Australasian Transport Research Forum 2010 Proceedings
29 September – 1 October 2010, Canberra, Australia
Publication website: http://www.patrec.org/atrf.aspx

Identification of ADS-B System Vulnerabilities and Threats

Mr Leon Purton, Professor Hussein Abbass and Dr Sameer Alam

Defence and Security Applications Research Centre, University of New South Wales

Australian Defence Force Campus, ACT 2600

Email for correspondence: leon.purton@student.adfa.edu.au; h.abbass@adfa.edu.au

Abstract

Air Transport has witnessed rapid growth in the past decade and it is foreseen it will need to accommodate growth to as many as twice the number of flights, by 2020. This challenging target will require a boost in capacity together with an increase of safety levels. Ground based legacy surveillance systems remain a bottleneck in addressing this challenge. At the forefront of the competing new surveillance technologies is Automatic Dependent Surveillance – Broadcast (ADS-B) where an aircraft transmits its position based on onboard navigational instruments and a satellite navigation link. The ADS-B system broadcasts information periodically to all aircraft in the immediate vicinity and all surveillance facilities in specified areas. This information can be translated into a 4D trajectory and made available both to the ground controllers and airline crew for better and shared decision making.

With any new technology lies uncertainty in system vulnerabilities and threats. Therefore, it is necessary to understand and where possible mitigate vulnerabilities and threats. This is especially true for an air transport system that can deliver capacity and safety improvements. This paper aims at addressing some of the uncertainties in ADS-B; this involves assessing the vulnerabilities and threats in the transmission and computation information path through examination of the system critical elements. As opposed to previous ADS-B system assessments which concentrate on procedural remedies for technical problems, this paper focuses on technical solutions for the problems. The system elements are explored using TOWS analysis addressing different types of network intrusions, message spoofing, and communication malfunction activities. Some vulnerability and threat mitigation strategies based on TOWS analysis are then developed.

Keywords: ADS-B, threats, vulnerabilities, TOWS, strategic actions

Introduction

Air transport continues to change and expand both in volume and in the areas of the world it serves. While recognizing that the current systems and procedures of air traffic system have served the international civil aviation successfully and safely for the past 60 years, ICAO felt that these systems are reaching their operational limits due to inherent shortcomings in Communication Navigation and Surveillance (CNS) systems viz. propagation limitation of line of sight systems, limitations of voice communications and lack of digital data link (ICAO, 2002). Advances in CNS technologies need to be incorporated in the Air Transport environment for safe and efficient management of growing air traffic.

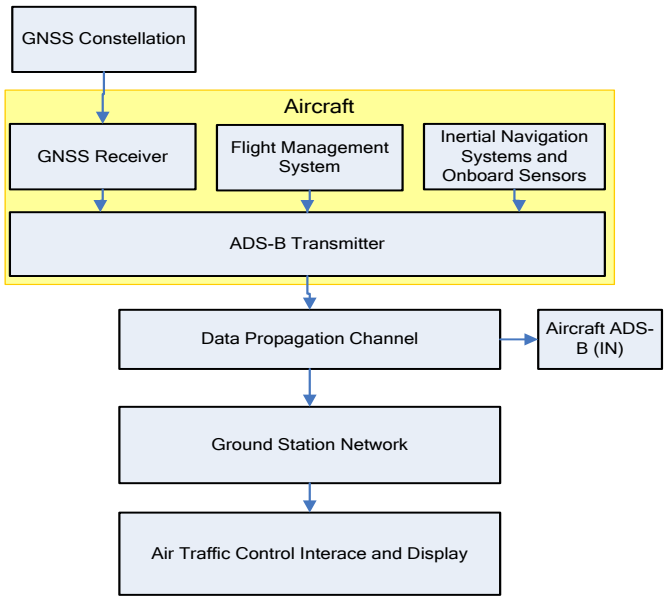
Several efforts are underway to address these challenges, such as SESAR Europe's Single European Sky Air traffic Research system (SESAR2007) and U.S. NextGen (Next Generation Air Transport System) (NextGen2007). The common SESAR and NextGen vision is to integrate and implement new technologies to improve Air Traffic Management (ATM) performance. SESAR and NextGen combine increased automation with new procedures to achieve safety, economic, capacity, environmental, and security benefits.

In light of the above improvements, the ICAO has adopted the Global Air Navigation Plan for CNS-ATM Systems "*to develop a seamless, globally coordinated system of air navigation services that will cope with worldwide growth in air traffic demand while improving upon the present levels of safety and improving upon the overall efficiency and capacity of airspace and airports*" (ICAO, 2002). This concept requires the use of data link communication, satellite based navigation systems (GNSS) and use of automatic dependent surveillance broadcast system (ADS-B).

Surveillance coverage and accuracy will be enhanced in the future by integrating the GNSS derived position information with the information provided by the PSR and SSR radars. This information can be translated into a 4D trajectory and made available both to the ATC and airline crew for better and shared decision making. ADS-B is proposed which will eventually replace ground based surveillance systems (RTCA, 1999). In ADS-B, an aircraft transmits its position based on onboard navigational instruments. The ADS-B system broadcasts information periodically to all aircraft in the immediate vicinity and all ATM facilities in specified areas. The primary objective of ADS-B is to improve the surveillance coverage in low or no radar coverage area. ADS-B will be a suitable medium for the transmission of FMS data to ground based Air Traffic Centres.

Formally, ADS-B is defined - “a means by which aircraft, aerodrome vehicles and other objects can automatically transmit and/or receive data such as identification, position and additional data as appropriate in a broadcast mode via a data-link” (ICAO Doc 444). The precision of ADS-B does not deteriorate with range from the receiver as with Radar systems. It does not require continual monitoring of the out of radar coverage aircraft through radio communication. ADS-B accuracy is normally less than 20m; this precision is greatly improved from Radar which at 60 nautical miles is approximately 300m. It has been mandated for fitment by AirServices Australia for aircraft operating above 29,000 ft by 2013 (CASA, 2004), with similar mandates outlined for the FAA in America and EUROCONTROL in Europe. A basic ADS-B system diagram can be seen in Figure 1 highlighting the various interdependent systems that makes up the ADS-B surveillance system.

Figure 1: General ADS-B System showing reliance on GNSS and on-board sensors to generate ADS-B message which can also be received by other Aircraft equipped with ADS-B (IN).



Other aircraft surveillance technologies which provide for higher accuracy include Wide Area Multilateration (WAMLAT), which uses the replies from radar transponders, timing their arrival at ground receiving antennas and calculating aircraft position from those time differences. This type of installation, though cost effective, is not feasible for Australia’s vast geographic size. For this reason AirServices Australia has decided to be one of the frontrunners in implementation of ADS-B technologies for the Australian airspace, with some

of the first airborne and ground trials in the Burnett Basin region in 2001 (Dunstone, 2007). Moreover, the SESAR Concept of Operations describe new methods of working which require certain enablers and only ADS-B can provide the support needed.

ADS-B is dependent on GNSS for position and on-board sensors for message information. ADS-B has a range of approximately 100 nautical miles and provides information such as traffic call sign, heading, speed, position and trajectory intent to all receiving stations, which include aircraft. Aircraft equipped with Cockpit Display of Traffic Information (CDTI) which is enabled through ADS-B (IN) can receive airspace information on a surveillance screen and have shared situational awareness with Air Traffic Controllers. Table 1 gives a comparison of the benefits and qualities of the legacy surveillance system Secondary Surveillance Radar (SSR), WAMLAT and ADS-B. It outlines that although there is a cost in initial fitment the benefits provided are beyond that of the competing technologies.

Table 1: Comparison Table of Surveillance Technologies

	SSR	WAMLAT	ADS-B
Position Fix-type	Time of reception	Time difference of arrival	Global navigational satellite fix
Accuracy (@ 90, 120 nm)	450, 600 metres	30, 60 metres	20, 20 metres
Cost of Fitment	Nil cost	Nil Cost	Cost involved
Potential for Global Coverage	No	No	Yes
Capacity Increase	Nil	Potential	Yes
CDTI enabler	No	No	Yes
Aircraft to Aircraft	No	No	Yes
Aircraft Intent	No	No	Yes
Separation Assurance	No	No	Yes

The benefits for ADS-B are extensive and include capacity and efficiency improvements, reduction in operating costs improved aviation safety for air and surface movements, reduction in ATC workload and greater information for environmental monitoring (JCP, 2007 and Smith et al, 2006). However, the process of moving the ATM legacy system to the state of art in CNS is naturally a slow process. Moreover, every new technology cannot be put in the cockpit without detailed operational and safety analysis. Several risk assessment exercises have been undertaken to identify risk in ADS-B and its sub-systems.

Previous Assessments

In July 2007 four Australian government bodies: AirServices Australia, Civil Aviation Safety Authority (CASA), Department of Transport and Regional Services and The Department of Defence prepared a report “Transition to Satellite Technology for Navigation and Surveillance” (JCP, 2007). This report provided an outline of the ADS-B system and developed some of the advantages of wide-scale fitment while addressing the community’s common questions and identifying the proposed legislative changes. It aimed at addressing the system from a security perspective without necessarily discussing some of the inherent system risks through a threat and hazards analysis.

Other risk assessments in the literature include:

1. **US FAA (FAA, 2000) Study:** This was done to compare the U.S. National Airspace System (NAS) with and without ADS-B. To better illustrate the risk reduction potential as well as new hazards introduced, the investigators included a third alternative entitled “ADS-B, Normal Operation.” This represents an artificial condition in which all equipment performs properly. It illustrates the intended benefits of the new service and procedures. The other alternative entitled “ADS-B, Abnormal Operation”

presents the effects of failures and their associated likelihoods. The alternative "With ADS-B, Abnormal Operation" considers failures of equipment, data link, and human errors. The study found ADS-B applications are low risk in nearly all cases. Some of the applications should improve the safety of the NAS, while others are intended to enable operational improvements and should not degrade safety in so doing.

2. **RTCA Study (RTCA SC186 WG4):** The study provides a derivation of the levels of performance that are assigned to each element of ADS-B analysed. By comparing the likelihood of the ultimate hazard to the acceptable level for its severity, it can be determined whether the overall safety using these allocations is acceptable. The objectives were to determine the required levels of surveillance quality and of performance of each element in the fault tree. These include human performance, communications, and hardware and software reliability.
3. **GPS Risk Assessment, 1999**: An assessment (John Hopkins, 1999) into using GPS for navigation was carried out in 1999 by the John Hopkins University Applied Physics Laboratory of Laurel, Maryland under the guidance of the FAA. One of the primary purposes of the study was to assess the risk to the augmented GPS signal from intentional interference, or jamming, and unintentional interference, such as heightened solar activity and interference from certain commercial TV and VHF broadcast signals. Essentially, the study found that a combination of procedural and technical measures to mitigate the effects of both types of interference are achievable and must be implemented as part of the future augmented GPS system to ensure acceptable performance with the need for additional GPS satellites.
4. **ADS-B Risk Assessment, 2005**: In 2005 a report was published by EUROCAE titled "Safety, performance and interoperability requirements document for ADS-B/NRA application" (EUROCAE, 2005). This report uses expert analysis to define a series of operational hazards and their severity with application of some internal and external mitigation techniques to manage them. The severity of each is assessed based on whether it is detected or undetected. This assessment is based on Air Traffic Controller interaction with the display and detection of faults and errors, not the risks in the critical elements of the system.

The previous studies do not assess ADS-B threats and vulnerabilities against the environment. A more logical way is to identify the extent to which the ADS-B system and its more specific strengths and weaknesses are relevant to, and capable of, dealing with the changes taking place within the Air Transport environment. A holistic approach for identifying threats and vulnerabilities in ADS-B system must aim to build on strengths, eliminate weaknesses, exploit opportunities and mitigate the effects of threats.

TOWS Methodology

This paper utilises Threats, Opportunities, Weaknesses and Strengths or the TOWS matrix (Weihrich, 1982) to analyse the ADS-B system. This is a qualitative assessment used with a holistic view to discern possible strategic actions for an organization or systems in the environment. SWOT uses internal elements to interact with the external elements. TOWS analysis which differs from SWOT in application arose from a need to assess how situations external elements can positively and negatively affect the internal elements. In essence TOWS starts with the external elements while SWOT starts with the internal elements. The aim of these analysis techniques is to identify the extent to which the current strategy of an organization and its more specific strengths and weaknesses are relevant to, and capable of, dealing with the changes taking place within the environment. To succeed, strengths and opportunities must be used to overcome or mitigate threats and weaknesses.

The transport sector is using SWOT analysis to develop and assess strategies; Dorin et al (Dorin, 2009) use SWOT for management of an urban transportation system, Verweij et al (Verweij, 2009) use SWOT to assess trends and developments in each transportation sector of the European Union. Upham et al (Upham, 2004) utilise SWOT for assessing environmental capacity and European air transport and Ahmed et al (Ahmed, 2006) assess the performance and quality of Air China. Literature also exists demonstrating the principle of SWOT or TOWS in analyzing problems and systems. Zoullias (Zoullias, 2004) uses

SWOT analysis to Hydrogen stand-alone power systems. Similarly Cole et al (Cole, 2006), use SWOT for analyzing the future of energy storage, and Sarkar et al (Sarkar, 2006) use SWOT analysis to identify solutions for Arsenic contamination of ground water in eastern India. The literature demonstrates the diverse application of these techniques showing that they are an adaptable and flexible structure that can be implemented in any scenario. With a focus on external elements interaction with a system, TOWS analysis is well suited to assessing the vulnerabilities and threats to the ADS-B system. The four elements of TOWS analysis applied to a generic system are:

- Threats - Refers to an external situation that is potentially damaging to the system. It can be an environmental factor or a third party act.
- Opportunities - Refers to an favorable situation in the system environment
- Weaknesses - Refers to an limitation, fault or defect in the system which will impact on the systems objectives
- Strengths - Refers to the systems resource or capacity that can be used to further the systems objectives

By establishing the premises that threats and opportunities are external to the system and induced through the environment, and that weaknesses and strengths are internal. The TOWS matrix is generated and strategic actions formed; explanations of strategic actions are given in Table 2.

Table 2: Strategic actions derived from TOWS matrix

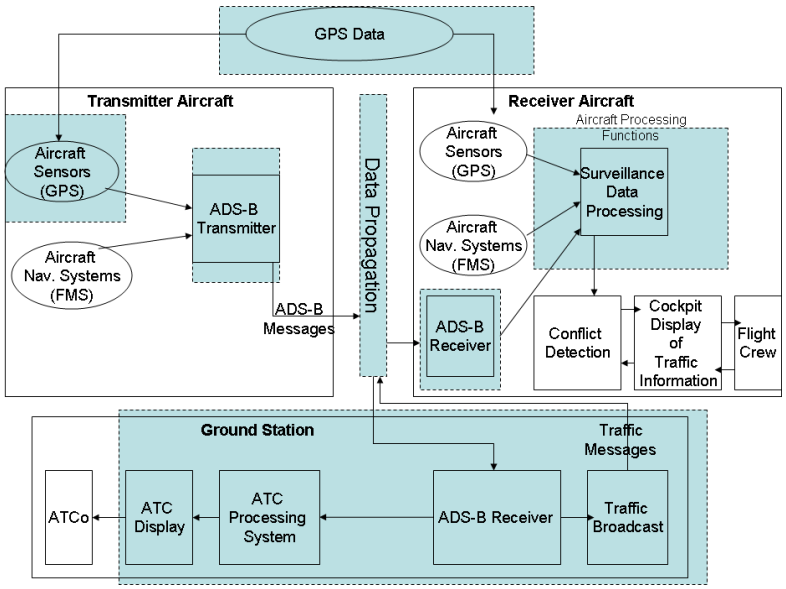
	External Threats and Hazard	**External Opportunities**
Internal Weaknesses	*W-T* The exploitation of weaknesses by threats (negative risk)	*W-O* Strategies that minimize weaknesses by taking advantage of opportunities
Internal Strengths	*S-T* Strategies that use strengths to minimize threats and hazards	*S-O* Strategies that use strengths to maximise opportunities (positive risk)

This analysis technique can be used to help bridge the gap between the practitioners and theoreticians when analyzing a system. It utilizes a combination of system understanding and environmental effects to identify means to improve the system and areas in which the system is vulnerable through examination of internal and external factors.

Identifying Vulnerabilities and Threats

ADS-B is a system of systems, where focusing on one component alone in separation for an assessment exercise is undesirable. Therefore, it is logical to assess the elements of the ADS-B system from the satellites to the ground. For this reason the system will be assessed as four main components: GPS, ADS-B transmitter, propagation path and ground infrastructure up to and including the ATC display. Even though the Global Positioning System can be defined as a system itself, it is integral to the operation of the ADS-B system. The same applies to the ATC display, without it the ADS-B system would be of no real use. By defining these components as internal to the ADS-B system, a clear boundary is defined outlining the internal and external system influences. Figure 3 shows the critical elements of the system and highlights the areas of vulnerability.

Figure 3: Critical Elements of ADS-B system with highlighted areas of vulnerability.



TOWS Analysis of ADS-B System

TOWS analysis is used to assess the elements of the ADS-B system and their interaction with the environment. To assess element a systematic top down approach was used; starting with GPS and finishing with the ground infrastructure.

To be able to identify the areas in which ADS-B is vulnerable a critical elements analysis was carried out. The critical elements of the system lie where there is a threat or hazard along with an opportunity to exploit it or for it to cause an undesirable outcome. The severity of the threats and hazards can be assessed based on OSA-ED78A/DO264 Hazard classification matrix (Table 2) giving them a rating of 1-5 with 1 being the most severe and 5 being the least. The TOWS matrix analysis method is used to identify the system factors.

Threats

When classifying threats there is no delineation between a threat and a hazard in the given numbering scheme.

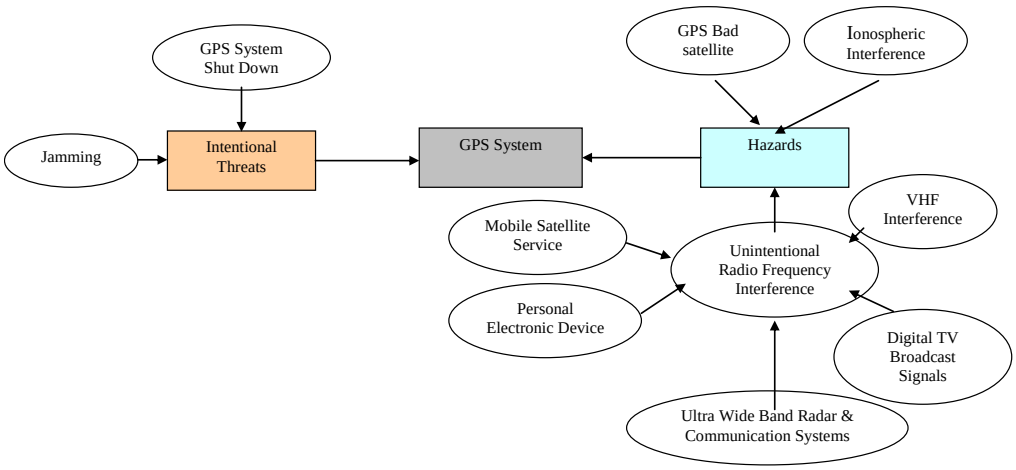
T1. The GPS system includes the link from the satellites to the receiver. Firstly the threat of GPS Denial of Service (DoS) must be assessed. GPS is a spread spectrum signal and is already transmitted below the noise floor. It relies on coding gains for reception. To jam an aircraft reception of GPS from a ground source would require extremely high power. GPS jamming from above the aircraft is likely only to occur in military situations from platforms such as the AEW&C aircraft. This threat is assessed with severity rating of 2 and a low likelihood. The likelihood assessment is based on the power levels required to sufficiently jam the GPS signal.

Table 3: Table Identifying Threat/Hazard Severity [Source: EUROCAE, 2005]

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or in ATC capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.
Example of ASAS operational effects	• *Mid-air collision* • *Controlled flight into terrain* • *Total loss of flight control* • *High speed surface movement collision (i.e. collision in runway)* • *Leaving a prepared surface at high speed.*	• *Large reduction in separation or safety margins* • *Loss of separation resulting in wake vortex encounter at low altitude.* • *Large reduction in safety margins like abrupt manoeuvre is required to avoid mid-air collision or CFIT (e.g. one or more aircraft deviating from their intended clearance)* • *Large reduction in aircraft functional capabilities* • *Total loss of air traffic control for a significant period of time*	• *Significant reduction in separation or safety margins* • *Loss of separation resulting in wake vortex encounter at high altitude.* • *Low speed surface movement collision (i.e. collision in taxiway)* • *Leaving a prepared surface at low speed* • *Significant reduction in aircraft functional capabilities* • *Significant reduction in air traffic control capability*	• *Slight reduction in separation or safety margins* • *Significant increase in air traffic controller workload* • *Slight increase in flight crew workload*	• *No effect on operations /traffic* • *Slight increase in air traffic controller workload* • *No effect on flight crew*

T2. ADS-B system hazards from GPS arise from GPS bad satellite or GPS receiver malfunction. The GPS is an integral component to the ADS-B system and any adverse effect has high consequence. GPS bad satellite occurs when the satellite transmits bad data which is not flagged by the control agency. This occurs from time to time but systems have been developed that reject satellite information if it improves the position solution. GPS receivers, as with any electronic device, can malfunction or fail from time to time. Importantly with this hazard, it is the level of failure and the systems ability to detect the fault that gives the level of consequence. These hazards are assessed as level 2 severity and medium likelihood. A diagram illustrating the links between the GPS threats and hazards is given in Figure 4.

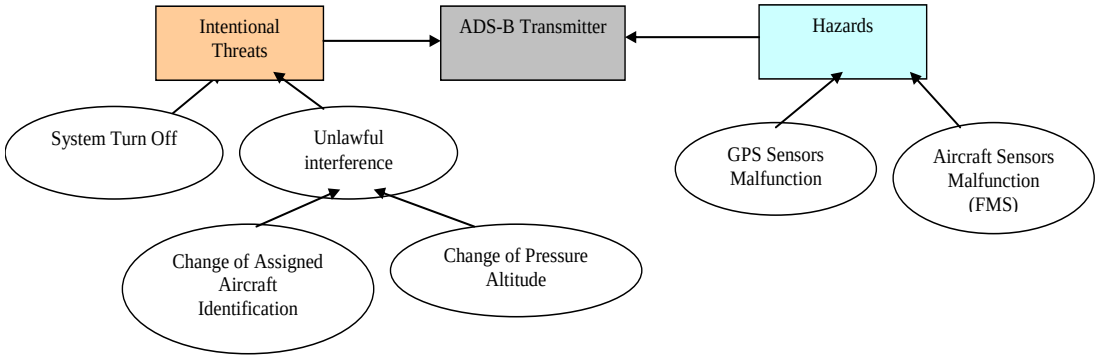
Figure 4: GPS System Threats and Hazards



T3. The only threat derived from the ADS-B system is that it is turned off. This makes the aircraft non-cooperative and any tracking is then based on flight plans and primary Radar. The severity level of this is 1, this is a similar scenario to the 9-11 incidents where SSR was turned off, and would normally indicate a malevolent act. The likelihood of this threat can be considered low, even though public perception and current threat mitigation is still prominent in thinking.

T4. The hazards surrounding the ADS-B transmitter involve bad input data and transmitter malfunction. This has been grouped as ADS-B transmitter data input errors or malfunction. The ability to detect bad input data is limited, while transmitter malfunction is likely to be detected. For this reason this hazard is assessed at severity level 3 with medium likelihood. A diagram illustrating the threats and hazards can be seen in Figure 5.

Figure 5: ADS-B Transmitter Threats and Hazards



The propagation path is the most susceptible critical element to threats. The threats can be grouped as ADS-B propagation manipulation and intrusion (T5-T7).

T5. The first threat is 1090 MHz jamming; this would occur in proximity to a ground station (aircraft reception jamming would be more difficult) and aims at increasing the interference level such that detection of ADS-B messages is not possible. This effectively disables the targeted ground station. Depending on the proximity to the ground station the power needed for this type of jamming is low and achievable with limited resources. The 1090 MHz spectrum is already crowded and ground stations receiving transmissions from multiple aircraft already have high interference (each aircraft not currently being received contributes to the interference noise). This threat, therefore, has a severity based on the number of aircraft currently being tracked and whether the aircraft are in airspace that is also monitored through Radar. Until a study is carried out calculating the effect of interference this threat will be assessed as level 3 severity with medium likelihood.

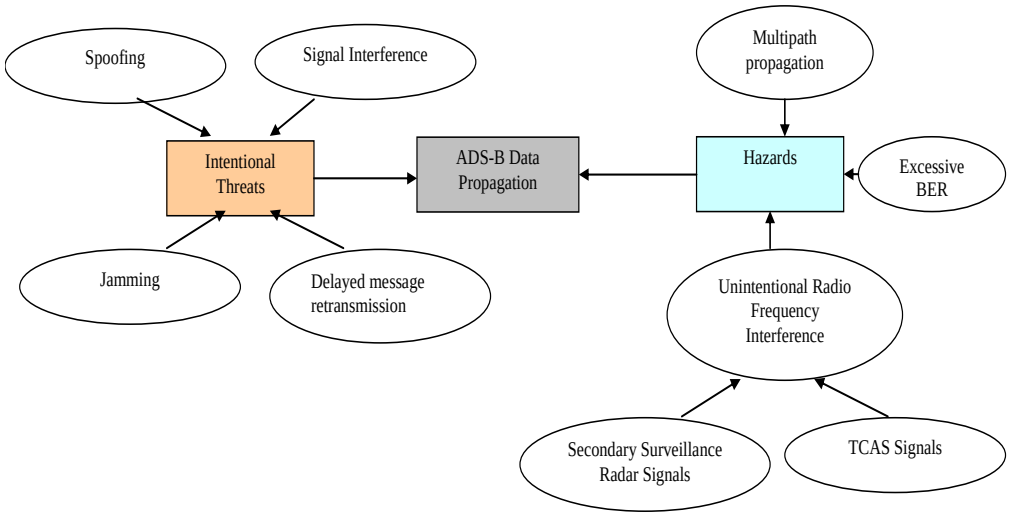
T6. The next propagation path threat is delayed signal retransmission. This occurs when the ADS-B messages are received, delayed, amplified and reradiated by a third party source. This would cause positional jittering of the aircraft. By itself, this is not of large consequence. However, if severe enough the ground station is likely to be disabled, achieving the same as jamming. This is more likely to affect aircraft equipped with ADS-B (IN). The severity of this is assessed as 4 with the likelihood of this threat assessed as low.

T7. The ADS-B signal can be spoofed. This was identified as a large risk to the ADS-B system when the technology was first broached (Dick Smith, 2006) but the hype surrounding it soon evaporated. The spoofing identified was random generation of aircraft designed to conflict with real aircraft in the airspace on the screens of the air traffic controllers. This would cause numerous false collision warnings and general confusion. AirServices Australia was quick to point out that these false aircraft would not have a logged flight plan. Even if this was the case they would simply treat the spoofed aircraft as a real aircraft until its identity could be verified or proven false and removed. The United States FAA have instigated a separate identity verification check involving a front-of-box code set prior to take-off and logged with the flight plan along with a simple time of transmission check to validate range but this to can be artificially manipulated. Australia has no such verification check and relies on the ability of controllers to identify false aircraft in a similar way they would identify false tracks with Radar or the TAAATS system to flag the position report because of the absence of a flight plan. These procedural controls may be somewhat effective for the ATC but the issue remains for aircraft fitted with ADS-B (IN), this is providing the spoofing party is able to generate enough transmission power to influence aircraft reception. This threat severity has been assessed as level 2 with moderate likelihood.

T8. There also exists hazards in the propagation path; these are excessive bit error rate (BER) and multipath reception. The BER effectively limits the range of reception but can be affected by weather and channel noise. Multipath reception occurs when a transmitted signal is received at different times due to a reflection from a building,

mountain range or ground plane causing it to take a longer propagation path to the receiver. The severities of these hazards are assessed as level 2 with high likelihood. A diagram illustrating the ADS-B propagation path threats and hazards is given in Figure 6.

Figure 6: ADS-B Propagation path Threats and Hazards

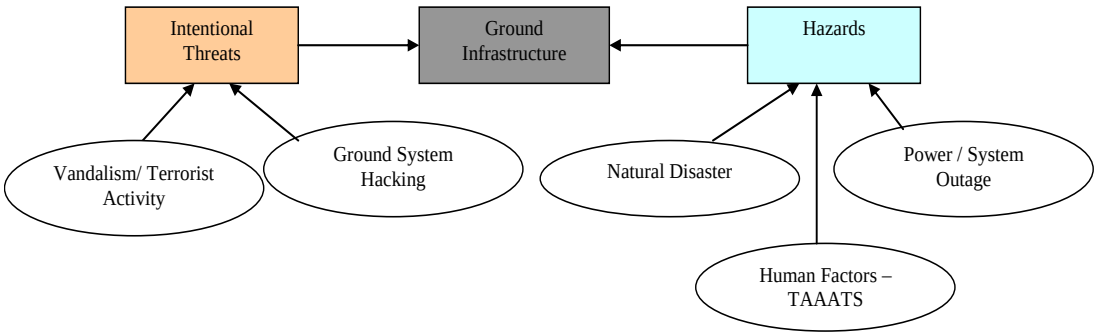


T9. The ground infrastructure is the last critical element and can be separated into two components; Ground station receiver and ATC display system. Each has different threats and hazards. The ground station receivers have been mounted at existing AirServices Australia infrastructure sites. The antenna systems are small and unobtrusive. With ready access to power and communication links. This is also a threat to the receiver, an intentional power or communication disruption would effectively disable the ADS-B receiver along with the existing infrastructure. AirServices Australia has not reported an occurrence of any deliberate attacks on the legacy systems. For a party with enough intent this would be simple, especially on more remote stations. This threat is grouped with deliberate vandalism of the ground station structure as Ground Infrastructure Security and Robustness, and is assessed as level 2 severity with low likelihood.

T10. The final threat lies in internal data manipulation through hacking of the ground station communication network. This would require sophisticated hardware and software and extended access to the network. The system is configured using a virtual private network system and would require network authentication to join the network. This threat has been assessed as level 1 severity with low likelihood.

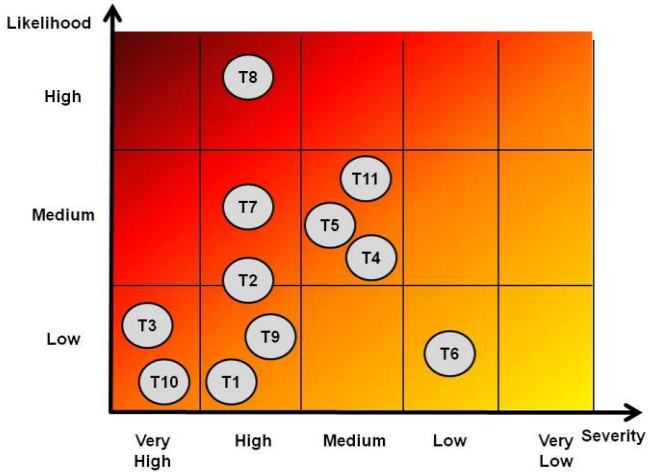
T11. The final hazard lies in the fact that with new technology there is a training latency and limited confidence to procedural changes. The main influence to this is in the display of the different position fixes. The TAAATS system displays different symbols depending on how the position fix was derived. For instance a position fix derived from radar will be annotated with a circle. A class 1 high-reliability ADS-B report position fix will be shown as a four blade propeller design while a fix from a class 2 ADS-B report is shown as a three blade propeller. A computer predicted position fix derived from the logged flight plan is shown using a square. Each of these symbols dictates different required aircraft spacing. This could become confusing and difficult to manage if the symbol changes. Particularly in the face of some of the threats and hazards previously discussed, the procedures used to manage the different symbols and recognising the required spacing requires familiarity with the system. This hazard is deemed to be at level 3 severity and medium likelihood. An illustration of the ground station threats and hazards is given in Figure 7.

Figure 7: Ground Infrastructure Threats and Hazards



A summary of the overall threat assessment matrix is given in Figure 8.

Figure 8: Threat assessment matrix showing likelihood versus severity



Opportunities

In any system there exists the ability for the environment to have a positive effect in the same way it offers threats or hazards. In TOWS analysis these are considered opportunities. These opportunities allow for improvement and refinement of the ADS-B system and will provide means for improving some of the weaknesses and complementing some of the identified strengths. Some opportunities identified for ADS-B are:

O1. The ADS-B system first opportunity arises in the generated market competitiveness for ADS-B avionics. This will reduce the cost of purchase and give rise to the potential for multiple transmitter fitments. It will also drive voluntary fitment which will further improve the ADS-B air traffic system. It is unknown if there will ever be a requirement for multiple transmitter fitment for some aircraft types, particularly in the civil aviation, passenger transport sector.

O2. The ADS-B system will benefit from mature ATC practices, procedures and trainings. The opportunity for instigation of an interactive realistic simulation environment will allow smoother transition to the new technology and promote more comfort with the required separation manipulation.

O3. There are plans to maintain large non-cooperative radar coverage over the dense air traffic areas. This will require replacement of some of the current Radar sites as they degrade with age. This opportunity will provide an ADS-B backup and allow for within range position verification.

O4. The ADS-B system allows for more precise position fixes than Radar but AirServices Australia have made the decision to use Radar position fixes when within Radar Coverage. There exists the opportunity for implementation of some form of ADS-

B/Radar data fusion. This allows for the use of the much more precise ADS-B data when in terminal areas. In parallel with this opportunity that may be implemented with it is the provision for trajectory smoothing and reasonableness tracking. A Kalman Filter implementation can be shown to accurately track an ADS-B trajectory in the presence of ADS-B spoofing and noise. A similar implementation that also allows Radar fusion is a great opportunity for development in the ADS-B system.

O5. Finally it is important that AirServices Australia maintain some technological awareness in the approved GNSS avionics systems for ADS-B. With the development of the Galileo and GPS-III technologies there exists an opportunity for multiple frequency receivers. This will improve the accuracy of the GNSS systems even further by allowing compensation for the largest source of positional error, Ionospheric disturbance. The Galileo system will also improve the reliability of the system by offering a backup in case of GPS malfunction or error.

Weakness

When discussing weaknesses it is important to reiterate that the ADS-B system boundary established incorporates systems from the GPS to the ground infrastructure. The following is a set of weaknesses identified internal to the ADS-B system;

W1. The first assessed weakness is the reliance on Radar position fixes where available for air traffic control. There is a legacy that Radar is preferred even though the accuracy of the position fix is inferior to ADS-B. There is a weakness in the fact that there is no ADS-B/Radar fusion. ADS-B is still considered a backup to Radar especially within terminal radar coverage areas. This is a weakness in the implementation and the ignored precision improvement prevents more efficient procedures due to comfort with the legacy technology.

W2. The next system weakness is the reliance on GPS, in the event of a lack of GPS signal ADS-B is redundant. There is no provision for using inertial sensors for position updates, this partly due to a non-encompassing requirement for GPS and INS carriage on most aircraft.

W3. There is a perceived strength of the ADS-B system against attack, which may in truth, be somewhat of a weakness in its implementation. This may generate a false security and this real weakness needs to be addressed.

W4. It has not yet been identified if there will be a requirement for multiple ADS-B transmitter fitments for some aircraft types. There exists provisions for aircraft flights with unserviceable ADS-B transmitters and the ATC will immediately revert to no-transponder tracking in the event of a failure. This still can be perceived as a weakness of the ADS system.

W5. The ATC rely on the TAAATS system to verify aircraft identity through SSR radar and/or logged flight plan information. A simple identity register similar to that implemented by the FAA in the United States could be used to completely eliminate identity problems. Identity management is a weakness in the ADS-B system.

W6. Further to this is the reliance on controllers to be aware of required aircraft spacing for the different position fix symbols on the TAAATS symbol. This is a further burden on air traffic controllers and in the future, when ADS-B is further accepted, it is likely to become less of a problem as ADS-B should be used as the preferred position fix.

Strength

The ADS-B system also has several internal strengths which can again be argued both technically and analytically. A list of these is included below:

S1. The first internal strength is the inbuilt system error correction methodology in the ground station. The ground station applies error corrections based on a sliding window detection method. There are other boosts to the received signal to help with edge detection, these all aid in reception of ADS-B signals in a high interference environment. There are other potential ground station strengths involving power level triggering and antenna design; they are explained in S2 and S3.

S2. The ground stations implement a minimum power level for triggering of the demodulation software. The minimum level depends on the class of ground receiver and is optimally -84 dBm which gives a probability of reception of 90% (RTCA, 2003). This strength of the ADS-B system limits the effect of multipath propagation which is nominally lower power than the first incident transmission.

S3. There exist ADS-B ground antenna designs that have reception lobes such that they do not receive transmissions arriving lower than a given vertical angle, normally around seven degrees. This is used to limit the effect of ground plane multipath propagation and the impact of ground based jamming and spoofing. There is antenna available that utilise relative detected power of each antenna array to determine an approximate bearing to the aircraft. These are normally 6 segment arrays arranged for 360^{o} coverage which can differentiate the quadrant the transmission arrived from by comparing received power levels. With appropriate software an approximate bearing to the transmission source can be calculated and compared to the transmitted position. Using this technique early detection of multipath false tracks and ground based spoofing can be implemented.

S4. The ADS-B system relies on the GPS position solution for generating position information. Due to this reliance ADS-B trials are being carried out that use GPS monitoring software to reduce the impact of bad satellite transmissions or signal integrity problems (i.e. Ionospheric disturbance). This technology called Receiver Autonomous Integrity Monitoring (RAIM) is used to identify which satellite is providing the bad information and remove it from its position solution. Implementation is being trialled by AirServices Australia and it may become recommended fitment in all ADS-B avionics package installations.

S5. Further to aircraft based monitoring, AirServices Australia has systems in place to reasonably predict GPS system outages and issue notice to aircraft. This monitoring allows for better transition to legacy procedures in the event of a failure. The GPS system is also normally quick in responding to outages, normally measured in minutes rather than days compared with Radar failures.

S6. Due to the small size of ADS-B ground stations, the relatively low power requirement (compared to Radar) and the need for fibre optic communication links ADS-B ground stations have been mounted on existing infrastructure. This gives the ground station some added security measures and often elevates them on Mobile phone towers or VHF antennas or within satellite dish compounds. This strength of the ADS-B system will limit the probability of vandalism. By using existing proven power sources and communication links the reliability of the receiver is improved.

S7. The final ADS-B strength exists in the ATC TAAATS function which is able to generate alerts for position reports that do not coincide with the computer predicted location from the logged flight plan. This strength will automatically flag suspicious reports and improve the robustness of the ATC surveillance system.

Strategic Actions for Remedies

In an attempt to design strategies TOWS matrix analysis is used to produce action plans. The Strategic actions are developed to provide benefit to the ADS-B system as explained in Table 2. The TOWS matrix is separated into two tables for ease of display; they are shown in Tables 4 and 5 and key points for each quadrant are further elaborated in this Section. Each quadrant is assessed as explained in Table 1.

The W-T quadrant of Table 4 is first elaborated in sequence. The W-T quadrant looks at ways of limiting the negative risks to the system. Firstly, the potential for ASD-B attack is real, awareness of such an attack must be raised. The FAA has already instigated front-of-box identity management to help prevent spoofing; this should be adopted in Australia. The development of a suitable training environment would ease transition and aid in procedure development. The risk of GPS receiver or ADS-B transmitter malfunction could be made redundant with multiple fitments. Robust fusion of Radar and ADS-B position data would increase the precision in which aircraft are tracked in the airspace. Utilization of other navigation data available onboard aircraft would increase the safety of aircraft travelling outside radar range in the absence of GPS data.

The S-T quadrant of Table 4 identifies the actions that can be undertaken to mitigate the ADS-B system threats and hazards using the systems internal strengths. This list details six actions that can be implemented to reduce the vulnerabilities identified in the ADS-B system. The ADS-B ground stations all utilise error correction methods to increase range and reduce incorrect reception. The ground station will not receive below a certain power threshold helping to limit the effect of multipath reception. Installation of on-board GPS monitoring along with ATM monitoring should be developed and incorporated. Continuos refinement of the ATC TAAATS system will manage propagation manipulation and ADS-B service interruption though identification of suspicious reports or activity. ADS-B ground station designs involving a six-segment array are available; these arrays can identify ground based non-bearing correct spoofing and limit multipath reception through reception lobe shaping to avoid ground based transmission. Lastly, by placing ADS-B ground stations on existing infrastructure the risk of service interruption, vandalism or network intrusion is limited. The

Table 4: TOWS Table showing ADS-B system Threats Vs Weaknesses and Strengths along with the derived strategic actions

<table>
<tr><td colspan="2">Threats
T_1 – GPS Denial of Service
T_2 – GPS Bad Satellite or Receiver Malfunction
T_3 – Non-cooperative Aircraft
T_4 – ADS-B transmitted data input errors or malfunction
T_5 – 1090 MHz Jamming
T_6 – Delayed Signal Retransmission
T_7 – ADS-B signal spoofing
T_8 – Propagation induced errors
T_9 – Ground Infrastructure Security and Robustness
T_{10} – Internal Data Manipulation
T_{11} – Training Latency with Procedural Change</td></tr>
<tr><td>Weaknesses

W_1 – No ADS/Radar Fusion
W_2 – Reliance on GPS
W_3 – Perceived ADS-B Strength against attack
W_4 – Reliance on Flight Log/SSR for verification
W_5 – No ADS-B Transmitter Back-up
W_6 – TAAATS Symbol Monitoring for separation standards</td><td>W-T
1. Raise awareness of the consequence and likelihood of an attack on ADS-B (W_3, $T_{1,3,4\text{-}7,9\text{-}10}$)
2. Incorporate Identity Verification (W_4, T_7)
3. Establish simulated training environment for training and procedural verification (W_6, T_{11})
4. Multiple ADS-B transmitter or GPS receiver fitments ($W_{2,5}$,T_4)
5. ADS-B/Radar Data Fusion to provide better managed surveillance ($W_{1,5}$, $T_{4\text{-}5}$)
6. Airborne Navigation Backup for ADS-B Transmitter ($W_{1\text{-}2}$, $T_{1\text{-}2}$)</td></tr>
<tr><td>Internal Strengths

S_1 – Error correction methods for received ADS-B signal in ground infrastructure
S_2 – Minimum Trigger Level for reception
S_3 – Received Angle of Transmission gives angle to transmitter and can identify ground based spoofing, also can have 6 quadrant reception for approximate position detection
S_4 – RAIM trials for GPS monitoring on Aircraft
S_5 – Reasonably predict GPS outages (outages in order of minutes not days as with Radar)
S_6 – Ground Stations located near existing hardware are unobtrusive and easily replaced or repaired
S_7 – TAAATS automatically generates alerts for suspicious position reports</td><td>S-T
1. Apply error correction techniques (S_1, T_8)
2. Evaluate minimum trigger threshold (S_2, T_8)
3. Establish aircraft and ATC GPS monitoring system ($S_{4\text{-}5}$, T_4)
4. Continually refine TAAATS system to manage propagation manipulation and ADS-B service interruption (S_7, $T_{5\text{-}8}$)
5. Incorporate more advanced ground station design to limit effect of Multipath and spoofing ($S_{1\text{-}3}$, $T_{7\text{-}8}$)
6. A reduction in vandalism likelihood and improvement of ground station reliability by using existing infrastructure (S_6, T_9)</td></tr>
</table>

W-O quadrant in Table 5 shows how the external opportunities can be used to strengthen the internal weaknesses. Market competitiveness will provide access for increased fitment and chance of multiple transmitter fitments. Tracking, smoothing and data fusion in the ADS-B system will increase robustness and maturity of the ATM and surveillance system. By fitting GNSS receivers with provision for reception of multiple frequencies will capitalise on the Galilleo and GPS-III technologies increased precision capability. Lastly, a robust ATC training environment would enable testing of procedures and development of familiarity with TAAATS symbols required for the new airspace management system with real-time simulations.

Table 5: TOWS Table showing ADS-B system Opportunities Vs Weaknesses and Strengths along with the derived strategic actions

<table>
<tr><td colspan="2">Opportunities
O_1 – Continual Competitive market for ADS-B avionics and fitment will reduce cost giving opportunity for multiple transmitter fitment
O_2 – Mature ATC practices, procedures and training
O_3 – Maintain Large Non-cooperative Radar coverage
O_4 – Potential for ADS-B/Radar Fusion
O_5 – Potential for Reasonableness Tracking/Trajectory Smoothing (Kalman Filter)
O_6 – Maintain Technological Awareness (Galileo, GPS III)</td></tr>
<tr><td>Weaknesses
W_1 – No ADS/Radar Fusion
W_2 – Reliance on GPS
W_3 – Perceived ADS-B Strength against attack
W_4 – Reliance on Flight Log/SSR for verification
W_5 – No ADS-B Transmitter Back-up
W_6 – TAAATS Symbol Monitoring for separation standards</td><td>W-O
1. Continually drive market competitiveness (W_5, O_1)
2. Implement Tracking, Smoothing and Data fusion ($W_{1,3-5}$, O_{3-5})
3. Provision to receive multiple frequencies for GNSS will increase reliability and accuracy (W_2, O_6)
4. Develop ATC simulation environment to verify practice, procedure and offer training (W_6, O_2)</td></tr>
<tr><td>Strengths
S_1 – Error correction methods for received ADS-B signal in ground infrastructure
S_2 – Minimum Trigger Level for reception
S_3 – Received Angle of Transmission gives angle to transmitter and can identify ground based spoofing, also can have 6 quadrant reception for approximate position detection
S_4 – RAIM trials for GPS monitoring on Aircraft
S_5 – Reasonably predict GPS outages (outages in order of minutes not days as with Radar)
S_6 – Ground Stations located near existing hardware are unobtrusive and easily replaced or repaired
S_7 – TAAATS automatically generates alerts for suspicious position reports</td><td>S-O
1. Environmental scanning will reveal opportunities for improvement to GPS monitoring systems (S_{4-5}, O_6)
2. Improving antenna design and ground station decision software will aid reasonableness tracking (S_{1-3}, O_5)
3. Improvement of the TAAATS system through incorporation of ADS-B/Radar fusion, reasonableness tracking and trajectory smoothing (S_7, O_{4-5})</td></tr>
</table>

The S-O quadrant in Table 5 in the TOWS analysis matrix identifies where the internal strengths align with the external opportunities (positive risk) and outlines actions that can be taken for improvement in the ADS-B system. Firstly, continual monitoring of the environment will reveal areas of improvement; it must be remembered that the first implementation is not always best. By investigating ground station designs that incorporate reasonableness tracking a more robust ATM surveillance system can evolve. Lastly the TAAATS system should be improved through addition of ADS-B/Radar fusion, reasonableness checking and trajectory smoothing such that a mature system evolves.

In this analysis, there are two key threats that have no identified strategic action for risk mitigation. These are threats T_3 and T_{10}. The processes used in the event of these threats will be described in order. Firstly, T_3 describes the threat of a non-cooperative aircraft. As discussed, this identifies that the ADS-B transmitter has been turned off or the aircraft is no longer identifiable using ADS-B. In this situation, two scenarios can evolve; firstly is the aircraft still tracked by Radar. In this case an effort must be made to establish voice communication and the aircraft be treated as a high threat. Separation must be established and the aircraft identified prior to interception with any critical national security elements. The second scenario evolves if the aircraft is not currently tracked by Radar, in this case voice communication must be established and a Search and Rescue emergency activated. The second un-mitigated threat (T10) lies in internal data manipulation. This can be treated as a malevolent act and care must be taken to identify the area of breached security. This can be somewhat mitigated through the implementation of a robust security plan and general alertness of air traffic controllers of suspicious activity. Importantly these action items are only recommended courses of action, without an understanding of the full implications of what a study in this area will reveal.

Conclusion

The implementation of ADS-B is moving from the realm of future plans to reality. It is mandated that all aircraft in the Australian airspace flying above 29,000ft be ADS-B equipped by 2013. However, no study – at least in the public academic literature – has attempted to apply a technical assessment of the vulnerabilities and threats. This paper attempted to identify strategic actions using TOWS analysis in a systemic manner. The main contribution of the paper is the vulnerabilities analysis picture painted through the TOWS analysis for ADS-B from a system-level perspective. Future work will include more in depth analysis of some of the threats and gaining better understanding of how to mitigate them. Recommendations are made from the threat identified as T6; that a study is initiated into the effect of 1090 MHz interference to more accurately calculate the severity this threat carries. Next weakness W6 identifies the need for a fully functional ATC simulation environment that can be used for training and procedural verification outside of the airspace. This will improve the confidence of Air Traffic Controllers when incorporating procedural changes from symbol identification using the TAAATS system. Finally time must be invested into developing sound procedures and security measures for the unmitigated threats identified in the strategic actions.

References

ICAO, 2002: The ICAO Global air Navigation Plan for CNS/ATM systems, volume 1. ICAO, Montreal, Canada.

SESAR, 2007: The ATM target concept: Sesar definition phase, deliverable 3. Technical Report DLM-0612-001-02-00, Eurocontrol, Brussels.

NextGen, 2007: FAA Office of Joint Planning and Development, Concept of operations for the next generation, Air transportation system ver 2.0.

RTCA, 1999: Development and Implementation Planning Guide for Automatic Dependent Surveillance Broadcast (ADS-B) Applications. Technical Report RTCA/DO-249, Washington, DC.

ICAO Doc 444: ICAO Procedures for Air Navigation Services. Technical report ICAO 444-RAC/501, ICAO, Montreal, Canada.

FAA, 2000: A. Zeitlin, "The Influence of Safety Assessment on Surveillance Performance Requirements", FAA/EUROCONTROL ASAS TIM, Brétigny, November 2000.

RTCA SC186 WG4: Minimum Aviation System Performance Standards (MASPS) for ADS-B (DO-242), Technical Report RTCA/DO-242A, Working Group #4 of RTCA SC-186, 2002

CASA, 2004: Civil Aviation Safety Authority - Carriage and use of Automatic Dependent Surveillance - Broadcast (ADS-B) avionics, Discussion paper.

Dunstone, 2007: ADS-B: Next generation technology for all airspace users. Flight Safety Australia, Sep-Oct Edition.

JCP, 2007: Joint Consulatation Paper - Transition to satellite technology for navigation & surveillance. Technical report, Australian AirServices and Civil Aviation Safety Authority and Australian Defence Force and Department of Transport and Regional Services.

Smith et al, 2006: "Impact of ADS-B on Controller Workload: Results from Alaska's CAPSTONE Program", 25th Digital Avionics System Conference.

John Hopkins Univesity, 1999 - GPS Risk Assessment, Final Report. Accessed at http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/Research/Other/Article/gps-risk-ass.pdf

EUROCAE, 2005: Safety, performance and interoperability requirements document for ADS-B/NRA application, available at: http://adsb.tc.faa.gov/RFG/ADS-B-NRA%20SPR-INTEROP%20_ED-126_%20v1.0.pdf

Weihrich, 1982 - The TOWS Matrix A Tool for Situational Analysis: Long Range Planning, Vol. 15, No. 2, pp. 54 to 66, 1982

Dorin, 2009: Decision Support System based on MADM for Urban Transport Management, Dorin D.M. Banciu, Monica C.G. Florea - The 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009.

Verweij , 2009: Trends, Developments and State-of-Play in the Transport and Logistics Sector in the EU, Kees Verweij, Igor Davydenko, Xun Li, Govert Gijsbers, Frans van der Zee -DG EMPL project Comprehensive Sectoral Analysis of Emerging Competences and Economic Activities in the European Union, 2009 Available at http://test.uic.asso.fr/IMG/pdf/DG_EMPLOY_REPORT_PART_1_transport_16012009pdf__EN_1.pdf

Upham , 2004: Environmental capacity and European air transport: stakeholder opinion and implications for modelling, Paul Upham, David Raper, Callum Thomas, Mark McLellan, Martin Lever and Arthur Lieuwen - http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VGP-4B4RRNS-4&_user=1975847&_coverDate=05%2F31%2F2004&_rdoc=1&_fmt=high&_orig=search&_sort=d&_docanchor=&view=c&_searchStrId=1419375391&_rerunOrigin=scholar.google&_acct=C000004218&_version=1&_urlVersion=0&_userid=1975847&md5=9825394c877920bd319cad3c0e8390e5_-_affdJournal of Air Transport Management, Volume 10, Issue 3, May 2004, Pages 199-205

Ahmed, 2006: SWOT analysis for Air China performance and its experience with quality, A.M. Ahmed, M. Zairi, K.S. Almarri - Benchmarking: An International Journal, Vol. 13 Iss: 1/2, pp.160 – 173

Zoulissa et al, 2006: Integration of hydrogen energy technologies in stand-alone power systems analysis of the current potential for applications :E.I. Zouliasa, R. Glocknerb, N. Lymberopoulosa, T. Tsoutsosa,e, I. Vosselerc, O. Gavaldac, H.J. Mydskeb, P. Taylord - Renewable and Sustainable Energy Reviews, 10 (2006) 432–46

Cole et al, 2006: Energy storage on production and transmission level: a SWOT analysis, WSEAS Transactions On Power Systems, Vol 1; Issue 1, Pages 31-38

Sarkar et al, 2006: Towards finding a sustainable solution for Arsenic contamination of ground water: A SWOT analysis. Epidemiology- Volume 17 - Issue 6 - pp S218-S219 ISEE/ISEA 2006

Dick Smith, 2006: Potential 'spoofing' of AirServices Australia ADS-B. www.dicksmithflyer.com.au/DS_to_Minister_re_ADS-B_spoofing.php . Letter to The Hon Warren Truss MP, Minister for Transport and Regional Services.

RTCA, 2002: *DO-242A: Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B).*

RTCA, 2003: *DO-260A: Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B).*