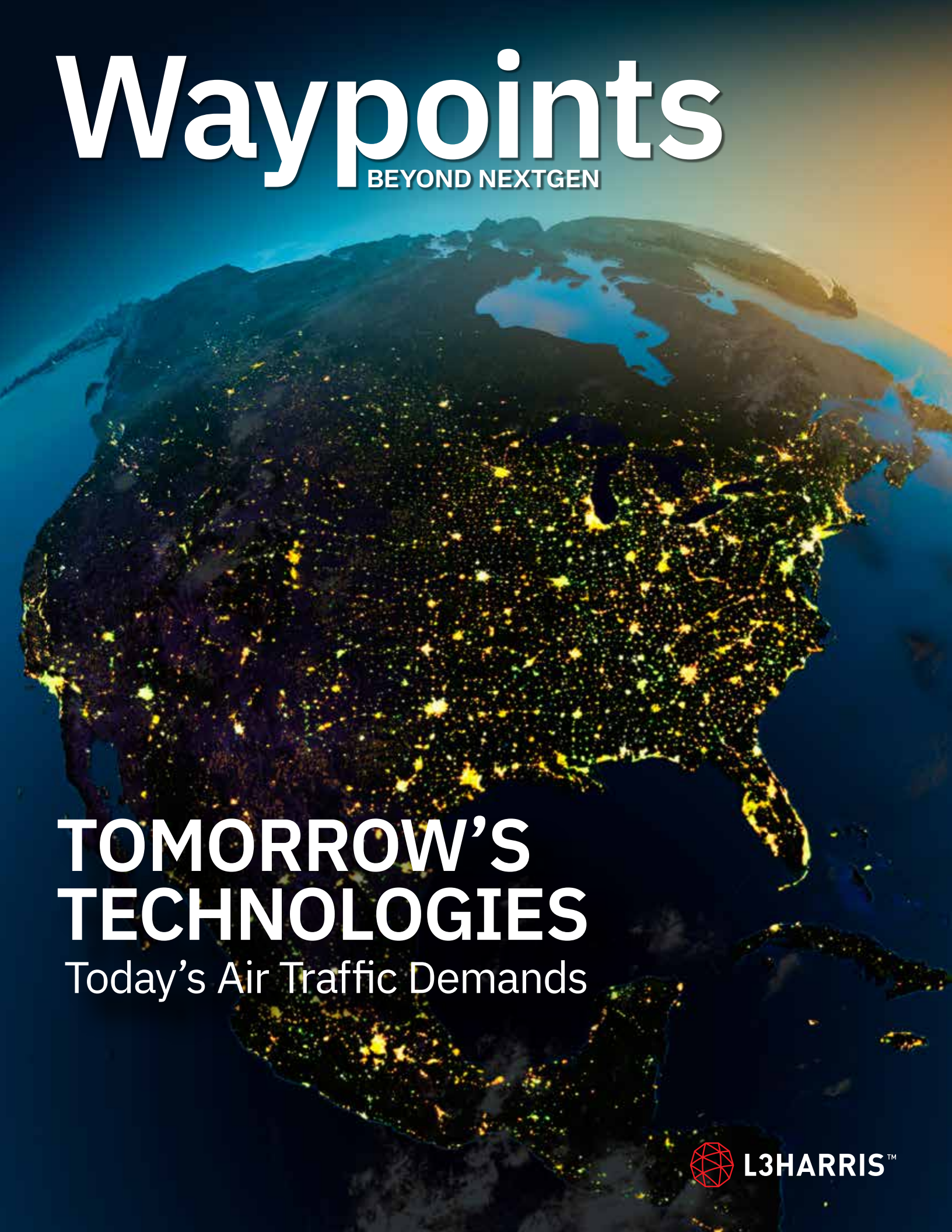
Waypoints

BEYOND NEXTGEN



TOMORROW'S TECHNOLOGIES

Today's Air Traffic Demands

L3HARRIS™

Waypoints
BEYOND NEXTGEN

Features:

L3HARRIS™
FAST. FORWARD.

AS COMPLEXITY CONTINUES TO GROW IN THE NAS, WE MUST RISE TO THE CHALLENGE AND CONTINUE TO DELIVER OPERATIONAL EXCELLENCE WHILE MAINTAINING THE SAFEST AIRSPACE IN THE WORLD.

[EXECUTIVE NOTE]

CONTINUING EXCELLENCE IN AIR TRAFFIC MANAGEMENT

Our National Airspace System (NAS) is transforming at an unprecedented rate. Continuous growth in air transportation coupled with uncertainties involving weather frequently results in less predictable airspace performance. As complexity continues to grow in the NAS, we must rise to the challenge and continue to deliver operational excellence while maintaining the safest airspace in the world.

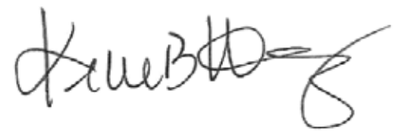
L3Harris sees a new horizon for air traffic technologies and we are positioned to play a big part. The organization continues to support the Federal Aviation Administration (FAA) with multiple NAS critical infrastructure programs in data communications, surveillance and information management. We are also engaged in the continuous technical evolution of the world's largest, safest air traffic telecommunications network known as the FAA Telecommunications Infrastructure (FTI), by investing in new technologies and solutions that will continue the seamless operational insight and excellence across all those capabilities. Finally, we have recently added new avionics capabilities to our commercial aviation portfolio that will dramatically extend air traffic surveillance needed for more efficient advanced procedures in all phases of flight.

2018 came and passed with new and different challenges to our Nation's airspace and L3Harris met them head on. The year ended without seeing an increase in delays despite the combination of increased air traffic and major weather events. One of the major contributors to keeping delays from growing was Data Communications (Data Comm), an L3Harris led FAA program deployed at 62 airports across the NAS that enables controllers and pilots to communicate more effectively with loadable route clearances. In fact, since its launch 2.5 years ahead of schedule in 2017, the program has prevented tens of thousands of communication errors, saved millions of minutes in delays, and reduced CO_2 emissions.

Not only was operational excellence achieved, but new technologies continue to be qualified and integrated into the NAS both safely and efficiently. FTI, the critical conduit to over 150 NAS systems and applications, reached another major milestone by delivering over 100,000 safe system upgrades encompassing over 4,000 FAA and partner facilities. This signifies a decades-long partnership between the agency and industry dedicated to delivering new, reliable and mission critical services safely, while providing the network scalability required to outpace the future of air travel.

Looking ahead, L3Harris is building key surveillance technologies to further enhance the NAS. Our team has expanded beyond traditional air traffic infrastructure and into the cockpit with Automatic Dependent Surveillance – Broadcast (ADS-B) In and ADS-B Out as well as Unmanned Aircraft Systems (UAS) infrastructure development. When we couple these developments with our new cloud-based System Wide Information Management capabilities, we can offer ever more efficient services for the NAS.

The road ahead provides new, exciting challenges for our Nation's airspace. As industry providers, we must remain in the forefront to deliver the gold-standard of safety and execution integrity that the FAA and their partners are known for across the globe.



Kelle Wendling
Vice President & General Manager, Mission Networks

“Together, FAA and L3Harris are developing technologies at the speed of safety to meet tomorrow’s operational demands.”

DELIVERING AIRPORT OPERATIONAL EXCELLENCE

Data Comm saves FAA and passengers millions of dollars in delays

2.8 million passengers fly in and out of airports in the United States every day. With passenger demand growing constantly, the Federal Aviation Administration (FAA) and their partners must evolve by continually making operational improvements.

Data Communications (Data Comm), a FAA NextGen initiative developed in partnership with L3Harris, provides Controller Pilot Data Link Communications (CPDLC) between air traffic controllers and pilots so they can more efficiently and safely transmit clearances, advisories, flight crew requests, and other essential messages with the touch of a button. Data Comm helped the FAA deliver operational benefits by avoiding air traffic delays in 2018. Despite an increase in bad weather and air traffic between 2017 and 2018, average delays remained flat thanks in part to this NextGen solution.

Deployed at 62 towers across the United States, Data Comm reduces the need for voice communications during pre-departure operations. This saves time on the runway, shortening delays, lowering carbon emissions and reducing errors during peak departure clearance periods. During the year, over 500,000 minutes of delays were saved, more than 600,000 minutes of communications time were saved and 4.7 million kilograms of CO2 emissions were prevented.

Data Comm is constantly saving time and fuel for the aviation industry by streamlining pilot and controller processes. Not only does the solution help with passenger movements, but it is being used for the transportation of freight.

“I have easily seen Data Comm save me 7 to 15 minutes in getting a clearance for takeoff. For UPS, we really have a time-critical sort,” said a UPS pilot. “Every minute I’m delayed could affect the transfer of packages onto 40 aircraft waiting in Louisville.”

With the ability to send clearances over text instead of voice communications, read-back hear-back errors are more easily avoided. Operators can more effectively focus during peak airport hours.

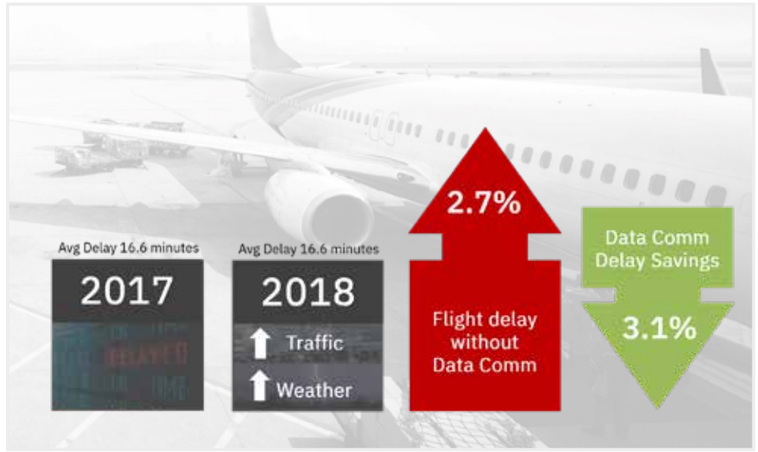
“I’ve had several experiences where the controller has to issue a Full Route Clearance, when I point out that the aircraft is CPDLC they immediately breathe a sigh of relief.” Said a controller at George Bush Intercontinental Airport in Houston, Texas. “(Received) a reroute, controller sent the clearance via CPDLC and 3 minutes later they were rolling down the runway. That would have been at least 10-20 min traditionally; if they needed more fuel, (it would have been) up to an hour.”

With air traffic complexity and weather continuing to evolve, FAA and L3Harris stand ready to deliver even greater operational excellence to U.S. and global airspace. Data Comm is transitioning into en route operations to further reduce delays related to weather and congestion. By allowing controllers to send messages directly to pilots en route, United States airspace will continue to be the safest, most efficient in the world.

Together, FAA and L3Harris are developing technologies at the speed of safety to meet tomorrow’s operational demands. ■

2018 DATA COMM DELAY SAVINGS IMPACT

Average delay remained flat despite increased weather and traffic – Data Comm benefits offset operational impacts



AIR TRAFFIC RESILIENCY MUST BE MEASURABLE

Enabling safety through resilient technologies

In May 2019, the Resorts Ballroom in Atlantic City, NJ hosted an event focused on the future of air travel. With technical co-chairs from the Federal Aviation Administration (FAA) and National Aeronautics and Space Administration (NASA), the Air Traffic Control Association (ATCA)-led event focused on the latest ideas and trends likely to impact air traffic control (ATC).

A major theme of the conference was resilience in air traffic management (ATM) systems and infrastructure. Panelists noted that the over-arching theme is comprised of key elements which include policy, process, people and technology. For any system, resilience depends on the proper construction of each of these elements and each is, in turn, dependent upon the others. For the technology element, many new technologies promise significant efficiency gains and can often achieve this through aggregation of processing, data and information management and communications. In some cases, the likelihood of a system outage might stay the same or even decrease as a result of implementing a new technology, but the impact to National Airspace Systems (NAS) operations may increase significantly. This critical balance was referenced during the conference's final panel "When Safety Meets Efficiency: Implementing New Technologies".

How can the aviation industry advance new concepts and move forward with technology implementations quickly and safely? To do so, it is crucial to begin with common terminology defined through FAA led engagements with industry.

How do you accurately define the resiliency of a system that will be integrated into or leveraged within the NAS? What about other meaningful terms such as survivability, sustainability, availability, avoidance and diversity? In many cases they are interdependent. Every word must be defined in relation to its counterparts so the aviation community can use them consistently to reduce risks to the entire system. Even a word like diversity needs further sub-definitions when being discussed in a modern network by use of pretenses like physical, electrical or logical.

The need for standardized and consistent FAA terminology is most apparent when discussing network resiliency, which is measurable through mathematical calculations and analyses based on other clear definitions.

For example, if the NAS network infrastructure is critical to operations, and a high bandwidth fiber line is accidentally cut in an Iowa cornfield, there must be "physical" diversity. This means that a separate independent line that is continuing to provide service to that area, or another available line with some measurable separation requirement is necessary, otherwise the entire system could be at risk. Likewise, if an IP storm, black hole, denial-of-service or other cyber threat is present in your network, you need an observable and measurable way to guarantee that traffic gets to its destination(s).

In 2017, the Department of Transportation Inspector General report identifying FAA top management challenges stated, "Resiliency is the ability of NAS systems, services, and facilities to be able to withstand and rapidly recover from air traffic operational capacity-impacting events." The definition provided was certainly not meant to be exhaustive, but it helps further amplify the need for exactness of terms when discussing any NAS system. Without supporting definitions and requirements, one network provider might interpret the stated ability to "withstand" as a need to propose dual independent networks. Alternatively, a second network provider might focus on the "rapidly recover" aspects and propose a singular network with more diverse circuit paths.

Is either network solution acceptable? Or, is the correct interpretation that both are necessary? The safety of the flying public demands certainty. The expectation from industry must be that any requirement set provided by the FAA has unambiguous and exhaustive definitions of all the resiliency subfactors. The definitions must include how they will be measured and how they will be used to calculate overall system resiliency. With this added clarity, the FAA and industry will jointly and confidently be better prepared to move innovations forward efficiently and safely.

Upcoming opportunities to begin to close the gaps are just ahead at key conferences such as the ATCA Annual Conference and Exhibition happening in October 2019 in Washington, D.C. But conferences alone are not inadequate. The FAA and the aviation industry must come together on a variety of topics through frequent and specifically targeted outreach events designed to establish explicit definition sets for many of the innovations discussed at the symposium. The next decade of safe air travel is upon us, and it is our collective responsibility to do it at the speed of safety. ■

> "The next decade of safe air travel is upon us, and it is our collective responsibility to do it at the speed of safety."

IMPLEMENTING WIRELESS TECHNOLOGIES **FOR AIR TRAFFIC INFRASTRUCTURE**

L3Harris deploys Aeromacs at airports across the United States

Louis Armstrong International Airport in New Orleans handles over 12 million passenger movements a year. With so many goods and passengers entering and exiting the airspace, it was essential that the airport use a cost-effective, efficient solution to securely transmit valuable air traffic information.

> “L3Harris and the FAA will continue to provide a gold standard of both security and efficiency for the flying public.”

To manage operational air traffic management (ATM) information efficiently, the Federal Aviation Administration (FAA) required a secure communication system that maintained strict performance requirements ensuring information is not lost due to bandwidth demands. In addition, the solution needed to be quick and cost-effective to implement on site.

L3Harris delivered the Aeronautical Mobile Airport Communications System (AeroMACS) to meet these demands.

AeroMACS is designed to reduce cost and implementation schedules by minimizing construction needs while meeting functional, performance and security requirements. It supports a wider range of ATM communications technology than its predecessors. AeroMACS also provides greater efficiencies like higher speeds and greater bandwidths than its predecessor, Cable Loop Communications Systems.

AeroMACS securely sends data from operational equipment located around the airfield to the ATC tower and beyond. To meet availability requirements, L3Harris AeroMACS uses redundant equipment that ensures continued operations should there be individual component failures. The solution increases information efficiencies at each location and greatly reduces unnecessary hardware costs compared to expensive terrestrial connections.

“Implementing wireless technology for our air traffic infrastructure is another step toward preparing our National Airspace System (NAS) for the next generation of air transportation,” said Kelle Wendling, Vice President and General Manager, L3Harris Mission Networks. “As we continue to develop innovative technologies, like AeroMACS, that deliver significant benefits for the NAS, we must keep safety in mind.”

After only a year, AeroMACS is operational at New Orleans and Portland airports. The system is scheduled for additional deployments at 17 airports across the United States to provide better access to surface information and track aircraft before takeoff.

As new airports come online with AeroMACS technology, L3Harris and the FAA will continue to provide a gold standard of both security and efficiency for the flying public. Wireless technology is only the beginning when it comes to safely deploying new solutions in the NAS and there are many more on the horizon. With 5G, cloud computing and other technologies coming relatively soon, the FAA will need cost-effective wireless solutions they can depend on to facilitate safer, more effective information sharing than ever before. ■

TECHNOLOGY ADVANCEMENTS AT THE SPEED OF SAFETY

Excerpts from the white paper published in the ATCA Journal of Air Traffic Control

> “By moving at the speed of safety industry can effectively integrate new, mature technologies and foster continued growth across the entire NAS.”

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.

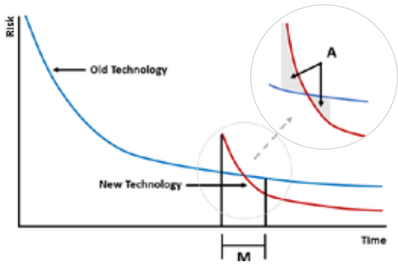
When the Federal Aviation Administration (FAA) was first established, it was chartered to “provide for the promotion of civil aviation in such manner as to best foster its development and safety, and to provide for safe and efficient use of the airspace by both civil and military aircraft, and for other 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.

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, the maturity curve (See below) 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.



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. 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.

> “Networks grew larger, more complex, drove additional management resources and became expensive to operate.”

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 a 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.

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.

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.

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 condi-

tions. 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.

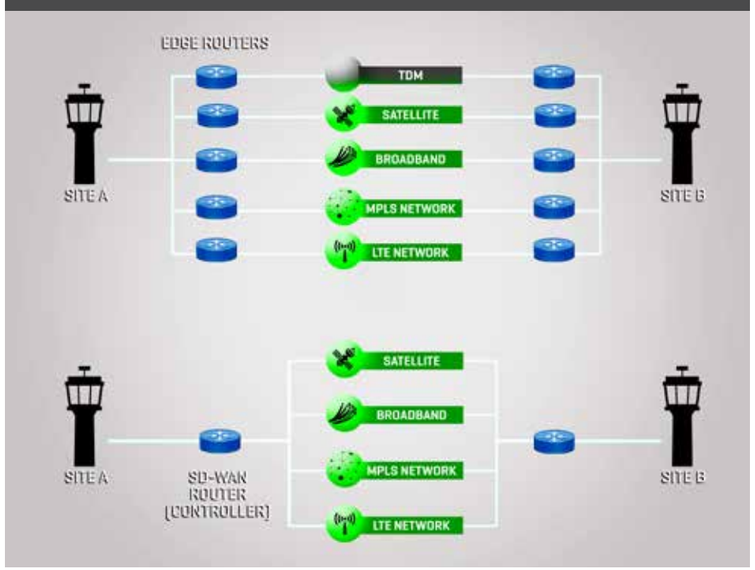
To reduce costs, cellular wireless providers share their transport with multiple customers in the public sector. While there are efforts underway for private 5G backbones, these solutions still share resources with a limited customer set and cause challenges with prioritization. While the promise of 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.

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.

A TYPICAL TDM & IP TECHNOLOGY VS. AN SD-WAN ARCHITECTURE



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.

> "Adopting new technologies and integrating them into safety critical, or even efficiency critical environments can pose their own risks."

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. ■

FAST. FORWARD.

WAYPOINTS, Beyond NextGen

L3Harris Technologies is an agile global aerospace and defense technology innovator, delivering end-to-end solutions that meet customers' mission-critical needs. The company provides advanced defense and commercial technologies across air, land, sea, space and cyber domains.

L3HARRIS™