Systems Engineering

Individual Research Portfolio

Protecting Passengers from Aircraft-Assisted Pilot Suicide

Luke Magyar
College of Engineering and Computer Science,
Australian National University,
Canberra
u5802436@anu.edu.au

May 13, 2016

Abstract

Aircraft-assisted pilot suicide is an unsolved issue in the commercial aviation industry, particularly when assessing passenger safety. The culmination of a systems engineering approach were recommendations for an objective, retrofittable and reactive **I**ntelligent **C**ockpit **A**ccess **S**ystem (ICAS) which addresses these concerns. The shortfalls of current preventative measures were considered extensively and the need for an alternate, engineered system established. Recent incidents of pilot suicide, largely enabled by the locking modes of cockpit doors designed to prevent and disincentivise hijacking, were treated as key use cases. The conditions required to 'deadlock' the cockpit door of an aircraft became the focus of the investigation and highlighted the opportunity to develop an eligibility-based system which utilises active, real-time monitoring of key flight indicators.

Contents

List of Figures

List of Tables

1 Recommendations

The investigation recommends developing and issuing an airworthiness directive based on the following:

1 **Objectivity** Instigate objectivity in flight procedures and pilots through a system which eliminates human factors and reliance that on-board crews will adhere to policy.

2 **Retrofit** Implement a system which can be integrated into existing flight systems and is generic for all aircraft and operating airlines.

3 **Reactive** The vulnerabilities of the current *preventative* system should be rectified by a system which *reacts* to unexpected events and affects a positive change.

4 **Monitoring** Critical flight attitude indicators should form the basis of a monitoring and evaluation system.

5 **Eligibility** The *deadlock* mode of the cockpit door should only be eligible to pilots if the monitoring system agrees the aircraft is on course.

6 **Clarity** Provide clarity on the locking mechanisms and logic behind cockpit doors and disseminate information beyond the commercial airline industry.

These recommendations form a basis for the development and implementation of an **I**ntelligent **C**ockpit **A**ccess **S**ystem (ICAS).

2 Introduction

In modern commercial aviation the lives of up to several hundred passengers and potentially many more civilians on the ground are in the complete control of aircraft pilots. The recent *Germanwings Flight 9525* and *LAM Mozambique Airlines Flight 470* accidents have been a stark reminder that despite advances in flight avionics, there is still the potential for untoward human intervention. In both cases the aircraft was brought down by the intentional act of one pilot who became isolated in the cockpit by locking the cockpit door (BEA 2016, CAAR 2013).

These tragic events were proceeded by a series of similar accidents over the past three decades which have been attributed to pilot suicide (Sinha 2015). Procedure and regulation has been unable to eradicate pilot isolation within the cockpit, or obvious, deliberate intentions to down an aircraft. Adhering to policy can easily become secondary to more immediate concerns, and overbearing obligations are often ignored by aircraft crew (Degani & Wiener 1997). Applying a systems engineering approach to the pilot-suicide scenario has enabled focus to be placed on removing human factors and reducing the likelihood and severity of commercial aircraft-assisted pilot suicides.

2.1 Current System

Although rare, pilot suicides are possible, resulting in intentional, dangerous and reckless flight commands which put the aircraft beyond its design limits, ultimately ending in catastrophe. Consequently, the problem was framed to consider how the control of a commercial airliner might be taken away from a single pilot or source. This led to the underlying question of whether a system could be engineered to eliminate the unpredictability of humans and the variabilities of decision making.

The airline industry currently relies on expert profiling and psychological evaluation to determine the mental suitability of pilots. Whilst this is a very similar process to that available to the general public, it is placed under far more pressure when dealing with pilots who work in a particularly stressful environment (Bor et.al. 2002, Voss et.al. 2013). The current system is prone to error, subjectivity and experts agree that is open to interpretation (de Castella 2015, Politano & Walton 2015). The inability of these methods to conclusively act against pilot suicide in a preventative manner is indicative of the need for a more robust and objective process.

Recommendation 1

Objectivity Instigate objectivity in flight procedures and pilots through a system which eliminates human factors and reliance that on-board crews will adhere to policy.

Research showed that experts do identify the limitations of the current profiling system and this formed a critical aspect of the systems design process. Recognising that the maximum potential of a given aspect (in this case psychological profiling) has been achieved but unable to eradicate the issue was a sound indicator that a new or alternate approach was required (Politana 2015). Improved psychological profiling was not immediately rejected, keeping with the initial broad problem scope. However, this scope was refined based on more in-depth analysis which focussed on the key aspects of the situation, environment, and the target group and its needs (Diefenthaler 2008).

2.2 Recommendation Target

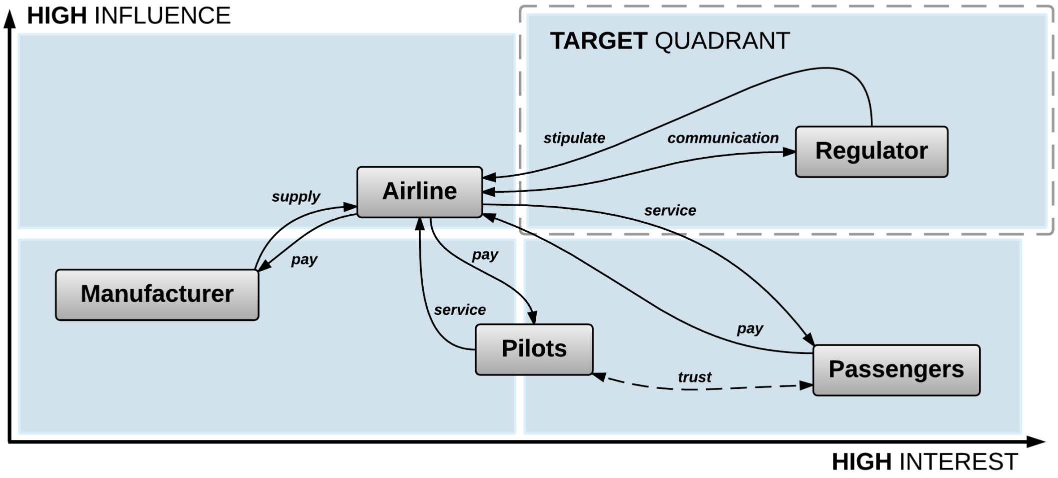


Figure 2.1. Stakeholder Map (overlaid with influence vs. interest chart)

Each time passengers board a commercial aircraft they place trust in the pilots' ability to control the aircraft, analyse situations and react accordingly. This creates a complex relationship dynamic between the passengers, operating airline and airline employees, including the pilots and crew. Whilst this project was targeted at a concerned airline passenger it resonates within society more broadly due to the popularity of air travel. Despite the number of passengers, flying is not a traditional user driven system. It is the pilots that have direct control over the aircraft during flight, and the airline which prepares the aircraft and trains its personnel. Furthermore a regulatory body, the Civil Aviation Safety Authority (CASA) in Australia, dictates procedures and requirements to commercial airlines. Thus, recognising the recommendations' target audience was the first step towards ensuring an effective solution. To actually address the client's concerns over passenger safety with respect to pilot suicide, a solution must either:

- **Advantage the airline:** Commercial airlines are driven by profit margins, which are largely dictated by the price passengers pay for air travel (see Figure 2.1). Due to the highly competitive industry, for an airline to willingly implement a new system it must increase profit or enhance brand image (Gowrisankaran 2002). If there is not a clear benefit to the airline, the system will not be implemented (a reflection of high power but low interest) and ultimately the client's (passengers) position is not improved.
- **Satisfy the regulatory body:** Regulators exist such that a sector is not entirely driven by profit but also quality and safety (France 2004). The relationship between the regulatory body and airlines is illustrated as two way in Figure 2.1, but the body has authority whereas airlines can only communicate back concerns. Based on the analysis in Figure 2.1 recommendations were actually targeted at the airline industry and thus the regulatory bodies as they hold both high interest in safety and high influence over the sector.

In order to serve the client and commercial airline passengers more generally, a system must be developed which reflects the industry needs. Stakeholder analysis has shown that targeting regulatory bodies with a conclusive improvement to passenger safety will ultimately change airline and pilot behaviour and it is these changes which will then directly impact passengers. Even in cases where upfront costs were paid, unenforced safety improvements have failed to be installed by airlines and airports (Catino 2010) Thus, pitching towards regulators such as CASA is the most promising avenue to protecting passengers from further pilot suicide accidents. These intricate stakeholder relationships are a reflection of the complexity of the airline industry itself and demonstrate the need to breakdown this complexity to form a refined scope for improvement.

2.3 Proposal Scope

Defining system boundaries typically forms the final phase of problem scoping. It allows a diverse range of problems to be considered during the early phase, but a more refined scenario to be taken forward to concept generation (Daly et.al. 2012). The first column in Table 2.1 highlights the components and surrounding operations of an aircraft than can be readily altered and controlled. This is a powerful indicator of where a solution could be implemented. Despite being well-established in the airline industry, the autopilot and flight computer were considered alterable as changes to software can be implemented without radical changes to infrastructure. Even if a computer requires further memory or processing power this can easily be added. However, factors such as pilot input and crew responsibility were considered external as they are critical to the regular performance of an aircraft. These behaviours cannot be changed without endangering other aspects of a flight.

Table 2.1. System Boundary Chart (categorised by factor type)

Internal		*External*		*Excluded*
Software	**Mechanical**	**Operation**	**Aircraft**	**Variables**
Autopilot	Cockpit	Pilots	Cockpit instruments	Location
Flight computer	Cockpit door	On-board crew	Cockpit design	Type of aircraft
Lock switch	Locking mechanism	Maintenance crew	Aircraft design	Operating airline
	Physical deadlock	Regulations		

Similarly, major cockpit equipment, controls, instruments and displays cannot easily be overhauled. Many decades of aeronautical design has been placed into modern commercial aircraft to improve both safety and performance (Morrison & Winston 2010). A new system cannot sacrifice this and must conform to existing aircraft design. In the case of a physical or software solution this must take the form of a retrofittable system. For airlines to be able to efficiently implement a new system and train pilots, it must function similarly for a variety of aircraft. The type of aircraft and operating airline were considered excluded factors as the system addresses a problem in the general category of modern commercial aircraft. Specific regulations that exist within a state or airline were excluded and instead the focus was placed on conforming to standardised common regulations (an external factor in Figure 2.1).

Recommendation 2

Retrofit Implement a system which can be integrated into existing flight systems and is generic for all aircraft and operating airlines.

Precedence exists for retrofitted safety systems on commercial aircraft. The catastrophic mid-air collision of two aircraft in 1956, and numerous fatal incidents since has prompted the continual development of TCAS (**T**raffic **C**ollision **A**voidance **S**ystem) (Wolochatiuk 2015). Initially a retrofit transponder system which provided alerts to the pilots of another approaching aircraft, the system now autonomously instructs pilots to descend or ascend to avoid a collision (Federal Aviation Administration 2011). It is this type of retrofit system, which primarily requires a change in software implementation, that could be effected.

3 Concept Generation and Selection

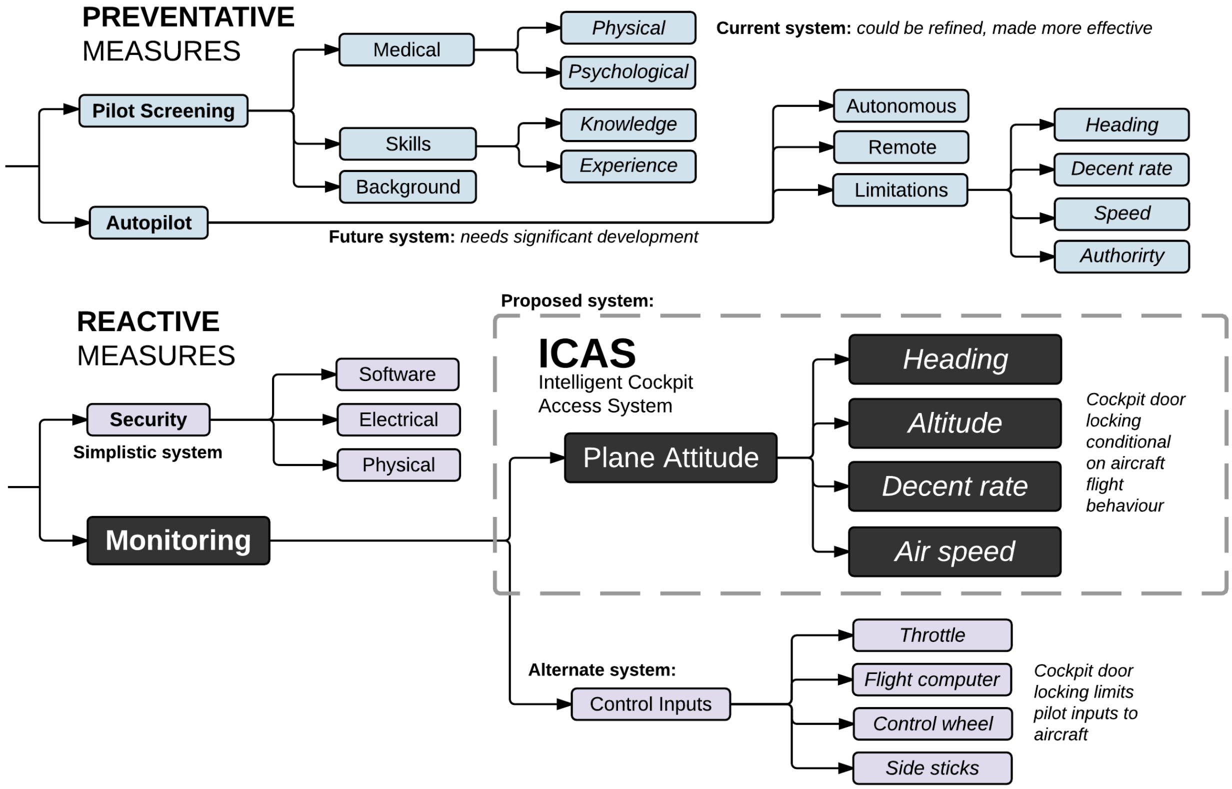


Figure 3.1. Concept Classification Tree (categorised from structured brainstorming)

Based on the target audience, stakeholder interactions and system boundaries developed, a diverse range of concepts were generated. Structured brainstorming was incorporated into the design process by considering the key issues raised in the preliminary research and analysis phases. In particular, the potential for preventative versus reactive systems was considered. This was contrasted with a technical engineering solution versus the more behaviour based systems which are currently in place in the form of psychological profiling. Adapting Ulrich and Eppinger's (1995) recommendations for idea generation, the concepts were categorised, presented in a classification tree (Figure 3.1) and narrowed based on analysis of existing, similar or relevant systems, performance measures, expert consultation, and situational awareness.

3.1 Experience Timeline

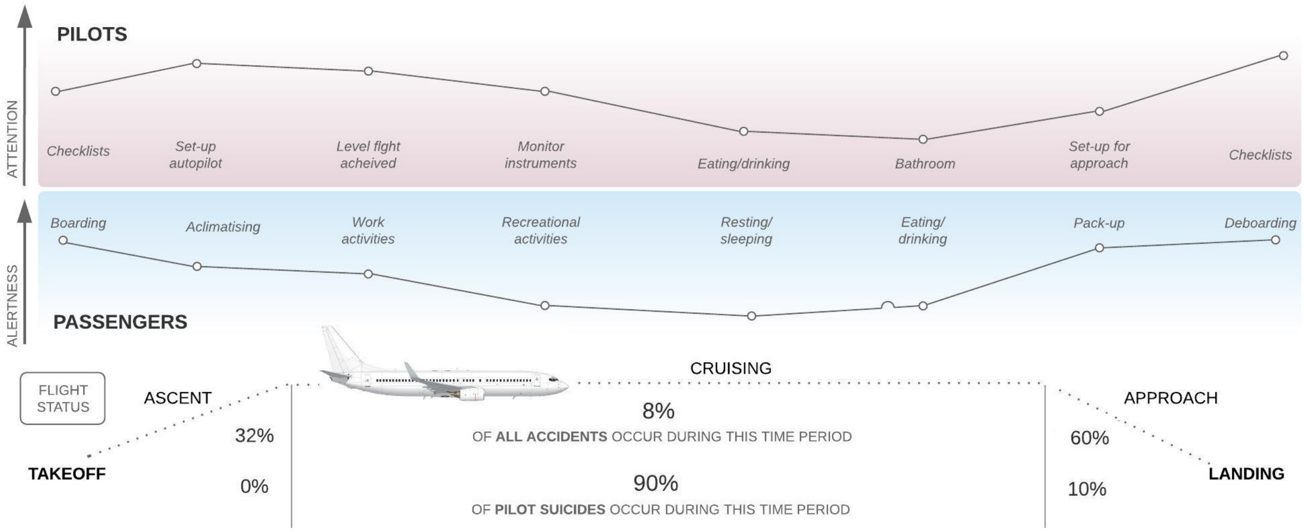


Figure 3.2. Journey Mapping (combined with personnel experience and accident statistics) (Sinha 2015, Lewis et.al 2007)

To understand when a problem might occur chronologically with respect the position of a solution, and verify the need for a reactive rather than preventative solution, a customer experience timeline was considered. The journey mapping framework was extended by considering the flight journey that passengers and pilots experience, highlighting the major vulnerabilities. The need for a reactive solution arises in the failings of preventative measures. Profiling and scrutineering, as has been discussed is subjective and will never form a perfect barrier to pilot mental instability. To protect passengers from aircraft assisted suicides, an improved system must react to a dangerous situation and make a change which alters or reduces the severity of the outcome. Whilst autonomous flight has the potential to eradicate not only intentional acts but also human error, the technology remains in development and pilots fear that in the event of a mechanical failure or emergency, the flight computer may deny them performing critical manoeuvres (Hoffman et. al. 2000). Thus, preventative measures were ruled out in Figure 3.1 as they do not radically improve the process or outcome during a pilot suicide attempt, or are too advanced to be implementable. This places focus on the development of an engineering solution which can react to unusual circumstances on an aircraft, interact with the pilots and improve the chances of recovering an aeroplane.

Recommendation 3

Reactive The vulnerabilities of the current *preventative* system should be rectified by a system which *reacts* to unexpected events and affects a positive change.

3.2 Performance Measures

Isolating the most promising and reactive engineering system was achieved by developing technical performance measures (TPMs). As the stakeholder analysis (see Figure 2.1) concluded that a proposal must address the regulatory body and thus airline industry in order to improve passenger safety, the requirements reflect the regulatory body's ideology. The client's requests were followed through the stakeholder relationships in Figure 2.1 to the regulatory body:

- The client fundamentally required that an effective system be implemented without significantly increasing the cost or inconvenience of air travel.
- Carrying these requirements to the airline dictates that the system is cost-effective and will not require significant increase in ticket price to be implemented on their fleet. It must be compact and retrofittable to the existing fleet, for immediate implementation without reducing the efficiency of passenger air travel.
- The regulatory body can authorise airlines and aircraft manufacturers to comply with any regulation but the communication avenues from these groups to the regulator would emphasise the need for an effective, reliable, cheap, unobtrusive, and secure system. Thus, whilst the regulator will emphasise the need for safety (effectiveness, reliability and security), the client's cost and convenience requests also reappear as regulator requirements.

The implementation of expensive, widespread safety initiatives such as the Commercial Aviation Safety Team (CAST) and European Strategic Safety Initiative (ESSI), are evidence that if a radical safety improvement is made, it will override expenditure or inconvenience (ICAO 2004, EASA 2016). Consequently, a natural, informal ranking of requirements occurred which prioritised effectivity and reliability. These concepts were unpacked further and a strong emphasis was placed on linking the client requirements to multiple design requirements. Accompanying metrics and a method by which to measure them were developed to highlight tangible goals and performance indicators of a proposal.

Effective The current profiling system and weak regulations for crew observance and transparency have been ineffective. A new engineering system must remove subjectivity, prevent a pilot from becoming isolated in the cockpit and be able to rapidly respond (*response time*) to a pilot's dangerous interference with the aircraft (*restore aircraft control*).

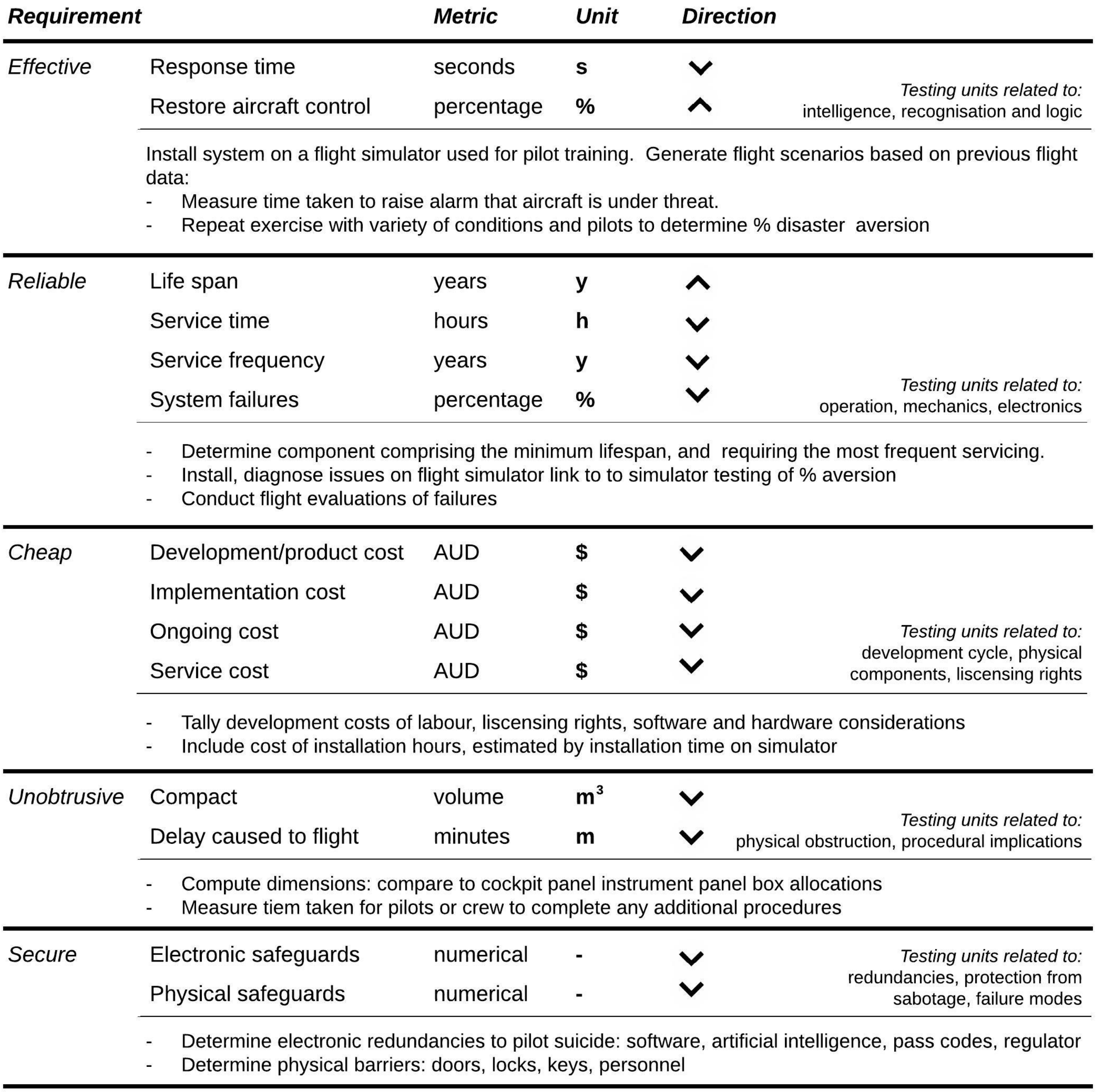
Reliable Regulators consider the long-term impact of aircraft systems and set out continuing airworthiness requirements for aircraft and aeronautical products (CASA 2011, Ferrel & Ferrel 2001). In order to achieve reliability, the frequency of system failures, lifespan and life-cycle of the solution must be considered as well as how often (*service frequency*) and time consuming servicing is (*service time*).

Cheap The cost of implementation of most safety systems is absorbed by airline companies but must be kept to a minimum to prevent consumers, which in this case are passengers, incurring the costs. Whilst there is a continual push for aircraft safety improvements, millions of passengers fly on commercial aircraft every day without fear of mechanical failure, or pilot suicide (Rose 2013). It is reasonable to assume that passengers would embrace a new system only if the *product*, *implementation* and *servicing costs* do not significant effect ticket prices.

Unobtrusive The client highlighted that the efficiency of air travel is already limited by the significant screening of passengers and luggage that occurs prior to a flight. A new system must not significantly delay the flight, reduce the convenience or comfort of air travel. Airlines and thus regulators hold similar views that a new system must not delay ordinary flights (*delay caused to flight*) or consume precious space on an aircraft (*compact*) (Gowrisankaran 2002).

Secure The issue of aircraft assisted pilot suicide is related to aircraft hijacking, particularly in relation to cockpit access. A new system which reduces the opportunity for pilot suicides must not sacrifice security from other scenarios. Thus the development of redundancies, *electronic safeguards* and *physical barriers* are critical measures of a system's performance.

Table 3.1. Performance Measures and Unit Testing (design requirements combined with relevent testing approach)



Requirement		***Metric***	***Unit***	***Direction***	
Effective	Response time	seconds	**s**	∨	*Testing units related to:* intelligence, recognisation and logic
	Restore aircraft control	percentage	**%**	∧	
	Install system on a flight simulator used for pilot training. Generate flight scenarios based on previous flight data: - Measure time taken to raise alarm that aircraft is under threat. - Repeat exercise with variety of conditions and pilots to determine % disaster aversion				
Reliable	Life span	years	**y**	∧	*Testing units related to:* operation, mechanics, electronics
	Service time	hours	**h**	∨	
	Service frequency	years	**y**	∨	
	System failures	percentage	**%**	∨	
	- Determine component comprising the minimum lifespan, and requiring the most frequent servicing. - Install, diagnose issues on flight simulator link to to simulator testing of % aversion - Conduct flight evaluations of failures				
Cheap	Development/product cost	AUD	**$**	∨	*Testing units related to:* development cycle, physical components, liscensing rights
	Implementation cost	AUD	**$**	∨	
	Ongoing cost	AUD	**$**	∨	
	Service cost	AUD	**$**	∨	
	- Tally development costs of labour, liscensing rights, software and hardware considerations - Include cost of installation hours, estimated by installation time on simulator				
Unobtrusive	Compact	volume	**m^3**	∨	*Testing units related to:* physical obstruction, procedural implications
	Delay caused to flight	minutes	**m**	∨	
	- Compute dimensions: compare to cockpit panel instrument panel box allocations - Measure tiem taken for pilots or crew to complete any additional procedures				
Secure	Electronic safeguards	numerical	**-**	∨	*Testing units related to:* redundancies, protection from sabotage, failure modes
	Physical safeguards	numerical	**-**	∨	
	- Determine electronic redundancies to pilot suicide: software, artificial intelligence, pass codes, regulator - Determine physical barriers: doors, locks, keys, personnel				

4 Concept Refinement

Recent catastrophic pilot suicide incidents have proven the current pilot screening is an important step in pilot training but remains vulnerable, particularly with respect to the *reliability* aspect of the prescribed requirements. Proposals have been made to radically increase the amount, and intensity of pilot scrutineering but little evidence suggests that the immense cost increase would actually increase safety (Bilefsky & Clark 2015, Bukszpan 2015). A similar conclusion was illustrated in Figure **??** when comparing screening to more certain methods such as improved or altered cockpit security. Even the development of hijacking alert systems, such that the current cockpit locking mechanism could be simpler, have failed to be accepted by the industry due to a high degree of uncertainty about their reliability and effectiveness (Ord 1972, Cordina 2004). Similarly, advanced cockpit protection curtains and flight deck instrument security is too obstructive to regular flight operations to enact widespread implementation (D'Alvia 2005, Martens et. al. 2005). Consequently, this investigation moved towards an active cockpit monitoring system.

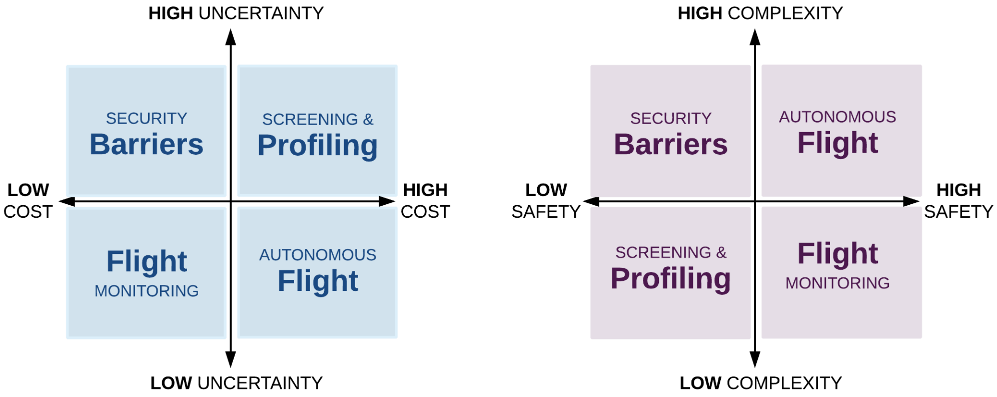


Figure 4.1. Scenario Planning (comparing cost and uncertainty, safety and complexity)

Flight monitoring formed the basis of the proposal, incorporating the door locking mechanism in an **I**ntelligent **C**ockpit **A**ccess **S**ystem (ICAS). Flight data recorders, which are steadily being updated to digital devices, already exist on all commercial aircraft for traceability purposes (Bondi 2015). Adapting these devices, or having an intermediary's stage would not be a radical jump for avionic systems. Specifically, ICAS would rely on the flight computer comparing the aircraft's attitude (heading, speed, altitude, descent or ascent rate) to the expected behaviour of that portion of the flight, thus describing a three-dimensional lane or route for the aircraft. In Australia, airlines are already required to provide flight paths to CASA, and similar procedures exist in most nations (CASA 2011). The detail of these logs could be improved to provide enough information to develop a guiding lane (with a tolerance) which the flight would be expected to remain inside. The ability to lock the cockpit door would then depend on the aircraft's position and behaviour with respect to the lane preprogrammed in the flight computer.

Recommendation 4

Monitoring Critical flight attitude indicators should form the basis of a monitoring and evaluation system.

Permission and eligibility-based systems are already in place within the airline industry. Air traffic controllers at busy airports comprised of many interconnecting runways and taxiways rely on electronic 'stop bars' denying pilots progression into active and dangerous areas (Hyslop 2012). Major commercial aircraft manufacturers such as Boeing and Airbus pre-program restrictions on an aircraft's performance in terms of speed, altitude and structural operating restrictions, referred to as a flight envelope (Barber 2004). Extensive and continuing development of these types of restrictions has restored faith in pilots and their ability to react in emergencies (Perhinschi 2015). More primitive devices that operate similarly to the proposed, 'pre-programmed lane' include virtual guidance systems.

'Glide slopes' refer to instrument landing systems which are installed at most major airports, aimed at helping guide pilots to the runway (Koenig & Schubert 2014). The high intensity strip of lights or Visual Glide Slope Indicator's (VSIs) are easily obstructed at airports surrounded by challenging terrain, mountain ranges, or are prone to fog and bad weather making approach difficult . Consequently, pilots rely on an instrument landing system which emits radio waves from the end of the runway, received by the aircraft's transponder, to guide them along a virtual route towards the runway based on heading, angle, speed and descent rate (ITU 2012). The same principles can be applied to monitoring on board an aircraft and be used to make intelligent decisions about access to the cockpit. In particular, the logic and conditions behind the eligibility of the cockpit door locking were developed.

5 System Design

5.1 System Operation

Currently all cockpit doors comprise three similar modes of operation, which can be selected by the pilots on the control panel inside the cockpit (Sirven 2002):

UNLOCK When the pilot wishes to open the door the toggle switch can be held to the 'UNLOCK' position and the door will remain unlocked whilst the switch is held (Bilefsky & Clark 2015, Sirven 2002). On release it returns to the 'NORM' mode, locking the door.

NORM The default position which locks the door from external access. A crew member can unlock the door from the cabin by entering an override code, primarily designed for use if the crew fears the pilots have become incapacitated (Sirven 2002).

LOCK A hard-lock which prevents access to the cockpit externally, override codes are rejected. Typically can be engaged by the pilots for up to five minutes at a time (Bilefsky & Clark 2015). Specifically designed in the event of hijacking to safeguard the pilots and protect cabin crew from being threatened for the passcode.

Analysing the current processes that logically succeed each other was a critical step towards developing effective logic in ICAS. Limitations were made on depth and detail such that some steps which do not directly affect the system could be simplified. For example, the door access code could substantiate a logical flow analysis on its own when accounting for incorrect passwords, number of attempts and other factors. Whilst these functions might have some effect on the design of ICAS they were considered outside the problem scope boundaries set here. Furthermore, pilot suicides are relatively rare but usually catastrophic events (Zuckerman 1999). Consequently, the logical flow analysis, both with (Figure 5.2) and without (Figure 5.1) the solution implemented, was developed based on a worst possible scenario. That is, it attempts to illustrate the flow of events that would precede a disaster, but would be a particularly poor reflection of an ordinary flight which would essentially loop through only the cockpit panel flow.

5.2 System Logic

The current logical flow (see Figure 5.1) highlighted that a cockpit door must still comprise an 'UNLOCK' mode to allow for pilots and crew to enter and exit the cockpit, as well as on the ground to allow maintenance staff to move in and out of the cockpit readily. Hijacking incidents have highlighted that the cockpit door should remain locked (NORM mode) by default and this is reflected in both the existing and proposed system. Similarly, to

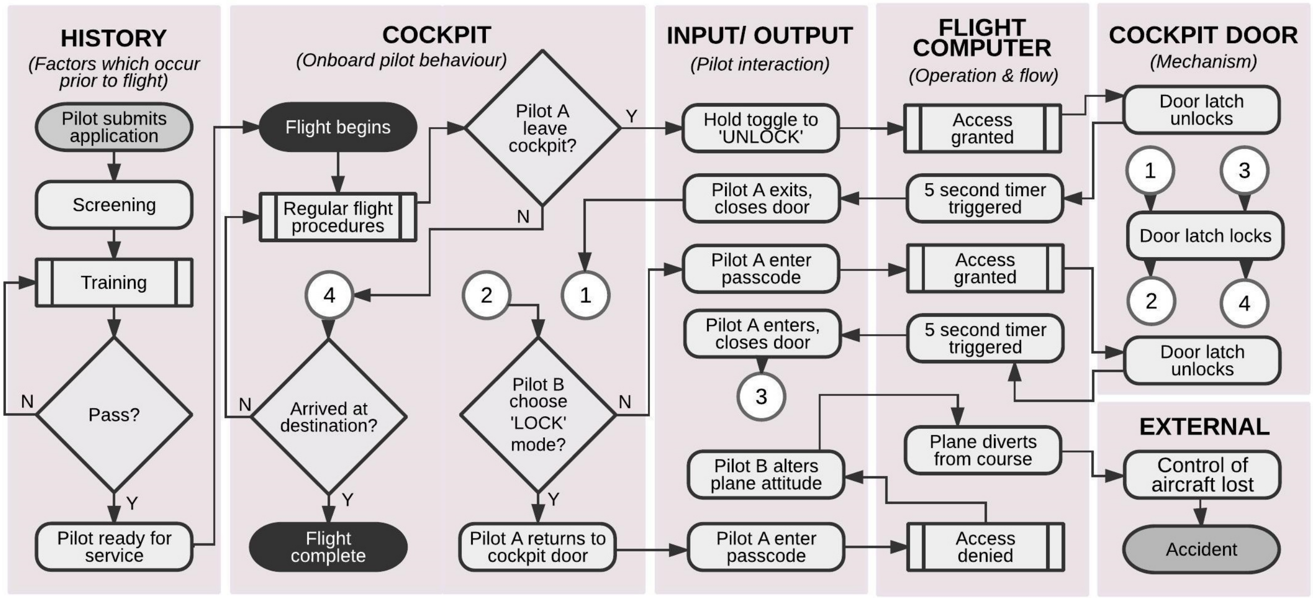


Figure 5.1. Logical Flow (of current systems pertaining to pilot suicide)

disincentivise hijackings, the industry has recognised the need for a dead-lock type mode (currently LOCK mode). It is this 'LOCK' mode which has contributed to aircraft-assisted pilot suicides. In the case of both Germanwings Flight 9525 and LAM Mozambique Airlines Flight 470 a pilot casually left the cockpit during cruising to use the bathroom or services on board and the remaining pilot repeatedly engaged 'LOCK' to deny their return (see Figure 5.1) (CEA 2016, CAAR 2016). Consequently, the pilot became isolated in the cockpit and was able to set the plane for a steady state descent into terrain or push the aircraft into an unrecoverable dive (Sinha 2015, CEA 2016).

Figure 5.2 demonstrates that in an aircraft with ICAS implemented, pilot(s) can only select the *dead-lock*-type mode if the monitoring system agrees the plane is within the expected 'lane'. The subsequent decision loops in Figure 5.2 highlight that in the case of Flight 9525 and 470, when the pilot breached the lane, the door would autonomously have returned to the 'NORM' mode, allowing the other pilot to return to the cockpit by entering an override code. The logical flow analysis demonstrates the system's ability to combat unusual or coincidental circumstances which might allow one barrier to be breached, but not the entire system. The intelligence inherent in the system isolates it from the current preventative and policy measures which have failed to make an impact on the sector.

Recommendation 5

Eligibility The *deadlock* mode of the cockpit door should only be eligible to pilots if the monitoring system agrees the aircraft is on course.

Importantly a cockpit hijacking is still preventable as the pilots can indefinitely select the new 'LOCK' mode as long as they are flying as expected. If a new flight plan is required, for example during a hijacking to land as soon as possible, the preprogrammed 'lane' is altered by ground crew once an emergency is declared. The proposed system still allows pilots to declare an emergency in regular situations, or respond to a mechanical failure and fly outside the 'lane' as the 'NORM' mode will remain engaged. Subsequently, acceptable results to probable in-flight scenarios promoted investigation of the implementability of ICAS.

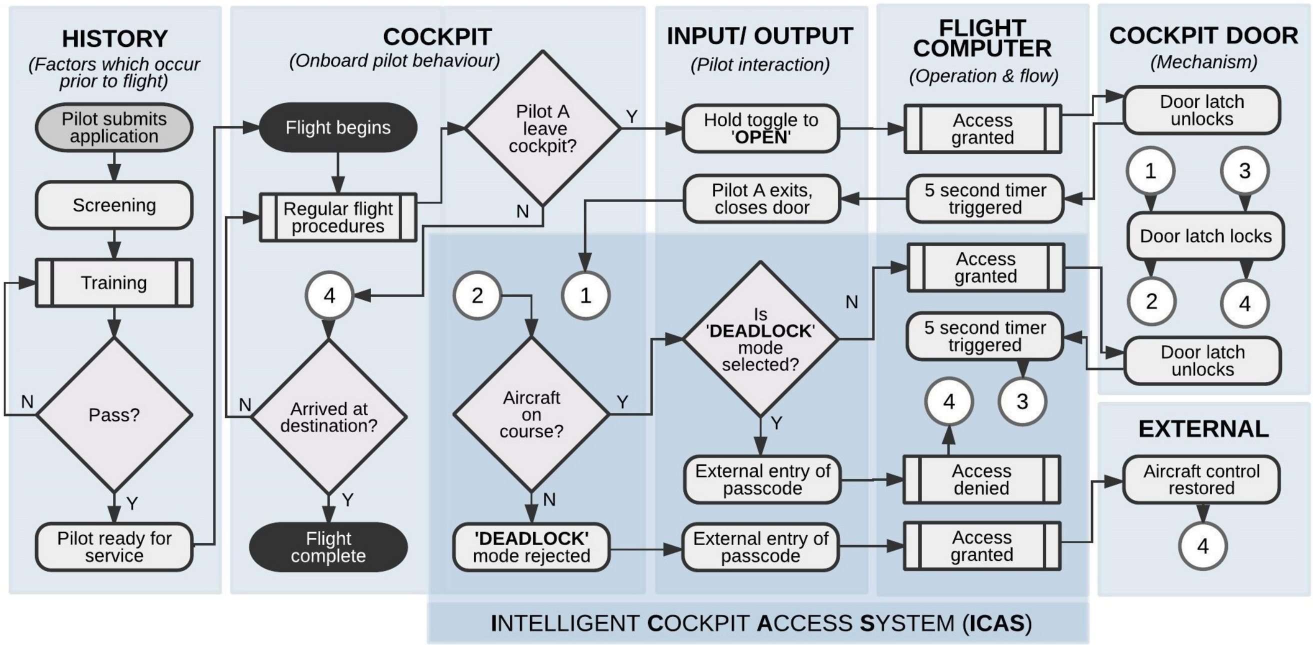


Figure 5.2. Logical Flow (of events on a commercial aircraft with ICAS installed)

5.3 System Integration

Aircraft are comprised of thousands of systems, ranging in complexity and type (Moir & Seabridge 2008). Thus, proposing a new addition requires significant thought about its role within the larger system. A key step in this process is the development of system architecture, focusing on the position, role and link between subsystems (Crawley 2004). The retrofittable attributes of ICAS have been discussed and link directly with how the new system will integrate with existing flight systems. In particular, the ability to retrieve critical flight data to conduct monitoring in real time was highlighted during the integration phase.

The comparator component of the ICAS computer system can only function if it is supplied with two inputs of the same type. A regular cause of program errors is a function which is asked to complete a task with two incompatible data types. Critically, the interface map (Figure 5.3) has raised comparable data types prior to implementation. Interfacing was conducted at a moderate level of detail to ensure important and relevant findings were made. However, defining fundamental boundaries and interfaces was favoured over excessive complexity (Crawley et. al. 2004). For example, where a key interaction with ICAS occurred, aspects of the flight system and controls were broken down into subsystems, but all flight avionics were not investigated. The retrofittable aspects of the design were made clear as the current connections that exists between systems (electrical, data, mechanical fluids) had to be replicated. These areas will become particularly important in the successive stages of the project as more technical developments are made.

5.4 Design Communication

As ICAS utilises software to interpret behaviour and decide the validity of a mechanical response, typical design communication tools, such as a technical drawing or model, are not as effective. Instead, an info-graphic was built on the logical flow and system architecture previously developed. As the decision making process will determine the solution's success, it became critical to represent this visually. Much discussion within the airline industry has been had over the advantages and disadvantages of 'closed' and 'open' cockpits, largely with respect to hijackings and pilot incapacitation (Linshi 2015). ICAS makes a key breakthrough as the locking state of the cockpit door is dependent on the aircraft's behaviour, providing a middle ground which was not previously possible.

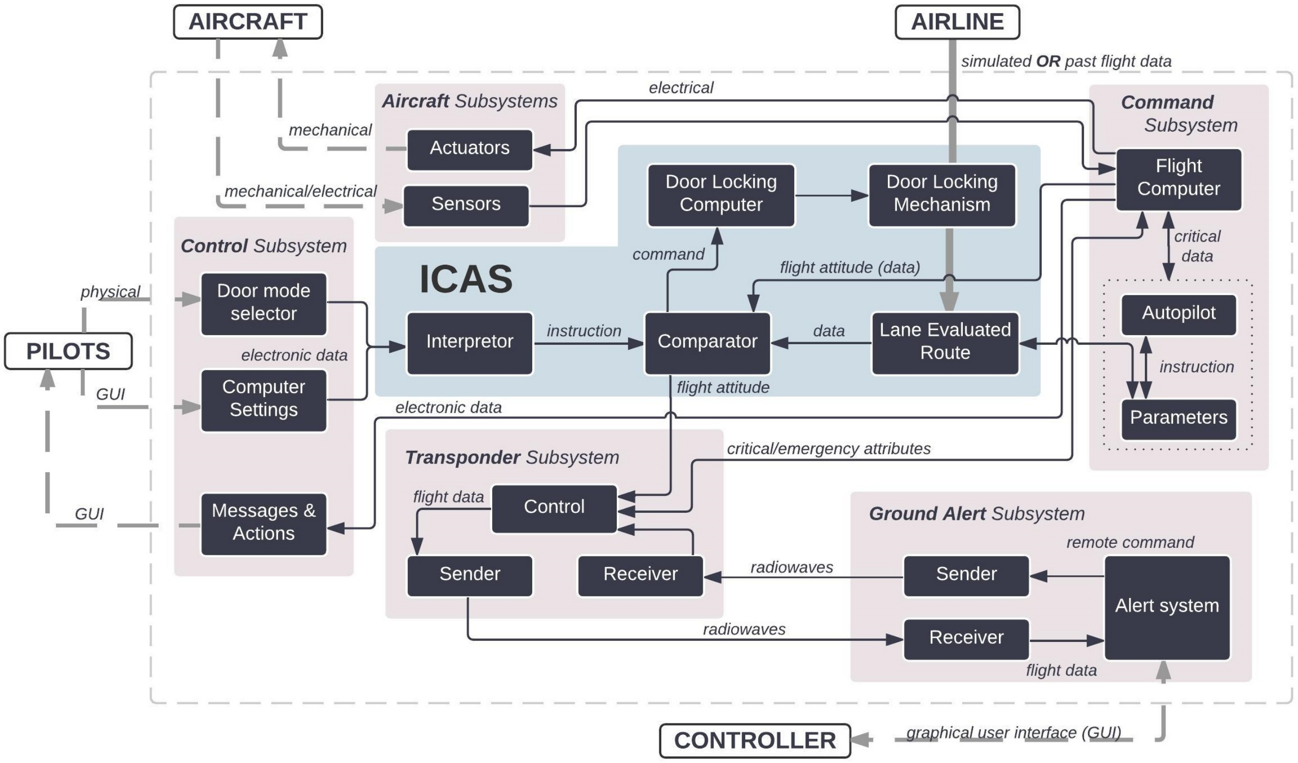


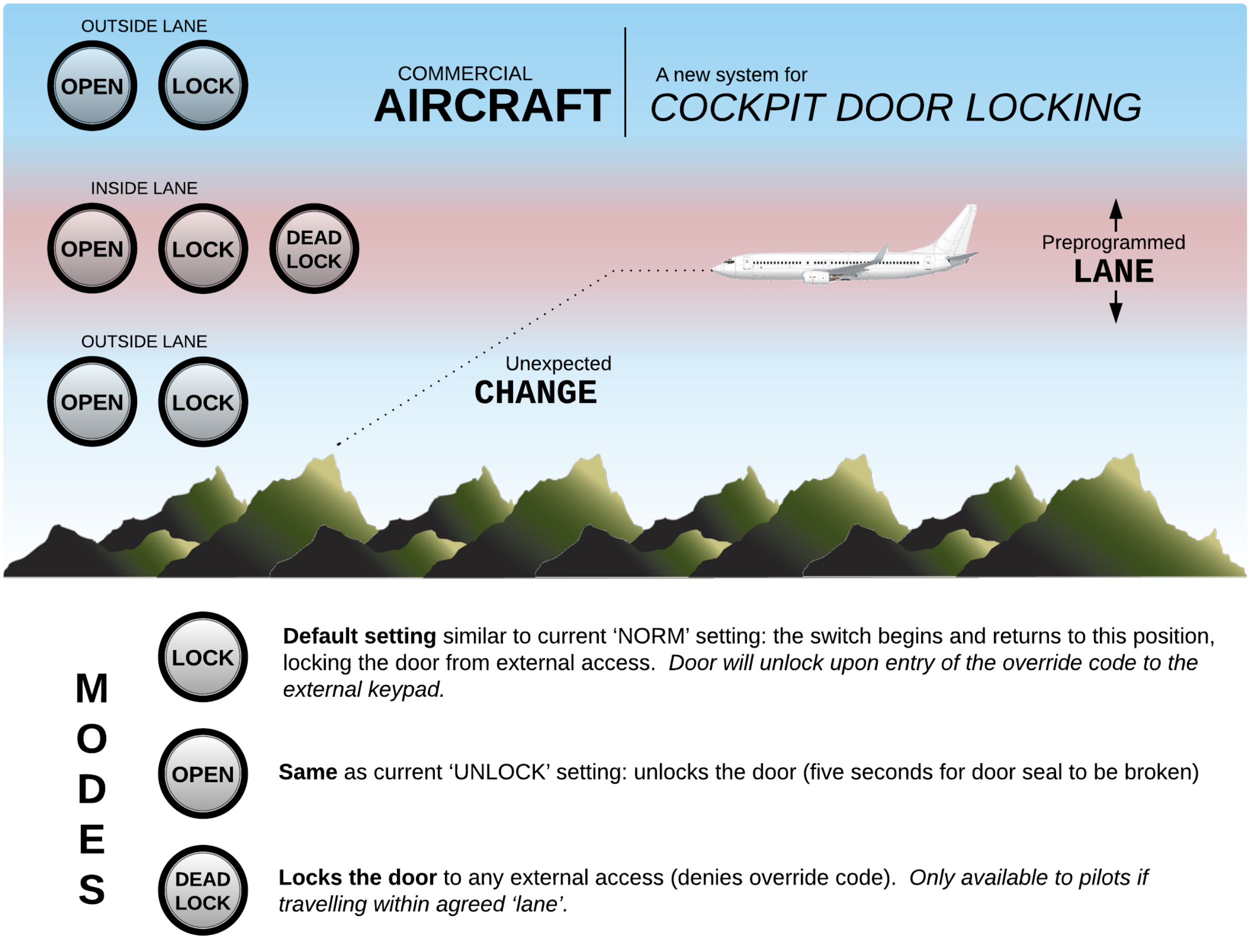
Figure 5.3. Subsystem Interface (of flight systems which interact with ICAS)

The ability to add logic, and thus an intermediary stage to the situation, is very beneficial. For this reason, Figure 5.4 has been designed to highlight that the available door locking options are dictated by the aircraft's heading, altitude, descent (or ascent) rate and speed. Altitude is the most easily illustrated and intuitive indicator of course and thus formed the visual for deviating from the preprogrammed lane. The design communication also reflects the recommendation to rename the modes to emphasise their new function. 'UNLOCK' would function identically but become 'OPEN' to highlight it is a temporary state, 'NORM' would become 'LOCK', and the existing 'LOCK' changed to 'DEADLOCK' to highlight that it is a mode for exceptional circumstances only and carries flight conditions. Clarity is exceptionally important in aircraft due to large number of cooperating systems and unique human-technology interface. Clarifying the locking modes of the new system not only retrains pilots of their use, but dissemination of this information is also likely to further dissuade hijackers. The more clarity provided both by the ICAS system itself and the accompanying design communication (Figure 5.4), the simpler cockpit manuals and procedures can be made, whilst still ensuring the correct operation of on-board systems.

Recommendation 6

Clarity Provide clarity on the locking mechanisms and logic behind cockpit doors and disseminate information beyond the commercial airline industry.

The events that occurred on a *Germanwings* flight in 2015 should be prevented by the revised cockpit door locking modes. The co-pilot who was able to lock the door to all external access for periods of five minutes would have only be able to select the new 'DEADLOCK' mode temporarily. With ICAS installed, if he had attempted to reprogram the autopilot for a steady descent as occurred, the on board system would have recognised the plane was deviating from the preprogrammed lane without authorisation for a change. The cockpit door would have



Default setting similar to current 'NORM' setting: the switch begins and returns to this position, locking the door from external access. *Door will unlock upon entry of the override code to the external keypad.*

Same as current 'UNLOCK' setting: unlocks the door (five seconds for door seal to be broken)

Locks the door to any external access (denies override code). *Only available to pilots if travelling within agreed 'lane'.*

Figure 5.4. Design Communication (info-graphic style abstract detailing the key operating principles of ICAS)

remained locked but switched to the 'LOCK' mode meaning the captain could have re-entered the cockpit using an override code. The 'DEADLOCK' mode would have remained unavailable to the co-pilot until the aeroplane returned to the expected path, or allowing the caption to return to the cockpit, likely averting catastrophe.

6 Outlook

6.1 Failure Modes

Safety and regulation are of utmost importance within the airline industry, and msut be considered both in ordinary flight procedure and emergency scenarios. The greatest barrier to ICAS implementation is pilot acceptance and trust that in the event of the emergency, having to deviate from the flight path will not cause adverse effects. The ICAS system assumes that in a hijacking event, pilots will continue along the original route, which as a principle has been promoted as it disincentivises hijackings. However, special circumstances on a flight could mean pilots may need to deviate from course, returning the door to the standard LOCK mode, and allowing an external passenger to enter an override entry code. The likelihood of such an evident is very low but certainly a consideration for future development. A provision exists for ground crew to modify a plane's preprogrammed route via wireless communication but remains primitive.

Aviation regulators already require that all new safety systems be classified on a five point scale based on the severity of the impact a system failure would have: (A) catastrophic, (B) hazardous, (C) major, (D) minor,

(E) no-effect (Ferrell & Ferrell 2001). Due to the extreme rarity of pilot suicide, hijacking or mechanical failure occurring simultaneously ICAS can remain in the minor category (D). Furthermore, in the event of an emergency, the cockpit door lock failing, or locking modes becoming unavailable is non-critical. Even if the DEADLOCK mode became permanently engaged, cockpit doors already have a door cut-out which can be manually removed from the inside to allow escape. Further development and analysis of these systems remains a critical part of later phase testing. Unit testing was proposed with relation to design requirements but the ICAS testing philosophy should be a progression from logic, data algorithm analysis to simulator testing and finally test flight evaluations to reduce the risks and understand failure modes. Furthermore, upon ICAS implementation, cockpit procedures and manuals would be updated to include a section detailing the failure of the cockpit door and the recommended troubleshooting behaviour as currently exists for all operation aircraft systems.

6.2 Roadmap and Future Work

Due to the complexity of aviation the system analysis conducted lies early within the overall design and implementation process, and thus findings were made at a relatively high-level breakdown. This had the advantage of maximising integrability and developing fundamental requirements for a relevant target. It does however mean the next stage of ICAS development requires further technical knowledge to be incorporated with systems thinking. Experts from the aviation industry, experienced pilots, software engineers and an extension of engineering disciplines would need to be coordinated to progress the project. In particular, an improved understanding of the form data transported within a flight computer would become important, and this is an aspect that would likely only be revealed by consultation with aircraft manufacturers. A study into what flight data is quantifiable and the establishment of firm tolerances would also form a key part of this next phase. Developing costing for future development as well as the ultimate implementation and ongoing cost of ICAS is a critical step in presenting the concept to industry. If the benefits can be communicated to regulatory bodies they are likely to develop a taskforce to develop the technology, in a continual strive for improved aircraft safety.

Autonomous flight is seen as the pinnacle of aircraft safety and even if never achieved it is likely to gradually appear in section of aircraft in the coming decades (Keith 1988, Wolochatiuk 2015). The monitoring aspects of the ICAS system pave the way for autonomous and intelligent flight. As technology, and trust in technology improves, flight computers will plausibly not only recognised an aircraft is deviating from course but also reject those changes. The biggest hurdle to these developments is pilot's fear that in the event of an emergency or failure, the flight computer might deny them providing critical inputs (Hyslop 2015, Casos 2010). ICAS is a cautionary step in this direction as it is still suspect to these problems but will not cripple critical flight systems. On an ordinary flight, a malfunction which prevents the pilots selecting the 'DEADLOCK' mode is unlikely to be of any concern. Opportunities for parallel project which investigate locking mechanisms, physical deadlocks, fingerprint and facial recognition exist and with the rapid advancement of these technologies in other sectors they are very real possibilities for future implementation with ICAS.

7 Conclusion

The project was initiated to address the concerns of a commercial airline passenger, in relation to the processes and systems which exist in protecting passengers from aircraft-assisted pilot suicides. As the design progressed, the scope narrowed, focussing on a reactive engineering system which could eliminate the shortfalls, primarily human subjectivity, of current preventative measures. The recommendations built around ICAS reflect a solution which allows a barred pilot (or crew member) back into the cockpit if erratic, unusual or dangerous flight behaviour ensues. A systems approach has furthered isolated engineering endeavours on cockpit doors and developed an intelligent solution which considers both broader impact and integrability aspects. The importance of an objective and retrofittable system were emphasised based on the shortfall of current processes and the limitations of already complex aircraft respectively. The ability to react to unexpected situations and utilise monitoring to determine the eligibility of door locking modes forms the foundation of an **I**ntelligent **C**ockpit **A**ccess **S**ystem (ICAS) and an improvement in safety for the client and all commercial airline passengers.

8 Reflection

I have realised that system's engineering is defined, moulded and shaped by the topic or situation concerned. The greatest benefit of a systems approach is the combination of structure and the ability to adapt the design process to the project's needs. This does mean the path that the design takes can be very different to the one anticipated at the outset, something I experienced with this portfolio. In particular, I compare the way I viewed by topic in small pieces during the Threshold Concepts (TC) stage and the ultimate outcome of the portfolio, and they are very different. I have ultimately addressed a similar problem but the final report has forced me to refine my lofty ideas from early in the semester, into a moderately achievable and realistic solution.

Presenting this solution in the form of a report, and intermingling recommendations with the design process and ultimate solution, has not been as intuitive as I envisaged. Understandably, the TCs were ordered according to the course topics, but this impinged my particular research area as the 'chronological' order was not always best suited. Furthermore, some tools from each aspect of the design process were more helpful than others, but this was not always reflected in the TCs. I was forced to think about my topic more laterally, which has likely improved the ultimate outcome. Unfortunately, the majority of discussion and information I developed during the semester and presented in TCs did not address the issues that substantiated my report. On a similar future task, I would develop skeleton ideas within TCs and emphasise the key aspects rather than the details, which are often formed later in the process.

I was quite apprehensive about the effectiveness of peer review so late in the design process. I have been involved in a peer review process in another class this semester and it was only a marginal success, limited by being held too early in the project. Here it was almost too late, if comments were constructive but required a change to requirements and the subsequent design it was difficult. Personally I still made use of the peer review process but I would also have benefited from some informal peer reviews, maybe conducted in tutorials after the idea generation and requirements analysis phases but before the solution was firmly established. I gained a lot of valuable feedback from peers just by exchanging portfolios and discussing ideas and different approaches.

In terms of the feedback I received during the formal peer reviews, I was quite pleased and able to make some improvements. After investing a large amount of time into reading and researching the two portfolios I reviewed, I would have been disappointed only receiving two reviews back as one was less than 500 words long and made no useful suggestions. Luckily, the third additional review was an exemplary replacement. The most formative feedback was actually the repeated commendation of an extension I made to the stakeholder analysis, which I have now tried to replicate in other techniques. One reviewer did express struggles with some of the technical language used and consequently I have tried to rein back these aspects, opening the portfolio to a wider target audience. However, simultaneously I want to maintain a high-level, professional conclusion and argument, which is acceptable within the airline industry, and some technical details are critical to this. I have spent significant time in the later drafting stages adding and removing technical detail to achieve this.

The next phase of my project would likely become more technical but still must maintain a systems approach to ensure integrability and human factors are consulted continuously. Thus far, the systems approach has enabled me to make non-trivial conclusions and recommendations about the operation of cockpit doors. My recommendations focus on replacing the current open and shut operation of cockpit doors with an intelligent system that provides a middle ground. Passengers and the airline industry alike are continually pushing for safety improvements and whilst I recognise how limited my analysis and solution is, I believe it targets the type of intelligent solutions developed on a large scale around the world.

9 References

'Aviation Occurrence Categories: Definitions and Usage Notes', 2004, *International Civil Aviation Organisation (ICAO): Commercial Aviation Safety Team (CAST)*, Ver. 4.1, June 2004

Barber, K 2004, 'Flight Envelope, The Canadian Oxford Dictionary', 2nd Edition *Oxford University Press*, Don Mills

Bilefsky, D & Clark, N 2015, 'Fatal Descent of Germanwings Plane Was "Deliberate", French Authorities Say', *New York Times*, 27th March 2015

Bukszpan, D 2015, 'Pilot Screening: Mental Health Issues', Fortune, Brooklyn, New York

Casos, D (ed.) 2010, 'Unmanned aircraft systems: strengths and weaknesses', *Nova Science Publishers*, New York

Catino, M 2010, 'The Linate Air Disaster: A Multilevel Model of Accident Analysis', *Crisis Management*, Nova Science Publishers, pp.187-210

Cordina, J, L & Couzelis, A, B 2004, 'Alerting system for aircraft crew', Patent: US 2004/0195449 A1, *I-Tex Design Systems*, Plano, United States

Daly, S, Seda, Y, Christian, J, Seifert, C & Gonzalez, R 2012, 'Design Heuristics in Engineering Concept Generation', *Journal of Engineering Education*, 101(4), pp.601-629

Diefenthaler, A, Erlho, M (ed.) & Marshall, T (ed.) 2008, 'Problem Setting, Design Dictionary: Perspectives on Design Terminology', p.306, *Birkhauser Basel*, Springer, Berlin

D'Alvia, G, R 2005, 'Cockpit access protection system', Patent: US 2005/0082429 A1, *Milde & Hoffberg*, White Plains, New York, United States

'Civil Aircraft Accident Report: ACCID/112913/1-12', 2016, *Ministry of Works and Transport: Directorate of Aircraft Accident Investigation*, Republic of Nambia, Windhock

Crawley, E et.al. 2004, 'The Influence of Architecture in Engineering Systems',*The ESD Architecture Committee Engineering Systems Monograph*, pp.1-2

de Castella, T 2015, 'How are pilots psychologically screened?', *BBC News Magazine*, 27th March 2015

Degani, A & Weiner, E, L 1997, 'Procedures in Complex Systems: The Airline Cockpit', *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 27(3), pp.302-312

'The European Plan for Aviation Safety (EPAS)', 2016, *European Aviation Safety Agency (EASA): European Strategic Safety Initiative (ESSI)*, Brochure, March 2016

Ferrell, T, K & Ferrell, U, D 2001, 'RTCA DO-178B/EUROCAE ED-12B: Software Considerations in Airborne Systems and Equipment Certification', *The Avionics Handbook*, Chapter 27, Technical Report, CRC Press

‘Final Report: Accident on 24 March 2015 at Prads-Haute-Bleone (Alps-de-Haute-Provence France) to the Airbus A320-211 registered D-AIPX operated by Germanwings’, 2016, *French Civil Safety Investigation Authority (BEA)*, Technical Report, Paris

France, R 2004, ‘Regulatory Reform in the Civil Aviation Sector’, *Organisation for Economic Co-operation and Development*, p.7

Gowrisankaran, G 2002, ‘Competition and Regulation in the Airline Indsutry’, *FRBSF Economic Letter*, 22(01), pp.1-3

Hoffman, E, Grand Perret, S, Zeghal, K 2000, ‘Pilot-in-the-loop evaluation of cockpit assistance for autonomous opeations’, *EUROCONTROL Experimental Centre*, p.2-5

Hyslop, J 2012, ‘The Invisible Plane’, *Air Crash Investigation: Mayday*, Television program, S11E12, Originally aired 23 March 2012

‘Introduction to TCAS II’, 2011, *U.S. Department of Transportation: Federal Aviation Administration*, Washington, pp.1-4, United States

Keith, L, A 1988, ‘System Design And Analysis’, Advisory Circular, *US Department of Transportation: Federal Aviation Administration*, pp.1-19

Koenig, R & Schubert, E 2014, ‘On the Influence of an Increased ILS Glide Slope on Noise Impact, Fuel Consumption and Landing Approach Operation’, *AIAC14 Fourteenth Australian Internation Aerospace Congress*

Lewis, R, Johnson, R Whinnery, J & Forster, E 2007, ‘Aircraft-Assisted Pilot Suicides in the United States, 1993-2202’, *Archives of Suicide Research*, 11(2), pp.149-161

Linshi, J 2015, ‘Why No One Agrees Whether Cockpit Doors Are Safer Locker or Open’, *Time*, 2nd April 2015, New York, United States

‘Maintenance Regulations: A guide to useful resources for CASRs Parts 42 and 145’, 2011, *Civil Aviation Safety Authority: Australian Government*, pp.1-2

Martens, L, Markle, B, L & Hebb, C, R 2005, ‘Flight Deck Security System’, Patent: US 2005/00116098, *Pearne & Gordon*, Cleveland, Ohio, United States

Moir, I & Seabridge, A 2008, ‘Aircraft Systems: Mechanical, Electrical and Avionics Subsystems Integration’, *John Wiley & Sons*, New York

Morrison, S & Winston, C 2010, ‘The Evolution of the Airline Industry’, *Brookings Institution Press*, Washington, pp.32-34

Ord, M 1972, ‘Airplane Hijacking Prevention System’, Patent: US 106 337, Pittsburgh, United States

Perhinschi, M G, Al Azzawi, D, Moncayo, H, Togayev, A & Perez 2015, ‘A Immunity based flight envelope prediction at post-failure conditions’, *Aerospace Science and Technology*, Vol. 46, pp.264-272

Perovic, J 2013, ‘The Economic Benefits of Aviation and Performance in the Travel & Tourism Competitiveness Index’, *International Air Transport Association (IATA)*, The World Economic Forum, Cologny

Politana, P, M & Walton, R, O 2015, 'Analysis of NTSB Aircraft-Asisted Pilot Suicides: 1982-2014', *Suicide and Life Threatening Behaviour*, 46(2), pp.234-238

'Radio Regulations', 2012, *International Telecommunication Union (ITU)*, Technical Bulletin, Vol. 4 p.2, Paris

Rose, B 2013, 'Plane truth: Aviation's Real Impact on People and the Environment', *Pluto Press*, London, pp.1-9

Sinha, S 2015, 'A History of Crashes Caused by Pilots' Intentional Acts', *The New York Times*, March 26 2015, New York

Ulrich, K, T & Eppinger, S, D 1995, 'Product Design and Development', Chapter 5: Concept Generation, *McGraw-Hill*, New York

Voss, W, Kaufman, E, O'Connor, S, Comtois, K, Conner, K & Ries, R 2013, 'Preventing addiction related suicide: A pilot study', *Journal of Substance Abuse Treatment*, 44(5), pp.565-569.

Wolochatiuk, T 2015, 'Carnage in Sao Paulo', *Air Crash Investigation: Mayday*, Television program, S15E10, Originally aired 16 February 2016

Zuckerman, L 1999, 'Some Crashes Classified as Deliberate', *New York Times*, November 17 1999, pp.8-9