Secure Network-Centric Aviation Communication (SNAC)

Paul H. Nelson*, Mark A. Muha†, and Charles J. Sheehe*
*National Aeronautics and Space Administration (NASA) John H. Glenn Research Center at Lewis Field, Cleveland, Ohio 44135
†V2 Technology, Northfield, Ohio 44067
Email: paul.h.nelson@nasa.gov, mark.a.muha@nasa.gov, charles.j.sheehe@nasa.gov

Abstract—The existing National Airspace System (NAS) communications capabilities are largely unsecured, are not designed for efficient use of spectrum and collectively are not capable of servicing the future needs of the NAS with the inclusion of new operators in Unmanned Aviation Systems (UAS) and On Demand Mobility (ODM). SNAC will provide a ubiquitous secure, network-based communications architecture that will provide new service capabilities and allow for the migration of current communications to SNAC over time. The necessary change in communication technologies to digital domains will allow for the adoption of security mechanisms, sharing of link technologies, large increase spectrum utilization, new forms of resilience and redundancy and the possibly of spectrum reuse. SNAC consists of a long term open architectural approach with increasingly capable designs used to steer research and development and enable operating capabilities that run in parallel with current NAS systems.

Keywords—Secure, Network, Aviation, Communication, Architecting

Structure of this paper: Chapter 1 is the introduction with background information. Chapter 2 is the details of the concepts being advocated and there challenges, Chapter 3 are the SNAC's desired outcomes from its research for the NAS. Chapter 4 SNAC possible research areas. Chapter 5 SNAC activities at the time of writing, with Conclusions and Next Steps.

I. Introduction

The National Airspace System (NAS) communications environment consists of a number of diverse communication, navigation and surveillance (CNS) types, methods and services. Each was developed, and further refined, based on largely separate requirements and developed to avoid impacting other areas of communication or operations in the NAS. Current pressures on the NAS due to increased capacity needs and near term disruptive introduction of unmanned and autonomous systems are already taxing the current CNS environment. Near term operating expansion will require expanded capacity in a number of CNS areas. This is not just an adjustment to a larger number of vehicles, but a fundamental change in the requirements for secure high-speed data connections. Unfortunately, many of these current technologies were not designed for these new realities, including a fundamental need to secure the communication links, address limitations in spectrum or provide scalable solutions. The SNAC will provide always on, flexible, routable, and resilient network service between aircraft and the ground, between aircraft and space and in between aircraft.

To address these needs, a fundamental change of approach is required. Instead of discrete solutions to secure CNS needs, a Secure Network-Centric Aviation Communication (SNAC) network system is proposed. This new network approach will allow all new NAS systems and applications to use the same underlying communications network, and over time, provide for a scalable transition of existing CNS solutions to a secure, high-speed and digital future. Clearly, this level of transformation will require the coordinated collaboration of industry, research and government organizations. To facilitate this, and avoid building a complex coordination organization, a SNAC reference architecture (RA) will be used. The SNAC RA, developed by the stakeholders, will provide a goal defined future state to enable independent actors to develop and deploy completely interoperable SNAC CNS solutions. The SNAC RA will initially provide a simplified reference; however over time this reference will be further refined and expanded to eventually illustrate the mature future state.

Once the simplified initial SNAC RA is in place, it is anticipated an initial SNAC operating capability will follow in short order. In order to avoid impacting current NAS operations during this trial phase, focusing on new Unmanned Aviation System (UAS) and On Demand Mobility (ODM) needs will provide a rich and complex enough environment to demonstrate capabilities and explore the path toward certification. Follow this initial phase; the SNAC RA will undergo an expansion followed by the next version of the SNAC. This iterative, spiral design path will eventually lead to the mature SNAC operating capability and in a carefully managed manner that limits negative impacts on the operating NAS.

The High Level Concept of SNAC is an operational concept for future aviation communication that provides always on, secure, flexible, routable, and resilient information service between aircraft, aircraft and the ground, and aircraft and space assets. Envisioning all participants as a node in a secure network, capable of sending and receiving critical data through application of network connectivity methods, protocols (rules), security technologies and robust capacity, SNAC utilizes all available link technologies (radio, satellite, terrestrial) in the operational environment to deliver information to all participants in the aviation ecosystem.

Current challenges and problems, according to the ATA (International Air Transport Association) forecast, by 2035, 7.2 billion passengers will travel by air annually[1]. This nearly doubles the 3.8 passengers expected to utilize air transport in 2016. The increased air traffic, new NAS entrants such as Unmanned Aircraft Systems (UAS) to 7 million by 2020 and

commercial space vehicles, as well as ubiquitous adoption of autonomous and smart technologies in the aviation ecosystem, will severely test capacity, affordability, and performance of the Federal Aviation Administration's (FAA) communications systems Next Generation Air Transportation System (NextGen) program implemented and retained[2]. As the challenges, associated with explosive growth of data, and opportunities to innovate, by mastering the use of data, led to proliferation of cloud-based platforms and service models, a new paradigm to enable production, exchange, and consumption of air domain information securely and cost-efficiently merits consideration. Enter Secure Net-centric Aviation Communication (SNAC).

II. Detailed Concept

Through the concerted use of Security Systems Engineering process this concept was developed. The SNAC is the application of network methods and technologies intended to improve aviation safety, reduce frequency congestion, expedite data transfer and provide secure information exchange throughout the NAS. SNAC is needed to support anticipated growth in air transportation. The SNAC involves integrating, transporting, and retrieving air transportation-related information and data, terrestrial and airborne, between providers and consumers on a reliable, scalable, flexible, and secure enterprise network, accomplished through the provision and management of infrastructure resources to sustain normal operations and service level agreements. The SNAC is a real-time, globally interconnected network environment, incorporating infrastructure, systems, processes, and individuals to enable an enhanced cross-agency information sharing approach to aviation transportation (Fig. 1).

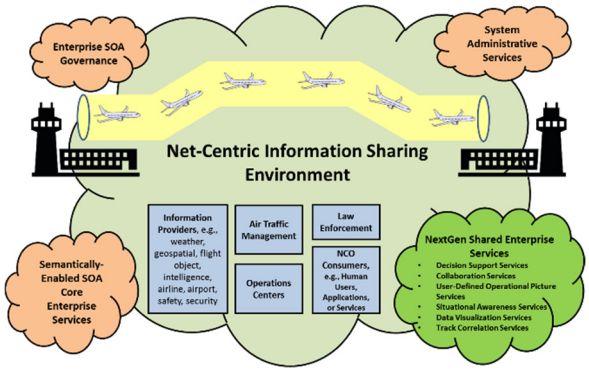

Fig. 1. Secure Net-Centric Aviation Communications Environment.

A. Layered Approach

The proposed SNAC model uses the following layers to create a universal set of net-centric integrated requirements to access these systems (Fig. 2):

- **Security Layer** – Performs user authentication and matches security attributes on interagency level between users and data/services providers
- **Ontology Layer** – Integrates metadata and service registries across information systems and provides searchable descriptions of all available data and services, based on user access level
- **User Agreements Layer** – Manages the agreements between users and providers at the enterprise level
- **Services Layer** – Provides qualified users and operators access to all available authorized services across participating agencies information systems and hosts tools that combine existing services with applications that use the data layer

Data Layer – Provides qualified users and operators access to numerous data systems made available by participating agencies information systems.

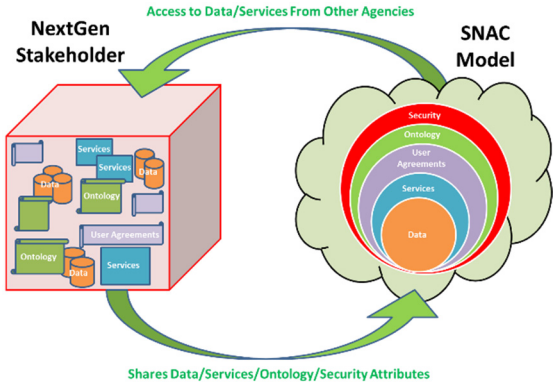

Fig. 2. Shared Services Attributes

The *security layer* is designed to control SNAC access. The security layer manages users' qualifications as well as security requirements of data and service providers across interagency information systems. In the SNAC, information from certified, authoritative sources will be accessible to any authorized consumer. The SNAC model will provide a robust and efficient way of addressing security concerns by employing the enhanced security system based on synergy of Federated Identity, Credential, and Access Management (FICAM); user security attributes; and data/services provider security attributes. The SNAC security layer will ensure only authorized users have access to the system and see only the information appropriate for their security attributes. On the other side, information providers will use the security layer to exert full control over who can access their data and services by managing data/services security attributes and user agreements. Once a user is authenticated and security attributes are matched, information passes on to the ontology layer which ensures data and services that users do not qualify for will remain invisible to them. The SNAC only serves as a conduit for information discovery and exchange; it will not hold actual data itself.

The *ontology* layer will provide critical metadata models necessary to facilitate data integration across NextGen systems, supporting interoperability of disparate information systems. Ontologies and data vocabularies will provide guidance to application developers and users about the precise meaning of data and services available across the stakeholders' information systems. Ontologies will enable metadata tagging of information resources and services and will make interagency information and services easily discoverable and reusable. The ontology layer will provide information about available data sources and services exclusively based on the users' level of access as determined by matching security attributes from the user and

data provider. User access to the SNAC will vary widely, and the amount of information provided will be based primarily on the users security attributes to keep sensitive information well separated from information and services suitable for public dissemination.

The *user agreements* layer will enable users and providers to opt in to the enterprise to collaborate and share information across the NAS. User agreements for specific data and services will automatically be provided to SNAC users, once they identify services they want in the ontology layer and request access from providers. User agreements will ensure data and services provided will be used in accordance with standards and rules set by their provider. This layer will also manage service level agreements to ensure level of service provided to users is sufficient to perform their mission. Certain data sources and services will be available for public use and will not require users to have user agreements.

The *service* layer will provide qualified users and operators with a medium to discover, access, and subscribe to information services from participating information systems. Operators will enjoy centralized access to existing services, while developers will create new tools to combine services from multiple information systems. These tools will provide users and operators new ways to capitalize on centralized information access. Some services will be native to the SNAC model, while others will be provided by the stakeholders' information systems.

The *data* layer will create a streamlined process for interpreting, accessing and integrating data sources from cross-agency information systems. Qualified users will have access to a wealth of data sources made available in one place. Synergy of data from participating agencies information systems will create a perfect environment for building new tools and services for specific user needs. These new tools and services will be registered in the ontology layer and available to other users, greatly reducing the systematic redundancy and excess costs associated with interagency use of new data sources.

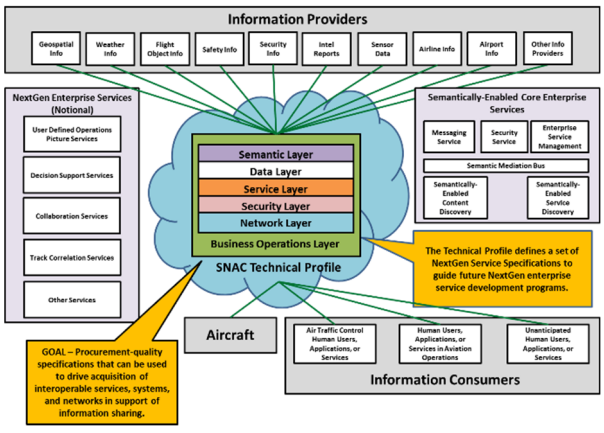

Fig. 3. SNAC Conceptual Overview

B. *SNAC Enterprise Services*

The following services would be provided through the SNAC enterprise:

- **Information Sharing Services** – Enables agencies, businesses, operational units, and stakeholders, throughout the NAS, to collaborate in a net-centric information infrastructure with the Air Navigation Service; airport & flight operations; compliance and regulation oversight authorities; and security, safety, environmental, and performance management services to create a shared situational awareness.
- **Ground Services** – Provided surveillance, communications, and flight data management to any service provider regardless of its physical location, thus removing geography as a limiting factor for air assets and ground control
- **Air-Ground Network Services** – Abandons frequency-to-airspace sector mapping in favor of a dynamic network environment. This network environment will require additions to network protocols to account for locality and diverse routing. Data communications are central to Trajectory Based Operations (TBO), including the use of four dimensional trajectories (4DTs), for planning and execution on the surface (pushback and taxi inclusive), automated trajectory analysis and aircraft separation assurance
- **Air-Space Network Services** – Follows the same approach as the Air to Ground. The additional latencies inherent in satellite communication services . This will require additions to network protocols to allow for latency calculations.
- **Air-Air Network Services** – Follows the same approach as Air to Ground with additions for bi-cast or multi-cast routing to enable sense and avoid schemes and enable complex routing possibilities.
- **Aircraft Data Communications Link** – Allowing aircraft and ground assets to connect to a common, authenticated data network for collaborative purposes
- **Infrastructure Management Services** – Ensuring quality of service (QoS), including high-level security and reliable, authoritative data.
- **Mission Support Services** – Providing information assurance, protocols, and standards applicable for the net-centric infrastructure services (access, connectivity, processing, posting, and pulling). This will include the critical Identity service needed to authenticate users, devices, services and data.

C. SNAC Challenges

Potential barriers to achieving the future digital data communications environment include:

- Spectrum expansion limited and is largely assigned to existing, often non-aviation, systems. Its under constant threat of reassignment to non-aviation purposes.
- New vehicle classes and proposed capabilities may exceed current data communications capabilities
- Security is challenging; Today's aviation communications systems are largely unsecured. They may be difficult or impossible to secure and they lack any system capability to identify or respond to compromise.
- Interoperability; Current capabilities were designed to independent requirements. Integrated operations were not part of the design
- Cost; Employing the current spectrum with digital instead of analog communications will require new equipment. Pricing should be competitive with current technologies. Limitations on size, weight and performance should be carefully attended to.
- Equipage lifecycles are not in favor of significant or rapid change in fundamental technologies. With a 7 year development and 20 year initial operation lifecycle for commercial aircraft, SNAC development will challenge the norm.
- Protocol Challenges in several key areas need to be addressed. There are 2 fundamental needs for the network transport protocol which need research. First, the ability to initiate connections to rapidly moving vehicles will require some mechanism to locate the vehicle relative to the ground and space network service assets. Second, it is anticipated that the applications depending on SNAC will need the ability to manage their communications state while the underlying link services are rapidly changing.

III. SNAC Research Desired Outcomes for the National Airspace System

SNAC's concept is a unified approach that will open the development process to the community which will allow increasing capabilities to be seamlessly integrated into the NAS.

Service independent applications are a key enabling concept the will enhance the rate of capability increases within the NAS.

SNAC would like to build on the successes of the telecommunications community as a way of integrating services. One example of a platform architecture that may be envisioned in SNAC is like the android platform, open, community supported with increasing capabilities, service independent applications that are based on open standards activities. Fig. 4 is such a platform architecture.

Fig. 5 is a time partitioned architecture that allows the flexibility to run operating systems and applications without interfering with other services.

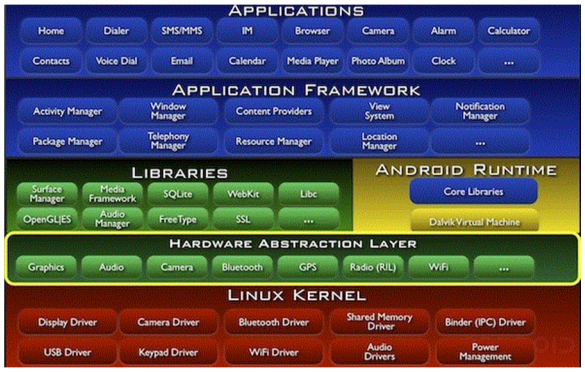

Fig. 4. SNAC platform API concept[4]

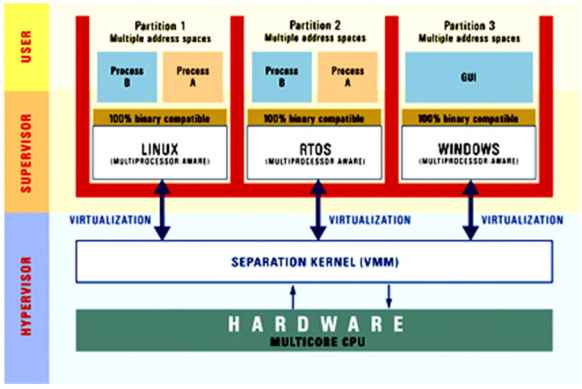

Fig. 5. Time portioned platform[5].

The platform is integrated into a structured standards based industry, yet providing and growing level of services to the user.

The SNAC authors intend to work diligently with the standards organizations to bring about this new NAS, like Future Airborne Capability Environment (FACE) of the Object Management Group, International Civil Aviation Organization (ICAO), and the Radio Technical Commission for Aeronautics (RTCA).

Security from the inside out concept illustrated in Fig. 6.

Fig. 6 depicts the Cyber-Physical security hardening the core and work outwards though the more complex layers.

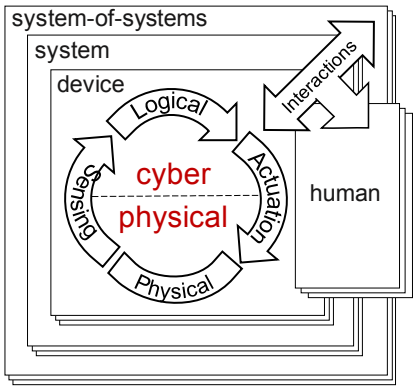

Fig. 6. Cyber Physical Security.

A holistic approach is intended securing the hardware, the system, securing the system of systems is the Framework for Cyber-Physical Systems[6].

Requiring civilian, military, and intelligence agencies to develop an integrated, comprehensive inventory of the specific legal authorities and capabilities that agencies could employ to support the cybersecurity risk management efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts[7].

Desired outcome of the SNAC project are;

1. Security in Communications
    a. Secured aviation communications
    b. Security methods applied to data as it traverses the SNAC.
    c. Methods are based on risk. Common data may just need integrity checks while sensitive operational data may need encryption and authentication.
    d. Methods may be applied at any level of the OSI model.
2. Spectrum Efficiency and Potential Reutilization
    a. Increase available spectrum/channels by the use of data compression in current analog systems
    b. Increase available spectrum/channels by the use of more efficient voice encoding
    c. Spectrum agnostic systems that enable utilization of currently disparate bands in combined ways
    d. A voice/data/information framework that will allow the information to be transferred over any available systems/spectrum/channels.
3. Operational Impacts
    a. Meets all safety and security needs in all locations and phases of flight
    b. Information meet the assurance necessary for the stage of flight
    c. Information meet the security and safety assurance necessary for the stage of flight
    d. Information meets the latency needs for the stage of flight
    e. Information meets the authentication necessary
    f. Information protection meets the privacy needs of the users
    g. Higher speed data transfer in all directions
    h. Increased data through-put between flight systems
    i. Increased data through-put between flight systems and air space control
    j. Automation to reduce or eliminate the need for end users to understand the complexities of communications and associated systems; Reduced user interactions in regards to selecting path/method of the communications.
4. Leverage existing design work or operational systems concepts to reduce cost and time. This work includes:
    a. Information for Global Reach (IFGR), [USAF][8]
    b. Collaboration Information Management (CIM), [FAA] [9]
    c. Physical and link layer, research and demonstrations[3].
    d. Use of bests practices and most promising research (physical and information)
    e. Traditional security practices such as risk mitigation strategies, asset evaluation, threat assessments, proportional defense based on risk
    f. A layered, incremental, extensible, synchronized, segmented role out strategy.

IV. SNAC AREAS OF POSSIBLE RESEARCH TO ENHANCE THE CAPABILITIES AND SECURITY OF THE NAS;

- Enhanced networking concepts that explore locating and connecting to rapidly moving vehicles.
- Application level methods that allow resilience in operation while underlying data services provide wide variances in data rates.
- Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. Securing the Core[6].
- Is IPV6 the right network protocol or is a more secure or non IP routing protocol needed for the flight or flight to ground systems ?
- How to maintain security and priorities across Network domains?
- Link Resilience, what is the needed capabilities for each type of operational flight system in each class of the airspace.
- Reduced crew operations in class A, airspace how many low latency, secure links, resilient communications paths are needed to ensure safe & secure operations.
- UAS operations, how many low latency, secure links, resilient communications paths are needed to ensure safe & secure operations.
- Vehicle to Vehicle (V2V) and Vehicle to infrastructure (V2I) capabilities that are already in development for the ground transportation industry
- Trust between all participants including users, systems and data
- Key and certificate management
- Quantum communications including key management and distribution
- Over the Air Rekeying (OTAR)
- Latency vs. Encryption, watermarking, Cyclic Redundancy Checks (CRC), lightweight encryptions.

- Proper amount of entropy for authentication in an operational environment for flight control communications
- Proper amount of entropy for privacy of user traffic for flight controls
- SNAC Concept of operations
- Continuity of Operations, a Bad Day management, Concept of Operations
- Security and resiliency requirements for back channels
- Management of selfish actors.

V. SNAC IS TO BE COMPREHENSIVE LOOK AT THE INTEGRATED SAFETY AND SECURITY OF THE FUTURE NAS

SNAC as of writing of this paper is in the concept exploration phase within NASA and among partner agencies. We have been working with several agencies in order to codify NASA's and SNAC activities with regards to its role in directing the Research and Development of Secure communications for NAS that meets the increased capacity, while ensuring privacy and safety of it users.

D. Conclusions

From the activities leading to this paper that research is ongoing on many fronts. No one group is in charge of or responsible for directing, coordinating and fully understanding the communications and security research to enable the dramatic growth necessary to support the increasing NAS demands both in types and numbers of operators.

The sheer number of different components, operators, technologies, architectures and needs has become a barrier to moving forward. In order to break through these barriers, a far more collaborative effort needs to start with the involvement of participants from industry, academia and government. The SNAC reference architecture is intended to be the common design language to allow for this open, transparent collaboration to occur without needing a monolithic management construct.

The SNAC research work, focused in the rapidly developing areas of UAS and ODM, is intended to help enable these new industries in an environment that isn't traditionally risk adverse while minimizing any impact on current aviation operations.

The benefit from taking this path is a vision that will enable our community to begin moving in a common direction. Some benefits could be realized in relative sort order. The long term vision of moving aviation communications to a secure, routed, trustworthy and always available network will be challenging but the long term benefit will be a level of security and flexibility in aviation operations that will enable considerable growth.

E. Next Steps

We are asking for your understanding of the need and advocacy for an activity like SNAC within the government to enhance the capacity and security of the NAS for you and the rest of the flying public.

REFERENCES

[1] IATA, IATA Forecasts Passenger Demand to Double Over 20 Years, 18 October 2016 http://www.iata.org/pressroom/pr/Pages/2016-10-18-02.aspx

[2] FAA, 2016, FAA Aerospace Forecast FY 2016-2036 https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/fy2016-36_faa_aerospace_forecast.pdfG.

[3] USAF, AFRL-IF-RS-TR-2005-308 Final Technical Report August 2005 www.dtic.mil/get-tr-doc/pdf?AD=ada439303

[4] Image of the Android Operating Architecture http://ngeleki.blogspot.com/2014/03/the-beginners-guide-to-android-android.html

[5] Virtualizing and securing your apps with a time-partitioned RTOS by Arum Subbarao http://www.embedded.com/design/operating-systems/4008192/PRODUCT-HOW-TO-Virtualizing-and-securing-your-apps-with-a-time-partitioned-RTOS

[6] Framework for Cyber-Physical Systems https://pages.nist.gov/cpspwg/ https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

[7] https://www.whitehouse.gov/the-press-office/2017/05/12/president-trump-protects-americas-cyber-infrastructure

[8] http://www.dtic.mil/get-tr-doc/pdf?AD=ada439303

[9] Collaborative Information Management (CIM) Task 10: Mini Global Integration Final Report: TO-23/DS #9b, REV: New, September 30, 2016