LF NETWORKING

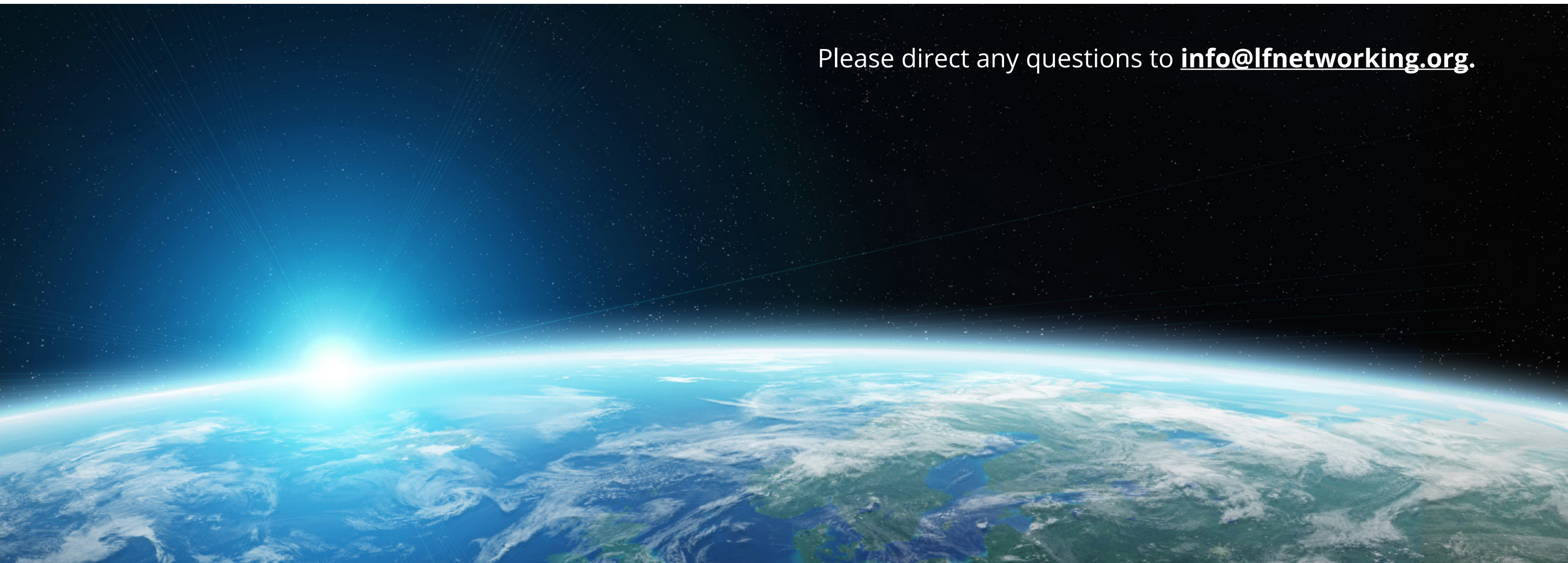
White Paper: NFV Testing and Automation

A Telecom Operator's Perspective

Authored by the Members of the Linux Foundation End User Advisory Group

Randy Levensalor (CableLabs)
Lei Huang (CMCC)
Ahmed ElSawaf (STC)
Saad Sheikh (STC)
Cecilia Corbi (TIM)
Massimo Banzi (TIM)
Beth Cohen (Verizon)

For more detailed information, please see the accompanying paper:
NFV Testing & Automation Research and Methodologies.



Please direct any questions to **info@lfnetworking.org**.

Table of Contents

1 Key Takeaways

- To take advantage of rapidly changing technologies, the Telecom industry needs to be able to deliver new NFV (Network Functions Virtualization) services quickly and efficiently.
- Successful and scalable NFV deployments require extensive testing, standard testing methodologies, and testing automation.
- A shared understanding of NFV testing processes across the industry is needed to optimize interoperability.
- Some systems and testing automation approaches are available today, but more R&D is needed across the industry to establish best practices.
- The open source community and Telecom standards bodies can play key roles in furthering the development of standard testing platforms, frameworks, and best practices.
- All stakeholders across the Telecom industry, operators, and ecosystem companies are welcome and encouraged to join this critical effort to define the testing projects and requirements in support of NFV deployments.

2 Overview

The software industry, leveraging virtualization, cloud native approaches, agile methodologies, and test-driven development has long been able to build applications and infrastructure flexible enough to be seamlessly modified multiple times a day. But should the Telecom industry, with its stringent requirements for high availability, and its distributed service delivery models, adopt these methodologies for its own infrastructure and systems? The answer is a resounding yes. However, due to a relatively poor understanding of the requirements and immaturity of Telecom specific testing frameworks, the industry has been slow to adopt these potentially industry changing technologies.

With the drive to deploy 5G, network slicing, and the dramatic changes in network service delivery due to the global pandemic, 2020 was the year that many carriers started large NFV deployments. This indicates the maturation of NFV technology and the acceptance of the need for virtualized networking workloads, reference architectures, and cloud infrastructures in general. As these deployments expand, it is past time to develop the testing tools needed to deploy them in a common, shared, programmable and automated manner.

However well the need for these new technologies is recognized, there are significant challenges to achieving this vision for supportable testing frameworks. NFV testing complexity hampers service agility and time to market; the two most important factors for adoption of NFV architectures. The situation is further aggravated by the different SDO (Standards Developing Organizations) and OSC (Open Source Communities) having both overlapping and sometimes conflicting objectives for the few standards that do exist, with no shared definition of how to support Day 2 operations infrastructure changes. This has resulted in unnecessary barriers for vendors, promoted technology silos, and increased complexity across the industry in general.

The Telecom industry urgently needs to define a standard reference testing framework that can be used to build a fully automated continuous testing (CT) framework. This framework would provide the platform to perform vendor agnostic testing and benchmarking, yet be flexible enough to integrate vendor specific tools to realize the operators' visions for supporting their deployments. As operators' NFV platforms evolve to meet cloud native requirements, there is a need to build platforms that support both VNF (Virtual Network Function) and CNF (Cloud Native Network Function) workloads as transparently as possible. This by extension will enable carriers to extend testing and CI/CD (Continuous Integration/Continuous Delivery) capabilities to networking IT applications and underlaying Infrastructure.

Creating a common understanding of testing methodologies is a way to address these concerns and enable the building of more robust systems and infrastructure that will benefit everyone in the Telecom industry.

The LFN (Linux Foundation Networking) End User Advisor Group (EUAG) is publishing this document to identify and highlight the latest thinking and recommendations for improving testing environments and some best practices for NFV and SDN (Software Defined Networking) platforms for the Telecom industry. For more details about the supporting research and methodologies that contributed to the recommendations and conclusions, an adjunct White Paper, *NFV Testing and Automation Research and Methodologies*, has been published to complement this document.

2.1 LFN EUAG: Role and Mission

The LFN (Linux Foundation Networking) End User Advisor Group (EUAG)'s mission is to share views, challenges, and best practices among organizations in the Telecom industry; particularly highlighting areas of opportunity for open source developer communities. LFN membership is comprised of various organizations from the industry including Telecom carriers, cable operators, network providers, and compute or storage service providers.

As the voice of the operator end user community, it represents the operators' perspective for various Telecom related open source projects, and their adoption across the industry. Recent projects that the EUAG has been active with include ONAP (BSS/OSS orchestration tooling) and the Anuket project's VNF infrastructure reference models, and testing functions stemming from the CVC (Compliance and Verification Committee) for the NFV/SDN/VNF Ecosystem, and former OPNFV work.

2.2 Assumptions

- As NFV applications and workloads mature, hardware and software disaggregation will increase with more multi-vendor solutions, requiring a more detailed understanding of the virtualized environments and more integration testing.
- The complexity of interoperability testing is increasing with the introduction of multi-vendor solutions replacing monolithic legacy systems.
- The community is interested in reducing the risks associated with implementing NFV systems brought to market before standards are available.

- Operators and vendors increasingly see the value of using reference models, architectures, and standardized testing to assure that vendor NFV software is compatible with infrastructure designed to support Telecom NFV workloads (NVFI).
- Commodity hardware with built-in hardware acceleration (Smart NIC, FPGA, GPU) will be standard infrastructure components.
- Virtualized components need to support multiple NFVIs and shared physical resources.
- The open source communities and standards bodies are in the best position within the industry to create the required reference testing frameworks and models.

3 Current Industry Status and Problem Statement

Based on the information shared by participating operator and vendor organizations, the level of sophistication of NFV testing is still relatively low, with little cross-departmental and cross-organizational communication, thus making manual errors and institutional bias inevitable. Some key issues uncovered include:

- Lack of or limited test environment configuration and deployment automation
- Little integration or coordination of test scripts across vendors
- No automated test process controls
- Little metrics standardization, meaning cross-vendor and cross-architecture results are difficult to analyze
- Different vendor test tools/test instruments deliver different metrics limiting traceability of test results, etc.

There is general agreement across EUAG member operators that automated network element code construction, integration, network element life cycle and service testing, automated network element deployment, and online full-process automated closed loop testing are all important to speed up network element development, deployment, and systems operationalization.

At the same time, while some operators have introduced DevOps tools into their delivery models to achieve this goal, it is by no means universal in the industry yet. Without standards to drive DevOps and testing cooperation, the service providers and VNF vendors are left to create their own proprietary systems to fill the gap. Typically, this means that VNF vendors provide the software packages without context or easy integration with the other systems in the operators' environments, leaving the operators to implement CI/CD and their own test suites in their DevOps environments. This then leads to further silos, fragmentation of testing activities and less efficiency across the industry.

4 NFV Testing Automation Requirements

Now that it has been established that there is a gap in the ability to rigorously test NFV environments, the next step is to identify the requirements for the test suites. Typically, any systems test follows a similar development and delivery path. The first phase is to define what is needed to be tested—not as easy as it might seem on the surface. Most component tests are carried out by following this method at the high level, "test framework + test instrument/tool + test object". This process includes preparation and deployment of the environment, configuration of the tests, determination, preparation and execution of service parameters, the development of test cases, and finally, a method for observing the test process, and provisions for gathering and analyzing the test results. In general, NFV automated testing requirements should include the following elements:

1. **Test environment:** NFV automated testing should support automated deployment processes including network configuration and network element instantiation. It also requires a method for delivering network workloads to test performance characteristics under different conditions, packet mixes, and types.

2. **Testing Tools:** These include the actual test suites and software modules used to complete the testing. Over time as technologies shift, these tools will need to be modified or changed to meet the changing requirements. A best practice here would be to modularize the tools as much as possible using APIs and other DevOps methodologies.

    a. Determination of how a specified test suite can be loaded.

    b. Test suites/test cases that can be executed regularly or in real time.

    c. Ability to set observation points to monitor the test process in real time.

    d. Capability to modify test logs to set indicators to support customized test reports.

3. **Test elements:** The components of the network that need to be tested include unit tests, integration tests, performance tests, End to End Testing capabilities and UAT; i.e., the full suite of tests that are needed to determine if the NFV applications and environments perform to their expected specifications.

a. **Network element:** It should support the issuance of remote configuration files and provide interfaces to facilitate access to key indicators of network elements.

b. Network element lifecycle testing and service function testing need to support automated deployment of network element, integration of test scripts from different vendors, and automated control of test procedures. At the same time, test tool/instrument integration of different vendors and test results must be traceable.

4. **Test configuration:** Including the test framework/tool and service configuration of the tested object, it should support the unified distribution of the configuration during the automated test processes.

5. **Test execution:** Automated execution of test tasks, providing a flexible automated test framework.

6. **Test process observation:** The test framework/tool should support real-time monitoring of the test processes to facilitate understanding of the execution of test cases.

7. **Test report:** The test framework/tool should support test data aggregation and provide customized test reports.

8. **Test results analysis:** The test framework/tool should support automated analysis and certification of test results and automatic release of certified objects.

To achieve the above recommended objectives, the following are needed. Having a common understanding of those environments and test suites needed is a good start towards developing a standards based approach to testing NFV workloads.

- **DevOps integration:** In the current model, VNF vendors usually provide VNF software packages and operators implement CI/CD in their own DevOps environment. It is recommended that there be a common method for loading a VNF software package into operators' DevOps environments.

- There is a need to develop automated testing pipeline tools and automated acceptance tools; it is recommended to follow the automated testing specifications and procedures developed by the SDOs and open source communities.

- Operators need to define/standardize the interface with third party or vendor automated testing tools, and adapt these tools to suit their specific environmental requirements; including but not limited to, automated deployment, automated data configuration, automated testing, automated upgrades, automated rollbacks, etc.

5 NFV Testing Automation Recommended Actions

5.1 NFV Testing Automation Process Recommendations

ETSI (European Telecommunications Standards Institute) under its TST standard has defined a cross-organization pipeline for the DevOps process for testing NFV type workloads. Given its relative maturity, it is recommended considering implementing the ETSI NFV automated testing process through the common test framework.

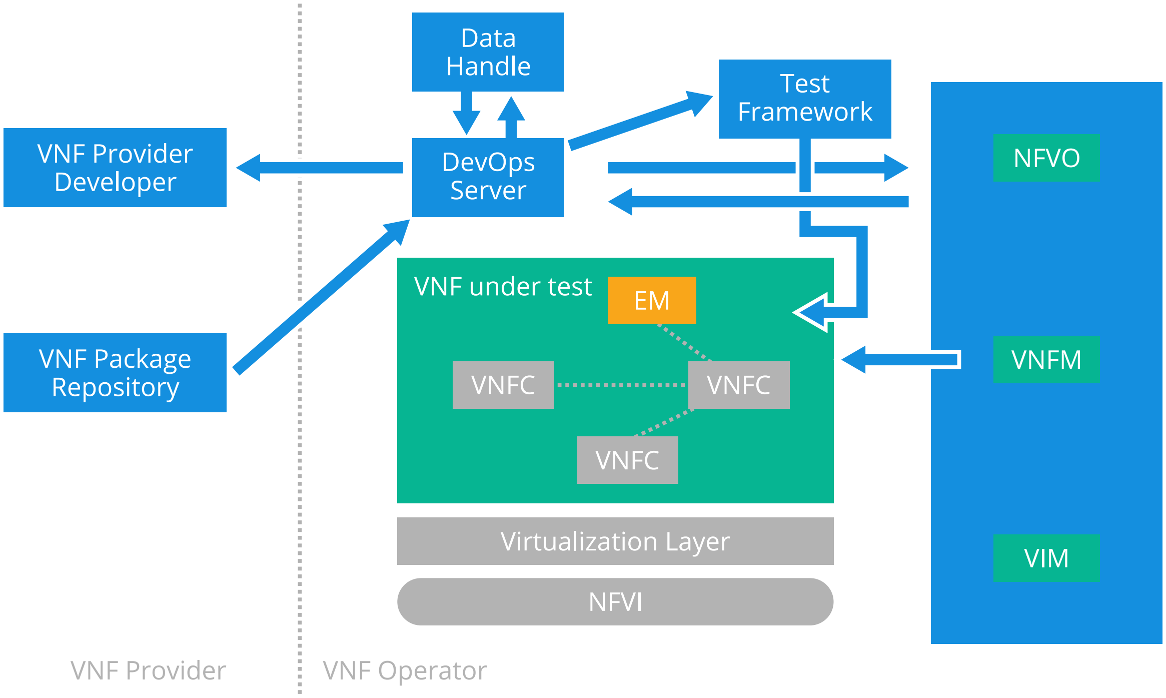


Figure 1: Test component architecture

The common test framework is used to execute the tests and record results. It includes the following elements:

- **Test Execution System (TES):** Used for executing the actual test suites.
- **Test Management System (TMS):** Used for setting-up the test configuration, deploys the TES (if needed) and requests the TES to execute the test suites.

When TMS is common for all vendors and TES might be vendor specific, it is recommended to:

- Enable the case when “TES is a vendor-independent test VNF” mandatory.
- Make it optional to enable the cases when “TES is a vendor-specific test VNF/VNFC”. Other potential extension considerations for containerized VNFs and E2E testing applicability:
  - It is not recommended to build a common test framework for VM-based VNF only.
  - It is mandatory to have the common test framework be able to support E2E testing as well.
  - It is optional to have the common test framework be able to support Containerized VNF testing as well.

5.2 Roles and Responsibilities for Testing Automation

While the entire Telecom industry bears some responsibility for the NFV testing activities, it is expected that each stakeholder will bring their own perspective, so it is important that the automated test frameworks support the needs of the different groups. These groups include operators, vendors, instrument manufacturers, and independent integration and interoperability testing providers.

Testing Perspective	Automated Testing Labor Division
Operators	Operators should provide DevOps joint pipelines that connect vendors, establish a common automated testing framework, integrate instrument and vendor’s maintainable and testing capabilities, integrate open source testing tool capabilities, and provide automated testing solutions.
Vendors	Vendors should provide interfaces, their own testing tools, test case implementation, and provide test feedback channels to obtain monitoring data of the vendor’s tested objects, such as log files, monitoring indicator interfaces, etc.
Instrument manufacturers	Instrument manufacturers should provide a standard test case implementation based on operator test specifications, provide integration capabilities with the operators’ common framework and provide customized test results.

Independent integration and interoperability testing providers	In order to test all of the interactions with the components that could interact in the field, a test bed with multiple NFVIs and other components needs to be continually validated for interoperability. Compliance testing reduces the risk of interoperability testing. However, there is still room for interpretation within these interactions that are not always covered by compliance tests and emerging standards. Using third party testing services, where competing solutions can be tested on the same platform, is one way of ensuring interoperability. The shared services provided by third party testing can reduce the risk of interoperability issues delaying deployments in the field.

5.3 Achieving Industry Acceptance

Based on the high level requirements outlined above, the following are some recommended actions to help gain acceptance within the Telecom industry for more rigorous NFV testing standards overall. By putting in the effort to develop standards based on these high level requirements and turning them into realistic testing frameworks that will work across the industry, everyone will be able to benefit with reduced risks, faster deployments, and more confidence that the systems will perform as expected.

1. Introduce common vendors/integrators to automated testing tools.
    - Operators initiate automated testing through automated testing tools processes.
    - Use common vendor and/or integrator deployment tools to deploy testing environments.
    - Use a common set of testing automation tools.
    - Analyze test results through operators, automated acceptance tools or third-party instruments.
    - Create a common methodology for automatically loading VNF software packages into operators' DevOps environments.
2. Modify existing manual test specifications to adapt them to support automated processes.
    - Reduce the number of rollbacks to the test environment by recombining test cases according to common test scenarios.

  - In order to better meet test automation objectives, the existing test cases should be modified. This includes but is not limited to the test content, test steps and acceptance criteria, etc.

3. Implement the automated testing processes in stages to minimize impact on existing systems.

   - Start by implementing automated testing of highly standardized test objects such as hardware and virtual layer, and gradually add test objects such as MANO and VNF.

   - For service function tests such as MANO/VNF testing that needs to rely on third party or vendor automated testing tools, the test execution processes should be automated, and the test execution results artificially determined to solve the test credibility problem. This allows the subsequent execution results to be automatically determined to achieve full testing process automation.

5.4 Promoting Open Source and Testing Standards

Based on the EUAG's members' findings regarding the relative maturity of NFV testing status of various operators and vendors in Open Source communities and standard organizations, the following are some recommendations on the promotion of automated testing by various open source communities and standard organizations.

Promotion method by community	Automated Testing Labor Division
Open source community	Gather common operator requirements for automated testing into the OVP as a third party testing and certification platform to implement the Validator platform defined in ETSI standard TST006.
Standards Developing organization	Align the DevOps joint delivery pipeline and relevant processes into the Validator defined by ETSI TST006, and align the ETSI TST013 standard test framework, and test case template to implement the DevOps process.

6 Conclusion and Call to Action

In conclusion, while there have been some efforts to create standard testing frameworks to support the new NFV architectures needed for the Telecom industry, there is still a long way to go towards having a common platform and understanding of the methods and processes required. The industry needs to work together by leveraging the open source and standards communities to create reference test frameworks to achieve this goal. If everyone, the operators, the vendors, the integrators, testers and others in the ecosystem all do their part in promoting common testing methods and building a common set of NFV testing frameworks and tools, the entire Telecom industry ecosystem benefits by being able to deploy NFV and NFV infrastructure faster and more efficiently.

7 Glossary

OSC	Open source communities
SDO	Standards Developing Organizations
CSP	Communications Service Providers
LFN	Linux Foundation Networking
EUAG	End User Advisory Group, a working group within the LFN