Airport Security Complexity : Problems with the Information System Components

Erman Coskun and Jessica Hoey
Sakarya University Business Department, Sakarya, Turkey
and
LeMoyne College Business Department, Syracuse, NY USA
ermanc@sakarya.edu.tr or coskune@lemoyne.edu

ABSTRACT
Airport security is a very relevant, diverse, and complex system in any country. September 11th made this issue an increasing concern for almost every country in the world. Prior to September 11th the media, watchdog groups, and commissions established by the United States Congress, were adamant that airport security had major flaws. Currently many countries are revamping their airport security systems. The U.S. and other governments are implementing many new systems and procedures. There are numerous potential pitfalls with this implementation process and these new systems will have impacts on the public. For example, these systems could reduce freedom, still be flawed, and affect the economy. The primary intents of this paper are to classify airport security as a complex large-scale safety-critical system, to discuss what make airports so complex, describe the information systems that are involved with such systems, and discuss the impacts on the people involved.

Keywords
Airport security, complexity, information systems

INTRODUCTION
Airports are very complex large-scale safety-critical systems. They are complex because there are huge number of subsystems, people, technology, and interest groups involved. Some of these are tightly coupled subsystems which means they rely on each other heavily and a small flaw in one system may have impact on some other systems. They are safety-critical because an incident or accident in these systems may cause loss of human life and big economic losses.

The information and data that flows in this system must be accurate, intelligent, quick, and easy to understand to make decisions. Security is key and crucial for the information system to accomplish the tasks it was designed for. Airport systems has to be tested extensively, with massive amounts of money and time invested in it. All components and subsystems must be coordinated and work together to prevent an accident or incident.

Placing blame after a devastating tragedy is a difficult and long process. Yet, an investigation must be conducted in order to fix and prevent similar disasters. So, we include some testimonies and opinions of experts abut why September 11 occurred and what went wrong. Based on analyses of these opinions, we will discuss the role of information systems on airport security.

Mary Schiavio, former Assistant U.S. Attorney and current Professor of Aviation at Ohio State University, is trying to speak out about the problems to make sure September 11th does not happen again. Schiavio felt that no one listened to warnings about terrorism. She specifically cites the FAA as the main factor of September 11th, "I don't know how many tragedies and disasters we've witnessed; this is not the first. The FAA was one of the causal factors cited as causing Pan Am 103. Now clearly, the agency is a causal factor here, no matter how you look at it. Either it is everything from bad screening to a bad policy, to a ridiculous system, where we have a thousand different security plans in place. Time and again, when I was working on…. cases, the FAA administrator at the time wanted it stopped because it costs the airlines too much money. I take it out on the government. In the end, the airlines do what they are supposed to. Because they are private business, they are supposed to try and get away with everything they can to save the bottom line, to make their investors on Wall Street happy. That is how this game works" (Fish, 2002). She suggests that the problems with the large-scale safety-critical systems are a result of the, "U.S.'s unwillingness to pay the price or take the time to improve them. Over the last decade airport security steadily deteriorated as the recommendation of two congressional commissions, followed by new legislation, were simply ignored". Schiavio (Fish, 2002) has also said, "They (FAA) had more public relations persons than security personnel.".
Jim Mckenna, former director of the Aviation Safety Alliance said (Saparito, 2002), "Everyone knew the system was broken." Not many in the aviation industry were completely surprised when September 11th occurred. The extent of the massive destruction and loss of life was startling, but the flaws in security system that lead to the devastation wasn't.

The information flow between agencies was not processed correctly or passed on to the correct agents or people. Repeated warnings from some agencies were ignored and officials failed to alert the proper authorities, such as the FAA, about the looming catastrophe. The FAA has been accused of causing disasters in the past. For example, as Schiavio pointed out, in 1988 the FAA did not alert the pilots of the Pan Am Flight 103 of a potential problem with suspected terrorism on that specific flight (Daniel, 2002). The FAA claims it did not want to frighten the pilots. The plane exploded from a bomb in a passenger bag aboard the plane. This example shows how the FAA, when provided information from the CIA or FBI, would ignore specific threats. The CIA's watch list had two of the September 11th hijacker's names on it, but the airlines never saw this information (Fish, 2002).

Passenger complaints about suspicious passenger activity were ignored. The FAA complaint system was called The Aviation Safety Reporting System (ASRS) (Johnson, 2002). Complaints and concerns about safety could be submitted confidentially or anonymously. ASRS relied on software tools to support the administration of their system and on ad hoc applications of conventional database technology. This is inadequate for large-scale reporting schemes (Johnson, 2002). This complaint system in place was so backed up the warning would not have reached anyone for several days or even weeks. This failure in information flow from several systems and people caused an unimaginable disaster.

Plus, the airlines were having economic problems and were cutting costs everywhere including security. The security companies hired by the airlines were failing to run background checks on their employees because of the high costs. These companies employed 90% of employees at airports (Rhea, 2002). The security personnel at airports were poorly paid, worked long monotonous shifts, and received very little training (GAO, 2001). The airlines may have actually encouraged these companies to cut costs anyway they could or they would lose their contracts. The General Accounting Office found in 2000 that the starting salary for screeners at 14 of the nations 18 largest airports was $6 dollars or less (GAO, 2001). An even more disturbing finding was that the rate of annual turnover of screeners averaged 126% at 19 of the largest airports (GAO, 2001). As a possible result of the poor pay and turn over rates, security screeners missed 20% of the banned objects located on passengers or contained in there carry-on luggage (GAO,2001). Tables 1, 2, and 3 provide more information about these rates.

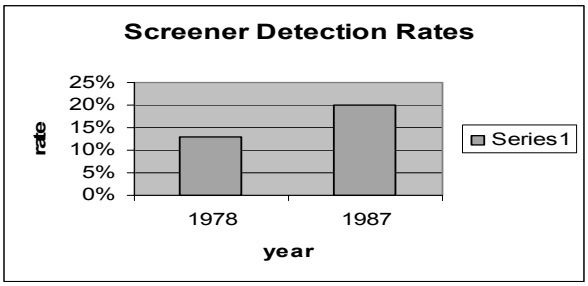

Table 1 Screener Detection Rates (GAO,2001)

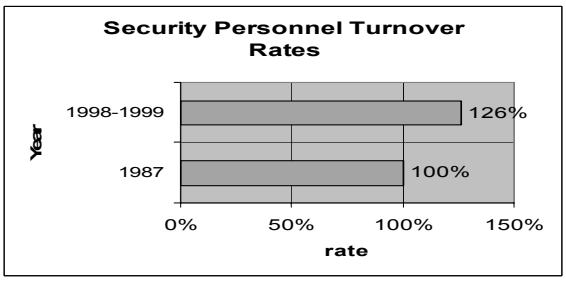

Table 2 Security Personnel Turnover (GAO, 2001**)**

When we analyze all these information, we can classify the problematic areas of any airport system as:

1. Communication and Coordination among subsystems, people, and all involved parties: This seems that it was the biggest problem for the occurrence of September 11th.
2. People: The problems with screener turnover rate, low salaries, and inadequate level of training.
3. Inadequate Hardware or Software: As it will be discussed in coming section, there are new hardware and software systems which could help with integration, intelligence, and communication.
4. Databases: Although there were available data, because of disintegrated systems and not using the latest database technology it was hard to pull out the right information from the databases.
5. Cost: Since the airline industry was in crisis, they always considered the cost and this resulted with vulnerable systems and security measures

Whatever people, agencies, or experts that are being blamed for September 11th, it is clear that almost the entire airline security system was weak and failed on several levels. The information systems involved with many agencies failed. It is apparent that this large-scale safety-critical system needs time, attention, and resources.

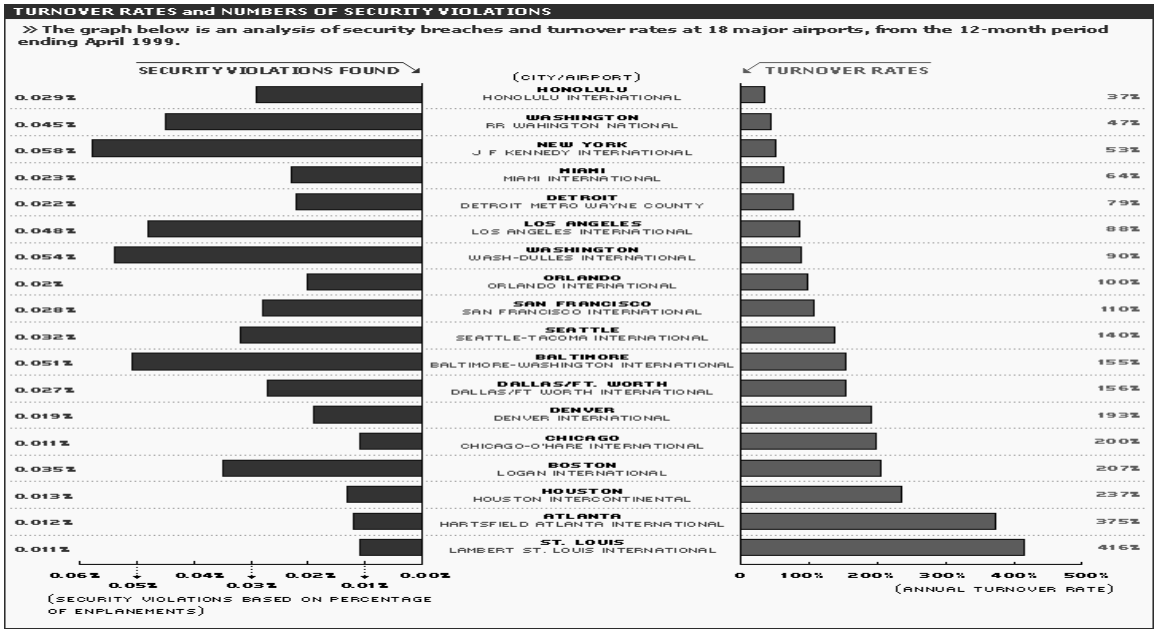

Table 3 Airport Turnover (CNN 2000)

AIRPORT EMERGENCY RESPONSE SYSTEM DEVELOPMENT

Emergency response systems are mostly rely on hardware, software and especially on human operators and decision makers. Since the hardware product development techniques and technologies have been improving steadily by years, we do not have relatively big problems with the hardware components and we are just listing some of crucial hardware components. But this is not the case with the software and people components.

Hardware Technologies Available for Airport Security Systems and Problems with Hardware:

The obvious hardware related problems are cost of them, integration of different devices, and cost of hiring well qualified people to use and utilize these hardware devices. Another problem is testing these newly developed hardware devices for all different situations. Especially after September 11th a lot of new hardware devices were developed but they could not be tested fully because of time restrictions. Some of new hardware technologies include

Satellite Imagery: Satellite Imagery is now being considered crucial to the safety of airports. Not only is important to provide security to areas around the airport, but it will help in the event of a terrorist attack or accident.

Scanners: There are many different functions and types of scanners. These scanners use software and hardware to serve their purposes. Some of them are: Body Scanners, Smelling and Scanning Devices, Baggage Scanners

Biometrics: Biometrics is a technology that uses characteristics to identify individuals.

Problems with Software Development:

Software development is very diverse and complicated with large-scale safety-critical systems. Typically, development is very expensive. Money is sometimes more important than safety, in the development process. Therefore, the reliance on software in such systems could be a problem. In addition, the developed software may be at risk when introduced to different types of hardware. New and developing technology should be introduced cautiously because of the uncertainty involved (Murray, 2002). The main goal in safety-critical software development is to decrease the risk of failures and at the same time reducing all other risks. These other risks, in terms of large-scale safety critical systems, are the three impact areas. Since you cannot really determine the reliability of software, because errors are more unpredictable and random, it is important to develop simple back-up systems for airport security systems.

Ethics are very important to software development of large-scale safety-critical systems. There are seven undesirable practices have been identified by Jonathan Bowen, to ensure success with this type of system software (Bowen, 2000). The first is *epideictic*, which is not using techniques to satisfy the concerns of management or be influenced by peer-pressure in developing large-scale safety-critical software. Formal methods should be stressed by everyone involved. The second term is hyperbole. *Hyperbole* is following exaggerated methods and tools because the benefits may be inflated. *Pistic* involves tools as well. Relying on tools and becoming to trusting of them may reduce the reliance of human reasoning power. The reasoning power of humans should be relied on in addition to tools. *Oligarchy* is having an expert on call at all times and not jumping to replace existing software because of some new methods. *Ephemeral* is properly testing the software in its old and new environment. *Epexegesis* urges that you not over document. You do not need to record unnecessary details. *Maiandros* is taking too long to develop software. Estimating the development time

of software is very hard to do, but taking too much time can hurt the project. Ethics are very important and have to be stressed to personnel and other key figures involved in order to develop such complex systems.

Problems with People:
The personnel who work on these systems have to be among the very best, unafraid to speak out because of potential consequences, and use best-practices. Not only are the people developing this type of software important, but the people who use it as well. Interfaces have to meet stakeholders and users criteria and function properly. People in all levels must be supported by hardware, software, databases, and communication technology provided by information systems. Decision makers' decisions should be based on detailed information coming from different agencies and the systems should analyze raw data and produce intelligent information by using techniques such as artificial intelligence, data mining techniques, intelligent agents, neural networks. User interfaces for these systems should be designed to address most common problems with interfaces and usability.

Some other people related problems can be listed as violation of privacy of individuals, violation of equal treatment among individuals, discomfort of the check in process. However, for better security there must be some sacrificing . The important point is balancing these sensitive issues correctly.

Problem with the Complexity:
Complexities cause unpredictability, something safety-critical systems do not want. The Y2K problem of the late 1990's is an example of unpredictability. No one knew what would happen to systems when the clocks changed years. Testing as mentioned, is very important, but it is not a guarantee that it can be predicted what the software will do in every circumstance. Even extensive testing is not one hundred percent. Misleading data may say that everything is normal or fine when in reality everything is not normal or fine. Watch-dog modes are advised to eliminate failures (Murphy 2000). However, it is still important to have software in which it is easy to move from an unsafe state to a safe state, but difficult to move from a safe to an unsafe state. Having the proper watchdog mode can decrease the risk of someone causing havoc on the system. Users of large-scale safety-critical systems are incredibly important. They need to be able to tell what the system is actually doing.

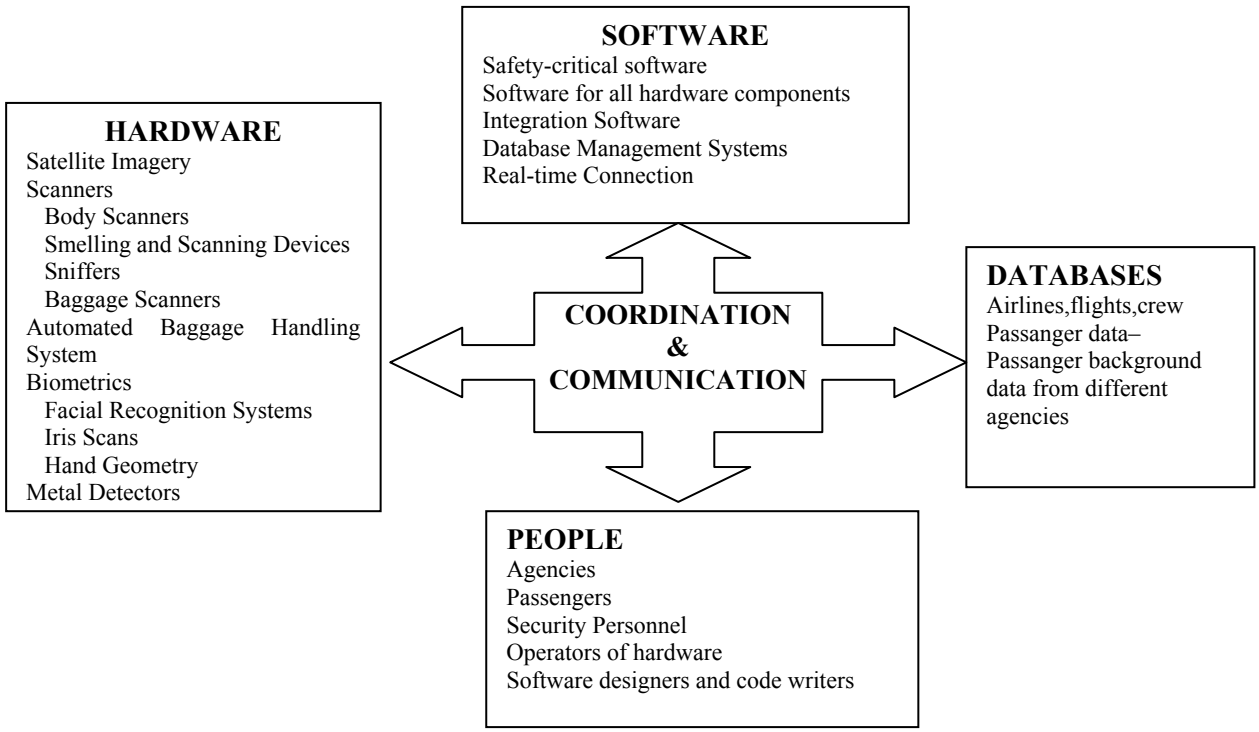

Figure 1. Airport Security and Required Information System Components

Michael Myers suggested an interpretive approach called critical hermeneutics as one way of conducting research into IS implementation (Bussen, Myers 1997). He argued that critical hermeneutics provides a richer more integrative view of IS implementation, with the researcher critically evaluating the totality of understanding a given situation (Bussen, Myers

1997). This approach "should focus on the broader scale and historical forces surrounding the implementation of any particular system."(Bussen, Myers 1997). These forces could include the economy and management. Other complexity research such as Coskun and Grabowski, 2004; Turoff, et al. 2004 can also help with design and implementation of Airport Security Systems.

SOLUTION APPOACH

After determining and describing the components which make airport security a complex issue, in this section we propose some solutions from the information systems view. For these solutions, we will assume that an airport already bought and implemented all technology related devices such as screeners, detectors, and other hardware components mentioned in hardware section. This is the case with most US airports especially since September 2001. But, for other countries, this may not be the case yet. For them the first step should be updating their technology.

If an airport is utilizing new technology and the problem is not technology per se, managing all these complex relationships among the components and making all components communicate with each other when and how it is necessary would be the biggest problem, So the solution is providing better communication and connectivity.

Airport security systems cannot rely solely on technology. The system has to rely on human knowledge, abilities, and other resources as well. Therefore, employees and passengers are a critical part of the system. Increased level of communication and connectivity will help to humans involved with airports. Since the technology is being used heavily, human judgment or human errors are making airport security weak. As mentioned in previous sections, humans are key component in airport security. They are checking baggage, screening passengers and employees and humans, controlling the screening devices, checking passenger information and documents, managing airports, and deciding to evacuate airports in case of an emergency. For all these activities, they must make timely and accurate decisions. Thus, information systems must be used to support human decision making. We need decision support systems. And, because of the complexity of airport security, we need integrated and intelligent decision support systems. With this, all departmental systems can be connected with others and information can be gathered from the subsystem where it stays. We see the application of this kind of systems in business world. ERP, MRP, Executive Support Systems are all can be considered as a model for this kind of intelligent integrated information systems. If all systems are integrated and made intelligent communication and coordination problem would be solved. For example, if the agent on ticket counter has some suspicion on a passenger who is checking in, he or she can notify his/her supervisor by entering some code to a field on the screen. Then, submission of this information can trigger an alert on supervisor's screen. The supervisor can use his/her computer to make a detailed background check (by connecting to databases of legal agencies). Once the results are in, the supervisor can notify security agents and or airport management to handle the situation. This is just a very simple example. However, it shows us that integrated systems are the solution. It also indicates that we need to support human decisions means our systems should be intelligent. In our example, if our system does not support the ticket counter agent's decision, there might be a lot of false alarms and the system can become a very inefficient one.

Finally, airports should also try to start to be standardized with uniform functions, procedures, operations, and environment. Implementing a large system that has a standardized environment may have less chance of failure and unpredictability, rather than in diverse structures that have to be modified, altered, and tested extensively to be workable. If every airport had the same components throughout it would be easier to detect weaknesses and test for weaknesses more efficiently. Currently there are standards for certain safety procedures at airports, but not for how to conduct many of these procedures. Decreasing failures and unpredictability can be reduced if standardization is implemented through utilization of information systems.

CONCLUSIONS

Airports are complex in nature and airport security must consider all aspects of complex airport systems. In this study, we analyzed the causes of September 11th events, determined the system components who failed one way or other. Then, we discussed what could be done during information system developments for airports. This is a very first phase of a research project and we will include more details for the final version of this paper and for the conference presentation.

REFERENCES

1. Bowen, Jonathan (2000) "The Ethics of Safety-Critical Systems;" *Association for Computing Machinery,* Communicator of the ACM, New York, April 2000.
2. Bussen, Wendy; Myers Michael, D; (1997), "Executive Information System Failure: A New Zealand Case Study;" *Journal of Information Technology*.
3. CNN (2000) Taken from CNN.com; "Airport Turnover;" http://www.cnn.com/SPECIALS/2001/trade.center/flight.risk/airport.turnover.html' GAO Aviation Security Report, June 2000.

4. Coskun, E. Grabowsk,. M. (2004) 'Impacts of User Interface Complexity on User Acceptance in Safety-Critical Systems' Proceedings of AMCIS 2004 New York USA
5. Daniel, J.H. III (2002) "Reform in Airport Security: Panic or Precaution?" *Mercer Law Review*, Walter F. George School of Law, Westlaw, summer, 2002.
6. Fish, Mike (2002) "CNN-In-Depth Specials; Part One: The System;" Date not available. [taken from WWW on November 15, 2002 http://www.cnn.cllpolitics.printthis.clickabliity.com]
7. "GAO Aviation Security (2001) Vulnerabilities in and Alternatives for, Preboard Screening Security Operations." GAO-01-1171T, September 25, 2001. [taken from WWW on March 21, 2003 http://www.gao.gov/airptsec.html]
8. Johnson, C. (2002) "Software Tools to Support Incident Reporting for Safety-Critical Systems;" *Safety Science*, Elsevier Science Ltd., V 40, I 9, p765-780, December, 2002.
9. Murphy, Niall (2000) "Lock up your Software;" *Embedded Systems Programming*, San Francisco, December 2000.
10. Murray, Charles J. (2002) "Safety-Critical Software Rolls*;" Electronic Engineering Times*, Manhasset, May 20, 2002.
11. Rhea, Jamie L. (2002) "Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats;" *DePaul Law Review*, Westlaw, spring 2002.
12. Turoff, M., Chumer, M., Van de Walle, B., Yao, X., "The Design of a Dynamic Emergency Response Management Information System (DERMIS)", *JITTA: Journal of Information Technology Theory and Application* Volume 5, No.4, 2004.
13. Saporito, Bill; Donnelly, Sally B. (2002) "Air Travel;" *Time - Person of the Year*, December 31, 2001 – January 7, 2002.