Accelerate 5G

Applying Strategic Testing to Meet 5G's Compressed Timeline

In our companion white paper "Simplify 5G," we pointed to the growing complexity created by the transition to 5G and showed how—by integrating automation, emulation, and new test methodologies—service providers can reduce the complexity and achieve their intended business outcomes, reduce overall development costs, and shorten time-to-market.

In this paper, let's take a look at another significant impetus for adopting new testing and assurance strategies to succeed in the 5G environment: time… or the lack of it. The 5G value chain is estimated to be worth $3.5 trillion by 2035 (IHS & Qualcomm), making the evolution to 5G a high-stakes race in which the early bird gets the worm. And the window of opportunity is narrowing rapidly. As we detail below, the 5G timeline has accelerated way faster than pundits had predicted.

To make 5G possible, everything will need to evolve: the devices we use, the radio we transmit across, and the networking technologies which service us. Meanwhile, initial standards have only recently been ratified, 5G technology research is still ongoing, and early vendor systems are still proprietary.

These technological challenges only add to the urgency felt by the industry—and by entire countries thinking of their national interest—to be first to market and benefit from the new digital economies.

When such complexity meets such urgency, testing and assurance become critical in order to assure that the communications industry fulfills its promise of safely accelerating to 5G.

Be Ready

Just how quickly has the 5G timeline accelerated? Consider that the industry originally predicted commercial launches of 5G for 2020 or even later. And that the first industry standards (5G Phase 1) were released end of 2017 (3GPP R15 New Radio Non-Stand Alone). During 2017 alone, 47 lab and field trials were announced. We'll very likely see the first launches later this year and early 2019.

That's not just speculation: Verizon has announced it will be launching 5G Fixed Wireless Access (replacement for fiber to the home) in three to five U.S. markets including Los Angeles and Sacramento during 2018. AT&T has announced it will launch 5G in 12 U.S. cities by the end of 2018. And China Mobile announced the world's largest 5G trial network across five Chinese cities during 2018 along with plans to offer a full commercial 5G service by the end of 2019.

Hybrid Networks

As Verizon's plans make clear, the initial commercial applications will not be for smartphones but rather for Fixed Wireless applications and 5G mobile hotspots. Only when 5G smartphones begin to appear in early 2019 will true 5G mobility services be catalyzed. This means the first 5G networks will be hybrid, with 5G New Radio anchored to the 4G LTE Radio and Core.

Fortunately, the Core's evolutionary path allows new functions to be added to exploit the 5G New Radio until we transition to a fully standardized 5G Next Generation Core. We'll be able to add, as needed, support for:

- 5G Non-Stand Alone (NSA) New Radio with 4G/5G dual-connectivity
- Massive IoT using NB-IoT and LTE-M
- Early network slicing using DECOR (dedicated core networks)
- Control User Plane Separation (CUPS) of Core signaling and data processing nodes coupled with Multi-access Edge Computing (MEC).

MEC enables flexible network deployment and independent scaling. It also provides for flexible management of 5G traffic types. One could, for instance, distribute User Plane (data processing) nodes closer to the User to reduce data latency for enhanced mobile broadband video services, or centralize Control Plane (signal processing) nodes for signaling intensive massive IoT applications to reduce costs and optimize utilization.

Move Fast But Avoid Risk

The acceleration towards 5G dramatically compacts the gestation period for understanding, proving, and validating the new technology—and increases the risks in many spheres. Besides the potential for technological and security failures, there's significant financial risk as well. As long as the industry is still in the spending cycle for 4G, the cost of accelerating 5G requires either new capital investment or prudent capital management.

Test and Assurance can play a pivotal role in managing this duality of acceleration and cost control through a combination of intelligent automation, new test methodologies, and the use of common tool chains across the end-to-end 5G DevOps lifecycle.

Now that you're aware, ask yourself: Are you ready for 5G?

Be Agile

Communications Service Providers (CSPs) must evolve their processes for launching new 5G services to attain the speed of tech giants like Amazon and Facebook. That's not an academic suggestion. Web companies are becoming Web-scale Service Providers (WSPs) and are starting to provide unified communications. CSPs today can take months to launch a new service while WSPs exploit their cloud native architectures and their agile development cultures to release new services and iterations of services within hours and minutes. The threat to CSPs' position in the enterprise voice and messaging market should not be ignored.

With WSPs also moving towards servicing industrial verticals, the opportunity for CSPs to provide advanced enterprise communications solutions is at significant risk. True differentiation for CPSs in 5G will depend on a mix of:

- Speed to market
- Perceived quality (compared to both 4G and Web-scale Providers' services)
- Delivery of truly relevant service offerings to target industry verticals (such as automotive, logistics, industrial processing, and healthcare)

Since 5G's architectural foundations is being built on virtualization of both Radio and Core, CSPs have an opportunity to build agility into their development and operational model, adopting Web-scale principals and transforming into Digital Service Providers (DSPs). This will require CSPs to adopt a DevOps culture, apply automation across the Lifecyle, and work with vendors to embrace the principles of cloud native architectures.

Step One: Adopt a DevOps Culture

A DevOps culture or blueprint encompasses Continuous Integration (CI), Continuous Test (CT), Continuous Delivery (CD), and Continuous Change Management (CCM) capabilities with automated orchestration helping improve efficiency for rapid-paced product development and deployment. With a goal of having 75% of its network virtualized by 2020, AT&T is leading the charge towards virtualization. In order to reach its virtualization goals, AT&T reviewed its internal processes and working groups and has been implementing DevOps across the board.

Step Two: Take to the Cloud

Cloud Native computing refers to software/applications that natively utilize services and infrastructure provided by cloud computing. These small, self-contained, and loosely coupled services are fast to develop, quick to launch, and individually scalable. Leading CSPs such as Vodafone and AT&T are mandating Cloud Native architectures. AT&T was a founding member of the Cloud Native Computing Foundation (CNCF) and Vodafone has publicly demanded Cloud Native from its vendors. Are you ready for DevOps and Cloud Native? Are you ready to be agile?

Be Secure

Now you've learned why you must move quickly to be ready for 5G, and that it will take start-up-like agility to differentiate yourself and fend off players you didn't even realize were competitors. Congratulations. But you're not safe yet. Not by a long shot.

The massive increase in connected devices and pervasive use of virtualization with edge and cloud distributions will exacerbate 5G security threats and broaden the attack surface. The very things that make 5G possible—virtualization, migrating to the Cloud, Networks Slicing, IoT, and even 5G Gateways—are also potential vulnerabilities.

5G infrastructure virtualization opens up the potential for network infrastructure attacks (such as Distributed Denial of Service or DDoS) to deplete resources, expose hypervisor vulnerabilities, capture data, cascade failures, trigger overload behavior, reduce resource availability, and create performance bottlenecks.

Migrating the 5G RAN to the Cloud creates the potential for devious Man-in-the-Middle attacks as well as packet-injection attacks at distributed virtual base stations and other threats to sensitive assets that occur while messages are temporarily decrypted during context transfers.

New 5G features such as Network Slicing could be vulnerable to impersonation attacks (slice faking), denial of service, and resource exhaustion to other slices. CUPS (Control & User Plane Separation) could be vulnerable to man-in-the-middle attacks or data session hijacking when nodes are distributed to unsecure network edge locations.

Massive Machine Type Communication (IoT) could cause access network resource overload via DDoS attacks using compromised, weakly secured IoT devices.

Implementing Next Generation Fronthaul using Ethernet (i.e. eCPRI) brings known Ethernet Layer 2 attacks on VLAN, MAC, DHCP, ARP to the fore. In addition, the move to converged ethernet networking from traditional point-to-point isolation enhances the risk of a converged resource attack and rapid spreading through horizontal and vertical penetration.

5G Security Gateways, which are designed to protect the network, are a target themselves running the risk of resource exhaustion, IPSec VPN tunneling fraud, and whitelist spoofing.

See the "Elements of a Robust 5G Security Strategy" chart on page 7 for a useful list of threats and tests to mitigate them.

The security threat in the 5G network is exacerbated and the industry must be vigilant to stay ahead of this evolving threat landscape. CSPs and NEMs need to factor continuous security testing and auditing of the 5G environment into their day-to-day processes to pre-emptively identify vulnerabilities and prioritize risk mitigation

Navigate the Complexity and Grab Your 5G Opportunities Safely

5G Network Validation

Network deployment and migration to 5G will be an evolution. The industry standard body 3GPP is defining both a new 5G Radio Network (NR) and Core Network (5GC). The first release, announced in December 2017, was for 5G New Radio operating in a Non-Standalone (NSA) mode anchored to the 4G Radio and Core, where the 4G Core has feature extensions to exploit the NR. This was followed in June 2018 by the standalone (SA) scenario which includes the 5G Core.

The 5G evolution architecture is designed to enable the integration of elements of different generations, such as LTE, in different configurations with 5G. This provides CSPs with a flexible migration path as well as choice in how the network will evolve based on the use case(s) they initially wish to deliver.

To ensure a successful adoption of this new technology, carriers and equipment manufacturers alike must define an evolution strategy—from 4G extensions and 5G non-standalone to true native 5G—and ensure that the infrastructure can handle the requirements of such evolution through rigorous network testing and validation. Consider these network testing and validation procedures for your 5G launch strategy:

Scale—Validate the massive scale of 5G device connections and diverse traffic patterns to the network in parallel to current 4G traffic and perform load testing with busy hour call modeling

4G Extensions—Verify compliance of Release 14 CUPS (Control User Plane Separation) nodes (i.e. SGW-U, SGW-C, PGW-U, PGW-C) and multi-node deployment scenarios.

New Core Features—Efficiently prototype network slicing based on services requirements and verify correct slice traffic routing and performance.

New Radio—Test dual-RAN access against different EPCs and network slices. Analyze RAN performance and handoff based on service quality requirements.

Backhaul Requirements—Utilize test emulation to design backhaul size and connectivity to support 5G demands.

Shared Networks—Characterize traffic prioritization and resources management policies for 5G in shared networks.

Network Distribution—Design automated procedures for network function distribution including Multi-access Edge Computing (MEC).

Integration and interoperability—Perform progressive network integration and interoperability of the new 5G nodes validating their functions, interworking and service chains.

DevOps Continuous Testing

To accelerate towards 5G, the industry needs a new approach to testing and assurance that breaks down the traditional process and department silos. Development and operations teams need a unified and automated set of tool chains, methodologies, and metrics that allows them to adopt streamlined DevOps Continuous Testing (CT) practices to improve efficiency, enable more releases (faster time to market), get better utilization of resources, and proactively address quality issues.

While development teams seek speed and agility and operations groups strive for stability, the risks of deploying incorrectly carry significant risk. Therefore, there can be no continuous delivery without Continuous Testing, and Continuous Testing depends on automation across the end-to-end service lifecycle though network validation, service testing, and operational assurance workflows is a key element of DevOps Continuous Testing. Harmonizing the test tools and methodologies allows the same approach used, for example, to benchmark and validate 5G NFV infrastructure (NFVi) in the lab to be used to isolate issues and measure the health of the 5G Cloud infrastructure as part of operational assurance activities.

Similarly, analytics developed and refined for operational assurance needs can be used to recreate issues and identify fixes or improvements to network functions in lab and pre-production environments. Consequently, key tenets of a successful DevOps Continuous Testing practice for 5G include:

Common Tooling:

- Test instruments and active test agents, which can be used simultaneously across the 5G lab, pre- and post-production networks
- Test cases, micro-services which provide the breadth of 5G tests to be used by the test instruments/agents across each stage of the lifecycle and can be intelligently chained together to create new test paradigms
- Test authoring to accelerate the creation of new test functions that allow non-developers to rapidly integrate new tests that can be seamlessly moved between lab and production environments
- Test library that provides a unified collection of test functions/cases from an open ecosystem of providers
- Test emulation of network functions, services and traffic mixes/loads, for simple, repeatable, and predictable testing of real-world network conditions

Common Control:

- Test and Service Assurance orchestration, highly scalable and elastic cloud-native software for provisioning and control of millions of test instruments, agents and cases. Integrates via simple interfaces to MANO and OSS functions.
- Test automation, intelligent policy driven, or intent driven automation of testing managed by Test & Service Assurance orchestration to enable Continuous Testing
- Open Interfaces, industry standard APIs allowing flexible integration

Common Analytics:

- Actionable intelligence, which transforms network and test result data into actionable insights providing end-to-end quality and performance visibility, contextual awareness and predictive and prescriptive analytics to enable closed-loop, zero-touch automation of workflows

Assuring 5G Cybersecurity

With increasingly sophisticated security threats and a broadened attack surface in 5G, threat prevention solutions must perform advanced security functions under constantly rising and increasingly complex user traffic. A robust security testing strategy would:

Test your networks security to reflect real-world conditions. This includes new 5G Networks and nodes, their distributions, new devices and applications, traffic mixes, new security gateways and firewalls performance, new cryptographic performance, and known and mutated malicious threats.

Perform stress tests that emulate the brute force attacks which hackers use such as Distributed Denial of Service (DDoS).

Test now, test tomorrow, and keep testing because hackers are not easily deterred even when blocked by Firewall or Security Gateways. Their threats continuously mutate.

Prioritize with the knowledge that Cybersecurity is a zero-sum game. You must understand the risks and prioritize where to mitigate and where to invest.

Find and fix vulnerabilities quickly so you don't leave vulnerabilities open.

Elements of a Robust 5G Security Strategy

Test	Type of Automation	Opportunities
Fuzz testing (fuzzing)	Involves inputting massive amounts of random data, called fuzz, to the test subject in an attempt to make it crash.	Allows you to uncover previously undetected bugs and compromises while hardening your solution against random data.
Mutation-based Fuzzing	Continuously modify or mutate the input seeds	Create new and smarter attack inputs.
Distributed Denial of Service (DDoS) attack	An attempt to make a service unavailable by overwhelming it with illegitimate traffic from multiple sources.	Validate your DDoS mitigation strategy at scale by emulating massive line-rate attacks generating tens of million packets per second. Test to confirm legitimate user traffic is not inadvertently impacted by your DDoS protection.
Man-in-the-middle	An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Exploits a weakness in Cryptography (encryption).	Test the robustness of encryption technologies such as TLS (Transport Level Security). Especially important since 5G Cloud RAN and MEC distributions are the most vulnerable to Man-in-the-Middle attacks.
Malware, short for malicious software	Intentionally designed to be introduced/ implanted onto a system to cause damage.	In the 5G network Firewalls and Security Gateways will be the main line of defence. To robustly test these systems, we generate real malware payloads and emulate network traffic from already-infected systems.
Performance	Overwhelming a system to cause damage or to create a new attack opening is a standard practice for attackers.	Test how systems handle under both real-world conditions and when pushed beyond their designed limits.
Vulnerability Scanning	An inspection of the potential points of exploit on a computer or network to identify security holes.	Detects and classifies system weaknesses.
Penetration Testing	Also known as a **pen test**. An authorized simulated attack on a computer system, performed to evaluate the security of 5G infrastructure by safely trying to exploit vulnerabilities.	Identifies both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

Be Ready, Be Agile, and Be Secure as You Accelerate to 5G

It may be only slightly hyperbolic to claim that by facilitating the move from personal communication to General Purpose technology servicing the digital landscape, 5G may herald the biggest opportunity since the Industrial Revolution. The industry, led by 3GPP, is pressing the pedal to the floor to develop standards, and service providers and enterprises are turbocharging their trials and rollouts so they can deliver 5G benefits to their customers.

Transitioning to 5G is already a complex business. Operators will need to run the gantlet of hybrid networks and virtualization on their way to the 5G future. And if the technical and economic obstacles aren't enough, ordinary glitches and malevolent actors are just waiting to pounce on your network's and device's slightest weakness.

Accelerate 5G

Applying Strategic Testing to Meet 5G's Compressed Timeline

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

Don't let complexity delay your progress to 5G. A thoughtful and practical testing strategy of 5G Network Validation, DevOps Continuous Testing, and 5G Cybersecurity testing will enable you to be ready to assume market leadership, to have the agility to deliver new and differentiated services, and to accelerate your journey to 5G with safety, privacy, and trust.

Spirent is a world leader in 5G Test and Assurance with end-to-end expertise and solutions to automate and harmonize test and validation across the lifecycle. We're ready to work with you every step of the way to develop the right testing strategy for your and your customers' needs.

You promise your customers to make 5G a transformative reality. Spirent is here to assure you succeed.

Spirent.
Promise. Assured.

Savings Achieved by Our Customers

Network Validation: 10x faster releases, upgrades and turn-ups

DevOps Continuous Testing: 85% reduction in release and deployment cycles bringing systems and services to market faster

spirent™
Promise. Assured.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev A | 08/18