L3HARRIS™
FAST. FORWARD.

Technology Advancements at the Speed of Safety

Paul Groppel
Sean Bowden

TABLE OF CONTENTS

LIST OF FIGURES

Technology Enhancements at the Speed of Safety

INTRODUCTION:

Safety and innovation are two core components to any industry. While technical innovation can enhance growth and create new opportunities, safety must always be considered when adapting to any environment, especially critical infrastructure. If not integrated at the right level of maturity, major impacts can happen to the industries which said technologies are being implemented.

When the Federal Aviation Administration (FAA) was first established, it was chartered to "provide for the promotion of civil aviation in such manner as to best foster its development and safety, and to provide for safe and efficient use of the airspace by both civil and military aircraft, and for other purposes". This led to the creation of the National Airspace System (NAS) and the establishment of a safe and efficient airspace environment for civil, commercial, and military aviation. Over time, the NAS has become a critical component of the FAA's mission to provide safety and efficiency in aviation operations. In 2013, the President signed Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience which defined the 16 Critical Infrastructure sectors for the United States.

With aviation considered as a critical infrastructure component in the United States, safety is an essential driver behind technology decisions that impact the NAS. As a result, some FAA solutions may take longer to integrate into the system when compared to other industries. However, as technologies mature, they present added efficiencies that the FAA can leverage to enhance air operations while providing a secure infrastructure to support air operations.

Careful Technology Adoption

Body Over the past fifteen years, the NAS infrastructure has evolved to incorporate a broad host of communication technologies to increase efficiency and meet safety standards. Some examples of these technologies include dense wavelength division multiplexing (DWDM) over fiber, cellular wireless, SATCOM, and microwave transport. To integrate these technologies into the NAS, they were tested and approved by the FAA. In recent years, the commercial networking industry has introduced a new set of network technologies such as network function virtualization (NFV), software-defined networking (SDN), software-defined wide-area networking (SD-WAN), 5G wireless, and advanced cybersecurity capabilities. Each of these advancements shows promise but can also lead to deployment and operational questions and concerns. Most importantly, how quickly can a company or entity benefit from emerging technologies while avoiding unacceptable risk? Also known as "the speed of safety," the answer to this fundamental question is dependent on the criticality of the network accepting the risk.

The speed of safety is not just relevant to the networking industry, but has a broad context that is applicable across multiple industries. An example of this concept is when aircraft manufacturers began switching from conventional mechanical flight controls to a fly-by-wire glass cockpit architecture. This conversion to electrical signals allows flight control computers to monitor and control aspects of flight once entirely controlled by the pilot. However, the conversion came with great risk. Airbus presented at the Flight Safety Conference in 1997 that between 1982 and 1984 aircraft with an automated glass cockpit had more hull losses per departure than conventional aircraft. This changed as technology risks were mitigated over time through consistent improvements to the cockpits systems and safety mechanisms.

To illustrate this phenomenon, *Figure 1* depicts the maturity curve and postulates the type of safety curve that applies to many applications and their lifecycles. Segment M represents the maturity period, whereas Region A represents an acceptability area. Both shaded areas within the acceptability area might be acceptable to a general audience, but for a critical mission such as execution of the FAA NAS, only the second Region A area beginning below the old technology line should be considered as acceptable. If interrelated technologies are introduced the risk can be compounded. Choosing a technology with the right level of maturity will yield the best results for the user.

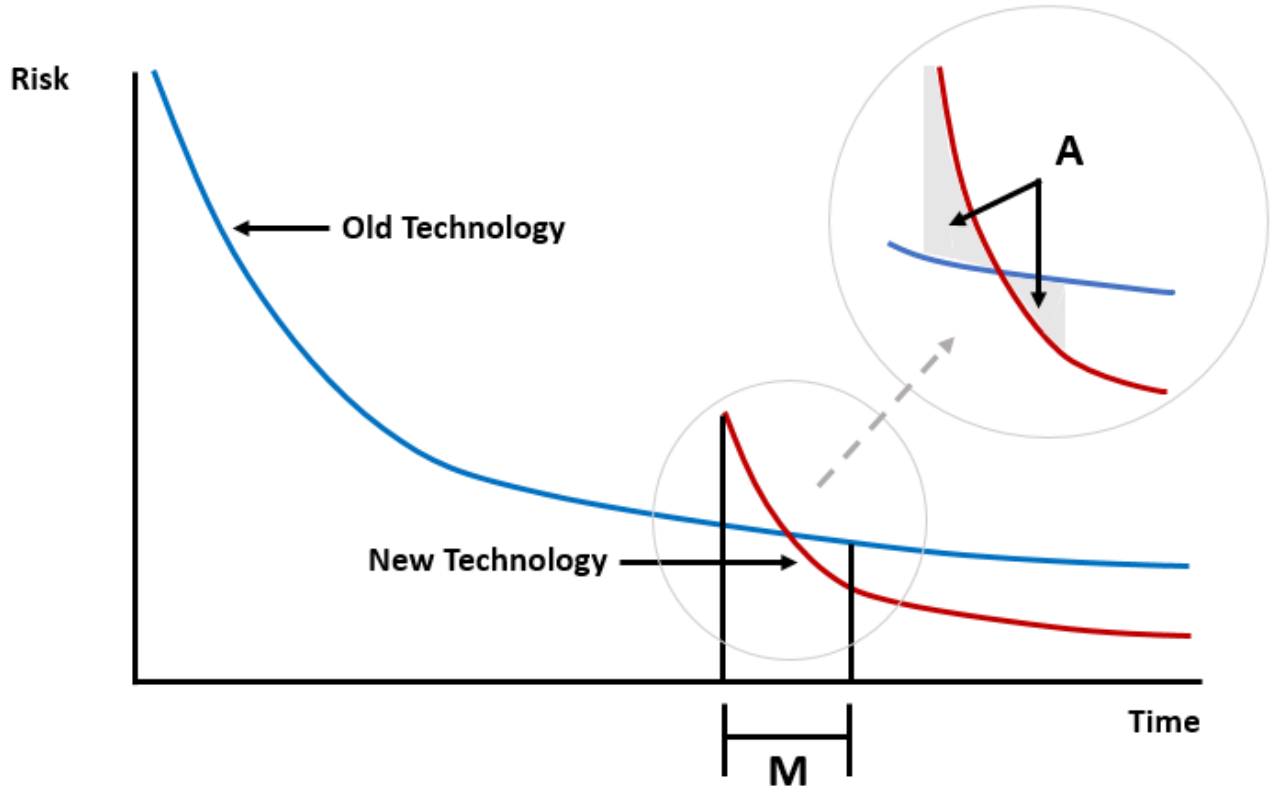


Figure 1 Maturity Curve of Technology

NFV

The impact of technology maturity on a mission-critical network can be illustrated through SDN and NFV capabilities. SDNs grew from the need to offer more network flexibility without the increased costs of operating and maintaining a large network infrastructure. Like SDN, NFV was developed to reduce costs and accelerate service development for network operators.

Where SDN decouples routing control from network devices, NFV decouples network functions from dedicated hardware and moves these functions to virtual appliances. It removes the need to purchase expensive, proprietary hardware that provides a unique function like routing, encryption, firewalls and load balancing. Instead it enables the ability to move these functions to less expensive devices that support virtualization. Virtualization reduces dependency on dedicated hardware appliances and allows for improved scalability and customization across the entire network.[1] NFV is also designed to reduce the manual effort of maintaining network devices by automating the application of standard configurations to devices. This reduces the impact of accidental misconfigurations caused by manual device management.

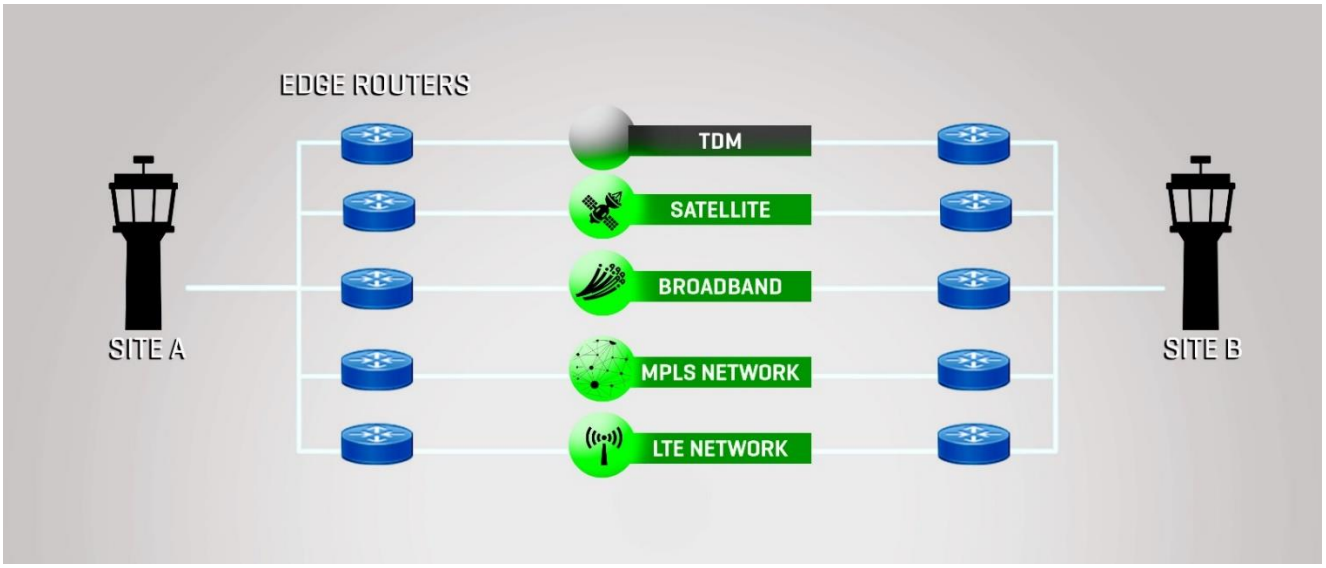
While NFV offers significant value and cost savings it also has its challenges. In traditional networks, proprietary hardware such as routers and switches are often designed as dedicated appliances with built-in failure protections or hardware configurations specifically to meet network traffic loads. In an NFV environment however, more generic components are used which may not be able to support throughput challenges. In addition, NFV software packages may contain open-source code or solutions which can add to the complexity of building a standardized and scalable infrastructure. This can lead to inconsistent architectures that can negatively impact network service offerings.

To address these challenges, organizations can leverage NFV solutions that have a standard baseline of hardware and software components that have been validated by industry and meet basic compliance standards. NFV solutions should be interoperable with legacy hardware and networking components to aide with migration efforts to the newer architecture. By building a standard component baseline, organizations can avoid complexities in managing “white box” solutions from vendors where the underlying hardware is inconsistent. This can cause connectivity issues or configuration management challenges.

Selecting vendors that offer NFV solutions that follow common government compliance requirements is a best practice. For example, many government customers require that their data be encrypted in transit. To comply with this requirement, the NFV vendor can be required to meet standards like the Federal Information Processing Standards Publication 140-2 (FIPS 140-2), Security Requirements for Cryptographic Modules. This publication has a specific set of standards for the cryptographic module on the device that is used to provide encrypted communications. The level of compliance requires evidence of evaluation and validation by government agencies and assures confidentiality and integrity of the information protected within the solution.

SD-WAN

SD-WAN is the next evolution in software-defined networking. Where SDN is designed for local area networks (LANs), SD-WAN was designed to bring NFV and SDN technologies to their maximum capabilities. SD-WAN has revolutionized how network architectures are designed, deployed, managed and secured across the WAN by removing the need for separate networks to pass different types of data. Traditionally, organizations had to use separate network architectures and paths to pass different types of data, as shown in *Figure 2*. SD-WAN devices virtually collapse these separate networks and create a single network designed to optimize application performance.



[1] *https://www.ciena.com/insights/articles/What-is-NFV-prx.html*

L3HARRIS™
FAST. FORWARD.

Figure 2: Typical TDM & IP Network Architecture

SD-WAN technologies have existed for many years, but the growth of cloud services and the rapid adoption of virtualization has shifted networking priorities. In the past, when more bandwidth or routes were needed, more devices were added to the network. As a result, networks grew larger, more complex, drove additional management resources and became expensive to operate. SD-WAN changes this model by creating network architectures optimized by dynamically selecting routes through software logic, placing a greater focus on how available bandwidth and routes are enhanced to support applications and services.

SD-WAN controllers remove the routing logic and control from individual network devices and manage all available routes to determine the best path for a service based on its performance needs. As depicted in *Figure 3*, it can include broadband (internet), a private multi-protocol label switching (MPLS) network, cellular wireless network (4G LTE or 5G), or satellite. There are some satellite communication providers who have adopted SD-WAN technologies to optimize their service offerings to customers which can add additional services to SD-WAN deployments. The SD-WAN controller, knowing the network parameters, will send data on the optimal path that meets the application performance requirements set for a specific service. The controller can use one network type or a combination of all available network paths so mission-critical industries, like air traffic services, receive the appropriate network priority to prevent communication delays or outages due to lack of bandwidth.

SD-WAN technologies are designed to enhance application performance by automating management of network resources. It removes the need to physically manage network devices independently, creating the ability to orchestrate management. The solution provisions resources by creating virtual overlays across by separating the upper stack from the lower stack of the Open Systems Interconnection (OSI) Model.

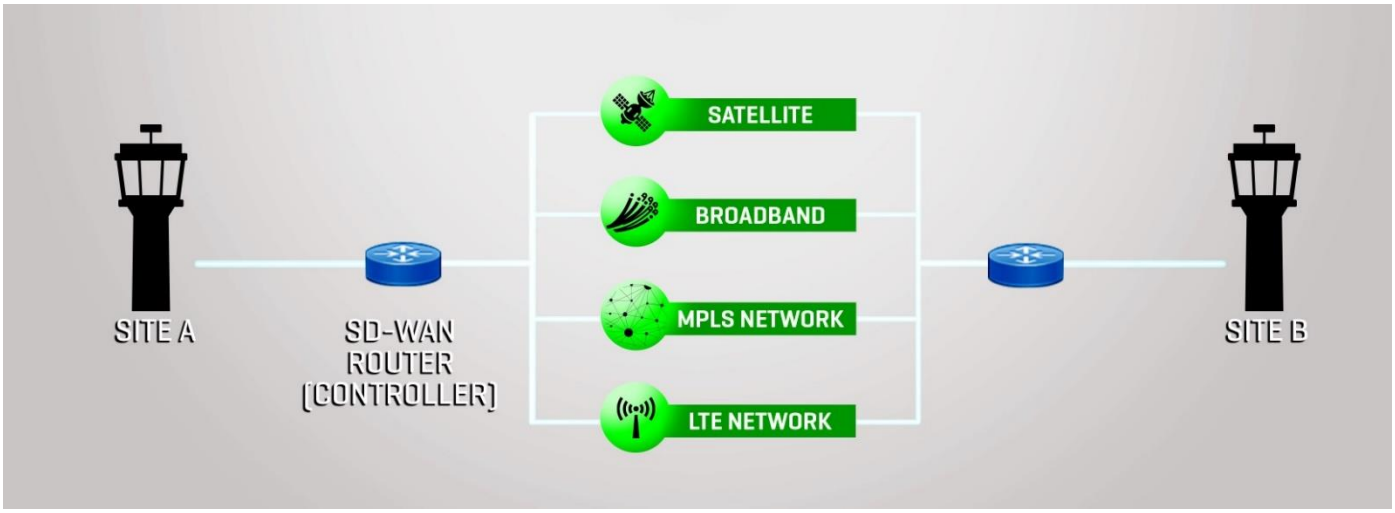


Figure 3: SD-WAN Configuration

Another recent addition to the SDN model is the idea of a Software Defined-branch (SD-branch). An SD-branch is an evolving technology that integrates SD-WAN technologies at the code level with SD-security technologies into a single device that automates network management and security protection.[2]

Although SD-WAN has many strengths it also imposes some risks to the network. For networks that rely on predetermined routes with strict path diversity and avoidance requirements, the automated changing of routes and procedures have the potential to introduce jeopardy conditions. As a precautionary measure, the orchestrator overlay should be well vetted, rigorously tested for failsafe operation, and policies should be coordinated with end users of the network. Without this added precaution, the advancements associated with SD-WAN can place the network configuration in a state that does not meet the more stringent requirements of life-critical networks.

LTE and 5G Cellular Wireless

Long Term Evolution (LTE) is the term given to the 4th generation (4G) high-speed radio technologies for cellular mobile communication systems. It has been around for many years and provides a valuable way to transmit data over airwaves. 4G enables mobile device users the ability to stream data at high speeds, which allowed the widespread adoption of mobile video streaming services. Soon 5G will be available offering even higher bandwidth and data transport options.

As a core information transportation option, 5G cellular wireless is an alternative way to establish connectivity to remote sites, which can be difficult and/or costly to reach with terrestrial telecommunications. Coupled with SD-WAN technologies, 5G cellular wireless communications can offer supplementary paths for data to aid in application performance and total network resiliency.

[2] https://www.versa-networks.com/enterprise/sd-branch/

L3HARRIS™
FAST. FORWARD.

To reduce costs, cellular wireless providers share their transport with multiple customers in the public sector. While there are efforts underway for private 5G backbones, these solutions still share resources with a limited customer set and cause challenges with prioritization. While the promise of higher bandwidth over the airwaves sounds like a great option for data paths, limiting the use of cellular wireless to non-critical services is a prudent approach. LTE has latency and jitter issues which is problematic when critical services may require extremely low tolerances to both. Leveraging SD-WAN can aid in boosting network and application performance to minimize these impacts.

Figure 4: LTE Evolution

Another challenge to consider when looking to adopt an LTE network is that cellular data is exposed to cyber threats. They can be directed towards exploiting or impacting radio frequency (RF) communication paths. A denial of service of wireless devices and networks is also possible. Saturating the device with RF noise, or jamming, could severely degrade a RF signal and in some cases, cause a device to shut down. In this example, technologies like SD-WAN are configured to recognize communication path interruptions and can often re-route traffic seamlessly and avoid the impacted link.

For commercial use, LTE might be a viable access solution to reach the masses and provide voice and data services, but for life-critical applications, like air traffic management, it may not be a suitable solution. Commercial networks are built on the premise of “best-effort” delivery which directly introduces delays and varied latencies often impacting applications that are unforgiving towards network changes. Prioritization can alleviate congestion, but it cannot resolve oversubscription. Traffic can be re-routed around failure points, but it might come at a price of added latency. With the accelerated deployments of 5G networks, wireless might start to be a viable redundant path option for life-critical services since it provides ultra-reliable, low-latency, secure connections for data transmissions.

Security

In the past, life-critical networks were isolated or segmented from public network traffic. This separation mitigated many common threats from exploiting the network. Time division multiplexing (TDM) leverages unique communication technologies which cannot comingle with newer internet protocol (IP) solutions and limits exposure of TDM data to common threats that impact IP networks. Unfortunately, TDM is now a legacy communication medium that is being phased out by vendors. Technologies like voice over Internet Protocol (VoIP) are replacing older TDM solutions to take advantage of lower cost IP network transports and eliminate the need for separate infrastructures. In doing this, critical communication systems are exposed to a large volume of cyberattacks that threaten IP-based networks daily across industries.

Critical infrastructures present a high-value target for both nation-state actors and hacker groups and additional safeguards are needed to defend life-critical data, systems, and networks from cyberattacks.

One of the largest threats to critical networks is a denial of service (DoS), or distributed denial of service (DDoS). Malicious actors often use DDoS attacks to flood a network endpoint with data packets using various techniques to prevent access to services or render the endpoint useless. They can paralyze an organization by causing network, server, and application downtime and/or service degradation which leads to major impacts to critical services.

Another challenge for critical networks is an insider threat, also known as the human error factor. Insider threat is often thought of as malicious but can often be accidental. While organizations can standardize methods and procedures for taking actions on network devices or systems, mistakes can happen. However, recent advancements in automation and orchestration for network and security devices have helped minimize human error impacts. Technologies like SD-WAN are designed to limit the amount of human interaction with devices and build in standardized configurations that can be tested prior to being deployed across the network. SD-WAN also offers built-in security functions like firewalls and intrusion detection and prevention systems (IDPS) that can further mitigate threats to the network and offer a single control platform to manage network security configurations.

While new technologies offer a multitude of benefits to protecting critical systems from cyberattacks, care must be taken on how these technologies are implemented across the network. Integrating new solutions and protections into a known baseline can initially cause negative and disruptive impacts to services and communications. A transitional period, typically based on the criticality and complexity of the network, must be part of the risk mitigation process and allows the network to be appropriately monitored and adjusted. While these challenges will decrease over time, it is important to consider these initial deployment challenges that could cause operational impacts.

Conclusion

Technology advancements are constantly changing how organizations operate and offer more efficient services that have created new ways to engage customers. However, this rapidly changing environment can come with great risk to those organizations that provide mission-critical services over infrastructures that require stability and security.

The FAA’s mission to provide the safest and most efficient airspace in the world must be done with careful consideration. As new technologies evolve and mature, it is important that the FAA carefully evaluate the technical improvements offered against the associated risk being introduced and the potential operational impact of accepting that level of risk.

Adopting new technologies and integrating them into safety critical, or even efficiency critical environments can pose their own risks. SD-WAN, NFV, 5G LTE and advanced security capabilities, require balancing risk against innovation to allow them the ability to provide safe and efficient air operations. By moving at the speed of safety industry can effectively integrate new, mature technologies and foster continued growth across the entire NAS.

L3HARRIS™
FAST. FORWARD.

L3HARRIS™
FAST. FORWARD.