National Airspace System Security Cyber Architecture

James H. Williams

Federal Aviation Administration

T.L. Signore
703 983 7919
MITRE Corporation
signoret@mitre.org

Abstract. The Federal Aviation Administration (FAA) manages US airspace to promote safe and efficient operations. The FAA is presently revamping its infrastructure to accommodate new air traffic control (ATC) services and to reduce risks associated with cyber threats. A description of the cyber security architecture, being deployed, is provided. The transition from a safety culture to a cyber security and safety culture is a part of this deployment. This transition is considered essential to the success of the architecture and it is also described.
Keywords National Airspace System, Security Architecture, High Reliability, Security Governance

1 The US National Airspace System

The United States National Airspace System (NAS) is a complex collection of systems, procedures, facilities, aircraft, and people. These components work together as one system to ensure safe and efficient services are provided to the flying public, airlines, the US military, general aviation, and airports. The NAS includes: the US airspace, air navigation facilities, equipment, services, airports, aeronautical charts, information/services, rules, regulations, procedures, technical information, manpower, and material. Many of these components are shared jointly with the military. FAA airspace management is different from many other nations because the FAA manages both military and civil aircraft in the US airspace.

The NAS is enormous by any way you choose to describe it. For example the following estimates are from the FAA Administrator's Fact Book, March 2010:

- 63,486 NAS operational facilities (unstaffed)
- 21 Air Route Traffic Control Centers
- 512 Air Traffic Control Towers
- 40,000 ground radios
- 400 radar sites
- 18,000 airports
- 35,000 people operating, maintaining and modernizing the system
- 18,519 commercial aircraft (CY 2009 data)
- 228,700 general aviation aircraft (CY 2008 estimate)
- 771,100,000 passenger miles flown by commercial aircraft
- 26,000,000 miles flown by general aviation aircraft (CY 2008 estimate)
- 706,000 passengers (CY 2009 data)

All control towers, control centers, radios, radars and many airports are interconnected to form the NAS operational communications network, This network supports the transfer of voice and data among pilots, controllers and airline operation centers. Nearly all network components are capable of providing status information in (near) real time to monitoring facilities.

Figure 1 shows conceptually how the system currently works and what equipment is used to provide the service. For more information on the current system and plans for the future evolution of the FAA NAS visit the NAS Enterprise Architecture Portal at nasea.faa.gov. There you can see how the information

security architecture is interwoven through the NAS Enterprise Architecture Views to create a seamless approach to Cyber Security. It is important for the reader to note that the NAS does not include the administrative Information Technology (IT) systems used to support the employees and nonoperational activities of the FAA. For example: NAS Communications networks are physically separated from the administrative networks even though they are managed under the same contract.

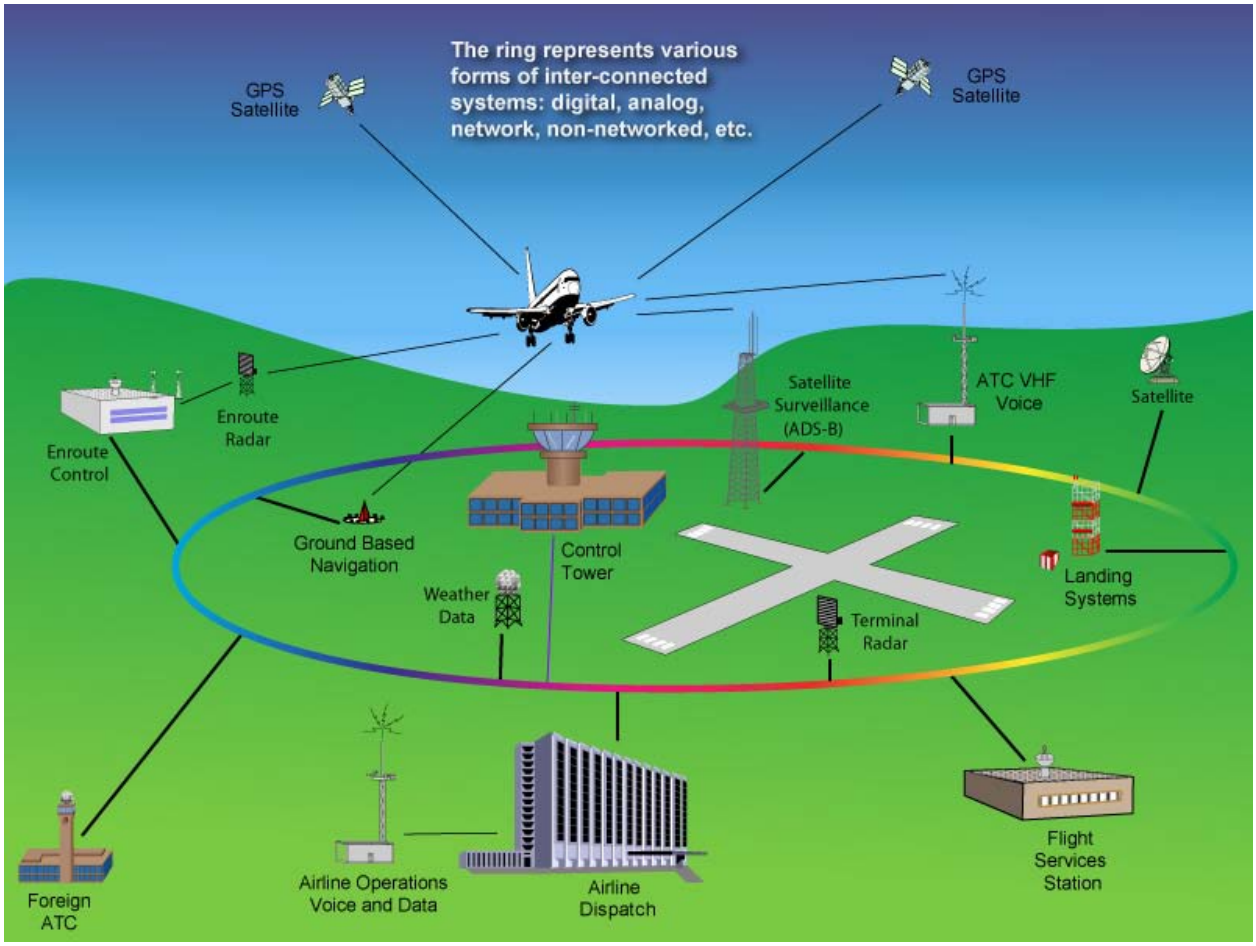

Figure 1: ***National Airspace System Major Components***

2 NAS Safety

Presently NAS operations and supporting administration procedures are designed for safety and efficiency of operation. One manifestation of safety within the NAS infrastructure is a highly reliable system. A primary means to achieve sufficient reliability is by the use of redundant systems. For example hot-standbys for all critical components, at least two physically separate communication paths for critical systems and overlapping radar coverage in many areas are all necessary. Such redundancy minimizes system failures and contributes to graceful degradation of services. The use of components isolated from the U.S. communication infrastructure has also been found to be necessary to meet reliability needs. Isolation extends to the use of dark fiber within the NAS communications infrastructure. That is, single purpose FAA dedicated equipment is used for all networking and switching functions, sharing only the access to commercially available fiber cable. Time and repeated failures over the entire 70 years of automated air traffic control have demonstrated that reliability decreases when the equipment is shared with other, non critical and non-NAS users.

To maintain the safety of the NAS infrastructure and its concomitant reliability the NAS requires fault reviews of all new components, all new procedures, and whenever performance is not as expected. Integral to these reviews is the information provided by a separate monitoring network that provides status information on all major NAS equipment.

The isolation of the NAS with a separated monitoring system was originally based on safety and performance needs. Now NAS isolation contributes significantly to cyber security.

3 FAA Next Generation Air Transportation System (NextGen)

NextGen is an umbrella term for the ongoing, wide-ranging transformation of the NAS. At its most basic level, NextGen represents an evolution from a ground-based system of air traffic control to a satellite-based system of air traffic management. This evolution is vital to meeting the future traffic demand on the NAS, and to avoid gridlock in the sky and at our nation's airports.

When fully implemented, NextGen will allow more aircraft to safely fly closer together on more direct routes, reducing delays and providing unprecedented benefits for the environment and the economy through reductions in carbon emissions, fuel consumption and noise.

NAS network architecture is changing drastically to support NextGen. Today's NAS relies on a combination of multiple networks and numerous point to point connections. These communications systems are physically isolated from the Internet. In the NextGen vision there will be a highly redundant network architecture that will allow for a high level of flexibility to support and promote new ATC services. These networks will be based on Internet Protocols but will remain physically separate from the Internet. Connections to NAS users, the US Military, and other Navigation Service Providers will be through redundant highly secure gateways. A key aspect of the NextGen Vision is the System Wide Information Management System or SWIM. The SWIM will be the NAS implementation of a Service Oriented Architecture (SOA) to enable easier discovery and sharing of key NAS data and information. These advances in information technology will greatly improve the flexibility of the NAS but will bring new challenges for the security of the system. For example, today's NAS relies on the security of a dedicated connection to an Airline. In the NextGen vision of the future explicit authentication and authorization will be required to access the NAS networks via a secure gateway.

4 Future Needs of the NAS

The present features of the NAS are not sufficient to guarantee efficient or uninterrupted operation in the future. Greater use of IP networking to interconnect systems and services in the NextGen era will adversely influence past resiliency, redundancy, and isolation solutions. Greater interconnections of systems will also increase the cyber risks to the NAS.

Improved cyber security requires changes to present NAS safety provisions. Consideration of deliberate actions, in addition accidental actions, is now required. A shift from safety review at specified times to continual analyses is needed. An expansion of responsibility for system administrators and network operators from maintaining performance to detecting intrusive actions is also imperative.

Improved cyber security also requires changes to the NAS infrastructure to provide more assurance that data provided by external partners and actions requested by external partners are not malicious in intent. Ultimately this means the NAS infrastructure must allow system modifications in a short timeframe to counteract changing cyber threats. Agility of function is now a requisite characteristic of the NAS. This future cyber security need counterposes a safety culture which values consistency and lack of change.

The future cyber security needs of the NAS require both NAS infrastructure and safety cultural changes to be effective.

5 The NAS Cyber Security Architecture

Introduction of a new cyber security architecture into the NAS infrastructure has two major constraints. The first is that NAS operations must continue during infrastructure changes. The second constraint is modifications of a processor that directly supports a safety function within the NAS must be minimized. As previously indicated the safety culture values constancy. Using host-based Incident Detection Systems (IDS) or Network Access Control (NAC) security solutions, for example, should not be mandated at the enterprise level. Such security tools may interfere with time-critical operations. Their use is best determined at the local level.

The NAS cyber security architecture has two characteristics based on these constraints. It is primarily a logical infrastructure over the existing IP network. This characteristic greatly eases the transition with the existing infrastructure still available in case of unforeseen issues. The second characteristic is the use of defined data flows within the NAS. The communication traffic is constrained to pre-established flows patterns. At certain points within the flow patterns, cyber security controls are placed which monitor, enforce, and restrict, as required, the data flow. The emphasis on cyber controls within a flow pattern means that the primary solution for security is not one which is based on client or host-based solutions. This minimizes perturbations to existing hardware/software and possible adverse consequences to NAS operations.

The traffic flows are intended to be constrained by the network infrastructure so that it is very difficult to bypass a flow. The intent is to have all network traffic use one of the following traffic flow classifications.

- **External Boundary Protection (EBP)** - The EBP examines data entering or leaving the NAS and provides boundary services such as VPN terminators, proxy applications, authentication and authorization services. The EBP thus forms the secure boundary for the NAS. The secured NAS is restricted to those components controlled or managed directly by the FAA. Aircraft, airline operation centers and foreign air traffic control authorities, for example, are not considered to be within the secured NAS boundary.
- **Certified Software Management (CSM)** - CSM examines software entering the NAS and provides controlled distribution points for the software within the NAS. A major feature is that all NAS software configurations would only reference internal servers for updates, patches, etc. and not reference any external sites. (The EBP would enforce this directive). Software within the NAS is signed for integrity and authentication purposes after both a cyber security and operational evaluation.
- **Intrusion Detection and Response (IDR)** - IDR examines NAS data traffic patterns at key communication points, and in concert with assembled log information assesses the cyber security status of the NAS. Information from the existing NAS network management system, which was developed to monitor NAS equipment performance, is incorporated into the log collection. The IDR uses a separate network so as not to adversely influence the NAS operations in any manner. Past safety analyses have concluded that a separate network is required, when a portion of the NAS operational network is failing, to allow access to needed status information and to allow an administrative path for reconfiguration.
- **Internal Policy Enforcement (IPE)** - IPE examines data traffic at strategic points within the NAS and provides a means to recognize and counteract malicious actions and data that originate internally or through deficiencies in the EBP installation.

Within each traffic-flow classification the type of cyber examination can change over time. This provides the needed agility to respond to new threats, while keeping major portions of the infrastructure

unmodified. In particular necessary cyber changes to NAS processors involved with critical operations can be minimized. A separate research effort is needed to monitor new cyber security software solutions and the changing threat environment with the goal of updating the type of flow examinations as needed. One result of this research has been the recommendation that all NAS data examined within the EBP and IPE capabilities occur at the application message level and be examined for consistency with NAS published formats for type, length, and value range. The NAS has a significant advantage over other organizations in that many of its data transfers are based on pre-approved messages with pre-authorized users. For example flight plans are internationally standardized and should be rejected if any unknown variation is encountered. This is a form of application content white-listing and has many advantages over checking for malware, as malware signatures are not involved.

Internal Policy Enforcement (IPE) assumes that traffic-flow patterns are based on partitioning of the NAS into enclaves. Information flow within an enclave is not constrained by the cyber security architecture, except as required by end-systems. But information across an enclave boundary is subject to authorization, flow control and application content white-listing. The intent is that a cyber attack in one partition would ideally not cross a partition boundary. In the worst case the enclave that has been compromised can be isolated from the rest of the NAS from a networking perspective. For example, it would be useful to continue to provide ATC services in an isolated enclave that no longer has the ability to receive or send flight plans to other enclaves. This type of partitioning allows for a graceful degradation of services while mitigation occurs within the compromised enclave.

The structure of enclaves within the NAS is not yet determined. Some possible enclave compositions that have been discussed are as follows.

- Apply the four color map solution. This would guarantee that neighboring terminal areas are always in a different enclave and therefore an alternate operating terminal area should be available if any terminal equipment has been compromised.
- Place the most important ATC functions (aircraft separation) in a separate enclave not directly connected to any entity external to the NAS. This *crown jewel* enclave would presumably be the last to incur malicious actions originating from outside the NAS.
- Define an enclave which is restricted to aircraft position report data and which only provides for the broadcasting out of such data. This preserves the integrity of aircraft report data, as the enclave would not have the capability of receiving data and consequently it would be very unlikely to be effected by malware.

One enclave has been defined for the NAS and is in the process of implementation. This is a research and development enclave. The R&D partition addresses the problem of providing NAS data to research facilities while minimizing the chance of ‘back doors’ into the NAS. As any data leaving or entering the R&D enclave would be subject to IPE review.

Any advantages in partitioning the NAS will only occur if the partitioning cannot be bypassed or ignored. If it is possible to transfer data from one enclave to another without IPE involvement, be it malicious or accidental, then many of the security benefits are negated. For this reason it is very important that inter-enclave communication without transfer through an IPE point not be possible. The use of BGP based VPNs with policy routing to forward inter-enclave traffic to IPE points would meet the requirements for IPE transition. Such a solution does not depend on the good faith of application providers. Nor does such a solution require a physical partitioning of the NAS. A logical foundation for partitioning allows the enclave definition to vary and mature over time.

6 NAS Governance Changes

The implementation of the NAS cyber security architecture is not entirely an infrastructure issue. Changes in culture by FAA employees and contractors are needed for improved cyber security. Heretofore procedures emphasized safety assessments and improvements. These now must be changed to include cyber assessments and improvements. The FAA has begun the process of including cyber security into the NAS operational management structure.

- The cyber security architecture is included within the NAS Enterprise Architecture so that all FAA employees and contractors are aware of its existence and importance. The NAS Enterprise Architecture is available for review via a web interface.
- The acquisition management system used by the FAA now requires all future NAS programs to use the NAS cyber security architecture. This means that funds can be denied to those programs which do not incorporate the NAS cyber security architecture into their operations.
- The NAS safety and performance review group, denoted the Security[1] Information Group or SIG, is being expanded to include cyber security assessments. A formal working relationship to convey incident reports and impact status on NAS operations is being established among the SIG, Cyber Security Management Center (CSMC), Security Operations Control Center (SOCC), Network Operations Control Center (NOCC) and Network Enterprise Management Center (NEMC). A common ticketing system is being established among these organizations (and NAS help desks). This is necessary as a security incident may first manifest itself as a performance issue. Conversely the significance of an incident may be assessed by reviewing performance information.
- NAS written policies are being updated to include explicitly the role and responsibilities of managers and departments in developing and supporting the NAS cyber security architecture. The effectiveness of these policies is largely dependent on the understanding of the NAS cyber security architecture by FAA employees and contractors. Therefore one of the goals for the NAS cyber security architecture is that the basics of the security solution be understandable by all and not viewed by the majority as an arcane technical solution with which they can have no connection. If everyone has some understanding of the basic feature of the NAS cyber security architecture, then the benefits of the NAS cyber security architecture should be achievable more quickly and efficiently.
- A program has been established with the FAA to help legacy (existing) NAS programs understand and transition to the NAS cyber security architecture. This program is known as the NAS Enterprise Information System Security (NEISS).

7 Conclusion

The performance characteristics of the NAS safety mission have always included resiliency solutions which are designed for continued operation during unintentional failures. NAS is leveraging these existing safety solutions for continued operations during cyber events. The advent of NextGen, which increases communication connections and services, requires additional cyber security controls for the NAS. These controls are a part of the NAS cyber security architecture. The NAS cyber security architecture constrains traffic flows to provide data examination and is designed to continue the proven benefits of isolation and redundancy employed by the present system.

[1] Originally the term security primarily denoted physical safety for the NAS.