Access 5 Project Office
NASA
P.O. Box 273
Edwards, CA 93523 USA
661-276-2440
661-276-3880 FAX
www.access5.aero

COVER SHEET

Access 5 Project Deliverable

Deliverable Number: CCC005

Title: *C2 Link Security for UAS, Technical Literature Study and Preliminary Functional Requirements*

Filename: CCC005_C2 Link Security for UAS_FINAL.doc

Abstract:

This document provides a study of the technical literature related to Command and Control (C2) link security for Unmanned Aircraft Systems (UAS) for operation in the National Airspace System (NAS). Included is a preliminary set of functional requirements for C2 link security.

Status:

WP – Work in Progress Draft
🟨

Limitations on use:

This is an interim deliverable only and has not been reviewed or approved by Access 5. It presents current thoughts of the C3 Work Package team and preliminary functional requirements for C2 link security.

C2 Link Security for UAS

Technical Literature Study
and
Preliminary Functional Requirements

Access 5 WP6 Team

Version 0.9 (Working Draft)

September 15, 2005

RECORD OF CHANGES

Revision	Date	Action
Version 0.1	August 15, 2005	Draft
Version 0.9	September 15, 2005	Draft

TABLE OF CONTENTS

1 INTRODUCTION

This document provides a survey of the technical literature related to Command and Control (C2) link security for Unmanned Aircraft Systems (UAS) and their operation in the National Airspace System (NAS). This work was tasked under the Command, Control, and Communications (C3) Work Package of the Access 5 program.

Access 5 is a national program sponsored by the National Aeronautics and Space Administration (NASA) and leading the way in enabling Unmanned Aircraft (UA) to routinely fly with other aircraft in the NAS. The Access 5 program consists of a strategic government/industry alliance to develop standards, regulations, and procedures; demonstrate the technologies; and implement infrastructure necessary to meet national priorities. To that end, Access 5 is investigating technology, procedures, and policies needed to operate UAS in the NAS safely and routinely. The results of the program will be the basis of recommendations to the FAA to implement the certification procedure for UA and UAS.

1.1 Background

Communications security is a very high priority issue for UAS in the NAS because it directly impacts the safety of the UAS and other aircraft, people, and property. If communications are compromised, injury, damage, delays, degraded operations, and loss of service could result. For instance, an interloper could issue commands to the UA that would cause it to collide with another UA, causing the loss of both aircraft.

As shown in Figure 1, the C2 link is the data conduit between the vehicle and the pilot-in-command (PIC) on the ground. The PIC controls the UA from the Air Vehicle Control Station (AVCS) by sending messages to affect the dynamics (such as attitude, altitude, and speed) of the UA. The UA sends data to the pilot to keep him/her informed of the flight status, health and status of the UA, and conditions surrounding the UA. In general, the C2 link may be a point-to-point link or involve a shared-media network.

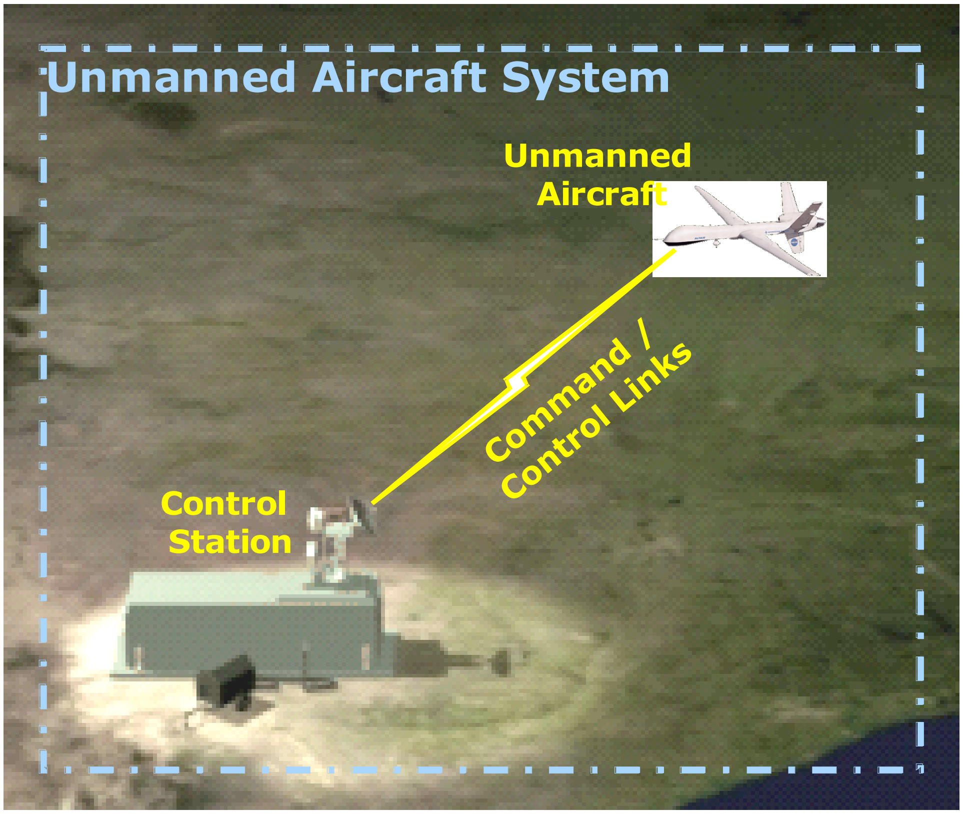

Figure 1. In the UAS, the C2 Link is Between the UAV and Control Station

The C2 link can be considered the most critical part of the UA operations since the PIC is not physically onboard the aircraft to handle events in person. Therefore the C2 link requires security measures in order to prevent unauthorized access to the control of the UA.

In general, communications security encompasses a wide range of topic areas that are addressed in the documents included in this survey. These topics include the following, all of which are applicable to security of the C2 link:

a. Access Control – limit access to only authorized personnel or entities
b. Authorization – determine if requestor is allowed to have access
c. Authentication – confirm that a sender is who they claim to be
d. Non-repudiation – verify that a sender or recipient is the one who claimed to send or receive a message; then cannot later deny sending or receiving
e. Attacks – methods to steal, corrupt, or remove information, such as jamming or denial of service attacks

1.2 Purpose

The purpose of this technical literature study is to gain a broad understanding of communications security as applicable to C2 links for UAS and for future integration into the NAS. The objectives are to status current security for C2 links; identify issues relevant to C2 links, the NAS, or technology that make security more difficult to attain; and determine the direction that C2 link security is going. This study will provide an overview of technical approaches that are currently used, being evaluated for use, under development, and concepts for the future.

From the study results, we can identify open issues, define subsequent tasks in C2 link security, and recommend initial C2 link security functional requirements. These results will be further evaluated and applied to an Access 5 task planned for FY06 to develop functional requirements for the C2 link security for the UAS.

1.3 Scope

The scope of this technical literature study is to research documentation in the open literature that covers communications security relevant to C2 links. These documents can address communications security in general or specifically in aviation. The documentation can be in a variety of forms, such as official regulations or standards, minutes of working groups or committees, industry or Government presentations, documents of commercial advances, and research papers.

1.4 Focus on C2 Link Security for UAS

Not only is communications security a broad issue but also the implementation of the C2 links may vary from one UAS manufacturer to the other. In addition, the ATN has been in operation for years and it is evolving to add more services as technologies and demands progress. In some areas, the ATN may have covered the services for sending command and control messages. However, most of them are ATC related communications for the human pilot in front of the cockpit.

In this study we focus on the relatively new perspective: namely, the C2 messages that are used to affect flight control functions and operations and the links that are dedicated to the UAS. More specifically, the communications security for C2 links requires timely protection and detection against threats. This is the main difference in communication needs between the current major UA operations and manned aircraft. On the other hand, we do not mean to exclude any traditional ATN operations that potentially will be applicable to UAS flight control in the future. Thus, we are also very interested in analyzing gaps in these established standards and procedures in the literature. In general, we focus on transmission security while being watchful of communications security involving conventional cryptographic methodology.

2 APPROACH FOR STUDY OF LITERATURE

This section describes the sources we examined for this study of communications security literature. Security covers a wide spectrum of topics and there is a vast amount of open literature available on these topics. We focused on the technical areas that will help with the development of functional requirements for C2 link security for UAS in the NAS. Therefore, Access 5 internal documents are a good starting point, since they serve as the reference for technical direction. Existing FAA policies and regulations specify current rules that are followed, while technical working groups address new issues and work toward formulating recommendations for aviation and the FAA. The Government has also published standards and procedures related to security. Activities within the aviation and commercial communications industries are another good source for security literature. Publications from academic, commercial, and government-sponsored research provide insights into the latest advances in security. These sources can be summarized as follows:

- Access 5 Internal Documents
- FAA Policies and Orders
- ICAO / ATN
- Government Standards and Procedures
- Aviation Industry Activities
- Commercial Communications Industries
- Research and Academia Activities

2.1 Access 5 Internal Documents

Two Access 5 internal documents report findings from an independent study funded by the Access 5 program in FY04. These documents identify and assess communication security issues for operating UA in the NAS. We used these documents to gain an understanding of the current state of communications security for UA. From this information, we can identify gaps related to C2 link security and efficiently define follow-on work to this literature survey.

2.2 FAA Policy and Order

The FAA is the highest administration office that manages the national airspace system (NAS). It is prudent to understand its policy and related regulations and orders.

2.3 ICAO / ATN Working Group Meetings

We have observed that some security issues had been addressed by very recent ICAO /ATN technical working group meetings. This is a good indication of the security awareness in the recent advancement of the ATN data communications. We researched their minutes to keep track of the technological evolvement by the official ICAO / ATN working groups. In addition, we examined the recent ATN publications like the 3rd edition of ATN Standards and Recommended Practices (SARPs).

2.4 Government Standards and Procedures

Understanding the government standards and procedures is by all means important in the study task like this for future recommendations back to the government agencies. The covered knowledge must expand from the existing literature (past requirements) to the contemporary activities (timely requirements). As a result, we have also spent significant effort in the research on publications by the National Institute of Standards and Technology (NIST) and Federal Information Processing Standards Publications (FIPS). The NIST is a designated standard development agency by the FAA.

2.5 Aviation Industry Activities

We also researched the concurrent aviation industry activities. One of the timely and significant events is Honeywell's press release in the Paris Air Show in June 2005. It announced that they successfully conducted flight tests of new secure Aircraft Communications Addressing and Reporting System (ACARS) recently. We thus investigated the technical details of this system and assessed its technical approach and compared to the operational procedures of the C2 link security that we are interested in. We also researched the security approach by the Global Hawk (GH) for its data communication implementation.

2.6 Commercial Communications Industries

The emerging communications in the mobile and wireless industries have been amazingly impressive in the past decade. This statement applies to both business and technological developments. The security aspect has been one of very critical requirements as well. Thus, quite a few technological developments can be helpful to our functional requirement generation process.

2.7 Emerging Researches

The research activities and topics in the academia and corporate IRAD can reflect the technological developments in the industry of concern. More often, we will be able to sense and forecast the needs and requirements in some pressing issues.

3 STUDY RESULTS

This section reports the findings of this communications security literature study. Each subsection outlines the aspects of security covered in the literature and summarizes its findings. Where possible, findings that specifically address C2 link security are highlighted. No attempt is made to draw any conclusion or emphasize any specific aspect or issue at this stage.

We kept discussions of conventional security functions or techniques to a minimum since they are well established subjects. For example, since encryption is a known technique that has been employed for information and computer data security for many years, it is not specifically discussed as a topic on its own or as a system solution. Rather, such topics are mentioned as appropriate.

3.1 Access 5 Program Internal Documents

The two Access 5 internal documents [A1, A2] provide a very good introduction and background information about communications security related to UA flying in the NAS. One source is a document, while the other is a presentation that highlights items from that document. This subsection focuses on the longer document.

The document uses the traditional Air-to-Ground and Ground-to-Ground communications infrastructure as the framework to discuss security concerns and recommendations. For background, the document describes communication needs for ATC, C2, payload, and flight termination. There is discussion regarding logons to initiate Air-to-Ground applications, ATN security services, and the significance of moving the ATN from Open Systems Interconnection (OSI) based protocols to Internet Protocol (IP) based protocols. The bulk of the document covers security holes, both in the communications infrastructure and in protocol suites, and offers suggestions for mitigation activities and additional study.

The document offers the following suggestions:

1. Add authentication, non-repudiation, and encryption to the C2 link
2. Use a "make before break" strategy for handoff
3. Use secure routing protocols
4. Unbundle C2, payload, and flight termination and put them in their own protected frequencies or RF paths
5. Consider using ATN Version 3 standards for C2

These are useful suggestions. However, some important C2 link characteristics are not fully addressed, such as dynamic and timely intrusion detection and protection, and anti-jamming provisions, etc.

3.2 FAA Policy and Order

It appears that the FAA Order 1370.82 is the latest and the highest authority document addressing the information security issue [Fa1]. It is published on June 9, 2000 and the subject of the Order is Information Systems Security. Its purpose is to establish policy and assign organizational and management responsibilities to ensure implementation of the Computer Security Act of 1987 along with several other related government laws. This Order causes cancellation of two previous orders 1600.54B and 1600.66 that are FAA Automated Information Systems Security Handbook, and Telecommunications and Information Systems Security Policy, respectively. As expected, this is a very high level government document. However, it provides a very useful guideline for our effort. For example, it calls to follow the publications by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in several occasions. This message endorses our study effort in various NIST documents. In general, it is our observation that the FAA library tends to maintain the documents on the established regulations and rules. It depends on other government standard organizations and processes, for example like RTCA, ICAO, and NIST, to address the emerging needs and requirements. However, we have also observed that the FAA would fund the government sponsored research institutions to study pressing issues. [Fa2] is the report prepared by the MITRE Corporation for the FAA addressing on the technology overview for the information system security. This is a very timely research activity by the FAA. The report discusses various technology areas such as authentication, access control, confidentiality, integrity, and availability. However, this document serves too general purposes. We believe that more detailed gap analysis and recommendation will be needed to address the C2 link security in a UAS.

We have researched the FAA website in a great detail. In particular, we found the documents provided in the Office of Assistant Administrator for Information Services & Chief Information Officer WebPages quite informative and useful [Fa3]. We browsed the other related existing regulations and rules and examined the Technical Standard Orders (TSO) more specifically. A TSO is a minimum performance standard for specified materials, parts, and appliances used on civil aircraft. We have not been able to find any TSO that specifically addresses the information security applicable to the C2 link security for a UA.

3.3 ICAO / ATN

We have researched the recent ICAO/ATN meeting reports on the security related subjects from the open literature. Aeronautical Communications Panel (ACP) of ICAO established the network working group in May 2003 the first time [I2] and set up a sub-working group focusing on the security matter [I3]. We examined two meeting reports in this regard with care. It appears that their interests have been on the ATS Message Handling Systems (AMHS) and the general upper layer applications such as the Internet access. Hence, they have studied the security tradeoffs from the IPv4 vs. IPv6 and the public key infrastructure (PKI) architecture points of view. In general, the IP-based networking security is their current concern.

We also examined the latest edition of the ATN Security (Volume VIII) in the ATN SARPs [I1] as recommended by [A1]. This manual first defines the framework standards that the ATN security is based on. Four International Standard Organization (ISO) open system standards are designated to use: ISO/IEC 10181-1, -2, -3, and -6. They are Framework Overviews, Authentication Framework, Access Control Framework, and Integrity Framework, respectively. These framework subjects are actually important security functions that we have to concern with. This manual then discusses the PKI infrastructure, and the cryptographic infrastructure in two full separate sections. Due to the nature of this manual, specific system security objects (service/application specific items) are covered in the last section of the document. Overall speaking, this is an in-depth security manual developed for the ATN. Most of the information can be useful for our purpose. However, it is short of discussing the functions or requirements that are specific to the UAS C2 links. For example, the dynamic or timely natures of the message integrity were not discussed in this document. This appears to be the gap between this official ICAO ATN security manual and our UAS C2 link characteristics.

3.4 Government Standards and Organizations

It is evident from our research that we should pay close attention to the study subjects and the publications of the National Institute of Standard and Technology (NIST). Not only has it published quite a few timely special topics in security, but it is one of the designated organizations by the FAA Order to provide security information standards and guidelines. Recommended Security Controls for Federal Information Systems [N1] is one of the most recent publications that address security controls. This document is generic and covering a very wide range of security controls, yet some applicable information and guidelines can be drawn for helping with the security functional requirements. Some important examples include, but not limited to, periodic assessment of risk, procedures that are based on the risk assessment, etc.

Moreover, the NIST has been interested in numerous emerging technical issues on security. From the recent special publications, we can tell that they are aware of the emerging wireless network security concerns [N2]. WLAN defines three basic security services in their system. They are authentication, confidentiality, and integrity. This special publication discusses some known vulnerabilities in the standardized security of the 802.11 WLAN standard and the recent remedy solution like WAP. It further discusses the security requirements and the threats in the WLAN environment. An intrusion detection system (ISD) is considered an effective tool for security control. Two tables on WLAN security checklist and WLAN risk and security summary in a later section contain quite interesting and useful information for addressing security functional requirements.

The NIST recently proposed the concept of the multi-mode authentication framework [N3] to address multiple-level security. The concept is further applied to the electronic authentication guidelines [N4] for use in the rising e-commerce activities. Enabling adequate user authentication is the first line of defense against unauthorized use. We believe this multi-mode authentication / multi-level security should be considered a very important function for the UAS C2 link security system.

We also found out that the Federal Information Processing Standards Publications (FIPS PUBS) is closely associated with the NIST in developing information security standards and procedures. FIPS PUB-190 [F3] provides a very comprehensive discussion on the use of advanced authentication technology alternatives. In the UAS C2 link security system, message authentication is an effective means to ensure timely protection. FIPS PUB-198 [F2] is an important standard for this function. The technique employed in this standard incurs iterative approved cryptographic hash function, in combination with a shared secret key. The cryptographic strength depends on the properties of the underlying hash function.

FIPS PUB-199 [F1] and NIST SP-800-60 [N6] are two important documents that address security categorization. This is one of the important realization functions in the NIST recommendation [N1].

3.5 Aviation Industry

The Aircraft Data Network (ADN) subcommittee of Airlines Electronic Engineering Committee (AEEC) launched ADN security awareness in a recent technical meeting held in April 2005 [Av1]. Although the meeting discussions centered on the Ethernet network issues, an action item plan was called out to access the GSM/UMTS technology. This was a visionary action plan to meet the ensuing security needs and requirements expected for emerging data communications. The group security specialists recommended basing on security practices for aviation communication upon the common criteria published by the NIST. The report outlines the security process to address three factors: protection, detection, and response.

Honeywell's recent press release [Av2] also shows the importance of the on-going security awareness when the ATN is transitioning to data communications. They have successfully demonstrated secure operations for the existing ACARS. The secure ACARS program was initiated and managed by the AFRL starting several years ago. The strategy of this program is based on the COTS Public Key Infrastructure (PKI) and secure ATN algorithms that are extended to the ACARS environment. This strategy will enable the USAF to fly in the civil air space with attainable investment cost while maintaining its security requirements. The specific techniques employed for security protection include the elliptic curve digital signature algorithm (ECDSA) scheme, the elliptic curve Diffie-Hellman key agreement scheme, and hashed message authentication code (HMAC) scheme. They are all commercially off-the-shelf (COTS) solutions [Av3].

We learned that the GH security architecture is built upon the encryption methods that have been the standards in the military communications for years. The GH has anti-jammed capability in some critical links. We cannot report more technical details in this document but some of the reference documents that the GH used have been reviewed in this study process [Fa4, Fa5, and I4].

3.6 Commercial Communications Industry

It generally consists of two major industries: wireless local area network (WLAN) and wireless wide area network (WWAN). The WLAN is also known as Wi-Fi and it has advanced its technology through generations [C4]. The latest security scheme is called Wi-Fi Protected Access (WPA) that has incorporated user authentication along with temporal key integrity protocol and dynamic key distribution method, etc. These elements are necessary countermeasures to the threats that exist in the shared communications media. The technologies adopted in the WLAN are strongly supported by the Institute of Electrical and Electronics Engineer (IEEE) Standard Committee. Specifically, it is IEEE Std. 802.11i [C3].

The typical WWAN of our interest is 3G mobile communications that should contain the most advanced and matured technology. Lessons learned from the 2G operations have been well incorporated into this new generation. They have conducted significant threat analyses and documented in their standard publications [C1 and C2]. These will be important resources to our activities in the near future.

The similarities of these two industries include that they deal with mobile users and the communication media is shared by the public. As a result, the security integrity must be maintained in a dynamic and timely fashion. These characteristics are also shared by the UAS C2 communications to a large extent. Therefore, we expect that the security concerns studied in these two industries can be useful to the C2 link security functional requirement development.

3.7 Other Emerging Research Activities

Secure mobile ad hoc networking routines and protocols seemed to be the recent popular topics in the academia and the corporate research activities. Since the UAS C2 systems are moving around the NAS, the mobile ad hoc network concept appears to be applicable to our case. So, the security concerns in these research works should be evaluated in our functional requirement development process. This presents alternative or additional approaches to enhance communications security on the move [E1, E2, and E3].

4 Summary of Technical Findings

We first summarize the high level findings in this section. Open issues and further threat study will be also discussed.

- IP-based network security is the main interest of the recent ICAO/ATN technical activities [I1, I2, I3]. It is only a subset when considered for UAS C2 link security. The noticeable gaps seem to include that no dynamic and timely protection concept, no anti-jamming provision are addressed in the traditional IP-based network.
- The MITRE's study report prepared for the FAA on the technology overview of information system security is a valuable reference for the functional requirement development. It reported in Section 4.2 of [Fa2] that more works are needed to be done for aircraft communications and security in today's aviation environment. We agree and actually expect much more work needed to be done for the C2 link security in tomorrow's aviation environment (UAS in the NAS routinely).
- The most recent NIST special publications covered wireless network security (in the area of WLAN) [N2] and proposed the multi-mode authentication concept subsequently leading to multi-level security [N3]. This multi-level security concept can be an important candidate for functional requirements.
- The latest security scheme (e.g., WPA) of the WLAN has been enhanced and supported by the IEEE standard committee. It is designed to deal with mobile users.
- AEEC points to access the GSM/UMTS technology [Av1]. We believe that is appropriate and applicable to the C2 communications for the UAS in several technical aspects.
- The worldwide 3G consortium (closely related to GSM/UMST) has conducted significant security threat analyses in the mobile communication environment. They have published official standards for this subject matter [C1, C2]. We believe this is another important resource to help the functional requirement development.
- The C2 link security in the UAS environment needs to ensure not only the traditional (static) information data security but also the transmission (dynamic) security such as jam-resistance, timely authentication and intrusion detection, etc.

As a result, we have identified some potential gaps (the best effort for now) between the current ICAO/ATN activities and the UAS C2 link security of our concern. We have also identified various information sources that can be further investigated for the functional requirement development process.

4.1 Open Issues

Is communication monitoring acceptable in the UAS environment? The current ATC voice communication is clear and anyone can listen to it as long as he/she has a VHF radio tuned to the frequency of interest. This is the normal condition in today's aviation environment and there has been no adversary event reported due to it. Can this condition be applied to the C2 link of a UAS? At the first glance, people tend to say "why-not" because it has been fine in the past. But, we need to think twice from the UAS operational point of view. The flight control messages may eventually become clear following some "observation" time and anyone can affect flight control by sending messages at their disposal. Is it adversary?

Perhaps, it may be arguable that the authentication step should prevent it from happening. However, it then becomes the chicken-egg argument. In general, we agree with that a real effective authentication method should prevent unauthorized access to the link in the presence of passive listening. But, those effective authentication methods often involve two-way protocols and some kind of key management. The cost of separating monitoring only communications and link access may be very high because this has not been done in the commercial scale. We believe we need to evaluate the benefit of the feature more specifically before opening up the option.

4.2 Further Threat Study

ICAO has determined that denial of service, masquerade, and modification of information are primary threats for ATS [I5]. The technical specifications of the 3GPP [C2] identify four threat categories on the radio interface: unauthorized access to data, threats to integrity, denial of service, and unauthorized access to services. The C2 link is expected to encounter the similar threats mentioned above.

The conventional concept of protected spectrum for the ATC communications was good. It was essentially based on the need of interoperability among all communicators in an ATC region. The same protected spectrum concept has been promoted for the UAS C2 communications. Although it is good for availability, the C2 link may be more vulnerable to the adverse conditions like intentional jamming. This kind of threat should be addressed when the protected spectrum is considered. For example, it will be necessary to allocate the frequency spectrum in such as a way that the anti-jamming techniques can be considered. In the 3GPP threat analysis [C2], jamming is considered as an example of denial of service.

We believe a further threat study for the UAS C2 link is appropriate. There are some unique characteristics to be considered in this application area. For example, the concept of timely detection and protection is very important to the UAS C2 link functions. The consequence of loss of (C2 link) use or any other threat attack can be enormous.

In addition, there are emerging RF weapon threats that have been reported by the National Air & Space Intelligence Center. The impact of such threat attack can be catastrophic and thus cannot be ignored. The challenge of this topic is that most of this kind of threat information is classified.

Included in the threat study should be to examine and establish security categorization of the C2 information for use in the NAS [F1].

5 Recommendations for Functional Requirements

We offer the following recommendations as the initial attempt to formulate the functional requirements, resulting from this limited study. More detailed examinations and iterations are needed.

- The UAS C2 system shall be jam-resistant and/or interference-resistant.
- The UAS C2 system shall develop a procedure for security categorization of the C2 messages
- The UAS shall provide multi-layer security architecture: physical and link layers as the minimum.
- The UAS shall authenticate each message directed to flight control.
- The UAS shall be able to detect intrusion events and protect the system integrity during attacks.
- The UAS shall be able to protect against unauthorized modification of all the C2 messages.
- The UAS shall be able to protect against denial of service (DoS) attacks.
- The UAS shall be able to provide disaster recovery and contingency planning during threat attacks.
- The UAS C2 system shall include multiple control stations.
- The operating control station shall be able to switch to a functional facility automatically as needed without compromising flight safety.

The following document was prepared by a collaborative team through the noted work package. This was a funded effort under the Access 5 Project.

6 Acronym list

ACARS	Aircraft Communications Addressing and Reporting System
ACP	Aeronautical Communications Panel
AEEC	Airlines Electronic Engineering Committee
ADN	Aircraft Data Network
AMHS	ATS Message Handling Systems
ATC	Air Traffic Control
ATS	Air Traffic Services
ATN	Aeronautical Telecommunications Network
COP	Common Operating Picture
CPDLC	Controller-Pilot Data Link Communications
C2	Command and Control
DoS	Denial of Service
FAA	Federal Aviation Administration
FIPS	Federal Information Processing Standards
FY	Fiscal Year
GH	Global Hawk
GSM	Global System for Mobile Communications
HMAC	Hash Message Authentication Code
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineer
IP	Internet Protocol
MAC	Medium Access Control
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NIST SP	NIST Special Publication
NSA	National Security Agency
OSI	Open Systems Interconnection
PIC	Pilot-in-Command
PHY	Physical
PKI	Public Key Infrastructure
SARPs	Standards and Recommended Practices
TSO	Technical Standard Order
UA	Unmanned Aircraft
UAS	Unmanned Aircraft Systems
UMTS	Universal Mobile Telecommunications System
VHF	Very High Frequency
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network

7 References

Access 5 Document

[A1] "Common Operating Picture UAV Security Study," October 29, 2004
[A2] "Initial Communication Security Study for UAVs," Hal Ludwig, November 4, 2004

Aviation Industry

[Av1] AEEC, Meeting Report on Aircraft Data Network (ADN) Subcommittee, May 27, 2005
[Av2] Honeywell Press Release and Presentation Charts
[Av3] "Security Strategy for US Air Force to Use Commercial Data Link," Aloke Roy, 0-7803-6395-7/00, IEEE, 2000

Commercial Communications Industry

[C1] "3G Security: Security Principles and Objectives," 3GPP TS 33.120, V.4.0.0, March 2001
[C2] "3G Security: Security Threats and Requirements," 3GPP TS 21.133 V4.1.0, December 2001
[C3] "Wireless MAC and PHY Specifications: MAC Security Enhancements," IEEE Std. 802.11i/D4.1, July 2003
[C4] "Wi-Fi Protected Access," Networld + Interop, April 29, 2003, Chair of Security Committee, Wi-Fi Alliance

Emerging and Academic Researches

[E1] "Secure Routing for Mobile Ad Hoc Network," Papadimitratod et al., in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002
[E2] "Secure Routing and Intrusion Detection in Ad Hoc Networks," Patwardhan et al., in Proceedings of Third IEEE International Conference on Pervasive Computing and Communications, March 2005
[E3] "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Hu et al., in Proceedings of Mobicom 2002

Federal Information Processing Standards (FIPS)

[F1] "Standards for Security Categorization of Federal Information and Information Systems," FIPS PUB-199, February 2004
[F2] "The Keyed-Hash Message Authentication Code (HMAC)," FIPS PUB-198, March 2002
[F3] "Guideline for the Use of Advanced Authentication Technology Alternatives,"

FIPS PUB-190, September 1994

FAA

[Fa1] "Information Systems Security Program," FAA Order 1370.82, June 9, 2000

[Fa2] "Federal Aviation Administration, Information System Security, Technology Overview" Prepared by The MITRE Corporation, September 30, 2002

[Fa3] FAA CIO Website, www.faa.gov/aio

[Fa4] "Guidelines for Design Approval of Aircraft Data Communications," FAA Advisory Circular, August 16, 1999, AC 20-140

[Fa5] "Initial Air Carrier Operational Approval for Use of Digital Communication Systems," FAA Advisory Circular, February 17, 2000, AC 120-70

ICAO / ATN

[I1] "The ATN SARPs," Subvolume Eight, ATN Security, ICAO DOC 9705/AN956, 3rd Edition, 2002

[I2] Aeronautical Communications Panel (ACP) WG-N-01, Report, May, 23, 2003

[I3] ACP, WG-N, SG-N4 (Security) Minute, April 30, 2004

[I4] "Aeronautical Telecommunications – Digital data Communication Systems," ICAO Annex 10, Vol. 3

[I5] "Overall Security Concept," ATNP/WG-1, WP6-11, Halifax, Canada, Eurocontrol, 1996

National Institute of Standards Technology (NIST)

[N1] "Recommended Security Controls for Federal Information Systems," NIST SP 800-53, February 2005

[N2] "Wireless Network Security 802.11, Bluetooth and Handheld Devices," NIST SP 800-48, November 2002

[N3] "A Framework for Multi-mode Authentication: Overview and Implementation Guide," NISTIR 7046, August 2003

[N4] "Electronic Authentication Guideline," NIST SP 800-63, September 2004

[N5] "Introduction to Public Key Technology and the Federal PKI Infrastructure," NIST, February 2001

[N6] "Guide of Mapping Types of Information and Information Systems to Security Categories, Vol. 1 and II," NIST SP 800-60, June 2004