Federal Aviation Administration



FAA National Airspace System (NAS)
Operational Environment

Prepared by:
FAA Telecommunications Infrastructure (FTI)-2 Program Office, AJM-3170

Date: October 7, 2015

Table of Contents

1.0 Purpose 3
2.0 Background 3
3.0 Description of Current Environment 4
3.1 FTI Network Operations Control Center (NOCC) and FAA Coordination 4
3.2 Relationship between FAA and Its Telecommunications Service Provider 5
3.3 U.S. Critical Infrastructure Support 5
3.4 Mission Critical NAS Services 5
3.4.1 Reliability, Availability, and Maintainability (RMA) 5
3.4.2 Diversity and Survivability 6
3.4.3 Security 6
4.0 FAA Critical Challenges 6
5.0 Questions 7

1.0 Purpose

The FAA's National Airspace System (NAS) presents many unique challenges from an operational perspective. The NAS is operational 24 hours a day and 365 days a year. Outages of NAS equipment and communications can result in airline delays and have a direct impact on the flying public. This paper discusses the NAS operational environment and the working relationship between the FAA and the FTI Vendor essential to preventing and mitigating potential impacts to the provision of telecommunications services on the NAS operational network(s).

This information is intended to provide context into the daily operations of telecommunications in the NAS today. The concept of operations for the FTI-2 program has not yet been determined; therefore, the requirements, processes, and procedures (or is it "required processes and procedures") in the FAA's current operational environment may not reflect the means to be used to assure high performance NAS telecommunications in the future operational environment.

2.0 Background

The NAS is a complex system that links pilots, aircraft, airports, ground equipment, and air traffic controllers to provide a system environment to safely move airplanes across the U.S airspace. The NAS provides Air Traffic Control services to the flying public that are highly available, survivable, and involve unique equipment only found in the ATC environment. Connecting these is a complex telecommunications network provided by the FAA Telecommunications Infrastructure (FTI) contract.

Airlines for America reported that the average cost for airline delays in 2014 was up to $81.18 per minute per plane[1]. Because of that impact and inherit risk to the safety of the flying public, the FAA places a high priority on preventing outages in the NAS including telecommunication services. This necessitates that the FAA and the NAS telecommunications provider have a close working relationship that focuses on the high availability of NAS services.

One unique aspect of the NAS operational environment is the visibility that the FAA requires into the performance of the telecommunications services supporting NAS systems. Outages that cause Air Traffic Control (ATC) related aircraft delays are tracked at the national level and may have visibility at the highest levels of management both at the FAA and the vendors involved in the outage. In addition, most outages that involve significant numbers of aircraft delays attract national media attention.

---

[1] Airlines for America, "Per-Minute Cost of Delays to U.S. Airlines", Retrieved from http://airlines.org/data/per-minute-cost-of-delays-to-u-s-airlines/ (2015)

3.0 Description of Current Environment

The FAA has a number of systems and procedures that help to prevent outages and mitigate impacts when outages do occur. They include real-time monitoring systems, daily reporting, operations control centers, and visibility into the systems that provide service to the NAS.

In the NAS, daily reports are used in outage briefings at the FAA National Operations Control Center (FAA NOCC) and the FAA Technical Operations Control Centers (FAA TOCC). The NAS telecommunications provider also provides daily outage reports and opens trouble tickets for each NAS telecommunications service that is out of service. NAS outages are assigned an importance level based on the type of facility and airspace affected which drives the level of daily outage reporting and any additional reporting that may be required. If an outage is ATC affecting, the FAA NOCC may open a teleconference bridge for constant monitoring of the outage till the issue is resolved.

3.1 FTI Network Operations Control Center (NOCC) and FAA Coordination

The FTI telecommunications network is controlled and monitored by the vendor's FTI NOCC. The purpose of the FTI NOCC is to monitor the network, perform restoration, communicate outage information to the FAA TOCC(s), and collect performance statistics on FTI services.

The communications between FTI NOCC and the FAA can take several forms. For outages, a trouble ticket system and scheduled maintenance request (MR) system is used to communicate outage related information to the FAA. Trouble tickets are posted in an on-line system that provides status of all scheduled and unscheduled telecommunications outages in the NAS. MRs are sent to the FAA TOCC(s) when scheduled outages of active FTI services are necessary for restoration, implementation, or other network changes. MRs are then coordinated by the FAA TOCC(s) with the system users for approval, rescheduling. Informal chronic service procedures are also in place to deal with repeating outages on the same service.

During significant outages, teleconferences may be set up by the NAS telecommunications vendor by request of the FAA so that the FAA TOCC(s) can receive real-time status on a particular restoration activity. In addition to teleconferences, there are escalation procedures that provide FAA management an escalation path with the NAS telecommunications vendor organization to ensure that restoration activities are receiving the appropriate priority. FAA personnel are collocated at the FTI NOCC facility as operations liaisons to support service restoration activities.

To ensure survivability of the NAS FTI monitoring and control capability, the FTI service provider is able to transfer operations to a backup FTI NOCC capability in a different geographic location from the primary NOCC facility. Loss of the NOCC capability does not disrupt the operation of individual telecomm services.

3.2 Relationship between FAA and Its Telecommunications Service Provider

Given the operational impact and visibility of outages in the NAS, it is imperative that the FAA and the NAS telecommunication provider have a cooperative relationship. When outages of NAS services occur, the goal of both organizations must be the restoration of the service in order to minimize impacts to the flying public. Open and honest conversation on both sides is required to facilitate this relationship. The FAA requires the FTI vendor to identify and advise the FAA of potential improvements to the telecommunications operating environment. This could include mitigation of vulnerabilities they discover, less expensive ways of delivering services, and other improvements.

3.3 U.S. Critical Infrastructure Support

The NAS is a key element in the U.S. Transportation Systems Sector critical infrastructure. The FAA and the FTI Vendor respond to a variety of situations of national importance including natural disasters, official government transportation, and military and law enforcement activities. A typical response may include the rapid and possibly temporary deployment of telecommunications infrastructure to various locations. The ability of the FTI telecommunications vendor to support this type of response is critical to support NAS operations during such situations.

The FAA also communicates with many non-FAA entities like Department of Defense, National Weather Service, Local Airports/Law Enforcement, and other Governments. These communications are routed through enterprise security gateways provided by the FTI vendor. The enterprise security gateways are a vital element of the FAA's telecommunications infrastructure and are crucial to supporting the coordination required during emergency conditions as well as day-to-day NAS operations. (See Security white paper for more detail).

3.4 Mission Critical NAS Services

The FAA specifies Service Level Agreements (SLA) for all NAS services that are verified upon installation and then continuously monitored. Reliability, Availability, and Maintainability (RMA) and Diversity and Survivability are discussed in this paper. Other traditional SLA parameters are also specified such as latency, jitter, packet loss, and security. They will be the subject of a separate paper.

3.4.1 Reliability, Availability, and Maintainability (RMA)

In order to provide the ability to support different levels of service criticality in the NAS, the FAA defined seven different RMA levels to provide the flexibility to match the price to performance for individual user requirements. Factors that make up an RMA level include the minimum availability (from 0.997 to 0.9999971), mean time between outage (MTBO), restoration time, and maximum number of outages. The FAA and the telecommunications vendor track the causes of all outages and verify service availability based on the outage start and stop times.

3.4.2 Diversity and Survivability

Service diversity is the logical or physical separation between components of a service necessary to achieve the specified availability of that service and protect that service from correlated failures. The FAA defines two types of diversity, electrical and physical. If physical diversity is needed to achieve a given availability and is not achievable without significant capital investment, the FAA may choose to waive the performance requirement as it relates to the non-diverse component.

With point-to-point TDM architecture, the ability of widespread failures to occur was mitigated through the use of service availability. But as Operational Internet Protocol (OPIP) services became more prevalent in the NAS that increasingly rely on shared platforms (like routing protocols), the need for increased survivability against common mode failures is obvious. Survivability in the FTI OPIP network defines whether a service needs diversity of backbone routing protocols. This limits the risk that multiple services will fail due to common mode failures in the backbone.

One of the functions of FAA's NAS Operations Team is to confirm that the telecommunications configuration meets availability, diversity, and survivability requirements for each NAS service. This means that the NAS telecommunications vendor shares information (including proprietary information) about the configuration of the NAS telecommunications services with the FAA. FAA and the NAS telecommunications provider have joint meetings to discuss network configuration.

The FTI vendor is required to perform continuous diversity audits on a rolling wave basis across the network to ensure that diversity is provided as required and carrier re-grooming actions have not resulted in diversity violations. When a diversity violation is identified, the FTI vendor must develop a mitigation plan in coordination with the telecommunications carriers and track the plan to closure.

3.4.3 Security

Security is an important part of NAS operations. It is addressed in a separate white paper.

4.0 FAA Critical Challenges

Given the movement toward packet-based communications in the telecommunications industry, it is anticipated that the NAS may not have access to the same level of dedicated resources in the telecommunications infrastructure that has been possible in the legacy operating environment. This raises a number of important concerns and challenges including the ability to:

- Maintain NAS telecommunications service availability and diversity requirements in an IP/Ethernet packet based environment.
- Provide confirmation of service diversity in a packet based environment.

- Support the NAS coordination requirements for service outages in a “shared” environment.
- Support mean time to repair at rural facilities as more rural users become wireless users in a cost-effective manner.

5.0 Questions

1. Are there any new/innovative models in development or recently implemented for monitoring and control of mission critical infrastructures? If so, how do they differ from the vendor-managed centralized NOCC model used on FTI today? What are the trade-offs (i.e., pros and cons) associated with the newer models compared the current model employed on FTI?
2. What level of visibility should the FTI-2 service provider be able to provide the FAA relative to the configuration and physical routing of services that have high availability or survivability requirements? Can this level of visibility be maintained across the operational life cycle (beyond the initial implementation) as the carriers reconfigure their networks and re-groom services? How does the move to IP/Ethernet service affect this visibility?
3. What level of visibility can be provided to the FAA into the real-time operation of the network? Is the level of visibility affected by specific technologies that may be employed? Given the shared nature of packet-based telecommunications networks today, what new concepts exist that can provide assurances to the FAA that their individual Air Traffic services meet availability and diversity requirements? Are there ways to provide the FAA with an assurance of service availability and resilience without identifying specific paths?
4. Can carriers continue to support the FAA’s requirement for obtaining the FAA’s “release of the service” before any maintenance actions are taken? (Note: This includes corrective and preventive maintenance.) Are there any implications to supporting this requirement based on specific technologies employed within the network?
5. What is the mean restoration time for telecommunications services in urban and rural settings? What is a reasonable restoration time the FAA should be able to expect in these settings? Does the use of the service affect those times?