An Introduction in the Risk Modeling of Aviation Security Systems

CATALIN CIOACA, MIRCEA BOSCOIANU
Faculty of Aeronautic Management
“Henri Coandă” Air Force Academy
160 Mihai Viteazul Street, Braşov
ROMANIA
catalin_cioaca@yahoo.com http://www.afahc.ro

Abstract: The paper defines concepts which are part of the same process of achieving aviation safety, although different in scope and responsibility. While the focus of this paper is the evaluation and mitigation of security risks in the aviation domain, the risk evaluation and mitigation concepts discussed here may be applicable to risk evaluation process carried out in the broader context of homeland security policy. Much of the current aviation security policy debate has been the product of different views regarding the extent to which further mitigation and risk reduction is needed in the areas where there are different opinions regarding the degree and nature of security risk.

Decision making problems in risk analysis often involve extreme events, where empirical data are usually either sparse or lacking. With sparse data, important parameters and quantities for risk and safety analyses may not be estimated and tested within an acceptable level of significance. This paper applies Bayesian Networks (BN) to reduce the estimation variance and thus build relatively robust models for extreme event data through borrowing strength from different but related systems or subsystems. Based on this application, this paper realizes a multi-dimensional approach of complex systems. Case studies with both simulated and real data demonstrate the effectiveness of BN in risk-based aviation system analysis.

Key-words: risk analysis, aviation system, Bayesian networks, extreme events, security

1 Introduction

Traditionally, the reliability and safety of complex transport, nuclear and aviation systems has been assured through the use of a number of approximate techniques including Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Monte Carlo simulation and Markov modelling. Each of these methods uses different approximate algorithms to model different aspects of the problem. It turns out that in all cases these can either be replaced or subsumed by BN methods.

Security risk is generally regarded as a function of the nature of the threat, the vulnerability to attack inherent in a given system, and the consequences for a particular attack scenario.

The aviation security system is a complex system of systems that has evolved since 9/11 to meet the objective of reducing the probability or likelihood of a successful terrorist attack. Threats must be viewed with regard to terrorist objectives and motives as well as possible terrorist tactics.

There are three origins of sources of threats to the air domain: terrorist groups, hostile-nation states, and criminals [1].

To analize risk there is a compelling requirement for an integrated approach. The aviation system needs to have the architecture to support and address ever-evolving requirements into the long-term.

While terrorists groups appear to have a specific interest in continuing to target the aviation system, defending and protecting this system and its assets against asymmetric threats is complex and resources intensive because terrorist adversaries behave in ways that can be difficult to predict and difficult to detect.

The management of risk is therefore a key issue for airliners, and there is now an increasing awareness towards taking risk analysis into account in the decision making context [2].

The source of risk can be decomposed into functional, spatial, temporal/planning and user aspects. In hierarchical perspective risks are subdivided into life-critical and mission-critical.

Extreme events are not only severe, but outside the classic experience of the system. That could be equipped with particular characteristics (low frequency, high impact). These events are generated by complex non-linear phenomena with synergistic effects. Also, hazard and operability studies (HAZOPS) are inductive and need customized procedures [3].

Bayesian networks, a risk modeling and analysis approach applied for various types of analyses and
purposes, provides not only quantified and auditable risk assessment, it also enables integration of multiple forms of data (financial, subjective) and can combine them to perform a powerful “what-if” analysis [4].

2. Basic aspects of the risk modeling dimensions

2.1 Introduction in the risk model for aviation system

This scientific approach defines three primary categories of threats against the aviation domain: aircraft, aviation infrastructure and exploitation of air cargo. A variety of tactics may be used to attack these targets, but for this model, I have just taken into account hijackings, bombings, biological weapons, and MANPADS (shoulder-fired guided missiles). To complete the model three solutions were identified to mitigate the threat: surveillance technologies, passenger and baggage screening and aircraft countermeasures. A synopsis of the relationships between threat origins, aviation targets and dimensions of resilient aviation system is presented in Figure 1.

a. Aircraft

Aircraft threats may be directed at aircraft or may involve the use of aircraft to attack other targets. Terrorists have perceived the hijacking and bombing attacks against such aircraft have significant potential to cause catastrophic damage and mass casualties the aviation system. Both passengers airliners and all-cargo aircraft could be at risk from possible attacks using the weapons as shown previously. Also, small aircraft, such as business jets and helicopters, even if they appear to be relatively unattractive targets because they carry few passengers, can be used by terrorists to destroy ground targets, especially critical assets and infrastructure.

b. Aviation infrastructure

The aviation infrastructure includes airports and air navigation facilities. Even though threats to aviation infrastructure are relatively few, there is a wide variety of potential threats. Terrorists may attack passenger terminal buildings with explosives, as was attempted in several historical incidents or man portable air defence systems (MANPADS). These type of attacks are less likely to materialize because they do not offer the opportunity to target large number of people and have a limited psychological impact.

c. Air cargo

The large scale, diversity and complexity of the air cargo industry make it potentially vulnerable to exploitation by terrorists. Post 9/11 actions to enhance air cargo security have been effective in reducing the threats of suicide hijacking and explosives, but this system is not yet immune to exploitation. In addition to possible threats to all cargo aircraft noted above, the threat of terrorist infiltration of air cargo handling operations and facilities remains a threat that could lead to exploitation of the air cargo system as a mean of conveyance for terrorist operatives and conventional weapons.

d. MANPADs

MANPADs were initially designed for use by individuals or small teams against helicopters or other small aircraft. Based on their method for detecting and engaging targets, the MANPADs are classified into three categories: command line-of-sight (CLOS) systems, laser beam riders and IR-guided missiles. As general capabilities of these systems it’s known that they are portable, reliable, inexpensive and fairly easy to use.

The threats posed by shoulder/fired missiles is certainly a credible threat from at least three reasons: terrorist posses these weapons; civilian aircraft remains quite vulnerable to an attack from these types of weapons; even if commercial aircraft are likely to survive such an attack, it may be extremely difficult to stop the decline in passenger traffic after a successful attack.

Even though the MANPADs attacks against airliners have been relatively small in number, the commercial aircrafts are especially vulnerable given the following situations: there are not maneuverable enough to evade a missile attack; they fly within the range of shoulder/fired weapons during takeoff and landing; presently they haven’t special countermeasures.

d. Hijacking

The September 11 attack showed how capable terrorist are in carrying out attacks by hijacking an airplane and this also showed that they can be able to use other aviation forms of attacks [5]. This technique of attack is an imminent threat to the aviation domain and has forced airport security authorities to focus on ensuring the procedures that screen the passenger.

e. Bombings

Terrorists have frequently used explosive devices as one of their most common weapons. In aviation system, this type of weapons have been used to damage and destroy the aviation infrastructure especially passenger terminal buildings or aviation
jet fuel storage facilities, where thousands of people could be injured and killed, the aviation system on a large scale could be disrupted, and also with a severe psychological impact [6].

The bombs are relatively easily to build, the materials needed for it can be found in many places and not very expensive, they are highly portable and also easily detonated from remote location or by suicide bombers [7].

The bombs would have been powerful enough to create an explosive decompression aboard an aircraft causing the plane to disintegrate while flying at high altitude over the ocean. The suicide bombers reportedly planned to target nine commercial airliners and would have likely killed between 2,500 and 5,000 people if successful.

Since the 1960s there are identified a whopping 86 cases related to airliner bombings, 53 of them resulting in deaths [8].

2.2. Build the Bayesian network for asymmetric extreme events in aviation

After identifying variables to be included in the model, to model variables in an integrated design is needed to fully understand the risk. Also, the next step is assigning numerical values to each of the parameters included in the model.

In aviation security system, when analyzing intangible risks, it is hard to find statistical data that can support the choice of data to use in the modeling. Also, it is known that security aviation risk is determined as a function of three variables: threat, consequence and vulnerability. Having classified the basic terms, we can express the risk as follows:

\[ R_{at} = T_{at} \times C_a \times V_{at} \]  

(1)

Subscript \( t \) relates to the type of threat (MANPADS, hijacking, bomb or biological) and subscript \( a \) is the aviation infrastructure affected by threat \( t \). The consequence refers to the potential lives lost regarding threat \( t \) in area \( a \). The vulnerability in equation 1 has to represent the average vulnerability of a single aviation system \( a \) in the context of a single threat \( t \).

Aviation risk management requires risk “dimensioning”, and risk measuring should take into account not only the expected physical damages, victims and economic equivalent loss, but also social, organizational and institutional factors. Most existing indices and evaluation techniques do not adequately express risk and are not based on a holistic approach.

The disaster risk management indicators can be used effectively taking into account the specific of extreme asymmetric event from aviation system.

The Attack Deficit Index (ADI) captures the relationship between resources required to cover the losses by the maximum considered event (MCE), and both public and private sector’s economic resilience.

\[ \text{ADI} = \frac{\text{MCE}_{loss}}{\text{Economic Resilience}} \]  

(2)
Potential losses are calculated by using a model that takes into account different events, calculated in probabilistic form according to historical data and the actual physical vulnerability of the elements exposed to such attacks.

Economic resilience represents internal and external resources that are available (to the Government and private air transporter) in its role as promoters of recovery.

The Risk Management Index (RMI) includes a group of indicators that reflect the organizational, development, capacity and institutional actions taken to reduce vulnerability and losses, to recover efficiently from attacks.

\[
RMI = \frac{RMI_{RI} + RMI_{RR} + RMI_{EM} + RMI_{FP}}{4} \quad (3)
\]

Risk identification (RI) is a measure of the objective assessment of risk. Risk reduction (RR) involves measures and mitigation measures. Event management (EM) involves measures of response and recovery [9,10].

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shootings aircraft</td>
<td>RI 1</td>
</tr>
<tr>
<td>Shootings aviation transportation system infrastructure</td>
<td>RI 2</td>
</tr>
<tr>
<td>Bombings aircraft</td>
<td>RI 3</td>
</tr>
<tr>
<td>Bombings aviation transportation system infrastructure</td>
<td>RI 4</td>
</tr>
<tr>
<td>Exploitation of air cargo</td>
<td>RI 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>RMI_{RI} estimation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: Author</td>
<td></td>
</tr>
</tbody>
</table>

Aircraft target can include: large passenger aircraft, large all-cargo aircraft, small aircraft or nontraditional aircraft.

Experience shows that it is hard to find statistical data that can support the choice of data to use in the modeling when analyzing risks in aviation security system.

But, the combination of numerical values for the parameters can be used by validation of expert judgments in the field or by analyzing events from a historical perspective [11,12].

For example, a terrorist expert might conjecture that the probability or likelihood of a terrorism plot to attack an airport within the US using conventional explosives over the next 10 years might be 25% (P_T = 0.25), where P_T is the probability value assigned to a given threat T witch, in this case, is the threat of an airport bombing.

Continuing with the example above, an aviation security expert may consequently assign the vulnerability to such an attack among US airports at 50%, meaning that any conceivable terrorist bombing of the airport would have 50% chance of causing notable structural damage or loss of life. This can be expresses in terms of probability as \( P_V = 0.50 \), where \( P_V \) is the probability that a specific vulnerability \( V \) can be exploited by a terrorist attack or other security breach.

In this example, the combined probability that an attack using a particular threat scenario, an airport bombing, is attempted and is successful, is the product of two individual probabilities.

\[
P_{T\cap V} = P_T \times P_V \quad (4)
\]

where \( P_{T\cap V} \) is the probability of being attacked and the attack being carried out successfully.

The vulnerability expressed as a probability value \( P_V \) is the conditional probability of a successful attack given that a particular threat scenario has been attempted.

\[
P_{V|T} = \frac{P_{T\cap V}}{P_T} = \frac{(P_T \times P_V)}{P_T} \quad (5)
\]

where \( P_{V|T} \) is the probability of vulnerability \( V \) being successfully exploited given that threat scenario \( T \) has been attempted, is the conditional probability of a successful given a threat attempt [13].

Regarding historically analysis, it is useful to examine past incidents involving, for example, shoulder/fired missile attacks against commercial aircraft. These incidents are listed in table 2.

<table>
<thead>
<tr>
<th>Date</th>
<th>Place</th>
<th>Aircraft</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov. 08, 1983</td>
<td>Angola</td>
<td>Boeing 737</td>
<td>130 deaths</td>
</tr>
<tr>
<td>Feb. 09, 1984</td>
<td>Angola</td>
<td>Boeing 737</td>
<td>Forced landing</td>
</tr>
<tr>
<td>Sept 21, 1984</td>
<td>Afghanistan</td>
<td>DC-10</td>
<td>Forced landing</td>
</tr>
<tr>
<td>Oct 10, 1998</td>
<td>Congo</td>
<td>Boeing 727</td>
<td>41 deaths</td>
</tr>
<tr>
<td>Nov. 28, 2002</td>
<td>Kenya</td>
<td>Boeing 757</td>
<td>Missed target</td>
</tr>
<tr>
<td>Nov 22, 2003</td>
<td>Iraq</td>
<td>Airbus A300</td>
<td>Forced landing</td>
</tr>
</tbody>
</table>

Source: Elias, B., 2010

Random nature of events in the aviation security system determines the use of statistical methods in order to calculate the probabilities of achieving them.

The quasiprobabilistic methods (such as fuzzy set theory, Dempster-Shafer theory, the theory of interval valued probabilities) relax some assumptions and could be useful in the case of
measuring the risks in aviation system related to the asymmetric extreme events (terrorist attacks).

Catastrophic theories and chaos are useful in the treatment of extreme events because they allow explicitly characterize the mechanism of transition.

The theory of surprised is a qualitative approach relevant to define in assessing the probabilities of these kind of events (table 3).

Table 3 Conditional probability table

<table>
<thead>
<tr>
<th></th>
<th>Bomb</th>
<th>Hijacking</th>
<th>MANPAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft</td>
<td>yes</td>
<td>yes 20</td>
<td>yes 10</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no 80</td>
<td>no 90</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Cargo</td>
<td>yes</td>
<td>no</td>
<td>yes 10</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td>no 90</td>
</tr>
</tbody>
</table>

Source: Author

The specification of probabilities of extreme events rely on Bayesian rather than classic statistical method. Bayesian methods are efficient in situation of sparse data, since important subjective and other nonstatistical types of evidence can be used in decision [14]. The subjective nature of judgemental distributions is problematic of small tail probabilities.

2.3 Analyze the model

In order to draw attention to the problem and to see how the input to the Bayesian Networks aggregate results in terms of estimated probability the Bayesian network model was used.

The final step is the analysis of the model and also to validate and calibrate the model against available sources of information (statistical data or expert opinions).

This type of analyses can also be used to simulate the effect if the one or more variables in the model are known [17]. Also, the model can be updated with more variables both in terms of methods of attack used (Biological threats), and especially including countermeasures already in place (Surveillance technologies, Passenger and baggage screening or Aircraft countermeasures) and that its effects are felt.

In order to ensure and maintain a safe aviation system, it is indispensable to develop an analytic method that identify the risk factors and understand of where to focus the efforts to optimize the spending of resources.

3. Conclusions

A simple quantitative methodology for the risk evaluation in aviation system is proposed.

However, through effective management, based on available technologies and allocation of security resources, can mitigate the threat sufficiently to an acceptable level.

Bayesian Networks are an appealing method for quantitative risk management in aviation security system due to their versatility for different risk problems. Reducing investments is a cost-cutting option that could affect the security in the context of increased terrorist threats.

The purpose of the risk modeling in the aviation security system is to offer a simple framework for a better understanding of the risk problem, and to indicate ratings for the alternative strategies.

The application of Bayesian Networks in the aviation domain requires also a new strategy for risk communication and decision making capable to identify, analyze and mitigate the interdependent security risk [18]. For a better efficiency, it is also important to provide this information to authorized institutions, decision makers, experts, and various stakeholders for the final decision.

The results of risk analysis demonstrate that the proposed model can become a very useful tool in practice. Finally, it contributes to establishing a risk informed basis for making right decisions.
References:


