

# ASSESSING SECURITY RISK OF AIRPORT INFORMATION SYSTEMS: THE AHP APPROACH

*Research-in-Progress*

## **Hak J. Kim**

University of Hofstra  
134 Hofstra University  
Hempstead, NY 11549  
Hak.J.Kim@hofstra.edu

## **Dan J. Kim**

University of North Texas  
1155 Union Circle  
Denton, TX 76203  
Dan.Kim@unt.edu

## **Abstract**

*The paper examines the security risks of airport information systems and then attempts to develop the model for assessing its security risks using the analytic hierarchy process (AHP) approach, which is a useful tool to analyze the complex problem by reducing its complexity. This paper give an inference that the AHP approach can provide the security professional with a solid approach to complex design of security controls in airport information system.*

**Keywords:** Cyber Security, Risk Assessment, Analytical Hierarchy Process, Airport Information System

## Introduction

Since the rapid increase in air travel beginning in the early 1990s, an airline has become more reliant on travel as a means to conduct global business and travel for leisure in the US (Skinner, 2009). There are now 15,079 airports in the continental US as of 2010 (CIA, 2011). According to the Federal Aviation Administration (FAA, 2011), Dulles International Airport, an average size airport in the US, processed more than 400,000 flights in 2010, averaging over 1,000 flights per day. With this increasing reliance on air travel, airports have strived to modernize technologies to ensure faster, safer, and more efficient air travel over the years.

Airport information systems (AIS) have evolved to meet the ever faster, more immediate expectations of Internet generations (Leng, 2009). To meet the demands, new information systems have been bolted on to older systems to provide newer interfaces, and present data in new ways. With this meshing of old and new infrastructures and technologies, security professionals are challenged on how to secure airport operations, while enabling the essential mission of continued safe air travel, as stated by the FAA.

To secure the information systems, rigorous and proven methodologies are necessary to address their threats and vulnerabilities. Cyber security risk assessment (Stoneburner et al., 2002) and security architecture design principles (Pfleeger & Pfleeger, 2007) assist security professionals in dividing the challenge into smaller, more approachable security designs and controls. A cyber security risk assessment serves as a tool to determine not only the appropriate security controls for addressing threats and vulnerabilities to systems, but also to assist in the prioritization, given the limitation of resources to apply to securing infrastructures.

Traditional cyber security risk assessment approach (Gordon & Loeb, 2001; GAO, 2004; Siponen, 2005) is to identify threats and vulnerabilities, to assess their impacts, and then to apply countermeasures of assets. However, applying this traditional cyber security risk assessment methodology to AIS can quickly become very complicated and lose the effectiveness as serving as a tool for security control identification and prioritization. In applying cyber security risk assessment principles with groups determining security controls, decisions analysis methodologies can be employed to couple the imprecise nature of decision making and group dynamics in complex problem solving.

This paper examines the security risks of airport information systems and then attempts to develop the model for assessing its security risks using the analytic hierarchy process (AHP) approach which is a useful tool to analyze the complex problem by reducing its complexity. This paper give an inference that the AHP approach can provide the security professional with a solid approach to complex design of security controls in airport information system.

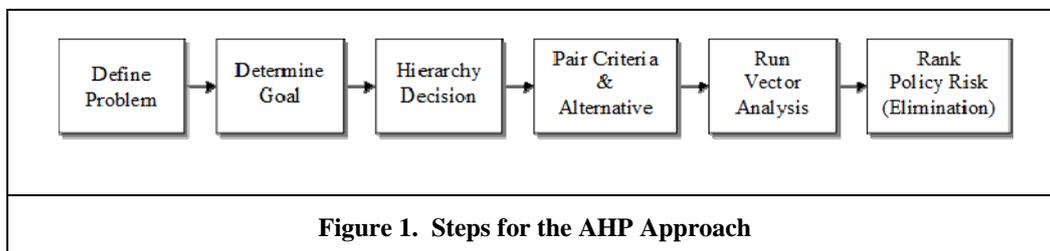
## The AHP Approach: a Brief Overview

Traditionally, security risk assessment (Wallace, 2003) is used as a tool for decision makers to determine the appropriate security controls. Either quantitative or qualitative (mission-based) risk assessment is conducted to determine appropriate security design and controls to employ; in this case, the mission is concrete and well known, so a mission-based risk assessment is an option. First, essential and important assets are identified. Next, the threats, vulnerabilities, and likelihood are assessed for the information systems, and then countermeasures are applied to mitigate the risks (Stoneburner et al., 2002). Current countermeasures deployed are also included in the assessment. The many threats and vulnerabilities are then mapped and prioritized, taking in consideration the importance of the assets to enabling the mission, in this case, continuing to ensure the continued safety of air travel.

Unlike traditional security assessment approach, the Analytic Hierarchy Process (AHP) used for subjective pairing comparisons among different criteria and alternatives with the main focus to eliminate any substantial risk within the network. The AHP approach divides diverse business lines into trust domains to assist security professionals and decision makers by simplifying risk analysis (Scholtz 2008). By dividing the cyber security information systems into business lines, similar security goals, designs, and controls can more easily be determined. Business lines, and therefore trust domains within an airport will also have diverse missions, and most likely different security goals. For example, in considering confidentiality, integrity, and availability, one trust domain may value confidentiality, whereas another might value availability more (Wright & Harmening 2009). The security controls for each might be very different. Also, although the overall mission for the airport is known, many smaller missions and goals within the airport need to be considered in applying this process. Table 1 shows the comparison of traditional approach and the AHP approach.

Table 1. Traditional Approach vs. the AHP Approach		
Category	Traditional Approach	AHP approach
Brief description of assessment method	A water flow method to identify requirements, to assess security risks, and to design security control mechanism.	A process to break down complexity into smaller scope comparisons, assign relative ratings, and analyze the results to determine the best outcome
Main advantages	<ul style="list-style-type: none"> <li>Easier to understand the assessment process</li> <li>a guide for the development of products or systems with security functions</li> </ul>	<ul style="list-style-type: none"> <li>AHP is well-suited to deal with moderate risk.</li> <li>The hierarchy helps to organize risk management</li> </ul>
Limitations	<ul style="list-style-type: none"> <li>Traditional approach doesn't take into account the big picture. By narrowly focusing only on assessment results, organizations can miss understanding the full extent of their risk.</li> </ul>	<ul style="list-style-type: none"> <li>The AHP analysis can undermine reproducibility, and large problems require since it requires a huge amount of time to complete the pairing comparisons of criteria and alternatives.</li> <li>Users must maintain near-logical consistency in their comparisons, which requires continuous guidance.</li> </ul>

The AHP was developed in the 1970's by Thomas Saaty (1980) to help users choose alternative when considering a decision objective and its supporting criteria. The AHP uses three hierarchical levels to solve a problem by reducing complexity; (1) objective – top layer, (2) criteria – intermediary layer, and (3) alternatives – bottom layer (Froman & Gass, 2001). A level's rating is presumably unaffected by another level. The measurement of alternatives are subjective comparisons rely upon integer scores 1 through 9, and upon reciprocity. For example, if alternative *A* is *X* times more attractive than alternative *B*, then *B* is 1/*X* times more attractive than *A*. A score of 1 means the two alternatives are equally attractive, a score of 9 means *A* has the greatest possible importance (or attractiveness) over *B*, and scores 2 thru 8 incrementally raise the attractiveness of *A* over *B*. Figure 1 shows the general process to apply the AHP approach.



The AHP has grown steadily over the last 40 years, and can be applied to many different applications. In information systems security, AHP studies (Farrokh 2002; Bodin et al. 2005; Kim and Lee 2006) have included guiding information security investment decisions, evaluating antivirus and content filtering products, and using analytic models on security systems. Saaty (2008) proposed a process to break down complexity into smaller scope comparisons, assign relative ratings, and analyze the results to determine the best outcome. His method consisted of defining the problem, or what is to be solved; determining the structure using a decision hierarchy, which includes determining the criteria and alternatives; comparing the alternatives and criteria in pairs to determine preferences and priorities; and analyzing the resulting priorities and preferences to determine the best outcome or alternative to choose to solve the problem. Using this process, AHP can assist decision makers and security professionals in group decision making to address a complex problem.

## **Airport Information System (AIS): an Overview**

Airports (Laskaris et al., 2007) are complex and unique entities involving multiple organizations (i.e., airline companies, retail shops, and government agencies (i.e., TSA, FBI, etc.)). With this complexity of diverse business lines coupled with tight regulation, securing airport information systems are extremely challenging to decision makers. While every airport may have its own unique infrastructure' policies, personnel, hardware, and software applications, they all must support passenger processing, baggage handling, and aircraft movement. In addition to processing thousands of flights every day, AISs facilitate many diverse businesses and services, including airline ticketing, ground transportation, luggage conveyance, and security screening. Airports rely on these disciplines and business lines to maintain smooth operations in moving people and baggage from destination to destination safely and efficiently. As such, AISs accommodate many different kinds of customers, from airlines to food vendors, fuel providers to security personnel, not to mention passengers. The systems are interdependent on communications to inform status on weather, flight delays, ticketing status of passengers, and security information.

Information systems in airports are extremely complex. Like many information systems in other industries, airport information systems have evolved over time, with new state of the art technology built on the front end interface or running in parallel to legacy systems. Further adding to the complexity, airports are publically owned, and the facilities and many of the services are regulated by the FAA.

Today's AISs provide a variety of services, such as ticketing and check-in systems, TSA security checking systems, passenger lounges, internet cafes, airport Wi-Fi services, control tower systems, air traffic control systems, immigration service systems, etc. Also a part of airport services are ground control systems including car rental company systems, aircraft ground handling, cleaning, resupply, service, special meals, fueling, airplane maintenance, customs, etc. Customs is responsible for inspecting and tracking goods being imported from other countries, checking luggage through customs. Baggage routing systems are also a part of the infrastructure, including, baggage claim, flight transfer of baggage, baggage screening systems including explosive detection systems. Air traffic control sites located outside the physical boundary of the airport as well as ticketing and control systems, and TSA checkpoint systems located within the boundary.

Airlines operating in the airport will each have their own information systems, in addition to the airport's own administrative center. The Washington DC Metropolitan Washington Airport (MWA) operates both Dulles and Reagan international airports, which each have unique information systems. Within these systems, individual restaurants, shops, and stores will have their own types of information systems. Above all of these individual systems, the FAA and Transportation Safety Board (TSA) operate normal and mission critical systems.

Individual airlines have information systems for ticketing, reservations, and baggage. These systems can be quite complex. Baggage systems can cost millions of dollars, and cause significant consequences in case of failure. In "Case in Point: An Information System Gone Awry: London-Heathrow International Airport," the baggage handling system cost \$500 million dollars to design, create, and test. This system failed on the first day of opening, causing flights to be delayed and bags to be misrouted. An analyst estimates the costs of the failure to be over \$50 million dollars (Valacich, & Schneider, 2009).

Airlines have extensive internal LAN or WLAN systems throughout the airport. For example, a LAN system could connect the ticketing area with the gate area. Airlines will also have a business to business (B2B) connection with suppliers and the airport authority - these connections must be secure. While the majority of airline systems are wired, recent trends indicate an increase in the use of wireless networks, which opens new security holes. Finally, the airlines' backend systems will have a type of VPN encrypted connection to protect the airlines' regional or corporate offices corporate email, corporate intranet, passenger manifest, ticketing information, plane location, personnel schedules, etc. The use of information systems by individual airlines is very extensive, and the examples above are only a small subset of airlines' information systems.

The FAA and TSA control the mission critical systems in airports. The FAA specifically maintains and operates the Air Traffic control systems (Leng, 2009): "Air traffic control (ATC) is a service provided by ground-based controllers who direct aircraft on the ground and in the air. The primary purpose of ATC systems worldwide is to separate aircraft to prevent collisions, to organize and expedite the flow of traffic, and to provide information and other support for pilots when able. ATC center consists of computers, radar, navigation weather data systems, and radio communications to allow aircraft to land, take off, and taxi without incident. In some countries, ATC may also play a security or defense role (as in the United States)" (FAA, 2011) TSA is part of the Department of Homeland

Security (DHS). The TSA is solely responsible for screening passengers and checked and carry-on baggage at 450 U.S. airports. They also control and maintain “the terror watch list” and “no fly passenger list.” (TSA, 2006)

Passenger systems for internet, Wi-Fi, and cell systems need to be segregated from the internal airport operations systems. While airports are complicated technical environments that may span square miles, separate systems need to be supported that may or may not interact with each other. These systems will see spikes in traffic due to load factors, time of day, and operational concerns. The IT systems architect with the CISO and IT security must determine data load factors balanced with the increased costs of separate systems, and number of access points to critical information systems in an airport. Can a traveler access the network that may contain traffic flow that supports security? Will a spike in systems used by travelers during a weather event degrade security? Can the airport authority afford multiple information systems, routers, and servers or do they attempt to save money by combining services?

## Airport Operations and Security Trust Zones

Examining the steps a typical passenger might take in an airport can inform basic understanding of information systems in airport operations. From the time a passenger decides to purchase a ticket, airline information systems are engaged and collecting credit card or other banking information necessary to process a ticket purchase. When the passenger arrives to check in, personal identification such as driver license or passport is checked. Baggage is logged in for final destination, and placed on a conveyor belt, and is screened in security for explosives and other prohibited items; this occurs whether the passenger conducts curbside or in terminal processing to check in. Next, the passenger must go through a security checkpoint. Systems scan for prohibited substances and items. The passenger can proceed to the departure gate. During the boarding process, the ticket is scanned (often electronically), and the passenger can then board the plane. During take-off, flight, and landing, pilots communicate with air traffic control to safely operate the airplane. Once the passenger arrives at their final destination, baggage is retrieved, and the passenger departs the airport in ground transportation.

From the examination, the functions and associated information systems can be categorized into one of three business lines: ground, security, and flight. The ground business line consists of the ticket purchase, passenger and baggage check in, gate determination, and ticket scan for boarding. All can be described in terms of airline and ground functions. The security business line consists of passenger and baggage screening, and ensuring passengers are safe while in the airport (with monitoring such as cameras) and can be grouped into security functions. Finally, take-off, flight, and landing communication of aircrafts, pilots, and air traffic control (ATC) can be grouped as flight functions. Once the functions are grouped into similar categories, trust zones or can be established around each: the Security trust zone, Airlines and Ground trust zone, and the flight, or National Airspace Systems trust zone. From a security perspective, the trust zones with functions and conceptual security boundaries are illustrated in *Figure 1*.

Figure 2 shows trust zones are formed around information systems functions; security boundaries represent all feeds into and out of zones. Each of the three trust zones has very different goals in terms of cyber security and defending against attacks.

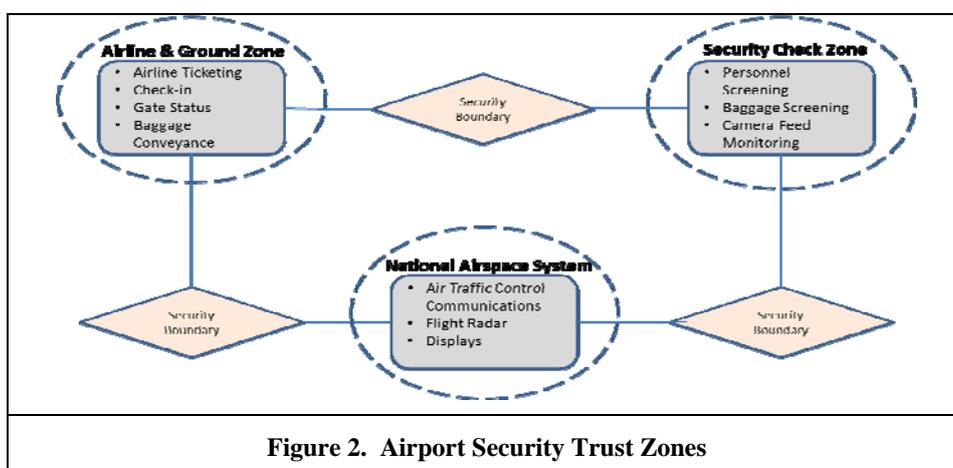


Figure 2. Airport Security Trust Zones

### ***Airline and Ground Trust Zone***

The Airline and Ground trust zone is comprised of the airline ticketing, check-in, gate communication, and baggage conveyance processing. Threats in this trust zone include ticketing criminals obtaining credit card and other personal information for identify fraud and other criminal activities. As a result, encryption, strong identification and authentication, and role based access are incredibly important financial transaction and personal identity activities such as ticketing, and check-in identity verification.

### ***Security Check Trust Zone***

The security Check trust zone systems will have strong elements of all three aspects of cyber security: confidentiality, integrity, and availability. This trust zone must focus on ensuring authorized security personnel only have access to systems necessary to perform security functions. Threats include unauthorized personnel viewing and modifying data, including the insider, and denial of service so personnel and baggage cannot be processed rapidly.

### ***National Airspace System Trust Zone***

Whereas the Security trust zone ensures all three principles are fully addressed, the National Airspace System trust zone is focused primarily on ensuring communications and data are available at all times. For each trust zone, the security controls for ensuring secure operations, while enabling the mission can now be considered by applying risk assessment and AHP techniques.

## **Assessing Security Risks: A Sample of NAS**

### ***Prioritizing Three Security Risk Principles***

Today, many people provide judgment in ensuring safety of airplanes while in flight; any one or even multiple sets of data can have flaws and impreciseness and still meet the mission of safe air travel. However, the total loss or unavailability of some data can be detrimental to ensuring the safety of air travel. As an example, if radar data and/or air to land communications are rendered altogether unavailable to an Air Traffic Controller, there is one less person providing judgment; the controller is one of the most important roles in terms of safe travel in addition to the pilot. Therefore, availability is the most important aspect of security relative to confidentiality and integrity to enable the mission. The next priority is integrity, then confidentiality.

### ***Deciding Goal, Criteria, and Alternatives***

In following AHP, the goal is first set to determine the optimum security controls for the NAS trust zone. It considers the mission of the NAS, which is to continue to ensure safe air travel. Next, the criteria are established identifying the specific threats and vulnerabilities imperative to be addressed by the alternatives. In applying cyber security risk assessment principles, a threat and vulnerability must be coupled to create a resulting impact. That is, a specific threat must exploit, or otherwise exercise, a vulnerability for a successful cyber attack to occur. The criteria are then listed in terms of confidentiality, integrity, and availability for simplifying evaluation. Finally, the alternatives are established. The alternatives are all the possible countermeasures or administrative, logical (or technical) or physical security controls to be considered (Wright & Harmening, 2009). The chosen controls are derived from National Institute of Standards and Technology (NIST) Special Publication standard 800-53 (NIST, 2009).

### ***Rating Security Risks***

In considering the complexity of ensuring the NAS mission, all three types of controls must be employed. The sample list is not exhaustive, but rather highlights the more salient controls or classes of controls to be considered. To conduct a full and complete risk assessment, all of the baselines controls referred to in Appendix D of NIST

Special Publication 800-53 might be considered. The security controls are identified terms of the criteria. Each control will address a specific cyber threat/vulnerability vector (as described in terms of impact).

Table 1 maps the Saaty’s AHP steps, with the risk assessment principles as described in NIST Special Publication 800-30 (Stroneburner et al., 2002), and security controls (sample) as listed in NIST Special Publication 800-53 (2009). In assessing the relative importance of each security principle, confidentiality, integrity, and availability are compared in pairs.

Table 1. Security Risk Assessment on NAS			
Goal	Determine Security Controls for NAS		
Criteria	Confidentiality (Rating: 1)	Integrity (Rating: 2)	Availability (Rating: 3)
		<ul style="list-style-type: none"> <li>•Intercepted data through unauthorized access (1)</li> </ul>	<ul style="list-style-type: none"> <li>•Damage to data through Modification of system (3)</li> <li>•False readings due to data corruption (3)</li> <li>•Unpredictable results due to software bugs (miscalculations) (2)</li> <li>•Damage through unauthorized access (3)</li> </ul>
Alternatives	<ul style="list-style-type: none"> <li>•Encryption in transit (1)</li> <li>•Encryption at rest (1)</li> <li>•Access controls (1)</li> <li>•identification and authentication to ensure confidentiality (1)</li> </ul>	<ul style="list-style-type: none"> <li>•Check hash values of software, applications, scripts (6)</li> <li>•Digital signatures</li> <li>•Software testing and validation (2)</li> <li>•Timestamps (4)</li> <li>•Configuration management (6)</li> <li>•Access controls to ensure identity authentication (6)</li> </ul>	<ul style="list-style-type: none"> <li>•Redundant communications network lines (9)</li> <li>•Spread spectrum (9)</li> <li>•Multiple sources of data provided (9)</li> <li>•High availability servers on certain data sources (radar, ATC systems) (9)</li> <li>•Contingency planning (9)</li> </ul>

## Result Analysis

In comparing confidentiality to integrity, the nature of NAS data is important. Much of NAS data has a short time to live. It is most important over a shifting window of just before a plane is scheduled to take off, to a short while after the plane has landed. While in the air, pilots and air traffic controllers rely on communications, and tracking an airplane accurately is more important than keeping the location secret, in most cases. Once a plane has landed, the value of keeping the data confidential is minimal in terms of cyber security attacks. Compared to integrity, it is more important to maintain accurate data than confidential data.

In comparing availability to integrity, human judgment might be considered. Today, multiple humans provide judgment in ensuring safety of airplanes while in flight; any one or even multiple sets of data can have flaws and impreciseness and still meet the mission of safe air travel. However, the total loss or unavailability of some data can be detrimental to ensuring the safety of air travel. As an example, if radar data and/or air to land communications are rendered altogether unavailable to an Air Traffic Controller, there is one less human providing judgment; the controller is one of the most important roles in terms of safe travel in addition to the pilot. Therefore, from the discussion, availability is the most important aspect of security relative to confidentiality and integrity to enable the mission. The next priority is integrity, then confidentiality. The ratings reflect the priority, with 1 the lowest, and 3 the highest priority.

Next, each specific criterion is compared horizontally to determine ratings. To evaluate the importance of the criteria to the goal, the risk of exposure is considered with the severity of impact to determine the appropriate countermeasures to mitigate the risk, as well as the level of resources to be applied (effort and dollars). The importance or numerical value assigned to each criterion reflects the risk of exposure and severity of impact with a

relative rating. The criteria range is 1 to 3, where 3 are the most critical to address, and 1 is least critical. This numerical value is imprecise, and reflects the preference of the decision maker in terms comparing each criterion to the other criteria. For example, in comparing loss of communications in availability to intercepted data through unauthorized access in confidentiality, we can determine the preference. (Note that this is a sample for illustration purposes, and unauthorized access can also result in a denial of service, so this should be considered in all categories, with different impacts). To a decision maker, the loss of communications is far more detrimental than unauthorized intercepting with no data modification, so a rating of 3 is assigned to loss of communications, and a rating of 1 is assigned to intercepted data. Each is compared and notional ratings are assigned to express relative preference. The relative ratings are provided in Table 1.

Each alternative is reviewed in terms of the criteria. In following the example, the redundant communications lines alternative in the table addresses the availability impact of loss of communications. The ratings are multiplied together to reach the alternative score (Saaty, 2008) provides alternative methodologies for calculating ratings in AHP, which can also be used in place of this methodology). Since availability is the most important in terms of the NAS mission, it follows that several if not all of the impacts in the availability criteria will be weighted more heavily in considering the appropriate controls.

In determining the alternatives with the AHP, the results suggest redundancy in the radar data feeds and the ATC communications lines are paramount. Also important are logical controls to ensure any routers, firewalls, and other devices in the path are redundant; additionally, servers that maintain, process, and present the data to ATCs must be highly redundant (high availability). Administrative controls necessary are contingency planning in the event of loss of one or multiple components or system in the NAS that enables radar and communications. Physical controls such as strong authentication controls to enter the ATC tower operations and server rooms are recommended.

The NAS trust zone risk assessment is the first step of analyzing and determining the security controls of an international airport information systems infrastructure. A similar risk assessment approach is necessary to apply to the other two trust zones as well for completeness. The Airline and Ground trust zone would be considered in terms of confidentiality to address the financial and personal data involved. Encryption of financial data will weigh into ensuring the confidentiality of this data. The Security trust zone may be considered in terms of all three security principles, and might require the highest degree of controls to ensure the security of the information systems in Security trust zone. In addition to strong security boundaries with tight firewall rules, monitoring of security personnel and limiting physical access, where possible, will also be important.

In applying risk assessment using AHP principles, decision makers might consider the method has impreciseness built in. Preferences to certain controls may consciously or unconsciously bias the results in exercising the methodology. In addition, decision makers might have intentional or unintentional motivating factors such as self preservation from unwanted politics and this may be reflected in not choosing unpopular security controls. Another consideration in applying the methodology is security controls or countermeasures can either partially or entirely address threats and vulnerabilities, and may be interdependent. Choosing the impacts to encompass classes of threats and vulnerabilities may assist in minimizing the interdependency. A final consideration in applying this methodology is the cost of the controls. Risk assessment considers cost as a factor in mitigating the impact of a threat-vulnerability pair. If the cost exceeds the willingness to take the risk, the countermeasure or control is not worth the cost to employ. Similarly, in the example the controls mentioned must be considered with the risk. Redundancy of communication lines can be extremely expensive. However, when the risk is losing lives if the communications lines go down, the cost is most likely worthwhile. Assessing the controls in terms of cost and value are also important in employing the methodology.

## **Conclusion**

Airport information systems are a complex multi-layered informational system supporting security, operations, vendors, and travelers. Airport terminals require high levels of computational power in a secure environment (Alani, 2009). The future of airports are going to need for more access for travelers as technology advances and airlines use new automated techniques.

As mentioned, airports are heavily regulated; subsequently, security controls are rarely determined by one person, but rather by a committee of stakeholders and regulators. These committees ensure that the controls enhance security and importantly do not adversely impact ability of any group to accomplish the mission of safe air travel. By creating trust domains to assess cyber security risk, the stakeholders or decision makers with common business

missions and interests can work with regulators to determine the best controls for their trust domain. These stakeholders and regulators would be a subset of the entire airport infrastructure, and more manageable in terms of group decision making. Dividing airport operations into trust domains addresses another factor in determining security controls. In combining the three methodologies of risk assessment, security architecture design, and analytic hierarchy process (AHP) as described, the complexity of addressing how to secure airport operations can now be solved.

In summary, applying cyber security risk assessment using AHP decision analysis methodologies can provide the security professional with a solid approach to complex design of security controls. In airport information systems operations, complexity of diverse business lines coupled with tight regulation add dimensions of complexity that are extremely challenging to any decision maker. Breaking the diverse operations into trust zones and approaching each trust zone with unique criteria and alternatives can tailor security controls. Each trust zone will have threats and vulnerabilities that are specific to the missions and functions, and will vary in impact importance from trust zone to trust zone. The analysis of alternatives will assist decision makers in establishing effective security controls.

## References

- Bodin, L., Gordon, L., & Loeb, M.. 2005. "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, 48(2), pp.79-83.
- CIA. 2011. "The World Factbook," *Central Intelligence Agency*, 26 April 2011, retrieved from <https://www.cia.gov/library/publications/the-world-factbook/geos/us.html>
- FAA. 2011. "Air Traffic Activity System: Airport Operations," *Federal Aviation Administration*, Retrieved from FAA web site <http://aspm.faa.gov/opsnet/sys/Airport.asp>
- Farrokh, M. 2002. "Evaluation and selection of an antivirus and content filtering software," *Information Management & Computer Security*, 10(1), pp.28-32.
- Forman, E., and Gass, S. 2001. "The Analytic Hierarchy Process – An Exposition," *Operations Research*, 49 (4), pp.469-486.
- GAO. 2004. "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," *United States General Accounting Office* (<http://www.gao.gov/new.items/d04321.pdf>).
- Gordon, L.A. and Loeb, M.P. 2001. "A Framework for Using Information Security as a Response to Competitor Analysis Systems," *Communications of the ACM*, 44(9), pp.70-75.
- Kim, S. & Lee, H. 2007. "A study on decision consolidation methods using analytic models for security systems," *Computers & Security*, 26(2), pp.145-153.
- Laskaris, A., Psycharis, N. and Ninou, E. 2007. "Developing user requirements for an airport flight information system," *Proceedings on the 15th IEEE International Requirements Engineering Conference (RE 2007)*, India.
- Leng, R.C. 2009. "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems," *Report*, No. FI-2009-049, retrieved from <http://www.oig.dot.gov/library-item/3911>.
- NIST. 2009. "Recommended Security Controls for Federal Information Systems and Organizations," *NIST Special Publication 800-53, Rev.3, Appendix D*, Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from NIST web site: <http://csrc.nist.gov/publications/PubsFL.html>.
- Pfleeger, C.P. and Pfleeger, S.L. 2007. "Security in computing," Upper Saddle River, N.J.: Prentice Hall.
- Saaty, T. 2008. "Decision making with the analytic hierarchy process," *International Journal of Services Sciences*, 1(1), pp.83-98.
- Saaty, T. 1980. "The Analytic Hierarchy Process," *McGraw Hill*, Revised editions, Paperback (1996, 2000), Pittsburgh: RWS Publications.
- Scholtz, T. 2008. "The structure and content of information security architecture," *Report*, Retrieved from <http://www.gartner.com/technology/home.jsp>
- Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems*, 14(3), pp.303-315.

- Skinner, R. 2009. "DHS' progress in addressing technical security challenges at Washington Dulles international airport," *Report OIG-09-66*, Washington, D.C.
- Stoneburner, G., Goguen, A., and Feringa, A. 2002. "Risk Management Guide for Information Technology Systems," *NIST Special Publication 800-30*, Rev.3, Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from NIST web site: <http://esrc.nist.gov/publications/PubsFL.html>
- Wallace, K. 2003. "Common Criteria and Protection Profiles: How to Evaluate Information Technology Security," *Report*, Practical Version 1.4b, SANS Institute.
- Wright, J., and Harmening, J. 2009. "Security Management Systems: Security Controls," In Vacca, J. (Ed.), *Computer and Information Security Handbook*, Boston, MA: Morgan Kaufmann Publishers.