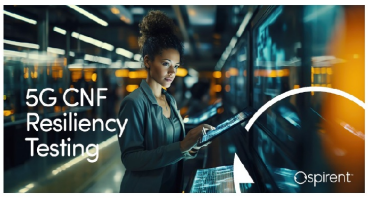


Spirent Cloud Native 5G CNF Resiliency Testing User Guide

Contents

Spirent Cloud Native 5G CNF Resiliency Testing

Specifications

- **Product Name:** 5G CNF Resiliency Testing
- **Author:** A Spirent Guide

Product Information

Cloud-native Architectures for 5G Success
Service providers expect 5G to help power critical business transformation by diversifying and growing revenue streams. The right strategy will support rollout of new services in weeks versus months, with always-on, high-performance, and expansive coverage attracting and delighting customers.

This vision cannot be achieved without cloud-native architectures, which service providers are adopting in anticipation of myriad benefits, including:

- Increased network efficiency
- Hardware utilization and automation
- Operational efficiency (reduced OPEX)
- Resource optimization (reduced CAPEX)

Cloud-native Efficiencies and Challenges
Cloud-native architectures represent a technology evolution to software-based services and networks that enable agility and efficiency. However, these advancements introduce considerable complexity.

The mobile evolution to cloud-native architectures:

- Mobile infrastructures have become increasingly software-based, comprising ever-smaller software entities that communicate and run on commodity hardware.
- Over time, these functional building blocks, known as network functions, have progressed from physical to virtual, and now, cloud-native.

Adoption challenges for 5G cloud-native architectures:

- The fine granularity of containerized cloud-native software
- Dynamic nature of 5G networks and services
- Customer and use cases with real-time response expectations

Product Usage Instructions

Section 1: Cloud-native Architectures for 5G Success
To achieve the benefits of 5G cloud-native architectures, follow these steps:

1. Understand the importance of cloud-native architectures in powering critical business transformation.
2. Implement a strategy that supports the rollout of new services in weeks with high-performance and expansive coverage.
3. Adopt cloud-native architectures to increase network efficiency, hardware utilization, and automation.
4. Ensure operational efficiency by reducing OPEX and optimizing resource allocation to reduce CAPEX.

Section 2: Cloud-native Efficiencies and Challenges
To navigate the complexities of cloud-native architectures, follow these steps:

1. Recognize the evolution of mobile infrastructures from physical to virtual and now to cloud-native.
2. Understand the advantages of software-based services and networks in enabling agility and efficiency.
3. Be aware of the challenges associated with cloud-native deployments, including fine granularity, dynamic nature, and real-time response expectations.

Section 3: Adoption challenges for 5G cloud-native architectures
To address the challenges of adopting 5G cloud-native architectures, consider the following:

1. Develop strategies to handle the fine granularity of containerized cloud-native software.
2. Implement solutions to manage the dynamic nature of 5G networks and services.
3. Ensure customer and use cases meet real-time response expectations through proper planning and implementation.

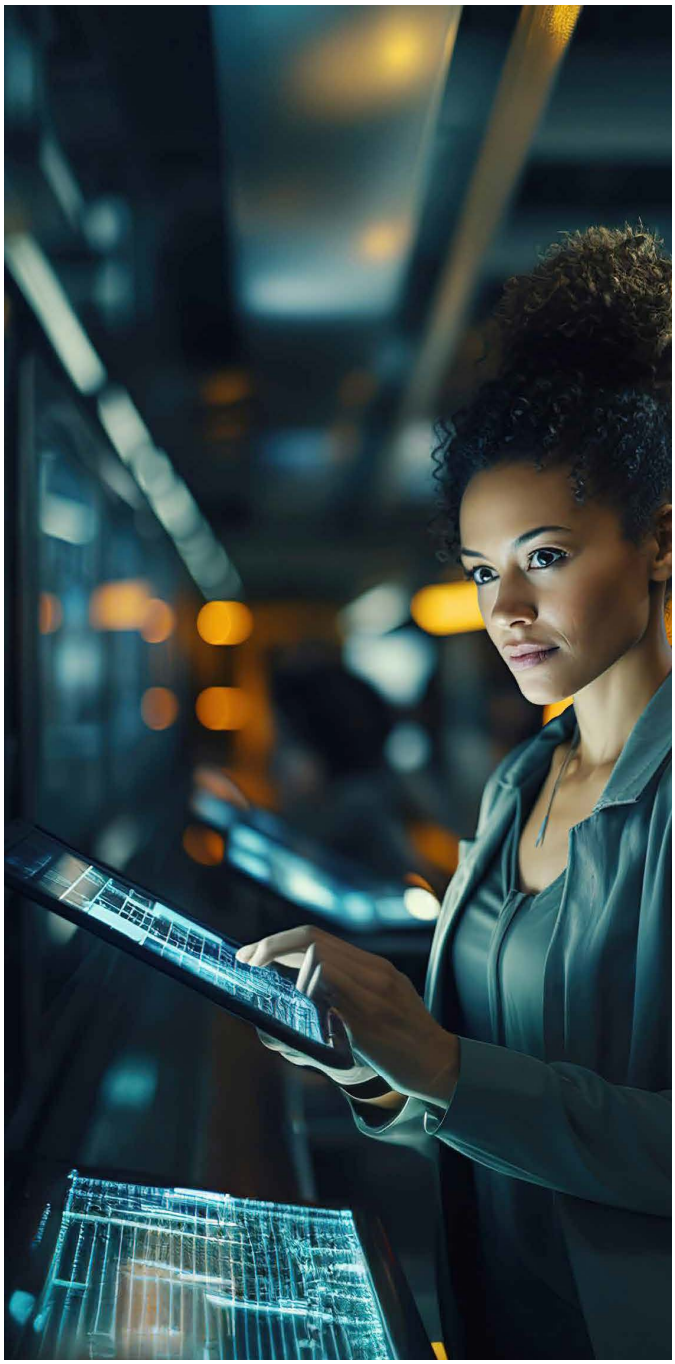
FAQ

- **Q: What are the benefits of cloud-native architectures for 5G?**
  A: Cloud-native architectures provide increased network efficiency, hardware utilization, and automation, resulting in operational efficiency and resource optimization.
- **Q: What are the challenges associated with adopting 5G cloud-native architectures?**
  A: The challenges include managing the fine granularity of containerized software, handling the dynamic nature of 5G networks and services, and meeting real-time response expectations for customer and use cases.

A SPIRENT GUIDE
5G CNF Resiliency Testing

Cloud-native Architectures for 5G Success

- Service providers expect 5G to help power critical business transformation by diversifying and growing revenue streams. The right strategy will support rollout of new services in weeks versus months, with always-on, high-performance, and expansive coverage attracting and delighting customers.
- This vision cannot be achieved without cloud-native architectures, which service providers are adopting in anticipation of myriad benefits, including:
    - Agility to adapt quickly to changing market demands and customer needs by rapidly deploying network services and applications.
    - Scalability to support 5G adoption by provisioning additional network capacity on demand.
    - Cost-efficiency to reduce operational spend by leveraging cloud infrastructure and automation tools.
- In short, cloud-native architectures provide the foundation service providers need to successfully pursue 5G opportunities across consumers and industry.



Cloud-native Efficiencies and Challenges

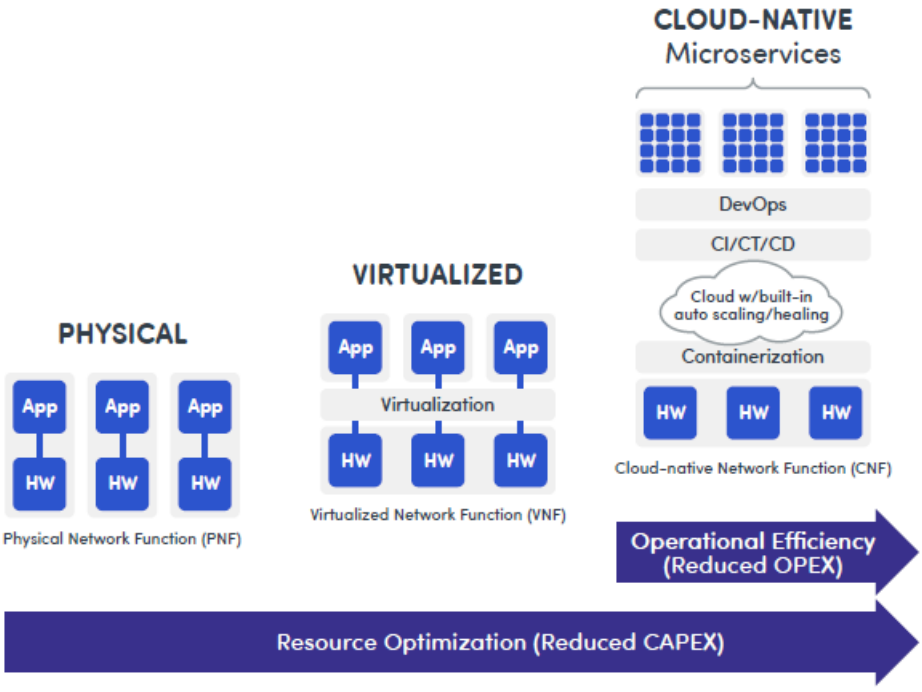
- Cloud-native architectures represent a technology evolution to software-based services and networksthat

enable agility and efficiency. However, these advancements introduce considerable complexity.

- This guide addresses the challenges associated with cloud-native mobile network deployments, and explores how test and assurance must evolve to mitigate service disruptions.

The mobile evolution to cloud-native architectures

- Mobile infrastructures have become increasingly software-based, comprising ever-smaller software entities that communicate and run on commodity hardware. Over time, these functional building blocks, known as network functions, have progressed from physical to virtual, and now, cloud-native. It's helpful to understand the advancements each of these evolutions have introduced:
  - Physical. Single vendors provide network nodes or functions (e.g., a switch) with integrated hardware and software.
  - Virtualized. Virtualized network functions are disaggregated from underlying virtual machines to improve hardware utilization, but rigid coupling between network function and virtual machines limits flexibility.
  - Cloud-native. Containerized cloud-native functions (CNFs) communicate via standardized APIs, supporting multiple vendors with services abstracted and exposed to smaller units of code (pods).
- **A cloud-native architecture increases network efficiency and hardware utilization to enable automation by:**
  - Breaking software into smaller pieces so more network functions can run on existing hardware and serve more customers with the same hardware investment.
  - Automatically adding or removing pods to efficiently and quickly meet demand changes.
  - Easily migrating all pods to different hardware when current hardware needs to be updated.
  - Quickly replacing a dysfunctional pod without impacting users.
  - Automatically optimizing resource utilization according to service provider policies.



Evolution to cloud-native architectures

Adoption challenges for 5G cloud-native architectures

The benefits of cloud-native architectures are also accompanied by technology and business challenges.

Technology challenges

- The fine granularity of containerized cloud-native software, dynamic nature of 5G networks and services, and customer and use cases with real-time response expectations pose new challenges versus monolithic physical networks or virtualized networks.
- Let's review the impact each of these challenges has on deployments.

Dynamic, "multi" environment.

CNFs and the clouds that interconnect them change continuously based on demand and routine operational challenges. These changes can introduce subtle, hidden issues that may not manifest until the system is under stress in the production network. Risk is increased because:

- Many vendors and multiple clouds need to work together in harmony.
- Continuous software churn of new releases, updates, and CI/CT/CD, from multiple vendors, can introduce faults.
- All software runs on shared hardware, increasing contention and performance issues.

Performance expectations.

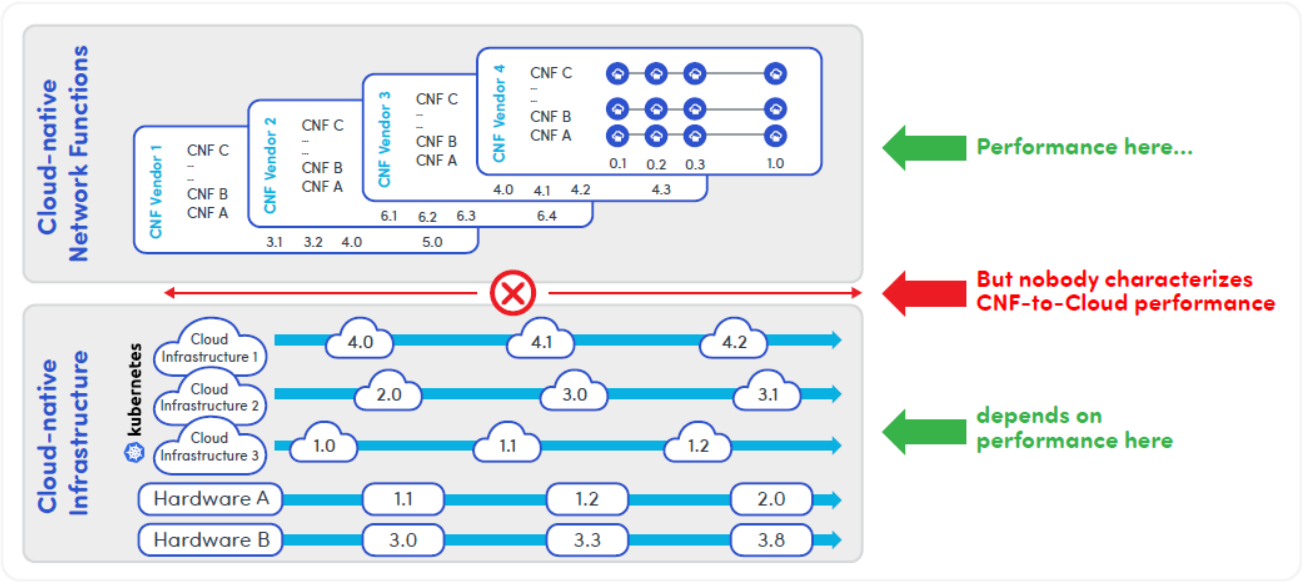
5G use cases require strict real-time responses for millions of concurrent users. Real-time responsiveness is challenged because each:

- 5G service contains multiple CNFs, that are highly interconnected, complex software elements that execute multiple workloads on a common hardware and software infrastructure.
- CNF and its pods rely on shared cloud infrastructure resources to function properly.
- CNF has specific requirements from the shared cloud infrastructure it runs on. If a workload doesn't get the compute and memory resources or network quality it needs, its performance will degrade.

Performance dependencies.

The performance of a 5G service depends on the CNF's performance, the cloud-native infrastructure's performance, and the performance of the CNF-to-cloud interface. Service performance is put at risk when:

- The performance required by a CNF is not supported by the cloud-native infrastructure.
- The CNF and the cloud can technically meet the specified functional requirements, but a slow response time between CNF and cloud may degrade the required user experience.
- Lack of understanding of the performance dependencies between CNFs and the cloud-native infrastructure can result in delayed issue resolution.



CNF-to-cloud: the missing performance metric

Business challenges
In the dynamic 5G cloud-native world, the performance of 5G applications depends directly on the performance of the underlying cloud. However, a service provider's CNF/application workloads team typically operates independently from the cloud software and hardware infrastructure team, with this silo extending to testing, too. The existence of multiple teams and lack of understanding of the cloud performance required by each workload complicates and delays fault resolution.

- A large public event or software bug that causes application performance degradation in the production network may impact service quality for large groups of customers. When that happens, the CNF and cloud infrastructure teams collaborate to identify the degradation's cause. All-hands conference calls between service provider and vendor teams may involve 20-30 people, with hours passing before the issue is pinpointed and days before it is fully resolved.
- The lack of performance dependency criteria for the application makes it difficult and expensive to identify and isolate the fault. The root cause may be a specific CNF that is no longer getting the network performance it needs from the cloud. But the cloud team may not know what performance that application expects. The workload and cloud teams may have properly conducted individual pre-production testing, but the app's performance dependency on the cloud has not been tested.
- This is an issue faced by every service provider.

A New Way: CNF Resiliency Testing

- Traditional pre-production testing is not sufficient for cloud-native architectures.
- In this complex and dynamic cloud-native 5G world, there is simply too much that can go wrong in the production network that traditional pre-production testing can't detect.
- During pre-production testing, the underlying cloud environment is typically lightly loaded and mostly free of degradations. It is also not the actual shared cloud network the application will use in the live network.
- As a result, many issues only present themselves during production, when congestion or unusual states are encountered.
- This is giving service providers pause as they migrate to cloud-native and question how to:
    - Ensure 5G CNFs will work as expected when pushed into production, especially into a cloud environment they don't own.

    - Ensure the cloud will provide the right networking, storage, memory, and latency performance to meet 5G SLAs.
    - Predict what will happen if the needed performance isn't met and what it will take to fix it.
    - Identify key cloud metrics that should be analyzed in production deployments to accelerate root cause analysis and recovery times.
- Open source tools provide some relief with a focus on introducing impairments but they do nothing to correlate them to application behavior.
- Service providers have an urgent need for new ways to identify problems during pre-production. Specifically, they require a
  5G-specific approach that provides correlation from the impairment to the application layer. This CNF resiliency testing identifies and resolves problems before they reach the production network.

The cloud-native approach to resiliency
Software-based, cloud-native architectures take a different approach to network resiliency versus hardware-based traditional networks that offer five-nines reliability through equipment redundancy.

Cloud-native architectures handle resiliency based on two fundamental principles:

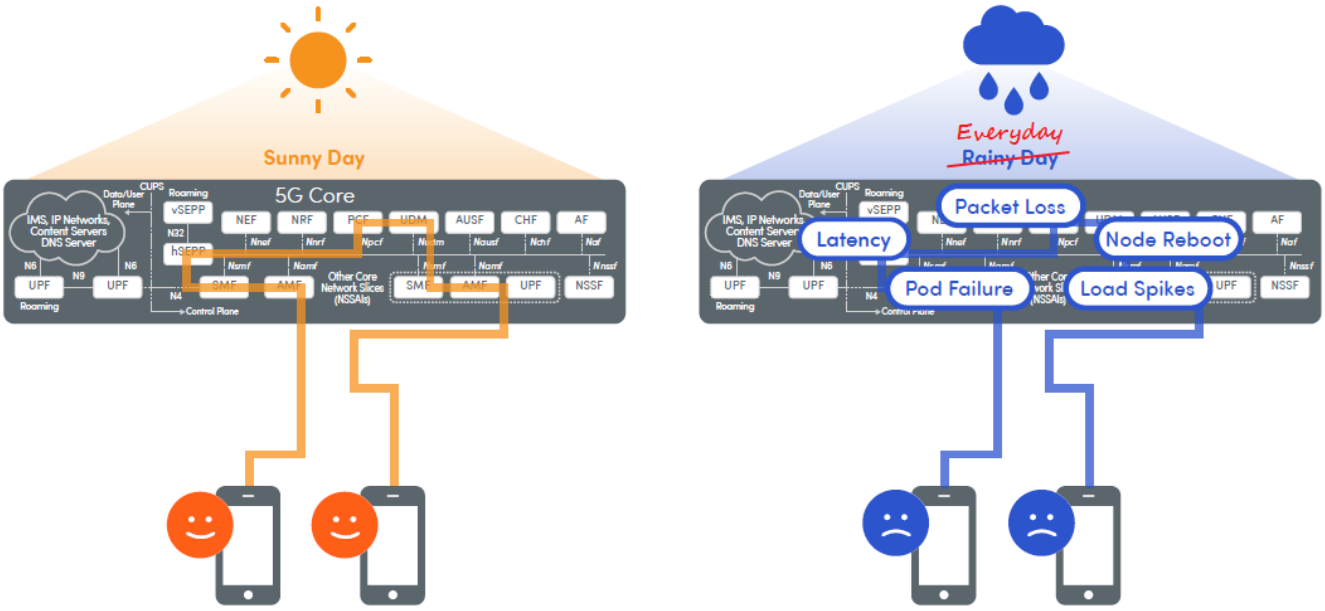
1. Limiting failure impact by breaking network functionality into small pieces to limit the "blast radius" of failure events, such as software bugs. Container and Kubernetes technologies distribute user traffic across small pieces of code (pods), so that if a pod fails, only a small number of users will be affected. The outage impact is reduced significantly compared to monolithic virtual and physical network function systems.
2. Quickly detecting and recovering from failures rather than overbuilding to avoid failures. Cloud hardware is optimized for maximum performance and lowest cost, not reliability. In the five-nines monolithic physical model, everything the network function needed was provided in a vendor's integrated, turnkey system and they were called to resolve problems.

The combination of limited blast radius and rapid recovery from failures supports high overall availability for cloud-native functions.

The challenges of pre-production CNF resiliency testing
The goals of cloud-native pre-production testing remain the same as for traditional environments–namely, understanding how each element behaves in isolation and in tandem with other elements.

- **However, achieving this for cloud-native is vastly different than in traditional networks due to:**
    - Variability. The production cloud the CNF runs on is dynamic and not always under the service provider's control, so the same user stimulus may result in varying cloud execution. Statistical simulation and analysis is needed to understand the probability of production network failures and likely causes.
    - Vulnerable performance. A production CNF might be deployed in 100 or more different pods. To deliver a 5G service (and maintain an SLA), all those pieces must communicate within certain latencies—often milliseconds—or they will time out. If any link in the chain gets delayed or disrupted, failures can result in 5G service failures.
    - Expect the unexpected. Issues like a noisy neighbor, slow cloud network fabric, or a software bug causing one or more links between CNF pods to break or time out are hard to anticipate.
    - Enormous variability. A 5G workload might be deployed on multiple types of distributed pods, running on

dozens of different physical or virtual hosts, across a variety of public and private clouds. A CNF's performance will depend on the actual path it takes.
    - Constant stream of updates. Continuous software updates from multiple vendors for multiple CNFs need to be validated before moving into the production network.
- Pre-production CNF resiliency testing needs to test those complex situations under realistic cloud-native scenarios to determine
- **how the CNF behaves, how 5G services will perform, and how** to respond if there is an issue. System-level visibility–not an IT workload "atomic" view–is required for cloud-native assurance.
- Current testing approaches are unsatisfactory for cloud-native. They test from the application layer on a more or less "perfect" cloud infrastructure with the assumption that the cloud is always performant and reliable. Unfortunately, live network clouds are neither.
- CNF resiliency testing enhances traditional application testing by introducing turbulent cloud conditions that mimic dynamic and unpredictable real-world clouds that have contention for hardware and software resources, constant fluctuations, and component failures.
- As a result, failures are identified in pre-production instead of in the production environment where they impact customers.



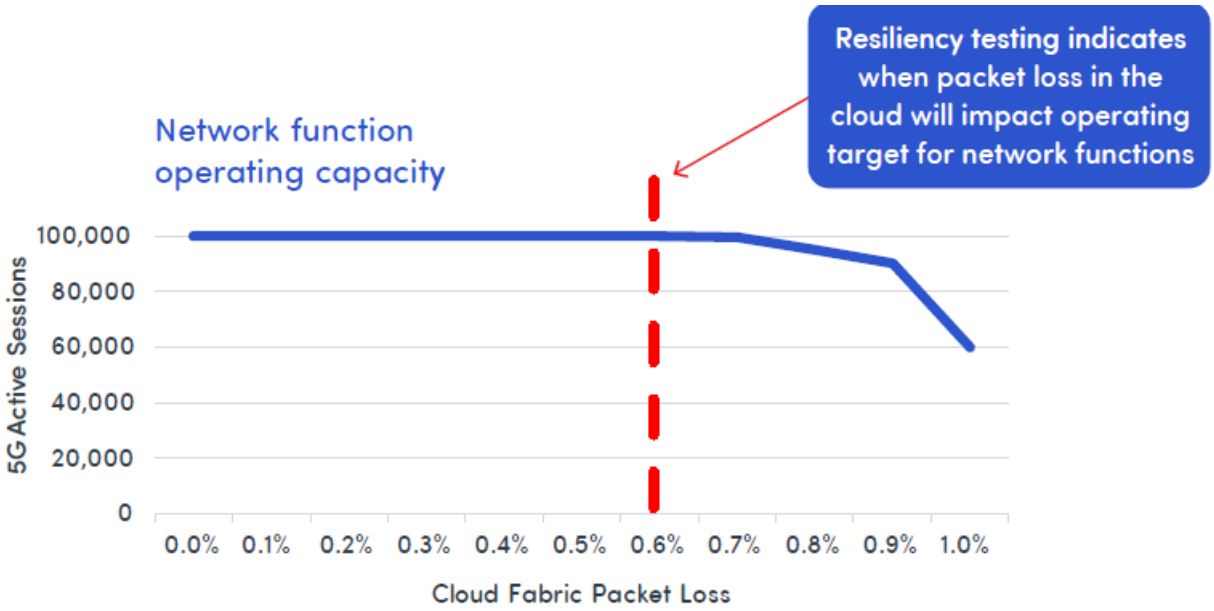
Simulating real-world cloud conditions for system-level visibility

How CNF resiliency testing addresses cloud-native challenges

- The dynamic and virtual nature of cloud-native means a given user activity may not lead to the same performance result or failure every time. So it is important to test each scenario (and intentionally create errors) multiple times to determine statistically meaningful error probabilities, causes, and their impact on customer service. This requires comprehensive resiliency testing under real-world traffic and challenges, not just ideal conditions.
- Some failures may impact individuals, while others bring down a large network footprint. 5G CNF pre-production resiliency testing determines which failure modes have the greatest impact on 5G services. Knowledge of failure impact is essential for pre-production fix prioritization as well as for production network troubleshooting.
- Since these are all software-based, nondeterministic systems, a CNF's behavior will change from one release

to the next. Resiliency testing needs to be performed for all system changes, including new CNF releases or updates to software configurations, hardware elements, or system designs.

Pre-production CNF resiliency testing entails:
Statistically significant fault insertions to map problems and symptoms and identify key performance indicators (KPIs) to be monitored for each CNF, and key failure indicators (KFIs) of a coming failure.



Using resiliency testing to determine 5G KPIs

- Thoroughly testing each 5G CNF to characterize the performance it needs across every cloud dimension (e.g., CPU, storage, etc.). These results should be shared between application and cloud teams.
- Proactively evaluating and measuring performance dependencies between CNFs and the cloud-native infrastructure, and the impact on service performance.
- Mapping that data to specific cloud configurations to provide critical context for troubleshooting.
- Providing insights to speed root cause analysis if issues surface in production.

How CNF resiliency testing supports production

- Pre-production CNF resiliency testing also plays a critical role in production network monitoring and troubleshooting by giving service providers the root cause probabilities of outages and impact on 5G services. This enables resolution prioritization based on subscriber impact, and rapid troubleshooting and remediation.
- Testing a CNF's dependency on the underlying cloud infrastructure in pre-production gives the service provider a statistical map where parameters indicate likely failure scenarios for that CNF, so they can be monitored proactively in the production network.

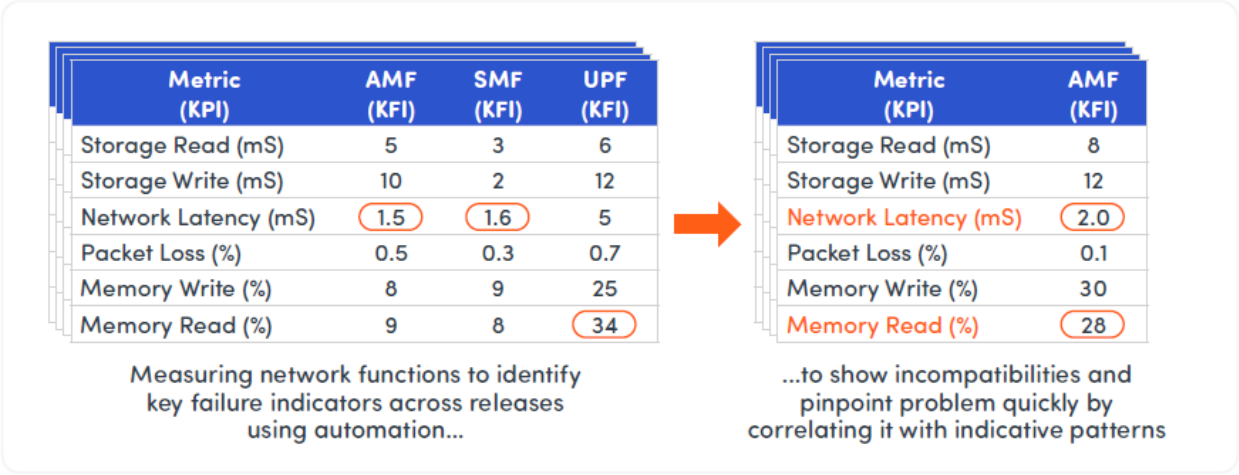
Scenario (Cloud infrastructure packet loss within namespace)	Registrations (1000 UEs)	Connect Times (mSec)	HTTP Traffic (Mbps)
Baseline – 0% loss	**100%**	**13**	**90.0**
1% loss	100%	2,000	10.0
3% loss	100%	25,000	5.0
5% loss	53%	13,000	0.5

Characterizing failure patterns for efficient monitoring

- Every CNF modification needs to be retested in pre-production, with cause and effect statistics updated before releasing the CNF into the production network.
- Pre-production CNF resiliency testing has a clear impact on a service provider's organization, involving collaboration between CNF/app and cloud teams, as well as between lab and production teams.

Outcomes from CNF resiliency testing

- CNF resiliency testing provides a framework for service providers to expand gross margins, including growing average revenue per account, by rolling out new services quickly and reliably.
- Using resiliency testing automation, results, and insights reduces the number of production network issues, thus improving customer satisfaction and significantly reducing operating expenses. Here's how:
- **Proactive, pinpointed identification of failures during CNF resiliency testing helps service providers reduce production outages by:**
  - Preventing a known broken or incompatible build from going into production.
  - Adjusting network designs to mitigate failures, such as changing cloud configurations or investing in higher performance servers for specific CNFs.
  - Having better insights for production CNF monitoring thresholds based on pre-production test results.
- Pre-production CNF resiliency testing provides holistic hard data service providers can use to quickly take action in the production network when failures or performance degradations occur. This enables:
  - Rapid mean time to fault isolation and recovery.
  - Reduced customer impact from prioritized remediation.
  - Reduction in all-hands troubleshooting by quickly pinpointing who needs to be involved in issue resolution.



Identifying key failure indicators across releases

Testing hard and soft cloud failures
Cloud failures are typically caused by hard object failures or performance (soft) degradations.

Hard (object) failure testing observes how the system responds to inserted, realistic failures and determines whether the system can automatically recover or degrade without significant impact on the overall system or service. For example, hard failure testing determines how a CNF reacts when a node fails, or how the system handles pod deletes, network links outages, or full storage. These tests are straightforward to create and simulate in the lab.

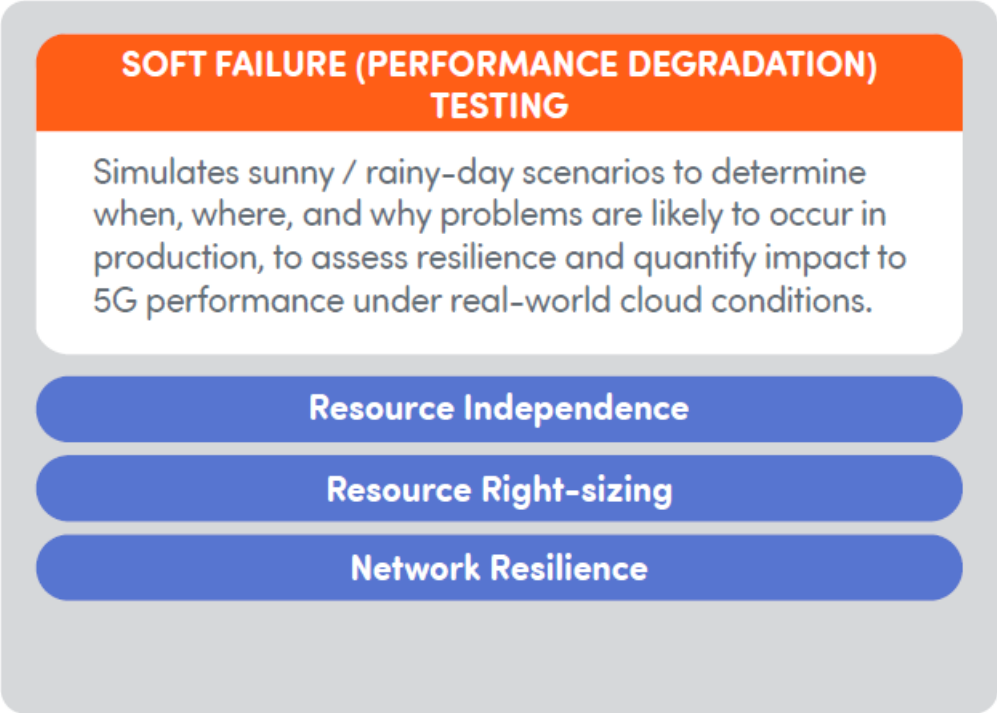
- **Hard failure resiliency testing proactively assesses:**
  - System resilience to identify potential vulnerabilities and dependencies of individual components that can lead to system-wide failures and performance degradation.
  - Fault tolerance to assess effectiveness of failure handling mechanisms, redundancy strategies, and failover procedures to ensure continuous availability of services and minimize downtime.
  - Recoverability to ensure backup systems, failover mechanisms, or replication strategies are effectively managing failed objects, ensuring smooth operations and data integrity.
  - Overall robustness to observe how the system handles errors, redistributes workload, and scales resources to compensate for failures to identify performance bottlenecks, capacity limitations, and load balancing.
- Hard failure testing proactively identifies sources of weakness, vulnerability, and errors in system architecture so necessary improvements can be made to system stability before deployment in the live network.

- Performance (soft) degradations are more complex to test and evaluate as they don't result from single, catastrophic events (e.g., "the server rebooted".) Instead, the goal of performance degradation testing is to determine the level of cloud degradation 5G CNFs can tolerate before they can no longer deliver acceptable service to users. For example, packet loss within the cloud fabric is gradually and selectively inserted into different parts of a system to simulate non-ideal but commonly occurring scenarios and determine when failover occurs or when the 5G performance result is no longer acceptable. Performance degradation testing explores how a system responds to CPU contention and its impact on application response time and overall system performance, as well as the impact of storage contention bottlenecks, memory contention, and network contention.

Degradation resiliency testing assesses:

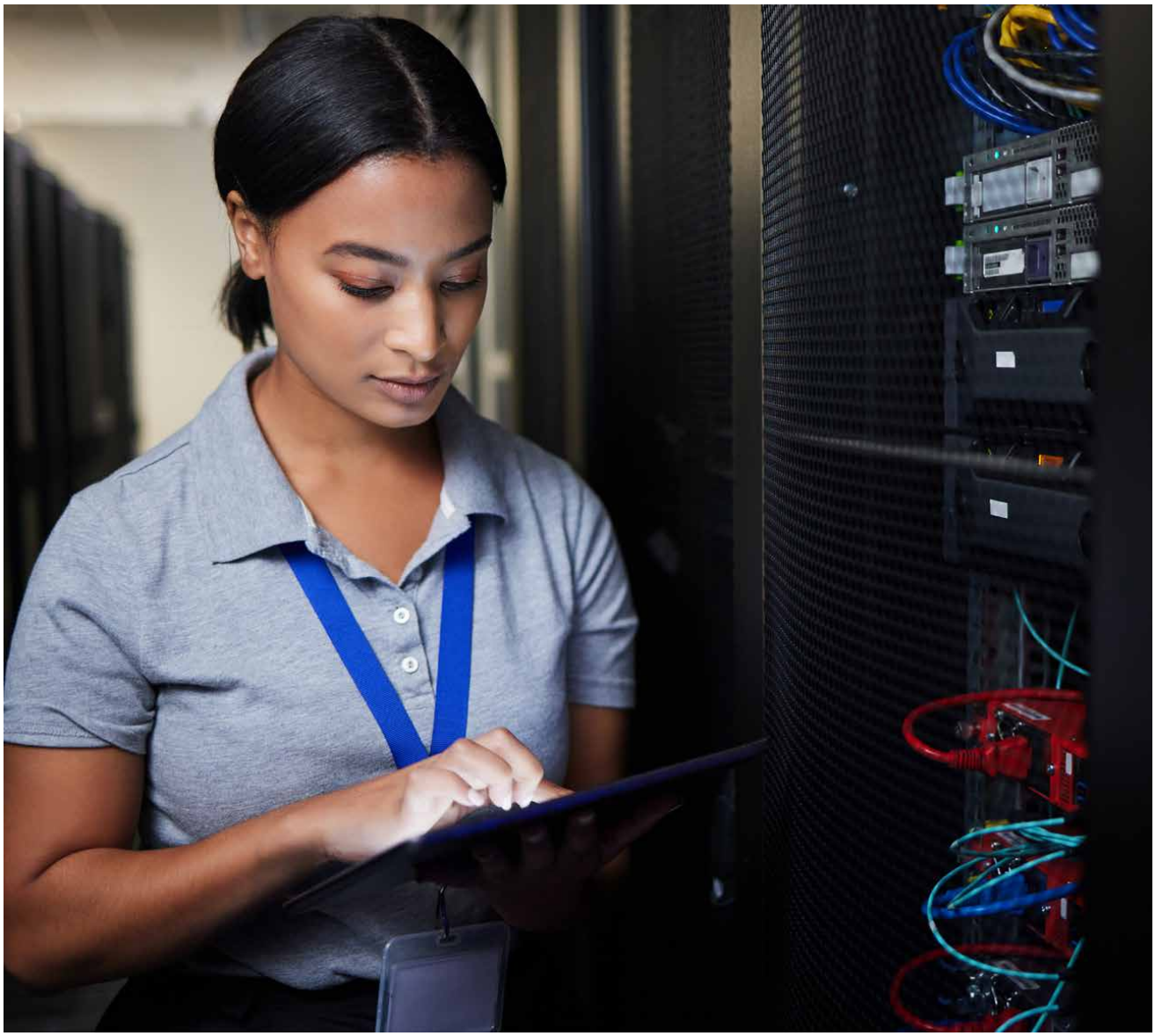
- CNF resilience to determine how well the system can maintain expected user experience as network, CPU, memory bandwidth, and storage bandwidth resources are gradually starved.
- Key Failure Indicators to determine which cloud performance metrics to monitor in production, and understand the levels at which corrective action must be taken.
- Resource requirements to determine if less expensive cloud infrastructure can be used to deliver high quality 5G services.

Performance degradation testing simulates sunny and rainy day real-world scenarios to determine when, where, and why problems are likely to occur in the production network. This testing empowers organizations with the knowledge needed to confidently deploy and troubleshoot production cloud-native networks.



The importance of automation in CNF resiliency testing

- Automation is critical for efficient, cost-effective pre-production CNF resiliency testing. Multiple hard object and soft performance test cases must be conducted to create statistically significant results for every network element, function, service dimension, and use cases.
- The result is thousands of tests for each situation. As software updates or new elements arrive, the tests must be redone and compared to prior test results to identify any changes in performance or resiliency. By running test-cases quickly, easily, and reliably, teams can identify and fix problems faster.



Automation can be used throughout resiliency testing to:

- Test the resilience of a system to a specific failure scenario. For example, a team might automate an experiment that simulates a database outage to see how the system responds to the outage and identify any potential problems.
- Test the overall reliability of a system. A team might automate a series of tests that introduce different types of failures into the system to see how the system responds to a variety of failures and identify any potential weaknesses.
- Use the historical record to identify and fix problems in a system. If a team runs an experiment and identifies a problem, they can use the automation historical record to quickly reproduce the problem and rewind to the last compatibility point to quickly pinpoint the source of the issue. This allows the team to quickly identify the party responsible to fix the issue and provides the technical context required to pinpoint the fault location and quantify a fix.

Automated pre-production CNF testing provides service providers with powerful and rapid answers that give them the confidence to deploy complex cloud-native solutions into the production network.

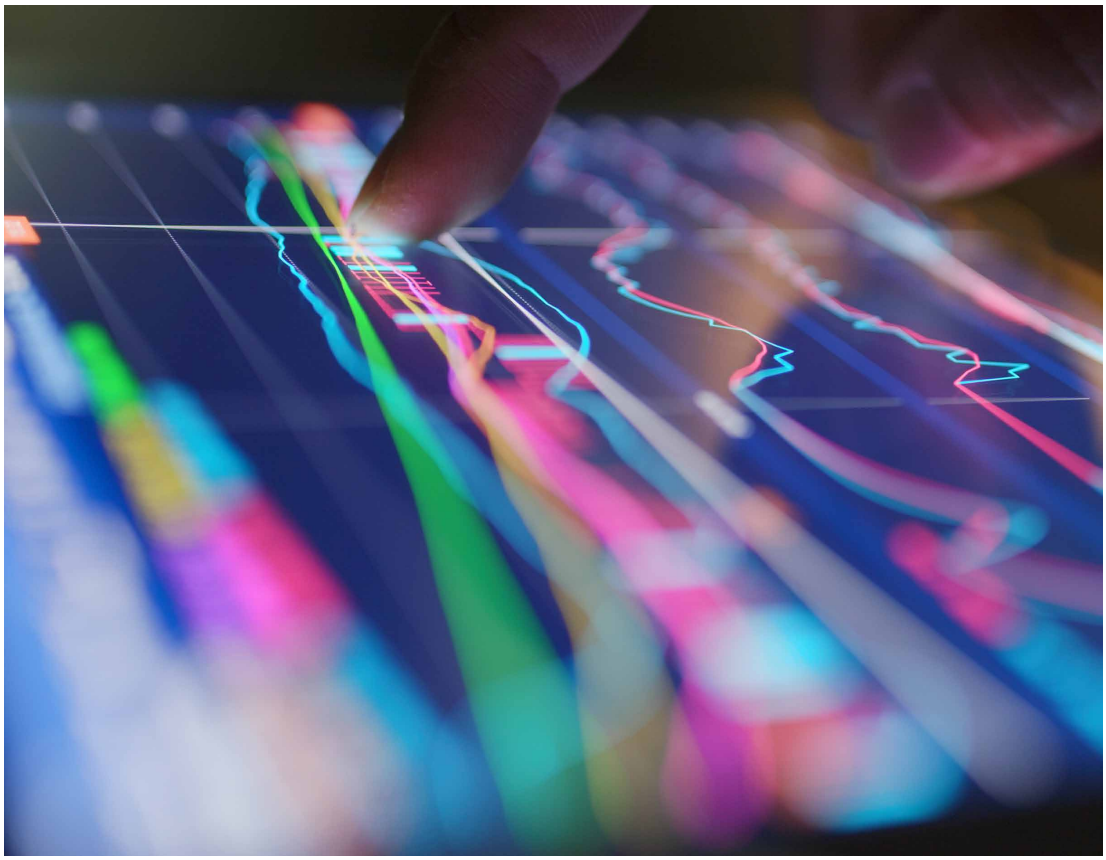
The Business Value of CNF Resiliency Testing

Although CNF resiliency testing can be complicated, it offers rich rewards to service providers, including:

- Fewer live network issues. Discover most issues during pre-production, when they're less expensive to fix, and proactively monitor for budding problems.
- Respond to issues quickly. Use test results to quickly pinpoint where and why a CNF isn't performing.
- Enable a more agile and effective business. Take full advantage of cloud-native efficiencies to reduce operating costs and unlock capital savings.
- Confidently deploy next-generation 5G services. Know that a dynamic 5G network can deliver desired service levels.

How Spirent Can Help

- Spirent has the solutions needed for CNF resiliency testing and deep expertise working with customers to pioneer new approaches. Spirent CloudSure and Spirent Landslide play key roles in ensuring the resilience and stability of 5G cloud-native applications.
- Spirent's CNF resiliency testing identifies and resolves problems before they get into the production network. Spirent's solutions focus on 5G and provide correlation from the impairment to the application layer.
- Spirent is positioned to accelerate adoption of this technology, whether through test system purchase or as a managed service.
- **CloudSure is a valuable tool for improving the reliability and resilience of 5G cloud-native applications by:**
    - Identifying and fixing potential problems before they cause costly outages or other disruptions.
    - Reducing the costs of operating 5G networks and applications.
    - Proactively testing how the system will react to unexpected change so teams can identify and fix potential problems before they cause outages or other disruptions.
    - Improving reliability and resilience of 5G networks and applications to ensure they provide a high level of service to customers, even during unexpected events.
    - Exposing systems to controlled and intentional hard failures and performance degradations, to identify vulnerabilities, and improve fault tolerance and 5G core application performance.
    - Integrating CloudSure into a CI/CD/CT pipeline to identify and remediate potential vulnerabilities in applications and infrastructure early in the development cycle.
- Spirent CloudSure builds off Spirent Landslide and enables existing Landslide customers to add CNF resiliency testing to existing test cases to gain system-level visibility into cloud-native environments. Adopting this continuous, proactive approach to 5G cloud-native validation lets communications service providers harness cloud-native efficiencies and ensure reliable 5G operations.
- Learn more about the benefits of validating the resiliency of cloud-native 5G services.



About Spirent Communications
Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled. For more information visit: **www.spirent.com**

- **Americas 1-800-SPIRENT**
  +1-800-774-7368 | **sales@spirent.com**
- **Europe and the Middle East**
  +44 (0) 1293 767979 | **emeainfo@spirent.com**
- **Asia and the Pacific**
  +86-10-8518-2539 | **salesasia@spirent.com**

Documents / Resources

	**Spirent Cloud Native 5G CNF Resiliency Testing** [pdf] User Guide Cloud Native 5G CNF Resiliency Testing, Native 5G CNF Resiliency Testing, CNF Resiliency Testing, Resiliency Testing, Testing

References

- **Automated Testing and Assurance Solutions - Spirent**
- **CloudSure – Cloud-Native Validation - Spirent**
- **User Manual**