places a digital fingerprint into the silicon when it is manufactured. Since this fingerprint is programmed into silicon, it is immutable once the chip is manufactured. The HPE iLO firmware uses this fingerprint to verify its integrity, and once it is verified, HPE iLO in turn verifies the integrity of other essential firmware such as the basic input/output system (BIOS), complex programmable logic device (CPLD), innovation engine (IE), and management engine (ME). This immutable connection between the silicon and firmware protects the server through the production process, through our supply chain shipping and distribution, right to the customer's final location.

HPE iLO is the first piece of circuitry that comes alive when the server is plugged into auxiliary (AUX) power. The silicon root of trust verifies all essential firmware at startup. Furthermore, if secure boot capability is enabled, the Unified Extensible Firmware Interface (UEFI)/BIOS can ensure a trusted OS is loaded. Over a million lines of firmware code runs, before the OS starts, making sure that all server essential firmware is free from malware or compromised code.

During operation of the server, the user has the option to perform runtime firmware validation of firmware stored on the serial peripheral interface (SPI) parts in the server. At any point, if compromised code or malware is detected in any of the essential firmware, an HPE iLO audit log alert is created to notify the customer that a compromise has occurred. In the unlikely event of a breach into the HPE server firmware, after detection has been completed the customer may then securely recover the firmware automatically to a previous known good state. The user also has the ability to save the compromised firmware for potential forensic analysis.

This unique ability to provide secure compute lifecycle and myriad other security features becomes very important when compute platforms are deployed at a very large number of unmanned 5G edge sites. These include:

- Memory authentication
- Digitally signed firmware for NICs and solid storage driver
- Data-at-rest encryption

- Electronic and biometric door locking on racks
- Temper-resistance
- Two-factor authentication using Common Access Card (CAC)
- Secure remote server management

OS/driver tuning for telco workloads

HPE is unique in maintaining an HPE NFV/Telco Lab dedicated to ensuring that our server platforms offer optimized performance specifically targeted at telecommunication use cases. The HPE NFV/Telco Lab's engineers have developed comprehensive OS/driver tuning expertise in areas such as Data Plane Development Kit (DPDK)/packet processing, BIOS and kernel tuning, and open virtual switch (OVS)/virtual machine (VM) tuning. This lab proactively collaborates with network technology partners on OS/driver validation and performance benchmarking. This process is facilitated by the deep engineering relationships established over many years with these partners. By identifying and resolving issues in early releases, it is ensured that the upstream drivers provided by network technology partners perform optimally. HPE also produces extensive performance benchmark reports, available on request, on various traditional and smart NICs.

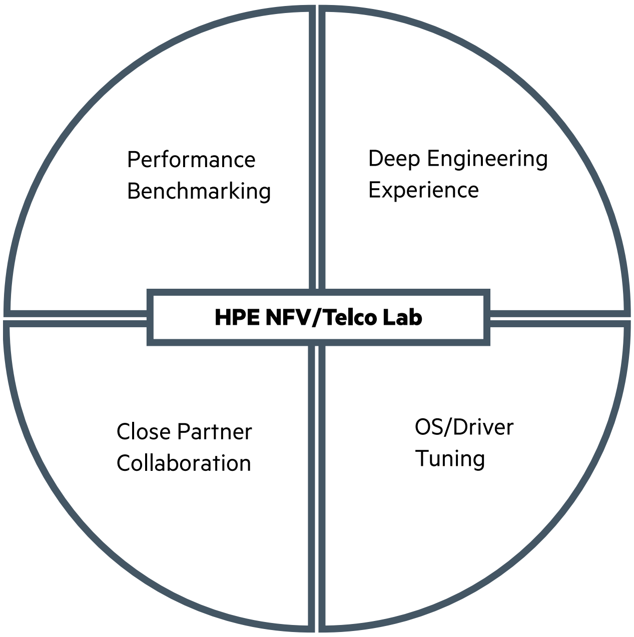


Figure 1. HPE NFV/Telco Lab

HPE has technical resources and deep technical expertise to support partners and customers if the need arises to troubleshoot issues in complex customer environments. The performance benchmarking and tuning procedures ensure that maximum NFVI performance is achievable on HPE platforms, with the capability of supporting the most demanding NFV applications. These validation and tuning processes include acceleration software such as DPDK (with bare-metal, Peripheral Component Interconnect (PCI)-pass through, and single-root input/output virtualization (SR-IOV) configurations), OVS with DPDK, IPSec encrypt/decrypt acceleration, and OVS offload. As a result, HPE telco test expertise is highly valued and includes collaboration with many networking partners.

For example, HPE has invested in network test generation infrastructure that allows us to perform standard packet processing benchmarking with DPDK such as RFC 2544, which determines the maximum packet load achievable with no loss at a range of packet sizes. In a recent test, an HPE ProLiant DL580 server configured with IPSec accelerator cards was able to achieve 720 Gb of encrypt/decrypt throughput.[1] Various OVS offload solutions with a range of packet sizes and numbers of flow definitions have also been analyzed. HPE NFV/Telco Lab is actively working on next-generation technologies such as PCI Gen4 platforms, SFP56 (PAM-4 NICs), and field-programmable gateway arrays (FPGAs).

[1] Based on tests done in HPE NFV/Telco Lab, Dec 2018.

Telco compliance certifications

Network Equipment-Building System (NEBS) was developed in the 1970s to standardize equipment that would be installed in a central office. A strict testing protocol, NEBS focuses on personnel safety, protection of property, and operational continuity. The test protocol includes physical, electrical, and visual requirements. Testing requirements are mandated by the network carriers, providing confidence that equipment has a high degree of reliability and will work under extreme environments while maintaining service for customers.

NEBS has multiple levels with Level 3 being with strict specifications for fire suppression, thermal margin testing, vibration resistance (earthquakes), airflow patterns, acoustic limits, failover and partial operational requirements (such as chassis fan failures), failure severity levels, RF emissions and tolerances, and testing/certification requirements. In order to be NEBS Level 3 compliant, equipment needs to be verified by accredited third-party independent test labs.

NEBS strict requirements help ensure that availability and reliability are designed into the equipment. NEBS Certification results in better-built, safer equipment. NEBS testing also:

- Provides personnel protection from injury caused by electrical power short circuits, lightning, overheating, and equipment movement resulting from earthquake or building motion
- Offers simpler equipment planning and installation for protection of the network from outages from incompatible equipment
- Prevents interference to licensed radio transmitters and cross-aisle equipment network interferences; minimizes the risk of fire in network facilities and other equipment, and the spread of fire while protecting personnel from smoke
- Ensures equipment operation under the broad range of temperature, humidity, vibration, and airborne contamination present within a network facility
- Ensures equipment and service survivability in the event of earthquake

A similar set of requirements are specified by the European Telecommunications Standards Institute (ETSI) for telco equipment being deployed in Europe.

HPE pioneered the use of industry-standard servers in telco and created the category of telco-compliant carrier-grade industry-standard servers. Carrier-grade testing entails more than just NEBS certification. HPE follows ASHRAE Class 3 and Class 4 guidelines and conducts testing for, amongst other things, high-performance fans/cooling optimization, temperature margining, enhanced electrostatic discharge (ESD) protection, flame/fire resistance testing and high-endurance component validation.

HPE testing certification covers both NEBS (GR-63-CORE and GR-1089-CORE) and ETSI (overlaps with NEBS plus 300 019-2-1, 2, 3, and 300 753), and seismic zone 4. If CSPs have specific technology needs, HPE has the business processes to support them.

Figure 2. NEBS-certified HPE platforms

HPE also works very closely with CSPs to optimize their existing compliance processes, resulting in savings and faster time to market.

Over the years, HPE has identified various design requirements needed to meet carrier-grade standards; when such design changes are identified, these changes are rolled into the mainstream offerings. Because HPE designs servers with NEBS in mind, we offer the same consistency, cost, and innovation for telco customers that our enterprise customers expect in their data centers.

HPE publishes carrier-grade specific QuickSpecs such as the following:

- h20195.www2.hpe.com/v2/getdocument.aspx?docname=a00042637enw

HPE Telco Blueprints

HPE Telco Blueprints are fully engineered reference NFVI designs, which are extensively validated along with various industry-leading third-party virtual infrastructure manager (VIM) and software-defined networking (SDN) products. HPE Telco Blueprints are constantly evolving and are specifically optimized for various telco use cases targeted at core, regional, and edge data centers. They are designed for flexibility with best practice guidelines for customization as required by CSPs and benchmarked with various VIM options to guarantee performance.

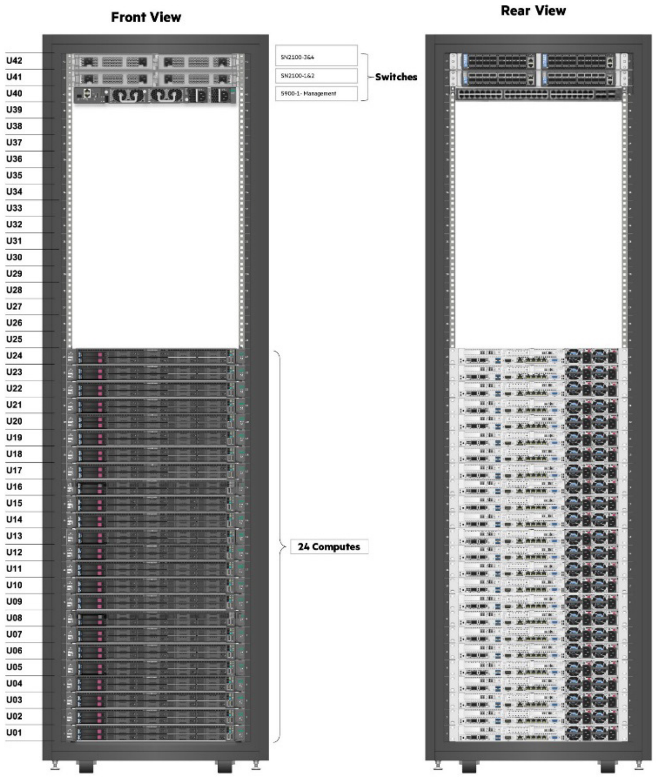


Figure 3. HPE Telco Blueprints

During the HPE validation and integration process, VIM software (such as Red Hat® OpenStack® and VMware vCloud® NFV™) undergoes rigorous testing to ensure suitability for telco deployment. This testing includes validating the system using industry acknowledged automation and performance benchmarking test suites such as Rally and Yardstick. Working with VIM vendors, NICs are benchmarked for data traffic performance. For example, SR-IOV, OVS-DPDK, and RFC 2544 tests for throughput, jitter, and latency performance are executed comprehensively. These tests help identify the optimal settings on compute nodes that will ensure acceptable NIC performance for data traffic.

Performance testing also includes tests to characterize the software-defined storage performance. These tests characterize the system and observe variations in storage metrics (input/output operations per second (IOPS), throughput, and latency) while simultaneously scaling resources on the system. These tests are executed for typical telco workload block sizes and access patterns (read/write ratio, random access).

HPE Telco SDI Toolset

The ability to optimally choose server, storage, and networking platforms along with virtualization infrastructure management (VIM) software and network applications provides telcos with numerous benefits including the elimination of vendor lock-in and the acceleration of service innovation. However, configuring and deploying these disaggregated next-gen telco clouds at scale to achieve carrier-class performance requires specialized expertise.

To reduce risk and complexity associated with deployment of telco infrastructure, HPE has developed an SDI Toolset for CSPs that provides smart utilities and reports needed to efficiently optimize infrastructure deployment, saving CSPs both time and resources. The HPE Telco SDI Toolset also ensures infrastructure configuration consistency and reliability across the network, and prevents human errors that could otherwise impact network stability and performance.

HPE Telco SDI Toolset benefits include:

- Simplified configuration
- Reduced errors
- Accelerated provisioning
- Optimized configurations with predictable performance metrics
- Faster time to value

The HPE Telco SDI Toolset is comprised of the following components:

- HPE Telco NFV Platform Software Toolkit (NPS Toolkit)
- HPE Telco Infrastructure Configuration Generator (TICG)
- HPE Telco Installer Utility for Yardstick
- HPE Telco Ceph Performance Tool
- HPE Telco Ceph Characterization Report
- HPE Telco NIC Characterization Report

Conclusion

Without doubt, 5G is knocking at the door. To gain the full technical and economic advantage of new technologies such as NFV, CSPs will face new complexity and risks. Some of these risks are due to hardware disaggregation, and are introduced because of technical architectures such SDN and NFV. CSPs need a trusted partner such as HPE to help them deploy NFVI while mitigating these risks. HPE has developed unique capabilities such as OS/driver tuning for telco workloads, telco blueprints, telco compliance certifications, and secure infrastructure to help CSPs during this transformation journey.

Learn more at

hpe.com/dsp/infrastructure

✉ **Share now**

Get updates

a50000141ENW, August 2019