A Holistic Approach to the Provision of Communications, Navigation, and Surveillance Services in the 21st Century National Airspace System

Mitchell J. Narins, *Federal Aviation Administration*
Sherman Lo, Yu Hsuan Chen, Per Enge, *Stanford University*

ABSRACT

Information technology applications in the 21st century essential to safety, efficiency, effectiveness, and growth – for day-to-day and even minute-to-minute operations – have been inextricably tied to the availability of radio spectrum and information bandwidth. The ability to securely and reliably exchange data and information and to support critical infrastructure applications is limited by the characteristics of the application's authorized spectrum (i.e., the modulation techniques a band of frequencies can support) and the environment in which it must operate (i.e., noise, multipath, co-channel/shared services, etc.). It is no wonder that spectrum has become so valuable, with commercial concerns willing to spend hundreds of millions of dollars and more at Government spectrum auctions for access to even the thinnest slices of the "choicest" frequencies.

From a data exchange/bandwidth perspective, some of the most valuable spectrum is found in the L-band – the spread of frequencies extending from 1000 megahertz (MHz) to 2000 MHz, where the Global Positioning System (GPS) civil frequencies (L1 at 1575.42; L5 at 1176.45 MHz), cellular telephone transmissions (1800-1900 MHz), Digital Audio Broadcasting (DAB) (1452-1492 MHz), Radio Astronomy (1420 MHz), Aviation Secondary Radar/Mode S/Traffic Collision Avoidance (1030/1090 MHz), and Aviation Distance Measuring Equipment (DME) and Tactical Navigation (TACAN) (960-1215 MHz) have allocations. It is this last frequency allocation, 960-1215 MHz – already designated for use by Aeronautical Radionavigation Services (ARNS), which will be the focus of this paper's discussion of the value of a holistic approach to the delivery of communications, navigation, and surveillance (CNS) services to support operation of the US National Airspace System in the 21st century. Rather than continuing to have the proponents of each service vying for use of this spectrum at the expense of the others (e.g., vacating DME navigation channels for use by Mode S and Automatic Dependent Surveillance-Broadcast operations at 978 MHz or creating new communications channels in the band by either vacating existing DME channels or through objectionable spread spectrum techniques), this paper recognizes the value of finding a more optimal way of using the spectrum while maintaining the independence and integrity of each function. It also recognizes the potential benefits to future avionic system design that could be achieved through receiver and antenna system synergies.

BACKGROUND

The US National Airspace System (NAS) ensures the safe and efficient movement of aircraft through the provision of Communications, Navigation, and Surveillance (CNS) services, on the ground and in the air, that support air traffic controllers, airline operation centers, airports, pilots, and passengers. Over the years the operational imperative of maintaining the independence of each of these CNS services to preclude common modes of failure has served the NAS well. This Safety Triad, composed of independent CNS services, is depicted in Figure 1. It ensures that risks resulting from a failure of any one of the services can be mitigated through the remaining, unimpaired availability of the other two – and the key Federal Aviation Administration (FAA) *Safety First* principle, which ensures that system safety will always be maintained – even at the expense of capacity and efficiency.

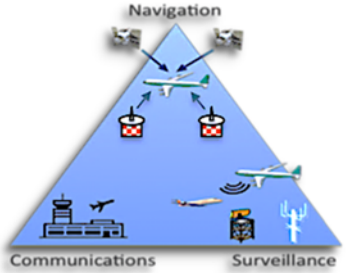


Figure 1 The CNS Safety Triad

The FAA plans to migrate today's NAS from its 20th century analogue communications, point-to-point navigation, and independent primary and secondary surveillance operations towards a Next Generation Air Transportation System (NextGen) relying on digital communications, performance-based navigation (PBN), and Automatic Dependent Surveillance – Broadcast (ADS-B) to serve the needs of the 21st century. Enabling NextGen will place significant demands on existing CNS resources – both on the ground and in the air and will usher in a new set of threats, risks, and challenges for the NextGen "end state" and throughout the NAS' evolution to meet NextGen needs.

While the independence of CNS services have served the NAS well, the compelling capabilities provided by the Global Positioning System (GPS), the US's Global Navigation Satellite System (GNSS), and the FAA's Wide Area Augmentation System (WAAS) is enticing system designers to deviate from this NAS "foundation principle." GNSS position, navigation, and timing (PNT) services have found their way into many of today's CNS services, and while today independence remains intact and capable of mitigating single service outages, implementation of NextGen operational improvements (OI) will increase the challenges associated with a transition from a NAS operational *normal* to a NAS operational *nominal* environment. While the *nominal* environment is one in which independence of CNS services is maintained, a significant reduction in operational capabilities and efficiencies may be necessary to ensure safety and security is maintained.

Additionally, the 20th century NAS was always perceived and operated as a collaborative environment, with voice and data information shared by design on unsecured and unauthenticated communications channels. Infrequent *phantom* controller incidents were handled procedurally, navigation relied on high power ground transmissions using many different very high- and ultra high- frequency channels, and independent (primary) surveillance assured that all targets would be seen regardless of their desire/intent to cooperate. However the migration of the 20th century NAS to 21st century NextGen services entails a move to digital communications, satellite-based navigation and timing, and dependent surveillance. It is a different world, a world with new challenges and threats – challenges with which the information technology (IT) sectors have already had to deal. It would be prudent for us to follow their examples (and lessons learned) as an integral part of our migration to NextGen services, along with maintaining the FAA's *Safety First* principle and the independence of CNS services.

20th Century Principles	21st Century Threats
Open Communications	Spoofing
Independence	Reliance on critical system

It is also prudent to utililze existing NAS assets to address CNS requirements and threats in the 21st century and to design safe and efficient systems with an underlying core capability required by all of CNS applications (i.e., security, authentication, precise time, and integrity). To allow us to build efficient and safe systems we will need to adhere to some key constraints, including the need to trtansition and integrate legacy systems and provided the necessary services in a safe, secure, yet limited bandwidth environment.

NAS CNS SERVICES TODAY

To fully appreciate the challenges associated with migrating the NAS to NextGen, it is prudent to first review the state of current CNS service delivery as a basis for assessing risks, issues, and opportunities that will present themselves through the transition.

Communications. Flying in the NAS requires numerous interactions between aircraft and air traffic control consisting of three main elements – negotiation of an aircraft's flight profile; formal request and acceptance of the to-be-flown clearance; and the execution of the clearance. Communications services rely on Very High Frequency (VHF) communications transceivers[1] located at thousands of locations throughout the NAS, connected to air traffic controllers by an extremely robust communications network. While today, the majority of these transmissions are analogue voice communications, the migration to digital communications has already begun and will eventually represent the normal mode of operation throughout the NAS.

Navigation. Navigation services in the NAS are provided to aircraft by ground-based systems, such as VHF Omnidirectional Ranges (VOR), Distance Measuring Equipment (DME), and Instrument Landing Systems (ILS); and via spaced-based capabilities by GPS and the WAAS. While VORs and VOR/DME support point-to-point navigation, DME-DME (with a certified inertial reference unit to bridge gaps in coverage) and GPS/WAAS support PBN area navigation (RNAV) and required navigation performance (RNP) operations.

Surveillance. While the FAA continues to provide primary radar services to Department of Defense (DoD) and Department of Homeland Security (DHS) customers, surveillance services are primarily provided via Secondary Surveillance Radar (SSR), an interrogation/reply system that utilizes ground-based UHF signals to interrogate an aircraft's transponder, which relies on a different UHF frequency. As this reply includes an aircraft's altitude as determined by its barometric altimeter, it allows a two-dimensional radar system to provide three-dimensional positioning.

CNS RADIO FREQUENCY SPECTRUM

Availability, access, and use of the radio frequency spectrum is a significant issue in the 21st century as both potential new providers of new digital capabilities and services and existing service providers challenge legacy frequency assignments and usage. In 2010, the proposed use of frequencies just below the GPS primary civilian frequency for ground-based systems galvanized the international navigation community and many US Government agencies to protect the GPS L1 spectrum. Their efforts took almost two years and certainly expended millions of dollars in both the public and private sectors to ensure this spectrum protection. Efforts continue to characterize the frequencies near GPS to determine where allocations might be made and at what power levels. Spectrum, in short, is a big issue, and one that is critical to the delivery of future NextGen CNS services.

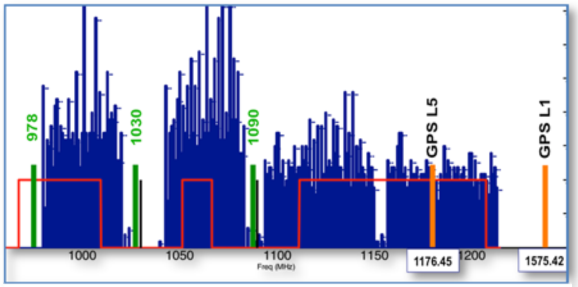
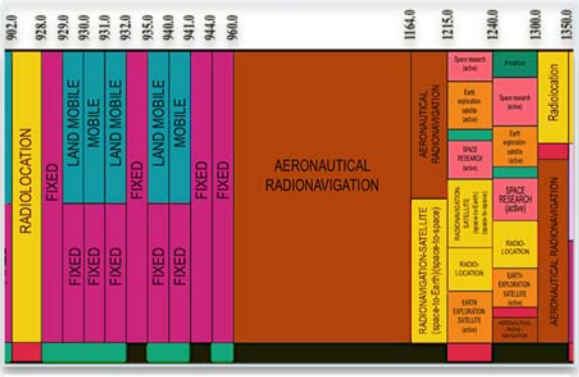


Figure 3 NAS CNS Services 960 MHz - 1215 MHz + GPS L1

While most air-to-ground communications, VORs, the Ground Based Augmentation System's (GBAS) data channel, and the Localizer (LOC) portion of the ILS utilize VHF


902.0
928.0
929.0
930.0
931.0
932.0
935.0
940.0
941.0
944.0
960.0
1164.0
1215.0
1240.0
1300.0
1350.0
RADIOLOCATION
FIXED
LAND MOBILE
MOBILE
LAND MOBILE
FIXED
LAND MOBILE
MOBILE
FIXED
FIXED
FIXED
FIXED
FIXED
FIXED
FIXED
AERONAUTICAL RADIONAVIGATION
AERONAUTICAL RADIONAVIGATION
RADIONAVIGATION-SATELLITE (space-to-Earth)(space-to-space)
Space research (active)
Earth exploration satellite (active)
SPACE RESEARCH (active)
RADIONAVIGATION SATELLITE (space-to-Earth) (space-to-space)
RADIO-LOCATION
EARTH EXPLORATION SATELLITE (active)
Amateur
Space research (active)
Earth exploration satellite (active)
SPACE RESEARCH (active)
RADIO-LOCATION
EARTH EXPLORATION SATELLITE (active)
AERONAUTICAL RADIO-NAVIGATION
Radiolocation
AERONAUTICAL RADIONAVIGATION
Figure 2 L-Band Radionavigation Spectrum

[1] FAA radio sites also include Ultra High Frequency (UHF) transceivers used to communicate with Department of Defense aircraft.

frequencies, and the ILS Glide Slopes (GS) uses lower UHF frequencies, signals from DMEs and GNSS systems use a portion of the UHF spectrum between 1000 and 2000 MHz known as the L-band. Figure 2 depicts a portion of this band. The spectrum between 960 MHz and 1215 MHz used by DMEs and Tactical Navigation Systems (TACAN) is internationally allocated and protected for Aeronautical Radionavigation Service (ARNS) use. It is located just above frequency allocations used by fixed and mobile communications services and, if not reserved for ARNS use, would be extremely valuable to cellular and other telecommunication service providers. Figure 3 shows the services provided within this ARNS band. The 1 MHz-wide channels shown in blue are the aircraft interrogations of DMEs and the DME responses. Mode S secondary surveillance radar interrogations and replies use the 6 MHz wide 1030 MHz and 1090 MHz channels, as does the ADS-B system, which also uses the 978 MHz channel for its Universal Access Transceiver (UAT) services and 1090 MHz for its Mode S ES. The new second GPS civil frequency, L5, uses 1176.45 MHz and the primary GPS L1 frequency uses 1575.42 MHz. Finally, the areas under the red line show frequencies used by the DoD Joint Tactical Information Data System (JTIDS) in accordance with an agreement between the US Department of Defense and the US Department of Transportation, that supports aviation safety, national defense, and efficient use of government resources.[2]

The fact that both navigation and surveillance services occupy a portion of the electromagnetic spectrum whose characteristics are so favorably suited for robust telecommunications (i.e., information exchange) presents a compelling opportunity to synergize 21st Century CNS services, better utilize valuable spectrum resources, and minimize both ground-based and airborne equipment diversity – all without impacting CNS independence or resilience. There may even be a potential to vacate existing channels in other parts of the spectrum if services currently residing there can be migrated to the L-band spectrum, where 21st century information technology initiatives can be implemented in a standard and holistic manner.

21st CENTURY NAS CNS CHALLENGES

To meet the CNS needs of the Next Generation Air Transportation System (NextGen), changes to the way in which CNS services are provided must be enacted – not only to ensure the 20th century metrics of accuracy, availability, integrity, and continuity service aspects, but to provide the 21st century cyber security demands for ensuring knowledge and trust of the source of these services (authentications) and establishing a clear, irrefutable record from whence these services/information/data are derived (non-repudiation). The safety, capacity, and efficiently of NextGen NAS operations will depend on the timely transfer of trusted information – both operationally essential and advisory. The CNS service delivery methodologies of the 20th century must give way to the secure information transfer methodologies of today, to a large extent by learning from the hard lessons of IT system developments, implementations, and use. The question is not "How can this be accomplished?" but "Where do we start?" The proposed answer is – "Start with our strengths."

There is good news. If this were a commercial project, a key issue from the outset would be to somehow identify limited and costly spectrum resources and transmission capabilities to support the required information transfer and system coverage needs (and in the case of navigation, provide the necessary geometry to achieve the required positioning accuracy). Even if spectrum could be found and made available at an affordable price, the task of identifying required locations and securing thousands of UHF transceiver sites would undoubtedly be extremely costly, time consuming, and risky. Interconnecting all of these sites with high speed, highly reliable, redundant communications links to support the provision of safety services would be a monumental effort. Fortunately, from the FAA

[2] Memorandum of Agreement between the Department of Defense and the Department of Transportation Regarding the 960-1215 MHz Frequency Band, December 2002

perspective, the majority of this effort has already been accomplished and is already in place providing today's NAS CNS services. It is these networks, migrated to serve the needs of NextGen, which can form the basis for the holistic 21st century provision of CNS services. The interconnection of thousands of NAS CNS sites exists today and each of these sites already has UHF/L-Band transceiver capability. Discussion of the challenges of using/ modifying/evolving these current L-Band resources to better utilize the spectrum, maximize services, minimize avionic equipage, and meet the cyber security challenges needs of the 21st century NextGen is the focus of the remainder of this paper.

CURRENT L-BAND SERVICES

DMEs (and their TACAN counterparts) are the primary users of the 960 MHz – 1215 MHz portion of the L-band spectrum. Aircraft determine their slant range distance to a DME by interrogating the DME on one channel and listening for the DME's echoed response on a channel 63 MHz above or below the interrogation channel, as show in Figure 4. By using two DMEs in "good" geometry, along with its barometric altimeter, an aircraft's Flight Management System (FMS) can determine its position in space and support area navigation (RNAV) procedures. Because of the robustness of the DME infrastructure and the relatively low update rate required (especially if an inertial reference unit (IRU) is included), DME-DME RNAV is able to suffer significant signal collisions and loss of signals while still maintaining the required availability and continuity of service.

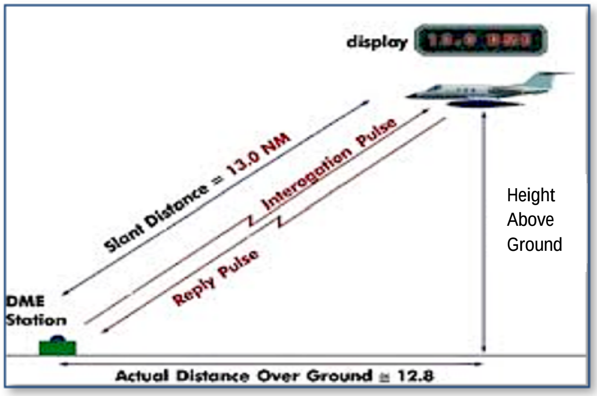


Figure 4 Use of DME to Determine Slant Range

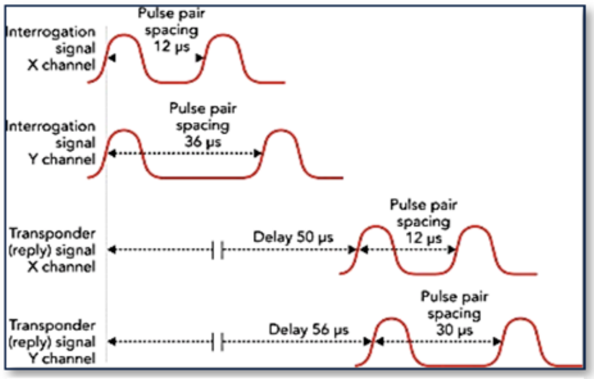


Figure 5 DME Channel Interrogations/Replies

An aircraft's DME interrogations consist of Gaussian pulse pairs precisely spaced in accordance with international standards. The DME equipment on the ground responds to interrogations with the echoed pulses, delayed by precisely 50 µs. This interrogation/reply mechanism is shown in Figure 5. By measuring the total time between its interrogation and receipt of the DME replies, subtracting out the 50 µs delay, and dividing in half, the aircraft calculates a true slant range to each DME. The good news is that the system works extremely well. The challenge lies in the fact that that this very valuable spectrum could support many more and challenging applications while still maintaining service to legacy users.

Each Gaussian pulse, whether initiated by the aircraft or by the ground-based DME or TACAN, is actually the envelope of a gigahertz frequency electromagnetic wave. While the shape of the envelope and time between pulses are important to legacy DME navigation equipment, the phase characteristics of the underlying carrier wave is not. Additionally, while the spacing between the pulses is important, the tolerance of this spacing (documented in standards developed in the mid-20th century) is sufficient to support pulse position modulation techniques, as well. Finally, additional unused pulse pairs may be modulated via their time of transmission allowing (pulse pair position modulation or PPPM) for additional data capacity. PPPM can be used in conjunction with the previously described data modulations.

This presents a real opportunity to utilize the DME carrier as a robust, highly frequency, diverse, 1 MHz-wide, 1 kilowatt power data channel – a data channel that can transfer information both from the ground to the aircraft and from the aircraft to the ground – as both a broadcast service and as an addressable, point-to-point network.

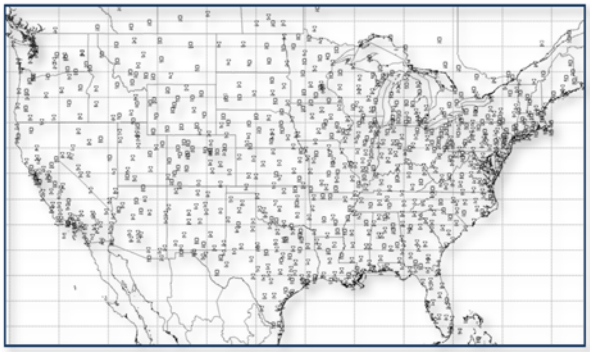


Figure 6a DME/TACANs in the NAS Today

While Figure 6a shows that there are approximately 1100 DMEs/TACANs operating in the NAS today, these are not the only L-band transmitters/locations of opportunity that should be considered. There are also ~700 ADS-B sites in the NAS that also broadcast and receive high power (400 W/500 W) signals in the L-band – on 978 MHz, 1030 MHz, and 1090 MHz. All of these facilities could be incorporated into a robust and geographically dense information network, as shown in Figure 6b. Then there are the en route and terminal SSRs, which broadcast their interrogations on 1030 MHz and receive replies on 1090 MHz – on 6 MHz wide channels! These also could be incorporated into this network. Finally, all of the interconnected air-to-ground communication sites are excellent candidates for future L-band communications hubs as well. The basis for and potential benefits of creating this robust and resilient aviation information network are immense.

As always, the devil is in the details – the primary question being the methodology by which one should modulate DME transmissions (and the 978 MHz, 1030 MHz, and 1090 MHz ADS-B and SSR signals) to provide maximum bandwidth to support multiple CNS broadcast, point-to-point, safety critical, advisory, and even command and control applications – without adversely affecting existing CNS services and providing a clear transition path for the FAA and all NAS users. Let's explore the possibilities by first looking at the necessary characteristics of a Secure Authenticated Information Link (SAIL).

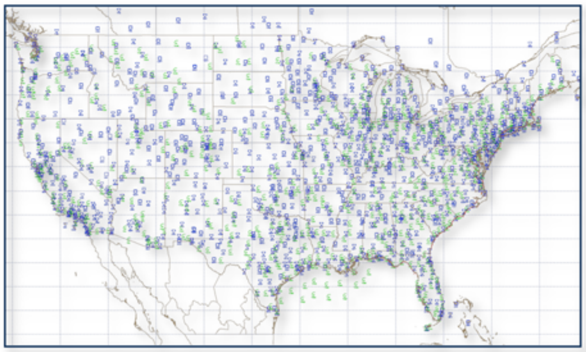


Figure 6b DME/TACAN/ADS-B Infrastructure Today

BASIC VALIDATED IT LINK SERVICES

In developing a SAIL, it is valuable to first define the basic, minimum link services that a link will provide as "overhead functions" to each individual information link "tenant" application. For a SAIL to best support current and emerging CNS tenant applications, it is proposed, as a minimum, that these services include:

- Transmission of precise clock information (to the nanosecond level) to both timestamp messages and support synchronous information transfer;
- Assured identification (authentication) of the source of each transmission; and
- Confirmation to information/service originators that the intended recipient(s) did, in fact, receive the information that was transmitted (non-repudiation).

There are multiple reasons for including a precise, nano-second-level time service as part of a SAIL's overhead services. First, maximum utilization of finite spectrum resources demands that we be able to slice the spectrum thinner and thinner – either in the time domain or the frequency domain. Either way, a highly precise clock is required. Additionally, synchronizing the clocks on the ground with the clocks in the aircraft enables synchronous data channels that maximize throughput, supports secure data transfer/cryptography, and provides an effective mitigation against re-broadcasting spoofing attacks.

Assured identification (authentication) of each transmitter ensures that the information being transmitted to support aircraft CNS functions comes from a trusted source. The days of implicitly trusting all parties using and interfacing with the NAS are long gone. Due diligence today means trust, but verify. This is especially important as we migrate to ADS-B, where surveillance is dependent on aircraft communications and navigation.

Just as authentication ensures that information used by receiving aircraft and ground systems is traceable to trusted parties, there may also be cases when the transmitting aircraft and ground systems must be able to prove that the CNS transmissions were, in fact, received correctly. This service is known as non-repudiation.

AN INTERESTING OBSERVATION

When one looks at the basic, minimum services SAIL should provide to its tenant applications, it becomes apparent that it is, in fact, these very services that are both necessary and sufficient to support an independent navigation function. If each known-location ground-based transmitter sends its trustable identification (station identification + authentication) along with the precise time-of-transmission (to the nanosecond level), aircraft can use this information to determine pseudoranges to multiple ground transmitters and determine their position. While the use of pseudoranges mimics the use of GPS satellites for navigation, the ground-based pseudolite transmissions would have the benefit of being high power, emanating from fixed locations (i.e., no ephemeris corrections), and travel relatively short distances (i.e., no iono corrections). Multipath concerns, however, will still need to be addressed.

Therefore, it appears that after providing the basic, minimum SAIL services that meet all navigation needs, any remaining bandwidth available via the selected modulation schemes should be allocable to communications and surveillance services.

DME MODULATION ALTERNATIVES

As shown in above in Figure 5, DME interrogations and replies consist of Gaussian pulse pairs with specific spacing between the pulses: 12 µs for X channel interrogations and replies and 30 µs for Y interrogations and 36 µs for Y channel replies.[3] The spacing is measured between the 50% maximum voltage amplitude point on the leading edge of the pulses with an allowable tolerance of ±0.25 µs. Both pulse rise and decay time is specified as 2.5 µs (+0.5 µs, -1.0 µs).[4] Given that these specified requirements were developed well over half a century ago, there appears to be wiggle room (no pun intended) to modulate both the spacing between the pulses and the phase of the carrier signal to support a robust SAIL.

Inter-pulse Spacing

The inter-pulse spacing tolerance of ±0.25 µs offers up the means to delay or accelerate the transmission of the second pulse relative to the first in multiple steps. Assuming a clock stability on both the transmitting and receiving end accurate to 0.25 ns, it would appear quite feasible to pulse position modulate the second pulse into X discrete slots, yielding Y bits of information per pulse pair. Given that the capability of current DME transmitters varies from 2700 pulse pairs per second (pps) for older equipment up to 5400 pps for the latest units, the potential data rate using this modulation technique would yield at least 4280 bits per second (bps), including the required error correction, which would reduce the effective data rate. This assumes a three level modulation.

Carrier Phase Modulation

The ability to alter the phase of the carrier describing the Gaussian pulse pairs is contingent upon three factors – first, that the peak power difference between any pair of pulses not exceed 1 dB; second, the modulation scheme ensures that the required effective radiated power stays

[3] Note: Although a Z channel is defined having 50 µs between pulses for both interrogations and replies, Z channels are not used in the US NAS at this time.

[4] FAA DME Performance Specification FAA-E-2996, April 1, 2008, para. 3.2.6.

within the required band, and lastly that the ability to detect the phase differences is unaffected by Doppler affects as aircraft fly to or from the transmissions. The solution for the first two constraints will be choose an appropriate modulation scheme that limits such products and distortions (e.g., Gaussian Minimum Shift Keying). The solution for the third constraint may be to ensure that phase modulation occurs only following the rise of the first pulse, thus being able to use the phase of the carrier during the rise time as a zero phase reference from which phase changes can be measured regardless of Doppler affects. The assumption is that the phase of carrier under the first pulse and the second pulse are the same and the spacing between them is the result of blanking and not on/off actions that could affect the phase relationship. Still, care will be necessary in the design to ensure preclude detrimental cross interference between PPM and carrier phase modulation.

ADS-B SUPPORT FOR HOLISTIC CNS

ADS-B is a system used for aircraft surveillance whereby each ADS-B equipped aircraft continuously broadcasts its identification and position for use by the ATC system and other aircraft. In the United States, the ADS-B system consists of ~660 ground stations and several master stations and is supported on two protocols: 1) Mode S Extended Squitter (ES) transmitting on 1090 megahertz (MHz) and 2) Universal Access Transceiver (UAT) transmitting on 978 MHz. A typical ADS-B ground station is shown in Figure 7, and consists of an omnidirectional UAT (978 MHz) antenna and four directional Mode S ES (1090 MHz) antennas. Each of these transmissions provide an L-band capability to support CNS services, albeit in different ways from each other and the neighboring DME/TACAN transmissions.

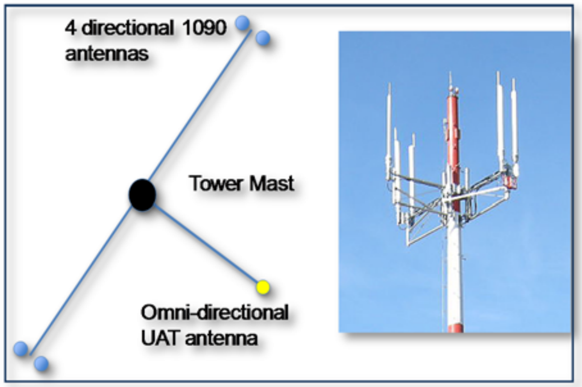


Figure 7 An ADS-B Ground-Based Transmitter

Universal Access Transceiver (UAT)

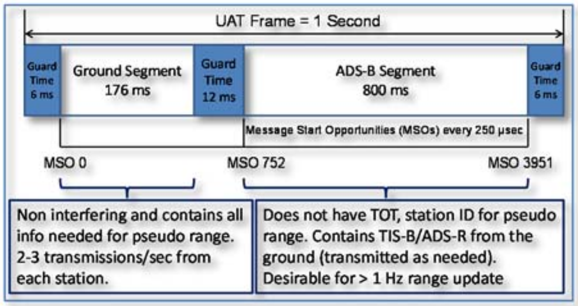

UAT Frame = 1 Second
Guard Time 6 ms
Ground Segment 176 ms
Guard Time 12 ms
ADS-B Segment 800 ms
Guard Time 6 ms
Message Start Opportunities (MSOs) every 250 µsec
MSO 0
MSO 752
MSO 3951
Non interfering and contains all info needed for pseudo range. 2-3 transmissions/sec from each station.
Does not have TOT, station ID for pseudo range. Contains TIS-B/ADS-R from the ground (transmitted as needed). Desirable for > 1 Hz range update

Figure 8 UAT Transmissions for Ranging in UAT Frame

UAT is a new signal developed specifically to support ADS-B services – both surveillance and the delivery of data (e.g., traffic and weather) to aviation users. It operates at 978 MHz, already has an existing basic passive ranging capability, and has several features that can be used to support other ranging functions (e.g., periodic messages to support a degree of synchronization to Coordinated Universal Time (UTC) USNO). Figure 8 shows the makeup of a UAT data frame.

The UAT frame is 1 second long starting on the UTC second, as shown in Figure 8. It is divided into two segments: Ground and ADS-B. Transmissions are only allowed to start at specified Message Start Opportunity (MSO), which are separated by 250 microseconds (µs). In the Ground segment, only transmissions from ground stations are allowed. There are 32 transmission opportunities, or slots for ground transmissions. Not all MSOs are used with the slots separated by 22 MSO. Each ground station transmits in 1-4 designated slots, which are organized for data. This results in a more challenging scenario for use of UAT for navigation. The ground segment messages are 4.2 milliseconds (ms) long and adjacent slots are separated by 5.5 ms. Hence, a message from one slot is unlikely to interfere with that transmitted in another, which minimizes intra-system interference.

UAT is also designed to support a comparatively high data capacity – 3456 payload bits in the ground segment and 144 or 272 payload bits for a basic or long message in the ADS-B segment. This is significantly higher than the Mode S ES transmission, which contains only 88 payload bits comprised of a 56 bits message field and 32 bits for message and address information.

The UAT signal still has several limitations: 1) it only allows for a roughly 1 Hz range update rate; 2) it only allows transmission timing variations of up to 500 nanoseconds (ns) off UTC; and 3) it can have significant multipath errors relative to accuracy and integrity targets. Still, as a contracted services, the potential is certainly there to *improve* these characteristics in the future to continue support of surveillance and data transmission services while utilizing these high power L-band transmissions to also support resilient performance-based navigation.

1090 MHz Mode S Extended Squitter

ADS-B is also transmitted using Mode S Extended Squitter (Mode S ES) on 1090 MHz. Mode S ES is an international standard for ADS-B and the preferred option for commercial air carriers. This 5 MHz bandwidth signal could be beneficial for ranging as it has greater multipath resistance than UAT. This is shown in Figure 9.

However, there are several limitations to using Mode S ES: (a) it does not have a built pseudo ranging capability; (b) it has limited data capacity; and (c) the 1090 MHz spectrum is already congested. Overcoming these limitations presents a significant challenge – solving the first two implies the need for new transmissions, which would further congest the spectrum and exacerbate the interference environment. Therefore, it would appear that the only prudent course of action would be to design ranging capabilities on Mode S ES that leverages as many existing transmissions as possible and find a means to use them to best support Holistic CNS.

Furthermore, Mode S ES also has the potential for increased data capacity. Like DME, current transmission use only is concerned with the envelope. Hence, Mode S ES phase modulation is a potential means of increasing data capacity without affecting existing users.

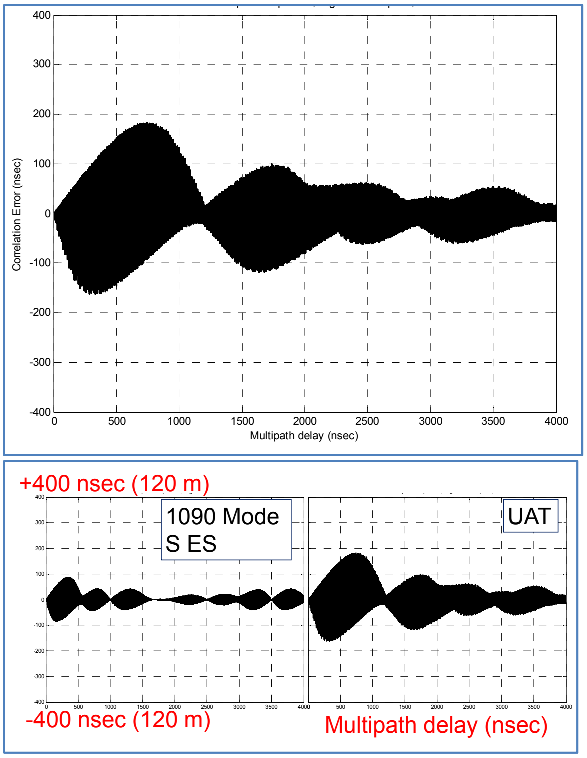


Figure 9 Multipath Envelope of Mode S ES and UAT for -6 dB power multipath

As shown in Figure 7, the ADS-B UAT and 1090 MHz transmission originate from the same tower of different antennas – antennas that are physically in relative close proximity to each other – approximately 10 feet apart. Thus, if we can derive time of transmission information from the UAT transmission and use it to learn the time of transmission of the 1090 MHz signal, we will have both a 1 MHz narrow UAT signal and a 6 MHz wideband to support ranging – each contributing its own benefit to the overall navigation solution.

Combined use of the two ADS-B protocols has some attractive features. First, the strongest points of each protocol can be leveraged to overcome weaknesses of the other. For example, as will be seen in the passive ranging designs, UAT with its higher data capacity would be used to provide data while existing Mode S ES could provide additional ranging measurements that are less affected by multipath. Another benefit is that they could be

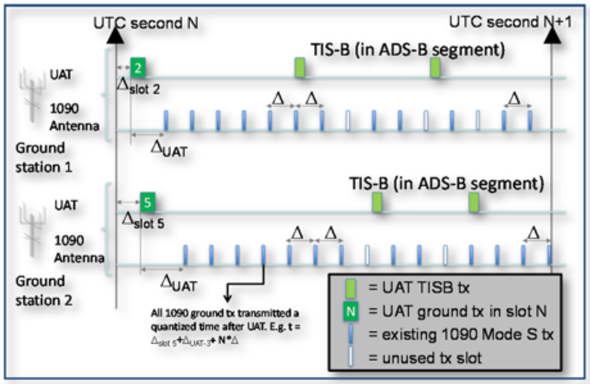


Figure 10 Transmission Concept to Use UAT and 1090 MHz Mode S ES to Support Pseudo Ranging

used as part of an interrogation-reply system to potentially provide true ranging without additional transmissions. Figure 10 shows a concept by which this could be accomplished.

THE REQUIREMENTS FOR INFOSEC

Authentication provides assurance to users of the data and source of a transmission and, in the case of a transmission used for positioning and navigation, it needs to provide a level of protection against spoofing the ranging elements of the signal. Designing the "right" authentication methodology for a specific application is always a balance between the required level of assurance, based on the analysis of potential "threats" and the characteristics of the data channel – without affecting the link availability or integrity. This is not a simple task – it is important to note that authentication is complicated and this discussion is meant as an overview and is not meant to cover, in detail, all of the important considerations involved. It is, however, an essential part of a 21st Century CNS solution and the following is provided to "open up" the discussion.

To develop a sufficiently strong authentication capable of defeating data spoofing over the lifetime of the system (which in the aviation sector is decades in duration) it is prudent to leverage an existing digital message authentication (DMA) because it uses an existing algorithm, has the benefit of already being extensively tested, and there is existing software and hardware available to support its implementation. As a proof-of-concept design, an elliptic curve digital signature algorithm (ECDSA) was chosen because it is one of the two most widely used signature schemes and is standardized by the US National Institute of Standards and Technology (NIST). ECDSA is implemented "in line", where the signature is treated as additional information appended to the end of the data to be authenticated. Hence, there is no alteration of the original data transmitted and the signature is either additional data within the message or contained in a new message. Additionally, the time of transmission information can be added in the hash generation, which encodes the time into the signature to prevent later replay of the message and provides some protection against range spoofing. Generically, this implementation is shown in Figure 11.**Error! Reference source not found.**

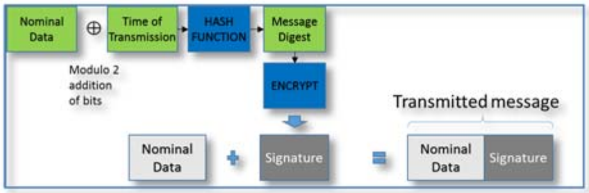


Figure 11 Generic Implementation of Digital Signatures on Data Transmission

ECDSA is based on asymmetric cryptology, where the signature is generated by the *Service Providers* (SPs), such as an Air Navigations Service Provider (ANSP) like the FAA, with a secure private key. With each private key is a corresponding public key, and each station may have its own private key. The private key does not need to be distributed because it is not needed to verify the signature. Instead, the airborne fleet would carry a public key to verify the signature of the SPs, but which could not be used to discover the private key or counterfeit the signature. While discussion of secure public key distribution is not included in this paper, it should be noted that there are several mechanisms within the aviation community by which this could be accomplished.

In ECDSA, the signature is a pair of elements (*S*, *H*), where S is a number derived from the elliptic curve used and H is the output dependent on the hash function of the data to be authenticated. NIST (2012) recommendations suggest an elliptic curve of 256 bits or more be used for systems that will operate beyond 2030. Larger elliptic curves (384 and 512 bits) are suggested if used well beyond 2030. Given this consideration and the *longevity* of aviation systems, it is prudent to employ 512-bit signatures (256 bits S and 256 bit H). However, if this proves to require too much of the available bandwidth, it is possible to use a variant of ECDSA, due to Schnorr. With Schnorr signatures, a NIST standard elliptic curve called P256 is used; however the hash size is reduced from 256 bits to a lower value.

The data rate required to support authentication depends on how often authentication needs to occur and the minimum time to authentication. For example, if integrity alerts need to be authenticated within a six- or ten-second time-to-alarm, authentication would need to occur every couple of seconds. If, for example, data authentication is required every second, 512 bits per second would be desired to support this capability.

The means to incorporate authentication is dependent on the specific characteristics of the intended data channel. For example, an APNT modulated DME L-band data channel could transmit 1000-bit long messages every second. Within this system, both the desired data and the ECDSA signature can be contained in each message as shown in in Figure 12. In contrast, a different implementation would be needed for ADS-B Mode S ES, which has messages with 88 bit payloads. Hence, each ECDSA signature would require seven messages. This ECDSA signature would have to authenticate multiple Mode S ES transmissions as it does not make sense to use seven messages to authenticate one or two nominal messages. Additionally, message loss must also be accommodated, as loss of any message would prevent authentication. A fountain code-based algorithm can be used to generate additional "recovery" messages, whose purpose would be recover the nominal data or signature should some messages be lost. This is shown in Figure 13. As seen from the examples, the implementation of the same authentication scheme can differ depending on channel characteristics.

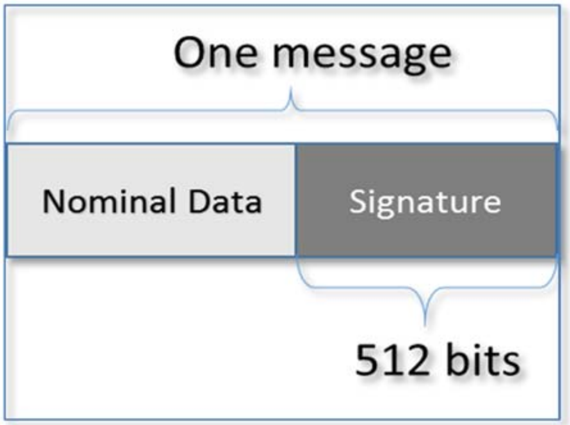


Figure 12 Example Implementation of Authentication for a Channels with High Data Capacity Messages (> ~ 700 bits per message). Data and Signature fully contained within one message

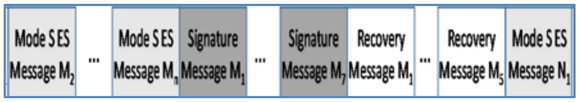


Figure 13 Example Implementation of Authentication on Channels with Low Data Capacity Messages (< ~500 bits per message) such as Mode S ES (88 bits per message). Seven messages contain the signature, which authenticates M_n prior messages. Recovery messages are included to recover loss messages (otherwise the user would be unable to authenticate with message loss).

CONCLUSION

The L-band spectrum between 960 MHz and 1215 MHz currently used for air navigation and surveillance services has the potential to support existing services while also offering the opportunity to not only incorporate a robust and resilient communications capability, but also to introduce authentication capability for all CNS services. This paper offers a mechanism whereby this can be achieved without impacting existing services within the band and a means to migrate these services to a model more compatible and compliant with the needs of 21st century users.

It should be noted that this paper is meant to open a dialogue between the communications, navigation, and surveillance communities to focus on the best means to ensure that each service can benefit from a new methodology without impacting current or future capabilities. In the end, there can be no forward progress without a win-win-win strategy and goal that all embrace.

Mitch Narins is the FAA's Chief Systems Engineer for Navigation Programs, a Certified Information System Security Professional (CISSP), and a Fellow of the Royal Institute of Navigation (FRIN).

Sherman Lo is a senior research engineer at the Stanford University GPS Laboratory.

Per Enge is the Vance D. and Arlene C. Coffman Professor in the School of Engineering at Stanford University and the director of the Stanford GPS Laboratory.

Yu-Hsuan Chen is a Postdoctoral Scholar in GPS Laboratory at Stanford University. He received his Ph. D in electrical engineering from National Cheng Kung University, Taiwan in 2011.