

Submission to Safety Review – M Wullemin, January 2014

Dear Mr Forsyth and Panel Members.

My name is Matt Wullemin [REDACTED]
[REDACTED]
[REDACTED]

I believe the terms of reference of your committee may allow matters of the nature below to be examined?

Boeing Electronics Hatch – Accessibility.

While operating as a B777 captain I observed that the electronics compartment access hatch located in the L1 area is not mechanically secured during flight.

See the following for a visual demonstration:

<http://www.youtube.com/watch?v=mLmzvF2qkDY>

In fact, Emirates had actually cut a section of flooring away to enable easy access for ground engineers rather than access the compartment from the external lower-fuselage hatch.

As a captain on these aircraft operating into some of the higher risk airports with passengers of a higher risk profile, this concerned me somewhat.

This design, from all research I have done, is identical to all Boeing wide-body aircraft of 767 and later variants, including the recently certified B787.

The only variation I can identify is the cutting of the flooring material may not have been carried out, or some operators may have unilaterally decided to mechanically secure the hatch under their own risk evaluations.

I researched this issue as part of my Master's thesis (a portion is attached if you wish to examine this further) including contact directly with Boeing and formally raising the matter with several regulatory agencies. I also designed several mechanisms that might cost-effectively reduce the risk of entry in-flight and filed an innovative patent application in Australia.

Most of the responses I received (including the Office of Transport Security, CASA, Boeing, Virgin, Emirates, ACCC and other operators of similar types) were to be honest, disappointing or in fact inaccurate assessments of in-flight defences against the risk I presented.

Of course that was merely my opinion.

Under the risk based/outcome focused regulatory system in Australia, it appeared to me that we were still confiscating liquids, hand creams, nail scissors and other innocuous items (all reactive measures after several events occurred) yet were missing the " elephant in the room".

If I were able to conduct a systems test (without committing an offence) I could easily demonstrate how a malevolent passenger carrying nothing restricted or indeed obviously harmful, could breach all the defences we have and interfere or indeed destroy an airliner in-flight. But no one else seems to share my concerns that can do anything about it.

Advice from other colleagues of mine flying the 747/767 at Qantas, advise me that the hatch is similar and from what they gather, also unlocked on their aircraft. Given your previous experience with QF engineering I am sure you would be able to independently verify these claims?

The anomaly I have now discovered is that the QF/JQ 787's may have a mechanical locking system installed that requires special tools to open. It is thus mechanically secure and removes the risk of unlawful interference. It would appear to me the internal risk assessment systems in Qantas have identified this as a problem and remedied it, at least on their new aircraft.

While this is a great outcome, there are still other affected aircraft flying both on the Australian register (Virgin) and from overseas, notably now code-share partner EK. It seems (fortunately) there has been some desire to address the issue, however I don't believe it goes far enough.

I recently contacted OTS to determine the apparent shift and from where it came. OTS (Peter Robinson) advises there has been no change to the risk assessment conducted in 2010 and they have no reason to mandate the securing of this hatch.

This also seems out of step with the current geo-political climate where Australians are traveling to Syria to fight and Indonesian relations are strained (along with the release soon of several hundred prisoners with terrorist links). But I am not an intelligence expert so perhaps the risk is still low?

I leave it up to you and your team to examine the youtube link I provided to make your own mind up if you would be happy traveling as a passenger on an aircraft with this system exposed.

Any action to minimise this risk, improve in-flight security and thus safety outcomes is what all of us in the aviation industry should be focused on, in my opinion.

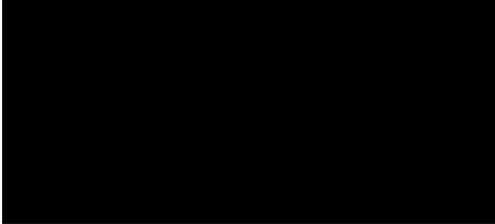
Although this may be more of a security than a safety matter, from the perspective of the traveling public, I don't believe they discriminate between the two. They pay for regulatory protection against both threats and expect a flight from A to B to be as safe and secure as reasonably possible.

The solution I propose is that all aircraft operating into Australia should be required to have the access hatch to the electronics hatch mechanically secured such that it cannot

be accessed in flight by passengers without special tools. There is no need or procedure which requires this area to be available to crew in-flight for any reason I have yet been able to establish.

Yours Faithfully,

Matt Wullemin



Aircraft In-flight Security -
An Investigation Into Potential Weaknesses Of Current Defences

Matthew Wullemin

A thesis in fulfillment of the requirements for the degree of
Masters of Science (Aviation and Technology)

UNSW
AUSTRALIA



School of Science

Faculty of Aviation

June 2013

Originality Statement

'I hereby declare that this document is my own work and to the best of my knowledge it contains no materials previously published or substantial proportions of materials which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of the thesis is the product of my own work, except to the extent that assistance from others in the projects designs and conception or in style, presentation and linguistic expression is acknowledged.

Signed

Dated.....

Disclaimer:

All work submitted is provided in good faith and in accordance with the National Security Legislation Act, 2010 Section 28 below:

28 At the end of section 80.3 of the Criminal Code

Add:

- (3) Without limiting subsection (2), in considering a defence under subsection (1) in respect of an offence against Subdivision C, the Court may have regard to any relevant matter, including whether the acts were done:
- (a) in the development, performance, exhibition or distribution of an artistic work; or
 - (b) in the course of any statement, publication, discussion or debate made or held for *any genuine academic, artistic or scientific purpose or any other genuine purpose in the public interest; or*
 - (c) in the dissemination of news or current affairs.

Extracts of all correspondence with various stakeholders are included to prevent accusation of mis-quote. If any stakeholder believes the author has mis-represented their position on this matter, adjustment will be made.

COPYRIGHT STATEMENT

'I hereby grant the University of New South Wales or its agents the right to archive and to make available my thesis or dissertation in whole or part in the University libraries in all forms of media, now or here after known, subject to the provisions of the Copyright Act 1968. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

I also authorise University Microfilms to use the 350 word abstract of my thesis in Dissertation Abstract International (this is applicable to doctoral theses only).

I have either used no substantial portions of copyright material in my thesis or I have obtained permission to use copyright material; where permission has not been granted I have applied/will apply for a partial restriction of the digital copy of my thesis or dissertation.'

Signed

Date

AUTHENTICITY STATEMENT

'I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis. No emendation of content has occurred and if there are any minor variations in formatting, they are the result of the conversion to digital format.'

Signed

Date

Abstract

The events of 11th September 2001 with the crashing of airliners into buildings lead to a paradigm shift in aviation security, aircraft design and crew operating procedures. The death toll from retaliatory actions precipitated by these events amounts to over 100 000 including almost 3000 killed in the actual events with an estimated financial cost of almost 3.5 trillion dollars to Allied Forces.

A potential weakness was identified in the design of the hatch that covers the electronics compartment in several Boeing aircraft. Located beneath, and accessible from, the passenger cabin, this hatch is unlocked during flight and might permit a potential hijacker to enter the under floor electronics compartment. This compartment contains several 'essential to flight' systems.

This research paper quantifies the risks and evaluates the value of the current defences of this compartment against intrusion. Examination of the ease of entry and defeat of current security protocols and aircraft systems that could be adversely affected are considered in the context of FAA system safety design regulations.

The aircraft manufacturer, several operators and various regulatory bodies were consulted for views and comments. Additionally, a survey to evaluate response from within both the aviation community and general public as to the perceived risk was conducted. The conclusion reached was the risk of interference is low but increasing, and further consideration should be given to mechanically securing the hatch.

Several cost effective solutions (with innovative patent) to address the matter were devised in addition to those commercially available and are presented as options to avoid another costly event such as 9/11. (260)

Table Of Contents

Introduction	pp 7-8
Aim	p 9
Methodology	pp 10-11
Main Report	
Chapter One - Aviation Security	
Background.	p 12
Australian Framework - Policy	pp 12-14
Office of Transport Security (OTS)	p14
Layered Defence	p 15
Chapter Two - Electronics Compartment	
Generic Hatch Design	p 16
Affected Aircraft	p 17
Affected Systems	p 18
Security Systems	p 18
Chapter Three – Video Presentation	
Video Clip	p 19
Chapter Four – Stakeholder Response	
Summary of Comments	pp 20-23
Chapter Five – Defences	
Evaluation	pp 24-26
Chapter Six – Online Survey	
Survey Results	pp 27-28
Chapter Seven – FAA Safety Design Regulations	
Safety Systems – FAR 25.1309	p 29
Failure Probability/Consequence	p 30
Failsafe Concept	pp 30-31
Chapter Eight – Solutions	
Solutions and Options	pp 32-34

Affordable Safety	p 34
Conclusion	pp 35-36
References	p 37
List of Figures	
Fig 1. Aviation Organisational Structure	p 14
Fig 2. Aviation Security – Layered Defence	p 15
Fig 3. General Failure Type – Reason	p 15
Fig 4. Generic Hatch - 747F	p 19
Fig 5. Reason Model Adapted to Security	p 26
Fig 6. FAA Risk Matrix	p 30
Fig 7. Airbus Hatch – KC30	p 32
Fig 8. Airbus Hatch – KC30	p 32
Fig 9. Hatch Locking Design (a)	p 33
Fig 10. Hatch Locking Design (b)	p 34
Enclosure One	
Briefing For Emirates Management – 2011	pp 40-49
Enclosure Two	
DVD – Video Presentation	p 50
Enclosure Three	
Stakeholder Correspondence	pp 51-67
Enclosure Four	
Detailed Response to Hatch (Author/Emirates Engineering)	pp 68-72
Enclosure Five	
Survey Comments, Questions and Results	pp 73-79

Introduction

“Better be despised for too anxious apprehensions, than ruined by too confident security”.

Edmund Burke Irish orator, philosopher, & politician (1729 - 1797)ⁱ

A paradigm shift in global aviation occurred on September 11th, 2001 (9/11) with the hijacking of four large airliners and their flight into buildings in the United States. There have been several cases of commercial aircraft hijack since 1931ⁱⁱ, but this was the first successful attempt to cause large-scale damage to ground infrastructure by an airliner.ⁱⁱⁱ

Standard Operating Procedures (SOPs), for flight crews before 9/11 was to comply with hijacker demands^{iv}. In most cases the intention was not to destroy the aircraft in a suicide mission, but to use it as leverage for political or personal demands.^v

Since 9/11 several agencies have been created to assess, review and monitor security threats to aircraft operations^{vi}. These agencies are required to proactively adjust aviation policies as needed to safeguard the public^{vii}. Aircraft design, SOPs and security protocols have also been modified to prevent a repeat of unlawful in-flight interference.

Specifically, the requirement to fit an impact hardened and lockable door to the flight deck is now mandatory for all aircraft (FAR Carriers, Part 129) carrying more than 30 passengers^{viii}. Video surveillance cameras are now fitted allowing flight deck crews to examine the forward galley area for loitering passengers.^{ix} SOPs have been modified limiting cockpit access inflight.^x Regardless of actions within the cabin, flight deck crew will no longer open the cockpit door if other crew or passengers are under duress or even threat of death. The control of the aircraft must be maintained as; *‘the needs of the many, out-weigh the needs of the few (or one)’*.^{xi}

In Boeing airliners of B767 or greater size, including the new B787, the electronics compartment under the main cabin floor has an access hatch located just inside the L1 (left forward) door, under the cabin flooring material. Aircraft are delivered from the Boeing factory with this hatch unlocked^{xii} and from available research this is how it remains on many aircraft in service.

Located in this compartment are systems essential to the operation of the aircraft including flight control and navigation computers, crew gaseous oxygen systems and importantly the power supplies, for the now mandatory cockpit door and video surveillance cameras. There is potential for a passenger to remove, lift or cut through the flooring material and access this area with potentially catastrophic results.

Given the aim of these new protocols and systems (at a cost of over \$36 000 per cockpit door)^{xiii} is to prevent access to the flight deck, an alternative method of defeating these defences may not have been adequately addressed.

Using the FAA probability/consequence matrix used in systems safety design for guidance, based on actual hijack attempts and possible consequence of hull loss, there would appear a requirement to further minimise risk. A method that completely satisfies the FAA concept is mechanical locking of this hatch.

Although the risk of unlawful interference via the access hatch from within the cabin area may be low, the consequences of any breach are severe. As such a cost effective method of mechanically securing the hatch should be investigated.

Aim

The aim of this paper is to promote further discussion on proactively improving the resistance to unlawful attack on commercial airliners. To achieve this the research will:

- a. Gather information on aircraft affected by this design issue,
- b. Investigate methods and ease of access to the electronics compartment,
- c. Evaluate systems potentially affected by unlawful interference,
- d. Discuss safeguards with relevant stakeholders under current procedures, legislation and protocols,
- e. Evaluate the risk/consequences in accordance with FAA design standards^{xiv} (using the rate of unlawful hijack attempts), and
- f. Suggest possible additional methods of reducing risk in accordance with the 'Affordable level of safety/As low as reasonably practicable' principle. (CASA).^{xv}

Methodology

Thesis methodology includes:

- a. Use of Internet and published resources, such as technical manuals to gather:
 - i. Information on the design of the hatch system,
 - ii. The basis of this design (location rationale),
 - iii. The number of aircraft affected, manufacturer and any operational differences with the installation to customers, and
 - iv. Systems located within the compartment.
- b. Construction of a short video clip of the hatch, its location and the aircraft systems within the compartment. This video:
 - i. Better describes the issue to stakeholders (in later discussions) for clarity,
 - ii. Ensures the information is as freely available to the general public as it would be in reality, and
 - iii. Does not contain any confidential information that may be protected under legislated obligations as an ASIC holder^{xvi}.
- c. Contact with several stakeholders to elicit both opinions and facts and if this hatch presents a concern to in-flight security. Stakeholders include:
 - i. Boeing Commercial Aircraft (Manufacturer),
 - ii. Airbus Industries (Manufacturer),
 - iii. Emirates Airlines (B777 Operator),
 - iii. Coventry University, Royal Aeronautical Society (Security experts),
 - iv. Department of Infrastructure and Transport (Office of Transport Security),

- v. Civil Aviation Safety Authority/s (Regulator),
 - vi. Australian Transportation Safety Bureau (Safety),
 - vii. Government Ministers as available,
 - viii. Australian Competition and Consumer Commission (Consumer Protection),
 - ix. Transport Workers Union (Occupational Health and Safety),
 - x. Virgin Australia (B777 Operator), and
 - xi. Other aviation professionals (Pilots/Cabin/Engineering crew).
- d. A brief survey conducted using publically available third-party resources (SurveyMonkey™). This method is used by Boeing to elicit responses from customers and was distributed to several social media sites, colleagues and the general public.

Main Report

Chapter One - Aviation Security

Background.

The death toll from the events of 11th September 2001 is estimated to be over 100 000 (including the 2 973 killed in the actual 9/11 attacks). The total financial cost so far to Allied Forces is around three trillion dollars^{xvii}.

The general trend in *accidental* aircraft hull losses is actually reducing. This has produced some of the safest years on record (down to around 0.02 – 0.04 hull losses per million departures)^{xviii}. Aviation is therefore actually becoming safer excluding unlawful interference events.

In contrast, IATA data indicates the number of terrorist *attempts* on civil aviation has steadily increased since September 2011^{xix}. If the seven subsequent events (including the seven airport bombing incidents) had been successful in destroying an aircraft the incident rate would exceed that of the accident rate since that time¹.

Australian Security – Framework and Policy.

In Australia the *Air Navigation Act 1920*^{xx} ratifies compliance with the standards and recommended procedures (SARPS) from the ICAO *Chicago Convention, 1944* security protocols^{xxi}. The *Aviation Transport Security Act 2004*^{xxii} was enacted following new legislation in the United States post-9/11. Specifically the *ATS Act 2004* covers features of aircraft security systems^{xxiii} and gives authority in case of a security incident that covers both Australian and Foreign registered aircraft.^{xxiv} The *Aviation Transport Security Regulations 2005*^{xxv} were introduced to support practical implementation of this *Act*.

Subsequent to this legislation the Australian Government produced the *National Aviation White Paper 2009* to establish what is now, the current division of responsibility for aviation security, safety and compliance agencies.

The Government's policy statement is:

¹ See Chapter Seven for calculation basis.

‘Aviation is critically important to Australia and the Government is committed to ensuring that it remains as safe as it can be. Safety remains the number one priority of the Government in aviation’

National Aviation White Paper, 2009^{xxvi}

Further to this White Paper, the Government introduced the *National Security Legislation Amendment Act 2010^{xxvii}* dealing specifically with terrorism (of all types). On January 23rd, 2013 Prime Minister Gillard released *Australia’s National Security Strategy^{xxviii}* that acknowledged:

‘The events of 11th September, 2001 as the most influential national security event in our recent history’.^{xxix}

Agencies. A functional diagram of the responsible agencies tasked to accomplish the Governments strategic goals of safe and secure air transport is detailed below:

- a. The Department of Infrastructure and Transport (Office of Transport Security - OTS) is responsible for security,
- b. The Australian Transport Safety Bureau (ATSB) is responsible for investigating accidents and incidents in an independent manner (note the line directly to the Minister), along with recommendations to prevent re-occurrence, and
- c. The Civil Aviation Safety Authority (CASA) is responsible for aviation safety regulation, licensing and compliance.

ICAO also recognise the strategic importance of innovation to the future of aviation safety and security² and an Aviation Security Innovation Symposium will be held in 2014: *‘To bring together State officials responsible for aviation security, international organisations and a wide range of industry stakeholders to discuss and endorse strategies to enhance the effectiveness and efficiency of aviation security technologies and processes’*^{xxx}.

² As stated in Statute 600 Public law 107-71 44905, (H) - already discussed.

Figure 8.1: Layered aviation security system

Source: Office of Transport Security, DITRDLG.

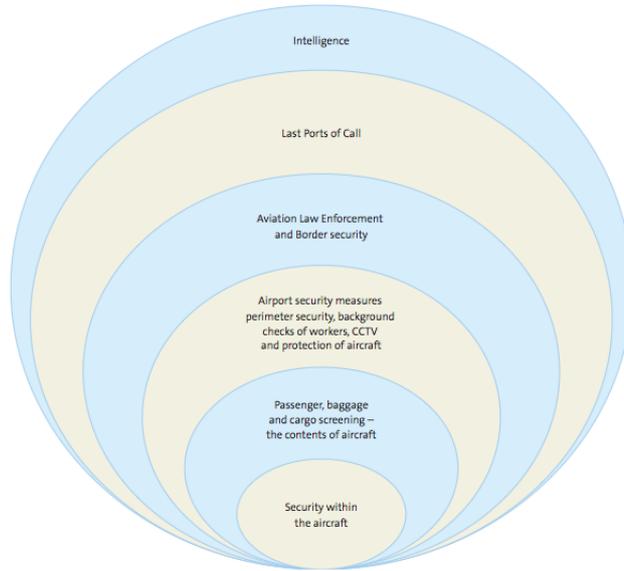


Fig 2. Use of layered defence system for aviation security

It is the last of these areas, ‘security within the aircraft’ that will be considered further. Adapting the Reason model (‘Swiss cheese’), from safety to security leads to the last line of defence (the final rectangle) against unlawful interference. This is analogous to the electronics compartment hatch.^{xxxii}

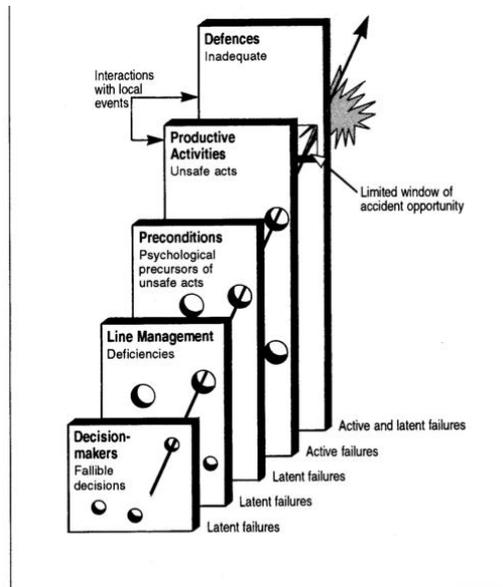


Figure 4-2. Modified version of James Reason's model of accident causation, showing the various human contributions to the breakdown of a complex system
(Source: James Reason, *Human Error*, 1990. United Kingdom: Cambridge University Press)

Fig 3. Use of the Reason Model for Aircraft Security.

Chapter Two – Electronics Compartment

Design - Electronics Compartment.

The electronics compartment of most modern jetliners has historically been located under the floor area beneath the flight deck.^{xxxiii} This area contains essential aircraft systems³.

Aircraft manufacturers normally design several (3) methods for entry to this area^{xxxiv}:

- a. Normal entry, from a hatch located under the fuselage that allows ground crew access for maintenance,
- b. Cargo compartment access from a door located on the forward (left or right) under-floor bulkhead, and
- c. Cabin access via a hatch located internally on the aircraft floor.^{xxxv}

Normal Entry.

All aircraft (Airbus and Boeing) have features at paragraph a. However, airside of an airport is a highly restricted area and ladders or steps are required for hatch entry.

Therefore access without observation is probably quite low. Some operators also use tamper evident seals to cover the external hatch handle.^{xxxvi} These items are held by maintenance, hence during a pilot pre-flight inspection there is visible proof of unauthorised access.

Cargo Compartment.

Access to the electronics compartment from the cargo compartment in most civilian aircraft has already been evaluated as an intrusion risk. This door is now mechanically locked such that it can only be opened from within the electronics compartment.^{xxxvii}

Cabin Access.

Airbus. Airbus aircraft have the electronics compartment access hatch located within the aircraft flight deck. That is, behind the now hardened flight deck door. Airbus aircraft are not vulnerable in this manner and are discarded from further consideration.

³ Also known as the 'lower 41', electronic equipment compartment, electronics bay.

Boeing. Since the B747 flew in 1969^{xxxviii}, Boeing has used a similar electronics and equipment (E/E) hatch in this and all B767, B777 and B787 (i.e. wide-body) aircraft. This hatch was originally manufactured by Triumph Composites (formerly ALCO) in Seattle; later acquired by Boeing.^{xxxix}

Enclosure One is a briefing prepared in 2011 from earlier research. The various photographs (Encl. p 5/p 44, Flag One) indicate the general design of the electronics hatch. Boeing has publically released photographs of the hatch system for the B787 that appears identical (Encl. p 8/p 47, Flag Two).^{xi}

E/E Hatch.

Research indicates aircraft are released from the Boeing factory with this hatch having no factory fitted locking mechanism.⁴ The cover is sometimes removed during the certification process to allow flight test equipment (FTE) to communicate with the onboard systems^{xli} and may explain why it remains in this position in later designs. Located in the same area since early B747 certification, the hatch redesign and movement may be impractical or costly.

Affected Aircraft. The number of aircraft affected⁵, all of which are Boeing aircraft are listed below:

a.	767 in operation (Jul 2012):	844
b.	747 (-400 only considered):	694 (with 106 orders for 747-8)
c.	777 (delivered/ordered):	1315
d.	787	50 delivered (890 ordered).
	Total aircraft fitted with this type of hatch	2 743 ^{xlii}

Systems.

Examples of aircraft systems located within this compartment are:

- a. Crew (gaseous) Oxygen cylinder,

⁴ If one is actually available is unknown. Boeing did not reveal this information (Caley, K).

⁵ Only passenger aircraft have been considered.

- b. Navigation Equipment;
 - i. Inertial reference systems (IRS),
 - ii. Air data systems (ADR), and
 - iii. GPS/Autopilot/Autothrottle computers,
- c. AIMS computers (databus systems or ‘neural network’),
- d. Flight control cable runs and computers (FCCs),
- e. Aircraft circuit breaker panels, and
- f. Flight deck security systems comprising the;
 - i. Flight deck surveillance cameras (FDC), and
 - ii. Flight deck door locking system (FDD).⁶

There are several other systems, however those above are significant for aircraft control, navigation and security. All computers use backplane power systems and are designed as quick line replaceable units (LRU) and easily removed.^{xliii}

Security Systems.

The FDD system is fail-safe. If depowered, the locks to the flight deck door de-energise to a relaxed state to permit access to the area if the door is shut with no crew inside the flight deck. A switch located inside the flight deck area also disarms the system for ground operation.^{xliv} The FDD system is energised during the pilot’s pre-flight cockpit checklist and de-energised on flight completion.^{xlv} If despatched with the power supply unserviceable, or interrupted, the door can be mechanically locked internally if required^{xlvi}.

⁶ Airbus nomenclature is CDLS or CDSS for the same systems - as designed by Goodrich. A330 FCOM.

Chapter Three – Video Presentation

Video Clip

A DVD (Enclosure Two)⁷ visually describes the information on the location, operation and construction of the hatch. Affected systems are presented in summary form.⁸ On occasion, passengers boarding via the L1 door have observed engineering crew conducting maintenance work with the hatch open⁹. At this time, use of personal video equipment is not restricted^{xlvii} and this information is freely available to the general public. It is suggested the reader view the clip [link] for clarity before proceeding.

In this example aircraft [an A6-registered B777], the flooring material is specifically cutout to allow access to the electronics bay. It should be noted that not all operators have this area cutout¹⁰. Generally, the area is covered with one-piece material (carpet or linoleum). As stated earlier, regardless of the covering, the hatch is delivered in an unlocked state [Boeing, Caley K].

Access to this area in flight by removing the covering, cutting through, or lifting the material may be possible.

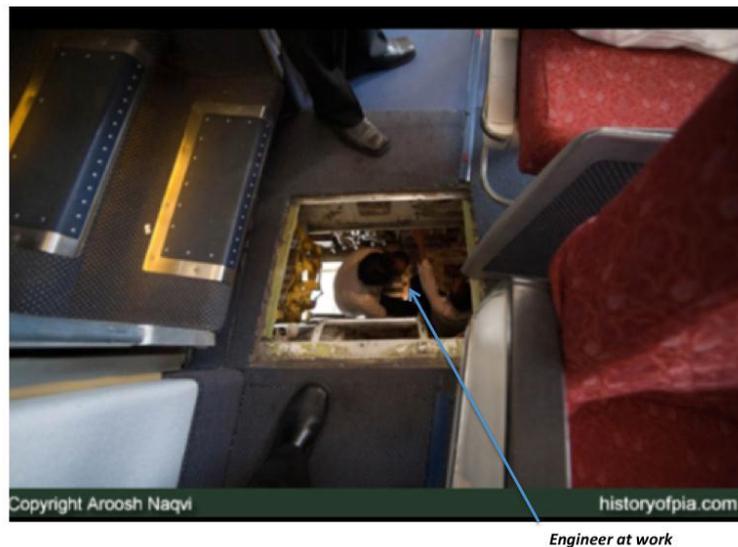


Fig 1. Access hatch B747F – courtesy Aroosh Naqvi

⁷ Also see <http://www.youtube.com/watch?v=mLmzvF2qkDY> for online version.

⁸ All of the information on the DVD was gathered legally and is not subject to restriction under any known protocol.

⁹ Author personal observation of crew oxygen bottle changeover.

¹⁰ From both personal experience and general conversation with fellow pilots in other Airlines.

Chapter Four – Stakeholder Response

Stakeholder Response

Several stakeholders were requested to comment on the issue. A consolidated list of emails and responses is at Enclosure Three and summarised below¹¹.

Boeing Company.

Dr Lou Mancini, VP Boeing Commercial Airplane, (via TELCON with the author and Boeing representatives), Mr Ken Caley (Director, Flight Operations and Services) and Captain Linda Orlady (Chief Test Pilot) were contacted. The comments from BAC are:

‘This matter has been considered and brought to operators for consideration in the past (FAA airworthiness directives do not require this hatch to be locked) hence no further action is required. This is an operator’s choice of configuration and concerns should be addressed to the operator’.

Coventry University/RAeS.

Professor N.L. Shanks¹² is a well-respected aviation security lecturer and was consulted for further advice. Professor Shanks states:

‘You have clearly identified a serious ‘design’ error which has been compounded by the modifying of the floor covering to allow ease of access and also brings this area into clear view. I agree with you that this represents a potential problem that if easily addressed at low cost should be followed up’. ^{xlvi}

Tim Robinson editor for the Royal Aeronautical Society Journal provided the following comments:

¹¹ *Italics* are quoted **red** in correspondence.

¹² <http://www.linkedin.com/pub/norman-e-l-shanks/5/513/a36> for biographical details.

‘Possibly a security loophole that could be exploited by someone with the right knowledge and experience... It does seem odd that a simple lock would probably suffice in averting most of the threat?’

Emirates Airline.

Enclosure One was presented to Mr Tim Clark, President, Emirates Airlines, mid-2011 Mr Andrew Hoad, Divisional Vice- President, Emirates Engineering responded.

Access to the area was considered low risk due to several factors:

- a. Cabin crew monitoring the area, and
- b. Camera surveillance,

Emirates considered the possible requirement for crew to access the area should there be a ‘*small*’ in-flight fire. Research indicated there is no procedure, checklist or protocol (manufacturer, regulator or operator) to support this latter position. In fact, Emirates Operations manuals (at that time) specifically prohibited crew accessing this area in flight.^{xlix} Emirates amended the Operations manual recently and re-phrased the section to ‘*enter only in an emergency*’^l.

This contradicts Boeing which state ‘entry to the electronics compartment in flight is not recommended’.^{li} A detailed response is at Enclosure Four.

Department of Infrastructure and Transport.

Mr Paul Retter was advised of concerns and followed up the issue with his staff (Skelton, G). The final response received from OTS, (after correspondence with Hon. Tony Albanese, Minister for Transport), was;

‘This matter was not considered to be one requiring further attention by the Department’.

Civil Aviation Safety Authority/s.

CASA were included in all correspondence, however they deferred to OTS for decisions on this issue. Comment was also sought from the United Arab Emirates

Civil Aviation Authority (GCAA) as the example aircraft is an A6-registration. The UAE GCAA (Mohd. Al Mansouri) also holds the chair for ICAO airline security and the seminar on the matter due to be held in 2014.^{lii}

No response has yet been received from the UAE GCAA.

Government Ministers.

A request for comment was sent to The Hon. Tony Albanese, Minister for Transport. Similarly, Senators Nick Xenaphon, Helen Kroger and Don Randall (MP for Swan) were also contacted. Senator Xenaphon's interest in the matter is ongoing. The Minister responded via the Department of Infrastructure.

Australian Competition and Consumer Commission.

The ACCC has powers to control airline ownership and protect consumers (*Trade Practices Act, 1974*).^{liii} The ACCC advised:

'Air travel (i.e. aeroplanes) are not a consumer product as defined in the Act', and deferred any comment to the OTS.

Australian Transportation Safety Bureau.

The ATSB was provided with an online REPCON¹³ describing the issue. The ATSB (Hargreaves, E) advised:

'As the matter had already been presented to OTS, ATSB would merely ensure that OTS had received the information' and additionally advised; 'That although ATSB have a research function, this does not include security research'.

Virgin Australia.

As the only Australian operator of the B777¹⁴, Virgin Australia was asked for comment. Mr Stuart Aggs', (General Manager Safety Systems) response was very similar to the reply received from Emirates Airlines:

'The OTS, and US TSA have assessed the risk of unlawful interference with aviation via the use of this avionics bay as low'

¹³ Confidential Report

¹⁴ Jetstar and Qantas will take delivery of B787 aircraft later in 2013. As the 747-4 and 767 are being slowly retired Qantas was not approached for comment on these types.

Informally however, Virgin cabin crew and other security staff had expressed concerns regarding the hatch in conversations during emergency refresher training.^{liv}

Transport Workers Union (Occupational Health and Safety).

The TWU has a responsibility to aircraft cabin crew and others staff associated with aviation with respect to OH+S. Currently, small knives on the prohibited item list is under review by the FAA. This has generated concern within cabin crew and airline management.

The matter is now tabled for discussion between the TWU and OTS in future meetings (Rocks, M).

Chapter Five - E/E Defences

Defences.

Defences cited (by OTS, Virgin and Emirates) preventing unlawful access from the cabin to the E/E compartment are:

- a. The covering of the area with carpet or linoleum,
- b. The fact the area is located near a crew seating position (L1),
- c. The monitoring of the area by crew (galley),
- d. The cockpit video system, and
- e. The screening of passengers for prohibited items (knives)¹⁵.

Covering.

The floor covering is optional depending on operator (Caley,K). As shown [Encl.1, p 5/p 44] the cutout panel reduces the defences at paragraph a. As cited (Hoad, A) the cutout is to provide the crew opportunity to fight a small in-flight fire. Research indicates this reason is unlikely as it is not standard procedure. The utility to perform engineering work on the ground via this access method appears the only identifiable purpose. No other operator than the example aircraft was found with this design. Logic suggests if required by airworthiness (fire fighting, a documented checklist or 'best practice') all aircraft might have the same design but do not.

Crew Seating.

The hatch area is located in the forward galley. Normally there would be a crewmember in this area to monitor galley equipment.^{lv} However anecdotal (and actual experience) shows the duties in the cabin often take crew away from this area. Unless there is a specific crewmember nominated for security duties^{lvi} then the area may be left unattended for significant periods of time.¹⁶

¹⁵ Enclosure Four discusses all these elements in further detail.

¹⁶ Personal observations of up to 20 minutes over several flights.

Flight Deck Camera.

The cockpit video system (FDC) consists of three cameras located in the forward galley area and near the flight deck door. These are obvious to any passenger and could easily be defeated using something such as a sticker, 'Post-It Note' or a small can of spray paint (as permitted under LAG restrictions)^{lvii}. Additionally, pilots do not monitor these cameras as a standard operating procedure.^{lviii} The cameras are only activated when a request for cockpit entry is made, or on a random interval. Camera information is shown on the forward display units (DU) or electronic flight bag (EFB) on the side consoles.^{lix} Operational information is suppressed when active. The flight deck crew therefore do not continuously monitor galley activity.

Screening – Prohibited Items.

The list of prohibited items (FAA/OTS) varies between ICAO signatories, but generally, the carriage of knives or weapons is banned.^{lx} The FAA/TSA has recently indicated relaxing the restriction to carry knives with blade length of <60 mm.^{lxi} Relaxation of this regulation would permit a Swiss army knife (for example) into the cabin. This has already created some discussion from cabin crew unions (Southwest), Delta Airlines (CEO) and others.¹⁷ The ability to cut through the floor covering may then be possible.

Tests using carpet and linoleum by the author found that the can opener on a standard Swiss army knife cut linoleum and carpet up to standard indoor/outdoor type as usually fitted to this area, with ease. The flooring can also be cut using other *permitted* items, including wallpaper or fabric cutters (the round 'pizza' wheel type).

Notably, after time the outline of the floor hatch becomes obvious as traffic wears a visible pattern over it.^{lxii}

All these factors could contribute to a breach by a knowledgeable and malevolent passenger.

¹⁷ Currently there are over 400 000 signatories to 'no knives on planes' to resist this change by the TSA.

Adapting the Reason model, latent general failures (regulatory oversight) combined with error producing conditions (crew inattention) and inadequate defences (unlocked hatch) could lead to a security breach.

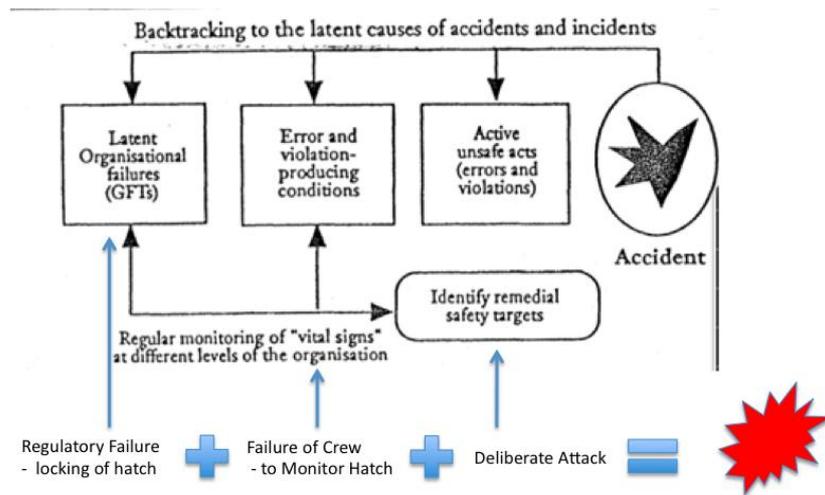


Fig 5. Use of the Reason Model Adapted to Deliberate Security Incidents

Chapter Six – Online Survey

Survey Results.

A ten-question survey¹⁸ was constructed and spread to as many social media outlets as possible. The results were directed to aviation and non-aviation sectors, general public and specific aviation websites. Total response was small with only 32 respondents and a total of about 120 viewings of the video clip. The survey questions and results are tabled at Enclosure Five and analysed below in summary form¹⁹ with explanatory comments by respondents to some questions.²⁰

Q1-4. From those who viewed the clip and answered the survey, 85% left contact information for follow up. The majority (80%) were involved in aviation. Of respondents:

- i. 80% were pilots,
- ii. 4% cabin crew,
- iii. 8% management, and
- iv. 8% engineering.

Q5. Regarding security concerns, responses were:

- i. Low concern 10%,
- ii. Medium/high concern 75%, and
- iii. Severe concern 15%.

Q6. Defences against hatch penetration were assessed as:

- i. Somewhat or completely inadequate 87%,
- ii. Adequate 0%.

Q7-8. In respect to prohibited items, responses indicated the list was:

¹⁸ See <http://www.surveymonkey.com/s/THHX32D>

¹⁹ Rounded values, not all questions answered.

²⁰ Grammatical corrections only applied.

- i. Inadequate or weak 80%, and
- ii. With respect to the proposed changes by the FAA (to allow small knives on board), most respondents were already concerned so did not alter their answers (87%),
- iii. Those not concerned was 13%.

Q9. The case for locking the hatch, given no valid operational reasons to leave it unlocked, was over 93%.

Q10. When assigned a cost to lock the hatch the responses to the locking case was still 93%.

Apart from a small percentage of responses, the results indicate merit in examination of the matter further. Concerns appear significant at an operational level (crew/passengers) and greatly divergent from the comments of other stakeholders.

The conclusion is this is a matter requiring further attention.

Safety Systems and Design – FAR 25.1309

The FAA is the airworthiness approval authority for the aircraft types in question. Application of safety design regulations [FAR 25.1309] may indicate grounds for further consideration with regard to the E&E hatch.

FAA regulations define fail-safe as the primary means of risk mitigation in system design. That is, any single element during flight (from brakes release) is assumed to fail *regardless* of probability.^{lxiv} Therefore redundancy is required to meet safety design regulations.^{lxv}

Consequence (c)

Catastrophic (hull loss) system failures require consideration if;

- a. There is one catastrophic failure per aircraft during its design life, or
- b. One failure per aircraft of a particular type.^{lxvi}

Probability (p)

The probability (p) of these events is quantified as;

- a. ‘Probable’ as more than 1×10^{-5} (one in 100 000),
- b. ‘Improbable’ as between 1×10^{-5} and 1×10^{-9} , and
- c. ‘Extremely improbable’ as less than 1×10^{-9} .^{lxvii}

Consequences of Hatch Breach - c

Although there have been no actual breaches of the hatch as yet, it would be reasonable to assume a catastrophic outcome given the results of 9/11. This would only have to occur on any one of the 2 743 aircraft soon to be operating to satisfy the FAA definition above.

Probability of Hatch Breach - *p*.

Total departures of this aircraft type are estimated at approximately 17.5 million²¹ since 9/11. Given there have been no *successful* repeat attacks since that time the four aircraft involved were destroyed at a rate of 0.23×10^{-6} (or about one in 4.3 million departures).²² This value falls within the FAA ‘improbable’ range of 1×10^{-5} to 10^{-9} in this context.

To quantify the potential risk other hijack attempts (7) are included.²³ IATA data indicates the number of terrorist *attempts* on civil aviation has steadily increased since September 2011^{lxviii}. If the seven subsequent events (including the seven airport bombing incidents) had been successful in targeting an airliner, the incident rate now becomes 18 per 17 500 000 departures, approaching FAA ‘probable’.

Applying the FAA risk treatment matrix to *p x c* above, the position of a hatch breach is now plotted:

Figure 1: Probability vs. Consequence Graph

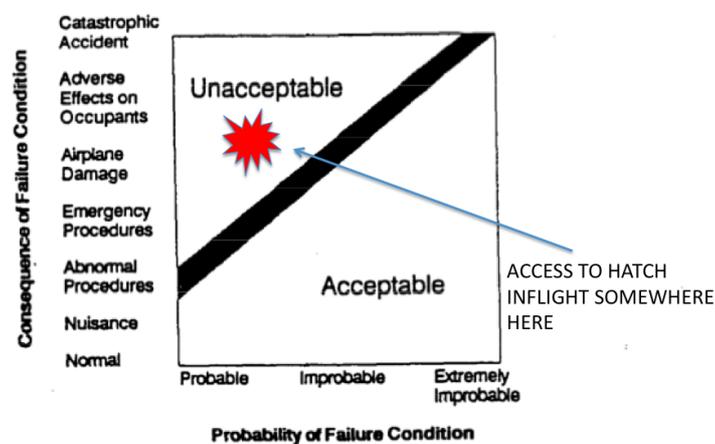


Fig 6. FAA Risk Matrix – hatch risk plotted.

Fail Safe Defences.

Using this systems safety design methodology, the list of defences (at Chapter Five paras. a. to e.) supporting the argument for hatch access, has a number of elements that rely solely on human defences. Human defences have already been discussed to

²¹ 2 000 aircraft (no 787s), 2 sector days, 365 days for 12 years: maximum 17.5M departures.

²² Incidentally, ten times the current hull loss accident rate of 0.02 to 0.05/m departures.

²³ Not including 7 events at airports with explosives.

be of limited 'fail-safe' value. It is therefore possible at least one of these human defences could fail and reliance on mechanical defences becomes necessary. The only mechanical defences are the flooring (if intact) and the hatch (if locked).

Chapter Eight - Solutions

Solutions and Options.

There are several solutions that could be used to secure this hatch. Examination of patent information shows a similar mechanism to the cockpit door could be installed into the floor hatch. A system already exists with Airbus for a hatch covering the rear bulk hold. These solutions are regulator approved and already available with modification²⁴.



Fig 7. Airbus Hatch For Aft Cabin Flooring - locking handle in view (KC30 RAAF).



Fig 8. Airbus Hatch – Closed.

²⁴ However, given Airbus possibly hold design rights, Boeing may be reluctant to use a competitors system – speculation.

Several other simpler and cheaper designs or methods could also be installed.

Option A.

Locking the hatch from the under floor area, as has been done to access via the cargo compartment. Given some utility to access the hatch from an engineering perspective and the concerns (albeit shown to be not practical), to fight in-flight fires, the ability to open the hatch externally is seen as having some merit.²⁵

Option B.

Enclosure One describes patented designs for several methods that would allow a cost effective system to be installed²⁶. A small plate could be installed over the hatch handle and 'coded head' screws with the correct driver bit (unique to each aircraft) held within the cockpit. These could be secured in lockable containers already fitted to the aircraft.

The plate would restrict the handle being lifted, yet with the screws released slightly, the plate would swing free and allow handle movement. This mechanism would also provide the last layer of defence against unlawful access.



Fig 9. Design (a) hatch handle prevented from lifting upward - coded screws in place.

²⁵ A Royal Brunei 777 diverted to an airport with no steps – the crew tried to use the hatch to exit the lower fuselage but found the hatch locked. Shillington, M, Pilot.

²⁶ Provisional Patent Application 2011902182 for these designs is not included in this thesis but is available on request. The figures illustrate the concept better than patent jargon.



Fig 10. Design (b) hatch handle with slotted plate in place – sideways movement frees handle.

Affordable Safety.

Previous CASA safety management systems used the concept of ‘As low as reasonably practicable’ (ALARP) to determine cost/benefit implications for imposing regulations.^{lxix} Given the obvious element of risk in aviation, there is a level of regulatory compliance above which the cost outweighs any incremental improvements in safety. This has resulted in the change to ‘affordable level of safety’ (ALOS).^{lxx}

Option A would possibly be the cheapest solution, however any utility to open the hatch would be lost. The Airbus hatch design could be quite expensive due to proprietary issues, as would the system used in the cockpit door.

It is estimated Option B would cost less than \$10 000 to design,²⁷ approve and manufacture and could be fitted during a turnaround flight (sub-two hours) with minimal downtime or training costs to install or operate.

²⁷ The hardened door cost upward of \$36 000 per aircraft so this system integrated into the hatch would probably be as costly and complicated to install.

Conclusion

'Life is full of risks, if you don't like risk my friend, then you shouldn't be living'

Unknown CEO- CNBC 'Meet the Leaders'

The complex socio-technical nature of aviation involves many hazards for which various stakeholders attempt to minimise. Some risks can be predicted and designed out of a system while others are less predictable, especially when dealing with human interactions.

The events of 9/11 demonstrated the paradigm shift in the nature of skyjacking as the perpetrators sought merely to create terror and destruction with no other seemingly rational motives. These events cost a vast amount in both human and financial toll and continue to do so.

Security agencies tasked to assess risks and threats to aviation must balance the freedom enjoyed by air travellers with financial viability of operators, yet ensure security is not compromised.

The implementation of a hardened cockpit door and video system to prevent a reoccurrence of 9/11, and limiting items from carry on luggage has reduced the risk of unlawful interference, *but not* the frequency of attempted attacks.

One area of weakness is the access hatch covering the electronics compartment and systems vital to the safe operation of several thousand Boeing Airliners. The Boeing Aircraft Company has been building aircraft with a similar hatch cover since 1969 and continues to do so on the new B787. Boeing wide-body aircraft are delivered from the factory with this hatch unlocked and in some aircraft a panel is specifically cut out allowing access to the compartment in-flight. Information is publicly available online describing the cockpit defences and systems located within this compartment.

This hatch may therefore be accessible inflight to a knowledgeable and malevolent passenger with catastrophic consequences.

Defences against intrusion cited include the use of cabin crew to monitor the area, (which is located in sight of passengers) and video monitoring by the flight deck

crew. However, these are all human defences and prone to failure and are therefore poor substitutes for a mechanical locking system of some kind.

Stakeholders given the opportunity to respond to the assertion that more should be done to secure this hatch, resulted in a general lack of interest to pursue the matter from a regulatory/operator standpoint.

Comments at an operational level, however (while only a small sample), indicated a strong desire (93%) to have the matter addressed.

Adapting the system of safety design as used by the FAA and applied to potential security threats, it was shown the case to mitigate a catastrophic result from a probable event should be required by mechanical locking of the E&E hatch.

Several designs are available; from a system similar to the cockpit door mechanism already certified, to simpler and more cost effective solutions. These latter solutions would solve the security concern for all stakeholders and meet the 'affordable level of safety' principle.

If the safety and security of Australian aviation is indeed the 'top priority' of the Government then the case for securing this hatch must be a cornerstone of this policy. To ignore the matter, given the fact it is now even more wide spread over social media may be to invite an incident.

Of concern is the polarised nature of the opinion between those responsible for inflight security regulation and those who have to deal with it at an operational level. If erring on the side of caution is prudent then this issue should be addressed further.

The singular most notable comment from aviation security expert Professor N Shanks of Coventry University was:

'If a cost effective solution can be found, there appears no reason not to do so'.

-----End-----

References.

-
- ⁱ Burke, E. (1729-1797). Also credited with; '*All that is necessary for the triumph of evil is that good men do nothing.*'
- ⁱⁱ See <http://www.2worldwar2.com/kamikaze-pilots.htm> last accessed 16 April 2013.
- ⁱⁱⁱ See http://en.wikipedia.org/wiki/Trans_Australia_Airlines_Flight_408 last accessed 18 May 2013.
- ^{iv} Operations Manuals. This is the author's experience with four different companies since 1994. Hijackers demands to be complied with as best as able, including access to flight deck. Since 2001, this has changed and the integrity of the flight deck is to be preserved at all costs.
- ^v Schuler, D (2010). '*A Short History of Air Hijacking*'. See <http://theglitteringeye.com/> last accessed 18 May 2013.
- ^{vi} *Aviation and Transportation Security Act, 2001*. ATSA. Pub.L. 107-71 November 19, 2001, United States Government.
- ^{vii} *ibid.* Part 44905 (a) and (b) inter-alia (H) '*The technologies that might be used in the future to attempt or otherwise threaten commercial aircraft and the way in which those technologies can be countered effectively*'.
- ^{viii} *FAR Part 129-38, 68 FR 42882*, July 18, (2003). Federal Aviation Regulations, United States Government.
- ^{ix} See <http://www.goodrich.com> last accessed 14 May 2013.
- ^x Operations Manuals – Emirates Airlines, China Southern – 'In-flight Security'.
- ^{xi} Bentham, J. (1748-1832).
- ^{xii} Caley, K. (2011). Boeing Commercial - discussion with author.
- ^{xiii} See http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6239&print=go - last accessed 15 May 2013.
- ^{xiv} *FAR AC 25.1309-1A - 'System Design and Analysis'*. (2003). Federal Aviation Regulations, United States Government.
- ^{xv} CASA Safety Management Systems, (2012). Booklet 3, p 9. Australian Government Printers, Canberra, ACT.
- ^{xvi} *Australian National Security Regulations, 2010*. Section 28.
- ^{xvii} Trotta, D. Reuters, 14 March 2013, accessed 31 March 2013 (as derived from Stiglitz, J, Bilmes, L '*The Three Trillion Dollar War – The True Cost of the War in Iraq*'). Cost also reported to be \$3.5 trillion by the US Joint Economic Committee.
- ^{xviii} Boeing Commercial Airplane Presentation (2012). '*Statistical Summary of Commercial Jet Airplane Accidents – 1959-2011*', July 2012. p 17.
- ^{xix} See <http://www.slideshare.net/IATA-Training/aviation-securityportfolio> last accessed 19 May 2013.
- ^{xx} *Air Navigation Order 1920*, Part 2, para 3A. Australian Government Printers, Canberra, ACT.

-
- ^{xxi} *Chicago Convention, 1944*, Annex 17 – Security. ICAO, Montreal, Canada.
- ^{xxii} *Aviation Transport Security Act, 2004*. Australian Government Printers, Canberra, ACT.
- ^{xxiii} *ibid.* Div 5, 62 Onboard Security para (1) (aa).
- ^{xxiv} *ibid.* 74D Incident Control Directions para (1) Australian aircraft and (2) Foreign aircraft.
- ^{xxv} *Aviation Transport Security Regulations, 2005*. Australian Government Printers, Canberra, ACT.
- ^{xxvi} *National Aviation White Paper, 2010*, p 113. Australian Government Printers, Canberra, ACT.
- ^{xxvii} *National Security Legislation Amendment Act, 2010* (Amendments No 127, 2010). Schedule II, Part 1. Australian Government Printers, Canberra, ACT.
- ^{xxviii} Department of Prime Minister and Cabinet, (2013), '*Australia's National Security Strategy – 2013*'. Australian Government Printers, Canberra, ACT.
- ^{xxix} *ibid.*, p ii.
- ^{xxx} See <http://www.icao.int/Meetings/avsecconf/Documents/Symposium> last accessed 19 May 2013 and *Airliner World*, Jan 2011, p 48.
- ^{xxxi} *National Aviation White Paper, 2010*, op cit., pp 136-137. Australian Government Printers, Canberra, ACT.
- ^{xxxii} Reason, J. (1990). '*Human Error*'. Figure 4.2. United Kingdom, Cambridge University Press.
- ^{xxxiii} Author's experience on B707/B777/A330/A340 hatch locations.
- ^{xxxiv} Airbus and Boeing are the major manufacturers. There are three methods of entry as shown in aircraft documentation/flight crew operating manuals (FCOM).
- ^{xxxv} See <https://crewroom.alpa.org/CARGO/DesktopModules/ViewDocument.aspx?DocumentID=40942> pages 5, pp10-15 last accessed 19 May 2013.
- ^{xxxvi} Aggs, S, (2013). Virgin Australia – General Manager Safety Systems. As stated in correspondence enclosed.
- ^{xxxvii} Hoad, A. (2011). Emirates Engineering.
- ^{xxxviii} See <http://www.boeing.com/boeing/commercial/747family/background.page> last accessed 19 May 2013.
- ^{xxxix} See <http://www.triumphgroup.com/about/history#past> for hatch manufacturer last accessed 10 May 2013.
- ^{xl} See http://www.boeing.com/commercial/aeromagazine/articles/qtr_4_07/AERO_Q407.pdf, April 2006, p 21 last accessed 26 May 2013.
- ^{xli} Watanabe, J. (2012). Flight Test Pilot, Boeing. As related to author.
- ^{xlii} See http://en.wikipedia.org/wiki/Boeing_767/747/777/787 for aircraft numbers last accessed 10 May 2013.
- ^{xliii} See http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/topic/p7edd/p7edd_71x_73x.pdf last accessed 26 May 2013.

^{xliv} Bartz, G. et al. (2002). US Patent Number US20040061027, Filed Sep 26, 2002, published 01 April 2004, The Boeing Company.

^{xlv} Boeing FCT 777 TM (2011) – Normal Operating Procedures. Boeing Airplane Company, Seattle, WA.

^{xlvi} Movsesian, S. et al. (2004). US Patent Number 6830217 B2, Grant 10/255-916 14 Dec, 2004. The Boeing Company.

^{xlvii} See http://legacy.icao.int/icao/en/assembl/a37/wp/wp125_en.pdf last accessed 15 May 2013.

^{xlviii} See <http://www.n sai.co.uk/page5/page5.html> - Professor N.L Shanks last accessed 26 May 2013.

^{lix} Operations Manual – Part A (OM-A) (2010). Emirates Airlines. Section 1.5.4.2. Policy pre-discussion with author, June 2010.

^l loc. cit. Policy changed post-discussion with author in 2012.

^{li} Boeing FC 777 TM, (2010). Section 8.2 Jun 30, 2010– access to E&E compartment is ‘not recommended in flight’. Boeing Airplane Company, Seattle, WA.

^{lii} See <http://www.thefreelibrary.com/ICAO+elects+Al+Mansouri+to+chair+security+conference.-a0302330604> last accessed 19 May 2013.

^{liii} *Trade Practices Act, 1974* Section 62(b). Australian Government Printers, Canberra, ACT.

^{liv} De Chesal, V. (2012). Flight Attendant - Virgin Australia. As related to author in 2012.

^{lv} Cabin Crew Operating Manual (CCOM), Emirates Airlines. ‘Galley crewmember duties’.

^{lvi} CCOM, China Southern. Specific crewmember is tasked with security function.

^{lvii} See <http://travelsecure.infrastructure.gov.au/international/lags/> last accessed 26 May 2013.

^{lviii} B777 FCOM and (OM-A), (2011). Emirates Airlines.

^{lix} B777 FCOM (2011). Normal Operating Procedures.

^{lx} See <http://www.tsa.gov/traveler-information/prohibited-items#4> p 4 last accessed 19 May 2013.

^{lxi} See <http://noknivesonplanes.com> last accessed 19 May 2013.

^{lxii} Observed by author as passenger on a Qantas B767 in 2011.

^{lxiii} *FAR AC 25.1309*. op.cit. Part-1A.

^{lxiv} *ibid* Sect 5 para. a

^{lxv} *ibid* para b (1) and (2)

^{lxvi} *ibid* para 9e (1) and (2)

^{lxvii} *ibid* para 10 b. (1)

^{lxviii} See <http://www.slideshare.net/IATA-Training/aviation-securityportfolio> last accessed 19 May 2013.

^{lxix} CASA Safety Management Systems. op.cit., page 9.

^{lxxlxx} loc.cit.