Towards the Certification of Non-Deterministic Control Systems for Safety-Critical Applications

Analysing aviation analogies for possible certification strategies

Chris R. Burger
CSIR Meraka Institute
P O Box 395, 0001 Pretoria,
South Africa
crburger@csir.co.za

Thomas Jones
Department of Electrical and Electronic Engineering
Stellenbosch University
Private Bag X1, 7602 Matieland, South Africa
jones@sun.ac.za

Abstract—**Current certification criteria for safety-critical systems exclude non-deterministic control systems. This paper investigates the feasibility of using human-like monitoring strategies to achieve safe non-deterministic control using multiple independent controllers. An architecture is presented that could form the basis for a stochastic description based on knowledge representation, so that the behaviour of a non-deterministic control system can be constrained within safe boundaries.**

Keywords-certification; learning systems; safety-critical systems.

I. INTRODUCTION

Safety-critical control systems are normally subject to some form of certification. Examples include control of nuclear plants, ships, aircraft and road traffic management systems.

Such certification protocols attempt to guarantee system behaviour to some pre-selected limit. In aviation, a 10^{-10} probability of failure is often quoted as a reasonable cutoff.

Non-deterministic control systems have traditionally been explicitly excluded from such certification. Concerns revolve around possible divergent behaviour of such systems during operation.

Unfortunately, this blanket restriction prevents use of the most advanced classes of control systems, including learning systems. Learning systems and other adaptive control systems can provide significant advantages in operating efficiency and smoothness if their safety can be guaranteed.

Although such restrictions could be construed as non-negotiable, safety-critical systems are routinely operated by non-deterministic controllers, often employing more than one such control system in cooperation. Flight test engineers refer to such human control systems by the rather unflattering term of “meat servos”.

Humans that operate safety-critical control systems are indeed non-deterministic, exhibiting behaviour that changes with time, both gradually and temporarily. If a safety-critical system can be operated by human operators, it should in principle be possible to formulate a set of constraints under which other non-deterministic control systems can also be certified to any selected level of certainty.

The solution is expected to contain elements of knowledge representation, control system theory and domain-specific safety analysis.

This paper investigates conventions in a two-person aircraft cockpit as a first step in an attempt to formulate the problem well enough so that knowledge representation and control system theorists can continue towards obtaining a sufficiently rigorous description of the dynamics. Behaviour envelopes for resulting systems can then be described sufficiently well to guarantee system performance to a pre-determined safety standard.

Once this model is complete, work can start on the processes for certification of non-deterministic systems in any safety-critical field, including the examples quoted. Certification will revolve around analytical and statistical proof that the system is guaranteed to meet the target failure rate.

No similar attempt to model autonomous control system behaviour on human operators could be found in the literature. The observations are those of the first author, based on a working knowledge of ergonomics and control systems and on several thousand hours of participation in multi-crew flight operations. During these operations, a conscious effort was made to observe and discuss the thinking patterns of the pilots involved in a wide variety of roles.

The outcome is indispensable for robotic controllers in all regulated industries and for autonomous robots. Many applications of mobile robots depend strongly on predictable behaviour within defined constraints to eliminate the possibility of autonomous robots causing harm to humans and the surroundings. Certifying such predictable behaviour is central to the successful resolution of the liability issues around autonomous robots of all descriptions.

II. OVERVIEW OF TWO-CREW OPERATIONS

A. Regulatory restrictions

Guidelines from ICAO (the International Civil Aviation Organisation) dictate two-crew operations in most civil aircraft engaged in revenue services. Such operations are operated in South Africa under Part 121 or Part 135 of the Civil Aviation Regulations [2].

Modern large transport aircraft are generally certificated under regulations that similarly require two crew members as the minimum flight crew [1].

Pilots undergo rigorous initial certification, followed by recurrent testing at intervals of as little as six months in transport applications [2]. This recurrent testing revolves around demonstrated competence in a wide variety of situations, including simulated emergencies. Simulators are widely used in this application, both for affordability and for the ability to simulate situations that are too dangerous for real aircraft.

B. Pilot interaction and variability

Most airlines and charter operators have a structure of apprenticeship training that involves flying as copilot for some time. The copilot arrives with a specified minimum experience level, and then learns on the job while flying with an experienced captain.

Pilots in such operations may have widely divergent backgrounds. The work on cultural predisposition by Hofstede and others [3] has been used to model interactions between pilots in different cultures. The situation is further exacerbated by the international nature of the airline industry, often grouping pilots from widely divergent backgrounds in the same cockpit.

Issues such as authority gradient, assertiveness and decisiveness are named as determining factors for culturally-determined interactions in the cockpit [3].

- **Authority gradient** is the subordinate's perception of the authority that the senior holds over him or her. This perception can significantly inhibit the subordinate's willingness to contribute unpopular but necessary perspectives.
- **Assertiveness** is a person's willingness to stand his or her ground. This ability is most important when the subordinate is attempting to point out something that the senior may have overlooked or done incorrectly.
- **Decisiveness** is the individual's willingness to make decisions. It is often impeded by the individual's cultural role or even religious inclinations and is closely related to the individual's perception of his or her ability to affect the outcome of a series of events.

Individuals may also vary considerably in terms of temperament, background and experience.

Some operators select staff members according to temperament, finding that certain personality types are more suitable to certain operations than others.

Pilots from different backgrounds may also have been conditioned differently. Every culture has its own unique differences, but an oft-quoted example is the the contrast between pilots trained by the military and the civilian sector, with the military pilot's typically thinking being founded on more autocratic patterns. Helmreich [4] refers to the impact of national, cultural and professional cultures in this regard.

C. Similarities to non-deterministic control systems

Non-deterministic control systems have behaviour that could change with time. Small variations in digitisation of sensors or in the sensors themselves could result in divergent behaviour over time, where different controllers could learn different lessons from the same scenario, even when installed in the same airframe.

In addition, the principle of line replaceability will result in controllers that were not part of the original aircraft installation being installed in a particular aircraft. Such controllers could be in a factory-default state, or may have been exposed to a different set of circumstances, and may have learned behaviours that are widely divergent from those of the other controllers in the aircraft.

One of the attractions of learning controllers is that one particular controller can learn lessons that can then be transferred to the entire user base of controllers. If one aircraft has flown through a threatening weather pattern, for example, the entire user base can learn the lessons learned, either by cross-programming of learned weighting factors or by repeatedly being exposed to the same circumstances in a simulated environment. However, distributing revised software would involve a non-zero update interval, during which each controller could exhibit behaviours different from all others.

Because of these individual differences between non-deterministic controllers, their operation is not dissimilar to that of human pilots. Controllers could provide different control inputs in response to the same requirements. If the benefit of multiple redundancy is to be realised, a way has to be found to enable controllers to accept the behaviour of another controller, even if that controller's actions are different to its own preferred course of action. However, behaviour that could lead to dangerous situations must still be prevented or vetoed.

III. TECHNIQUES APPLIED IN TWO-CREW OPERATIONS

Post-war two-crew airline operations started with a single relatively well-qualified captain, typically a war veteran, with a second pilot as an assistant. This second pilot was typically inexperienced and served mainly to run errands for the captain.

During the Fifties, it was realised that the prevailing accident rate, combined with the growth in air traffic, would result in a major airliner crash every week by the Seventies. Furthermore, most crashes were not the result of equipment unserviceability, but rather of crew action or inaction. This realisation resulted in a major drive to redesign cockpit operations into a form that would better use the collective decision-making skills in multi-crew cockpits. The resulting techniques have become widespread, and are now included in pilot certification and recurrent testing requirements. The techniques are now most often referred to as Cockpit Resource Management (CRM).

CRM revolves around a few common principles:

- **Humans err:** Humans can and do make mistakes. Even captains.

- **High workload leads to low awareness:** A lightly-loaded person is less likely to make or overlook a mistake than someone who is being kept very busy. The presence of a second person, even when far less experienced, can therefore considerably enhance the safety of operations.
- **Handling skills:** Newly-trained pilots often have handling skills that surpass the atrophied skills of their more-experienced colleagues.

To accommodate these assumptions and to provide a platform for optimally coaching the copilot to become a captain eventually, the technique used most often is to fly sectors alternately, with the captain flying the one sector and the copilot flying the next. Only in exceptional circumstances do such pilots deviate from this pattern.

During such operations, four definitions are used to define roles:

- **Captain:** The captain takes ultimate responsibility for the flight and normally operates from the left seat, regardless of who is actually controlling the aircraft.
- **Copilot:** The copilot typically operates from the right seat, and is subordinate to the captain, regardless of who has the highest level of experience. The copilot often goes by the term “First Officer”.
- **Flying pilot (FP):** The pilot who is actually controlling the flight path of the aircraft at the time, either captain or copilot.
- **Monitoring pilot (MP):** The pilot who is not controlling the flight path of the aircraft, but is responsible for aircraft configuration and for liaison with the outside world and the cabin crew. The monitoring pilot is also responsible for identifying flight path deviations and bringing them to the attention of the FP.

Because of control station asymmetries, roles are often defined according to Captain and Copilot on the ground, but in flight the roles are most often defined as FP and MP.

A further definition required is the principle of a **Standard Operating Procedure (SOP)**. SOPs dictate speed and altitude profiles, power settings, crew interaction protocols, terminology, callouts (verbal cues used during crew interaction) and the assignment of roles and responsibilities in various phases of flight. They are normally compiled by the organisation, based on industry best practice.

IV. Control Strategies in Fly-by-Wire Aircraft

The intention of this paper is to draw analogies that can be used to define acceptable thresholds of behaviour for automatic control systems, so that slight differences in behaviour can be tolerated without jeopardising the safety of operations.

Some airliners and business aircraft now use fly-by-wire systems, in which the pilot has no direct control over the aircraft. Instead, the pilot’s thrust lever and sidestick or yoke inputs are interpreted by a control system, which then applies suitable control deflections to achieve the desired flight path.

In addition, most fly-by-wire aircraft include envelope protection systems. These systems impose limitations to the control system to safeguard a variety of parameters, including speeds, mach numbers, angles of attack, roll and pitch rates, g loading and absolute bank and pitch values. The pilot can therefore apply full control stick deflection with impunity, knowing that the control system should not allow safe values to be exceeded.

Due to the difficulty of making complex systems reliable, real-life control systems may implement simpler control algorithms that may allow limits to be exceeded in practice. When an absolute limit is approached at a very high rate, the limit may be overshot before corrective action takes effect. However, in emergency conditions pilots are encouraged to apply full control inputs if deemed necessary.

Certification authorities initially imposed very strong requirements on redundancy in fly-by-wire control systems. The first such platform to be certified in commercial use, the Airbus 320, used two completely independent controllers, each driving completely separate control surfaces, based on multiple microprocessors from different vendors, using different high-level languages and compilers from different vendors, and with the development teams having no access to one another’s work. The intention was to obviate the possibility of a common fault in both systems.

Traditional airliners, including modern Boeing designs, continue to give the pilot direct control of the aircraft, while providing a range of warnings when safe parameters are likely to be exceeded. Even in modern Boeing fly-by-wire airliners (777 and 787), the pilot is allowed to override the envelope protection system if required.

However, regardless of the architecture used, the FP typically does not provide direct control inputs to the system using a yoke or sidestick. Instead, the pilot provides guidance to an autopilot system, which then controls the flight path of the aircraft. Most airlines mandate the use of an autopilot during all phases of flight, except perhaps during some takeoffs and landings.

Further discussion in this paper assumes that there is already an envelope protection system in place, so that parameters that would pose an immediate threat to the safety of the aircraft would be excluded. It therefore assumes that the actual control of the aircraft is taken care of, and that the focus is on decision-making strategies instead. The control signals provided by this control system will be applied to the input of an existing autopilot, including an envelope protection system.

V. The Function of the Monitoring Pilot

The monitoring strategy between pilots is substantially different depending on whether the captain or the copilot is acting as FP. The captain always retains ultimate responsibility for the safe operation of the aircraft. When the copilot is the FP, the captain as MP can therefore be said to have a form of veto. The same is not true when the captain is the FP, as the

copilot at best can provide observations to be considered by the captain.

If non-deterministic control systems are to be allowed in safety-critical operations, certification requirements will include a similar mechanism, where behaviour outside pre-defined limits will result in control inputs being overridden by a monitoring system.

We therefore investigate the thought processes of an MP who has the right to veto the actions of the FP. Other situations, such as where equally senior pilots are flying together or where the captain is the FP, do not mirror the situation we are interested in as closely.

Background differences might lead pilots to apply different control inputs when faced with the same circumstances. These factors may or may not translate into the analogy of non-deterministic controllers, but some examples are offered to illuminate the differences that exist in human pilots:

- **Previous career path:** The pilot's origin and experience will influence decision making and behaviour. As an example, a former fighter pilot and a former civilian charter pilot might have widely-different attitudes to risk, passenger comfort and rule observance.
- **Flying experience:** A more experienced captain might have a better idea of how closely one could approach threatening weather because he or she may have done it hundreds of times before, while the less-experienced pilot might deviate more widely than necessary or may plunge into truly-threatening environments with too much confidence.
- **Recent scares:** A recent event in a pilot's career might have made him or her overly cautious in specific circumstances.
- **Personal circumstances:** The pilot may be preoccupied with personal, domestic or employment problems that might reduce alertness or temporarily alter risk tolerance.

It is therefore very likely that the MP's opinion may differ from the FP's regarding the actual control inputs required to achieve the desired result. There may even be differences of opinion on what exactly the desired outcome might be.

Intervening too often is not conducive to allowing the FP to learn optimally. In general, therefore, the MP will want to allow the FP to execute a control strategy to completion before intervening, provided that this control strategy will not result in a dangerous or excessively wasteful outcome.

Once the outcome is evident, or once the MP has decided to intervene, the MP may then discuss the situation with the FP, trying to maximise learning and ensuring that the FP's likely future behaviour is suitably corrected.

The first author has been involved for some decades in training flight instructors and pilots who operate in multi-crew environments. Because these pilots routinely have to decide whether to intervene when a student or copilot is seen to be making a mistake, the author has developed a formal model to help relatively inexperienced aircraft commanders to assess whether intervention is justified.

The MP extrapolates the outcome of the FP's actions and then compares this estimated final state with the desired state. The difference is then evaluated in terms of several factors:

- **Absolute limits in execution:** The estimated final state must be within absolute limits imposed by law, SOP, cost and safety risk. Other factors, such as prohibited airspaces, thunderstorms or noise abatement may similarly impose absolute limits on acceptable outcomes or on the trajectory followed to get there.
- **Certainty of the estimated outcome:** The MP's estimation of his/her own ability to accurately assess this outcome and its acceptability. An experienced MP can assess the outcome with greater certainty, leading to a large tolerance envelope. A less experienced MP cannot afford to allow wide deviations, as the outcome is not as certain to remain within acceptable limits.
- **Recovery potential:** The MP's estimation of his/her own ability to recover the resulting situation to an acceptable outcome. An experienced MP can allow wide deviations without jeopardising safety, while a less-experienced MP may have to operate within narrower limits.
- **Didactic value:** The MP's estimation of the likely value of allowing the control strategy to run to its natural conclusion so that resulting lessons can be learned. If a lesson is valuable, a greater deviation from the desired outcome can be tolerated.

In terms of the automated systems under discussion, these four factors can be said to define an envelope around the desired outcome within which the projected final state must fall if the MP is not to interfere with the FP's actions. The first factor is absolute, while the other three are strongly dependent on the MP's experience level.

VI. Implementing an Automated System

Figure 1 shows the proposed architecture for a monitored control system.

The diagram is deliberately generic, to allow tailoring to milieus other than aviation. Accordingly, the FP has been labeled as Controller and the MP as Monitor. The Controller could be made non-deterministic, and could consist of multiple redundant units as dictated by the required integrity. The Monitor could, as a first step, be made deterministic, using pre-determined Deviation Envelopes designed before certification. These envelopes would be based on similar considerations to those sub-consciously used by MPs—allowing maximum leeway to engender learning without creating a hazardous situation.

In safety-critical applications, both the Controller and the Monitor could consist of multiple units, using a voting or other multiple-redundant architecture.

The system has a series of sensors, providing environmental and performance inputs. In aviation, these sensors could include static pressure, dynamic pressure, temperature, icing indications, angle of attack and position information (e.g. GPS-derived coordinates). These sensors are used by both the Controller and the Monitor to determine the current state.

External inputs or policies are used by both Controller and Monitor to derive the Desired State. In plants, these inputs could be provided by demand forecasts or actual demand measurements. In aviation, these inputs would typically be provided by a combination of pre-programming and datalinked commands, including those from Air Traffic Control.

The Desired State should not be seen as the final objective, such as where the aircraft is safely parked at the gate and the passengers are in the building, or the nuclear plant is safely decommissioned at end of life. Instead, a series of shorter-term objectives are defined to facilitate concrete execution of an immediate plan. The defined architecture then ensures that the plan is executed within the constraints of the allowed envelope around the next Desired State.

SOPs are used by both Controller and Monitor to determine the most appropriate course of action to achieve the Desired State. These SOPs are typically formulated by the operator, taking into account best practices in the industry, as well as legal and other limits.

The Controller uses a Performance Model to determine a means to arrive at the Desired State. This Performance Model is variable, subject to a learning algorithm that is intended to improve with time.

The Controller provides control signals to control the plant. In the case of an aircraft, these control signals would be applied to the existing autopilot and flight control system, which would include a suitable envelope protection system to avoid exceeding airframe limits with inappropriate inputs. In aircraft that do not have such safeguards, limiting would have to be introduced between these control inputs and the existing autopilot. Similar assumptions would apply to other applications (such as nuclear plants) where threats like thermal runaway would most likely be regulated independently.

In normal operation, assuming that the Controller achieves an outcome sufficiently close to the Desired State determined independently by the Controller and the Monitor, the Monitor does not intervene in the Controller's operation, and the Controller fully controls the plant (or airframe). If the learning system performs as designed, performance should improve with time and the improved algorithms can be transferred to other similar controllers.

At all times, the Monitor will continue to derive a Current State from the sensors, independent of the Current State derived by the Controller. It also determines an independent approximation of the Desired State, independently derived from the same External Instructions and the SOP.

The Monitor will also attempt to reconstruct the Controller's intent by monitoring the control inputs provided to the plant (or autopilot). The intent inferred from these control inputs must then be examined to determine an Estimated Outcome, using a performance model similar to that used by the Controller to construct the normal control signal (except in a reverse sense). This Estimated Outcome is then compared to the Desired State. The discrepancy is tested for compliance with the Deviation Envelope. If an outcome outside the approved Deviation Envelope is detected, a Veto signal is issued. This signal can force the Controller to revert to deterministic behaviour, or can temper its actions to produce an Estimated Outcome that falls into the Deviation Envelope. A related signal can also be passed to the Controller to allow learning to take place, as the Controller must not learn behaviour that will consistently place its actions outside the acceptable Deviation Envelope.

A further function of the Monitor should be to calibrate its own estimate of the outcome (derived from the Controller's input to the autopilot) against the actual rate of change of the Current State to determine whether control inputs are indeed having the expected result. Phrased differently: The actual extrapolated Current State must converge to the Desired State.

This step becomes even more important if the Controller has the ability to apply exaggerated inputs to the plant in the case of unexpected behaviour, such as malfunctioning actuators or structural damage. In this case, because the actual plant response is not in accordance with the Performance Model used by the Controller and the Monitor, the inferred intent is likely to quickly diverge outside the Deviation Envelope, even though the Controller is in fact acting appropriately to compensate for a malfunction elsewhere in the system. The actual effect of the control inputs on the plant state must therefore be analysed to determine the actual partial effect of the control inputs.

VII. Long-Term Use of the Architecture

Initial certification of the proposed architecture is likely to occur around a very conservative system, using fail-safe strategies and a very tight Deviation Envelope.

As usage statistics accumulate, it should become possible to define a wider Deviation Envelope, hence allowing greater leeway to the learning systems.

Once the certification process and the system performance are sufficiently well understood, and based on the precedent of systems controlled by multiple humans with full authority, it could eventually become feasible to include learning capability in the Monitor too.

VIII. Future Directions in Research

Several steps remain in the process of bringing this goal to fruition:

- Describing the behaviour of a control system in stochastic terms.
- Finding envelopes within which such control system's behaviour is provably safe.
- Inferring intent from control inputs provided by a Controller on a closed-loop basis (i.e. taking into

account possible deviations in plant behaviour, such as damaged control surfaces or malfunctioning actuators).

- Building a safety case to constrain the provable safety level achievable by the system.
- Modifying blanket prohibitions on non-deterministic control systems in existing standards, including those used by military and civilian certification authorities, using the safety case compiled in the previous section.

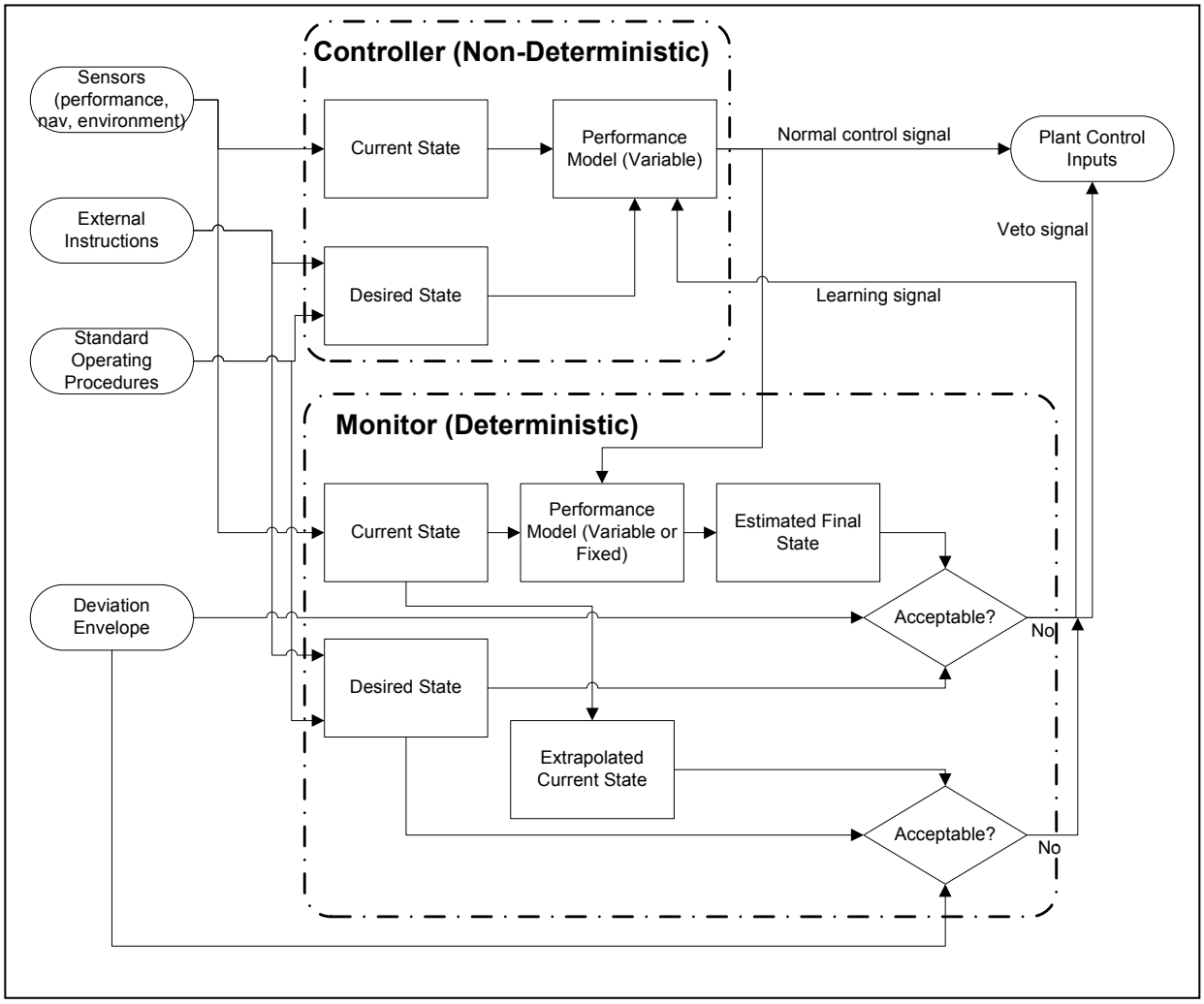

Figure 1: Proposed architecture for deterministic monitoring of non-deterministic control system.

REFERENCES

[1] Title 14 of the Code of Federal Regulations of the US Government, accessible at http://ecfr.gpoaccess.gov/, specifically Part 25 dealing with aircraft certification.

[2] CAR 121.02.1 and 135.02.1, accessible at http://www.caa.co.za/

[3] Helmreich R L, "Culture, threat and error: Assessing system safety", in *Safety in Aviation: The Management Commitment: Proceedings of a Conference*, Royal Aeronautical Society. Accessible at http://homepage.psy.utexas.edu/homepage/group/helmreichlab/

[4] Helmreich R L, "Building safety on the three cultures in aviation", in *Proceedings of the IATA Human Factors Seminar*, Bangkok, Thailand, 1999-08-12.