REQUIREMENTS FOR AN INTEGRATED UAS CNS ARCHITECTURE[1]

Fred L. Templin, The Boeing Company, Seattle, WA

Raj Jain, Washington University in Saint Louis, St Louis, MO

Greg Sheffield, The Boeing Company, St Louis, MO

Pedro Taboso-Ballesteros, The Boeing Company, Madrid, Spain

Denise Ponchak, NASA Glenn Research Center, Cleveland, OH

Abstract

The National Aeronautics and Space Administration (NASA) Glenn Research Center (GRC) is investigating revolutionary and advanced universal, reliable, always available, cyber secure and affordable Communication, Navigation, Surveillance (CNS) options for all altitudes of UAS operations. In Spring 2015, NASA issued a Call for Proposals under NASA Research Announcements (NRA) NNH15ZEA001N, Amendment 7 Subtopic 2.4. Boeing was selected to conduct a study with the objective to determine the most promising candidate technologies for Unmanned Air Systems (UAS) air-to-air and air-to-ground data exchange and analyze their suitability in a post-NextGen NAS environment. The overall objectives are to develop UAS CNS requirements and then develop architectures that satisfy the requirements for UAS in both controlled and uncontrolled air space. This contract is funded under NASA's Aeronautics Research Mission Directorates (ARMD) Aviation Operations and Safety Program (AOSP) Safe Autonomous Systems Operations (SASO) project and proposes technologies for the Unmanned Air Systems Traffic Management (UTM) service.

Communications, Navigation and Surveillance (CNS) requirements must be developed in order to establish a CNS architecture supporting Unmanned Air Systems integration in the National Air Space (UAS in the NAS). These requirements must address cybersecurity, future communications, satellite-based navigation & APNT, and scalable surveillance and situational awareness. CNS integration, consolidation and miniaturization requirements are also important to support the explosive growth in small UAS deployment. Air Traffic Management (ATM) must also be accommodated to support critical Command and Control (C2) for Air Traffic Controllers (ATC). This document therefore presents UAS CNS requirements that will guide the architecture.

1. Introduction

In a companion paper [1], we discuss considerations that affect CNS requirements. These considerations include UAS classes, UAS Mission Classes, UAS demand forecast, etc. Using those considerations, this paper addresses requirements for communication networks (Layer 3), communication datalinks (layer 2), Navigation and Surveillance. Within each of these focused areas, requirements are based on individual mission needs as well as scaling to accommodate large numbers of UAS.

Requirements for communication networks are driven by mission needs for all UAS classes and demands. NASA has articulated a vision for an Unmanned Air Traffic Management (UTM) system [2] that will provide a communication network ensuring effective C2 coordination. Small UAS operating in uncontrolled airspace will initially be controlled by ground pilots who must be reachable through on-demand C2 communications from the UTM ATC. Ground pilot requirements will diminish as greater levels of UAS autonomy are incorporated according to regulatory and technical advancements to the point that UTM ATC will eventually require direct C2 communications with each UAS. Similarly, large UAS operating in controlled air space must be under active C2 coordination with UTM ATC at all times. Communication network requirements therefore include a global UTM internetwork, global addressing for pervasive UAS C2 tracking, multilink support, scalability, global

mobility support, and tactical communications for off-nominal conditions.

Communication datalink requirements include range, velocity, latency, availability, integrity, security, and bit rate. The pilot may have a direct link to UAS when in radio line of sight (RLOS). Beyond RLOS, pilots will use cellular or satellite links. We concentrate on the bi-directional wireless datalinks that connect directly with the UAS. The range refers to the transmission distance of the last hop of the network to the UAS. For missions operating in the controlled airspaces and at airports, the datalinks for communication on the ground, take-off, or in flight may be different and have different range, velocity and latency requirements.

Regardless of UAS size and mission, all UASs require navigation accuracy supporting guidance and control within a given airspace (e.g., Class A – G). To allow UAS to operate within controlled airspace, a certified navigation source will be required on all UAS to ensure accuracy of location being reported to both UTM and ATM systems. UAS navigating within uncontrolled airspace will require at least GPS-like accuracy for areas of operation with confidence of avoiding terrain and non-cooperative objects. UAS will require better than GPS-like accuracy when operations need to be closer to the terrain, spacing tighter being aerial vehicles, and for quicker response to non-cooperative object detection and avoidance. Overall, UAS navigation requirements are driven by safety of flight and mission needs for all classes of airspace operations.

In terms of surveillance, requirements are focused on providing novel systems to fulfill the needs of the upcoming UAS paradigm. These requirements will be used as a starting point to develop cooperative and non-cooperative surveillance systems. They will be developed with the objective to overcome the limitation of current surveillance systems (accuracy, saturation, ability to detect non-cooperative target, etc.). These new systems will make use of alternative transmission means (using IP-based channels) and of modern technologies such as image recognition, or radio frequency and noise signatures.

Requirements for each of the CNS focused areas must therefore lead the way to an integrated architecture that can accommodate the expected demand for integrating UAS into the NAS. These requirements must satisfy emerging regulations such as the FAA Part 107 amendment for small UAS operation [3]. In this paper, we present requirements intended to shape CNS technology identification and selection.

2. UAS CNS Requirements

We organize the UAS CNS system requirements according to the four focused areas of Communication Networks, Communication Data Links, Navigation and Surveillance. Within each of these focused areas, requirements are based on individual mission needs as well as scaling to accommodate large numbers of UAS. The following sections present the requirements.

2.1 Communication Networks

Requirements for communication networks are driven by mission needs for all UAS classes and demands. sUAS operating in uncontrolled airspace will initially be controlled by ground pilots who must be reachable through on-demand C2 communications from the UTM Air Traffic Control (ATC). Ground pilot requirements will diminish as greater levels of sUAS autonomy are incorporated according to regulatory and technical advancements to the point that UTM ATC will eventually require direct C2 communications with the sUAS. Similarly, large UAS operating in controlled air space must be under active C2 coordination with UTM ATC at all times.

The UTM global network will connect small and large UAS to UTM ATC throughout all flight phases and mobility patterns. All UTM correspondents (i.e., (s)UAS, ground pilots, ATC stations, etc.) are seen as UTM end systems in the global network. The following sections present requirements for both small and large UAS under all mission conditions:

REQ CN1: UTM Global Internetwork Service

A global Internetwork UTM service for UAS mission coordination is needed. The UTM service will be deployed as an overlay network layered on top of the global public Internet and will make maximum use of existing Internet infrastructure for

cost savings. The UTM service must use Internet Protocol version 6 (IPv6) [4] and use existing Internet access links such as 4G/5G cellular services, WiFi hotspots, satellite links, etc. The UTM service will be manifested through encapsulation of UTM messages within packet headers that can be routed across the Internet as shown in Figure 1 below.
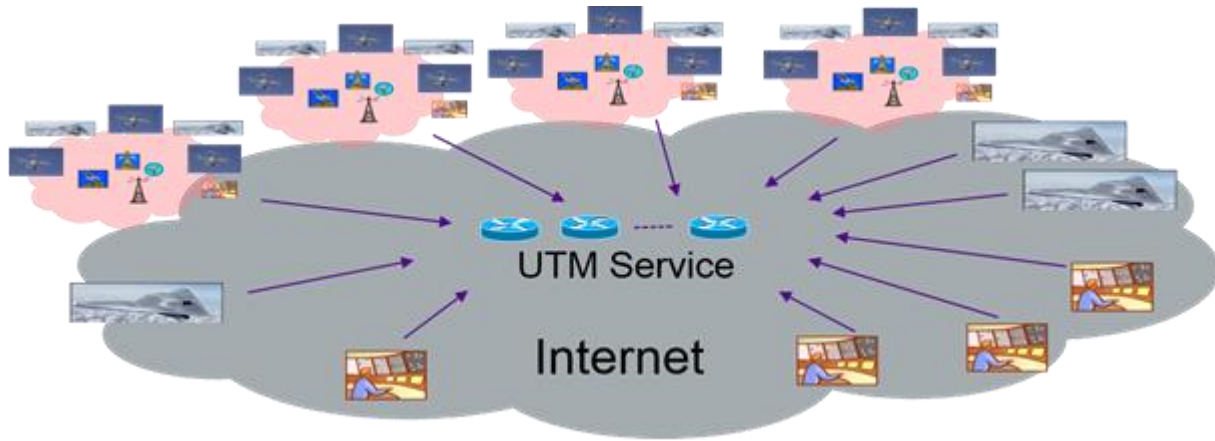

Figure 1 - UTM Global Internetwork Service

REQ CN2: Global Addressing

Each UTM end system will require a global IP address or IP subnet prefix that can be used for the source and destination addresses of UTM packets. These addresses must be uniquely delegated to each UTM end system so that communications will unambiguously reach the correct destination, i.e., much in the same way that our cellphones have a unique phone number allocated by our service provider. Since the IP version 4 (IPv4) [5] address space is depleted, only IPv6 can satisfy this requirement.

REQ CN3: Multilink Support

The communications network architecture must support multiple available data links on each UTM end system. The links may have different cost, performance, availability and integrity profiles during different phases of flight. But, the multilink UTM end system must be able to maintain a stable IP address or prefix that never changes even if the underlying data links change and must be able to orchestrate its available data links according to current mission requirements.

REQ CN4: Scalability

Scalable networks must be able to accommodate current load levels and future demand without depleting the available IP address pool and without overwhelming the network routing system. The UTM network must be designed as a scalable global network architecture beginning in the United States National Air Space (NAS). Small-scale early deployments must carry forward to support increasingly larger UAS populations. The system must also be designed to work in conjunction with the ATN/IPS service currently under formulation by ICAO for manned aviation [6].

REQ CN5: Global Mobility Support

UTM end systems will naturally travel between different data link points of connection during missions that extend beyond a single line-of-sight connection. Additionally, existing data links may become unavailable and new links may come into use through various phases of flight. When UTM end systems travel, their data link IP addresses may change, but their UTM network IP addresses must remain stable and unchanging. UTM end systems must therefore maintain single, stable IP address or prefix as nodes move between access network connections.

REQ CN6: Small UAS (sUAS) in uncontrolled low-altitude airspace

sUAS will operate in uncontrolled airspace between 200-400ft. As sUAS incorporate more and more levels of autonomy, the ground pilot role will evolve into more of an advisory capacity rather than precision flying. There will soon be millions of sUAS registered in the US. Each sUAS must therefore support C2 communications for both ground pilots and UTM ATC for secure and pervasive control.

REQ CN7: Large UAS in non-segregated controlled air space

Large UAS will initially be under control of ground pilots who will coordinate with UTM ATC. As greater levels of automation are incorporated, the ground pilot's role will evolve into an advisory capacity. Within non-segregated controlled air space, however, UTM ATC active involvement will be critical for ensuring safe operations in conjunction with manned aviation

REQ CN8: Reliability

The UTM global network must provide a high degree of reliable message delivery. The service model for the Internet IP network layer is known as "best effort" where each packet is delivered if possible, but may be dropped due to unavoidable conditions such as link failures or network congestion. Since any packet originated from or destined to a UAS may contain safety-of-flight parameters, this means that the UTM will require "better-than-best-effort" reliability at the network layer. This can be accomplished through reliable network protocols such as the Border Gateway Protocol (BGP) [7] and through UAS multi-link management. Figure 2 depicts the multi-link concept for increased network-layer reliability.

REQ CN9: Security

As for all Internet-based communications, cyber-attacks against the UTM Internetwork and end systems themselves could lead to catastrophic failures and compromise safety of flight. UTM end system hijacking and C2 breaches are mitigated through strong end-to-end confidentiality, integrity and authentication, but a class of attacks known as Distributed Denial of Service (DDoS) poses a serious

threat for safe UTM operations. The architecture must therefore withstand DDoS attacks without disruption to UAS communications.
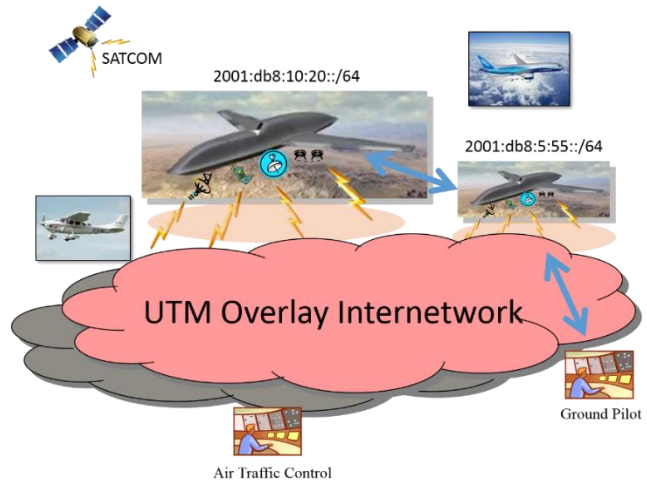

Figure 2 - UAS Multilink Operation

REQ CN10: C2 Messaging

Command and Control (C2) messaging allows ground pilots to control UAS, and allows ATC to communicate with ground pilots. sUAS pilots will require a more tactical messaging set that supports precision flying and near-real time communications. At the same time, ATC will require a means of C2 coordination with ground pilots at first, and then evolving to direct ATC C2 communications with pilot-less autonomous UAS as greater levels of autonomy are incorporated. The pilot-to-UAS tactical messaging set should be based on STANAG 4586 [8] or proprietary messaging, while ATC-to-pilot strategic messaging will use Controller-Pilot Data Link Communications (CPDLC) [9].

REQ CN11: SA Messaging

UAS can and do send streaming media content such as motion video and acoustic sensor data to ground controllers. This need will only increase as UAS are used more and more for aerial reconnaissance, televised sporting events, and any other UAS missions that produce multimedia data. The UTM network architecture must therefore support high data rate streams of correlated Situation

Awareness (SA) messages in addition to the non-correlated individual messages used for C2

REQ CN12: Off-Nominal Communications

Regardless of any communications network or data link layer adaptations, UAS will still occasionally travel outside of the coverage areas of all available communications systems leading to a condition known as "lost link". The UTM communications network must therefore observe lost link procedures and/or adopt Delay/Disruption Tolerant Networking (DTN) [10].

2.2 Communication Data Links

Figure 3 shows a simplified architecture of a UAS. The pilot controls the UAS and communicates with the air traffic control (ATC). The pilot may have a direct link to UAS when in radio line of sight (RLOS). Beyond RLOS, pilots will use cellular or satellite links. All wireless links are shown by dashed lines while the solid lines indicate links that are generally wired but can also be wireless. The capacities of solid datalinks are assumed to be sufficiently high to be of any concern. We concentrate on the bi-directional wireless datalinks that connect directly with the Unmanned Aircraft. Thus, the GPS links, which are unidirectional, are not included. Also, ground stations to satellite links that do not connect to the UAS are excluded.
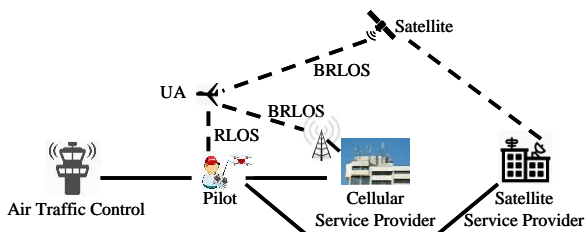

Figure 3 - Command and Control Data Links

REQ DL1: Range

The range refers to the transmission distance of the last hop of the network to the UAS. For example, in case, of GEO satellites, this distance is 35,786 km.

- For Category A and B missions [1] limited to visual line of sight, the range of the datalink should be at least 5 km.

- For Category C missions that go beyond VLOS, the range of the mission is limited by the on-board power. It is expected that the UAS can hand-off to the next ground transmission station as the signal from the previous transmission station decreases significantly. This is similar to driving on the highway. Therefore, ground-based datalinks should support at least 5 km.

- For Category D1 (UAS stationary in the airports), the range of 5 km is required. Larger airports may have multiple transmission towers to communicate with UASs stationed further away.

- For Category D2 (UASs in Taxi and Takeoff), the datalink should be able to support a range of 100 nm or 160 km.

- For Category D3 (UAs in flight), the datalink should be able to support a range of 1,000 km for ground based transmitter and 36000 km for satellite datalinks.

- For Category D4 (UAs in Oceanic areas), the datalink should be able to support 35,786 km.

REQ DL2: Velocity

Speed of the UASs affects the choice of the communication datalink technologies. For example, WiFi is designed for stationary objects and can work for objects moving at a low speed. WiMAX and most 4G/pre-4G cellular technologies are designed for cars moving at 100 km/hr.

- For Category A and B, the datalink should support at least 100 km/hr.

- For Category C, the datalink should support at least 100 km/hr

- For Category D1 missions, the datalink should support at least 100 km/hr.

- For Category D2 missions, the datalink should support a velocity of 1000 km/hr.

- For Category D3 missions, the datalink should support UASs traveling at 1000 km/hr

- For Category D4 missions, the datalink should support 2000 km/hr.

(Note that 100 km/hr is equivalent to 28 m/s).

REQ DL3: Latency

The round-trip latency affects how far the UAS can deviate from its trajectory. Assuming 10 m is an acceptable deviation (allowing 20 m minimum distance between sUASs), and 100 m is an acceptable deviation for larger UASs traveling at high-speed over ground and 200 m for aircrafts above the ocean, the latency requirements for all classes is 350 ms.

REQ DL4: Availability

The downtime of the link can affect the UAS missions. Therefore, it is important to put availability requirements. Normally, phone systems have an availability requirement of 5 nines (99.999% availability). Assuming the same for longer missions and assuming slightly less for shorter missions, the availability requirements are as follows:

- For Category A and B mission, the datalink availability should be more than 99.99%

- For Category C and D missions, the datalink availability should be more than 99.999%.

REQ DL5: Integrity

Integrity refers to the bit error rate. Bit errors can be recovered by various error correction and redundant transmission schemes. Wired Ethernet based links have an error rate of 10-9 while the wireless links have error rates in the vicinity of 10-3. These are detected bit error rates which result in packet discard. Undetected bit error rates should be extremely low since they can result in mission failure.

- The detected bit error rates should be less than 10-3 for all missions

- The undetected bit error rates should be less than 10-6 for all missions.

Note that Category C and D missions will be semi-autonomous or autonomous. Therefore, they can operate with the same level of packet loss as other categories.

REQ DL6: Security

It is difficult to measure security quantitatively. Currently, WiFi with WPA2 security is commonly used in all critical ground infrastructures and so we require that all UAS datalinks be at least as secure as WPA2. In particular, it is required that all messages be encrypted.

REQ DL7: Bit Rate

Datalink bit rate depends upon the level of autonomy. The fully autonomous operation will require lower data rates since the UAS does not need to wait for instructions from the pilot during flight. RTCA white paper [11] provide the an estimate of required bit rates as shown in Table 1 and Table 2 for uplink and downlink, respectively.

Table 1. Uplink Bit Rates

Activity	bps
Telecommand	4,593
Navigational Aid Setting	666
ATC Voice	4,800
ATS Data	49
Total	10,108

Table 2 - Downlink Bit Rates

Activity	bps
Telemetry	7,595
Navaid Display Data	1,137
ATC Voice	4,800
ATS Data	59
DAA	4,800
Weather	27,770
Video	270,000
Total	316,161

2.3 Navigation

Regardless of UAS size and mission, all UASs share the need for navigation accuracy supporting guidance and control within a given airspace (e.g., Class A – G). To allow UAS to operate within controlled airspace, a certified navigation source will be required on all UAS to ensure accuracy of location being reported to both UTM and ATM systems. UAS navigating within uncontrolled airspace will require at least GPS-like accuracy [12] for areas of operation with confidence of avoiding terrain and non-cooperative objects. UAS will require better than GPS-like accuracy when operations need to be closer

to the terrain, spacing tighter between aerial vehicles, and for quicker response to non-cooperative object detection and avoidance. Overall, UAS navigation requirements are driven by safety of flight and mission needs for all classes of airspace operations and will require a multi-source inertial navigation system (Figure 4). The following sections present requirements for UAS under all mission conditions.
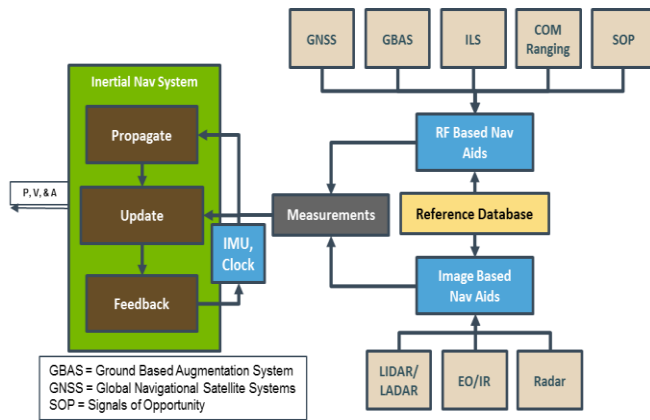

Figure 4 - Multi-source Inertial Navigation System Architecture

REQ NV1: GPS Augmentation

GPS signals alone are extremely weak due to high frequency and useless in certain environments, such as, low urban and deep canyon operations. To deal with GPS-denied condition, an alternate navigation system to augment GPS is needed. The following are some candidate navigation aiding systems:

- **Vision or image-based navigation system –** used to determine the position and attitude.

- **Signals of Opportunity Navigation System –** use of any and all signals for determining a navigation solution.

- **Cooperative Navigation System –** GPS (and GNSSs) like system for obtaining range measurements from beacons at known locations.

- **Assisted Navigation System –** system used to significantly improve startup performance (i.e., time-to-first-fix (TTFF)) of a GPS satellite-based positioning system.

REQ NV2: Certifiable Navigation Computing Architecture

Safety certification is needed to ensure safety of commercial aviation and to ensure safe integration of UAS into the NAS. UAS certification challenges related to software verification/validation requirements to operate in NAS will likely require rewriting code due to most existing software was not designed to be certifiable. Certification can be expensive, time consuming, and risky which can cost approximately $100 per each line of code to develop and defend artifacts. Therefore, a focus on a cost affordable certifiable UAS safety of flight computing architecture (Figure 5) to support navigation algorithms is desired for implementation on any size UAS operating within NAS.
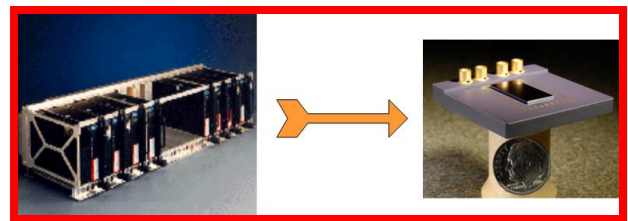

Figure 5 - Cost Effective Certifiable UAS Computing Solution

REQ NV3: Navigation Source Error Detection and Correction

Whether using GPS/GNSS/etc. or RF navigation aids the need for error detection and correction is required for UAS operating in the NAS. Today, most navigation systems do not require error detection and correction since these systems are implemented with a human in the loop with the ultimate responsibility for safety of flight during time of loss of GPS signals.

GPS signals are susceptible to interference and jamming. Civilian GPS signals are unencrypted, unauthenticated, and are publicly documented making GPS a target for intentional spoofing or jamming. In addition, GPS can become unavailable in a given geographical area because of Radio Frequency Interference (RFI) either non-intentionally (i.e., greater noise to signal ratio) or intentionally (i.e. spoofing). A spoofing attack is one where a malicious transmitter broadcasts a GPS-like signal with the intent to deceive GPS users. RFI can be the result of unintentional, off-band transmissions by otherwise

legitimate radio equipment (e.g., radios, TV broadcasts, radars, etc.) or a malicious jammer.

To detect and correct navigation errors from RF-based navigation systems (i.e. GPS), it is recommend to develop techniques for comparing RF-based navigation source calculations to non-RF-based navigation source calculation for real-time error detection and dynamic switching between navigation sources to maintain continuous position accuracy. The following is a list of candidate visual sensor sources for use on UAS to augment the loss of GPS or other regulatory approved RF-based navigation aids by means for error detection and correction:

REQ NV4: Ground Controlled UAS Navigation Accuracy

To properly define UAS navigation accuracy requirements for ground controlled UAS operations, two conditions have to be managed. First, the maneuverability (e.g., speed, rate of turns, climb, descent, etc.) profile for UAS has to be defined within a given airspace of operation. Secondly, the closed loop time has to be defined for worst case. Some of the factors impacting closed loop communications are: UAS navigation calculation processing time; Communication latency between UAS and ground station; Ground station command and control processing time; Communication latency between ground stations and UAS; and, UAS processing time to alter flight.

REQ NV5: Universal Navigation Message Schema

Up to now UASs are typically formed by a UAV and a control station designed to interact with each other as a closed system. Type of data-link, communication protocol, message format shall follow STANAG 4586 messaging schema for UAS operations. Next, additional and optimal message types need to be defined within STANAG 4586 to support exchange of navigation information.

REQ NV6: BLOS Navigation Accuracy

UASs have been used for beyond line of sight (BLOS) missions, especially for military use, where the operative scenario resulted to be very far from the control station position, the direct link range has a limitation for the UAS control. Then the use of satellite communication is utilized for controlling UASs. The use of satellite communication for UAS control has one major problem which is the time of the signals to travel BLOS. Therefore, the need for increase autonomous operations helps to reduce the latency problem requiring a high available navigation solution to be implemented.

REQ NV7: Autonomous Navigation Accuracy

Autonomously UAS landing on a stationary pad will need sensor capabilities to augment the human in a similar scenario of visual landing. Algorithms will need to be developed supporting sensor fusion framework producing estimates of the UAS state and a control system that computes appropriate actuator commands.

2.4 Surveillance

This section presents a series of surveillance requirements to satisfy the needs of novel surveillance systems in order to enable UAS operations within controlled and uncontrolled airspaces.

REQ SV1: Safety

It is imperative to develop surveillance systems that allow UASs to operate within both controlled and uncontrolled airspace without increasing the operations level of risk.

Surveillance systems to be developed shall focus on maintaining, and potentially increasing, current aeronautical safety criteria.

Safety analysis of the new systems shall be performed to demonstrate that such systems will provide the necessary performance in its nominal mode of operation.

REQ SV2: Capacity

Current surveillance systems such as SSR or ADS-B use the 1090MHz frequency band to operate [13]. This requirement makes the design and integration of new surveillance systems easier. However, in environments with high levels of air traffic density, the 1090 MHz data link works on close to saturation conditions.

The capacity of new surveillance systems shall be dimensioned to overcome the limitations of current systems. Instead of the 1090 MHz frequency,

surveillance systems shall rely on alternative datalinks and networks.

REQ SV3: Efficiency

Air Traffic Management (ATM) is evolving worldwide towards a more efficient way of flying with less emissions and more capacity for the airports and the airspace. This implies new procedures and new Communications, Navigations and Surveillance (CNS) technologies. Such technologies will modernize the current ATM scenario, but they will also represent opportunities for new security threats.

Surveillance systems to be developed shall contribute to fulfill the efficiency needs of the increasing air traffic density and complexity.

Especially challenging in terms of improving the ATM efficiency with an increase on the traffic operations as the one expected with the integration of UAS operations are those areas close to airports.

Surveillance systems to be developed shall also be designed with the objective of having an efficient performance. The principle of best effort shall be applied in order to minimize the use of the available bandwidth and the impact over the communication network underlying the surveillance applications.

REQ SV4: Security

Legacy surveillance systems were designed with a functional dimension but not with a security one. They present very few or no security measures. The information managed by current surveillance systems is accessible to anyone having a receiver without any special restriction. The easy accessibility to such relevant data may facilitate exploitation by interested adversaries for disturbing and attacking indistinctly specific flights or the complete traffic within an airspace sector.

Main vulnerabilities of the CNS/ATM system can be categorized in three groups according to their impact:

- Spoofing or injection of fake flight information or fake ATC directives using a dedicated emitter.
- Jamming or interference of some of the aeronautical frequencies used for surveillance.
- Cyber-attacks, including the installation of malicious software (malware) in the

ground-based infrastructure or in the onboard systems that might affect the adequate progress of a flight.

Security shall be one of the premises for the surveillance systems to be developed. They shall be defined and developed under the premise of security by design.

REQ SV5: Integration

Two levels of integration shall be considered in the development of the surveillance systems:

- Surveillance systems for UAS operating within controlled airspace – Controlled airspace is regulated according to a series of requirements defined in terms of altitude, proximity to airports, ATC clearances, avionics, instrumental flight rules and visual flight rules. All these requirements are mandatory for any vehicle flying within controlled airspace. Due to the conservative nature of this scenario, probably a pragmatic solution might be the best approach.
- Integration of surveillance systems for both controlled and uncontrolled airspace – Uncontrolled airspace allows more creative, complex and novel surveillance systems. However the systems for this scenario shall be developed in such a way that a transition of their features to the controlled airspace scenario is possible. The surveillance systems developed for uncontrolled airspace shall enable a progressive transition of the solutions to a controlled airspace scenario.

REQ SV6: Dependent Cooperative Surveillance

Dependent cooperative systems present great benefits compared to those non-cooperative. ADS-B is the main current surveillance dependent cooperative system. However, ADS-B features make it not valid for the UAS integration purposes.

Automated cooperative surveillance systems shall be developed in order to include ADS-B benefits, while improve its capabilities and overcoming its vulnerabilities.

REQ SV7: Non-cooperative Surveillance

Current non-cooperative surveillance systems do not provide the required features for an efficient UTM. Thus, the development of new non-cooperative surveillance systems is required to be able to cope with the features of the upcoming UAS paradigm.

Non-cooperative surveillance systems for UAS pose a big challenge. In order to develop such systems different technologies shall be investigated (i.e. image recognition systems, noise and RF signature detection).

REQ SV8: Surveillance data flows

Surveillance data shall be interchanged between different actors (UASs, commercial aircraft, ATCs, AOCs, etc.). While some of them might only receive data, others will not only receive but also transmit surveillance data. Different data flows will be taken into account for the surveillance systems design and development.

- Air-to-ground: An air-to-ground (and ground-to-air) surveillance data flow will be established between UASs and the systems on the ground. UASs when using dependent surveillance systems will determine their own position and transmit it to the ground. In order to transmit these data, different data-links might be used (3G/4G, Wi-Fi, WiMAX, Satellite, 1090 MHz, UAT, etc.).

- Air-to-air: Some surveillance data will be transmitted directly between UASs or between airplanes and UASs. "ADS-B In" applications receive data from the surrounding aircraft broadcasting ADS-B messages. Communications shall be established between near UASs in order to interchange surveillance data. Hence, the air-to-air sector shall be considered when defining systems and architectures to enable the integration of UASs' operation within controlled and uncontrolled airspaces.

- Ground-to-ground: The ground-to-ground sector shall also be taken into account as there shall be different scenarios where surveillance systems on the ground might

need to interchange surveillance data. This will be the case of the integration of surveillance systems for controlled airspace. Another scenario might be that where two or more systems on the ground need to share surveillance data from overlapping areas of service as shown in Figure 6.

Figure 6 - Overlapping areas of service

REQ SV9: Performance

Surveillance systems to be developed shall be designed to provide for a continuously updated presentation of surveillance information, including position indications. New surveillance systems shall be developed in order to enable such integration.

The set of parameters and associated definitions that shall be used to define the proposed surveillance systems shall include: Data item (the information (e.g., position, identity and intent) that the surveillance system is required to deliver), accuracy, availability, integrity, latency, update period, continuity, coverage, and reliability.

3. Summary

The requirements identified in this document are intended to provide guidance for the development of a CNS architecture for all classes of UAS operating in both controlled and uncontrolled air space. Accordingly, UAS CNS architecture studies will be conducted under the continued investigations of the NASA SASO program. We further see the UTM concept as a foundational principle for the formulation of new CNS architectures. In our future

work, we will explore synergies between the UTM concept for UAS CNS and the emerging CNS solutions under consideration for manned aviation. A harmonized architecture will be necessary to allow for effective Air Traffic Management of all aerial vehicles to assure safe and secure integrated operations.

4. References

[1] Templin, F. et al., 2017, Considerations for an Integrated UAS CNS Architecture, iCNS Challenges for UAS Integration Conference, 11 pp., Herndon, VA.

[2] Kopardekar, Parimal, Joseph Rios, Thomas Prevot, Marcus Johson, Jaewoo Jung, and John E. Robinson III, 2016, Unmanned Aircraft System Traffic Management (UTM) Concept of Operations, 16th AIAA Aviation Technology, Integration, and Operations Conference Washington, D.C.

[3] Federal Aviation Administration (FAA), 2016, Summary of Small Unmanned Aircraft Rule (Part 107), Washington, DC, https://www.faa.gov/uas/media/Part_107_Summary.pdf

[4] Deering, S. and R. Hinden, 1998, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, 39 pp., http://www.rfc-editor.org/info/rfc2460.

[5] Postel, J., 1981, "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, 51 pp., http://www.rfc-editor.org/info/rfc791.

[6] International Civil Aviation Organization (ICAO), 2011, "Aeronautical Telecommunication Network (ATN) Manual for the ATN using IPS Standards and Protocols (ATN/IPS), Document 9896, 118 pp.

[7] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., 2006, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271 DOI 10.17487/RFC4271, 104 pp., http://www.rfc-editor.org/info/rfc4271.

[8] NATO, 2012, NATO Standardization Agreement 4586 (STANAG4586 (Edition 3)), Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability, 509 pp.

[9] RTCA, 2016, Controller Pilot Data Link Communications (CPDLC), RTCA DO-350/351/352, Washington, DC,

[10] Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, 2007, "Delay-Tolerant Networking Architecture", RFC 4838, 35 pp., https://www.rfc-editor.org/rfc/rfc4838.txt

[11] RTCA, 2014, UAS Command and Control (C2) Data Link White Paper, WP-2_C2, 88 pp.

[12] FAA, 2016, Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Analysis Report, Report #93, 144 pp., http://www.nstb.tc.faa.gov/reports/PAN93_0416.pdf

[13] RTCA, 2002, "Minimum Aviation system Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)", DO-242A, 475 pp.

Acknowledgements

Email Addresses

Fred L. Templin (fred.l.templin@boeing.com)

Raj Jain (jain@acm.org)

Greg Sheffield (greg.l.sheffield@boeing.com)

Pedro Taboso-Ballesteros

(pedro.tabosoballesteros@boeing.com)

Denise Ponchak (denise.s.ponchak@nasa.gov)

Conference Identification

2017 Integrated Communications Navigation and Surveillance (ICNS) Conference
April 18-20, 2017