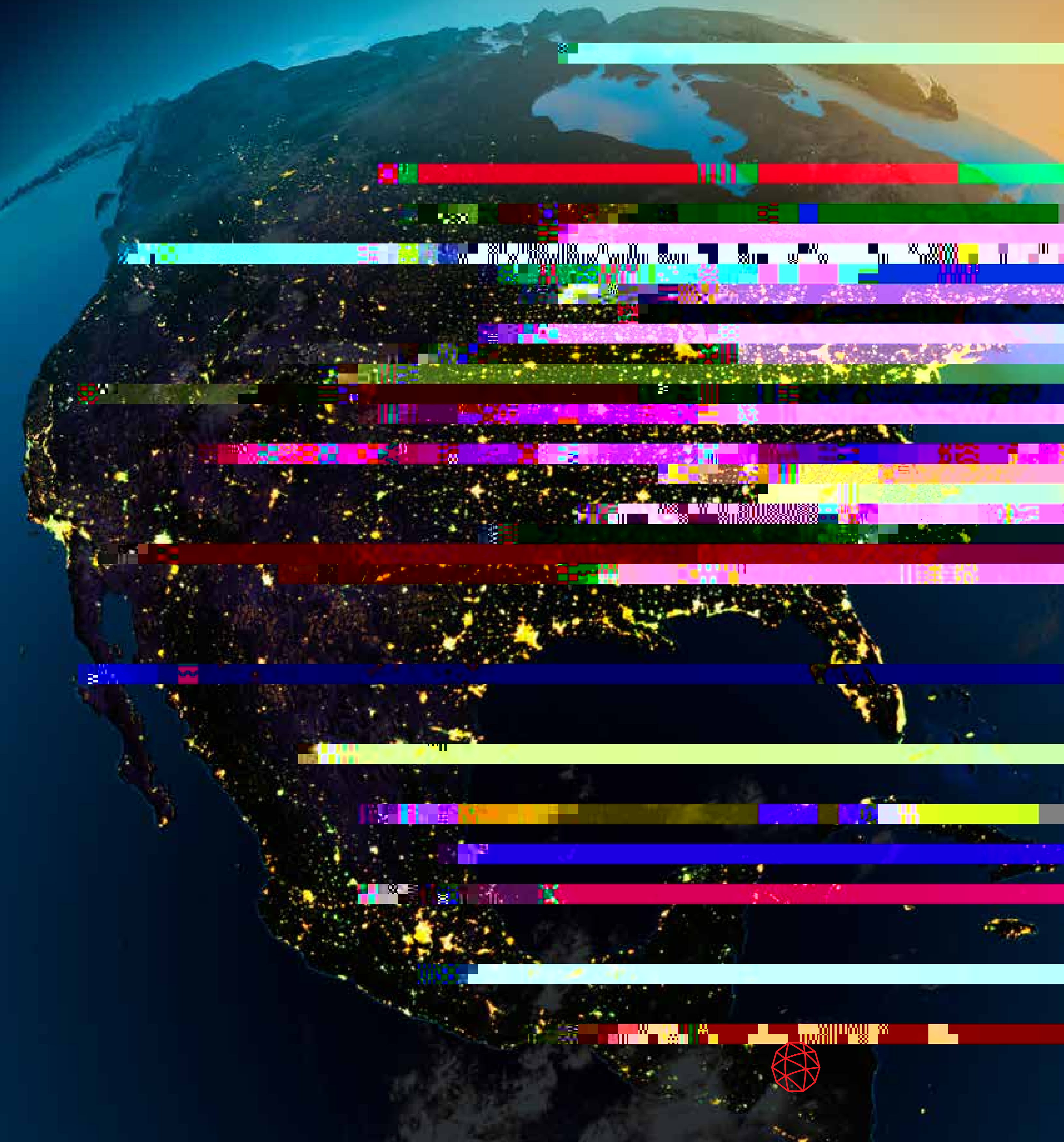
Waypoints



Waypoints

BEYOND NEXTGEN

Fea /1nD0CS0 s 0.201 0.2 0.205 sc/T1_2 1 Tf 0.006 Tc 0.016 Tw 10 0 0 10 108.472 2.

L3HARRIS™

RWARD.

Data Comm saves FAA and passengers millions of dollars in delays

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 CO_2 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.”

W( )]emg pa9 (t b-13.2 (a)Td [(c)4 (n)k)79 4end ro-2(e)-r-11.33 (e)79 4areeil “I have e cet-17.7.5 (O)

ao 4b-5.12.9 (r4 7 (e)--7.2 (e))0.8 (-4)-1.3 (-4-14.1 ((c)-10.3 (e)-4.4 (n)4.4 (t)9.7-7.2 (3 (-4-14.-3.5 (

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 de ned 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-de nitions 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 ber line is accidentally cut in an Iowa corn eld, 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 traf c gets to its destination(s).

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.

To manage operational air traf c management (ATM) information ef ciently, 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 ef ciencies like higher speeds and greater bandwidths than its predecessor, Cable Loop Communications Systems.

AeroMACS securely sends data from operational equipment located around the air eld 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 ef ciencies at each location and greatly reduces unnecessary hardware costs compared to expensive terrestrial connections.

(5 h (5 . 2) t (. 1 -) i (6 . 2) t (5 i
2 1 - r 6 1 5 r) ,) A ((9 r 0 1 T) 5 e A

“Implementing wireless technology for our air traf c 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 signi cant bene ts 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

Td [(A)-252

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 rst 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 ef cient 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 ef cient 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 ef ciency in aviation operations. In 2013, the President signed Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience which de ned the 16 Critical Infrastructure sectors for the United States.

With aviation considered as a critical infra-structure component in the United States, safety is an essential driver behind technol-ogy 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 technolo-gies mature, they present added ef ciencies that the FAA can leverage to enhance air operations while providing a secure infra-structure to support air operations.

Over the past fteen years, the NAS infrastructure has evolved to incorporate a broad host of communication technol-ogies to increase ef ciency and meet safety standards. Some examples of these technologies include dense wavelength division multiplexing (DWDM) over ber, cellular wireless, SATCOM, and microwave transport. To integrate these technolo-gies 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 technolo-gies such as network function virtualization (NFV), software-de ned networking (SDN), software-de ned wide-area networking (SD-WAN), 5G wireless, and [illegible]

NFV

The impact of technology maturity on a mission-critic al 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, rewalls 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 con gurations to devices. This reduces the impact of

Cryptographic Modules. This publication has a speci c 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 con - dentiality and integrity of the information protected within the solution.

SD-WAN

SD-WAN isthe next evolution in software-de ned 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 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