A SYSTEMS-THEORETIC SECURITY MODEL FOR LARGE SCALE, COMPLEX SYSTEMS APPLIED TO THE US AIR TRANSPORTATION SYSTEM

by

Joseph R. Laracy

B.S., Computer Engineering (2005)
Minor: Mathematics

University of Illinois at Urbana-Champaign

Submitted to the Engineering Systems Division
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering Systems

at the

Massachusetts Institute of Technology

May, 2007

Signature of author……………………………………………………………………
Engineering Systems Division
May 11, 2007

Certified by……………………………………………………………………………
Nancy G. Leveson
Professor of Engineering Systems
Thesis Supervisor

Accepted by…………………………………………………………………………...
Richard de Neufville
Professor of Engineering Systems
Chairman, Education Committee

A SYSTEMS-THEORETIC SECURITY MODEL

FOR

LARGE SCALE, COMPLEX SYSTEMS

APPLIED TO THE

US AIR TRANSPORTATION SYSTEM

JOSEPH R. LARACY

2007

ABSTRACT

Classical risk-based or game-theoretic security models rely on assumptions from reliability theory and rational expectations economics that are not applicable to security threats. Additionally, these models suffer from serious deficiencies when they are applied to software-intensive, socio-technical systems. Recent work by Leveson in the area of system safety engineering has led to the development of a new accident model for system safety that acknowledges the dynamic complexity of accidents. Systems-Theoretic Accident Models and Processes (STAMP) applies principles from control theory to enforce constraints on hazards and thereby prevent accidents. Appreciating the similarities between safety and security while still acknowledging the differences, this thesis extends STAMP to security problems. In particular, it is applied to identify and mitigate the threats that could emerge in critical infrastructures such as the Air Transportation System. Furthermore, recommendations are provided to assist systems engineers and policy makers in securely transitioning to the Next Generation Air Transportation System (NGATS).

Thesis supervisor: Nancy G. Leveson
Professor of Engineering Systems
Professor of Aeronautics and Astronautics

DEDICATION

This thesis is dedicated to my parents,

Paul and Catherine Laracy,

for their love and support.

ACKNOWLEDGEMENTS

I would like to thank my colleagues, Dr. Nicolas Dulac, Brandon Owens, and Maggie Herring for sharing their knowledge, experience, and time to make this research successful.

Dr. Benjamin Adida was very helpful in understanding security protocol issues relevant to my research.

Laudate Dominum, omnes gentes; laudate eum, omnes populi; quoniam confirmata est super nos misericordia eius et veritas Domini manet in aeternum.

Gloria Patri, et Filio, et Spiritui Sancto. Sicut erat in principio, et nunc, et semper, et in saecula saeculorum. Amen.

No evil shall befall you, no scourge come near your tent. For He will give His angels charge of you to guard you in all your ways. On their hands they will bear you up, lest you dash your foot against a stone.

Psalm 91:10-12

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: Introduction

1.1 Introduction

"Don't cross the street with a dead horse." This popular Midwest expression captures the idea that if one seeks to accomplish a task, one must be prepared. Unfortunately, since the Internet achieved wide-spread usage about ten years ago, the popular media has been flooded with stories of stolen credit cards, distributed denial of service (DDoS) attacks, viruses, and other malicious activities. It is clear that insufficient attention is being paid by the technical community in the area of system security engineering. We are not prepared.

The author's hypothesis is that:

> *System Theoretic Accident Models and Processes (STAMP) can be extended beyond the field of system safety into the realm of security. STAMP will be useful in identifying and controlling threats. Additionally, it will be valuable in early stages of design, identify non-"event" security issues, and illustrate dynamic relationships.*

This proposition is validated by extending the classical STAMP framework for hazard analysis and applying the new methodology to the US Air Transportation System (ATS). First, the security of the current ATS will be studied. After that, changes resulting from the transition from the current architecture to NGATS will be examined. The results of the analysis are presented in a format accessible to system engineers who design the Next Generation Air Transportation System and policy makers who influence and direct it.

According to Ross Anderson,

> "security engineering is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves. Security engineering requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of applied psychology, organizational and audit methods, and the law. System engineering skills, from business process analysis through software engineering to evaluation and testing, are also important…" (Anderson 2001)

The interdisciplinary nature of the security problem is one of the key factors that makes the solution so elusive. Traditional, disciplinary approaches on their own are often insufficient to accomplish the security goals of a system. Only a *comprehensive* methodology has the potential to succeed.

Many security related terms have moved into colloquial language and unfortunately lost their rigorous definitions. Key security terms are defined below to remove all ambiguity about the author's use of the terms in this thesis.

Security: A *system* property that implies protection of the informational, operational, and physical elements from malicious intent.

Vulnerability: A weakness in a system that can be exploited to violate the system's intended behavior relative to security.

Threat: An intentional action aimed at exploiting a vulnerability.

It is also necessary to clarify the relationship between system security engineering and similar activities such as information assurance (IA), reliability engineering, safety engineering, and trust. The 1996 DoD Directive 5-3600.1 defines IA as "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, and non-repudiation; including providing for restoration of the information system by incorporation, detection, and reaction capabilities." In practice, assurance activities usually involve a process of ensuring that availability, integrity, authentication, and non-repudiation activities are performed, not *how* to perform them or *how well* they are performed. Therefore, information assurance is only part of a security engineering solution.

Reliability "is the probability that a component will perform its intended function satisfactorily for a prescribed time and under stipulated conditions." Probability values are usually based on accidental failure rather than malicious intent. However, if security is inadequate, an attacker could decrease the reliability of a system.

Safety "is freedom from accidents or losses." (Leveson 1995) Similarly, safety analyses typically assume no malicious intent, but the results of a security breach could certainly jeopardize the safety of a system. (Hasselbring 2006) define trust as a property that is achieved when correctness, safety, availability, reliability, performance, security, and privacy qualities are met. In this definition, security is a subset of trust because one may trust a system if one perceives it to be safe, reliable, and secure. Clearly, system security and security engineering are related to IA, reliability, safety, and trust, yet are distinct concepts. Nevertheless, much can be learned from methodologies used in safety, assurance, and other related fields. "…Although safety-related systems is a specialized topic, the fruits from safety-related process research could, and should, be applied to support the development of system engineering and the management of other system properties, such as *security* and reliability." (Eliot 1998) Therefore, this thesis investigates the applicability of adapting a safety engineering methodology based on systems theory to a security problem.

1.2 Types of Security

Large scale, complex systems require physical, communication, computer, information, and operational security. Vulnerabilities often emerge in an engineering system when one or more of the aforementioned types are omitted. This will be shown in detail in the following sections where the Air Transportation System is analyzed. Attackers rarely choose to directly engage the most secure aspects of a system such as the cryptographic algorithms. In the words of the former Internet Chief Protocols Architect, Dave Clark, “Encryption is perfect, no one break codes, they just steal the key.” (Clark 2006)

Physical security is concerned with preventing damage to the physical system as well as theft. The activities to achieve this goal involve maintaining power supplies, controlling physical access to the system, maintaining environmental conditions, and protecting the system from radiation, fire, and other disturbances. Historical approaches to physical security such as guarding a “computer room” are inadequate in large scale systems because computation is distributed among hundreds or thousands of devices. Therefore, securing the physical system requires considering all the physical subsystems and components (Anderson 2001).

Communications security requires the confidentiality, integrity, and availability of data. Confidentiality is achieved *only* when a message is received by the intended recipient(s). Integrity is achieved when the recipient receives the same message that the sender originally transmitted. Finally, receipt of data in an acceptable time window defines availability. Cryptology, the science of cryptography (creating and using cryptosystem) and cryptanalysis (breaking cryptosystems) first emerged in communications security to achieve confidentiality and in some cases integrity (Menezes 1997). With the development of computers, it also found use in computer security.

Computer security is concerned with the activities of authorized and unauthorized users of a computer system. Activities involve prevention, detection, and minimization of consequences. Threats can be classified as both passive and active.

Active Threats	**Passive Threats**
Overwriting	Browsing
Modifying	Aggregation and interference
Inserting	Replaying
Deleting	Leakage
Blocking access to	Copying and distributing

Table 1. Threat Classifications.
Table Source (Herrmann 2002)

A variety of computer security models exist to mitigate the aforementioned threats. The Bell-LaPadula model, commonly referred to as "no read up, no write down" is a formal state transition model that defines access control rules. "Users can only create content at or above their own security level" and "only view content at or below their own security level." (Bell 1973) The model was the foundation of the DoD Trusted Computer System Evaluation Criteria (TCSEC) commonly referred to as the "Orange Book." Although the authors explicitly mention the use of system theory in the development of their model, they still view security as a mathematical property. Significant weaknesses such as neglecting the problem of the clandestine exchange of information motivated other researchers to develop competing models. Additionally, research shifted from military/intelligence computer systems to commercial systems. During this time period, other models focusing on data integrity rather than confidentiality arose such as the Biba model (1977), which is the mathematical dual of Bell-LaPadula – a “read up/write down” model (Bishop 2005).

In a fundamental departure from earlier models, David Clark and David Wilson defined a model that focuses on what users actually do, concentrating on user transactions. Constrained data items are subject to integrity constraints with integrity verification procedures to determine if the system is in a valid state. The model also permits transformation procedures to move the system from one valid state to another (Clark 1987). Not surprisingly, hybrid models also exist, such as the Chinese Wall Model, that are concerned with both integrity and confidentiality (Bishop 2005).

In the early 1990s, the convergence of computers and communication gave birth to the concept of *information security*. It is “the protection of information against unauthorized disclosure, transfer, or destruction, whether accidental or intentional.” Standards and procedures for information security were initially developed by primarily European and International bodies. The US response emerging from the NSA and Office of the Secretary of Defense became the Systems Security Engineering Capability Maturity Model (SEE-CMM). SEE-CMM is structured very similar to its predecessors: the system engineering capability maturity model and software engineering capability maturity model. As a result, it unfortunately suffers from many of the same weaknesses. According to Bach: “At worst, the CMM is a whitewash that obscures the true dynamics of software engineering and suppresses alternative models.” (Bach 1994)

The final type of security is operational security. Procedures include personnel operations, data operations (such as audit procedures), and administrative operations. Security clearances and badging, security training, virus scan procedures, backup schedules, password rules, computer usage rules, and other similar activities fall into operations security. Like physical security, operations security is far more challenging to achieve in distributed, complex systems (DoD 2006). Tight coupling related to security exists among infrastructure systems. Telecommunications, banking, power, oil and gas distribution, water, transportation, EMS, and government interact and exhibit intricate dependences.

CHAPTER 2: The Next Generation Air Transportation System (NGATS)

The Next Generation Air Transportation System

In 2004, the US Congress passed the Vision 100 – Century of Aviation Reauthorization Act in response to pressures on the current US Air Transportation System. Post 9/11 economics and demand asymptotically approaching capacity at many key airports necessitates a radically new approach. A senior policy team made up of the Secretary of Transportation (Chair), Secretary of Defense, Secretary of Homeland Security, Secretary of Commerce, Director of the Office of Science and Technology Policy, Administrator of the National Aeronautics and Space Administration (NASA), and Administrator of the Federal Aviation Administration (FAA) was formed to provide policy guidance. Also, a Joint Program Development Office (JPDO) was created to manage the development of NGATS.

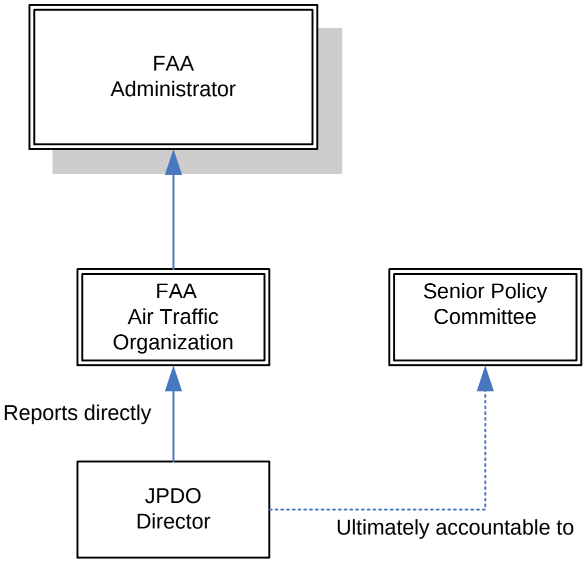

Figure 1. JPDO Reporting Lines.

On page *ii* of the Strategic Plan, it states that the JPDO strategies are centered on:

- Developing the airport infrastructure to meet future demand by empowering local communities and regions to create alternative concepts of how airports will be used and managed in the future.
- Establishing an effective security system without limiting mobility or civil liberties by embedding security measures throughout the air transportation system – from curb to curb. Creating a transparent set of security layers will deliver security without creating undue delays, limiting access, or adding excessive costs and time.
- Creating a responsive air traffic system by devising alternative concepts of airspace and airport operations to serve present and future aircraft. As new vehicle classes and business models emerge, such as remotely operated vehicles and spaceports, the safe and efficient operation of all vehicles in the National Airspace System will be critical to creating new markets in aviation and beyond.
- Providing each traveler and operator in the system with the specific situational awareness they need to reach decisions through the creation of a combined information network. All users of the system will have access to the air transportation system data they require for their operations.
- Managing safety through a comprehensive and proactive approach that can integrate major changes, such as new technologies or procedures. This will be done in a timely manner and without compromising aviation's current superior safety record.
- Introducing new policies, operational procedures, and technologies to minimize the impact of noise and emissions on the environment and eliminate ground contaminants at airports. This effort includes exploration of alternative fuels, engine and aircraft designs. These actions will result in reduced environmental impact and sustained aviation growth.
- Reducing the impact of weather on air travel through a system wide capability for enhanced weather observations and forecasts, integrating them with the tools used by air system operators. This capability will substantially improve airspace capacity and efficiency while enhancing safety.
- Harmonizing equipage and operations globally by developing and employing uniform standards, procedures, and air and space transportation policies worldwide, enhancing safety and efficiency on a global scale.

There has never been a transformation effort similar to this one with as many stakeholders and as broad in scope. The objective of this plan is to provide the opportunity for creative solutions for the future of air transportation, our security and our hope for a vibrant future.

Table 2. NGATS Strategic Plan.

Table Source (JPDO 2004)

The United States Air Transportation System faces challenges in three areas: security, gridlock, and maintaining global leadership. The current customs service will need to be substantially modified to accommodate the projected three-fold increase in international passenger and cargo volume resulting in 120 million additional passengers by 2015 (FAA 2004a). Gridlock is already a major problem at US metropolitan airports. One hour wait times were encountered by millions of American in 2000 (FAA 2004b). Economic models predict that in 2025, US consumers could lose $20 billion due to congestion.

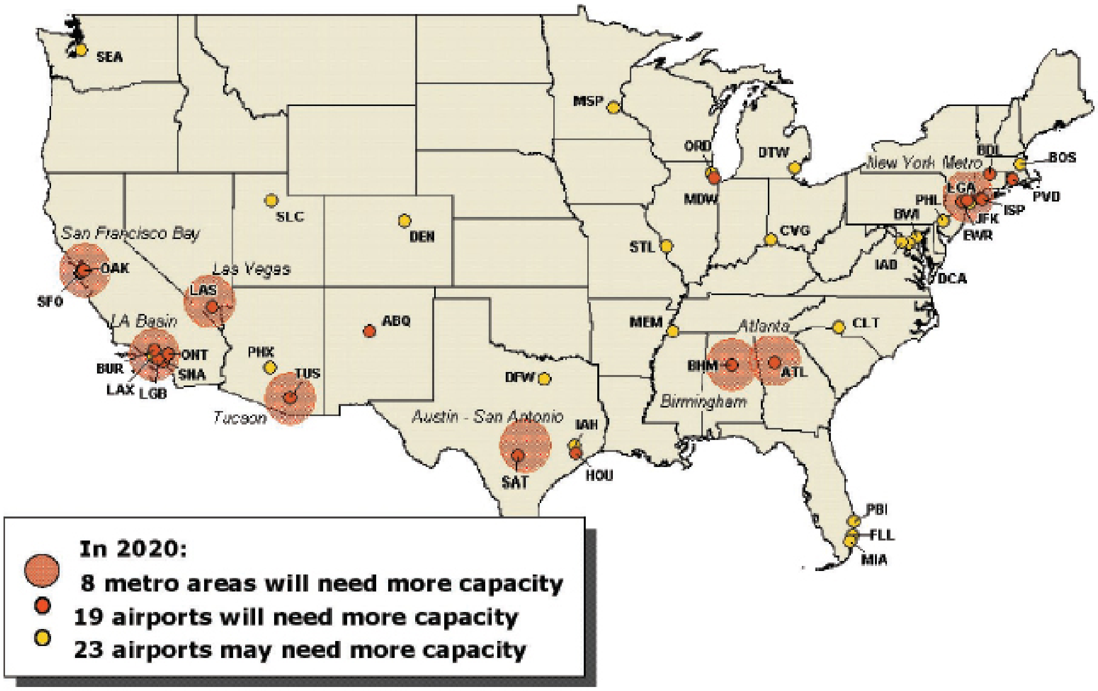

Figure 2. Estimated Congestion in 2020.
Image Source (JPDO 2004)

If the congestion issue is not resolved, same-day travel and reliable scheduled travel will exist only in people's memories. By 2025, twenty additional airports will have 500,000 annual departures (the size of Detroit's current operations) (FAA 2004b). According to the JPDO, "The current method of handling traffic flow will not be able to adapt to the higher volume and density demanded of it in the future, even if twice as many or more resources are devoted to it." The red and black areas in the graphic below dominate most of the US land area and indicate demand exceeding supply.

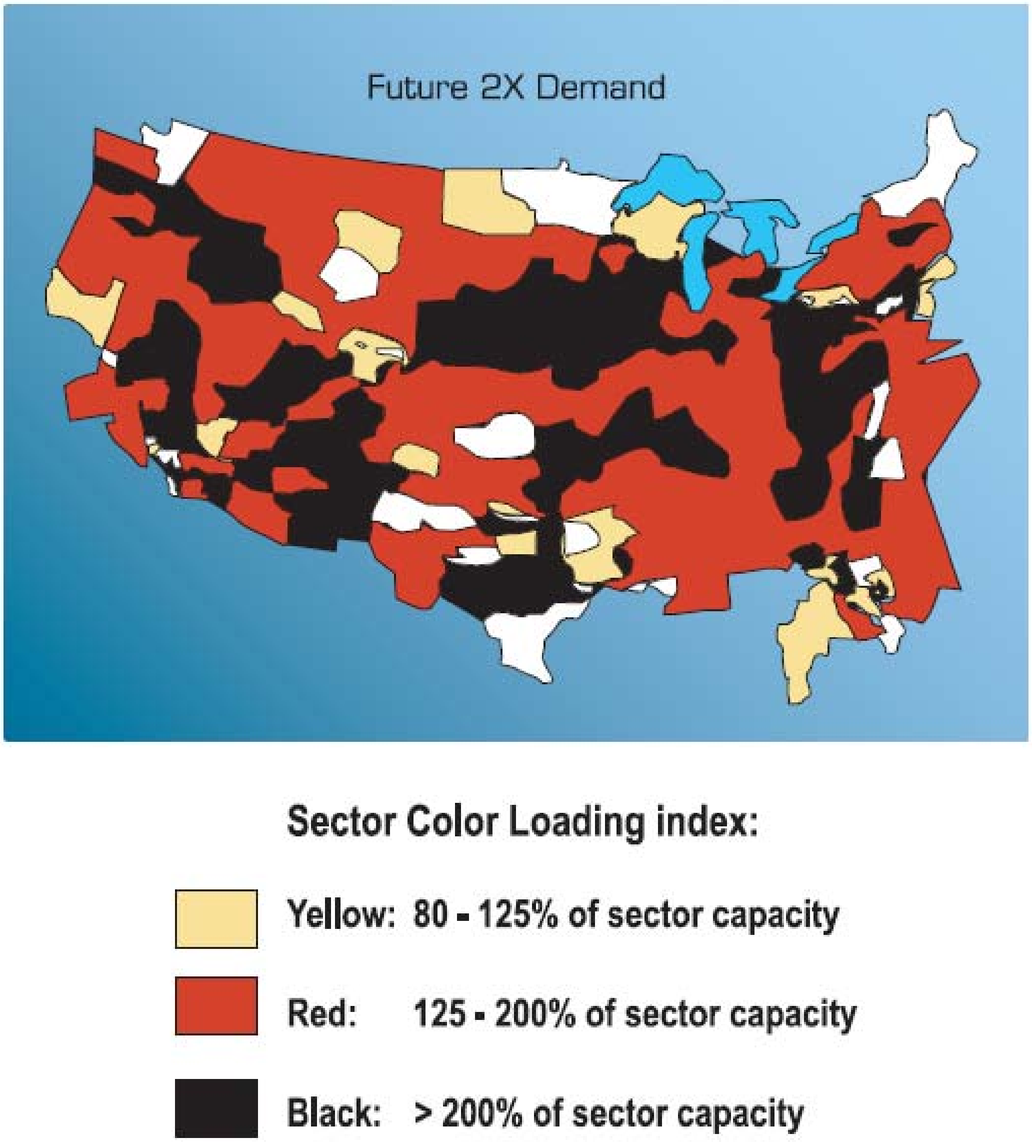
Future 2X Demand
Sector Color Loading index:
Yellow: 80 - 125% of sector capacity
Red: 125 - 200% of sector capacity
Black: > 200% of sector capacity

Figure 3. Effect of Doubling Demand on Sectors.
Image Source (JPDO 2004)

The variety of transportation options will grow in the next two decades. UAVs, micro-jets (5 passengers), super jumbo-jets (600 passengers +), and other 21st century innovations will radically change US airspace. Small perturbations in how people travel and transport goods will require major overhauls of the transportation infrastructure. "A shift of 2% of today's commercial passenger to micro-jets that seat 4-6 passengers would result in triple the number of flights in order to carry the same number of passengers." (JPDO 2004)

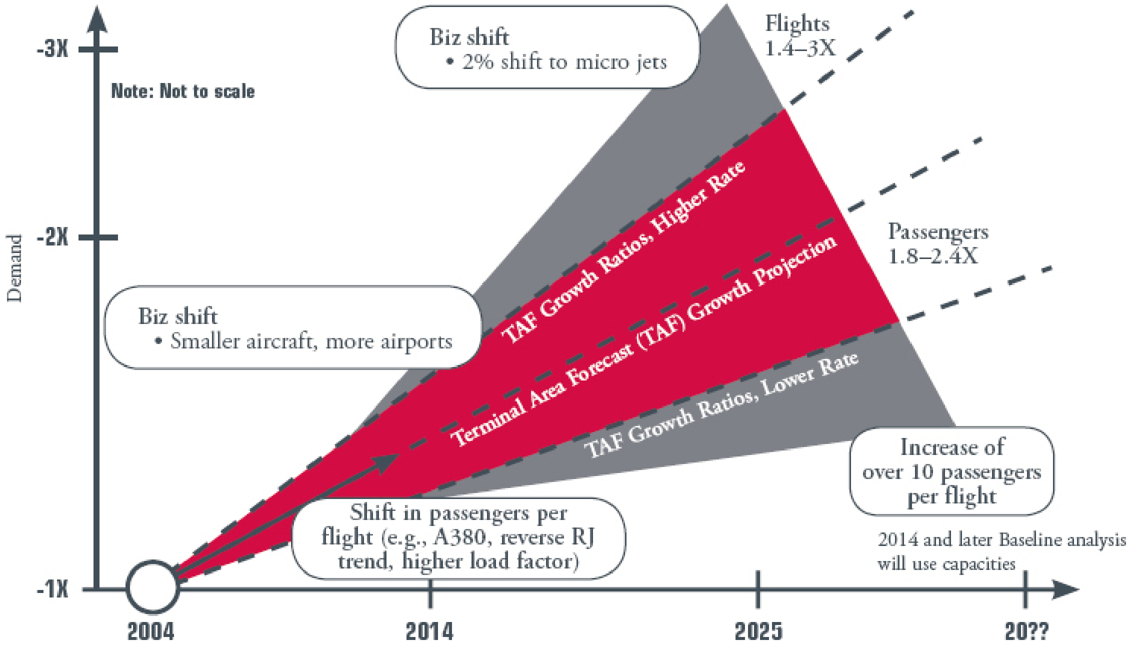

Figure 4. Uncertainty in Vehicle Capacity.
Image Source (JPDO 2004)

The JPDO has three performance goals:

- Satisfy future growth in demand (up to three times current levels) and operational diversity
- Reduce transit time and increase predictability (domestic curb-to-curb transit time cut by 30%)
- Minimize the impact of weather and other disruptions (95% on time)

However, the uncertainty associated with the profile of aircraft in twenty years makes it difficult to develop a strategy. Industry estimates for micro-jet usage place operations at 40% of daily passenger travel by 2025 (Royce 2004). The current 5000 airports will need to adapt as daily passenger traffic will rise from 2 million to 4-5 million and cargo traffic will triple. Parallel runways, improved wake vortex sensing, and relaxation of single runway occupancy restrictions are being considered to improve system throughput. Without expensive ground-based equipment, the JPDO hopes to have precision approaches available on every US runway.

Aircraft themselves will be transformed to achieve the goals of NGATS. "Future aircraft will sense, control, communicate, and navigate with increasing levels of autonomy." In some cases co-pilots will be replaced by computers, in others, there will be no pilot at all. UAVs will be subject to reduced separation standards and more flexible spacing will be applied to both aircraft in-flight and on the ground. Additionally, a paradigmatic shift is planned for air traffic control. Controllers will move from controlling individual aircraft to managing airspace based on flows. There exists a large body of knowledge around optimization of network flows that will surely guide these efforts. Also, recent work by Tom Krenzke (Krenzke 2006) at Draper Laboratory offers powerful techniques for UAV route planning. Other changes include (under normal conditions) the elimination of voice communication from data link capable aircraft and the incorporation of new technologies that make two sets of flight procedures, instrument and visual, unnecessary.

Given the proposed changes, the pressing question remains, "How can the US transition to NGATS in such a way that security improves, rather than worsens?" With the goal of assisting JPDO leaders in making an informed decision, this research provides a systematic review of the threats that could emerge. Also, acknowledging the colossal failure of the FAA's Advanced Automation System in the mid 1990s resulting in $2.9

billion spent on a system that was never deployed (Barlas 1996), the JPDO must not allow complexity to grow out of control.

CHAPTER 3: Classical Security Analysis Techniques

3.1 Classical Approaches

A variety of approaches exist both in industrial practice and the academic literature for conducting security analyses on large infrastructure systems. These methods include "best practice engineering," quantitative risk assessment, game theory, and red teaming. The four classical approaches each have their own strengths and weaknesses but unfortunately do not provide total coverage for the *system security* problem.

The most common security technique is simply to apply best practices. This approach is usually conducted in an unsystematic way and reduces or removes only the most obvious vulnerabilities. If a systematic approach is taken to develop a comprehensive body of best practice literature, the best practice approach would be far more useful to engineers developing large systems. Usually, security engineers will employ one or more of the following methods to supplement best practice approaches.

3.2 Risk-Based Security

Risk-based security seeks to quantify security risks by assigning severity and likelihood ratings to attack scenarios. The emphasis of this technique has been on risk-based decision-making whose goal is to direct security investments as opposed to modeling particular kinds of threats. The approach is derived from reliability models of accident causation that are rooted in a chain-of-events perspective. Whether part of a preliminary hazard analysis or an accident reconstruction activity, the reliability engineer attempts to understand the potential or actual accident by identifying the events or faults that could initiate the accident. Such fault and event trees are usually part of a method called probabilistic risk assessment (PRA). The goals of PRA are to estimate both the likelihood and severity of a risk. PRA was developed in the mid 1970s to improve nuclear power plant safety. Professor Norm Rasmussen of MIT chaired the Reactor Safety Study that was the first real probabilistic risk assessment (Apostolakis 2000).

A probabilistic risk assessment is a four step process:

1. Identify undesirable events.
2. Identify accident scenarios (sequences of events).
3. Estimate the probability of each scenario either based on statistical testing data, or expert judgment if scenarios are rare.
4. Rank the accident scenarios according to likelihood.

The framework yields a probability for each undesirable event identified in stage 1.

PRA turned out to be very successful for assessing risks in nuclear power shut-down systems. Such systems were historically very simple, electro-mechanical systems designed to minimize unnecessary complexity and used proven analog electrical technologies. PRA carries with it a number of important assumptions:

1. The events or faults at each node in the trees are collectively exhaustive — all possible events are identified.
2. The events or faults at each node in the trees are mutually exclusive — they cannot occur simultaneously.
3. The probability of each scenario is accurate enough to be useful to decision makers.

In the reactor shut-down system, nuclear engineers with decades of experience can probably develop trees that satisfy the first two assumptions due to their intimate knowledge of reactor design and operation. Furthermore, component technologies such as electrical relays could be extensively tested in the laboratory to compute reliability metrics such as mean time between failures (MTBF).

However, when complex systems like the Space Shuttle are considered, serious questions arise regarding the appropriateness of PRA. For instance, how does software change the picture? How can the MTBF of unique digital electronics be estimated? How many events or faults must be accounted for? Herein lies the problem of applying PRA to software-intensive systems (Laracy 2007a). Software does not wear out and fail; it only implements a set of requirements that may or may not be correct. According to PRA analysts, subjective probability (expert judgment) must be used when thousands of laboratory MTBF tests cannot be carried out. However, software in one environment may produce desirable behavior, while in a slightly different one it may do the worst possible action. Therefore, the meaning of the subjective probability value is not clear. Additionally, if a spacecraft computer has 128 MB of memory, or 2^{30} bits, then it has $2^{\text{number of bits}}$ or $2^{2\wedge30}$ states. Clearly, each state cannot be analyzed.

Before the Space Shuttle Challenger disaster, NASA headquarters reported the probability of a failure with loss of vehicle and human life as 10^{-5} (Feynman 1986). Before the Space Shuttle Columbia disaster, the reported probability was 1/250 (Stamatelatos 2002). According to NASA space operations spokesman, Allard Beutel, the post-Columbia figure is now 1/100 (Scottberg 2006). Recently, researchers in the field of PRA acknowledged that PRA should not be the sole basis for decision making and that the quantitative results should be part of risk-*informed*, not risk-*based* decisions. They acknowledge that human factors, software, safety culture, and design errors are not well handled by PRA (Apostolakis 2004).

Given the central role of human factors, software, culture, and design errors in security, PRA's applicability to security problems is also dubious. Donn Parker makes an insightful observation in this regard:

> Security risk is not measurable, because the frequencies and impacts of future incidents are mutually dependent variables with unknown mutual dependency under control of unknown and often irrational enemies with unknown skills, knowledge, resources, authority, motives, and objectives – operating from unknown locations at unknown future times with the possible intent of attacking

> known by untreated vulnerabilities that are known to the attackers but unknown to the defenders. (Parker 2007)

None-the-less, a variety of researchers have attempted to supplement pure, reliability-based PRA with other techniques to make it relevant to security.

Michaud and Apostolakis developed a scenario-based methodology to rank elements of an infrastructure system according to their value to the stakeholders. Through a combination of probabilistic risk assessment, multi-attribute utility theory, and graph theory, the methodology models the infrastructure system as a network. After scenarios are generated, a value tree is built to evaluate scenarios and their consequences. The value tree incorporates the disutility of each scenario and vulnerability categories are assigned ranging from level I (Red) to level V (Green). The high level goal of this approach is to answer the following questions (Michaud 2006):

1. What can go wrong?
2. What are its consequences?
3. How likely is it?

However, the first two questions are actually answered by qualitative hazard or threat analysis techniques, while the last question may not be answerable in rare events such as the terrorist attack of 9/11/2001.

In order to address the problem of high-level screening of vulnerabilities, Paté-Cornell and Guikema have synthesized techniques from probabilistic risk assessment, decision analysis, and game theory. Their goal is to develop a "model for setting priorities among threats and among countermeasures." The model is represented by a decision tree, or statically as an influence diagram. In the introduction, the authors acknowledge that:

> Some of the probabilities may be based on frequencies of past events, but most reflect the opinions of the best available experts….results may reflect classic

> biases grounded in the nature of the last attack or in a professional familiarity with some terrifying scenarios. (Pate-Cornel 2002)

In order to address this bias on the subjective probabilities, Paté-Cornell and Guikema suggest enlisting experts from different fields.

It is not clear that this remedy addresses all the concerns raised in the Kahneman's 2002 Nobel Memorial Prize in Economics work on biases in judgment of subjective probabilities. According to Tversky and Kahneman's seminal paper (Tversky 1974), the three common heuristics used from making decisions under uncertainty often lead to flawed results. The first heuristic is *representativeness*. *Representativeness* is used by humans when they are challenged to guess the probability that an event α belongs to a process β. Insensitivity to prior probability outcomes, sample size, and predictability, as well as the illusion of validity, and misconceptions of regression, plague the use of representative thinking for generated subjective probabilities. The second heuristic is *availability* (of instances or scenarios). *Availability* is used to assess the plausibility of a particular development. It suffers from biases due to the retrievability of instances, the effectiveness of a search set, and imaginability, as well as illusory correlation. The last heuristic is called *adjustment from the anchor*. Often, people estimate values, such a probabilities, by starting with an initial p_0 and make a series of adjustments until a desirable p_f is obtained. However, it has been shown that "different starting points yield different estimates, which are biased toward the initial value." A*djustment from the anchor* is prone to insufficient adjustment, biases in the evaluation of conjunctive and disjunctive events, and anchoring in the assessment of subjective probability distributions.

Paté-Cornell and Guikema's technique has four steps:

1. Identification of an exhaustive set of *classes* of attack scenarios
2. Assessment of the likelihood of occurrences of these classes of scenarios based on intent, chances of success given intent, and attractiveness from the point of view of the perpetrators.
3. Prioritization of these attack scenarios based both on their likelihood and on the expected damage to the US if they occur.
4. Modeling of the dynamics of the situation as a "game" between the different parties with learning on both sides, by updating both the model and the parameter values after each time period. (Pate-Cornel 2002)

A key assumption in this analysis is the use of the rational decision analysis model in descriptive mode (Von Neumann 1953). However, the authors rightly point out that "in reality, human behaviors generally violate these axioms (of rationality). For example, people show circularity in preferences (which they often do not know how to evaluate), and do not necessarily satisfy the 'sure thing principle'(Savage 1954) ."(Pate-Cornel 2002) "The Sure-Thing Principle says that if a decision maker would take a certain action if he knew that an event E was obtained, and also if he knew that its negation E' was obtained, then he should take that action even if he knows nothing about E." (Aumann 2005)

In the game-theoretic aspect of the approach, each side assigns a probability distribution on the beliefs of the other side. The US computes the probability of an attack scenario with the following method (Pate-Cornel 2002):

$$E_{TE}(U_j \mid W_i, I_j) = P_{TE}(S \mid W_i, I_j) \times U_j(S \mid W_i, I_j)$$

E_{TE}: US assessment of the expected value of a random variable as viewed by the terrorists.
U_j: Utility function (preferences) of group j.
W_i: Choice of weapon for an attack attempt.
I_j: Intent from group j to attack in the next time period.
P_{TE}: Probability as assessed by the US of a terrorist probability estimation (e.g., of their own chances of success in a specified attack scenario).
S: Successful attack (of any kind)

Where

$$U_j(S \mid W_i, I_j) = \sum_k \nu(X_{ijk})$$

ν (X_{ijk}): Value of attribute k (e.g., the number of causalities inflicted) for terrorist group j (e.g., Islamic fundamentalists) in the case of a successful attack with weapon i (e.g., a biological attack).

The utilities are then renormalized to provide probabilities of terrorist actions W_i for each group conditional on that group's intent I_j to launch an attack. It is important to note that there is great uncertainty about the terrorist's utility functions. The model also assumes that for each time step of the game, each terrorist group plans only *one* type of attack. Furthermore, "the probability of a specified type of attack is proportional to the ease of execution and the damage inflicted on the US." (Pate-Cornel 2002) Finally, the attack scenarios are assumed to be mutually exclusive and collectively exhaustive. Therefore, the probability as assessed by the US to represent US beliefs of scenario W_i, given intent to attack by group j (I_j) is:

$$P_{US}(W_i \mid I_j) = \frac{E_{TE}(U_j \mid W_i, I_j)}{\sum_i E_{TE}(U_j \mid W_i, I_j)}.$$

Additional steps including cost-benefit analysis identify the countermeasures that produce the greatest decrease in disutility to the US. A graphical illustration of a game theory example is given below.

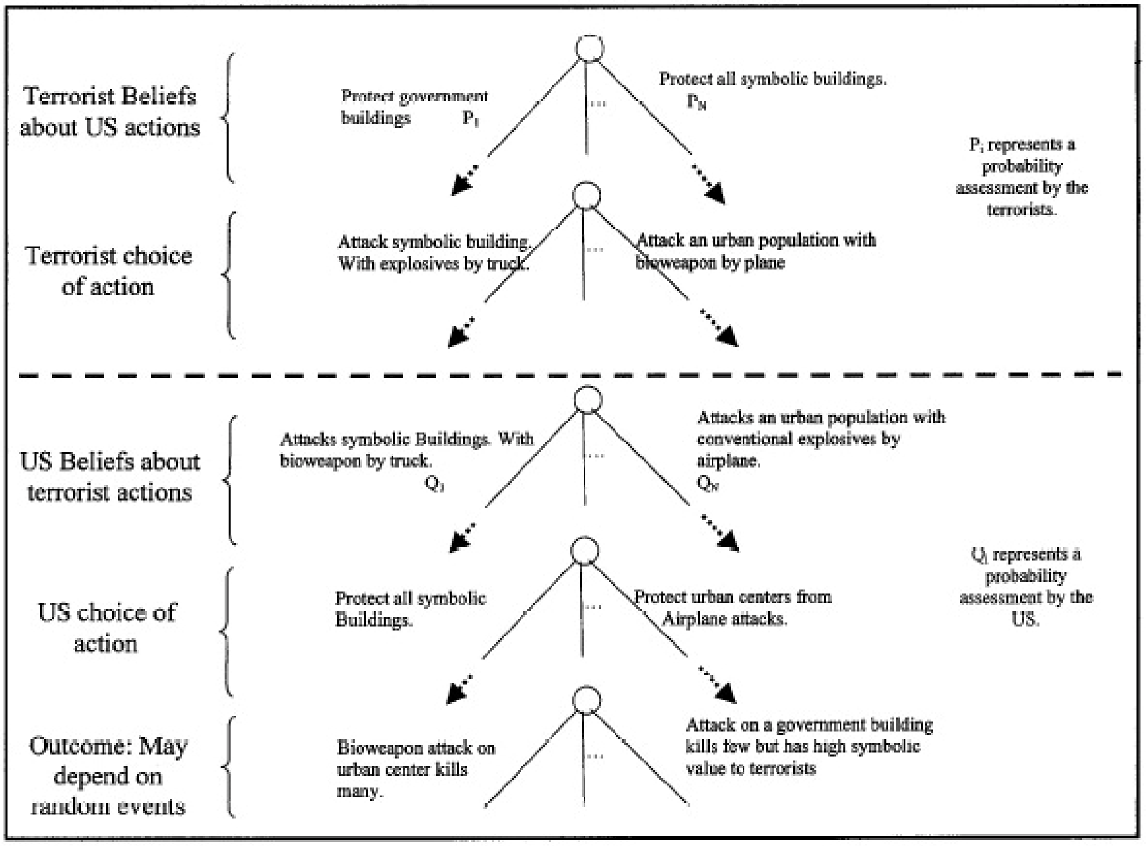
Terrorist Beliefs about US actions
Protect government buildings P_1
...
Protect all symbolic buildings. P_N
P_i represents a probability assessment by the terrorists.
Terrorist choice of action
Attack symbolic building. With explosives by truck.
...
Attack an urban population with bioweapon by plane
US Beliefs about terrorist actions
Attacks symbolic Buildings. With bioweapon by truck. Q_1
...
Attacks an urban population with conventional explosives by airplane. Q_N
Q_i represents a probability assessment by the US.
US choice of action
Protect all symbolic Buildings.
...
Protect urban centers from Airplane attacks.
Outcome: May depend on random events
Bioweapon attack on urban center kills many.
...
Attack on a government building kills few but has high symbolic value to terrorists

Figure 5. Game Theoretic Model for Terrorism.
Image Source (Pate-Cornel 2002)

Patterson and Apostolakis build on Paté-Cornell and Guikema's overarching model to define a screening methodology in order to determine the distribution of anti-terrorism funding for regions with multiple critical infrastructures. While this work identifies the sites on which to focus resources, it does not offer insight about what to do at the sites. This research is an extension of work done by Apostolakis and Lemon that merges multi-attribute utility theory (MAUT) and PRA, but also adds Monte Carlo network analysis and geographic analysis methods (Patterson 2006).

Companies such as Risk Management Solutions, Ltd. (RMS) also make use of quantitative methods of risk assessment. In a company technical report on PRA, Woo acknowledges the work of the RAND Corporation in applying complexity theory to social networks. This research has focused on developing models of swarm intelligence based on ant colony principles used in cellular robotic systems. Such an approach acknowledges the architectural structure of many terrorist organizations: decentralized, independent hubs. It is significant that the notion of swarming is not restricted to 3-D spatial location, but could include dimensions "such as support for jihad; disdain for democracy, western culture, etc."(Woo 2002)

Risk Management Solutions is developing a stochastic terrorism model based on an event-tree of detrimental operational factors. This is very surprising given that Dr. Gordon Woo, Chief Architect for the RMS terrorism model, acknowledges that "obviously, a different approach is required to the traditional reductionist bottom-up approach used for modeling the inanimate world of engineering physics: the human dimension to conflict must be incorporated." (Woo 2002) The RMS model is concerned with events of *macroterrorism*, "spectacular acts of terrorism that cause more than $1 billion of loss, or 500 deaths." While he acknowledges that a Monte Carlo simulation would be ideal to analyze the temporal pattern of acts of macroterror, Woo simplifies the problem to a two-state Markov process:

State 1: Relaxed security, conducive conditions for an attack
State 2: Strict security, not conducive conditions for an attack.

This view of the world implies that it is optimal for terrorists to patiently wait for State 1 so as to secure the "infinite payoff of paradise promised to martyrs." (Woo 2002)

Like (Michaud 2006), (Pate-Cornel 2002), and (Patterson 2006), Woo attempts to quantitatively prioritize targets. He begins by invoking Fechner's Law which states that an arithmetic progress in perceptions requires a geometrical progression in their stimuli. expressed as:

$$p = k \times \ln \frac{S}{S_0}$$

where

p: perception
k: empirically determined constant
S: instantaneous stimuli
S_0: initial stimuli.

Therefore, the logarithm of the utility for the C'th city tier and T'th type of attack is:

$$Ln[U(C,T)] = k_0 - k_1 C - k_2 T \ .$$

Weber's law assumes that just noticeable differences are additive. This means that they can be added in an analogous manner to the addition of units of a physical quantity (Britannica. 2007).

Game theory is used to define the functional dependence of target probability on utility to produce the target probability distribution. Al-Qaeda has been shown to adopt a strategy of avoiding targets with unknown security measures, conducting detailed surveillance of potential targets, and randomizing target selection.

For an attack using a specific weapon against:
a target in category [C,T] and
defense D
Let P_D be the probability that the defense is unable to prevent or stop the attack.

For a defense saturation condition expressed as a power law:

$$\frac{\partial P_D}{\partial D} \propto -U[C,T]^{-\lambda} .$$

According to game theory optimization using a mixed strategy, the probability of selecting a target is:

$$\frac{1}{P(U[C,T])} \propto -U[C,T]\frac{\partial P_D}{\partial D} \propto U[C,T]^{1-\lambda}$$

Finally, combining the formulas yields:

$$Ln\{P(U[C,T])\} = a - (\lambda - 1)k_1 C - (\lambda - 1)k_2 T$$

Let $b_1 = (\lambda\text{-}1)k_1$ and $b_2 = (\lambda\text{-}1)k_2$.

So:

$$Log\{P(U[C,T])\} = a - b_1 C - b_2 T$$

The final equation states that the relative likelihood of targets being attacked depends on only b_1 and b_2 (Woo 2002).

A US Department of Homeland Security program at the University of Southern California, the Center for Risk and Economic Analysis of Terrorism Events (CREATE), was created to “evaluate risk, costs, and consequences of terrorism and to guide economically viable investments in countermeasures that will make our Nation safer and more secure.” (USC 2005) The modeling framework of CREATE is based on classical risk analysis.

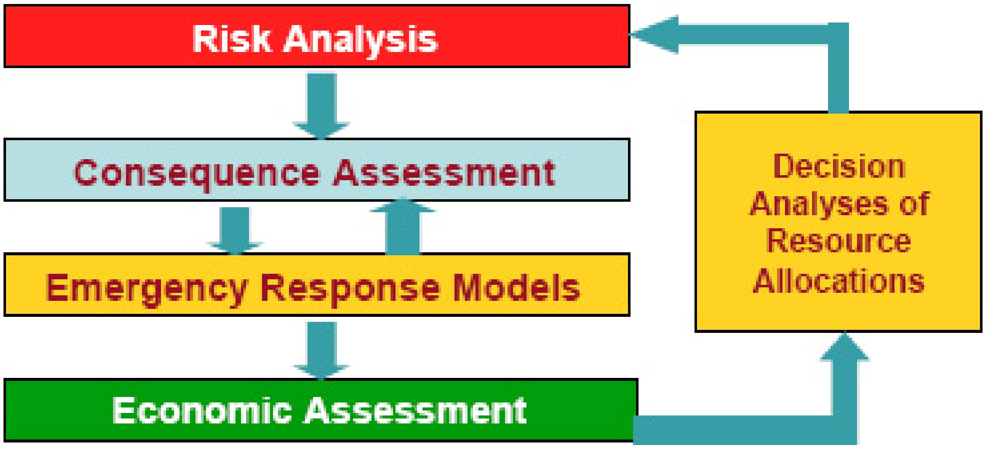
Risk Analysis
Consequence Assessment
Emergency Response Models
Economic Assessment
Decision Analyses of Resource Allocations

Figure 6. CREATE Modeling and Analysis Areas.
Image Source (USC 2005)

One of CREATE's projects is an investigation into improving commercial aviation security against the threat of man-portable-air-defense-systems, MANPADS. The risk analysis makes use of both qualitative methods for studying threat scenarios as well as simulation models for estimating probabilities of successful attacks given characteristics of the weapon, aircraft flight path, attacker location, and other parameters. The economic assessment utilizes a decision tree model (USC 2005).

Haimes and Horowitz, of the University of Virginia Center for Risk Management of Engineering Systems, define a "holistic approach for managing intelligence collection and analysis." The first component is a hierarchical, multi-objective, probabilistic, and dynamic input-output model that calculates the economic losses associated with attacks on particular targets. The second component combines a hierarchical holographic model (HHM) and a two-player HHM game for information collection on target vulnerabilities based on expert opinion. Risk filtering, ranking, and management (RFRM) is then employed to reduce the number of risk scenarios from the HHM. A partitioned multi-objective risk method (PMRM) analyzes the risks of extreme events. The fifth and sixth parts include a Bayesian analysis for adding value and capability to intelligence and a sequential decision-making process under uncertainty using the multi-objective decision tree (MODT). Finally, Bayes' theorem and Bellman's principles of optimality define a resource allocation method for intelligence analysis (Haimes 2004).

The effect of misapplying quantitative, probabilistic techniques can create a dangerous illusion of strong security. Good work has been done by Dean Wilkening in missile defense strategy development comparing shoot-look-shoot and barrage firing options (Wilkening 1998). This work was based on extensive *empirical data* from test firing exercises and live military operations. Unfortunately, much of the research that attempts to apply traditional risk models from electro-mechanical reliability engineering without experimental data to security problems suffers from serious flaws. For the same reasons that these models are not applicable to system safety, they are also not applicable to system security, i.e. human factors, software issues, the influence of organizational culture, and design errors. Additionally, security problems introduce an *intelligent* adversary – the threat is adaptive:

> In most applications of risk analysis, risk reduction actions follow the usual "80/20 rule" (originally due to Pareto) – the decision-maker can review a list of possible actions, ranked based on the magnitude of risk reduction per unit cost, and choose the most cost-effective, typically getting something on the order of 80% of the benefit for perhaps 20% of the cost. This does not work so well in the security context (especially if the attacker can readily observe system defenses), since the effectiveness of investments in defending one component can depend critically on whether other components have also been hardened (or, conversely, if the attacker can easily identify alternative targets that have not been hardened. (Bier 2005)

Questions of likelihood for rare events cannot be accurately estimated and expert judgment is often systemically biased. Simplifying assumptions such as assuming that terrorist groups will only plan one method of attack are inconsistent with reality.

Furthermore, developing event or decision trees with mutually exclusive and collectively exhaustive attack scenarios at each node can easily produce a tree that exceeds intellectual manageability. Therefore, it is unlikely that reductionist, bottom-up approaches will succeed.

3.3 Game Theory

(Bier 2005) asserts that managing risks from intelligent adversaries is very different from other types of risk and suggests game theory over decision theory. Previous work in this area focused on “policy insights” such as the relative merits of deterrence and other protective measures (Frey 2003). (Sandler 2003) presents a number of compelling reasons for the applicability of game theory to security problems:

1. Game theory captures the strategic interactions between terrorists and a targeted government, where actions are interdependent and, thus, cannot be analyzed as though one side is passive.
2. Strategic interactions among rational actors, who are trying to act according to how they think their counterparts will act and react, characterize the interface among terrorists or among alternative targets.
3. In terrorist situations, each side issues threats and promises to gain a strategic advantage.
4. Terrorists and governments abide by the underlying rationality assumption of game theory, where a player maximizes a goal subject to constraints.
5. Game-theoretic notions of bargaining are applicable to hostage negotiations and terrorist campaign negotiations over demands.
6. Uncertainty and learning in a strategic environment are relevant to all aspects of terrorism, in which the terrorists or government or both are not completely informed.

However, game theory “requires strong assumptions about the availability of mutual information and the rationality of opponents.” (Banks 2007) As mentioned earlier, empirical work by (Tversky 1974) has shown that these assumptions often break down in reality. Additionally, traditional games are organized to pursue a minimax solution for a two-person, zero-sum game. However, as Banks and Anderson point out, such a model is only an approximation because defender and attacker will value successful and failed attacks differently (Banks 2007).

Many game-theory models of security carry the traditional, simplifying assumption that the probability of a successful terrorist attack on a location is a convex function of the defensive resources. Some security measures, such as relocating a facility to a more secure location, are inherently discrete. Discretization introduces step changes into the function so there is no longer a smooth, convex function due to declining marginal returns on defensive investments. Also, if a particular level of defensive investment completely deters an attack, the probability of terrorist success drops rapidly beyond that point. This scenario would also produce a non-convex function in certain regions. When non-convex functions are permitted, multiple local optima may emerge, thereby complicating the defense resource allocation problem (Bier 2005).

In order to populate payoff matrices with values, statistical techniques from quantitative risk assessment are usually used (Banks 2007). The problems identified in the previous session can create the following conundrum.

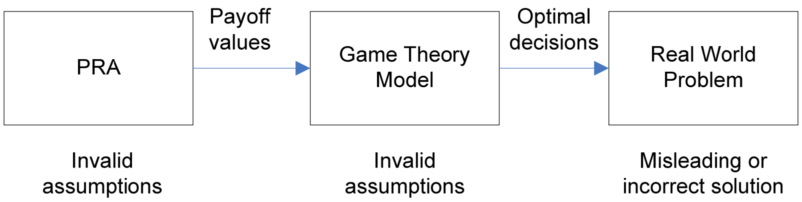

Figure 7. Propagation of Bad Assumptions.

For example, given a Smallpox scenario, the following cost matrix could be defined:

		No Attack	**Single Attack**	**Multiple Attacks**
Target Group for Vaccine	**Stockpile Vaccine**	C_{11}	C_{12}	C_{13}
	Biosurveillance	C_{21}	C_{22}	C_{23}
	Key Personnel	C_{31}	C_{32}	C_{33}
	Everyone	C_{41}	C_{42}	C_{43}

Table 3. Smallpox Payoff Matrix.
Table Source (Banks 2007)

Each C_{ij} corresponds to payoffs (or costs) that would result from a particular combination of attack and defense. Many factors go into the computation of the C_{ij}, including an estimate for the monetary value of human life, $2.86 million according to the US Department of Transportation. However, a great deal of uncertainty persists:

> The total cost in each cell is a random variable. These random variables are not independent, since components of the total cost are common to multiple cells. Thus it is appropriate to regard the entire game theory table as a multivariate random variable whose joint distribution is required for satisfactory analysis. (Banks 2007)

If the minimax criterion is invoked for the normal-form game, the analyst assumes that the two players are unaware of the judgment made by their adversary until committed to a course of action. Therefore, an extensive-form version of the game is created that uses the minimum expected loss criteria. Expert judgment populates the table below:

		No Attack	**Single Attack**	**Multiple Attacks**
Target Group for Vaccine	**Stockpile Vaccine**	0.95	0.040	0.010
	Biosurveillance	0.96	0.035	0.005
	Key Personnel	0.96	0.039	0.001
	Everyone	0.99	0.005	0.005

Table 4. Baseline Probabilities of Attacks.
Table Source (Banks 2007)

Probabilities in Table 3 are multiplied by payoffs (or costs) in Table 2 and the results are summed along the rows. At this point, the criterion chooses the defense, in this case a target group for the vaccine, with the minimum expected loss.

One useful insight that a game-theoretic analysis can offer even if the payoff numbers are imprecise is problem framing. For example, in a scenario where both the US and European Union (EU) are concerned about the threat of Iranian ballistic missile attack, three categories of games emerge:

	European Union	
United States	**Preempt**	**Do not preempt**
Matrix *a*: PRISONERS DILEMNA		
Preempt	2, 2	-2, 4
Do not preempt	4, -2	Nash 0,0
Matrix *b*: asymmetric-dominance equilibrium		
Preempt	6, 2	Nash 2, 4
Do not preempt	4, -2	0, 0
Matrix *c*: COORDINATION		
Preempt	Nash 2, 2	-4, 0
Do not preempt	0, -4	Nash 0,0

Table 5. Three Alternative Game Forms for Preemption.
Table Source (Sandler 2003)

In Matrix *a,* preemption by each country confers four in benefits on both countries at a cost of six to the country doing the preemption.   This creates a prisoners dilemma because an incentive exists for not taking action against the Iranian threat. Matrix *b* represents a game where the US gains a net benefit for preempting as it is Iran's preferred target. Preemption costs six units while US preemption confers eight in benefits. EU preemption credits four units to both parties. As the authors point at, "This game representation may well characterize the US position after 9/11, where US action was going to yield high payoffs to the US government." (Sandler 2003) However, another game is possible as shown in Matrix *c*. Preemption by one nation may confer no reward and only imply a cost to the preemptor. However, in a coordination game, joint preemption yields the greatest benefit to both nations. Finally, as the three matrices indicate, Nash equilibriums arise whenever no player has anything to gain by changing only his strategy unilaterally. For a related game that factors in a deterrence option, see (Arce M. 2005).

According to (Fricker 2005), game theory's role in security focuses on analyses related to:

1. Assessing strategies for how national antiterrorism expenditures,
2. Measuring how military strategies encourage/discourage terrorism,
3. Assessing insurance risks, and
4. Evaluating the effects of focusing either on deterrence or preemption.

As the list above indicates, game-theoretic models focus on strategic decision making. Questions of how to design and operate infrastructure systems that may be the target of terrorist attacks is the focus of the systems-theoretic analysis later in this thesis.

3.4 Red Teaming

Red teaming is an excellent activity to complement other security analyses as well as reduce the complacency that often sets in after extended periods without attacks. The goal of any red team is to challenge the plans, programs, and assumptions of the client organization. Teams may challenge organizations at strategic, operational, or tactical levels depending on the area that needs the most attention. The words of Dr. William Schneider, Jr., Chairman of the Defense Science Board, best capture the state of red teaming: “Red teams can be a powerful tool to understand risks and increase options. However, the record of use of red teams in DoD is mixed at best.” (Schneider 2003)

The greatest benefit derived from red teaming exercises is “hedging against catastrophic surprises.” A good red team is capable of elucidating a deeper understanding of an adversary’s options, and identifying vulnerabilities in concepts, programs, plans, postures, and strategies. Red teams also challenge “the accepted assumptions and accepted solutions” as well as identify inexperience. They may function as surrogate adversaries, devil’s advocates, or simply as sources of independent judgment.

Schneider also points out that “red teaming is important but it is not easy nor often done very well.” He identifies the following causes of failure (Schneider 2003):

The red team:

1. Does not take its assignment seriously.
2. Could lose its independence.
3. Could be too removed from the decision making process.
4. Could have inadequate interaction with the “blue” (team) and be viewed as just another sideline critic.
5. Could destroy the integrity of the process and lose the confidence of decision makers by leaking its findings to outsiders.

Red team effectiveness is easily impaired by a corporate culture that does not value criticism and challenge, managers that do not want issues to arise that may “rock the boat,” dysfunctional interaction between red and blue teams, unqualified red team staff, and calling in a red team when the problem has grown out of control. The red team must have independence with accountability as well as a process that enables the game results to be seriously considered by senior management (Schneider 2003).

Unfortunately, the red teaming process failed miserably before 9/11/2001. Testimony by Bogdan Dzakovic, an FAA Red Team veteran, to the National Commission on Terrorist Attacks Upon the United States, on May 22, 2003, reveals how a good red team can become completely ineffective in the face of management resistance. The Presidential Commission investigating the bombing of Pan Am 103 in 1990 created the FAA red teams that are in place today. After the TWA 800 crash, Congress passed the FAA Reauthorization Act of 1996. The law states that “…the Administrator [of FAA] shall conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of such systems…” Later, in 1997, a White House Commission stated that “…Red Team testing should also be increased by the FAA, and incorporated as a regular part of airport security action plans. Frequent, sophisticated attempts by these Red Teams to find ways to dodge security measures are an important part of finding weaknesses in the system and anticipating what sophisticated adversaries of our nation might attempt.”(Dzakovic 2003)

Unfortunately, as Dzakovic's testimony indicates, the value of these red teams has been seriously undercut:

> Although we breached security with ridiculous ease up to 90% of the time, the FAA suppressed these warnings. Instead we were ordered not to retest airports where we found particularly egregious vulnerabilities to see if the problems had been fixed. Finally, the agency started providing advance notification of when we would be conducting our "undercover" tests and what we would be checking. (Dzakovic 2003)

For example, in the late 1990s, over two-thirds of red teams breached airport security with firearms undetected. This revelation led the FAA to stop testing with guns. According to Dzakovic, managers at the highest levels of the FAA chose to ignore warnings such as these: "What happened on 9-11 was not a failure of the system, it was a system designed for failure. FAA very consciously and deliberately orchestrated a dangerous façade of security." (Dzakovic 2003)

Compelling evidence existed prior to 9/11 of the likelihood and severity of this threat. In testimony to the US Senate Committee on Commerce, Science, and Transportation Subcommittee on Aviation Security on April 6, 2000, the Associate Administrator of the FAA for Civil Aviation Security stated, "Moreover, members of foreign terrorist groups and representatives from state sponsors of terrorism are present in the United States. There is evidence that a few foreign terrorist groups have well-established capability and infrastructures here." (Dzakovic 2003) Additionally, many of the 9/11 hijackers were identified by the Computer Assisted Passenger Pre-Screening Systems (CAPPS). CAPPS is a system that automatically researches anyone that buys an airplane ticket and generates a risk score based on a variety of factors.

The following hijackers were flagged by CAPPS:

Hijacked Aircraft	Terrorists
American Airlines Flight 11 (Logan)	Wail al-Shehri, Satam al-Suqami, Waleed al-Shehri, Mohamed Atta
American Airlines Flight 77 (Dulles)	Hani Hanjour, Khalid al-Mihdhar, Majed Moged, Nawaf al-Hazmi, Salem al-Hazmi
United Airlines Flight 93 (Newark)	Ahmad al-Haznawi
United Airlines Flight 175 (Logan)	*None*

Table 6. 9/11 Terrorists Identified by CAPPS.
Table Source (NCTAUS 2004a)

Such a failure is not surprising when one learns that a FAA Security Special Agent wrote a letter to the Department of Transportation Inspect General in 1999 saying that "…Logan International Airport is in a critical state of non-compliance with Federal Aviation Security Regulations…" (NCTAUS 2004a)

Can a security model be developed that does not rely on the assumptions of quantitative risk assessment, considers issues at a level closer to system design and operation compared to game theory, and supports successful red teaming? According to (Haimes 2004):

> The authors of the chapter on complex and interdependent systems in a report by the National Research Council (2002) assert that "the basic tools of systems analysis and modeling are available today and are widely used in the military and industrial applications. But these tools have severe limitations when applied to interdependent complex systems, and research is required to extend them." The report identifies the following needed initiatives, which should not be the domain of single disciplinary perspectives:
>
> - System-of-systems perspectives for homeland security.
> - Agent-based and system dynamics modeling

A systems-theoretic approach that integrates system dynamics modeling is presented in the following chapter in an attempt to answer the question stated above.

CHAPTER 4: Systems Theory and Complexity

4.1 STAMP

Systems-Theoretic Accident Models and Process (STAMP) is an accident model based on systems and control theory created at MIT by Nancy Leveson. Although originally developed for system safety engineering, many of the theory's constructs are directly applicable to security. Zipkin has shown the applicability of the model to malicious software (Zipkin 2005) and Laracy to biodefense planning (Laracy 2006). The model with security extensions that is defined in this thesis is referred to as STAMP-Sec.

4.2 Systems Theory

Before explaining STAMP-Sec, it is important to understand its theoretical underpinning. In contrast to the traditional scientific method that relies on analytic reduction, systems theory states that complex systems must be considered holistically. The theory was well developed by Bertalanffy, Ashby, and Wiener in the 1940s and 50s in response to challenges encountered in biology, communication, and control. During this time, scientists and engineers began to recognize a new type of complexity.

Organized simplicity is exhibited in traditional, deterministic systems that easily can be decomposed into subsystems and components such as in structural mechanics. The re-synthesis of the subsystems does not yield any unexpected properties because the component interactions are well defined and often linear. Conversely, it is not straightforward or useful to decompose systems that exhibit *unorganized complexity*. However, statistical techniques are applicable because of the regularity and randomness that characterize the network structure. The Law of Large Numbers becomes applicable and average values can be computed such as in statistical mechanics (e.g. ideal gases in chemistry). The "new" complexity theory, *organized complexity*, describes systems with a sufficiently complex structure to make it impractical or impossible for them to be modeled with analytic reduction, and not random enough to be modeled using statistics (Leveson 2002).

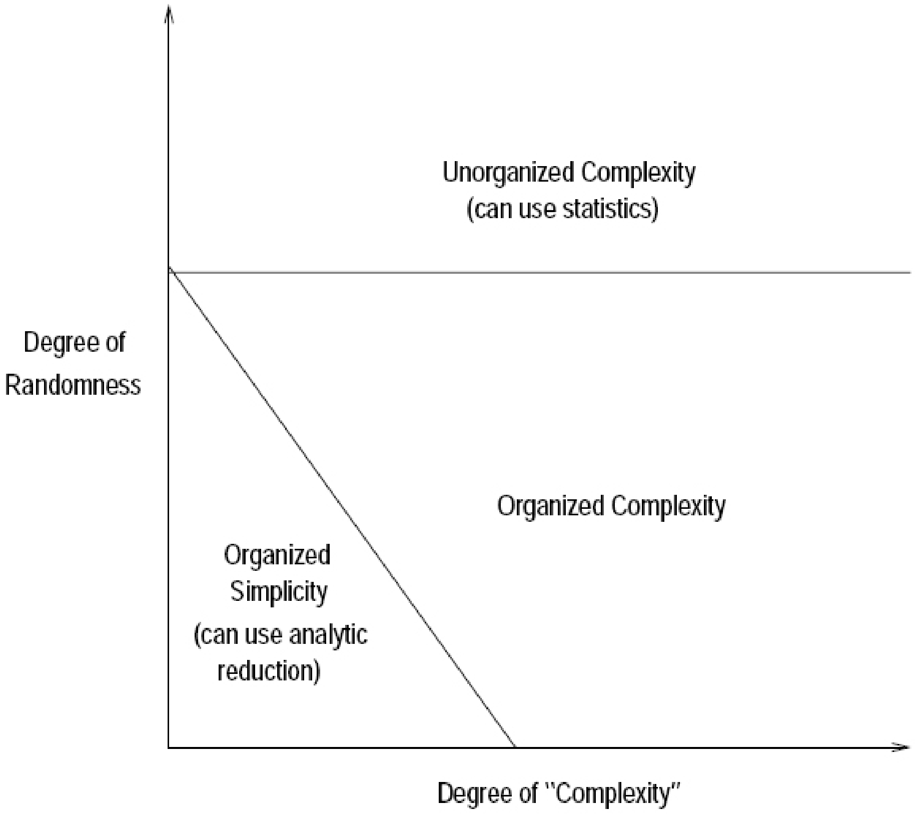

Figure 8. System Organization and Complexity.
Image Source (Weinberg 1975)

Systems characterized by organized complexity exhibit strong, non-linear interactions and coupling between subsystems and components. Therefore, a top-down approach needs to be applied to such systems. Two underlying concepts provide insight into these complex systems: emergence/hierarchy and communication/control.

Abstractions for complex systems often involve layers. In the case where the abstraction is hierarchical, the level of organization increases as one moves toward higher layers. Additionally, the step from level *n* to *n + 1* yields new properties that are not discernable at level *n*. This phenomenon is referred to as emergence, or emergent properties. Leveson provides a good example of this behavior using an apple's shape: "The shape of an apple, although eventually explainable in terms of the cells of the apple, has no meaning at that lower level of description."(Leveson 2002) Security is an emergent system property. For example, it is not possible to completely evaluate the security of an individual personal computer in isolation. The security of a PC can only be determined by its relationship within a broader context, i.e. a socio-technical system. A PC might be considered "secure" when it is sitting isolated at home. However, once that computer is brought to work, connected to the LAN, and therefore the Internet, a whole new class of vulnerabilities emerges. An individual computer may be bolted to a desk, require a boot-up password, and have an encrypted file system. However, a security expert would never classify such as system as "totally secure." This is because security is a *system* property. A computer network is more than the sum of individual PCs, the behavior of the PCs in isolation does not tell us all the possible behaviors it may exercise in connection with other computers, and the performance of a network cannot be characterized by a simple additive composition of PCs.

As Graham, Baliga, and Kumar point out, over the last 50 years, the fields of communications, control, and computation have converged (Graham 2004). The resulting theoretical foundations are contained in systems theory and directly relevant to the goals of system safety and security. One especially sees the need for communications to coordinate required control in open systems (Leveson 2002). Control is exercised in complex systems by imposing constraints on lower levels in the hierarchy. According to Peter Checkland:

> Control is always associated with the imposition of constraints, and an account of a control process necessarily requires our taking into account at least two hierarchical levels. At a given level, it is often possible to describe the level by writing dynamical equations, on the assumption that one particle is representative of the collection and that the forces at other levels do not interfere. But any description of a control process entails an upper layer imposing constraints upon the lower. The upper level is a source of an alternative description of the lower level in terms of specific function that are emergent as a result of the imposition of constraints (Checkland 1981).

Ashby provides four conditions that are required to exercise control over a system:

- *Goal condition* – The controller must have a goal or goals.
- *Action condition* – The controller must be able to affect the state of the system.
- *Model condition* – The controller must be (or contain) a model of the system.
- *Observability condition* – The controller must be able to ascertain the state of the system. (Ashby 1956)

The controller in Leveson's generic control loop must be able to observe the controlled process through the sensors, relate the observation to its model, and actuate the process if the system has deviated from the goal condition.

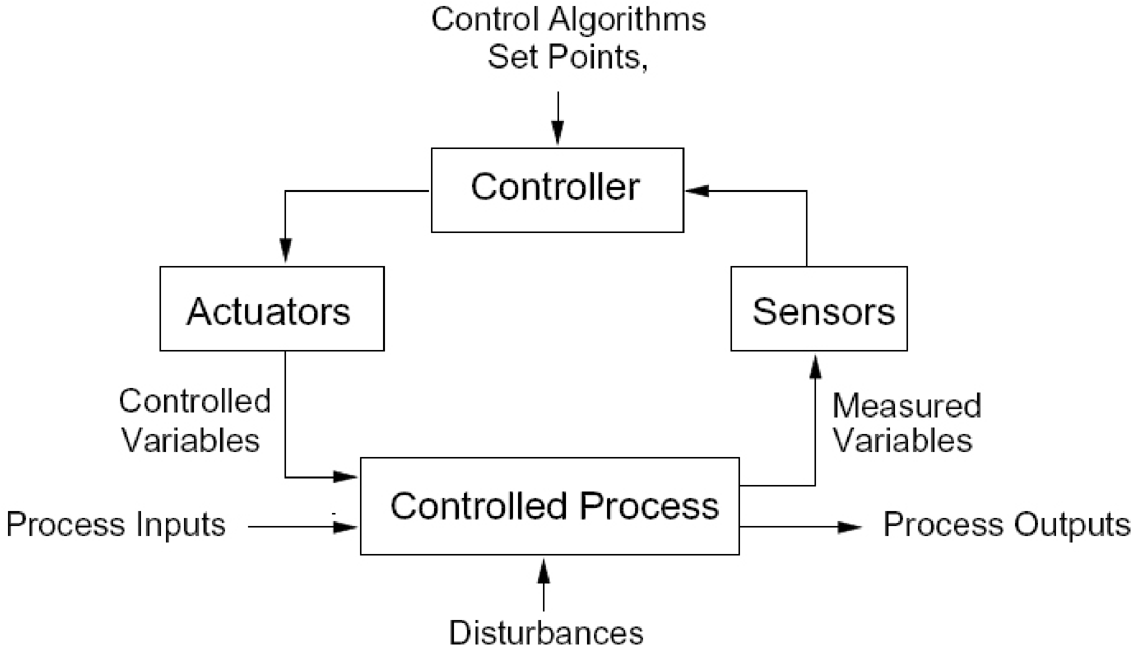

Figure 9. Generic Control Loop.
Image Source (Leveson 2002)

4.3 Systems Thinking

Systems thinking is the application of systems theory to mental models and thought. It acknowledges that learning is a feedback process and views problems through the lens of interconnected networks governed by systems of non-linear relationships. System thinkers advocate holism over the traditional reductionism found in modern science. Operations Researcher, Russell Ackoff, and Computer Engineer, Jay Forrester, developed the approach in the late 1950s in response to challenges encountered in studying complex, socio-technical systems. Forrester created the System Dynamics modeling technique, which is based on the theory of non-linear dynamics. His successors include Peter Senge, who applies systems thinking to organizational learning (Senge 2006), and John Sterman, the leader of the system dynamics community who uses it to improve managerial decision-making in complex systems (Sterman 2000).

Ackoff's system thinking is best understood as carrying on the spirit of Operations Research as it was practiced in the 1950s and 60s before mathematical methods overtook problem framing and formulation as the forte of OR specialists (Kirby 2003). Ackoff's successor is Jamshid Gharajedaghi, the leader of the Interactive Design (ID) movement. ID focuses on human choice in socio-technical systems and incorporates iterative inquiry and operational thinking. Iterative inquiry theory suggests that to gain understanding in complex systems, a successive technique of investigating function, structure, process, and context can lead to greater understanding.

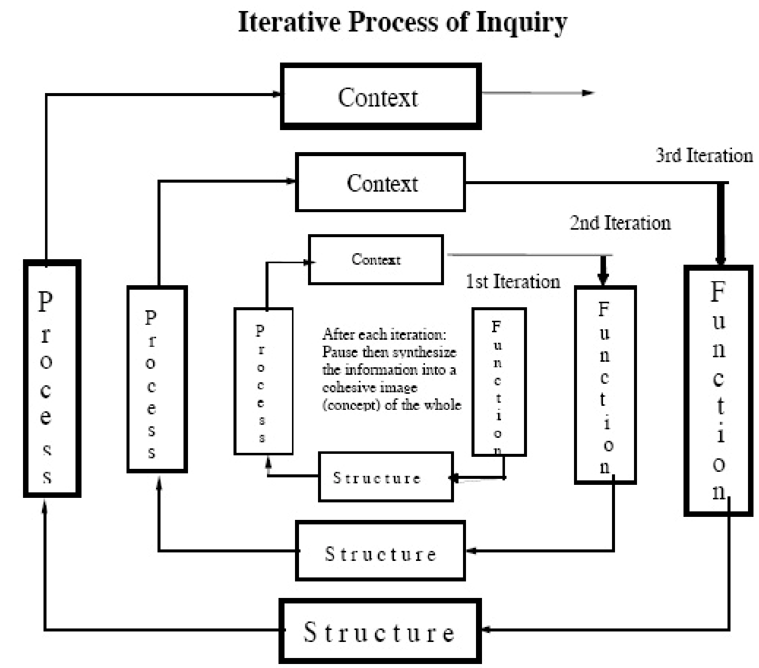
Iterative Process of Inquiry
Context
Context
Context
3rd Iteration
2nd Iteration
1st Iteration
Process
Process
Process
After each iteration: Pause then synthesize the information into a cohesive image (concept) of the whole
Function
Function
Function
Structure
Structure
Structure

Figure 10. Iterative Inquiry.
Image Source (Gharajedaghi 2004)

Operational thinking requires a systems scientist to think about how systems actually work as opposed to how they could theoretically work. Non-operational thinking is best captured in econometric models that seek to predict milk consumption but do not factor in cows (Richmond 1993). Overall, ID advocates participatory design and offers an approach both for formulating problems and developing solutions in teams (Gharajedaghi 1999).

In Britain, Peter Checkland developed another systems thinking approach for modeling organizational processes and managing change in complex social systems called the Soft Systems Methodology (SSM) (Checkland 1981). SSM is a qualitative technique that seeks to impose systems thinking in non-systemic situations where human social activity is more important that other factors such as technology. Conceptual models and graphics are developed to promote deeper understanding of the complex social system.

Systems thinking has yielded significant results in the Engineering Systems Division at MIT. In particular, it has proven to be very useful for the investigation of cultural and organizational factors that jeopardize the safety of complex engineering systems (Dulac 2007c). This thesis research will show that system thinking insights are equally as applicable to security problems.

CHAPTER 5: System Theoretic Accident Models and Processes for Security (STAMP-Sec)

5.1 STAMP-Sec

STAMP-Sec views security incidents as the result of inadequate control, rather than strictly a failure, such as a cryptographic device breaking (Rae 2006) or a code cracked. Security is an emergent property that is achieved through the enforcement of *constraints*. This perspective allows security problems to be transformed into control problems for which powerful tools can be employed. *Control structures* are defined to capture the communication and control in the system and illustrate the presence and absence of feedback. They are hierarchal in nature and need to be constructed both for system development and system operation.

Security must be designed into a system as well as be part of how it is operated. Historical examples of large systems where security was added in "after the fact" have been plagued by systemic security risks. For example, current approaches to information security suffers from serious deficiencies as evidenced by the influence of SPAM, Internet worms, viruses, phishing, and other attacks that plague the common Internet user. This is largely a result of the fact that network research in the 1960s through the 1980s focused on achieving performance (e.g. throughput and robustness) objectives with little emphasis on security. As a result, when threats began to emerge in the 1990s, Internet security was approached from an ad-hoc perspective – applying patches to vulnerabilities already identified by attackers. The problem remains that the underlying architecture was not designed to support strong security.

A STAMP control structure informs design by defining the necessary communication and control between subsystems and components to enforce security constraints. Effective communication between levels of the hierarchy is essential to successful system security. Layer *n + 1* must be able to assert goals, policies, and constraints through a *reference channel* and layer *n* must be able to communicate operational experience through a *measuring channel*.

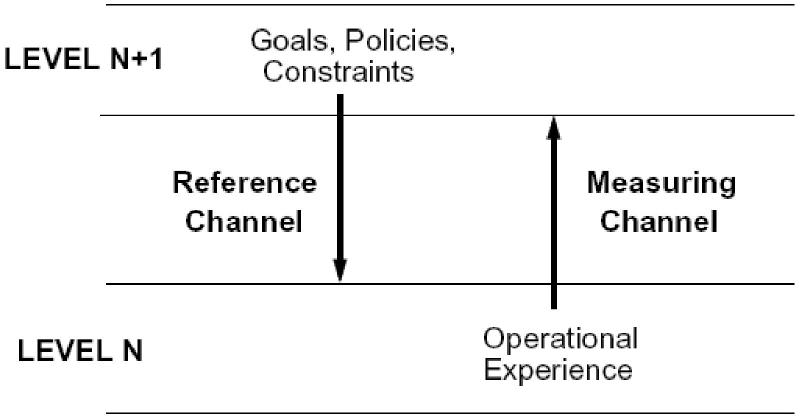

Figure 11. Communication and Control in Layered Systems.
Image Source (Leveson 2002)

In a top-down security engineering activity, threat analyses may be conducted using a variant of STPA, (STAMP-based Analysis). Threats that the system must guard against are identified and constraints are defined that prevent their instantiation as a result of design or operational decisions. The complete list of constraints should be part of a system's requirements document. After that, the static control structure is modeled. Components in the control structure are assigned responsibility to maintain the constraints. Finally, possible control actions for the components are defined (Leveson 2003). System Dynamics is used to understand how the control structure and the malicious actor could evolve.

The five steps of STAMP-Sec are provided below.

STAMP-Sec

1. Identify the system level threats.
2. Write security constraints for the threats.
3. Define the static control structure to prevent or mitigate the threats.
    a. Assign constraints to the system components responsible for implementing them.
    b. Define the control actions for the components that prevent or mitigate the threats.
4. Identify inadequate control actions that could lead to an insecure state.
5. Determine ways that constraints could be violated and attempt to eliminate them. In particular, use System Dynamics to consider how and why the security control structure might change over time, potentially leading to ineffective controls.

Figure 12. STAMP-Sec Methodology.

5.2 STAMP-Sec for an Air Transportation System

In "The Law of Loopholes in Action," David Gelernter argues that "every loophole will eventually be exploited; every loophole will eventually be closed." (Gelernter 2005) According to (Fricker 2005):

> The effect of the Law of Loopholes, as anyone that flies regularly today knows, is an ever-expanding set of security measures and requirements put in place, generally in response to *past* security breaches. Such rules and requirements are useful for helping prevent a reoccurrence of a particular incident. But, to the extent a determined adversary's focus is on causing destruction and mayhem, these types of rules and requirements simply mean that as one loophole is plugged the adversary shifts its attention and energies to looking for and then trying to exploit a different loophole."

Instead of participating in the Law of Loopholes game, a STAMP-based analysis takes a top-down approach to proactively design and operate systems to meet security requirements and prevent the instantiation of system-level threats. Air transportation systems must control against the following threats:

1. A terrorist takes control of or disrupts an aircraft or persons onboard.
2. A terrorist takes control of or impersonates air traffic control.
3. A terrorist sabotages an aircraft.
4. A terrorist shoots an aircraft down.
5. A terrorist disrupts the critical infrastructure of the air transportation system (e.g. destroy a runway or radar).
6. A terrorist interferes with the aircraft communication, navigation, or surveillance systems.

However, before a threat assessment of the Next Generation Air Transportation System is conducted, the existing socio-technical control structure must be analyzed. It is useful to understand the lessons of 9/11 and keep them in mind in the evolution toward NGATS. For a timeline of background and proximal events leading to the attack in 2001, see **Appendix I**.

The reconstruction of a security incident begins with identifying the threat carried out by the attacker as well as the constraints that were violated. After that, the taxonomy of inadequate controls is used to identify the dysfunctional interactions that enabled the violation of security constraints. In general, for each component in the control structure, the following items are provided (Leveson 2002):

1. Constraints
2. Controls
3. Context
    a. Roles and Responsibilities
    b. Environmental and Behavior Shaping Factors
4. Flaws in the Controlled Process
5. Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions
6. Reasons for Flawed Control Actions and Dysfunctional Interactions
    a. Control Algorithm Flaws
    b. Incorrect Process, Interface, or Mental Models
    c. Inadequate Coordination among Multiple Controllers
    d. Reference Channel Flaws
    e. Feedback Flaws

This model is a useful tool to understand how and why the security constraints were violated.

5.2.1 Security on 9/11/2001

The security control structure for air transportation in the US in 2001 is shown below. The red, dotted lines indicate instances of inadequate communication and control.

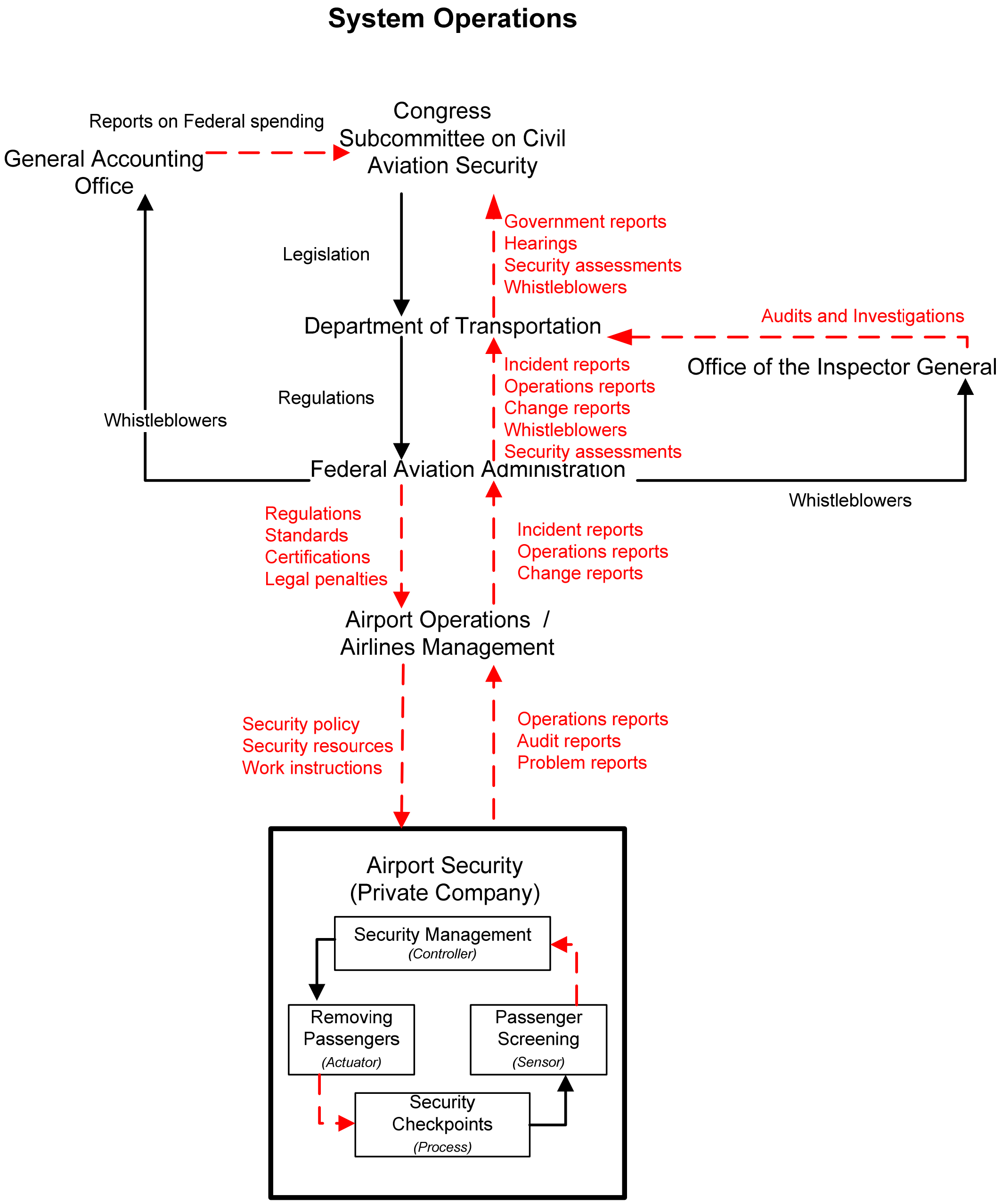
System Operations
Reports on Federal spending
General Accounting Office
Congress Subcommittee on Civil Aviation Security
Legislation
Government reports
Hearings
Security assessments
Whistleblowers
Department of Transportation
Audits and Investigations
Office of the Inspector General
Regulations
Incident reports
Operations reports
Change reports
Whistleblowers
Security assessments
Whistleblowers
Federal Aviation Administration
Whistleblowers
Regulations
Standards
Certifications
Legal penalties
Incident reports
Operations reports
Change reports
Airport Operations / Airlines Management
Security policy
Security resources
Work instructions
Operations reports
Audit reports
Problem reports
Airport Security (Private Company)
Security Management (Controller)
Removing Passengers (Actuator)
Passenger Screening (Sensor)
Security Checkpoints (Process)

Figure 13. Security Control Structure on 9/11/2001.

Airport Security

In 2001, private companies were contracted to perform the passenger and baggage screening function at US Airports. Airports and carriers provided policies, resources, and instructions, but a clear line of accountability was not present to ensure that these directives were successfully executed.

Security Constraint Violated: Security personnel must remove passengers that are judged to be a risk to the air transportation system and contact law enforcement officials.

Controls: Computer Assisted Passenger Pre-Screening Systems (CAPPS), verification of ID, metal detectors, and X-Ray bag screening were the primary controls in place to enforce the constraint.

Context: The FBI and FAA were responsible for administering CAPPS. Those tagged by the system would then be subject to more rigorous baggage screening for explosives. CAPPS did not specify special screening of the passengers themselves.

Flaws in the Controlled Process: CAPPS, and the passenger screening system in general, did not have a specified mechanism to prevent high risk passengers from boarding an aircraft.

Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions: At Logan International Airport, Wail al-Shehri and Satam al-Suqami were chosen for special screening of their checked bags, before they boarded American Airlines Flight 11. CAPPS identified Waleed al-Shehri but he did not check any luggage. Portland Airport identified Mohamed Atta. The hijackers of AA Flight 77, Hani Hanjour, Khalid al-Mihdhar, and Majed Moqed were also identified by CAPPS. Nawaf al-Hazmi and Salem al-Hazmi were chosen because of insufficient identification. United Airlines Flight 93's hijacker, Ahmad al-Haznawi, was flagged but none of the hijackers of United Airlines Flight 175 were identified by CAPPS (NCTAUS 2004b).

Reasons for Flawed Control Actions and Dysfunctional Interactions: US airliners had not been hijacked in over a decade and a false sense of security was present. In the late 1990s, a Fox News/Opinion Dynamics poll indicated that 78% of Americans surveyed thought poor maintenance was "a greater threat to airlines safety" than terrorism. Also, increasing demand for flights led airliners to focus on changes to the system that improved throughput. The "Passenger Bill of Rights" emphasized providing a convenient and efficient passenger experience. According to statements from the 9/11 Commission, “Domestic hijacking in particular seemed like a thing of the past.” (NCTAUS 2004b) Finally, screeners have a very monotonous job and are paid a low wage. These environmental conditions do not enable motivated, diligent execution of duties.

Airport Operations / Airlines Management

In 2001, US airports did not have any operational authority over checkpoint screening activities. With the airports lacking the jurisdiction to enforce FAA regulations, only the airlines were empowered to manage the passenger screening process.

Security Constraint Violated: Airlines shall ensure that passenger screening companies comply with all FAA regulations and take additional measures to prevent passengers that pose a risk to the Air Transportation System from boarding an aircraft.

Controls: The airlines two principal control actions were sharing threat information with screeners and enforcing regulations.

Context: Airports and airlines knew that passenger screening was not effective from red teaming exercises and other assessments.

Flaws in the Controlled Process: The regulations that the airlines enforced were incapable of implementing the security constraint. Federal regulations stated that airlines were required to “conduct screening…to prevent or deter the carriage aboard airplanes of any explosive, incendiary, or a deadly or dangerous weapon on or about each individual’s person or accessible property, and the carriage of any explosive or incendiary in checked baggage.” (NCTAUS 2004b) Inherently dangerous persons nor box cutters are mentioned here.

Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions: With the exception of guns, large knives, and bombs, the FAA simply told airliners to “use common sense” in establishing screening regulations. The airlines responded to this suggestion by working together to create the “Checkpoint Operations Guide,” which was later approved by the FAA. Box cutters were listed as restricted items and not permitted to be brought in the cabin. Obviously, the carriers did not enforce the Checkpoint Operations Guide.

Reasons for Flawed Control Actions and Dysfunctional Interactions: Utility knives with blades less than four inches were permitted in the cabin. The Checkpoint Operations Guide did not provide information about the difference between a pocket knife and a box cutter. A culture of "passing the buck" between the FAA and the airlines created an ambiguous guide that was then not taken seriously by airport screeners.

Federal Aviation Administration

The FAA was the principle regulatory agency of the Air Transportation System in 2001. It possessed the statutory authority to issue and enforce aircraft and airport security rules and procedures.

Security Constraint Violated: The FAA shall issue directives to airlines, airports, and security screening companies that prevent the hijacking of an aircraft.

Controls: The FAA security system imposed control through a seven layered defense:

1. Intelligence
2. Passenger Screening
3. Airport Access Control
4. Passenger Checkpoint Screening
5. Passenger Checked Baggage Screening
6. Cargo Screening
7. On-board Security

As with any layered defense, a hierarchy is present starting with Level 1. The goal of this system was to use intelligence to remove threats from the system before they arrived at an airport. In the event that the first six layers were breached, on-board security, i.e. air marshals, was the last line of defense.

Context: The FAA leadership focused on air transportation economics, customer service, and safety issues. Security was not a large concern. The civil aviation system was at the equivalent of a Threat Level Yellow. This intermediate threat level was to be invoked when "Information indicates that a terrorist group or other hostile entity with a known capability of attacking civil aviation is likely to carry out attacks against US targets; or civil disturbances with a direct impact on civil aviation have begun or are imminent." (NCTAUS 2004b)

Flaws in the Controlled Process: Two principle flaws were present. First, the FAA did not have the 9/11 hijackers in their database of high risk passengers on the no-fly list. In fact, only twelve terrorists were in the database. The State Department's TIPOFF database contained 61,000 terrorists include two 9/11 hijackers. Second, the FAA did not certify screening companies in accordance with the requirements set forth in the FAA Aviation Reauthorization Act of 1996 and the 1997 Gore Commission.

Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions: FAA security analysts did not recognize an increased threat to domestic air transportation due to dysfunctional interactions with intelligence agencies. "Civil aviation security officials testified that the FAA felt blind when it came to assessing the domestic threat because of lack of intelligence on what was going on in the American homeland as opposed to overseas." (NCTAUS 2004b) The FBI, CIA, and State Department intelligence shared with the FAA focused on threats in the Middle East despite the fact that these agencies had data on domestic risks (e.g. Phoenix memo). Erroneous controls were also exercised. Instead of implementing anti-hijacking procedures in response to the heightened threat level in the spring and summer of 2001, the FAA only issued "general warnings to the industry to be more vigilant and cautious." (NCTAUS 2004b) Additionally, many flawed decisions resulted from dysfunctional interactions between the FAA and the airlines in the development of the "common sense" screening guidelines.

Reasons for Flawed Control Actions and Dysfunctional Interactions: Inadequate coordination among stakeholders is a major reason for the dysfunctional interactions in the FAA. FAA intelligence officers were granted liaison status with the FBI, CIA, and State Department intelligence divisions concerned with aviation security. However, the FAA did not obtain key information from these organizations. Additionally, a feedback flaw was present because liaisons were not assigned to the National Security Agency (NSA) and the Defense Intelligence Agency (DIA). More generally, a feedback flaw was present because operational experience and threat assessments were not used to develop proactive policies. Rather, the features of the civil aviation security system were the result of responding to specific historical incidents.

Department of Transportation

The Department of Transportation (DoT) is a cabinet level executive department concerned with all areas of transportation. In addition to the FAA, it administers the Federal Highway Administration, Federal Railroad Administration, Maritime

Administration, St. Lawrence Seaway, and other transportation related agencies in the government. According to the Office of the Inspector General (OIG) mission statement, "The Office of Inspector General works within the Department of Transportation to promote effectiveness and head off, or stops, waste, fraud and abuse in departmental programs. We do this through audits and investigations. OIG also consults with the Congress about programs in progress and proposed new laws and regulations." Unfortunately, it is now apparent that neither the DoT nor the OIG was diligently performing its duties with regard to aviation security in 2001.

Security Constraint Violated: The DoT shall execute federal laws pertaining to transportation security and empower constituent agencies to enact regulations to achieve security goals.

Controls: The DoT exercised two primary control actions for transportation security. First, it was responsible for providing the necessary resources, directives, and leadership to the FAA. Second, it was responsible for suggesting legislative action if necessary changes to the security of the ATS required Congressional approval.

Context: The vulnerabilities in the ATS were well documented in unclassified reports from the DoT Inspector General and the General Accounting Office. Additionally, the results were published by the media.

Flaws in the Controlled Process: In its administration of the FAA, and its interactions with the Congress, the leadership of the DoT did not emphasize the well documented weaknesses of the ATS.

Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions: Incident and change reports, security assessments, and whistle blowers were unable to successfully communicate concerns to DoT leadership. The OIG did not provide the necessary oversight that its mission requires. According to Red Team leader and whistleblower Bogdan Dzakovic, "I went to the Department of Transportation's OIG. This too proved to be a wasted effort. A senior official in the Inspector Generals Office actually explained to us that because of the political situation between the FAA and the IG's office, the IG couldn't take any action against the FAA." (Dzakovic 2003)

Reasons for Flawed Control Actions and Dysfunctional Interactions: Efficiency and economy were priorities at the DoT. The leadership's mental models with regard to security were satisfied with the illusion of security.

Congress

Congress passed the FAA Reauthorization Act of 1996. The law states that "…the Administrator [of the FAA] shall conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of such systems…" Unfortunately, as described above, the red teaming process was rendered impotent and additional legislative action was not taken to strengthen the security of the ATS.

Security Constraint Violated: Congress shall pass laws to strength the security of the Air Transportation System. The GAO shall investigate the execution of these laws and report its findings to the Congress.

Controls: Congress exercises control by soliciting government reports and conducting hearing and finally passing legislation based on these inputs.

Context: Although whistleblowers were not given adequate access to the Legislative branch, Congress was not ignorant of the terrorist threat to the ATS. In testimony to the US Senate Committee on Commerce, Science, and Transportation Subcommittee on Aviation Security on April 6, 2000, the Associate Administrator of the FAA for Civil Aviation Security stated, "Moreover, members of foreign terrorist groups and representatives from state sponsors of terrorism are present in the Unite States. There is evidence that a few foreign terrorist groups have well-established capability and infrastructures here." (Dzakovic 2003)

Flaws in the Controlled Process: The Congress did not hold the DoT or the FAA accountable for not complying with their statutory obligations. Blatant violation of federal law such as the fact that the FAA was not certifying passenger screening companies, as well as obstructing red teams, were permitted.

Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions: Dysfunctional interactions between the Congress and its investigate arm, the GAO, enabled the DoT to continue to persist in a state of noncompliance to federal statutes. The GAO had the necessary data to make a strong case for Congressional intervention, but failed to do so. “The GAO people we spoke to were extremely concerned about our revelations, but explained they have no authority to actually do anything.” (Dzakovic 2003)

Reasons for Flawed Control Actions and Dysfunctional Interactions:
Reference channel as well as feedback flaws contributed to the dysfunctional interaction. The flaws were both FAA noncompliance and the inability for whistleblowers to establish a line of communication to an empowered individual in the Congress.

5.2.2 Summary of Inadequate Controls in the ATS

There are many ways inadequate control can lead to a security system being compromised. STAMP provides a useful categorization scheme that captures most safety control flaws. Broadly, they fall into one of three categories: Inadequate enforcement of constraints, inadequate execution of control actions, or inappropriate or missing feedback (Leveson 2004). The introduction of a malicious agent does not violate the assumption of the taxonomy originally developed for safety. In a safety scenario, poor engineering or management may offer inadequate enforcement of constraints, execution of control actions, or feedback such that a hazard that is “exploited” inadvertently in system operations. In a security scenario, poor engineering or management may offer inadequate enforcement of constraints, execution of control actions, or feedback such that a vulnerability is created that may be intentionally exploited in system operation. Whether one is concerned with safety or security, the problem is inadequate control. STAMP-Sec extends the safety list to capture security issues:

1. Inadequate Enforcement of Constraints (Control Actions)
    - 1.1. Unidentified threats
    - 1.2. Inappropriate, ineffective, or missing control actions for identified threats
        - 1.2.1. Design of control process does not enforce constraints
            - 1.2.1.1. Flaws in creation process
            - 1.2.1.2. Process changes without appropriate change in control (asynchronous evolution)
            - 1.2.1.3. Incorrect modification or adaptation
        - 1.2.2. Process models inconsistent, incomplete, or incorrect
            - 1.2.2.1. Flaws in creation process
            - 1.2.2.2. Flaws in updating process (asynchronous evolution)
            - 1.2.2.3. Time lags and measurement inaccuracies not accounted for
        - 1.2.3. Inadequate coordination among controllers and decision makers (boundary and overlap areas)
2. Inadequate Execution of Control Action
    - 2.1. Communication flaw
    - 2.2. Inadequate actuator operation
    - 2.3. Time lag
3. Inadequate or missing feedback
    - 3.1. Not provided in system/organizational design
    - 3.2. Communication flaw
    - 3.3. Time lag
    - 3.4. Inadequate detection mechanisms

The reader should take note that many of these inadequacies are not associated with simply an event-based risk. Rather, *flaws in communication and control* as well as *time lags* and *flaws in the design process* contribute to threats.

5.2.3 Security After 9/11/2001

Now that the STAMP framework has been used to understand the attack of 9/11/2001, one can begin to study the Air Transportation System of 2007. Improvements have certainly been made over the last six years. The creation of the Terrorism Threat Integration Center, a more vigilant civil defense program, an improved port and commercial shipping inspection program, hardened cockpits, and other changes have changed the security landscape. As a result, over 100 attacks have been thwarted since

9/11 (NCTAUS 2004a). This is due to improvements in the security of the ATS as well as increased "human vigilance, unprecedented law enforcement, security, and intelligence cooperation, and the worldwide hunt for Al Qaeda, denying the group time, space, and resources to plan and mount spectacular attacks." (RMS 2003)

However, this is certainly not the time for complacency to set in. According to the State Department, Al Qaeada (Sunni Islamists), Hizballah (Shia Islamists), Al Gama'a Al-Isalamiyya (Egyptian Islamists), Kahane Chai (Israeli extremists), Mujahdein e-Khalq (Marxist-Islamists) are believed to be operating in the US. Fortunately, many of the major flaws in the control processes and the dysfunctional interactions identified above have been corrected. The current operations control structure for the US is shown below.

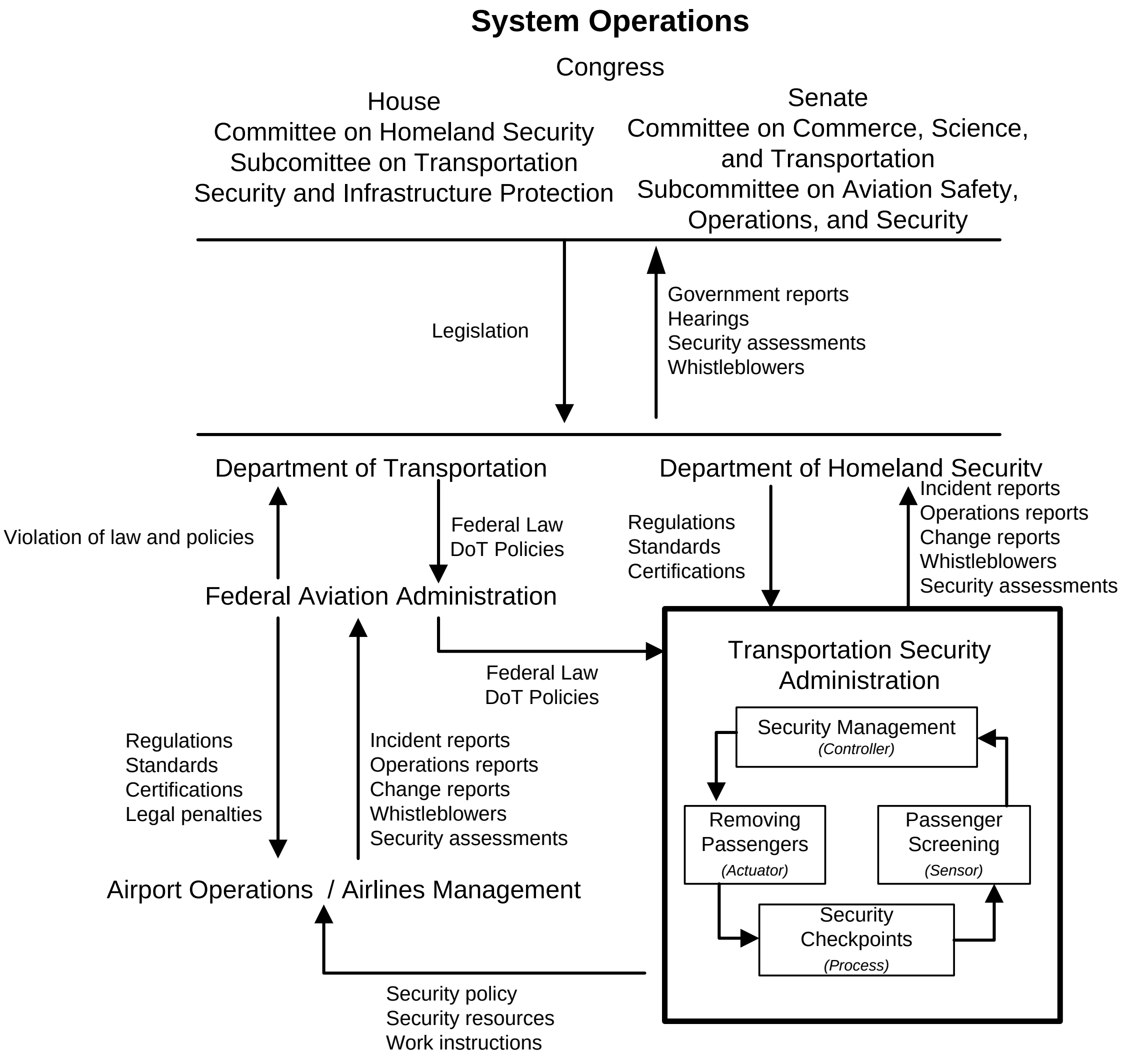

Figure 14. Post 9/11 Security Control Structure.

Congress

The House Committee on Homeland Security; Subcommittee on Transportation Security and Infrastructure Protection, and the Senate Committee on Commerce, Science, and Transportation; Subcommittee on Aviation Safety, Operations, and Security have oversight over US non-military air transportation. In the post 9/11 political climate, the Congress is very receptive and willing to hear the testimony of whistleblowers and critique security assessments and government reports with professionals on their own staffs. Additionally, concerns from the GAO on the topic of aviation security would receive much greater priority than in the pre 9/11 environment that Bogdan Dzakovic encountered.

Department of Transportation

The DoT has been stripped of its lead role in transportation security. While it still administers the FAA, DoT no longer controls passenger and cargo screening. As a result, the DoT's priorities of passenger/cargo throughput and transportation economics no longer *directly* affect ATS security. It is not known whether the political situation between the DoT OIG that prevented disciplinary actions from being taken against the FAA has improved.

Department of Homeland Security and the TSA

The Department of Homeland Security (DHS) was established on November 25 by the Homeland Security Act of 2002. This decision introduced organizational complexity to the ATS because two executive departments share control of the ATS. The Transportation Security Administration (TSA) was created to replace the private companies that airlines contracted to perform passenger and baggage screening. As a part of DHS, the Administrator of the TSA is an Assistant Secretary of Homeland Security. With a cabinet level department focused on security, there is greater likelihood that poor red team results and whistleblowers will not be ignored. Additionally, the TSA imposes security policies, shares security resources, and informs work instructions for the airports and airlines. While the transformation of passenger screening from a private entity to the government does not necessarily improve security, it is preferable to have the screening organization reporting to the DHS rather than the airlines. DHS can impose the necessary control on TSA without being concerned about airline profitability.

Federal Aviation Administration

The FAA ensures that Federal Law and DoT policies are enforced in the air transportation system. The FAA also enforces regulations and standards on the airlines and airports and has the power to impose sanctions and raise issues to the DoT. The control flaws resulting from dysfunctional interactions between the FAA intelligence organization and other Federal intelligence agencies is no longer an area of major concern. Responsibility for terrorist intelligence is now located within the Department of Homeland Security and TSA. As part of this effort, the CAPPS program has been expanded and strengthened to identify terrorists and *prevent* them from boarding aircraft. It is expected that the new program, Secure Flight, will be deployed in 2010 (EPIC 2006). All in all, the restructuring of the security control structure for air transportation appears to have addressed many of the proximate causes of the attack on September 11, 2001 having to do with inadequate control in the socio-technical system.

5.2.4 Evolution to the Next Generation Air Transportation Systems

The pressing question that arises in the context of developing NGATS is:

> *How can the JPDO evolve the current systems such that security does not degrade and perhaps even improves?*

(Dulac 2007a) has shown that the transition of a complex system from an operations environment to one that includes development introduces significant risks. Therefore, it is important that as the US transitions to the NGATS, the required communication and control from the earlier system is maintained and additional constraints are imposed to satisfy new security requirements. In order to achieve this objective, a high level model of socio-technical control is provided below.

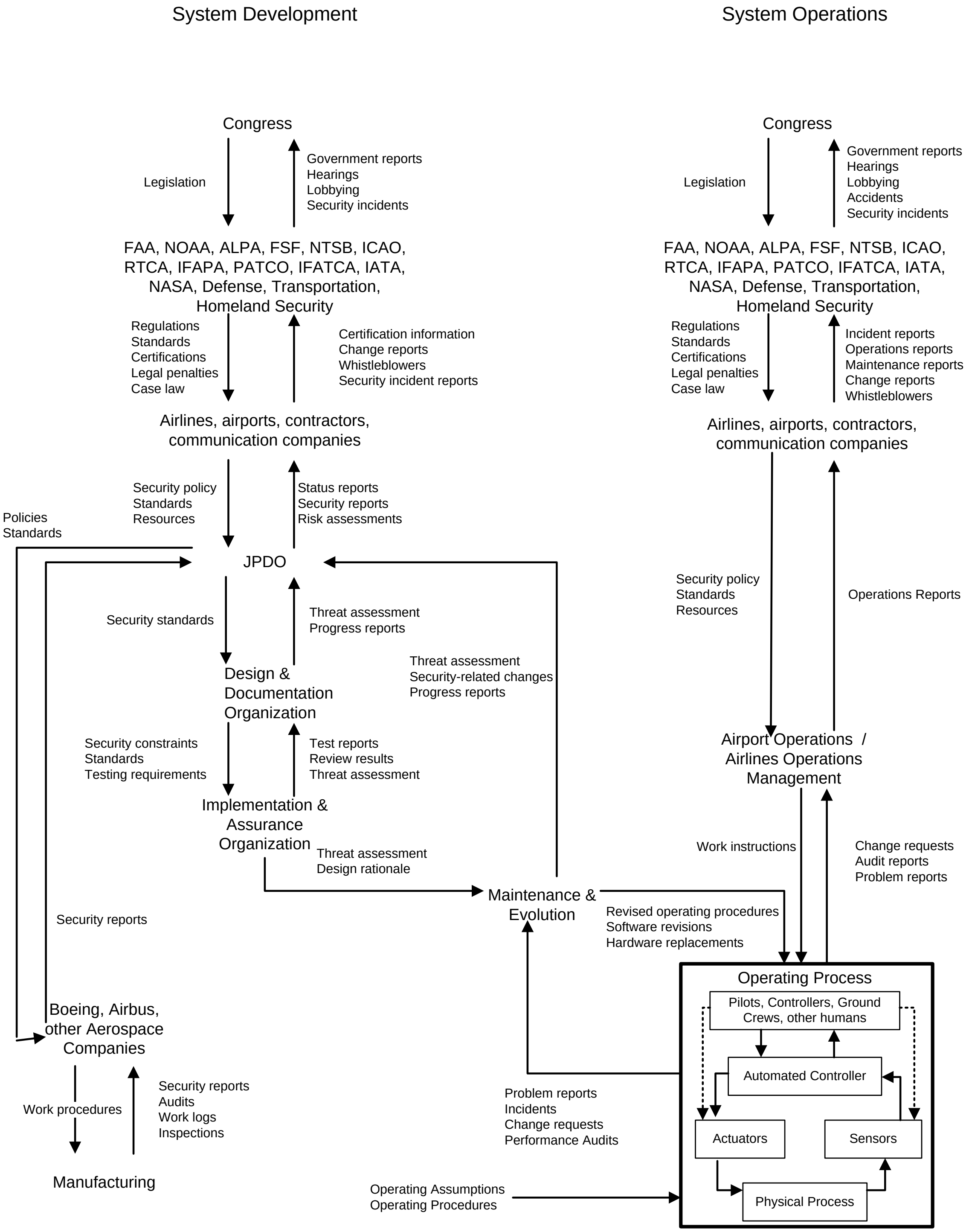

Figure 15. NGATS Socio-Technical Control Structure.

Risks emerge in a system when “basic inadequacies in the way individual components in the control structure fulfill their responsibilities” or when the “coordination of activities and decision-making can lead to unintended interactions and consequences.” (Leveson 2005) Therefore, the components in the control structure above will be analyzed to identify these risks. In general, a controller can provide four types of inadequate control (Leveson 2002):

1. A required control action is not provided.
2. An incorrect control action is provided.
3. A potentially correct or adequate control action is provided too late (at the wrong time).
4. A correct control action is stopped too soon.

The four inadequate controls are applied to the component responsibilities below to prevent poor engineering and management decision-making from enabling an attack.

Congress

In order for legislation to be maximally effective in the area of security, legislators must be well informed of policy level security issues in the form of hearings, executive department reports, and security incident reports. The fundamental role of the Congress in air transportation operations does not change appreciably with the transition to NGATS. However, some additional roles are added for the *development* portion of NGATS.

Item	Responsibility	Inadequate Control
Congress		
1	Pass legislation affecting NGATS	Congress does not pass adequate legislation to effectively address security issues.
		Congress passes legislation that is detrimental to security issues.
		Congress passes legislation only after an attack has occurred.
		Congress succumbs to pressure and amends or removes laws necessary to address security issues.
2	Approve NGATS budget	Congress' budget inadequately funds the system so control actions are inappropriate, ineffective, or missing.
		Congress' budget funds aspects of the system that do not improve security or are detrimental to it.
		Congress' budget is not passed on time or does not provide forward-thinking plans.
		Congress' budget withdraws funding for security engineering during the development of the system.
3	Approve senior leadership appointments	Congress approves executive leadership that is incompetent or does not consider security a high priority.
		Congress approves executive leadership that opposes strong security.
		Congress approves executive leadership only after an attack has occurred.
		Congress interferes with the operation of the executive branch and disrupts security decision-making.

Table 7. Inadequate Controls for Congress.

Executive and Regulatory Agencies, Industry Associations, and Unions

The next level in the control structure includes government regulatory agencies, industry associations, unions, courts, and other stakeholders which exert control over airports and airlines. They receive information from certification reports, incident reports, and whistleblowers. The Federal Aviation Administration (FAA), NOAA's Aviation Weather Service, Air Line Pilots' Association (ALPA), Flight Safety Foundation (FSF), National Transportation Safety Board (NTSB), International Civil Aviation Organization (ICAO), Radio Technical Commission for Aeronautics (RTCA), International Federation of Air Line Pilots Association (IFAPA), Professional Air Traffic Controller Organization (PATCO), International Federation of Air Traffic Controllers' Association (IFATCA), and International Air Transport Association (IATA) all influence the creation of standards, regulations, and certifications.

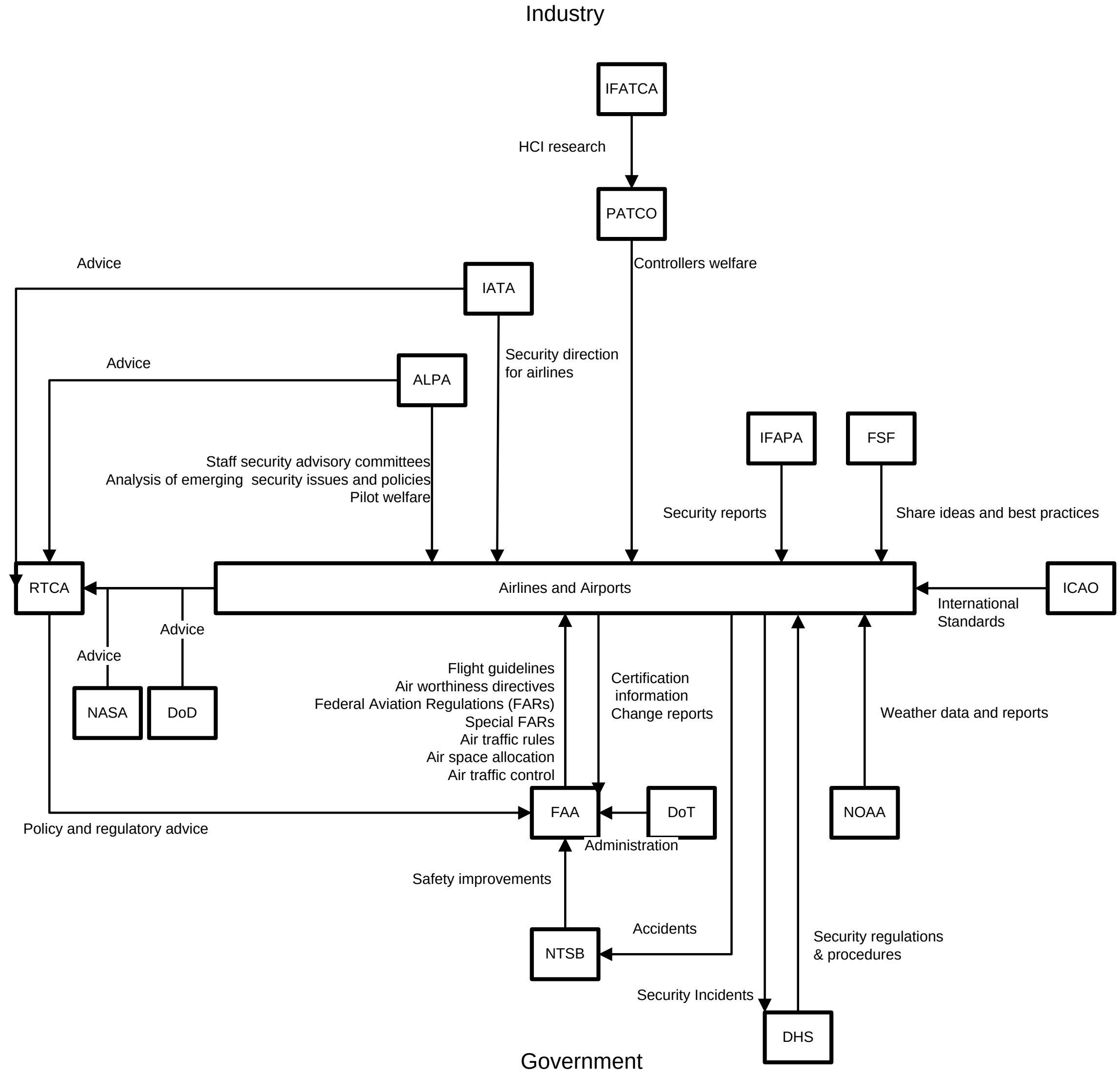

Figure 16. Current Airline/Airport Control Structure.

Above is a control structure diagram showing the lines of communication and control for the airlines and airports in the pre-NGATS environment. As the system evolves and NGATS is implemented, it is important that security-critical feedback is not lost. For example, the Radio Technical Commission for Aeronautics (RTCA) plays an important role by synthesizing the interests and advice of industry associations, unions, airlines, airports, and governmental entities and developing policy and regulatory advice for the FAA to influence the airlines and airports. The alignment of stakeholders on security objectives is essential to success. Key responsibilities and risks are shown below.

Item	Responsibility	Inadequate Control
Executive Departments and Agencies		
4	Issue security regulations and procedures	DHS regulations and procedures have not identified important vulnerabilities or threats.
		DHS regulations and procedures create new vulnerabilities and threats.
		DHS regulations and procedures are only issued after an attack has occurred.
		DHS regulations and procedures are rescinded in response to external pressure.
5	Issue flight guidelines, aviation regulations, and air traffic rules	FAA does not receive necessary policy and regulatory advice from the RTCA and proper administration from the DoT.
		RTCA advice and DoT administration interferes with the FAA's ability to issue guidelines, regulations, and air traffic rules that promote strong security.
		RTCA advice and DoT administration are not provided to the FAA until after an attack has occurred.
		RTCA advice and DoT administration are not present during a critical period.
6	Provide leadership for the development and operation of NGATS	Senior leadership lacks competence or places minimal priority on security issues and therefore does not adequately implement the security strategy.
		Senior leadership intentionally disrupts the security strategy.
		Senior leadership does not exercise good judgment or place priority on security issues in the period before an attack.
		Senior leadership stops providing competent judgment and making security a priority due to external pressure.

Table 8. Inadequate Controls for Executive Agencies.

Airlines, Airports, Development Companies, and the JPDO

Airlines, airports, communication companies, and others involved with the development of engineering systems associated with NGATS influence the JPDO by developing security policies, defining standards, and allocating resources. They have three principle responsibilities:

Item	Responsibility	Inadequate Control
Airlines and Airports		
7	Define the security policies	Industry associations do not provide necessary concerns, reports, best practices, and independent analysis.
		Industry associations provide concerns, reports, practices, and analysis that are not focused on improving security.
		Industry associations do not provide necessary concerns, reports, best practices, and independent analysis on time.
		Industry associations stop providing necessary concerns, reports, best practices, and independent analysis due to pressure from constituencies.
8	Modify policies and standards based on security reports from the JPDO	Airlines and airports do not create effective policies and standards.
		Airlines and airports create policies and standards that reduce security.
		Airlines and airports do not create policies and standards in a timely fashion.
		Airlines and airports stop creating policies and standards due to pressure.
9	Allocate resources for security	Insufficient funding is provided for security due to economic considerations.
		Funding for security is not provided.
		Security funding arrives late.
		Security funding is stopped before an attack.

Table 9. Inadequate Controls for Airlines and Airports.

Conversely, the JPDO provides feedback to the aforementioned companies through status and security reports. The JPDO also imposes policies and standards on aircraft manufacturers as well as infrastructure companies and system integrators. If security constraints are defined for the system in the development phase, they can be passed on to implementation and assurance organizations that provide feedback to the design group through test reports, review results, and threat assessments. The JPDO's roles and risks are provided in the table below.

Item	Responsibility	Inadequate Control
JPDO		
10	Set policies for aircraft manufacturers and other aerospace companies	JPDO policies are not helpful to aerospace companies.
		JPDO policies reduce the security of products and services from aerospace companies.
		JPDO security policies are shared with aerospace companies after design decisions have been made.
		JPDO stops providing security policies to aerospace companies.
11	Set security standards for the air transportation system design	Threat assessments do not influence subsequent standards.
		Security standards do not mitigate threats because they are inappropriate.
		Security standards are not provided when they are needed.
		Security standards are no longer issued so security-related changes are not incorporated.

Table 10. Inadequate Controls for the JPDO.

Those responsible for the maintenance and evolution of the system have the unique responsibility of bridging the development and operations activities. The development organizations must share design rationale and threat assessments and in turn accept security change reports reflecting system evolution. In parallel, the maintenance and evolution organization must receive problem reports, change requests, and performance audits from the operating process, the air transportation system, in order to develop revised operating procedures, software revisions, and hardware replacements.

Item	Responsibility	Inadequate Control
Design & Documentation / Implementation & Assurance / Maintenance & Evolution		
15	Define security constraints as well as testing standards	Test reports, review results, and threat assessments do not influence constraints and standards.
		Test reports, review results, and threat assessments lead to incorrect constraints and standards.
		Test reports, review results, and threat assessments are not available in time to inform constraints and standards.
		Test reports, review results, and threat assessments are no longer provided.
16	Share threat assessments and design rationale with the Maintenance organization	Maintenance organization does not receive design rationale and security analyses necessary to securely evolve the system.
		Maintenance organization receives incorrect design rationale and security analysis.
		Maintenance organization receives design rationale and security analysis after maintenance activities have been completed.
		Maintenance organization stops receiving design rationale and security analysis during maintenance activities.
17	Revise operating procedures and software as well as replace hardware	Problem reports, change requests, and performance audits do not influence changes to procedures, software, or hardware.
		Problem reports, change requests, and performance audits are flawed or misinterpreted so they produce detrimental changes to procedures, software, or hardware.
		Problem reports, change requests, and performance audits are not provided in a timely fashion so they have less effect on procedures, software, or hardware.
		Problems reports, change requests, and performance audits are not created or withheld from personnel responsible for revising operating procedures and software as well as replace hardware.

Table 11. Inadequate Controls for Development and Maintenance Organizations.

Change requests, audit reports, and problem reports must also be sent to airport and airline operations organizations so that work instructions from these groups influence the system's human controllers in the desired way. Similar to the development phase, the airports, airlines, and related companies define security policies as well as standards and allocate resources for the operations organizations. Operations reports must be sent to the company management in order to influence policies, standards, and resources. At the regulatory and industry association as well as legislative levels, the communication and control exhibited during system operations is very similar to system development.

5.2.5 Aircraft Operations

At this point in the analysis, now that the *organizational* risks have been elucidated, it is appropriate to consider the security implications of two major changes to *operation* of the aircraft themselves: removal of human(s) and removal of voice communications as a standard communication medium. There is no question that the removal of humans eliminates an entire class of security vulnerabilities. Nevertheless, automation has not been shown to be *inherently* more secure. When done improperly, automation can inject vulnerabilities. Similarly, voice communications are often involved in security incidents. However, any PC user that has gotten a virus or been involved in a distributed denial of service (DDoS) attack knows that computer-to-computer digital communication is often not secure. Leveson explains the need for humans in automated systems in *Safeware*:

> Computers and other automated devices are best at trivial, straightforward tasks. An *a priori* response must be determined for every situation: An algorithm provides predetermined rules and procedures to deal only with the set of conditions that have been foreseen. Not all conditions are foreseeable, however, especially those that arise from a combination of events, and even those that can be predicted are programmed by error-prone humans…Human operators are included in complex systems because, unlike computers, they are adaptable and flexible…Humans can exercise judgment and are unsurpassed in recognizing patterns, making associative leaps, and operating in ill-structured, ambiguous situations (Leveson 1995).

Pilots, air traffic controllers, radio operators, and others involved in the operation of aircraft must be aware of four classes of inadequate control actions that could interfere with their primary responsibility of operating the system without security incidents.

Item	Responsibility	Inadequate Control
Aircraft and Ground Operators		
18	Operate the system without security incidents	ATS operators make bad decisions because of poor assumptions and procedures.
		ATS operators choose to make decisions contrary to security objectives.
		ATS Operators does not make security decisions in a timely manner.
		ATS Operators make decisions supporting security but do not follow through and therefore have insufficient impact.

Table 12. Inadequate Controls for ATS Operators.

(Midkiff 2004) provides a detailed account of current aircraft operation procedures. Historically, these procedures have not been exploited to accomplish terrorist objectives. The reason for this is that attackers will almost always pursue the vulnerability that is most easily exploited. In this case, the vulnerabilities associated with passenger and cargo screening were blatantly obvious and enabled (suicide) hijackers to board an aircraft and take control. The current control structure for aircraft operations is shown below. The essential communication and control between aircraft, ground assets, and satellites are highlighted. As a representative example, threat six:

A terrorist interferes with the aircraft communication, navigation, or surveillance systems.

will be analyzed.

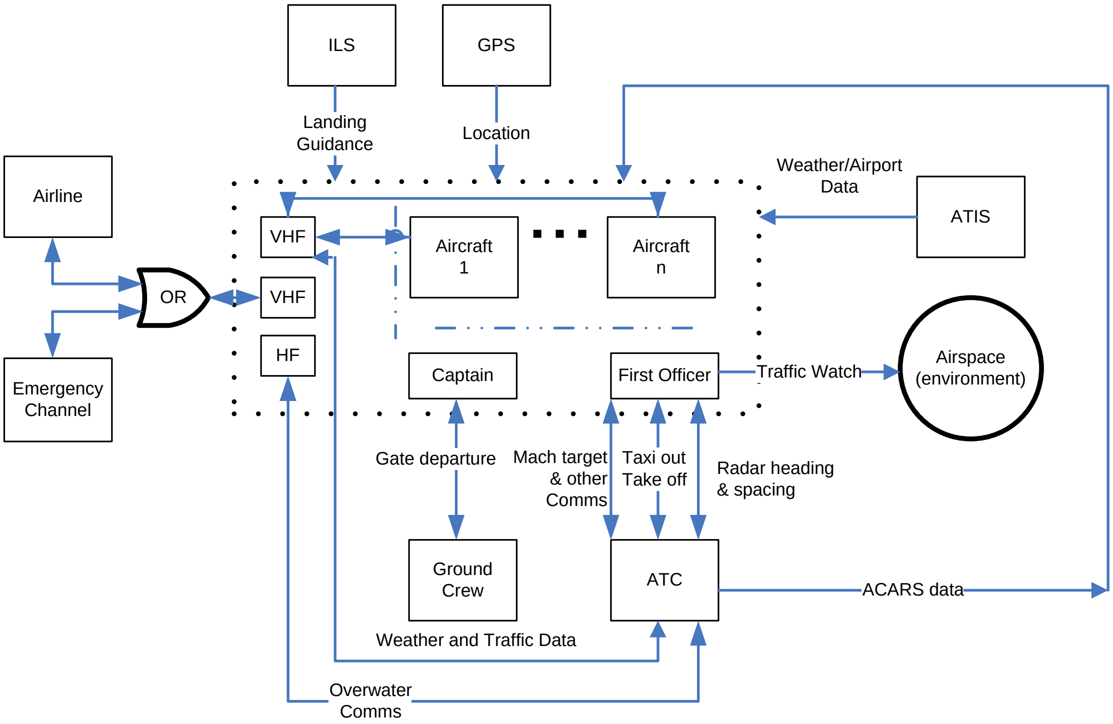

Figure 17. Current Aircraft Operations Control Structure.

During a flight, the airline communicates with an aircraft over a VHF radio. In the event of an emergency, if the aircraft is out of communication range with the airline, the cockpit may attempt to communicate with other aircraft or ground assets over the emergency channel. The second VHF radio is used to communicate with other aircraft in flight or air traffic control. Weather and traffic data is passed along over this channel. Finally, a HF radio is also required to provide over-water communications with ATC.

A variety of digital data links also exist to send data between aircraft and ground assets. The Aircraft Communication Addressing and Reporting System (ACARS) enables aircraft to transmit location (from GPS), altitude, and velocity information stored in the Flight Management System (FMS) computer to ATC over a satellite link. Similarly, ATC can send messages back to the FMS. Vital communications during the final phases of flight include position data from the Instrument Landing Systems (ILS) and automated audio recordings of non-control airport data (e.g. weather conditions) from the Automatic Terminal Information Service (ATIS).

Not surprisingly, the captain and first officer also play a key role in the control structure. Prior to takeoff, the captain coordinates activities with the ground crew while the first officer receives taxi out and take off information from ATC. Once the aircraft is airborne, the captain controls the aircraft as the first officer provides visual traffic watch, inputs the radar heading and spacing, sets the mach target, and handles any other additional communications with ATC.

With the drastic changes made to the ATS socio-technical control structure following 9/11, terrorists will likely be more inclined to instantiate threats in the operation of aircraft procedures. A detailed list of changes to current air operations that may introduce vulnerabilities are provided in **Appendix II**. Many of the changes in the control structure for NGATS are captured in the figure below.

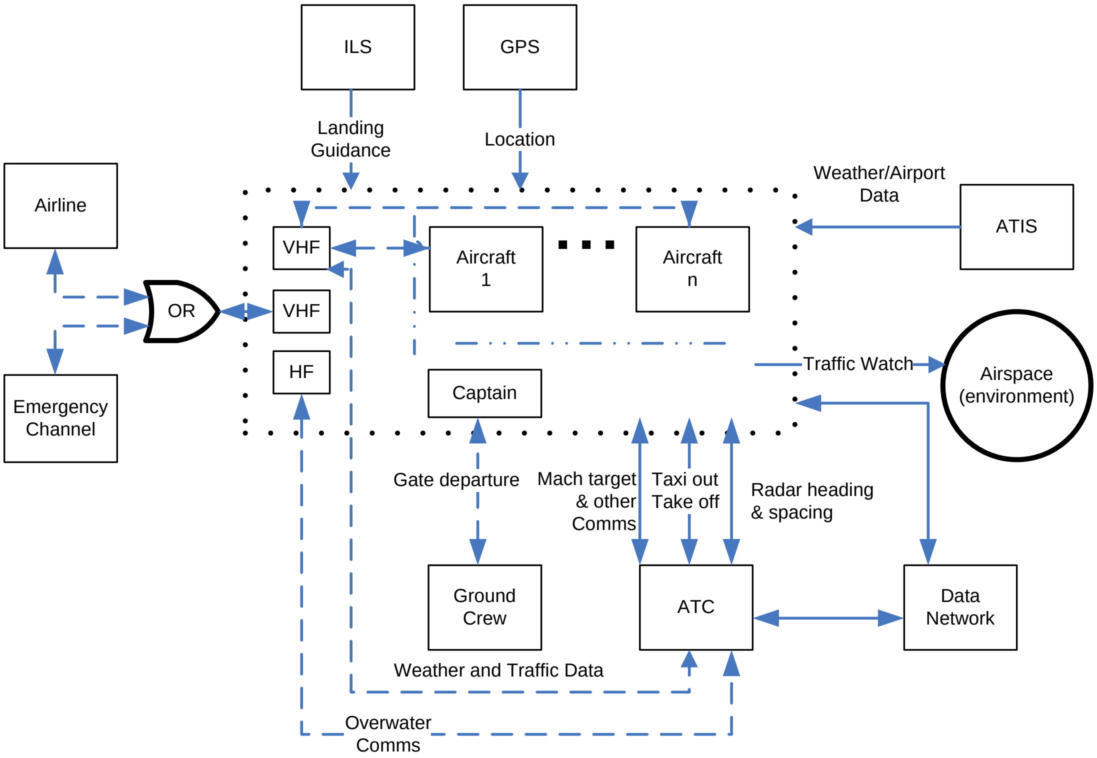

Figure 18. NGATS Aircraft/ATC Control Structure.

Immediately, one notices the fact that the traffic watch and early phase communications fall to the Captain. Additionally, a data network will be incorporated and used in place of voice communications (although voice communication equipment will still be onboard). The security requirements, control actions, and potential inadequate controls for the three principal components in this control structure are provided next.

Cockpit Crew (Captain and First Officer)

Security Constraints:

1. It must not be possible to disable TCAS from the cockpit. TCAS shall be functioning before ATC authorizes takeoff.
2. Pilots shall make setting the appropriate velocity a top priority.
3. Pilots shall make resetting the altimeter a top priority.
4. Pilots shall confirm over secure voice communications any suspicious ACARS data.
5. Cockpits shall display ATIS data visually as well as audibly.
6. Cockpits without crews (i.e. UAVs) shall have preprogrammed runways and landing information to be executed if communication with ATC is lost during descent, terminal area arrival, final approach, or landing.

Control Actions:

1. Regulation – Design: All new aircraft shall be designed to satisfy this security requirement. If the collision avoidance system is disabled, it is much easier for a terrorist to orchestrate a collision.
2. Regulation – Training and Standard Procedures: Operating procedures, flight simulators, and mandatory training shall equip pilots to set the appropriate velocity despite interruptions and distractions at different times. If the correct velocity is not set, it is much easier for a terrorist to orchestrate a collision.
3. Regulation – Training and Standard Procedures: Operating procedures, flight simulators, and mandatory training shall equip pilots to reset the altimeter despite interruptions and distractions at different times. If the correct altitude is not set, it is much easier for a terrorist to orchestrate a collision.
4. Regulation – Training and Standard Procedures: Operating procedures, flight simulators, and mandatory training shall equip pilots to verify suspicious ACARS data over voice communications.
5. Regulation – Design: Human factors experts will be responsible for ATIS subsystem design. If a terrorist distracts a pilot in the later phases of flight and he misses important ATIS information, a text-based version of the report will allow him to quickly get the necessary data.
6. Regulation – Design: All UAVs certified for operations in the NGATS shall be designed to satisfy the preprogrammed runway requirement. In the event that communication between ATC and a UAV is jammed, the UAV must still successfully land. One way to do this is to preprogram before takeoff an assigned runway as well as other details necessary for the UAV to reach its destination airport if communication is lost.

Potential Inadequate Controls:

1. TCAS
    a. Design regulations do not prohibit TCAS deactivation in the cockpit.
    b. Design regulations require TCAS deactivation in the cockpit.
    c. Design regulations prohibiting TCAS deactivation go into effect after NGATS certified aircraft are built.

    d. Design regulations prohibiting TCAS deactivation are suspended during NGATS operations.

2. Setting Velocity
    a. Procedures and training are insufficient to direct pilots to ensure that the correct velocity is set after they are interrupted.
    b. Procedures and training form pilots that are careless about setting the target velocity.
    c. Good procedures and training for setting the velocity target are developed too late.
    d. Procedures and training for setting the velocity target are withdrawn.
3. Resetting Altimeter
    a. Procedures and training are insufficient to direct pilots to ensure that the altimeter is reset at the proper time after they are interrupted.
    b. Procedures and training form pilots that are careless about resetting the altimeter.
    c. Good procedures and training for resetting the altimeter are developed too late.
    d. Procedures and training for resetting the altimeter are withdrawn.
4. ACARS Data
    a. Procedures and training are insufficient to direct pilots to ensure that suspicious ACARS data is verified with voice communications.
    b. Procedures and training form pilots that do not verify suspicious ACARS data over voice communications.
    c. Good procedures and training for verifying suspicious ACARS data over voice communications are developed too late.
    d. Procedures and training for verifying suspicious ACARS data are withdrawn.
5. ATIS Subsystem
    a. Design specifications do not require visual presentation of ATIS information.
    b. Design specifications do not allow visual presentation of ATIS information.
    c. Design specifications that mandate visual and audible presentation of ATIS information are created too late.
    d. Design specifications that mandate visual and audible presentation of ATIS information are withdrawn.
6. UAVs
    a. Design specifications do not require preprogrammed landing routines.
    b. Design specifications do not allow preprogrammed landing routines.
    c. Design specifications that mandate preprogrammed landing routines are created too late.
    d. Design specifications that mandate preprogrammed landing routines are withdrawn.

Air Traffic Control

Security Constraints:

1. A terrorist must not be able to remotely take control of an aircraft on the ground.
2. A terrorist must not be able to remotely take control of an airborne aircraft.
3. All UAVs shall be equipped with override technology to permit the FAA to take over control if suspicious behavior is observed.

Control Action:

1. Regulation – Design & Training and Standard Procedures: When the landing gear of a piloted aircraft is deployed, automated aircraft coordination technology (e.g. externally commanded separation distances) must be disabled. There is no reason for pilots not to have control during this period. Aircraft technology as well as pilot training must implement this control.
2. Regulation – Design: In order to optimize the queuing of airborne aircraft, NGATS plans to implement technologies to enable optimization of aircraft throughput. It is envisioned that aircraft in a flock would automatically coordinate altitude, separation distance, and velocity. Aircraft technology must permit pilots to override external controls and automatically inform other aircraft in the flock that the aircraft is breaking formation. This control prevents a terrorist from creating conditions with inadequate separation distance, dangerously low altitude, or dangerously high velocity for example.

   Additionally, in order to securely transition to reduced aircraft separation distances, more precise navigational aids are required. The current infrastructure associated with the terrestrial radio navigation is highly vulnerable. VHF Omni-directional Radio Range (VOR), Non-directional Beacons (NDB), and Distance Measuring Equipment (DME) are often located at remote positions at an airport and protected only by a chain-link fence or locked door. According to (Blakey 2006):

   > The current system of radio navigation aids is a large complex network of transmitters that require extensive resources to operate and maintain. The new global threat of terrorism also poses a threat to these systems. Security for these facilities is minimal. A coordinated effort to take a number of the transmitters off-line could cause disruptions throughout the air travel system. *Satellite and airborne surveillance systems provide a more secure system and increased operational safety*…With most of the money spent on aviation security directed toward the passenger, little focus has been spent on the radio navigation ground stations.

   The Automatic Dependent Surveillance-Broadcast (ADS-B) system is the solution to this problem. ADS-B receives positions information from the GPS network and combines it with an aircraft's altitude and velocity vector. This state variable is then broadcast to other aircraft and ground assets. It essentially provides the same information as TCAS but it does not coordinate maneuvers so cannot be considered a collision avoidance system. Finally, GPS is a much more secure system compared to terrestrial radio navigation. There are only five ground monitoring sites world-wide and even if they were all disabled, GPS could function for six months autonomously. Additionally, the US reliance on GPS for military operations makes the system well protected. Local jamming attempts have often proven ineffective due to error correction and signal integrity codes (Blakey 2006). See **Appendix III** for a possible deployment schedule.

3. Regulation – Design: It is possible that a terrorist may program a UAV to behave as a guided missile. In order to mitigate this threat, it must be possible for the FAA to securely access an in-flight UAV and redirect it to an airport or remote location if the UAV deviates from its flight plan and heads to a potential target. For example, if a UAV is supposed to carry cargo from Boston to New York but continues on past New York toward Washington DC, it must be stopped. Before takeoff, an FAA authority should provide the UAV with symmetric cryptographic keys valid only for the particular flight so that no one else may remotely access it afterwards.

Potential Inadequate Controls:

1. Ground Aircraft
    a. Approved aircraft designs do not disable remote control before takeoff and after landing.
    b. Approved aircraft designs make it impossible to disable remote control before takeoff and after landing.
    c. Aircraft designs that disable remote control before takeoff and after landing are approved after the system has been fielded.
    d. External pressure forces the regulation that mandates disabled remote control before takeoff and after landing to be withdrawn.
2. Airborne Aircraft
    a. Pilots are not able to override external controls.
    b. External controls are designed to override pilot actions.
    c. It takes long time for pilots to override external controls.
    d. Pilot actions can be interrupted by external controls.
3. UAVs
    a. UAVs are created that the FAA cannot control in an emergency
    b. UAVs are designed to override external FAA control.
    c. It takes an excessive amount of time for the FAA to take control of a UAV.
    d. FAA control of a threatening UAV can be disrupted.

Data Network

Security Constraints:

1. A terrorist must not be permitted to send data to aircraft during gate departure/taxi out/take off.
2. The signal carrying the Mach target shall be jam resistant.
3. A terrorist must not be able to communicate with airborne aircraft and impact flight operations.
4. All data transmitted over ACARS shall contain sender identity.
5. A terrorist shall not be able to send ATIS data that appears valid to a pilot.
6. A terrorist must not be able to send incorrect data during landing and rollout.

Control Action:

1. Regulation – Design: Communication between the cockpit, ground crews, and ground control, must be strongly secured. Given that such features as remote control of aircraft will be implemented over this network, firewalls and intrusion detection mechanisms are necessary, but not sufficient technologies. Attacks can develop from passengers within an aircraft as well as from external attackers over the satellite connection. Flooding and eavesdropping are particularly relevant issues in satellite networks due to their broadcast nature.

   Most researchers agree that an IP based scheme for the air to ground link is the best approach. IPSec is a solution that operates at the network layer. This guarantees compatibility with a variety of applications that use different schemes at the application and transport levels. The Authentication Header provides data authentication, the Encapsulating Security Protocol provides an encryption algorithm, and the Key Exchange Protocol defines how keys are shared. Additionally, IPSec can operate in two different modes. The payload of the packet is encrypted in Transport mode, while in Tunnel Mode the entire packet is encrypted and the IP header of the tunnel end point is appended. For more details see **Appendix IV**.
2. Regulation – Design: If the correct velocity is not set, it is much easier for a terrorist to orchestrate a collision. Therefore, electronic protection of the Mach target signal must be employed. The primary electronic protection technique relevant to aircraft operations is spread spectrum communications. Particular instantiations of spread spectrum technology include frequency hopping, direct sequence spread spectrum (DSSS), and burst transmission. Frequency-hopping devices jump from one frequency to another according to a pseudorandom sequence known only to trusted parties. Two metrics gauge its effectiveness, process gain and jamming margin.

   Process gain is: $\frac{SignalBandwidth}{InputSignalBandwidth}$

   For example, a 1 Mbit/sec signal spread over 100Mhz has a process gain of 100 dB.

Jamming margin is: $\dfrac{\Pr ocessGain}{MininumBit\left(\dfrac{Energy}{Noise}\right)}$

or more colloquially the "maximum tolerable ratio of jamming power to signal power." (Anderson 2001) Unfortunately, an attacker only needs to execute partial band jamming that creates enough errors that the signal is unreadable.

DSSS relies on similar principles compared to frequency hopping. The original narrow band signal is over-sampled and XORed with a wide band pseudonoise signal defined by a stream cipher. The receiver must XOR the same pseudonoise signal to recapture the demodulated signal from which the original signal can be extracted. DSSS provides the same theoretical jamming margin as frequency hopping but usually operates in a low power mode that makes it difficult for an enemy to detect the signal from the background noise.

Burst communications is achieved by compressing data and transmitting it in bursts at times defined by a similar pseudorandom sequence. This technique is not particularly jam resistant but offers the advantage of making the signal difficult to detect in the first place. "Modern military systems will use some combination of tight beams, DSSS, hopping, and burst" (Anderson 2001) and NGATS communication should as well. See **Appendix V** for more details.

3. Regulation – Design: An IPSec scheme based on elliptic curve cryptography describe in the first control action is also suitable for securing the ATN during the climb and cruise stages. In order to address particular details related to inter-aircraft communication and aircraft-ATC communication, **Appendix VI** provides more design details.
4. Regulation – Design & Training and Standard Procedures: Incorrect location, velocity, and altitude information can assist a terrorist in creating a collision. If the identity of sources transmitting ACARS data to the Flight Management System (FMS) computer cannot be verified, pilots should not act on them. Using the techniques discussed in **Appendix VI**, a sender ID should be bound to all messages. Additionally, pilot training must instill an instinct to distrust ACARS messages from unknown sources.
5. Regulation – Design: False weather reports may lead pilots to take the wrong action during the final phases of flight. Automated audio recordings of non-control airport data must be secured in a similar way as ACARS data.
6. Regulation – Design: The solutions in control actions 1 and 3 and their corresponding appendices effectively implements security requirement 6.

Potential Inadequate Controls:

1. Terrorists Compromise Communications during Gate departure/Taxi out/Take off
    a. Security protocols are not properly implemented and operators are not trained to use them correctly.
    b. Communications during Gate departure/Taxi out/Take off are not secured.
    c. It is possible to disable secure communications and terrorists exploit data transmitted over an open channel.
    d. Aircraft and ground crews/control begin communicating in a secure way but cease to do so at some point during gate departure, taxi out, or take off.
2. Mach Target Signal
    a. The Mach target signal is not designed to be jam resistant.
    b. The Mach target signal is designed to be easily jammed.
    c. Tight beams, DSSS, frequency hopping, and burst communications are used only after the Mach target has been set.
    d. Tight beams, DSSS, frequency hopping, and burst communications are used in the early phases of flight but disabled shortly before the cruise phase.
3. Terrorists Compromise Communications during Climb/Cruise
    a. Security protocols are not properly implemented and operators are not trained to use them correctly.
    b. Communications during Climb/Cruise are not secured.
    c. It is possible to disable secure communications and terrorists exploit data transmitted over an open channel.
    d. Aircraft and ATC begin communicating in a secure way but cease to do so at some point during the climb or cruise phases.
4. ACARS Transmissions
    a. ACARS data is sent without verifiable sender information.
    b. ACARS data is sent with false or unverifiable sender information.
    c. System operators start checking for verifiable sender information after they have received or acted on unverified data.
    d. System operators stop checking for verifiable sender information.
5. ATIS Transmissions
    a. Anyone can transmit what appears to be valid ATIS data.
    b. Terrorists change ATIS information transmitted by an airport.
    c. Terrorists send incorrect ATIS information for short time and pilots act on it.
    d. Terrorists send incorrect ATIS information after correct information was transmitted and pilots act on the new data.
6. Terrorists Compromise Communications during Landing and Rollout
    a. Security protocols are not properly implemented and operators are not trained to use them correctly.
    b. Communications during landing and rollout are not secured.

c. It is possible to disable secure communications and terrorists exploit data transmitted over an open channel.
d. Aircraft and ATC begin communicating in a secure way but cease to do so at some point during the landing or rollout.

5.2.6 System Dynamics Modeling

The final step of a STAMP-based analysis is System Dynamics (SD) modeling. System Dynamics is used to understand how the static control structure designed in the earlier stages *and* the attackers themselves could evolve. In particular, one is interested in evolution to insecure states such that security constraints would no longer be enforced by components in the socio-technical system. Unlike system safety engineering in which many risks and hazards are “generated” endogenously within the socio-technical system, security engineering risks and threats often develop exogenously. While the “insider-threat” must be addressed, malicious actors outside of the ATS must be modeled. Terrorist groups such as Al Qaeda, are an example of an exogenous factor. To illustrate the SD modeling approach in this thesis, a causal loop diagram model of terrorism and the outside factors that influence it was developed and analyzed.

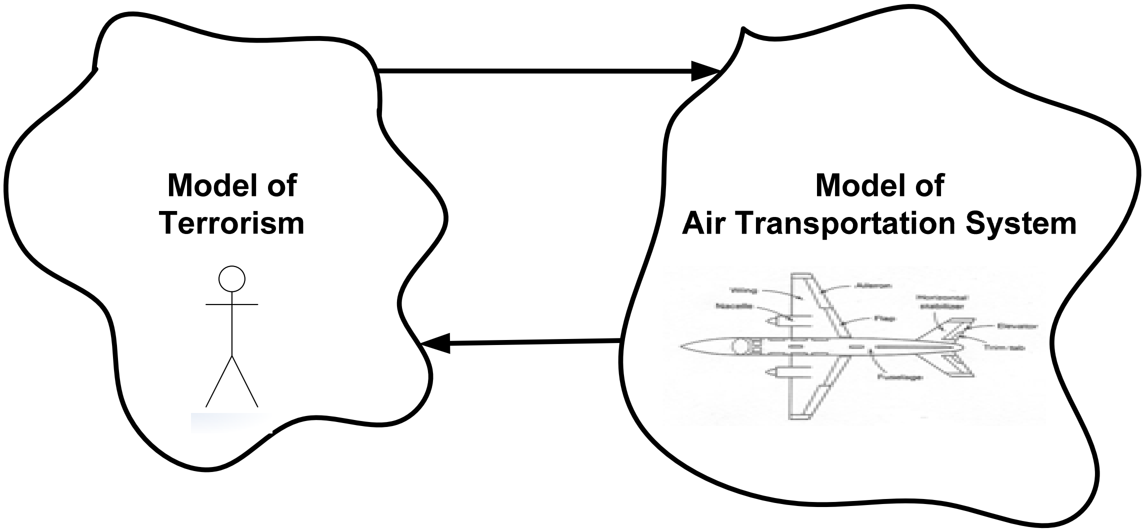

Figure 19. Relationship of Terrorism and ATS Models.

System Dynamics was created at MIT in the 1950s by Jay Forrester. Its theoretical basis comes from control systems and non-linear dynamics. Complex systems, whether they are technical, organizational, or some combination, often exhibit highly non-linear behavior where the relationship between cause and effect is not intuitively obvious. According to (Martinez-Moyano 2005):

> System Dynamics is a computer-aided approach to policy analysis and design that applies to dynamic problems arising in complex social, managerial, economic, or ecological systems. Dynamic systems are characterized by interdependence, mutual interaction, information feedback, and circular causality.

System Dynamics models are constructed by a combination or positive (reinforcing) and negative (balancing) feedback loops in addition to state and rate variables (Sterman 2000).

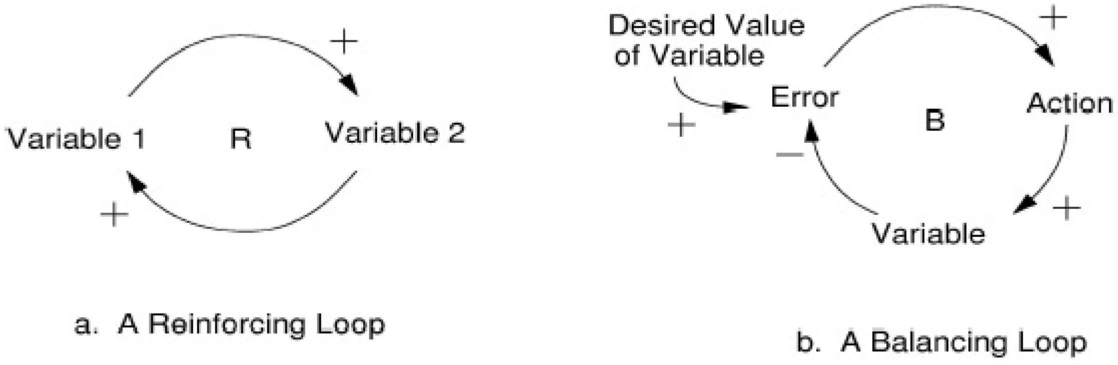

Figure 20. Reinforcing and Balancing Loops.
Image Source (Dulac 2007c)

At its lowest level, a SD model is a system of coupled, first order, non-linear ordinary differential equations presented in an easy to understand graphical form accessible to policy makers. The models can be simulated to obtain numerical results. In order to show the connection between traditional mathematics and SD visualizations, the figure below presents the graphical representation of a differential equation. While this level of understanding is not necessary for policy makers and managers to benefit from causal loop diagrams, the diagram is shown to assist scientists and engineers learning System Dynamics (Laracy 2007b). The state variable, *X*, is controlled by two rate variables, *Y* and *Z*. Three auxiliary variables also are also provided, *A*, *B*, and *T*, that define *Y* and *Z* and each other. Ultimately, this SD model integrates the differential equation, shown over the state variable, *X*.

$$\dot{X} = Y - Z$$

$$Y = 2B$$

$$A = \frac{X}{B}$$

$$Z = \frac{A}{T}$$

$$\dot{X} = 2B - \frac{X}{BT}$$

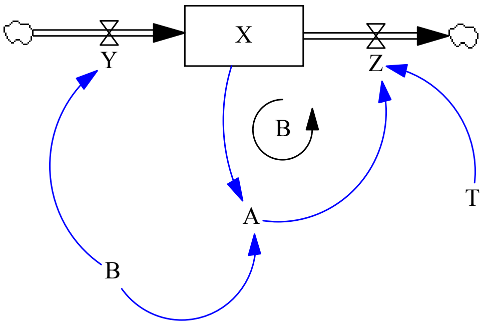

Figure 21. A Differential Equation Implemented as a System Dynamics Model.

The following quote by John Sterman, a leading scholar in the field, communicates the philosophy of System Dynamics (Sterman 2002):

> While it's hard to define what system dynamics is, I don't have any trouble answering why it is valuable. As the world changes ever faster, thoughtful leaders increasingly recognize that we are not only failing to solve the persistent problems we face, but are in fact causing them. *All too often, well-intentioned efforts to solve pressing problems create unanticipated "side effects."* Our decisions provoke reactions we did not foresee. Today's solutions become tomorrow's problems. The result is policy resistance, the tendency for interventions to be defeated by the response of the system to the intervention itself. From California's failed electricity reforms, to road building programs that create suburban sprawl and actually increase traffic congestion, to pathogens that evolve resistance to antibiotics, our best efforts to solve problems often make them worse. At the root of this phenomenon lies the narrow, event-oriented, reductionist worldview most people live by. We have been trained to see the world as a series of events, to view our situation as the result of forces outside ourselves, forces largely unpredictable and uncontrollable…System dynamics helps us expand the boundaries of our mental models so that we become aware of and take responsibility for the feedbacks created by our decisions. –John Sterman

The "well-intentioned efforts to solve pressing problems create unanticipated 'side effects'" mentioned above will be explored in the thesis' terrorism model.

It is helpful to consider SD models at various levels of abstraction. Dulac and Owens (Dulac 2007b) have defined a five layer hierarchy of abstraction. At the highest level of a model are the major loops. These are captured in what is usually referred to as a causal loop diagram. Large models may be broken into components, or modules, to achieve intellectual manageability goals. Within these modules, state, rate, and auxiliary variables are defined. Like any modeling activity, these variables carry a number of assumptions that are made explicit with data and equations.

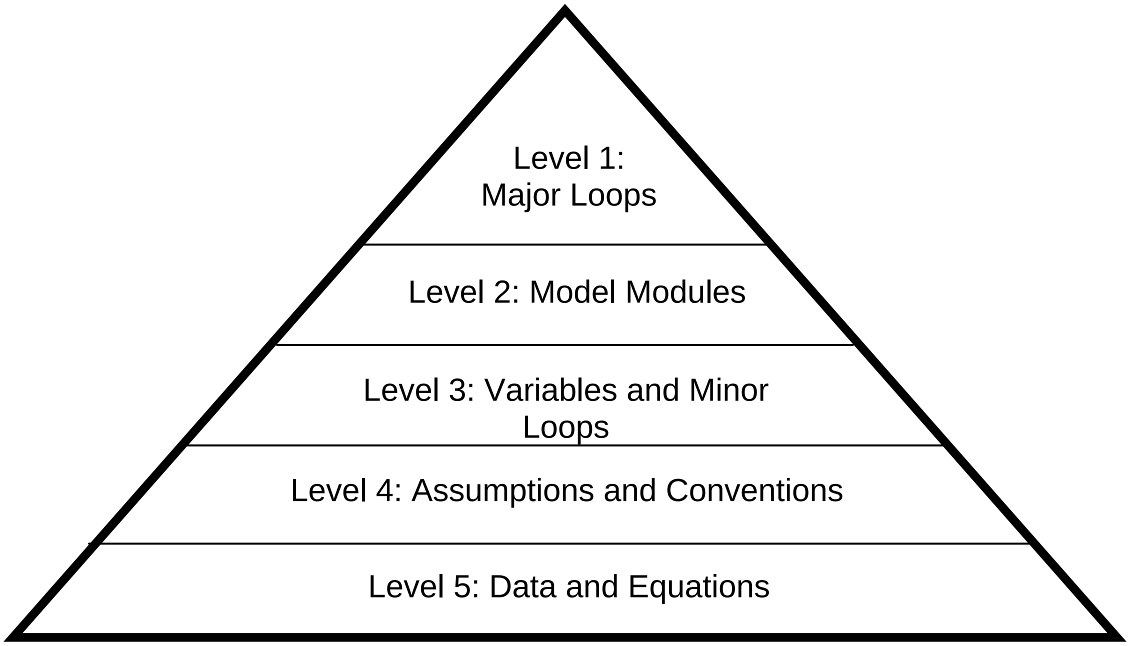
Level 1:
Major Loops
Level 2: Model Modules
Level 3: Variables and Minor
Loops
Level 4: Assumptions and Conventions
Level 5: Data and Equations

Figure 22. Owens-Dulac Abstraction Model for System Dynamics.
Image Source (Dulac 2007c)

5.2.6.1 A Model of Terrorism

Initially, simple causal loop diagrams are developed that elucidate the non-linear cause-effect relationship. These qualitative models suggest policies that acknowledge feedback in the system and can prevent delayed unintended consequences. Causal loop diagrams, and more generally system archetypes (Senge 2006), anchor the development of high fidelity, quantitative models that allow the use of simulation to explore scenarios and rigorously investigate dynamic hypotheses (Gonzalez 2005). The causal loop diagram below corresponds to Level 1 in the Owens-Dulac hierarchy. It was developed by the author in a modeling activity with John Sterman and Kim Thompson.

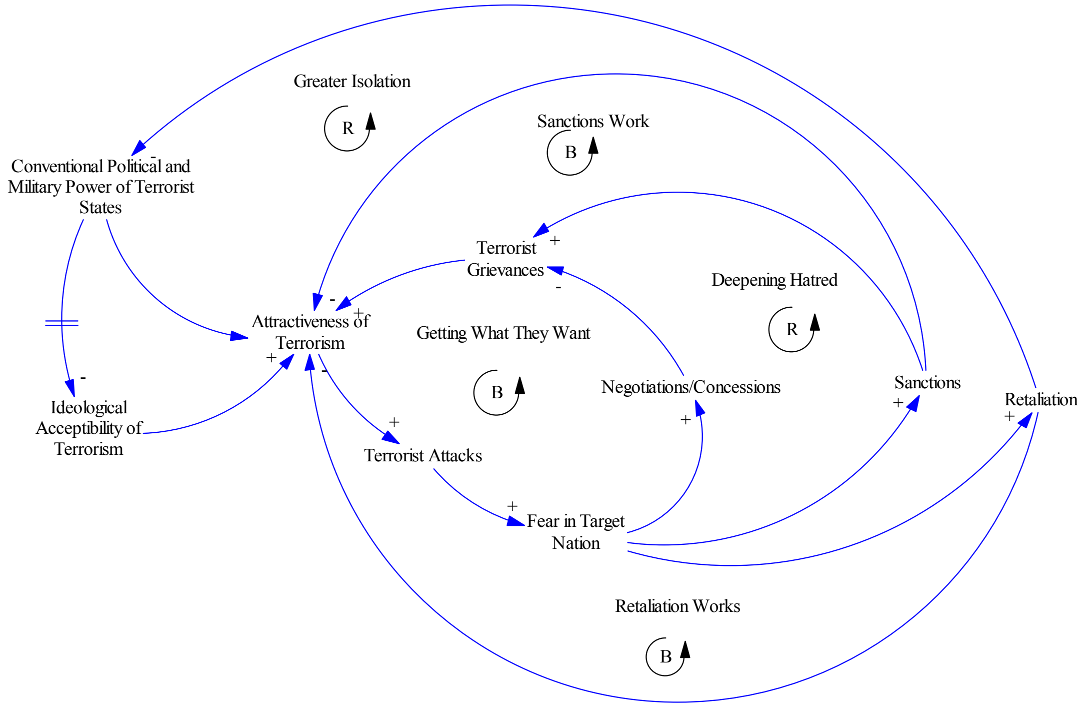

Figure 23. Causal Loop Diagram of Terrorism.

The model contains the major feedback loops that govern the behavior of terrorists, such as those that would attack the Air Transportation System. In order to accomplish the goal of minimizing the *Attractiveness of Terrorism*, one must examine the reinforcing and balancing loops that influence terrorist behavior.

Retaliation Works (Balancing Loop)

The first balancing loop is called *Retaliation Works*. In this loop, one sees that as the *Attractiveness of Terrorism* increases, *Terrorist Attacks* increase, *Fear in Target Nation* increases, and so does *Retaliation*. The net effect of this is that *Attractiveness of Terrorism* decreases. This result was certainly not intended by the terrorists involved, but nonetheless has shown to be true in some instances (e.g. Barbary Pirates in 1815 and the Taliban Government in 2001).

Greater Isolation (Reinforcing Loop)

However, an increase in retaliation also has the potential to reinforce the *Attractiveness of Terrorism*. Retaliation has the effect of reducing the *Conventional Military and Political Power of Terrorist States*, thereby increasing the attractiveness of asymmetric warfare, such as the attack on 9/11. Part of this causal loop also has the potential, with a delay, to increase the *Ideological Acceptability of Terrorism*, thus increasing the *Attractiveness of Terrorism*.

Sanctions Work (Balancing Loop)

Instead of retaliation, *Sanctions* are another option to be explored to mitigate the threat of terrorism. An increase in the *Attractiveness of Terrorism* will lead to an increase in the *Fear in Target Nation*, an increase in *Sanctions*, and finally a decrease in the *Attractiveness of Terrorism*.

Deepening Hatred (Reinforcing Loop)

However, *Sanctions* can also lead to deepening hatred. *Sanctions* may fuel *Terrorist Grievances* and therefore increase the *Attractiveness of Terrorism*. In the later half of the twentieth century, economic sanctions against Middle Eastern states that support terror have been a cause for terrorists to incite populations against the United States.

Getting What They Want (Balancing Loop)

Another loop can create the situation where the increase in *Terrorist Attacks* leads to an increase in *Fear in Target Nation* that leads to an increase in *Negotiations/Concessions*. *Negotiations/Concessions* reduce *Terrorist Grievances* and finally reduce the *Attractiveness of Terrorism*. The terrorist attack in Spain on March 11, 2004 days before the national election led to the selection of a government sympathetic to the causes of Jihadists and the cessation of terrorist attacks in that country.

5.2.6.2 Impacts of System Dynamics

New strategies must be developed to prevent an attack as well as manage the aftermath. Informal, ad hoc approaches will almost certainly fall short of accomplishing the desired goal of little to no casualties (Laracy 2006). A rigorous, systematic method is necessary to develop an appropriate approach. Traditional mathematical modeling has made significant contributions to this end. However, according to John Sterman, "The greatest potential for improvement comes when the modeling process changes deeply held mental models." (Sterman 2000) The author proposes an approach that brings the power of control theory in an accessible way to security professionals and policy makers involved in the Air Transportation System. In consultation with air transportation security experts, future work in this area would involve defining the references modes for the key variables described above and instantiating a simulation model.

CHAPTER 6: Conclusion

6.1 Results

In Chapter Three, the question was asked:

> Can a security model be developed that does not rely on the assumptions of quantitative risk assessment, considers issues at a level closer to system design and operation compared to game theory, and supports successful red teaming?

The STAMP based analysis presented in this thesis offers an approach that answers in the affirmative. STAMP-Sec addresses many of the pitfalls associated with applying quantitative risk assessment and game theory to security problems. Additionally, it implicitly supports the use of red teaming to test that the socio-technical system has not evolved in such a way that security constraints are no longer enforced.

Unlike probabilistic risk assessment approaches (Apostolakis 2004), STAMP-Sec appropriately addresses the role of software, human factors, security culture, and design errors in the development of engineering systems. In fact, it explicitly addresses how to incorporate these key factors into the security requirements (i.e. constraints) of the Air Transportation System. The inherent flaws in the use of subjective probability (i.e. expert guessing) identified by (Tversky 1974) are completely avoided. No assumptions are made as to the adherence of system users and attackers to the axioms of rationality (Savage 1954). Perhaps most importantly, the engagement between the attacker and the defender of the system has not been excessively simplified (e.g. abstracting the engagement to a two-stage Markov process) to facilitate modeling. Finally, the intelligence of the adversary is appreciated unlike reliability-based approaches that apply the 80/20 rule (Bier 2005).

Similarly, the STAMP approach does not share the inherent weaknesses of game-theoretic security modeling. Game theory models of security often make simplifying assumptions such as the attacker can only execute one attack at a time. STAMP-Sec does not engage in these types of assumptions. The fact that defenders and attackers may value targets differently is not relevant and no mathematical assumptions are made such as the fact that the probability of an attack is a convex function of the defensive resource spending. If a STAMP-based executable simulation is developed, sensitivity analysis of System Dynamics models eliminates the uncertainty that initially exists with quantitative model parameters. Lastly, unlike game theory's emphasis on strategy, STAMP-Sec informs both the design and tactical operation of complex engineering systems.

STAMP-Sec provides concrete information that can be directly incorporated into requirements and design documents. Furthermore, it provides recommendations for how to address these security issues through the definition of constraints, responsible components, and control actions. Finally, the possible inadequate controls and causes for constraint violation are explored.

Informational, operational, and physical security issues are addressed holistically. Notably, many of the security issues identified in this thesis are not associated with the failure of any device or subsystem. Rather, threats emerge from inadequate control. By showing where communication and feedback could be lost in the transition from the current ATS to NGATS, many risks are identified. Additionally, given the use of increased automation in NGATS, STAMP-Sec is particularly applicable because it acknowledges the role that software plays in security incidents. In conclusion, the aforementioned strengths, sustained by the valuable results obtained for the Next Generation Air Transportation System, support the hypothesis that STAMP provides insight into security problems and motivates future research to further categorize its strengths and weaknesses.

6.2 Future Work

The results from this thesis motivate a variety of future work in the field of system security. With regard to the Next Generation Air Transportation, the analysis provides a good starting point for the JPDO to pursue a STAMP-based approach to achieving security goals. Given its applicability to the ATS, it would also be worthwhile to apply the methodology to other infrastructure systems such as damns, tunnels and bridges, and oil- natural gas rigs. Finally, this research inspires continued work showing the interconnection of technology, organizations, and human behavior in security.

"What's the difference between a highly secure computer and a brick?
It's cheaper to use a brick to hold a door open."
- David Clark

And you will know the Truth, and the Truth will set you free.

John 8:32

APPENDIX I – 9/11 Timeline

1988: Al Qaeda was formed.
1992: Al Qaeda attacked Yemeni hotel housing US military personnel.
1993: Al Qaeda shot down US helicopters in Somalia.
1995: Al Qaeda bombed US troops training the Saudi National Guard in Riyadh.
July, 1995: A National Intelligence Estimate (NIE) predicted terrorist attacks in the US. It warned that the danger was increasing and that the "White House, the Capitol, symbols of capitalism such as Wall Street, critical infrastructures such as power grids, areas where people congregate such as sports arenas, and civil aviation" were particularly vulnerable.
1996: The "Gore" Commission on Aviation Security that was formed to identify deficiencies in Aviation Security did not identify suicide hijackings as a possibility.
1997: A NIE stated that "Iran and its surrogates, as well as terrorist financier Usama Bin Ladin and his followers, have stepped up their threats and surveillance of US facilities abroad in what also may be a portent of possible additional attacks in the United States."
June, 1998: Intelligence briefing entitled "Bin Ladin Threatening to Attack US Aircraft."
August, 1998: Intelligence reports indicate interest by Libyan terrorists to crash a plane into the World Trade Center. Also, hundreds are killed by Al Qaeda terrorists in the bombings of US embassies in Dar es Salaam, Tanzania and Nairobi. President Clinton ordered a missile attack against terrorist targets in Afghanistan.
December 4, 1998: DCI Tenet issued a directive to CIA officials on the importance of counter-terrorism operations stating: "We are at war. I want no resources or people spared in this effort, either inside CIA or the Community."
January, 1999: Intelligence briefing entitled "Strains Surface Between Taliban and Bin Ladin".
April, 1999: The *New York Times* ran an article entitled "US Hard Put to Find Proof Bin Laden Directed Attacks" that attempted to debunk claims that Bin Ladin was a terrorist leader.
June, 1999: Intelligence briefing entitled "Terrorist Threats to US Interests in Caucasus."
December, 1999: Intelligence briefing entitled "Bin Ladin to Exploit Looser Security During Holidays."
August, 1999: The FAA Civil Aviation Security Intelligence Office report judged a "suicide hijacking operation" to be unlikely because "it does not offer an opportunity for dialogue to achieve the key goal of obtaining Rahman and other key captive extremists."
December 12, 1999: Jordanian authorities arrested 16 members of Al Qaeda plotting to bomb a hotel in Jordan, a site along the Israel/Jordan border, and 2 Christian holy sites.
December 14, 1999: Ahmed Ressam, a member of Al Qaeda, was arrested at the US/Canada border for plotting to bomb Los Angeles International Airport.
March, 2000: Intelligence briefing entitled "Bin Ladin Evading Sanctions."
October 12, 2000: USS Cole attacked by Al Qaeda agents.
January/Feburary, 2001: DCI Tenet and Deputy Director for Operations Pavitt brief President Bush, VP Cheney, and NSA Rice on the threat of Al Qaeda. Bush asked whether killing Osama Bin Ladin would solve the problem. Tenet and Pavitt answered

that it would reduce the threat, but to completely remove it required disrupting Al Qaeda's ability to use Afghanistan as a sanctuary.

February, 2001: Intelligence briefing entitled "Bin Ladin's Interest in Biological, Radiological Weapons."

March: Terrorist advisory issued for a heightened threat of Sunni extremists against US facilities, personnel, and interests. Additionally, due to the fact that the CIA Counterterrorist Center (CTC) staff was overwhelmed just doing collection duties, DCI Tenet created a strategic assessments branch with a senior manager reporting to him and 10 new analysts.

April 13: The FBI directed field offices to query human sources and databases for information pertaining to "current operational activities relating to Sunni extremism." There was no mention of a domestic threat.

May: An intelligence report stated that "Bin Ladin network's plans advancing." A FBI walk-in suggested attacks were planned against London, Boston, and New York. A US embassy received a phone call indicating that Bin Ladin planed to attack the US with "high explosives." The FAA issued a notice to airlines about the potential for "an airline hijacking to free terrorists incarcerated in the United States."

May 17: US Counterterrorism Security Group (CSG) #1 agenda item was "UBL: Operation Planned in US."

May 29: The head of the CSG, Richard Clarke, asked NSA Rice to ask DCI Tenet what the US could do to prevent Abu Zubaydah from launching "a series of major terrorist attacks." He further stated that "when these attacks occur, as they likely will, we will wonder what more we could have done to stop them."

June 12: CIA reported that Khalid Sheikh Mohammed was recruiting terrorists for Bin Ladin to travel to the US to meet operatives there.

June 21: US Central Command raised force protection level to Delta (highest level).

June 22: CIA notified all station chiefs that al Qaeda was planning suicide attacks against US targets over the next few days.

June 25: Clarke warned Rice and her deputy, Hadley, that "A series of new reports continue to convince me and analysts at State, CIA, DIA, and NSA that a major terrorist attack or series of attacks is likely in July." An al Qaeda intelligence report warned that something "very, very, very, very" big was about to happen.

June: Terrorist advisories issued in late June were entitled "Bin Ladin Attacks May be Imminent" and "Bin Ladin and Associates Making Near-Term Threats."

July 2: FBI Counterterrorism Division notified federal agencies as well as state and local officials that "The FBI has no information indicating a credible threat of terrorist attack in the United States." Meanwhile, overseas, al Qaeda disruptions activities were occurring in 20 countries.

July 5: Clarke arranged for the CIA to brief the INS, FAA, Coast Guard, Secret Service, Customs Department, and FBI on the al Qaeda threat.

July 9: Clarke met with 27 agencies including the groups present on July 5 on the "current threat level."

July: In mid-July, reports indicated that al Qaeda's plans were delayed two months. Additionally, an FBI agent in Phoenix sent a memo to FBI HQ and NY identifying the "possibility of a coordinated effort by Usama Bin Ladin" to send terrorists to US flight schools. The agent felt that there was an "inordinate number of individuals of

investigative interest" studying aviation in Arizona. He recommended compiling a list of aviation schools, establishing a liaison with the schools, discussing the matter with the Intelligence community, and seeking authority to obtain visa information on the students.
July 27: Clarke informed Rice and Hadley that a "spike in intelligence about a near-term al Qaeda attack had stopped."
July 31: An FAA notice stated that "reports of possible near-term terrorist operations…particularly on the Arabian Peninsula and/or Israel." Tenet stated that his world was "blinking red" and that it could not "get any worse."
August 1: FBI issued an advisory that increased attention should be paid to security planning.
August 3: Intelligence advisory indicated that "al Qaeda was lying in wait and searching for gaps in security before moving forward with the planned attacks."
August 6: In response to questioning by President Bush starting in the spring about whether there was a domestic threat, a PDB on this day was entitled "Bin Ladin Determined to Strike in US." At this time, the FBI had 70 on-going investigations into Bin Ladin.
August 17: INS arrested Zacarias Moussaoui on immigration violations and a deportation order was issued. FBI HQ felt that FBI agents in Minneapolis were trying to get people "spun up." The supervisor in Minneapolis stated that he was **"trying to keep someone from taking a plane and crashing into the World Trade Center."** FBI HQ thought this was very unlikely and wasn't sure if Moussaoui was a terrorist.
August 23: DCI Tenet read a brief entitled "Islamic Extremist Learns to Fly" and learns about Moussaoui. "Tenet was told that Moussaoui wanted to learn to fly a 747, paid for his training in cash, was interested to learn the doors do not open in flight, and wanted to fly a simulated flight from London to New York."
September 4: In response to DoD and CIA foot-dragging, Clarke wrote a memo to Rice asking "are we serious about dealing with the al Qida threat?"
September 10: The first senior manager of the CIA Counterterrorist Center (CTC) reports for duty.
September 11: Three planes are taken over by suicide hijackers from Al Qaeda.

Source: Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition.

APPENDIX II – NGATS Vulnerabilities

Gate Departure/Taxi Out/Take Off

Activity	Vulnerabilities
1. When the aircraft is ready for departure, the Captain talks with the tug driver or ground crewmember over the interphone while the First Officer communicates with ATC or ramp control over the VHF radio.	A. Standard operating procedure (SOP) (JPDO 2004) does not involve human communication and coordination of cockpit with tug driver, ground crew, ATC, or ramp control. B. Captain must coordinate departure with both the ground crew and ATC.
2. During initial climb-out, a crew member must perform "traffic watch" in addition to monitoring TCAS.	C. TCAS is practically the only traffic advisory system because a Captain cannot perform visual "traffic watch."
3. During terminal area departure, ATC provides radar heading assignments to provide for adequate spacing and minimize ground track.	D. Separation distance is too close for a human to safely operate the aircraft.
4. During the climb, the crew compares the optimal and maximum cruise altitudes as well as the desired velocity by reviewing the FMS and/or performance charts. The optimal cruise altitude is defined by sharing this information with ATC.	E. The Captain will be required to compare the optimal and maximum cruise altitudes as well as the desired velocity by reviewing the FMS and/or performance charts without assistance. F. SOP does not involve human communication and coordination of cockpit with ATC.

Climb/Cruise

Activity	Vulnerabilities
5. After the aircraft passes 18,000 feet MSL, the altimeter is reset by the crew from a local barometric pressure setting to the standard atmosphere pressure reference. It is important that all aircraft at high altitudes use the same pressure reference.	G. The Captain must reset the altimeter in addition to the traditional duties.
6. At cruise altitudes, 2000 ft vertical separation is required. 1000 ft is permitted if the aircraft meets requirements for reduced vertical separation minimums.	H. Separation distance is too close for a human to safely operate the aircraft in flight.
7. When the aircraft approaches cruise altitude, the Mach target is set and reported to ATC.	I. SOP does not involve human communication and coordination of cockpit with ATC.
8. Aircraft should have 2 VHF transceivers and 1 HF radio if overwater certified. 1VHF radio is set to ATC and the other is set to a company channel or the universal emergency channel. SATCOM is a superior technology over HF when available. When out of ATC contact, the aircraft switches VHF frequencies to the air-to-air channel to get ride reports and en-route weather reports from other aircraft.	J. SOP does not involve human communication and coordination of cockpit with ATC, the airline, or other aircraft. K. En-route weather and ride reports are not shared as much.
9. ATC coordinated deviations due to thunderstorms over the VHF.	L. SOP does not involve human communication and coordination of cockpit with ATC however an improved weather monitoring and response system will be in place.

Descent/Terminal Area Arrival/Final Approach/Landing and Rollout

Activity	Vulnerabilities
10. When descent begins, ATC communicates over VHF radio or ACARS. The aircraft provides its touchdown estimate and any other important information. ATC sends arrival gate assignment and ground power status vocally over VHF or electronically through ACARS.	M. All descent, approach, landing, and rollout information will be sent over ACARS. N. SOP does not involve human communication and coordination of cockpit with ATC.
11. Descent planning uses the FMS to calculate the flight profile. Pilots do mental math to confirm the FMS instruction.	O. In UAVs, no independent confirmation of the flight profile from the FMS will take place.
12. Automatic Terminal Information Service (ATIS): Continuous radio broadcast of weather, instrument approach procedures, active runways, wind shear reports, visibility values for individual runways, braking capability, bird activity, and other safety information.	P. The Captain must monitor ATIS in addition to other responsibilities.
13. As the aircraft descends below 10,000 ft, it switches to a local barometric setting from ATC or ATIS and uses STAR or radar vectors from ATC to define a flight path.	Q. Increasing use of standard arrival routes and less interaction with ATC for a flight path. R. SOP does not involve human communication and coordination of cockpit with ATC.
14. 10 miles from landing, during precision approaches, GPS and ILS (Instrument Landing Systems) [Localizer and Glide Slope] are required.	S. New aircraft and crews trained for these aircraft will not integrate well with antiquated airports that do not offer precision approaches.
15. Non-precision approaches use a local navigation aid or satellite for lateral track data but vertical track data comes from barometric referencing.	T. New aircraft and crews trained for these aircraft will not integrate well with antiquated airports that do not offer precision approaches.
16. During very low visibility, autoland or HUD guidance is required.	U. UAVs cannot use *existing* technologies designed to assist humans such as a HUD to facilitate with landing.
17. Once the aircraft leaves the runway, the First Officer communicates with ground control from taxi instructions and local ramp control to confirm gate status.	V. The Captain must communicate with ground control and ramp control as well as operate the aircraft. W. SOP does not involve human communication and coordination of cockpit with ground and ramp control.

Table 13. Vulnerabilities

Clearly, given the JPDO intentions (Swenson 2006) of removing crew, eliminating voice communications, and reducing separation distances, many of the vulnerabilities identified above cannot be eliminated by changing the design. However, the following vulnerabilities can be mitigated with appropriate design.

K. En-route weather and ride reports are not shared as much
L. SOP does not involve human communication and coordination of cockpit with ATC. However, an improved weather monitoring and response system will be in place
Q. Increasing use of standard arrival routes and less interaction with ATC for a flight path
S/T. New aircraft and crews trained for these aircraft will not integrate well with antiquated airports that do not offer precision approaches

A well designed user interface (UI) for sharing weather and ride reports with other aircraft over bodies of water and other zones that separate aircraft from ATC would do much to facilitate report sharing. Similarly, a strong UI that takes advantage of the improved weather monitoring and response system could provide a suitable, and perhaps superior, replacement for the current voice system with ATC. Also, an easy to use procedure must be developed for pilots to get a real time, dynamic arrival route when they feel uncomfortable with the STAR. Finally, <u>all</u> airports should be fitted with precision approach equipment and <u>all</u> aircraft and crew should be equipped and trained to land in conditions where the precision system has failed.

APPENDIX III – ADS-B Deployment Schedule

Time for Implementation and Absorption of Cost

Years	Objective
0	Start of Transition, Execution of FAA Mandates.
0-3	Certification of GPS SPS signal as the primary domestic navigation means. Increase coverage area of ADS-B system to cover low volume traffic areas.
3-6	Require all commercial transport aircraft to certify or install an approved GPS navigation system. Increase ADS-B coverage to all areas except the area with the highest traffic area. Place low volume area NDB, VOR, and DME stations in inactive mode.
6-8	Require installation of ADS-B by all commercial transport aircraft. Complete ADS-B coverage area. Inactivate NDB, VOR, and DME stations except those around major airports or route transitions.
8-10	Inactivate remaining NDB, VOR, and DME stations; require all ATC users to have a certified GPS SPS system and ADS-B system.
10	Transition Complete, NAS is Free-Flight Capable.

Table 14. ADS-B Transition Plan.
Table Source (Blakey 2006)

APPENDIX IV – Cryptographic Designs

Unlike IPSec, SSL/TLS operates at the transport layer. It uses symmetric key algorithms to protect messages while a public key system handles key exchange. After a handshake with the server, the communicating pair agrees on version, session ID, encryption method, and compression technique (Thanthry 2006). An example of the activities that occur at the seven layers of the Internet layered architecture is presented below.

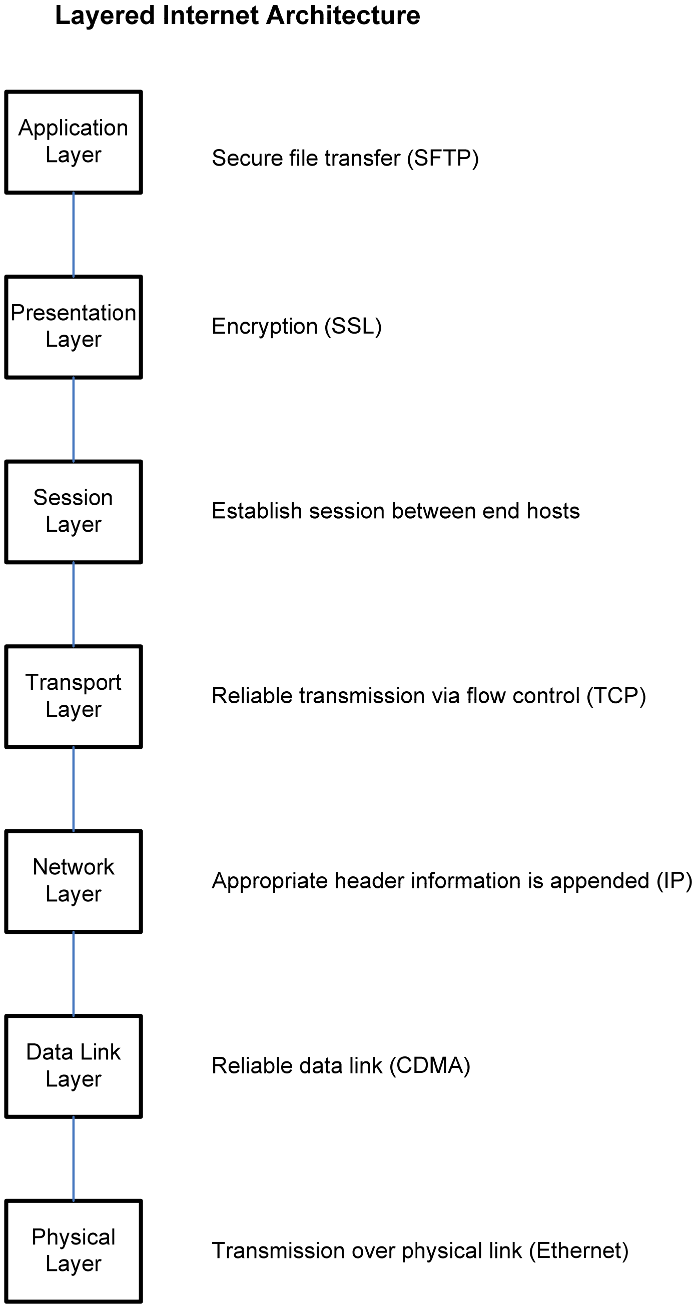
Layered Internet Architecture
Application Layer
Secure file transfer (SFTP)
Presentation Layer
Encryption (SSL)
Session Layer
Establish session between end hosts
Transport Layer
Reliable transmission via flow control (TCP)
Network Layer
Appropriate header information is appended (IP)
Data Link Layer
Reliable data link (CDMA)
Physical Layer
Transmission over physical link (Ethernet)

Figure 24. Layered Internet Architecture.
Image Source (Shah 2006)

Significant latency and variable round trip time in the ATN motivates the use of Performance Enhancing Proxies (PEP). However, PEPs must have access to the transport layer header and IPSec hides this information both in transport mode and tunnel mode.

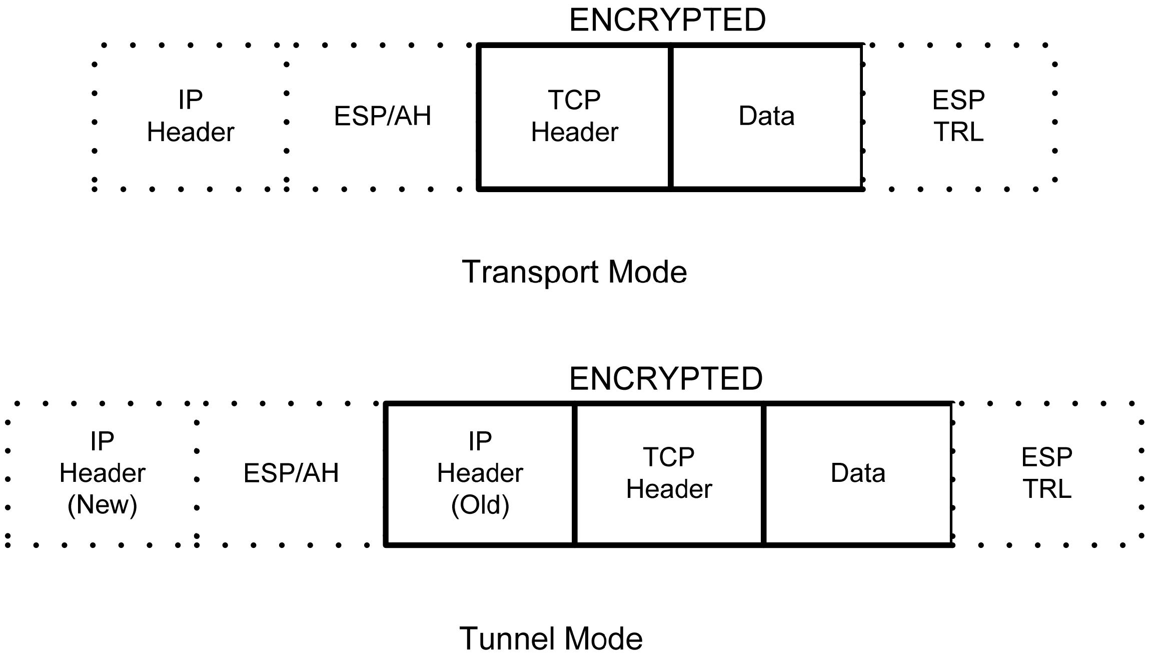

Figure 25. IP Datagrams.
Image Source (Thanthry 2006)

Solutions exist that involve multiple encryption/decryption operations at each PEP agent, but complexity makes this approach undesirable. SSL/TLS is compatible with PEP agents but leaves the network susceptible to transport layer attacks. This situation yields the classic security vs performance engineering tradeoff. Thanthry et al's simulation results presented below indicate that without PEP, IPSec and SSL/TLS are virtually identical. However, the incorporation of PEP agents almost triples performance in the SSL/TLS implementation.

Throughput in Mbps

	Without PEP	With PEP
Normal Scenario	6.7	-
Normal Scenario with Satellite Link Impairments	0.61	1.77
IPSec	0.5925	0
SSL/TLS	0.5975	1.76

Table 15. Effect of Performance Enhancing Proxies.
Table Source (Thanthry 2006)

Thanthry et al feel that the performance gains offered by SSL/TLS are significant and offer sufficient security. This author disagrees because a vulnerable transport layer permits certain distributed denial of service attacks (DDoS) (Greenspan 2004) and session hijacking. A DDoS attack could cut off all aircraft from ground control if the satellite constellation was overwhelmed. Session hijacking permits a hacker to masquerade as either an aircraft or ATC once a connection between the two is established (authentication occurs only at the start of the session).

The current US airspace system is protected against the so called “MIG-in-the-Middle Attack” by encrypting the identify-friend-or-foe (IFF) system. As the number of aircraft identification events will undoubtedly increase in NGATS, the MIG-in-the-Middle Attack should be well understood by system architects in order to maintain or improve current levels of security. The scenario is best explained through a supposedly true story:

> Several MIGs had loitered in southern Angola, just north of the South African air defense belt, until a flight of SAAF (South African Air Force) Impala bombers raided a target in Angola. Then the MIGs turned sharply and flew openly through the SAAF’s air defenses, which sent IFF challenges. The MIGs relayed them to the Angolan air defense batteries, which transmitted them at a SAAF bomber; the responses were relayed back in real time to the MIGs, which retransmitted them and were allowed through (Anderson 2001).

Reflection attacks arising from mutual authentication further complicates the story but the current NATO mode XII system, which utilizes many different encrypted challenges, is sufficient for NGATS.

Elliptic Curve Cryptography (ECC) was selected by the FAA to secure the ATN. It is compatible with both SSL/TLS and IPSec. ECC is a public key cryptographic system based on the discrete logarithm problem. Elliptic curves are of the form:

$$y^2 = x^3 + ax + b$$

and takes shapes similar to the examples below.

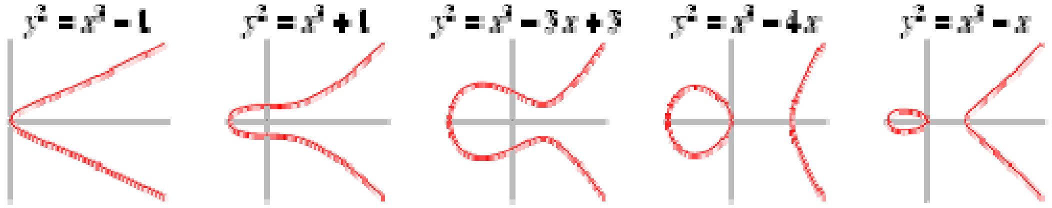

Figure 26. Elliptic Curves.
Image Source (Weisstein 2003)

In ECC, the curve defines the elements of the set over which the group is calculated and the operations between elements.

To construct an ECC implementation, define a graph of size *p* by *p* where *p* is a very large prime. This enables the construction of a field of integers modulo *p*, *Fp*, (all integers 0 to p-1). Now, construct an elliptic curve such that there exists some (*x*,*y*) where *x* and *y* are members of the prime field. The set of integer points on the curve forms a group. The basic operation for encrypting and decrypting messages is point multiplication: $Q = kP$.

Q: public key
P: base point (curve parameter)
k = private key (integer)

Suppose Alice and Bob want to communicate without Joseph comprehending their communications. They may use the following algorithm for key exchange.

1. Alice and Bob choose an elliptic curve and point, P. Neither the curve nor the point must be kept secret.
2. Alice's private key is k but she only sends kP to Bob.
3. Bob's private key is l but he only sends lP to Alice.
4. Both Alice and Bob can compute the symmetric key klP and begin sending secure messages.

Note: It is very difficult for Joseph to extract k or l from kP or lP

Joseph's dilemma is called the Discrete Logarithm Problem. Formally, the problem is defined in the following way:

Given points Q and P, find integer k such that $Q=kP$.

The problem of finding a log in a group on an elliptic curve over a prime field is computationally expensive for a large prime field. Brute force work of computing $2P$, $3P$, until reaching kP is one option. For example, suppose:

$k = 11$
Then $11P = 2(2(2P)) + 3P$ which requires 3 doubling and 3 addition operations.

The National Institute of Standards and Technology (NIST) defines the P192 curve which would require on average a doubling followed by 3 x 10^{57} additions. If all the computers on the planet were employed to solve this problem, it would take thousands of years on average. Although most applications use ECC for key exchange and a symmetric block cipher for "bulk encryption," it should be noted that other algorithms exist that permit ECC to be used to encrypt/decrypt messages as well as provide digital signatures (Certicom 2004).

APPENDIX V - Electronic Warfare

Information security within the civilian sector has historically isolated itself from the military field of electronic warfare (EW). However, the recent application of EW techniques such as DDoS on computer networks has led to the incorporation of EW issues into non-military security strategies. While information security is concerned with confidentiality, integrity, and availability, EW has similar priorities:

Electronic Warfare Priorities

1. Denial of service: jamming, mimicry, and physical attack
2. Deception: targeting automated system or people
3. Exploitation: obtaining operationally valuable information from the "enemy's" use of electronic systems

Table 16. Electronic Warfare.
Table Source (Anderson 2001)

Ultimately, EW is about control of the electromagnetic spectrum.

NGATS is concerned with electronic protection and electronic support. While protection is concerned primarily with resisting attack, electronic support seeks to "identify and locate sources of intentional and unintentional electromagnetic energy." The FAA should take the lead in electronic support activities, while all stakeholders in NGATS are responsible for electronic protection.

APPENDIX VI – Protocol Considerations

Weak Protocols

A variety of standard security protocols with well understood properties exist. Some should be used in NGATS while others should not. So called "Simple Authentication" and "Challenge and Response" protocols should not be used in NGATS. Simple Authentication is found in devices such as IR tokens, commonly found on cars that permit them to enter secure parking garages. They work by the token transmitting its name, *T*, as well as an encrypted value of *T* concatenated with *N*, the "nonce" (number used once). The key is *KT*. The freshness of the message is guaranteed by the nonce. Using standard protocol engineering language:

$$T \rightarrow G{:}T,(T,N)_{KT}$$

The gate, *G*, uses *T* to lookup *KT* and verifies that *T* emerges concatenated to a unique nonce. There are numerous known attacks on this protocol so it should not be used for high security environments such as NGATS.

Challenge and Response is a two-pass protocol found on remote keyless entry systems in cars. In this case the vehicle, *V*, sends a "random" number *N* to the key's receiver. The key then transmits back its identifier *T* along with the *N* encrypted under *K*.

$$E \rightarrow T{:}N$$

$$T \rightarrow E{:}(T,N)_K$$

The lack of true randomness in generating *N* makes this protocol inappropriate for high security systems.

Strong Protocols

The correct use of certificates, digital signatures, and message encryption is essential to securing the ATN. Certificates were first defined by (Kohnfelder 1978). They securely bind a user to a public key by signing it. Trusted certification authorities (CAs) issue digital certificates that include information such as the user's name and public key, certificate expiration date, algorithms, and other supporting data. Immediately, the issue of validating the issuer's certificate arises, but this is easily resolved by constructing a hierarchy of certificate signatures up to the level of an authority that can be trusted and the public key is known.

Digital signatures are a method whereby a sender can encode a message in such a way that the recipient can be sure of the sender's identity. This encoding is accomplished by the sender applying his private key to "encrypt" the message and the recipient applying the sender's public key to get the original message. Finally, encryption is used to ensure that third parties cannot read the message.

The correct application of certificates, signatures, and encryption can achieve four objectives:

1. Evidence that the message has not been altered
2. Evidence as to the identity of the sender of the message
3. Evidence as to the identity of the recipient of the message
4. Evidence that third parties have not read the message

Misapplications of certificates, signatures, and encryption as documented by Davis (Davis 2001), such as simply signing and then encrypting, permits surreptitious forwarding (Alice sends a message to Bob that he forwards to Joseph so Joseph thinks that Alice was communicating with him). If Alice includes both her name and Bob's name in the original plaintext message, this problem can be avoided. Also, the use of certificates can give Alice confidence that she has Bob’s correct public key in the first place. The following scenario provides a correct application of the technologies and satisfies the constraints derived in the earlier analysis:

Asymmetric Key Approach

If ATC wants to communicate with the aircraft, ATC should:

1) Obtain the aircraft’s certificate from the FAA.
2) Use the universally available public key from the Certification Authority to verify the aircraft’s public key.
3) Include ATC’s and the aircraft’s identifiers in the message.
4) Sign the plaintext message with its private key.
5) Encrypt the message with the aircraft’s public key.
6) Send the encrypted message to the aircraft.

When the aircraft receives the encrypted message, it should:

1) Obtain ATC’s certificate.
2) Use the universally available public key from the Certification Authority to verify ATC’s public key.
3) Use its private key to decrypt the message.
4) Use ATC’s public key obtained in step 2 to verify the signature and get the plaintext message.

Note:

a) The public keys need only be verified once. Then, many messages can be exchanged without having to re-verify the public keys.
b) If ECC is used for key exchange and a symmetric block cipher is used for bulk transfer, the Station-to-Station protocol should be used. It is an authenticated key agreement with key confirmation protocol, achieves perfect forward secrecy, and does not use time stamps. Further information on the correct use of key establishment schemes using discrete logarithm cryptography is available from NIST (Barker 2006).

Table 17. Secure Communication Protocol.

The robust scheme defined above also avoids the "Byzantine Failure" problem, which is a serious issue in a large ATC network. Anderson describes the general problem below:

> …*n* generals defending Byzantium, *t* of whom have been bribed by the Turks to cause as much confusions as possible in the command structure. The generals can pass oral message by courier, and the couriers are trustworthy. Each general can exchange confidential and authentic communications with each other general. What is the maximum number *t* of traitors that can be tolerated?
>
> The key observation is that, if we have only 3 generals, say Anthony, Basil, and Charalampos, and Anthony is a traitor, then he can tell Basil, "Let's attack," and Charalampos "Let's retreat." Basil can now say to Charalampos "Anthony says let's attack," but this doesn't let Charalampos conclude that Anthony is the traitor. It could just as easily be Basil; Anthony could have said "Let's retreat" to both of them, but Basil lied when he said "Anthony says let's attack."

Lamport, Shostack, and Peace have shown that the traitor(s) can be identified if and only if:

$$n \geq 3t + 1$$

(Lamport 1982)

Fortunately, the proper use of certificates, signatures, and encryption does not allow Anthony (if he is the traitor) to get away with sending contradictory messages to Basil and Charalampos.

REFERENCES

Anderson, R. (2001). *Security Engineering*, Wiley Computer Publishing, New York.

Apostolakis, G. (2000). "The Nuclear News Interview - Apostolakis: On PRA." Nuclear News, 27-31.

Apostolakis, G. E. (2004). "How Useful is Quantitative Risk Assessment?" *Risk Analysis*, 24(3), 515-520.

Arce M., D. G., Todd Sandler. (2005). "Counterrorism: A Game-Theoretic Analysis." *Journal of Conflict Resolution*, 49(2), 183-200.

Ashby, W. R. (1956). *An Introduction to Cybernetics*, Chapman and Hall, London.

Aumann, R. J., Sergiu Hart, Motty Perry. (2005). "Conditioning and the Sure-Thing Principle." Center for Rationality and Interactive Decision Theory, Hebrew University, Jerusalem.

Bach, J. (1994). "The Immaturity of CMM." *American Programmer*, September.

Banks, D. L., Steven Anderson. (2007). "Combining Game Theory and Risk Analysis in Counterterrorism: A Smallpox Example." Statistical Methods in Counterterrorism: Game Theory, Modeling, Syndromic Surveillance, and Biometric Authentication A. G. Wilson, Gregory D. Wilson, David H. Olwell, ed., Springer, New York.

Barker, E., Don Johnson, and Miles Smid. (2006). "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography." Special Publication 800-56A, NIST.

Barlas, S. (1996). "Anatomy of a Runaway: What Grounded the AAS." *IEEE Software*, 13(1), 104-106.

Bell, D., Leonard LaPadula. (1973). "Secure Computer Systems: Mathematical Foundations." MITRE Corporation.

Bier, V. M. (2005). "Game-Theoretic and Reliability Methods in Counter-Terrorism and Security." Modern Statistical and Mathematical Methods in Reliability: Series on Quality, Reliability and Engineering Statistics, World Scientific Publishing Co.

Bishop, M. (2005). *Introduction to Computer Security*, Pearson Education, Inc., Boston.

Blakey, J. H. (2006). "Navigating Toward the Future: Transitioning From Terrestrial Radio Navigation to Satellite Navigation and Airborne Surveillance." *IEEE Aerospace and Electronic Systems*, 21(5).

Britannica. (2007). "Weber's Law." Encyclopædia Britannica.

Certicom. (2004). "An Elliptic Curve Cryptography (ECC) Primer." Certicom, Herndon, VA.

Checkland, P. (1981). *Systems Thinking, Systems Practice*, John Wiley & Sons, New York.

Clark, D. (2006). "Personal Communication on Security." J. Laracy, ed., Cambridge.

Clark, D., David Wilson. (1987). "A Comparison of Commercial and Military Security Policies." IEEE Symposium on Security and Privacy, Oakland, CA, 184-194.

Davis, D. (2001). "Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML ", Cambridge.

DoD. (2006). "Operations Security." Joint Chiefs of Staff, Defense Technical Information Center.

Dulac, N. (2007a). "A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems," MIT, Cambridge.

Dulac, N., Brandon D. Owens, Nancy G. Leveson (2007b). "Modelling Risk Management in the Development of Space Exploration Systems." Proceedings of the 2nd Annual International Association for the Advancement of Space Safety (IAASS) Conference, Chicago, IL.

Dulac, N., et al. (2007c). "Demonstration of a Powerful New Dynamic Approach to Risk Analysis for NASA's Constellation Program." MIT Complex Systems Research Laboratory Report, Cambridge.

Dzakovic, B. (2003). "Statement of Bogdan Dzakovic to the National Commission on Terrorist Attacks Upon the United States."

Eliot, J. (1998). "System Engineering and Safety-related Systems." *Safety Systems*(7(3)), 14-16.

EPIC. (2006). "Secure Flight." Electronic Privacy Information Center, http://www.epic.org/privacy/airtravel/secureflight.html.

FAA. (2004a). "Aerospace Forecasts: FY 2004-2015." FAA.

FAA. (2004b). "Future Airport Capacity Task - Final Report." FAA.

Feynman, R. P. (1986). "Rogers Commission Report: Appendix F - Personal observations on the reliability of the Shuttle." NASA.

Frey, B. S., S. Luechinger. (2003). "How to Fight Terrorism: Alternatives to Deterrence." *Defense and Peace Economics*, 14, 237-249.

Fricker, R. D. (2005). "Game Theory in an Age of Terrorism: How can Statisticians Contribute?" Statistical Methods in Counterterrorism: Game Theory, Modeling, Syndromic Surveillance, and Biometric Authentication A. G. Wilson, Gregory D. Wilson, David H. Olwell, ed., Springer.

Gelernter, D. (2005). "The Law of Loopholes in Action." Los Angeles Times, LA.

Gharajedaghi, J. (1999). *Systems Thinking: Managing Chaos and Complexity*, Butterworth Heinemann, Boston.

Gharajedaghi, J. (2004). "A Holistic Language of Interaction And Design: Seeing Through Chaos and Understanding Complexities." *Ackoff Collaboratory for Advancement of the Systems Approach (ACASA).* .

Gonzalez, J. J., et al. (2005). "Helping Prevent Information Security Risks in the Transition to Integrated Operations." *Telektronikk*, 101(1), 29-37.

Graham, S., Girish Baliga, and P.R. Kumar. "Issues in the convergence of control with communication and computing: Proliferation, architecture, design, services, and middleware." *43rd IEEE Conference on Decision and Control* Atlantis.

Greenspan, R., Joseph R. Laracy, and Adnan Zaman. (2004). "Real-time Immersive Network Simulation Environment (RINSE)." Software Architecture, UIUC, Urbana.

Haimes, Y. Y., Barry M. Horowitz. (2004). "Modeling Interdependent Infrastructures for Sustainable Counterterrorism." *Journal of Infrastructure Systems*, June, 33-42.

Hasselbring, W., Ralf Reussner. (2006). "Toward Trustworthy Software Systems." *Computer*(April 2006).

Herrmann, D. S. (2002). *Security Engineering and Information Assurance*, Auerbach Publications, New York.

JPDO. (2004). "Next Generation Air Transportation System Integrated Plan." Joint Planning and Development Office.

Kirby, M. W. (2003). "The intellectual journey of Russell Ackoff: from OR apostle to OR apostate." *Journal of the Operational Research Society*, 54(11), 1127-1140.

Kohnfelder, L. (1978). "Towards a Practical Public-key Cryptosystem," MIT, Cambridge.

Krenzke, T. (2006). "Ant Colony Optimization for Agile Motion Planning," MIT, Cambridge.

Lamport, L., R. Shostack, M. Peace. (1982). "The Byzantine Generals' Problem." *ACM Transactions on Programming Languages and Systems*, 4(3), 382-401.

Laracy, J. (2006). "A Systems Theoretic Accident Model Applied to Biodefense." *Defense and Security Analysis*, 22(3), 301-310.

Laracy, J. (2007a). "Addressing System Boundary Issues in Complex Socio-Technical Systems." Proceedings of the 5th Annual Conference on Systems Engineering Research, Hoboken, NJ.

Laracy, J. (2007b). "Dynamical Models: System Dynamics and Agents." ESD Generals Study Group Presentation.

Leveson, N. (2002). *System Safety Engineering: Back to the Future*, Cambridge.

Leveson, N. (2003). "A New Approach to Hazard Analysis for Complex Systems." International Conference of the System Safety Society, Ottawa.

Leveson, N. (2004). "A New Accident Model for Engineering Safer Systems." *Safety Science*, 42(4), 21.

Leveson, N., Nicolas Dulac, Betty Barrett, John Carroll, Joel Cutcher-Gershenfeld, Stephen Friedenthal. (2005). "Risk Analysis of NASA Independent Technical Authority." MIT, Cambridge.

Leveson, N. G. (1995). *Safeware*, Addison-Wesley Publishing Co., Reading.

Martinez-Moyano, I. J., Eliot Rich, Stephen Conrad, David F. Anderson, Thomas R. Stewart. (2005). "A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach." Center for Policy Research, Albany, NY.

Menezes, A. J., Paul C. van Oorschot, and Scott A. Vanstone. (1997). *Handbook of Applied Cryptography*, CRC Press, Inc., Boca Raton.

Michaud, D., George E. Apostolakis. (2006). "Methodology for Ranking the Elements of Water-Supply Networks." *Journal of Infrastructure Systems*, 12(4), 230-242.

Midkiff, A. H., R. Hansman, Tom Reynolds. (2004). "Air Carrier Flight Operations." MIT.

NCTAUS. (2004a). "9/11 Commission Report." National Commission on Terrorist Attacks Upon the United States.

NCTAUS. (2004b). "The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3." National Commission on Terrorist Attacks Upon the United States

Parker, D. B. (2007). "Risks of Risk-Based Security." *Communications of the ACM*, 50(3).

Pate-Cornel, E., Seth Guikema. (2002). "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures." *Military Operations Research*, 7(4), 5-23.

Patterson, S. A., G.E. Apostolakis. (2006). "Identification of Critical Locations Across Multiple Infrastructures for Terrorist Actions." *Reliablity Engineering and System Safety*, October.

Rae, A., Colin Fidge, and Luke Wildman. (2006). "Fault Evaluation for Security-Critical Communications Devices." *Computer*(May 2006), 61-68.

Richmond, B. (1993). "Systems thinking: critical thinking skills for the 1990s and beyond." *System Dynamics Review*, 9(2), 113-133.

RMS. (2003). "Managing Terrorism Risk." Risk Management Solutions, Inc.

Royce, R. "Rolls Royce Forecast." *NBAA Convention*, 22.

Sandler, T., Daniel G. Arce M. (2003). "Terrorism and Game Theory." *Simulation and Gaming*, 34(3), 317-337.

Savage, L. J. (1954). *The Foundations of Statistics*, Wiley, New York.

Schneider, W. (2003). "The Role and Status of DoD Red Teaming Activities." Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September.

Scottberg, E. (2006). "NASA Says Shuttle Risk Overstated; Yet Some Risk Unavoidable " Popular Mechanics.

Senge, P. (2006). *The Fifth Discipline*, DoubleDay, New York.

Shah, D. (2006). "Quantitative Foundations of Engineering Systems Lecture Notes." MIT, Cambridge.

Stamatelatos, M. G. (2002). "New Thrust for PRA at NASA." NASA, ed.

Sterman, J. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin McGraw-Hill, Boston.

Sterman, J. (2002). "All models are wrong: reflections on becoming a systems scientist." *System Dynamics*
Review, 18(4), 501-531.

Swenson, H., Richard Barhydt, Michael Landis. (2006). "Next Generation Air Transportation System Air Traffic Management -Airspace Project
", NASA.

Thanthry, N., M.S. Ali, and R. Pendse. (2006). "Security, Internet Connectivity, and Aircraft Data Networks." *IEEE Aerospace and Electronic Systems*, 21(5), 12-16.

Tversky, A., Daniel Kahneman. (1974). "Judgment under Uncertainty: Heuristics and Biases." *Science*, 185, 1124-1131.

USC. (2005). "Center for Risk and Economic Analysis of Terrorism Events - Final Report." University of Southern California, Los Angeles, CA.

Von Neumann, J., O. Morgenstern. (1953). *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, NJ.

Weinberg, G. (1975). *An Introduction to General Systems Thinking*, John Wiley.

Weisstein, E. W. (2003). "Elliptic Curves." Mathworld.

Wilkening, D. (1998). "A Simple Model for Calculating Ballistic Missile Defense Effectiveness." Center for International Security and Cooperation.

Woo, G. (2002). "Quantitative Terrorism Risk Assessment." Risk Management Solutions - Technical Report.

Zipkin, D. (2005). "Using STAMP to Understand Recent Increases in Malicious Software Activity," MIT, Cambridge.