Chapter 4
Safety Versus Security in Aviation

Heinz Wipf

Abstract The two domains safety and security have traditionally been kept separated in aviation. While the first treats risks associated with aviation activities, the latter safeguards civil aviation against acts of unlawful interference. While national and international guidelines exist in addressing the installation of risk management for organizations having hazardous operations in aviation, an appropriate application of established assessment techniques, both quantitative and qualitative are crucial to both domains. For an incorrect hazard identification and the quantification of an adverse outcome may strongly affect both the level of protection and the investments required to reach it. The empirical example and data shown stem from safety risk assessments in HEMS (helicopter emergency medical service) flight operations. These flight operations use advanced instrument flight procedures in obstacle rich environments under low visibility conditions and are therefore a safety concern on the one hand. On the other hand, one analyzes security, whenever HEMS flights are operated in adverse weather conditions, having as a sole navigation source signals from a global navigation satellite constellation. A traditional safety risk assessment (Wipf in Aviation risk and safety management, Springer, p 108, 1) under these circumstances, considers only factors of human performance under technical failure conditions. A security analysis, however, should treat all forms of jamming, meaconing, and spoofing of the satellite signals and the adverse impact on the performance of the receiver to calculate a valid position. The chapter illustrates to which extent commonalities reign in both domains and where practices go separate ways.

Keywords GNSS · Air navigation · HEMS · Safety · Radio frequency interference · Game theory

H. Wipf (✉)
Airnav Consulting Zurich, Zurich, Switzerland
e-mail: airnavconsulting@bluewin.ch

C. Bieder and K. Pettersen Gould (eds.), *The Coupling of Safety and Security*, SpringerBriefs in Safety Management,
https://doi.org/10.1007/978-3-030-47229-0_4

4.1 Introduction

Over the last years based on our experience with light helicopter operations for disaster relief, search and rescue, and Helicopter Emergency Medical Services (HEMS), the necessity of an ever-widening operational scenario with all-weather capability has become apparent.

The use of Global Navigation Satellite Systems (GNSS) as a primary navigation source under low visibility conditions was, therefore, obvious. Due to weight restrictions and topographical circumstances, these signals often are the only means of getting a position solution. The relevant signals containing navigation information allowing the receiver to estimate the position are transmitted over an openly accessible radio frequency channel. Propagation effects [2] induced by flight attitude in conjunction with the receiver's antenna pattern may impair the quality of the navigation solution. Moreover, such a channel is prone to noise and interference stemming from different radio sources (Fig. 4.2). If such transmissions are intentional, then one can classify it as an unlawful interference. So while the former are safety-related, the latter is a security issue (Fig. 4.3).

The two domains safety and security have traditionally been kept separated because the International Civil Aviation Organization (ICAO) published different definitions in their annexes to the Chicago Convention. In these documents, security is defined as "Safeguarding civil aviation against acts of unlawful interference", while safety is "The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level". While security is handled by entities like law enforcement agencies and airports, safety is said to depend on personnel, procedures, and equipment, which is foremost the field of air operators and air navigation service providers. Another view on this separation comes from applying Systems Engineering (SE) methods. An approach is shown in Fig. 4.1.

The SE philosophy is quite in line with the saying that hazards lead to safety incidents in the same way that vulnerabilities lead to security incidents. The same view in a more formalized arrangement is shown in Table 4.1.

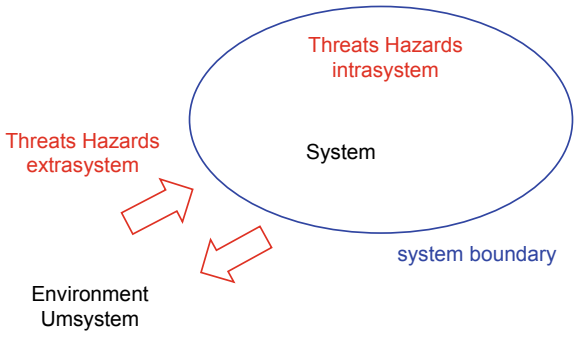

Fig. 4.1 Context of safety and security from a systems engineering viewpoint

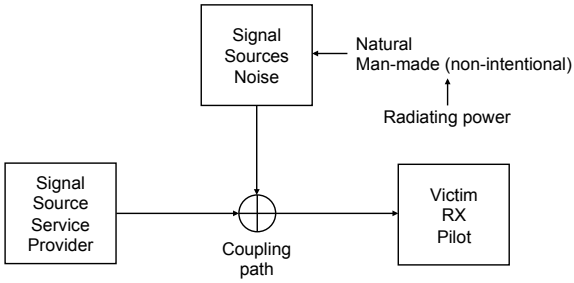

Fig. 4.2 Radio Frequency (RF) channel with noise and non-intentional interference

Table 4.1 Threat matrix formalizing the context in Fig. 4.2

Attacker	Victim	
	System	Environment
System	NA	Safety
Environment	Security	NA

This formalization of the 2 by 2 threat matrix in Table 4.1 reveals two entries (NA) that remain unaddressed. When asked what the synergies are between the two, the author would rather rephrase the question as: What are the commonalities? The question brought up here will be whether the two fields have to be treated differently or whether their unification is thinkable, notwithstanding the fact and existence of different authorities and jurisdictions.

4.2 The Economic Good in Question

The good in question is a radio frequency channel. The practical example chosen is at the same time relevant and valid, due to the fact that satellite navigation signals are extensively used for all sorts of critical infrastructure and hazardous operations.

Such a channel can be characterized by simple metrics, the bandwidth and the signal-to-noise ratio [3]. For this example, we would extend this ratio to also include any interfering signal power. The metric would then be signal-to-(noise + interference). The block schematic in Fig 4.2 is for the situation where only machines or one operator are present $N = \{0, 1\}$.

The system bandwidth is largely given by the base-band signal, and any interference being natural or man-made is, to the first order, only relevant within this channel bandwidth, because the receiver (RX) will band-pass all signals and suppress the others. This also means the interference format has to match the bandwidth to be effective.[1] In the case of meaconing and spoofing, this is per se the case, because the signal used to interfere is identical to the original one (Fig. 4.3).

[1] Here, we limit ourselves to one possible interference scenario: in-channel interference.

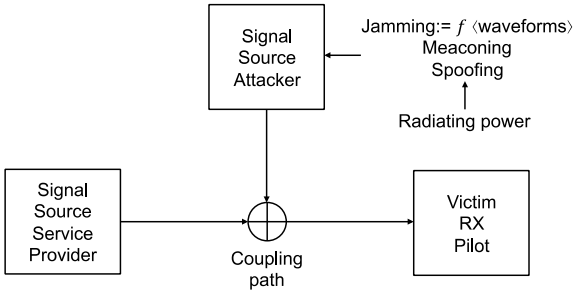

Fig. 4.3 RF channel with intentional interference

So the only free variables for the interferer are the duration and the radiated power. Although a jamming attack has the freedom of different signal formats, the classes are limited to only four.[2]

Jamming is the emission of radio frequency signals of sufficient power and with such characteristics to prevent the receivers from working properly.

Meaconing is the reception, delay, and rebroadcast of a signal with a larger power than received. At the receiving antenna, the wanted and unwanted signals are added to confuse the system. Ground- and space-based augmentation radio links could also be prone to meaconing, especially if the correct differential signal is suppressed with a stronger one containing false corrections.

Spoofing is a technique to cause a receiver to lock onto legitimate-appearing false signals. The attack will inject misleading information and thereby eventually even control the flight [4, 5, p. 63].

The radiated transmission power is a continuous variable that the attacker is free to choose for each attack. However, as indicated above, certain bounds exist. Every RF channel is specified in five dimensions. So out of frequency, time, space, modulation, only polarization would remain an issue for an optimization on the side of the interferer.

An air navigation service provider, supporting hazardous flight operations, has to inform the user of three probabilities

1. Reliability[3]: using the service and not losing it.
2. Availability: requesting the service and getting it.
3. Integrity: correctness of the information supplied.

The above include the condition that the provided signals are within specified error bounds in space and time.[4]

The constant presence of interference from natural sources is an important aspect. So even in the absence of man-made interference, the receiver has to cope with noise from intra- or extra-system sources.

[2] Continuous Wave (CW), chirp, pulses, and noise.

[3] Also Continuity of Service (CoS).

[4] See ITU definitions.

Another aspect indicated by the signal-to-(noise + interference) ratio is the diminishing of the signal power due to an increase in radio path attenuation. These two factors are relevant when discussing game-theoretic approaches, namely in the absence of an attacker $N = \{0, 1\}$.

4.3 A Game-Theoretic Approach Put to Practice

The title of this section reads like a contradiction in terms, but it is well worth to attempt to get practical. Game theory, a branch of mathematics, offers an analytical approach to situations of a practical nature. The situations considered are games with different parties having common or different interests. Mathematical solutions are possible for certain cases. The situations include true games as such[5] as well as real-world problems in politics, economics, or warfare. The theory has also recently been applied to terrorism [4, p. 198].

This contribution treats a real-world problem, and classical game theory is being tried. It means players may strategize,[6] decide, and act. Whereby chance, hidden or incomplete information are pertinent circumstances. A game consists of players[7] (individuals/organizations), strategies (a plan, objectives, decisions, and actions), situations, and a gain from participating (utility). In short, a theory of mathematical models is applied to formalize interdependent players with their decisions and actions under a condition of conflict or cooperation.

Thus, the question is what are the provisions of such an approach to safety and security and what are the elements necessary to model the chosen real-life situation. Elements in this example are discrete and can, therefore, be described in a set-theoretic way. The only exception is the radiated power P of the interferer. If an attacker intends to maximize impact while minimizing the probability to be detected, then this value is bounded. This parameter, therefore, is also accessible to set theory. So let the radiated power be $P = \{0, P_{\max}\}$. The two values are then equivalent to abstain or execute an attack.

4.3.1 The Players

The complete setup includes three players with different coalition aspects summarized in Table 4.2.

Although a coalition of interest exists between the user and the service provider, it may not be strong enough to have the service provider actively taking part in the

[5] E.g., card games or chess.

[6] To have a plan of what to accomplish, while taking intentions of other involved parties into account.

[7] For completeness, it is advisable to attribute participation and interest of the players.

Table 4.2 Players attributes

	Service-related	Coalition	
		Participation	Interest
Players	User (U)	True	True
	Provider (P)	False	True
	Attacker (A)	True	True

game. The reason lies in important investments like upgrading or replacing space-based assets. Such actions would have a negative impact on service provider's utility, which is cost versus the number of users. Thus, the service provider is excluded.

4.3.2 Available Strategies

The course of action or possible strategies in this example form finite sets (SA and SU). The setup of the game has one attacker (A) and one victim, the user of GNSS (U) in a flight under low visibility condition (IMC), under Instrument Flight Rules (IFR) with no redundancy in navigation. The attacker intends to deny the use of this only system. This situation asks for an offensive strategy on the side of the attacker and a defensive one on the side of the user. The attacker has three distinctive but feasible attacks or strategies, and they constitute a finite set:

$$\mathrm{SA} = \{\text{Jamming, Meaconing, Spoofing}\}.$$

For the location of the jammer, different options exist. It could be on a fixed, ground-mobile, or airborne platform. We limit our case to the fixed option. Although a mobile jammer would be more difficult to detect, target jamming an airborne asset would be more of a challenge, since the road network would not be coincident with the projection of the victim's flight path. An airborne jammer finally would offer a number of attacking advantages, but operating costs would be considerable, to be effective. Moreover, detecting and locating the attacker would be fairly simple. The set of strategies of the attacked U[8] on the contrary is a purely defensive set:

$\mathrm{SU} = \{$spectrum/signal monitoring, reducing the coupling between receiving antenna and attacker's transmission, minimizing the exposure time$\}$.

[8] *P* is only indirectly affected by the attack unless his assets are impacted. U has little influence on *P* to, e.g., motivate an increase in transmitting power, which would increase his signal/noise.

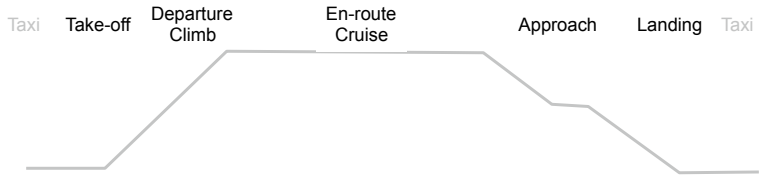

Fig. 4.4 Phases of flight after [6]

Table 4.3 FP, T_{exp}, height to the victim's antenna contrasted with criticality

FP	T_{exp}	Unit	T_{exp} h	Height in m	Criticality
Takeoff	10	sec	2.78E-03	5.0E + 01	High
Departure	5	min	8.33E-02	2.0E + 02	Medium
En-route	45	min	7.50E-01	2.0E + 03	Low
Approach	5	min	8.33E-02	2.0E + 02	Medium
Landing	30	sec	8.33E-03	2.0E + 01	High

[a]In principle from [6]

4.3.3 The Situations

The situations are governed by the phase of flight and its need for a precise aircraft position. The user counts on the three probabilities (1., 2., 3.) above indicated by the service provider. These are estimated from empirical failure rates[9] or reliability calculations. Together with corresponding exposure times, it results in failure probabilities. Figure 4.4 defines the general Flight Phases (FP).

A FP is ended and another started as decided from the flight deck (decision instance, player A). Possible scenarios, therefore, are determined and finite. Although a loss of a position solution in low visibility on ground is not irrelevant, ground movements are discarded for the sake of simplicity. The set is consequently reduced to FP = {Takeoff, Departure, En-route, Approach, Landing}.

Exposure times vary considerably. Table 4.3 shows typical mean values for helicopter operations. While T_{exp} shows changes of the order of a magnitude along the flight trajectory, the distance and with it the radio path attenuation for a potential interfering source toward the victim's receiving antenna also change.[10]

There is an intrinsic relation between exposure time and the height of the victim above the antenna of a potential interferer. This relation allows some ground for an operationalization of the probability of losing a position due to an interferer located on the ground while executing a specific flight phase. The risks for the victim depend on the status of the signal received. If the signal is in use and a critical flight

[9]The rates for rare events are assumed to be Poisson distributed and have an exponentially distributed duration.

[10]Path attenuation $a = 1/r^2$.

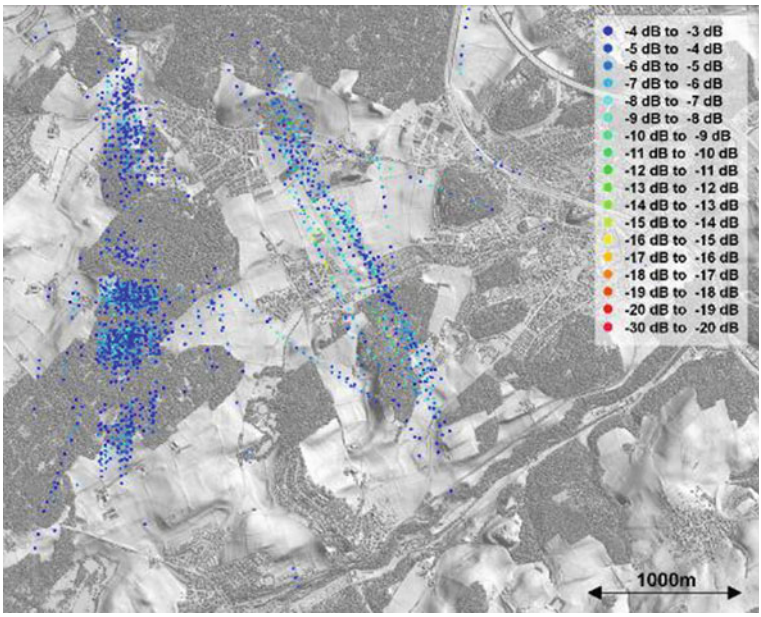

Fig. 4.5 Result of a monitoring action [7] (Figure courtesy of M. Scaramuzza, Skyguide. Included with the permission of the author.)

phase being flown, then the loss of the signal leads to a hazardous situation and the risk of an accident. If the signal is to be acquired but not available, then the mission will be aborted and economic loss results. The attacker may of course choose the interfering power[11] at his discretion. However, radiating too much power increases the Probability of Intercept (POI). This condition in turn increases the possibility of being detected by some monitoring processes [7–9]. Figure 4.5 shows the result of monitoring recorded during normal helicopter missions where the Quality of Service (QoS) is repeatedly degraded. The colors indicate the severity of potential Radio Frequency Interference (RFI).

If detected, the victim will initiate an evasive action rendering futile the attempted attack. Moreover, detection could lead to getting located by an authority in charge, so the attacker has to make a tradeoff.[12] However, the maximum radiated power of the interferer is not only bounded for tactical reasons but also for technological ones. Table 4.4 underlines the risks of an attack.

[11] Effective Isotropic Radiated Power (EIRP).

[12] There are more elaborate strategies in the fundus of the electronic warfare arsenal.

Table 4.4 Attacker's costs on equipment and the probability of intercept

Attack	Investment €	Knowledge	POI
Jamming	1000	Low	High
Meaconing	10,000	Medium	Low
Spoofing	1,00,000	High	Low

4.3.4 The Outcomes of the Game

The outcomes must illustrate potential gains in the areas of cost, risk, and utility. It is possible, though to include the cost in the risk for both players. The risk R for the attacker may be approached in the following way $R = (I + K) \bullet \text{POI}$, where I is the investment for the equipment, K is the knowledge, and $I + K$ the total cost. POI is the detection of a monitoring instance within the interfered region. An attempt for the payoff matrices of the two players (A and U) is shown in Table 4.5, where the gain (1) and loss (−1) are indicated in each entry.

In this example obviously, the gain of the attacker A is the loss of the attacked U. The gain matrix above suggests a strategic advantage to attack. However, the matrix does not display the entire picture. Table 4.6 gives an indication of the likelihood that the attack is being detected and consequently a flight operational action is initiated.

The likelihood of being detected is about two orders of magnitude smaller for meaconing and spoofing compared to jamming due to the difference in signal formats.

Table 4.5 Gain matrix

Attacked / Attacker	No action	Climb	Accelerate	climb and accelerate
Jamming	–1 1	1 –1	1 –1	1 –1
Meaconing	–1 1	1 –1	1 –1	1 –1
Spoofing	–1 1	1 –1	1 –1	1 –1

Table 4.6 Likelihood of the attacked gaining situational awareness due to detecting an attack

Attacked	Attacked
	Likelihood of situational awareness
Jamming	High
Meaconing	Low
Spoofing	Low

Table 4.7 Game classification

Players	Action domain	Game type	Approach	Example
0	Safety	Non-strategic	Descriptive mathematics	Automata
1			Optimization	Socio-technical systems
2	Security	Strategic	Game-theoretic	Competition
≥3				Cooperation

In general, technical infrastructures providing a common good, accessible to the general public, are seldom attacked. An explanation may be that the attacker or his allies need the service they intend to impair for their own purposes.[13] There is a generally accepted utility attached to this good.[14] In this case, the payoff matrix must be modified to reflect such situations and to find the Nash-equilibrium [10, p. 286], which could give an explanation for this phenomenon.

4.3.5 Game-Theoretic Classification

To summarize and make use of game theory, an attempt is made to classify the example at hand. Games are classified according to the different sets mentioned above. The most obvious one is the number of players. A game can have one, two, or n players. Each manifestation has its own distinctive features, and the players need not be individuals. It may be a group of persons with common interests being part of some organization. Even organizations could federate in a game. The possibilities are summarized in Table 4.7.

The empty and the unit set of players are included to propose a possible unified approach under game-theoretic aspects. The empty set (no players) would be a purely machine-to-machine interaction, unless artificial intelligence is actively involved. The unit set (1 player) is also called a one-person game. With no rivals, the player only needs to list available strategies so to choose an optimum outcome.

When probabilities are involved, it may turn out to be more complicated. Ways and means to cope with such problems are laid down in decision theory. Or as often said, the single player is engaged in a game against nature, where nature is indifferent to the player's decision.

Whether the objectives of the players coincide or conflict is another aspect of the classification. Constant-sum games show an entirely conflicting situation (pure

[13] See also today's conflict zones, where mobile telephone base stations keep on working, although used for warlike actions.

[14] See physical attacks on single aircraft, but not on the infrastructure supporting flight, like vulnerable assets of air navigation or airport services.

Table 4.8 Game-theoretic classification for the example

	This example	Bi-matrix game	Matrix game
No. of players N	2	2	2
Non-cooperative	True	True	True
Finite	True	True	True
Zero-Sum	True	False	True
Strategic	True	True	True

competition),[15] with no communication between the adversaries. This fact leads to incomplete information on both sides.

Whether a game is called finite depends on finite sets above [10, p 286]. Moreover, the game cannot have an indefinite duration. In practice, there exists a window to act.

A finite non-cooperative game between two players is called a bi-matrix game. It is specified by two matrices $A = \|a_{ij}\|$ and $U = \|u_{ij}\|$ of the same dimension $m \times n$. These two matrices represent the payoff matrices (gain matrices) of the players. The strategy of player A is the selection of a row, that of player U the selection of a column. Let player A choose i $(1 < i < m)$, while player U chooses j $(1 < j < n)$, their respective payoffs or gains will be a_{ij} and u_{ij}. If $a_{ij} + u_{ij} = 0$ for all i, j, then the bi-matrix becomes a matrix game. The two candidates reflecting this example are either a bi-matrix or a matrix game. Table 4.8 indicates that the latter matches the situation.

4.4 Conclusion

An attempt has been made to structure a real-world problem to make it accessible for a game-theoretic solution and it appears as if the two aspects of safety and security can be assessed in one single unified solution space. Both fields turn out to be different subsets of a more fundamental superset. More formally, one rationalizes the synergy between safety and security solely in the number N of involved instances or players. So there is a temptation to see game theory as a possible means of offering a unifying approach.

A pertinent question has come into focus, namely why vulnerable basic infrastructure like radio channels in the case of air transportation has been so seldom the target of elaborate electronic attacks. One possible answer is the utility it has for all conflicting parties. In the case of openly accessible radio channels, the utility may even extend to gather information about the adversary.

[15] Rolling dice is an example, because the combined wealth of the players remains constant, although the distribution in the course of the game changes.

4.5 Outlook

There are other situations in aviation where game theory seems an appropriate way to model other interactions, namely flight operators, air traffic service providers, and airports. A typical example where airport security is negatively influencing professionals concerned with flight safety is described and analyzed in [11]. Unlike the non-cooperative nature of the example above, these entities are engaged in a coalition game, because they have the opportunity to collaborate for mutual benefit in several ways. Moreover, it would be advantageous to industry if rule-making and supervisory activities would be included in such models.

References

1. H. Wipf, Risk management in air traffic control—operators risk back to basics. Aviation risk and safety management, Springer (2014)
2. A. Geiger et al., Simplified GNSS positioning performance analysis. Monterey ION-IEEE-PLANS (2014)
3. C.E. Shannon, A mathematical theory of communication. Bell Syst. Techn. J. **27**, 379–623 (1948)
4. B. Golany et al., Nature plays with dice–terrorists do not: allocating resources to counter strategic versus probabilistic risks. Eur. J. Oper. Res. **192**(1)
5. Vulnerability assessment of the transportation infrastructure relying on the global positioning system. In: 2001 Final Report J. A. Volpe National Transportation Systems Center
6. Statistical summary of commercial jet airplane accidents worldwide operations. Seattle Boeing (2016)
7. M. Scaramuzza, Localization of GNSS RFI transmitters using digital surface models. Belgrade IFIS (2016)
8. M. Scaramuzza et al., GNSS RFI detection—finding the needle in the haystack. Tampa GNSS-ION (2015)
9. M. Scaramuzza et al., RFI detection in Switzerland based on helicopter recording random flights. Oklahoma IFIS2014 (2014)
10. J.F. Nash Jr., Non-cooperative games. Ann. Math. **54**, 286–295 (1951)
11. K.A. Pettersen et al., Organizational contradictions between safety and security perceived challenges and ways of integrating critical infrastructure protection in civil aviation. Saf. Sci. **71**,167–177 (2015)