SECURITY RISK ASSESSMENT PROCESS FOR UAS IN THE NAS CNPC ARCHITECTURE

Dennis C. Iannicca, NASA Glenn Research Center, Cleveland, Ohio
Daniel P. Young, DB Consulting Group, Inc., Cleveland, Ohio
Suresh K. Thadhani and Gilbert A. Winter, Verizon Federal Network Systems, Cleveland, Ohio

Abstract

This informational paper discusses the risk assessment process conducted to analyze Control and Non-Payload Communications (CNPC) architectures for integrating civil Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS). The assessment employs the National Institute of Standards and Technology (NIST) Risk Management framework to identify threats, vulnerabilities, and risks to these architectures and recommends corresponding mitigating security controls. This process builds upon earlier work performed by RTCA Special Committee (SC) 203 and the Federal Aviation Administration (FAA) to roadmap the risk assessment methodology and to identify categories of information security risks that pose a significant impact to aeronautical communications systems. A description of the deviations from the typical process is described in regards to this aeronautical communications system. Due to the sensitive nature of the information, data resulting from the risk assessment pertaining to threats, vulnerabilities, and risks is beyond the scope of this paper.

Introduction

Overview

Unmanned Aircraft System (UAS) integration into the National Airspace System (NAS) represents many new challenges in aviation. One of the challenges is the development of a new command and control communication system capable of providing reliable, safe, secure, routine operation of an unmanned aircraft (UA). Additional challenges associated with the development of a new command and control communication system include the assignment of a dedicated frequency spectrum, the development of a communications datalink, and the security testing and certification of the communications system. RTCA Special Committee 203 (SC 203) identified this new UAS command and control communication system as the Control and Non-Payload Communication (CNPC) system. The purpose of the CNPC system is to exchange information between the UA and the UAS Control Element (CE) to ensure safe, secure, and reliable communications. Figure 1 below shows the various elements that comprise the Unmanned Aircraft System [1]. The CNPC is part of the Communications Element.

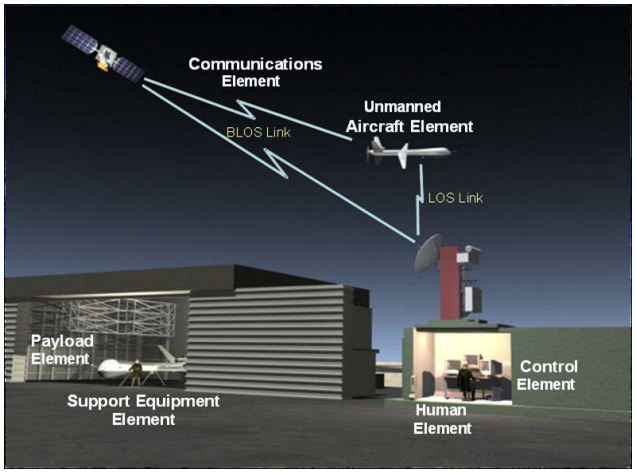

Figure 1. Unmanned Aircraft System Elements[1]

The risk assessment was guided by federal standards, so as the CNPC system evolves the FAA could utilize this assessment as a contributing component of a final assessment and eventual CNPC system certification. The federal standards were authorized by The Federal Information Systems Management Act (FISMA). FISMA tasked the National Institute of Standards and Technology (NIST) with the responsibility for developing standards that provide security of federal information systems. The standards shall include information security standards necessary to improve the security of federal information systems. The risk assessment contains the results of a security risk

assessment conducted on a notional CNPC system supporting the operations of UAS in the NAS. The risk assessment followed the guidelines found in the NIST Special Publication 800-30 (July 2002) Risk Management Guide for Information Technology Systems [2] and NIST Special Publication 800-53 (Revision 3 August 2009) Recommended Security Controls for Federal Information Systems and Organizations [3]. This assessment process builds upon earlier work performed by RTCA Special Committee (SC) 203 to define candidate architectures and its ad-hoc security sub-group to suggest following a NIST-based risk assessment methodology [4]. We concur with [4] that a NIST-based risk assessment methodology was the most logical choice to follow as:

- NIST standards and guidelines are developed from commercial best practices.
- While NIST standards are required for all government systems, they are free for the private sector to use.
- The FAA's Security Certification and Authorization Package (SCAP) already implements the NIST standards and guidelines.

Purpose

The risk assessment identified the threats, vulnerabilities, inherent risks, and the controls that may be used to mitigate the risks encountered in a notional CNPC system. It provides a basis in which core architectures, standards, and technologies may be evaluated in a consistent manner in regard to security. The risk assessment process provided a thorough qualitative and quantitative evaluation of threat-sources, vulnerabilities, risks, and controls associated with both our conceptual, as well as envisioned future, CNPC systems. Due to the sensitive nature of this information, data resulting from the risk assessment pertaining to threats, vulnerabilities, and risks is beyond the scope of this paper. Although the details of a specific, final implementation may differ in some aspects, the effort allows for the selection, evaluation, and verification of a substantial portion of the security components anticipated in those future CNPC systems. The format and content of the risk assessment may be used as the foundation for risk assessments by system implementers, certifying authorities or agencies when the final CNPC systems are constructed.

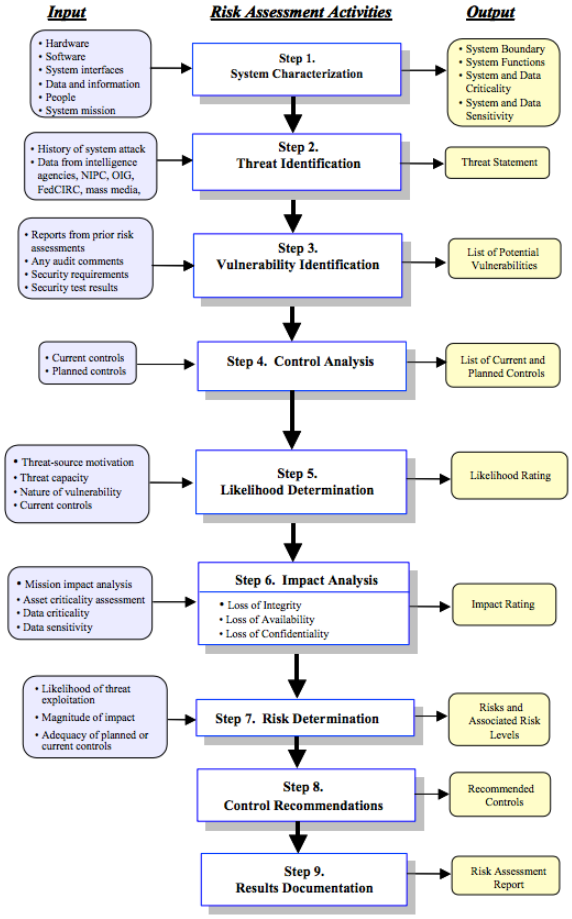

Figure 2. Risk Assessment Methodology Flowchart [2]

Figure 2 shows the common Risk Assessment Methodology as documented in NIST SP 800-30 [2]. It became apparent in the early stages of this effort that an operational, or even early-development, model of a system architected and built for certification under the future FAA and RTCA standards existed. Several assumptions and a few process adjustments were necessary as we exercised the NIST framework. We also acknowledge that while we are aware of the many examples of public and military UAS operating by exception within the NAS, we did not feel these provided a suitable likeness for an analysis of how future civil UAS would be operated. Military CNPC systems are proprietary, rely on separate spectrum allocations, utilize cryptography not available for

civilian use, and details about the systems are largely unavailable to the general public.

Methodology

System Characterization

Scope

The development of civil UAS routinely flying in the NAS is still in its early stages. No civil UAs are routinely flying in the NAS at present. The UAs that are flying in the NAS are primarily military, federal government, test and development aircraft owned by private companies, or universities flying under exception. These UAS utilize either military or proprietary communications systems specifically tailored to their mission's scope. No FAA authorized communication system for UAs currently exists, so the analysis conducted in the risk assessment process was based on a baseline architecture of a notional CNPC system. The architectures of these CNPC systems were derived from RTCA Inc.'s, SC-203 Issue Paper, UAS Control and Communications Architectures [5] and European Aviation Safety Agency's (EASA) Inception Report of the Preliminary Impact Assessment on the Safety of Communications for Unmanned Aerial Systems (UAS) [6]. The baseline architecture consists of a CNPC system utilizing wireless datalinks along with optional wired terrestrial components. It is assumed that a real-time computer operating system with a protocol specific to the UAS is used to generate the data communications necessary and that the data will be transmitted via wired and/or wireless systems. The CNPC system may be point-to-point, line of sight, or transmitted through a series of ground stations and/or satellite system. It is from this notional CNPC system that threats, vulnerabilities, likelihoods, impacts and risk were derived.

The risk assessment identifies two baseline communications architectures, direct and networked, for supporting the CNPC system. These baseline architectures are designed for use in the study, development, and evaluation of the security controls needed to secure communications between the various types of unmanned aircraft (UA), the associated control element (CE), and the Federal Aviation Administration's (FAA) Air Traffic Control (ATC) facilities. UAs are being developed in various sizes with different operating altitudes, airspeeds and communications requirements, each presenting unique demands on the communication architectures. A conceptual architecture attempts to reduce these various communications architectures into two baseline architectures from which a communications security risk assessment can be performed.

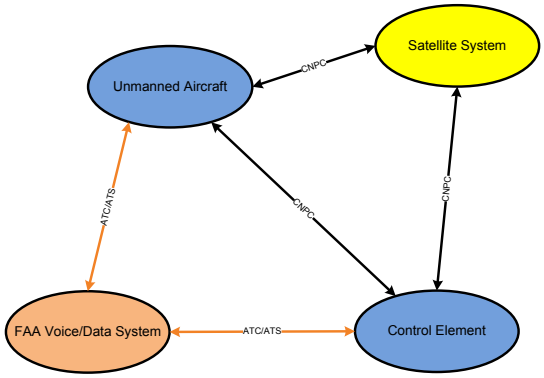

Figure 3. UAS Direct Control and Non-Payload Communications (CNPC) Security Baseline Architecture

The architecture displayed in Figure 3 shows a direct CNPC communications path between the CE and the UA for line of sight (LOS) communications or direct CNPC communications path between the CE and the UA via a satellite system for beyond line of sight (BLOS) operations. Redundant paths implementing both LOS and BLOS may also be used to enhance communications reliability and range. In this architecture, ATC/Air Traffic Services (ATS) communications may be relayed through the UA to the CE as part of the CNPC or direct to the CE via ground or non-UA airborne communications links.

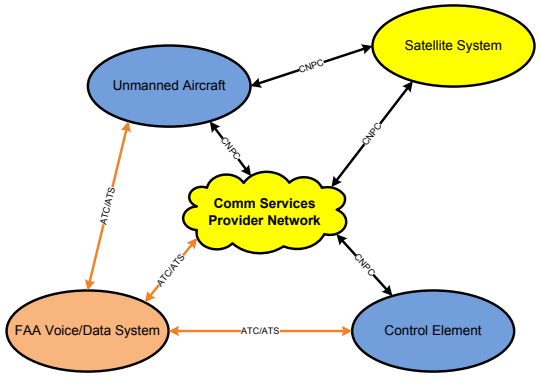

Figure 4. UAS Networked Control and Non-Payload (CNPC) Security Baseline Architecture

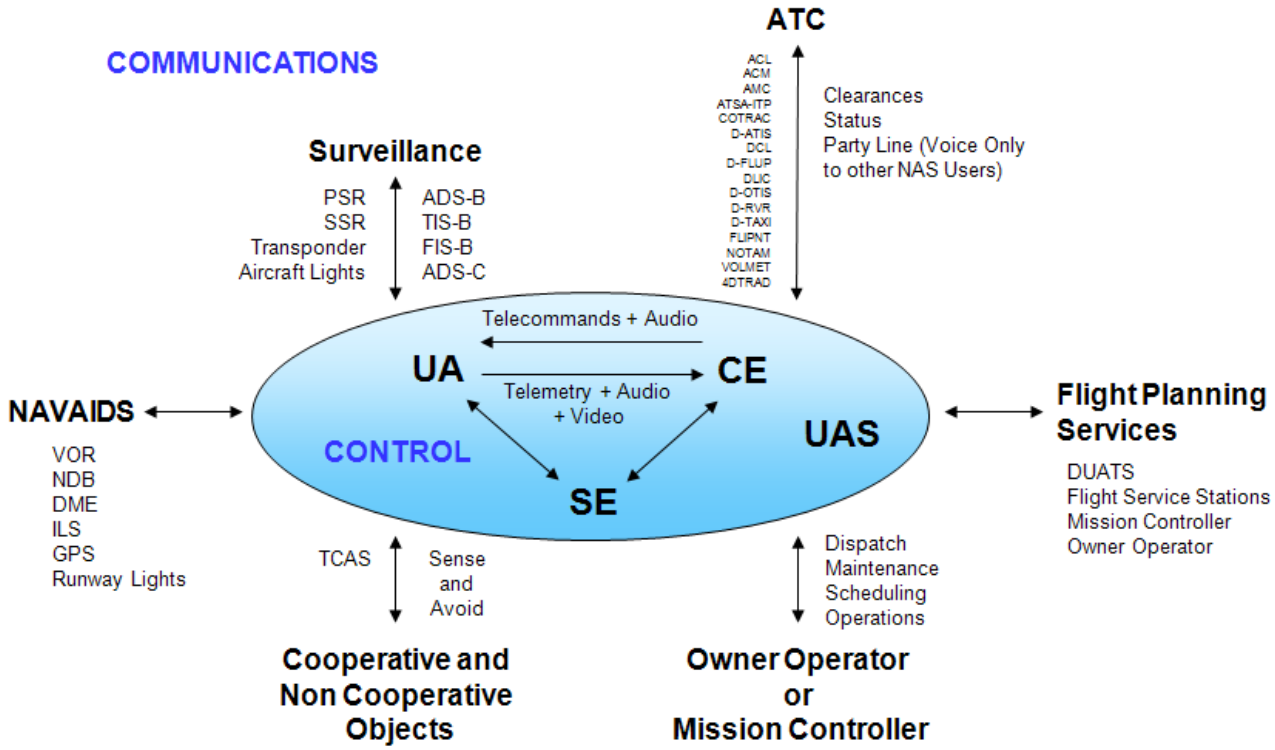

Figure 5. Overall View of System Inputs and Outputs [7]

The architecture shown in Figure 4 uses an aeronautical communication service provider network to supply the primary CNPC links between the CE and the UA. The communications service provider network may be supplied by a third party, the UA owner/company or the FAA and provides a network of communications services within a small to global geographic area. The details of these services are not defined here but are considered a potential service offering in the future to support LOS and BLOS CNPC communications on a large scale. Redundant paths from the FAA facilities and CE to/from the service provider network may be used to enhance the availability of the communications links.

The CNPC system is a data link comprised of several functions needed for the safe operation of a UA. Several of the functions can be combined depending on the capabilities of the UA and or its operational function. The following functions make up the CNPC data link: Telecommand Data, Telemetry Data, Navigational Aids (NAVAIDS) Data, Air Traffic Control (ATC) Voice Relay, Air Traffic Services (ATS) Data Relay, Target Data, Airborne Weather Data and Non-Payload Video Data for safety of flight. Figure 5 shows the expected normal Communications, Navigation, and Surveillance functions associated with the operation of an unmanned aircraft in the NAS [7]. The figure also shows the relationship of the data to the primary elements that comprise a UAS. The CNPC data link connects the UA to its CE and associated Air Traffic Services (ATS). Communications with the support element (SE) pertains to transport, maintenance and launch of the UA; it is not part of the CNPC.

The risk assessment process includes evaluating the security of the CNPC and ATC/ATS information sent to and from: the UAS control element, the unmanned aircraft element, the FAA's ATC/ATS facilities, and the satellite and/or network service providers. While securing the physical facilities associated with UAS operation is an important contributor to the overall security of the entire system, it was deemed outside the scope of the

current CNPC risk assessment. Since threats from the environment, utilities, and other natural or manmade sources are unique to specific system implementations and operating environments, they could not be properly evaluated as part of the notional CNPC architecture. As our focus was to concentrate on the expected technical aspects of the CNPC security, organizational policies and procedures that would enhance the security posture of a UAS were also considered outside the scope of the evaluation. In a risk assessment of an operational system seeking certification from a governing authority, such as the FAA, we fully acknowledge that these aspects would play a crucial role in defining the system's security architecture.

Security Categorization

Security categorization is the characterization of information systems and information types based on assessment of the potential impact that a loss of confidentiality, integrity or availability of such information and information types would have on organizational operations, organizational assets, or individuals [8].

Security categorization of an information system begins with the identification of the parts (information types) that make up the system, continues by performing an analysis of the impact the loss of confidentially, integrity and availability has on the information types and ends with a "high-water mark" analysis of the information types upon the system as a whole. The highest impact on the information types becomes the impact for that information type on the information system. This information is then used during the system's risk analysis process to select the minimum security controls for the information system. The security categorization process is described in the Federal Information Processing Standards Publication 199 (FIPS PUB 199) and the National Institute of Standards and Technology (NIST), Special Publication 800-60.

A security categorization was conducted on the notional CNPC information system described above and its individual functions (information types). The information types identified for the categorization process are the seven functions of the CNPC system: Telecommand Data, Telemetry Data, Navigational Aids (NAVAIDS) Data, Air Traffic Control (ATC) Voice Relay, Air Traffic Services (ATS) Data Relay, Target Data, Airborne Weather Data and Non-Payload Video Data. The impact of losing confidentiality, integrity or availability of each information type was evaluated. An impact of Low, Moderate, or High was assigned to the loss of confidentially, integrity and availability of each information type based on the definitions found in FIPS PUB 199. The highest impact value for confidentiality, integrity and availability then becomes the overall security categorization impact level for the information type. This process delivered an overall security categorization for each information type based on the formula below.

$$\mathbf{SC}_{\text{information type}} = \{(\mathbf{confidentiality}, \textit{impact}), (\mathbf{integrity}, \textit{impact}), (\mathbf{availability}, \textit{impact})\}$$

Once the security categorization of the information types was completed, a security categorization for the overall CNPC information system was conducted. The security categorization for the CNPC system was determined by selecting the highest impact value for each information type. The highest impact value for confidentiality, integrity and availability then becomes the overall security categorization impact level for the CNPC information system. The generalized format for expressing the Security Categorization for the CNPC System is:

$$\mathbf{SC}_{\text{CNPC System}} = \{(\mathbf{confidentiality}, \textit{impact}), (\mathbf{integrity}, \textit{impact}), (\mathbf{availability}, \textit{impact})\}$$

The resulting impact level from the security categorization of the CNPC system was then used to identify the appropriate baseline security controls needed to mitigate the risks identified during the risk analysis process.

Risk Identification

Risk is defined as the overall negative impact to the system when considering the probability that a vulnerability is exploited by a threat-source.

The risk identification phase of the risk assessment is the process by which risks to the system are identified and prioritized so that system owners are able to make a determination on how to allocate resources to mitigate overall impact to the system. Risk identification involves identifying threat sources, system vulnerabilities, and determining the probability that a known vulnerability can be exploited by the threat-source based upon inherent system controls.

Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability [2]. A known threat-source does not present a risk when there is no vulnerability that can be exploited within the system.

Threat-sources for a specific system are identified as any circumstance or event that can cause harm to the system. In assessing threat-sources, it is important to consider all threat-sources that can harm the system and its processing environment. During the assessment process, we investigated threats related to both a general information technology communications system and, more specifically, aeronautical communications systems. Using these threats as a baseline, we were able to extract a list of likely threat-sources that would impact our notional CNPC system.

The threat statement produced from this step of the process was created to provide a description of the anticipated threat types that can cause an adverse effect on the system.

Vulnerabilities

A vulnerability is a weakness in the system that can be exploited either intentionally or accidentally. The goal of this step was to develop a list of the system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources [2]. The identification of vulnerabilities can take many forms based on various types of risk assessments. For the purposes of this risk assessment, we compiled a list of common information technology (IT) and communications-related system vulnerabilities that applied to our notional UAS CNPC system. Once an actual system is under development, these vulnerabilities would need to be re-evaluated to reflect the configuration of the implemented operational system and the operating environment.

Risks

Risk is the likelihood that a threat-source exploits a vulnerability and that it in turn results in an adverse impact to the system.

The risk analysis for each vulnerability consists of assessing the threats and compensating controls to determine the likelihood that vulnerability could be exploited and the potential impact should the vulnerability be exploited. A general depiction of the analysis is shown in Figure 6, where risk is the intersection of a threat and vulnerability, influenced by likelihood and impact:

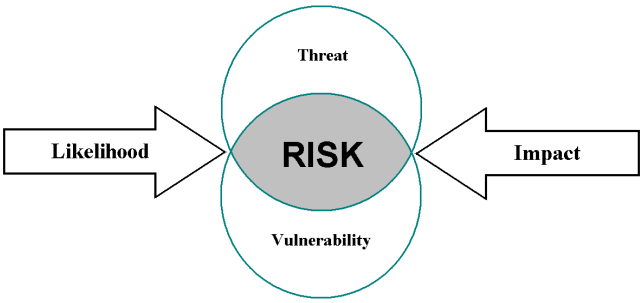

Figure 6. Link between Likelihood, Impact, and Risk [2]

Essentially, risk is proportional to both likelihood of exploitation and possible impact.

Determination of threat and vulnerability pairing was accomplished by analyzing each vulnerability classification and applying a threat source to determine if the threat source pertained to the vulnerability. This iterative process of identifying relevant threat and vulnerability pairings resulted in the creation of a table of system risks.

Control Analysis

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize the adverse effect of the risk to the system. Security controls encompass the use of technical and non-technical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Non-technical controls are management and operational controls such as security policies, operational procedures, and personnel, physical, and environmental security [2].

Security controls used for the risk assessment were defined in NIST Special Publication 800-53 (Revision 3 August 2009) Recommended Security Controls for Federal Information Systems and Organizations [3].

For the purposes of the evaluation, given that the system is in a pre-development phase, we determined a list of likely applicable inherent system security controls that would be included in a commonly deployed system using commodity equipment and

software. For example, basic account management functionality is an inherent security control found in all modern operating systems that would likely be deployed for use in a UAS CNPC system.

Likelihood Determination

Likelihood is the probability that a given vulnerability will be exploited in a threat environment and is determined by analyzing the effectiveness of existing (in this case inherent) controls against the threat-source's capability and motivation as well as the nature of the vulnerability. Existing controls consist of safeguards in place that effectively reduce the access to, or successful execution of, a given vulnerability by a threat-source. While determining threat source motivation is somewhat subjective, this is only one part of the "likelihood determination".

Table 1. Likelihood Definitions [2]

Likelihood	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivate and capable, but controls are in place that may impede the successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Each documented risk was evaluated against the standardized definitions for each level, listed in Table 1, and the most appropriate likelihood was selected. Numerical values for the likelihood are assigned based on the NIST SP 800-30 recommended approach, which is: High (1), Medium (.5), and Low (0.1). These values provide quantitative assignments of likelihood that are then utilized in the remaining steps to calculate the risk in a more precise manner than afforded by purely qualitative means.

Impact Analysis

Impact is the resulting effect if a given vulnerability is successfully exploited by a threat-source. An impact to the system or data's confidentiality, integrity, or availability is determined in accordance with the NIST SP 800-30 criteria and associated with the particular risk. The rationale for evaluating impact is that the exploit of a vulnerability with little or no adverse effects on the system or the data will typically result in a lower priority than vulnerabilities with higher adverse effects.

Given that we were evaluating a notional system, we were still able to apply the standard impact definitions to our vulnerabilities. The impact definitions are not specific to any system design so we were able to correlate system impact to our threat-vulnerability pairs. The impact analysis provides prioritization of risk and illuminates areas for immediate improvement of system vulnerabilities.

Table 2. Impact Rating Definitions [2]

Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Each risk identified was evaluated against the standardized definitions for each level, listed in Table 2, and the most appropriate impact selected. The results of this analysis provided both an impact level and rating value. The numerical values are assigned based on the NIST SP 800-30 recommended approach, which is: High (100), Medium (50), and Low (10). These values provided numerical assignment of impact that was utilized in future steps to calculate the risk in a more precise manner than afforded by qualitative means.

Risk Determination

Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [2]. This section takes the qualitative threat-sources, vulnerabilities, and risks along with the quantitative likelihood and impact

values to derive a risk level associated with the notional CNPC system. Determining the risk level was accomplished by creating a matrix of the likelihood and impact values, shown in Table 3, to determine a risk rating for each individual risk.

Table 3. Likelihood vs. Impact Matrix [2]

Threat Likelihood	Threat Impact		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	Low 10x1.0=10	Medium 50x1.0=50	High 100x1.0=100
Medium (0.5)	Low 10x0.5=5	Medium 50x0.5=25	Medium 100x0.5=50
Low (0.1)	Low 10x0.1=1	Low 50x0.1=5	Low 100x0.1=10

Creation of a rating scale for each individual risk allows for prioritization of effort during risk mitigation efforts.

Control Recommendations

In this section, controls that provide mitigation of the identified technical risks are suggested. The assessment concentrated on selecting the NIST Special Publication (SP) 800-53, Revision 1 controls most likely to provide substantial reductions in the likelihood or impact of an identified risk beyond the inherent security controls found in the base system (or in this case technologies). The goal of the recommended controls was to reduce the residual risk level of the implemented system and its associated data to an acceptable level in order to gain accreditation by certifying authorities.

Results Documentation

The final step of the Risk Assessment Methodology involves the creation of the Risk Assessment Matrix, which brings together an executive view of all the previous steps into a final summary table. This compilation of information reveals to interested parties the threat-sources, vulnerabilities, inherent and recommended controls and assessed risk of the UAS CNPC system.

Conclusion

During this risk assessment we were able to successfully adapt the NIST SP 800-30 Risk Assessment Methodology to a notional UAS CNPC architecture in the very initial stages of development. To adapt the process to our needs we made certain assumptions regarding aspects of the system such as our hardware, software, communications architecture and interfaces, as well as drew upon information from similar IT and aeronautical communications systems to identify threats, vulnerabilities, risks, and inherent system controls that are likely to be present in civil UAS integrated into the NAS.

The process allowed us to deliver a list of recommended security controls and enhancements for a representative architecture that is being fed into the follow-up work to develop a risk mitigation plan for the notional UAS CNPC system. Current work involves developing a list of representative products and technologies that map against the recommended security controls identified during the risk assessment so that we can perform testing with those controls applied in a prototype architecture.

Finally, we feel that UAS implementers in the future should be able to successfully utilize this NIST risk assessment process by adapting it to their particular system's environment in order to assist in the certification and accreditation process with the FAA.

References

[1] United States Department of Defense, March 2011, "Unmanned Aircraft System Airspace Integration Plan", Version 2, Appendix D.

[2] National Institute of Standards and Technology, July 2002, "Risk Management Guide for Information Technology Systems", SP 800-30.

[3] National Institute of Standards and Technology, August 2009, "Recommended Security Controls for Federal Information Systems and Organizations", SP 800-53, Revision 3.

[4] Wargo, C.A., Frye, G.E., Robinson, D.W., 13-15 May 2009, "Security Certification and Accreditation analysis for UAS Control and Communications", Integrated Communications, Navigation and Surveillance Conference, 2009, pp. 1-12.

[5] RTCA Inc., December 2008, "UAS Control and Communications Architectures", SC-203-CC005_UAS Control and Communications Architectures_vD_23Dec08.

[6] European Aviation Safety Agency, 13 February 2009, "Inception Report of the Preliminary Impact

Assessment of the Safety of Communications for Unmanned Aerial Systems (UAS)", Issue 1.1.

[7] RTCA Inc., 22 May 2012, "Control and Communications Functional Requirements", RTCA SC203 WG2.

[8] National Institute of Standards and Technology, February 2004, "Standards for Security Categorization of Federal Information and Information Systems", Federal Information Processing Standards Publication 199, pg 8.

Acknowledgements

The authors would like to thank Vic Patel and Tom McParland at the FAA Technical Center for their assistance and guidance in developing the CNPC risk assessment.

Conference Identification

2013 Integrated Communications Navigation and Surveillance (ICNS) Conference

April 23-25, 2013