

Formal Analysis of Pilot Error with Agent Safety Logic

Seth Ahrenbach

University of Missouri, Columbia, Missouri

Alwyn Goodloe

NASA Langley Research Center

Abstract In this paper, we show that modal logic is a valuable tool for the formal analysis of human errors in aviation safety. We develop a modal logic called Agent Safety Logic (ASL), based on epistemic logic, doxastic logic, and a safety logic grounded in a flight safety manual. We identify a class of human error that has contributed to several aviation incidents involving a specific kind of pilot knowledge failure, and formally analyze it. The use of ASL suggests how future avionics might increase aircraft safety.

1 Introduction

Modal logic provides a rich set of tools for formal methods research. We apply modal logic to the domain of aviation safety to reason about pilot behavior during mishaps. Central to the quality of a pilot's decision-making is his *situational awareness*. Situational awareness is generally agreed to involve the pilot's knowing the pertinent facts of the aircraft's state so as to predict its behavior in a changing environment. Danger arises when the pilot lacks knowledge of the aircraft's state, but does not realize he lacks it. Thus there is a divergence between what the pilot believes to be the case and the actual state of the world. This divergence affects his actions, the quality of which often determine the outcome of the mishap. Formal methods from philosophy, mathematics, computer science, and economics have

been used to model and reason about an agent's knowledge, beliefs, and rational decision-making. Specifically, epistemic logic allows logicians to reason formally about an agent's state of knowledge. Doxastic logic allows logicians to reason formally about an agent's state of belief. We introduce a *Safety* modality for reasoning about the quality of a pilot's actions, whether they are safely permitted. We use the resulting logic, Agent Safety Logic (ASL), to analyze a class of aviation incidents involving a failure of what is called *negative introspection*: knowing what one's unknowns are. Simply put, the combined logics allow us to trace a logical thread from the pilot's actions to the information he lacks.

This paper proceeds as follows. Section 2 presents summaries of several aviation incidents spanning the past 40 years and identifies the relevant knowledge failures that played a crucial role in the pilots' dangerous actions. Section 3 introduces the modal logics we shall combine into ASL, and apply ASL to the class of pilot errors previously identified. Section 4 identifies future work. Section 5 discusses related work, and Section 6 concludes.

2 The Problem

This section provides summaries of several aviation incidents that involve a failure of negative introspection as an important component. We should note that we do not claim that a failure of negative introspection is the sole cause of any of these incidents. What typically happens in these cases is that the avionics encounters some contradiction in its data and gives control of the airplane to the pilot. The pilot then comes to rely on the false piece of data, not realizing that it is in conflict with

Seth Ahrenbach

Department of Computer Science, University
of Missouri, Columbia, Missouri, USA

E-mail: Seth.Kurtenbach@gmail.com

Alwyn Goodloe

NASA Langley Research Center, Hampton, Virginia

E-mail: a.goodloe@nasa.gov

other sources of information. He then provides input to the airplane that makes the situation worse. We focus on this one aspect of what is undoubtedly a much larger chain of events contributing to the crash. Indeed, a variety of factors often contribute to aviation incidents. Likewise, the interaction among crew members often contributes to the incident in complex ways. We hope to analyze the information flow among crew members in future work, but for this paper we show that our formal methods can successfully analyze a single moment of action for the pilot flying.

The following cases are all crewed flights that experienced a complex sequence of failures leading to fatal accidents. One element of each sequence involves a pilot not knowing that he does not know some important piece of information about the state of the plane, and taking incorrect actions. The pilot is confused, but unaware of the missing or contradictory data that is the true source of the confusion. We draw a distinction between simple confusion and this particular kind of knowledge failure for the following reason: if a pilot is simply confused about some state of the aircraft, and knows what he is confused about, he has available to him many protocols that can clear up his confusion or mitigate risk in spite of the confusion. Often, he can look to other instruments, or if that's not an option, provide control inputs specific to the type of confusion he is experiencing. For example, merely being confused about one's airspeed is not necessarily a problem, because a certain combination of thrust and pitch will guarantee that airspeed remains in a safe envelope until the problem is resolved. Pilots learn these procedures during training, and flight operations manuals specify which procedures to take in various circumstances.

The problems here arise when the pilot is unaware of the nature of his confusion, or fails to cross-check his instrument with the other instruments. In these situations, the pilot does not know that he does not know something, and may provide control inputs that make the situation worse, based on his false belief. It is this special kind of confusion, unawareness, that plays a role in the following cases.

Air India flight 855 from Mumbai, India to Dubai, UAE, January 1, 1978 [23] [21]. The Boeing 747 was flying over the Arabian Sea at night, when the captain's Attitude Indicator became incorrectly fixed in a right bank position. After miscommunication with the First Officer, whose Attitude Indicator read correctly, the pilot came to mistakenly believe that the plane was in a right bank, and directed the aircraft into a steep left bank. An additional backup Attitude Indicator would have settled the matter, but the Flight Engineer's at-

tempt to draw this to the pilot's attention proved too late, as seconds later the aircraft crashed into the sea.

Aeroperu flight 603 from Miami, Florida to Santiago, Chile, October 2, 1996 [14]. Around midnight and shortly after takeoff, the pilots became overwhelmed by a series of contradictory alarms, preventing an accurate assessment of the state of the Boeing 757. They knew they had a serious problem, but their specific knowledge failure here concerned their true altitude. A maintenance worker had placed tape over the static ports, which are required for a variety of instrument readings, including altitude. Among the contradictory alarms was the ground proximity warning system, which the pilots ignored, believing it to be a false alarm. According to the incident report, they believed the alarm was false because an Air Traffic Controller received the aircraft's false instrument readings, and read them back to the pilots as if they were independently confirmed. Unable to verify their altitude visually, and failing to notice the more accurate radar altitude reading due to information overload, the pilots allowed the plane to descend to the ocean's surface.

Birgenair flight 301 from Puerto Plata, Dominican Republic to Frankfurt, Germany, February 6, 1996 [13]. For 30 days the Boeing 757 sat dormant in a hangar in the Dominican Republic without a protective cover on its Pitot tubes. Somehow, likely due to a mud-dauber wasp nest, one of the Pitot tubes became clogged. The pilot noticed that his indicated airspeed was incorrect (too slow) during takeoff, but as the trapped air began to expand during ascent it created an artificially high indicated airspeed, and the pilot believed the problem to be fixed. Soon an overspeed alarm began to sound, resulting in the pilot decreasing thrust, despite an accurate reading from the co-pilot's airspeed indicator and the center console backup indicator both contradicting the pilot's indicator. The stall warning began to sound, causing information overload and confusion. Unaware of his dangerously low speed and high attitude, the pilot attempted to save the plane by increasing thrust, resulting in an engine flame out. The plane spiraled into the ocean.

Air France flight 447 from Rio de Janeiro, Brazil to Paris, France, June 1, 2009 [4]. The Airbus A330 encountered adverse weather over the Atlantic ocean, resulting in a clogged Pitot-static system. Consequently, the airspeed indicators delivered unreliable data concerning airspeed to the pilot flying, resulting in confusion. A chain of events transpired in which the pilot overcorrected the plane's horizontal attitude again and again, and continued to input nose up pitch commands, all while losing airspeed. Perhaps most confusing to the pilot was the following situation:

the aircraft's angle of attack (AOA) was so high it was considered invalid by the computer, so no stall warning sounded until the nose pitched down into the valid AOA range, at which point the stall warning would sound. When the pilot pulled up, the AOA would be considered invalid again, and the stall warning would cease. The aircraft entered a spin and crashed into the ocean. Palmer [25] argues that had the pilot merely taken no action, the Pitot tubes would have cleared in a matter of seconds, and the autopilot could have returned to Normal Mode.

In each of the above cases, the pilot does not know some crucial piece of information, and he is unaware of this failure, even though he knows there is a problem in general. Several cases also involve confusion due to information overload and contradictory alarms. The relevant data often were directly available to the pilot in each case, but he failed to notice them, and formed a false belief based on what he saw. Had he noticed, there is a good chance he would have realized his knowledge failure and ceased to provide problematic inputs to the aircraft. Thus, the problem is not an absence of information, but that a more appropriate management of its relationship with the pilot's mental state is needed. Examining these incidents on this level of abstraction reveals a specific similarity among them. Having established that this class of errors exists, we turn to their formal analysis using epistemic logic.

3 The Logic

The logics we use in this paper belong to a family of modal logics, which increase the expressiveness of propositional logic with modal operators for things like necessity and possibility [19, 29, 5]. Epistemic logic is a modal logic for reasoning about knowledge [16, 15]. It was developed by philosophers and economists who were interested in formally analyzing knowledge in agent-based systems. Doxastic logic is a related logic for reasoning about belief [17]. Modal logics often share a related semantics, called Kripke semantics, and they differ primarily in the details of those semantics and their interpretation or application to the real world.

A Kripke frame is a tuple $\langle W, R_i \rangle$, where W is a non-empty set of possible worlds, and each R_i is a relation between worlds. We can obtain different modalities by varying conditions that constrain the relation. A modal logic corresponds to a class of frames with each axiom in the logic uniquely determined by a single frame condition. A multi-modal logic, that is, a logic with more than one modal operator, has a relation R_i for each modal operator. Our logic contains modal op-

erators for a single pilot's belief and knowledge, with relations R_b and R_k respectively.

A Kripke structure is a graph that serves as semantics for modal logics. Formally, the structure is a tuple $\langle W, R_i, V \rangle$, where W is a set of worlds, R is a relation $R \subseteq W \times W$, and V is a valuation function that takes a propositional constant and returns the set of worlds in which the proposition is true. A Kripke structure is basically a Kripke frame with propositional constants added to each world, corresponding to what is true and false in each world.

The general syntax for a modal logic is the following:

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \psi \mid \Box\varphi,$$

where p is a propositional constant from some set of propositional constants, and \Box denotes *necessity*.

The language has the semantics given in Figure 1. We define \vee , \Rightarrow in the usual way, and the operator $\Diamond \equiv \neg\Box\neg$, denoting possibility. Our modal logics for this paper will be identical syntactically and semantically to these general definitions, but for the syntax and semantics for the modal operators, which will have relations specific to them.

In addition to the above semantics, all *normal* modal logics include the following rules of inference:

$$\text{NECESSITATION: } \frac{\vdash \varphi}{\vdash \Box\varphi}$$

$$\text{MODUS PONENS: } \frac{\vdash \varphi \quad \vdash \varphi \Rightarrow \psi}{\vdash \psi}$$

The modal logic we describe is normal, and so includes the above inference rules, with the appropriately substituted modal operator in the case of *Necessitation*.

Having described modal logic in general, we now turn to the specific modal logics to be used in this paper.

3.1 Epistemic Logic

In all of the cases we consider, we wish to reason about what a pilot does not know, and as such, we must be able to formally express this. This section describes the epistemic logic that we will use.

The syntax and semantics are the same as those for all modal logics, with the relation R_k denoting an epistemic relation between worlds for a pilot. The relation captures the notion of how the world might be, given the evidence available to the agent. For our pilot, a world is the current state of the airplane, and the

$$\begin{aligned}
& \text{For } w \in W, R \subseteq W \times W, \\
& V : PropConst \rightarrow \mathcal{P}(W), \\
\\
& W, w \models p \quad \text{iff} \quad w \in V(p) \\
& W, w \models \neg\varphi \quad \text{iff} \quad \text{not } W, w \models \varphi \\
& W, w \models \varphi \wedge \psi \quad \text{iff} \quad W, w \models \varphi \text{ and } W, w \models \psi \\
& W, w \models \Box\varphi \quad \text{iff} \quad \text{For all } u \text{ s.t. } wRu, W, u \models \varphi \\
& \text{not } W, w \models \text{False}.
\end{aligned}$$

Fig. 1: The Semantics of Modal Logic

way the world might be depends on what his instruments say. If one altimeter reads 30,000 feet and another reads 20,000 feet, then the pilot considers both to be possible, and therefore does not know his altitude. That is, of course, assuming he notices the discrepancy. If he has paid attention to only one altimeter, then he might believe something false. To capture this scenario, we introduce doxastic logic in the next section.

We use the normal Kripke semantics for truth in our models. The relation defined over the Kripke frame is reflexive and transitive, satisfying the desired epistemic properties, presented below. We denote knowledge with the \mathbf{K} operator, which corresponds to \Box above. We denote epistemic possibility, the dual of knowledge, with $\langle \mathbf{K} \rangle$, defined $\langle \mathbf{K} \rangle \equiv \neg \mathbf{K} \neg$, just as with \Diamond above.

Epistemic logic includes the following axioms with corresponding frame conditions, which represent idealized assumptions about knowledge.

The first axiom holds for all Kripke structures, so any system to be reasoned about using a modal logic with Kripke semantics must include this axiom.

Axiom 1 (Distribution of \mathbf{K})

$\mathbf{K}(\varphi \Rightarrow \psi) \Rightarrow (\mathbf{K}\varphi \Rightarrow \mathbf{K}\psi)$. *An agent knows everything that is a logical consequence to his knowledge, also called logical omniscience.*

We follow the standard view in epistemology that truth is a necessary condition for knowledge. Formally, this corresponds to a frame condition saying the epistemic relation is reflexive, meaning that for all worlds w , $(w, w) \in R_k$, yielding the following axiom:

Axiom 2 (Knowledge is True) $\mathbf{K}\varphi \Rightarrow \varphi$

The next axiom says that an agent may reflect on what he knows and be aware of it, called Positive Introspection.

Axiom 3 (Positive Introspection) $\mathbf{K}\varphi \Rightarrow \mathbf{K}\mathbf{K}\varphi$.

If an agent knows that ϕ , then he knows that he knows that ϕ .

The axiom of Positive introspection corresponds to a transitive property of the epistemic relation.

The fourth condition says that an agent can reflect on what he currently does not know and be aware of it. In Rumsfeldian terms, all unknowns are known unknowns. Formally, this corresponds to a frame condition that the epistemic relation satisfies the Euclidean property, which, in conjunction with the other properties, makes the relation an equivalence relation.¹

Property 1 (Negative Introspection) $\neg \mathbf{K}\varphi \Rightarrow \mathbf{K}\neg \mathbf{K}\varphi$. If an agent does not know ϕ , then he knows that he does not know ϕ .

A moment's reflection reveals that the idealized assumptions do not hold generally for human knowledge. However, assuming them as idealizations causes no harm for the most part, with the exception of Negative Introspection. We are concerned with identifying failures of *negative introspection* for the pilot and correcting them. We can assist the pilot in becoming more like an ideal reasoner, resulting in better decisions. In formalizing the above class of errors, we relax the assumption that the pilot has *negative introspection*, but we keep the other properties as axioms. To avoid confusion, *negative introspection* is labelled as a mere property which may or may not be true of a model. Table 1 summarizes the frame conditions and the corresponding axioms of our epistemic logic.

Theorem 1 *For all formulas ϕ and ψ , and models M with R_k as a reflexive, transitive relation, the following hold:*

1. $M \models (\mathbf{K}\varphi \wedge \mathbf{K}(\varphi \Rightarrow \psi)) \Rightarrow \mathbf{K}\psi$.
2. $M \models \mathbf{K}\varphi \Rightarrow \varphi$.
3. $M \models \mathbf{K}\varphi \Rightarrow \mathbf{K}\mathbf{K}\varphi$.

Proof See [16] pages 33-34. \square

¹ A Euclidean relation is defined as follows, for any relation R , and elements x, y, z , if $(x, y) \in R$, and $(x, z) \in R$, then $(y, z) \in R$.

| Frame Condition | Axiom |
|--|--|
| N/A | Distribution Axiom (Knowledge) $\mathbf{K}(\varphi \Rightarrow \psi) \Rightarrow (\mathbf{K}\varphi \Rightarrow \mathbf{K}\psi).$ |
| Reflexive $wR_k w$ | Knowledge is True $\mathbf{K}\varphi \Rightarrow \varphi$ |
| Transitive $wR_k u \wedge uR_k v \implies wR_k v$ | Epistemic Positive Introspection $\mathbf{K}\varphi \Rightarrow \mathbf{K}\mathbf{K}\varphi.$ |

Table 1: Epistemic Logic Frame Conditions and Corresponding Axioms

Our model of a pilot's mental situation requires a distinction between belief and knowledge, and we have the logical tools accomplish this by introducing another modality. Next we introduce and discuss doxastic logic.

3.2 Doxastic Logic

The syntax for doxastic logic is exactly analogous to that of epistemic logic, with the \mathbf{B} operator replacing \mathbf{K} , and $\langle \mathbf{B} \rangle$ replacing $\langle \mathbf{K} \rangle$ [17]. Similarly, the semantics are Kripke structures, with the accessibility relation determined by slightly different frame conditions.

Doxastic logic, like Epistemic logic, allows \mathbf{B} to distribute over \Rightarrow :

Axiom 4 (Distribution of B)

$\mathbf{B}(\varphi \Rightarrow \psi) \Rightarrow (\mathbf{B}\varphi \Rightarrow \mathbf{B}\psi).$

The primary difference between knowledge and belief is that beliefs might be false. Thus, the doxastic relation should not be valid on reflexive frames, a condition which guarantees truth. Instead, we follow the literature by imposing a relaxed condition, that agents' beliefs are consistent. Formally, this corresponds to a serial frame condition on the doxastic relation stating that for all w , there exists a u such that $wR_b u$.

Axiom 5 (Non-Contradiction) $\mathbf{B}\varphi \Rightarrow \langle \mathbf{B} \rangle \varphi$. *An agent does not believe conflicting beliefs. Equivalently $\neg(\mathbf{B}\varphi \wedge \mathbf{B}\neg\varphi)$.*

Just as with knowledge, and perhaps more realistically, we assume agents have positive introspection regarding beliefs.

Axiom 6 (Belief Positive Introspection)

$\mathbf{B}\varphi \Rightarrow \mathbf{B}\mathbf{B}\varphi$. *If an agent believes that φ , then he believes that he believes φ .*

The standard approach to doxastic logic, as with epistemic logic, imposes a Euclidean condition on the doxastic relation. Without reflexivity, this does not amount to equivalence, but it is still expressed by a negative introspection property exactly analogous to the one we omit regarding knowledge. We include it for our doxastic relation.

Axiom 7 (Belief Negative Introspection)

$\neg\mathbf{B}\varphi \Rightarrow \mathbf{B}\neg\mathbf{B}\varphi$. *If an agent does not believe that ϕ , then he believes that he does not believe that ϕ .*

The above axioms are valid for frames with a serial, transitive, and reflexive doxastic relation. Table 2 summarizes the frame conditions and their corresponding axioms.

Theorem 2 *For all formulas ϕ and ψ , and models M with R_b as a serial, transitive, Euclidean relation, the following hold:*

1. $M \models (\mathbf{B}\varphi \wedge \mathbf{B}(\varphi \Rightarrow \psi)) \Rightarrow \mathbf{B}\psi.$
2. $M \models \neg\mathbf{B}(\varphi \wedge \neg\varphi).$
3. $M \models \mathbf{B}\varphi \Rightarrow \mathbf{B}\mathbf{B}\varphi.$
4. $M \models \neg\mathbf{B}\varphi \Rightarrow \mathbf{B}\neg\mathbf{B}\varphi.$

Proof (1) Suppose $M, w \models (\mathbf{B}\varphi \wedge \mathbf{B}(\varphi \Rightarrow \psi))$. Then $M, w \models \mathbf{B}\varphi$ and $M, w \models (\mathbf{B}\varphi \Rightarrow \mathbf{B}\psi)$. By R_b , for all u such that $wR_b u$, $u \models \varphi$ and $u \models \varphi \Rightarrow \psi$. So $u \models \psi$. Thus, for all u , where $wR_b u$, $u \models \psi$, and therefore $M, w \models \mathbf{B}\psi$.

(2) Suppose that $M, w \models \mathbf{B}(\varphi \wedge \neg\varphi)$. Because R_b is serial, there exists some u such that $wR_b u$, and by definition of \mathbf{B} , it must be that $u \models \varphi \wedge \neg\varphi$, a contradiction. Thus, for all $w, M, w \models \neg\mathbf{B}(\varphi \wedge \neg\varphi)$.

(3) Suppose $M, w \models \mathbf{B}\varphi$, then $M, u \models \varphi$ for all u such that $wR_b u$. Since R_b is serial, there is a world v such that $uR_b v$. Because R_b is transitive then $wR_b v$. From the definition of \mathbf{B} and $wR_b v$ it follows that $v \models \varphi$. Since $uR_b v$ we can conclude $u \models \mathbf{B}\varphi$. Since $wR_b u$, $M, w \models \mathbf{B}\mathbf{B}\varphi$.

(4) Suppose $M, w \models \neg\mathbf{B}\varphi$. Because R_b is Euclidean, for all w, u, v , if $wR_b u$ and $wR_b v$, then $uR_b v$. By definition of $\langle \mathbf{B} \rangle$, $w \models \langle \mathbf{B} \rangle \neg\varphi$, so for some u , such that $wR_b u$, $u \models \neg\varphi$. For all v , such that $wR_b v$, $vR_b u$. Thus, $v \models \langle \mathbf{B} \rangle \neg\varphi$, or equivalently, $v \models \neg\mathbf{B}\varphi$. Therefore, $M, w \models \mathbf{B}\neg\mathbf{B}\varphi$. \square

This concludes our discussion of the doxastic component to our logic, and we now turn to combining the modalities.

| Frame Condition | Axiom |
|---|--|
| N/A | Distribution Axiom (Belief) $\mathbf{B}(\varphi \Rightarrow \psi) \Rightarrow (\mathbf{B}\varphi \Rightarrow \mathbf{B}\psi)$ |
| Serial $\forall w \exists u. (w, u) \in R_b$ | Non-Contradiction $\neg \mathbf{B}(\phi \wedge \neg\phi).$ |
| Transitive $(w, u) \in R_b \text{ and } (u, v) \in R_b \Rightarrow (w, v) \in R_b$ | Belief Positive Introspection $\mathbf{B}\varphi \Rightarrow \mathbf{B}\mathbf{B}\varphi.$ |
| Euclidean $(w, u) \in R_b \text{ and } (w, v) \in R_b \Rightarrow (u, v) \in R_b$ | Belief Negative Introspection $\neg \mathbf{B}\varphi \Rightarrow \mathbf{B}\neg \mathbf{B}\varphi.$ |

Table 2: Doxastisc Logic Frame Conditions and Corresponding Axioms

3.3 Combining the Logics

When we combine these two modal logics, we generate the multimodal logic **ASL**, for “Agent Safety Logic”. We must define the conditions that govern the relationship between the modalities, that is, how knowledge and belief logically interact.

The semantics of ASL is defined in terms of both the epistemic and doxastic relation. The frame condition $R_b \subseteq R_k$ imposes a partial order on the modalities [1]. The partial order gives rise to a basic property of knowledge, that knowledge entails belief.

Axiom 8 (Knowledge Entails Belief) $\mathbf{K}\varphi \Rightarrow \mathbf{B}\varphi$.
If a pilot knows that ϕ , then he believes that ϕ .

However, knowledge and belief are still distinct from each other, because one can generate a counterexample to the converse epistemic principle, that belief entails knowledge. Instead, we impose a restricted version of the converse, expressed by an axiom to follow. We denote justified belief by the composition of the R_b and R_k relations: $R_k \circ R_b$. This captures the internal component of justification, where the pilot has direct epistemic access to his reasons for believing a proposition. If he believes it, and he has a good reason, then he thinks it is true, so he thinks he knows it. Thus, he justifiably believes p iff he believes that he knows p .

Counterexample $\neg(\mathbf{B}\varphi \Rightarrow \mathbf{K}\varphi)$. Consider the world $W = \{t, u, v\}$ with the following truth assignment $v \notin V(\varphi)$, $u \in V(\varphi)$, and $t \in V(\varphi)$, and the following relation over W :

$$R_k = \{(v, v)\} \cup R_b$$

$$R_b = \{(v, u), (u, t), (t, u), (t, t), (u, u)\}$$

This is illustrated in Figure 2, where R_k is represented by the dotted edge and R_b by the solid edges. We therefore have $v \models \mathbf{B}\varphi$, because $u, t \models \varphi$, but $v \models \neg \mathbf{K}\varphi$, because $v \models \neg\varphi$.

Axiom 9 (Justified Belief) $\mathbf{B}\varphi \Rightarrow \mathbf{B}\mathbf{K}\varphi$. If a pilot believes that φ , then he believes that he knows that φ .

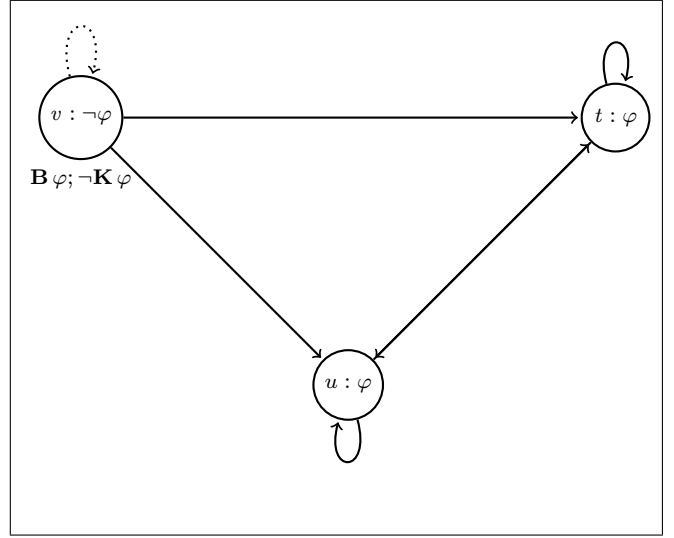


Fig. 2: Counterexample

This corresponds to the frame condition $(R_k \circ R_b) \subseteq R_b$, and represents the restricted converse of Axiom 8, and the view that pilots believe things about the aircraft only if they have good reason, like a particular instrument reading indicating as much. We can think of this property as representing the notion that all pilot beliefs are justified, even if they are in fact false.

Table 3 summarizes the axioms and frame conditions of the combined logic.

The following lemma follows from Axiom 9.

Lemma 1 (Epistemic Principle 2)

$\mathbf{B}\mathbf{K}\varphi \Rightarrow \neg \mathbf{K}\neg \mathbf{K}\varphi$. If a pilot believes that he knows that φ , then he does not know that he does not know that φ .

Proof From Axiom 5 $\mathbf{B}\mathbf{K}\varphi \Rightarrow \langle \mathbf{B} \rangle \mathbf{K}\varphi$, and the contraposition of Axiom 8 yields $\langle \mathbf{B} \rangle \mathbf{K}\varphi \Rightarrow \neg \mathbf{K}\neg \mathbf{K}\varphi$. \square

For this principle to be applied to the real world, we must ask whether agents can believe they know something even if they know that they do not know it, for in that case the principle would be falsified. Cases like this might occur when sensory input conflicts with level-headed rational thinking, as in a hallucination or spatial

| Frame Condition | Axiom |
|--|--|
| Partially Ordered $R_b \subseteq R_k$ | Knowledge Entails Belief $\mathbf{K} \varphi \Rightarrow \mathbf{B} \varphi$. |
| Composition $(R_k \circ R_b) \subseteq R_b$ | Justified Belief $\mathbf{B} \varphi \Rightarrow \mathbf{B} \mathbf{K} \varphi$ |

Table 3: EDL Frame Conditions and Corresponding Axioms

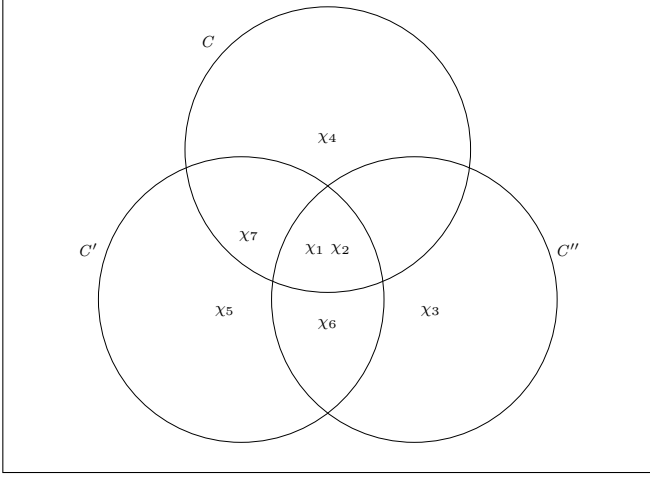


Fig. 3: $FSM(\alpha) = C \vee C' \vee C''$.
 $MSC(\alpha) = (\chi_1 \wedge \chi_2) = \chi$

disorientation. Indeed, such confusions can occur during flight, where a pilot's senses create a powerful feeling of one orientation or another, which disagrees with all reason and instrumentation. Pilots are trained to ignore their senses in these situations, and rely instead on their instruments. This research does not address pilot training, so we assume the pilots in our model follow their training, and resist beliefs that conflict with knowledge based on instrumentation. The cases we have selected for analysis involve false beliefs based on faulty instruments or inattention, not adverse sensory perception, so we avoid the cases where Lemma 1 might not apply.

This concludes our discussion of epistemic and doxastic logic. We now turn to a formalization of safety.

3.4 Formalizing Safety

Results from game theory and decision theory establish a strong connection between the quality of an agent's decision and his epistemic state [2] [3]. We follow the spirit of these results in our formalization of pilot rationality, although we leave many formal details for future work. Note that we use 'rationality' as a technical term here, meaning roughly that an agent makes decisions based on minimizing some measure of disutility associated with actions, determined by a flight safety manual.

For rationality, we are concerned only with whether a pilot's action is safe given what he believes the current flight data to be. Safety propositions are of the form 'the flight data χ say action α is safe'. A pilot's rationality then, is a logical connection between action and beliefs about safety propositions.

Think of the flight safety manual as an association between actions and complete configurations of instrument readings, formalized as the function $FSM(\alpha)$:

$$FSM(\alpha) = (\chi_0 \wedge \dots \wedge \chi_n) \vee (\chi_m \wedge \dots \wedge \chi_k) \dots$$

It indicates the conditions χ_i under which an action is safe. Each conjunction $(\chi_i \wedge \dots \wedge \chi_j)$ is a maximally complete configuration C of instrument readings, χ_i . Each instrument reading χ_i is an atomic proposition of type $FD \subset PropConst$, where FD stands for flight data. Each action α is an atomic proposition of type $Actions \subset PropConst$. For notation purposes, if a configuration's conjunction does not contain a propositional constant, then that constant is false in the conjunction.

The flight safety manual may indicate that an action is safe under many possible configurations. We identify the instrument readings that are true in all safe configurations by simplifying the FSM , extracting each constant and its negation, for example:

$$simplify((p \wedge q \wedge s) \vee (p \wedge q \wedge \neg s)) = p \wedge q$$

To associate with each action a particular partial configuration, we define the *minimal safety condition* MSC :

$$MSC(\alpha) \stackrel{def}{=} simplify(FSM(\alpha)),$$

which yields a conjunction of χ_i instrument readings true in all safe configurations. This conjunction is no longer maximally complete, so it is called a partial configuration. We refer to this conjunction with the special name χ .² Figure 3 illustrates the definition of FSM and MSC of α .

A safety proposition can be formalized using a modal operator \mathbf{S} , where $\chi \mathbf{S} \alpha$ stands for: the configuration χ says α is safe, according to the flight safety manual.

² A special case is if the $FSM(\alpha)$ simplifies to complementary conjunctions, in which case χ is their disjunction.

We extend the syntax of our logic to include safety.

$$\varphi ::= \dots \mid \chi \mathbf{S}\alpha \mid ,$$

For the semantics of \mathbf{S} , we have the following:

$$w \models \chi \mathbf{S}\alpha \text{ iff } w \models \chi \wedge \exists v, w(\text{Safety})v \wedge v \models \alpha$$

We define the *Safety* relation in terms of the *MSC* relation:

$$\text{Safety} \stackrel{\text{def}}{=} \{(w, v) \mid w \in V(\text{MSC}(\alpha)), v \in V(\alpha)\}.$$

The following lemma holds.

Lemma 2 (Safety to Flight Data) $\chi \mathbf{S}\alpha \Rightarrow \chi$. *If χ says α is safe, then χ is true.*

Proof Suppose $w \models \chi \mathbf{S}\alpha$. Then $w \models \chi$, by the semantics of \mathbf{S} . \square

In addition, we define

$$\text{Safety}(w) \stackrel{\text{def}}{=} \{v \mid (w, v) \in \text{Safety}\},$$

where $\text{Safety}(w)$ is a partial application of the *Safety* relation, returning the set of worlds in the relevant codomain, specifically those with the permissible actions. This allows us to define basic pilot safety.

For basic pilot safety, the notion of rationality we are concerned with, we want the following intuitive situation to hold. Take a world at which α holds and step down the doxastic relation to another world, w' , where χ the minimal safety condition of α is true, and from there one may find a world v reachable by the *Safety* relation where α is true, capturing the notion that a pilot believes he is in a world where α is safe according to the current flight data. Formally, this is:

Property 2 (Basic Pilot Safety Condition) A pilot has basic safety iff for all actions α , and for all $w \in V(\alpha)$, $R_b(w) \subseteq V(\chi)$, where $\chi = \text{MSC}(\alpha)$, and $(\text{Safety} \circ R_b)(w) \cap V(\alpha) \neq \emptyset$.

Axiom 10 (Basic Pilot Safety) $\alpha \Rightarrow \mathbf{B}(\chi \mathbf{S}\alpha)$. *A basically safe pilot engages in action α only if he believes that the flight data indicate the action is safe.³ This is perhaps the weakest claim one can make about the nature of rationality, wherein the pilot acts only if he at least believes the action to be overall safe.*

Theorem 3 (BPS Valid) *Axiom 10 is valid for all frames with Property 2.*

³ Sometimes pilots will take “unsafe” action to mitigate what they perceive to be the greatest safety concern. For our purposes, we consider the action’s warrant in terms of the all-things-considered safety of the plane.

Proof Suppose $w \models \alpha$. Because the pilot is basically safe,

$$R_b(w) \subseteq V(\chi) \text{ and } (\text{Safety} \circ R_b)(w) \cap V(\alpha) \neq \emptyset.$$

The doxastic relation is serial, so there is at least one world, call it w' , such that wR_bw' . Then, by the BPS condition, χ is true at w' , and we can partially apply *Safety* to w' and find some v such that $w'(\text{Safety})v$, and $v \models \alpha$, also by the BPS condition. Recall the semantics of $w' \models \chi \mathbf{S}\alpha$, that $w' \models \chi$ and there exists some v , where $w'(\text{Safety})v$ and $v \models \alpha$. This holds for w' , so $w' \models \chi \mathbf{S}\alpha$. Since wR_bw' , it follows that $w \models \mathbf{B}(\chi \mathbf{S}\alpha)$. \square

From this we deduce the following stronger property of pilot rationality.

Lemma 3 (Pilot Rationality) $\alpha \Rightarrow \mathbf{BK}(\chi \mathbf{S}\alpha)$, *where α is the proposition that the pilot engages in some action. The pilot performs some action (which turns out to be dangerous) only if he believes that he knows that the flight data indicates that the action is safe. In essence, the pilot acts only in ways that he thinks he knows are overall safe. The principle highlights the fact that rational pilots are cautious and risk-averse.*

Proof Follows from Axiom 9 and Axiom 10. \square

Finally, we complete the thread from action to knowledge of flight data, with the following theorem.

Theorem 4 (Action to Flight Data) $\alpha \Rightarrow \mathbf{BK}\chi$. *A pilot engages in an action only if he believes that he knows some relevant flight data.*

Proof Follows from Lemma 3 and Lemma 2. \square

3.5 Analyzing Pilot Error

We can now use these formal tools to analyze the class of accidents from section 2. We formalize the accidents in the same way that one might formalize an argument in natural language, or represent a circuit as a formula in digital logic. We identify aspects of the case that matter logically, and appropriately represent them in the formal language. We start with Air India Flight 855, wherein the pilot did not know the plane’s attitude, but provided banking commands as if he did know.

Example (Air India 855) Let α be the proposition, “the pilot commands a steep left bank.” Let χ be the flight data expressing the proposition “all artificial horizons indicate a steep right bank”. As a matter of fact, χ is false, because the current flight data included contrary bank attitude data, which proscribed a steep left

| Frame Condition | Axiom |
|---|---|
| BPS Condition $\forall \alpha, \forall w \in V(\alpha), R_b(w) \subseteq V(\chi) \text{ and } (Safety \circ R_b)(w) \cap V(\alpha) \neq \emptyset$ | Basic Pilot Safety $\alpha \Rightarrow \mathbf{B}(\chi \mathbf{S} \alpha)$ |

Table 4: Basic Pilot Safety Frame Condition and Corresponding Axiom

bank. By Axiom 2, we have $\neg \mathbf{K} \chi$. We assume the pilot is minimally rational, so he commands a steep left bank only if he believes that he knows the aircraft's bank attitude permits a steep left bank: $\alpha \Rightarrow \mathbf{B} \mathbf{K}(\chi \mathbf{S} \alpha)$. Furthermore, it follows that he believes he knows χ , the flight data that would make α safe: $\alpha \Rightarrow \mathbf{B} \mathbf{K} \chi$. Of course, it is also a fact of the case that the pilot commands a steep left bank, α . Thus, he believes that he knows the relevant data: $\mathbf{B} \mathbf{K} \chi$. By *Epistemic Principle 2*, it follows that he considers it possible that he knows his action is permitted by the data: $\neg \mathbf{K} \neg \mathbf{K} \chi$. Thus, combining this with the earlier fact of the case, we have $\neg \mathbf{K} \chi \wedge \neg \mathbf{K} \neg \mathbf{K} \chi$. But recall from propositional logic that $\varphi \wedge \neg \psi \equiv \neg(\varphi \Rightarrow \psi)$. Substituting $\varphi := \neg \mathbf{K} \chi$, and $\psi := \mathbf{K} \neg \mathbf{K} \chi$, we have, $\neg(\neg \mathbf{K} \chi \Rightarrow \mathbf{K} \neg \mathbf{K} \chi)$, which is the failure of negative introspection about the flight data safety-related to his dangerous action.

Example (Birgenair 301)

- Let $\chi \equiv$ “The airspeed data all indicate a dangerously high airspeed”
- $\alpha \equiv$ “The pilot reduces thrust.”

Then we have, by the same reasoning as above, a failure of negative introspection that the airspeed data all indicate a dangerously high airspeed. That is, he does not know the airspeed data are such and such, and he does not know that he lacks this knowledge.

By identical reasoning and the appropriate assignment of propositions, one can formally prove that in each of the cases previously presented, a failure of negative introspection logically follows. We illustrate this in Table 5.

In each case, the pilot performs some dangerous action, and he does not know some data appropriately related to that action, whether it be airspeed or control mode. Our analysis proceeds by formally representing the general form of the cases, wherein a pilot is rational, takes dangerous action, and lacks relevant knowledge. The analysis yields the following theorem.

Theorem 5 (Negative Introspection Failure) *A rational pilot lacking knowledge of data entailing an action to be safe performs that action only if he lacks negative introspection regarding the safety-related data to that action.*

Proof We assume that the pilot acts in some dangerous way, $w \models \alpha$, and that he lacks knowledge of some relevant information, $w \models \neg \mathbf{K} \chi$. We proceed to show that $w \models \neg \mathbf{K} \neg \mathbf{K} \chi$ follows. By Lemma 3 the pilot does α only if he believes he knows the current flight data χ says α is safe: $\alpha \Rightarrow \mathbf{B} \mathbf{K}(\chi \mathbf{S} \alpha)$, from which by Theorem 4, $w \models \alpha \Rightarrow \mathbf{B} \mathbf{K} \chi$ follows. By Lemma 1, $w \models \mathbf{B} \mathbf{K} \chi \Rightarrow \neg \mathbf{K} \neg \mathbf{K} \chi$. Thus, $w \models \neg \mathbf{K} \neg \mathbf{K} \chi$ (discharging the assumption $w \models \alpha$).

Therefore, $w \models \neg \mathbf{K} \chi \Rightarrow \neg \mathbf{K} \neg \mathbf{K} \chi$. \square

We can see from the above that the pilot's action in the case, when formalized in ASL, logically entails that the pilot lacks negative introspection. Thus, we have good reason to think that a failure of negative introspection with respect to certain data plays a crucial role leading up to the incident, as it is a necessary condition to the action.

We can now identify a key insight resulting from our formal analysis. If we wish to prevent the pilot from engaging in the dangerous action, we must enable the flight deck management system to detect the particular failure and encourage the pilot's negative introspection on the data. If the premises jointly entail a failure of negative introspection, and we somehow grant the pilot negative introspection, then one of the premises must become false, by the logical rule of Modus Tollens. The only candidate premises to falsify are 1) $\neg \mathbf{K} \chi$ and 2) α , as the rest are theorems.

Theorem 6 (Negative Introspection vs Action)

If a rational pilot with missing safety data has negative introspection, then he does not execute a dangerous action.

For proof, we map the argument from proof of Theorem 5 into propositional logic.

- Let $a \equiv \alpha$ (the pilot engages in a dangerous action),
- $\neg(\mathbf{kf}) \equiv \neg \mathbf{K} \chi$ above (the pilot does not know the flight data related to the action),
- $r \equiv$ Lemma 3 above (the pilot is rational),
- $\neg \mathbf{ni} \equiv$ the conclusion above.

| | | | |
|--------------|-----|--|---------------|
| <i>Proof</i> | (1) | $(r \wedge a \wedge \neg(\mathbf{kf})) \Rightarrow \neg \mathbf{ni}$ | Thm 5 |
| | (2) | \mathbf{ni} | Assumed |
| | (3) | $\neg r \vee \neg a \vee \mathbf{kf}$ | from (1), (2) |

| Flight | Assignment |
|----------------|--|
| Aeroperu 603 | $\chi \equiv$ “No instruments confirm that the altitude is dangerously low” $\alpha \equiv$ “The pilot reduces pitch” |
| Air France 447 | $\chi \equiv$ “All instruments indicate dangerous overspeed” $\alpha \equiv$ “The pilot increases pitch” |

Table 5: Unknown flight data and dangerous actions

- (4) $\neg kf$ Assumed
- (5) r Assumed
- (6) Therefore, $\neg a$ (3), (4), (5)
-

The lack of knowledge of χ cannot be fixed in most cases. Typically, the instrumentation is experiencing a mechanical error of some kind, causing the autopilot to disconnect and return control to the pilot. In this case, the instruments are unreliable, and so knowledge is prevented.

This leaves only pilot rationality and the dangerous action. We assume pilot rationality for the formal work, but it is important to keep in mind that our solution must not inhibit the pilot’s rationality, for example by contributing to information overload. Thus, our solution is to encourage negative introspection in such a way as to also encourage pilot rationality. Doing this formally falsifies assumption α , that the pilot engages in dangerous action, giving us good reason to think that the pilot will actually avoid engaging in the dangerous action in the real world, assuming our formalization does a good job modeling the real world.

4 Future Work

Safety in highly automated modern cockpits requires interdisciplinary input from human factors experts, safety engineers, systems engineers, and aerospace engineers, all of whom collaborate to improve safety. We believe logicians can also make important contributions by formally modeling pilot reasoning. Having demonstrated the value of analyzing loss of pilot situational awareness from an epistemic logic perspective, we recommend future work to investigate combining modal reasoning with modern sensor technology to improve cockpit safety.

Our analysis suggests that there is a potential advantage in an approach that embraces teamwork in the pilot-autopilot relationship, in which the autopilot monitors the pilot and actively finds ways to properly assist, rather than an active decider/passive informer relationship.

Second, and importantly, our analysis suggests investigating a shift from an alert model centered on the idea that brighter is better, toward a more focused way of differentially brightening the right things at the right time, and dimming the rest. The flow of information from the flight deck to the pilot is a resource to be managed just like any other, with priority given to information that can immediately stop the pilot from doing something dangerous. The phenomenon of information overload during emergency situations plays a large role in the resulting incidents by diminishing the pilot’s decision-making ability [20] [28]. For whatever psychological reasons, an excess of information seems to decrease an agent’s situational awareness. In our formalization, this amounts to a falsification of *pilot rationality*. So a solution must alert the pilot in a way that does not overload his senses and diminish his rational decision-making. If *pilot rationality* is false, then an encouragement of negative introspection does not necessarily prevent a dangerous action. Modern avionics have many safeguards built in to alert the pilot that they are taking unsafe action. Yet we have seen that they can overwhelm a crew, and especially an individual pilot during an emergency. An alternative approach would seek to encourage *negative introspection* without diminishing *pilot rationality*. We believe this can be accomplished by removing extraneous data from the pilot’s attention, by dimming temporarily irrelevant data, so that he can notice the critical piece of information without being overwhelmed. In future work, we hope to collaborate closely with the human factors community and validate our approach through empirical testing.

5 Related Work

The work presented by this paper lies at the intersection of formal methods and human-computer interaction.

Previous researchers have applied formal mathematical methods to the analysis of mode confusion [26], [10], [27], [8]. Mode confusion is a phenomenon that occurs when a pilot believes that an airplane is under the automated protections of a particular autopilot flight mode

when in fact it is not. Though viewed as a distinct phenomenon, we think cases of mode confusion and negative introspection failure overlap. A pilot might be confused about the aircraft's mode, and as a result of this come to believe false things about the state of the aircraft. For example, if he believes it is in a mode that prevents the airspeed from falling below a certain level, and fails to glance at his airspeed indicator for some time. He would not know his airspeed, and would not know that he did not know it.

Chen, Ely, and Luo [11] analyze "Agent A is unaware that P" as "Agent A does not know that he does not know P", consistent with our analysis of cases in which a pilot is unaware of some piece of information.

Rushby [26] and Combefis [12] bring formal methods to bear on the analysis and discovery of automated surprises, which are closely related to the notion of mode confusion. Where mode confusion refers to a pilot's not knowing some feature of the aircraft's current mode, automated surprises are the frequent result, where some feature of the mode produces behavior that the pilot did not expect.

Oishi et. al. [24] describe a method for identifying the minimal amount of information required by the pilot in order to safely perform a maneuver, and for proving that a given interface provides this sufficient information. This is extremely promising work in the effort to reduce information overload, a shared goal of this paper, and future extensions of our research will surely appeal to their work in showing that the temporary removal of instrument data will not result in a more dangerous circumstance than the one being solved. If our solution is to, for instance, remove unnecessary instrument data in order to show the pilot that the airspeed data is contradictory, and the correct action in response requires knowledge of attitude and thrust, then our mechanism must not remove those data from the pilot's awareness. The work of Oishi et. al. will help us identify the minimally sufficient information for executing a correct control input while also highlighting the failure of negative introspection to the pilot.

Bolton et. al. [6] [7] apply model checking to the relationship between a human operator and a system. They do so by incorporating the operator's behavior into a task analytic model of the system, along with task analytic models of its other components. They then characterize the normative behaviors of the operator as component tasks to be verified. If a model can be found in which a normative behavior fails, then this represents a potential case of human error. This relates to our work in that it formalizes the human component of a system and identifies errors that can occur. However, their approach applies during the specification phase,

while ours identifies a method for relating the pilot's actions to his mental picture of the aircraft, which could be used as part of a real-time safety monitor of the pilot.

For more on the application of modal logic to various aspects of knowledge and agency, see chapters in the Handbook of Philosophical Logic [22], the Handbook of Epistemic Logic [15], any number of recent papers by van Benthem et. al., [29] for example. Future extensions of this work will incorporate a modal analysis of action, extensive work on which has been done by Horty [18] and Broersen [9], among others.

6 Conclusion and Acknowledgements

In this paper, we applied basic tools from epistemic logic to the analysis of a specific class of pilot error. This formal analysis revealed a relationship between dangerous actions, pilot rationality, and a pilot's negative introspection. By exploiting this relationship, we can mitigate the role the class of error plays in aviation accidents. We illustrated the role logic can play in the safety engineering community, by taking formal work done in philosophy and economics, and using it to analyze the human component of complex systems. This improves researchers' ability to automate and rigorously test safety procedures meant to mitigate human error. In future work, we hope to further explore this work by using our logic to develop algorithms that simultaneously encourage negative introspection and pilot rationality.

We would like to acknowledge Kelly Hayhurst and C. Michael Holloway for their insights on safety. We would also like to thank Aaron Dutle for helping us improve the presentation of the mathematical results in the paper. We especially acknowledge Brenton Weathered for his valuable insights in interpreting accident reports and helping us understand pilot behavior.

References

1. Allwein, G., Harrison, W.L.: Partially-ordered modalities. *Advances in Modal Logic* **8**, 1–21 (2010)
2. Aumann, R.J.: Interactive epistemology i: Knowledge. *International Journal of Game Theory* **28**, 263–300 (1999)
3. Aumann, R.J., Brandenburer, A.: Epistemic conditions for nash equilibrium. *Econometrica* **63**, 1161–1180 (1995)
4. BEA: Final report on the accident on 1st june 2009 to the airbus a330-203 registered f-gzcp operated by air france flight af 447 rio de janeiro - paris. Tech. rep. (2012)
5. Blackburn, P., de Rijke, M., Venema, Y.: *Modal Logic*. Cambridge University Press (2001)
6. Bolton, M.L., Bass, E.J., Siminiceanu, R.I.: Using formal verification to evaluate human-automation interaction: A

- review. *Systems, Man, and Cybernetics: Systems*, IEEE Transactions on **43**(3), 488–503 (2013)
7. Bolton, M.L., Siminiceanu, R.I., Bass, E.J.: A systematic approach to model checking human–automation interaction using task analytic models. *Systems, Man and Cybernetics, Part A: Systems and Humans*, IEEE Transactions on **41**(5), 961–976 (2011)
8. Brederke, J., Lankenau, A.: A rigorous view of mode confusion. *Proceedings of SafeComp* **1** (2002)
9. Broersen, J.: Deontic epistemic stit-logic distinguishing modes of mens rea. *Journal of Applied Logic* **2**(9), 127–252 (2011)
10. Butler, R.W., Miller, S.P., Potts, J.N., Carreno, V.A.: A formal methods approach to the analysis of mode confusion. *17th Digital Avionics Systems Conference Proceedings* **1** (1998)
11. Chen, Y.C., Ely, J.C., Luo, X.: Note on unawareness: Negative introspection versus au introspection (ku introspection). *International Journal of Game Theory* **41**, 325–329 (2012)
12. Combefis, S.: A Formal Framework for the Analysis of Human-Machine Interactions. Ph.D. thesis, Universite catholique de Louvain (2013)
13. DGAC: Reporte final accidente aereo birgenair, vuelo alw-301, febrero 06, 1996. Tech. rep. (1996)
14. Director General of Air Transport: Accident of the boeing 757-200 aircraft operated by empresa de transporte aereo del peru s.a. aeroperu. Tech. rep., Ministry of Transport, Communications, Housing and Construction (1996)
15. van Ditmarsch, H., Halpern, J.Y., van der Hoek, W., Kooi, B. (eds.): *Handbook of Epistemic Logic*. College Publications (2015)
16. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: *Reasoning about knowledge*. The MIT Press, Cambridge, MA (2003)
17. Hintikka, J.: *Knowledge and belief: an introduction to the logic of the two notions*. Cornell University Press, Ithaca, NY (1962)
18. Horty, J.F.: “Agency and Deontic Logic”. Oxford University Press (2001)
19. Hughes, G., Cresswell, M.: *A New Introduction to Modal Logic*. Routledge (1996)
20. Hwang, M.I., Lin, J.W.: Information dimension, information overload and decision quality. *Journal of Information Science* **25**, 213–218 (1999)
21. Langewiesche, W.: *Inside the Sky*. Pantheon Books, New York
22. Meyer, J.J.C.: *Handbook of Philosophical Logic*, chap. Modal Epistemic and Doxastic Logic, pp. 1–38. Springer Netherlands, Dordrecht (2003)
23. Network, A.S.: Asn aircraft accident boeing 747-237b vt-ebd arabian sea, off bandra (2014). URL <http://www.aviation-safety.net>
24. Oishi, M., Mitchell, I., Bayen, A., Tomlin, C.: Hybrid verification of an interface for an automatic landing. *Proceedings of the IEEE Conference on Decision and Control* **1** (2002)
25. Palmer, B.: *Understanding Air France 447*. William Palmer (2013)
26. Rushby, J.: Using model checking to help discover mode confusions and other automation surprises. *Reliability Engineering and System Safety* **75**, 167–177 (2002)
27. Rushby, J., Crow, J., Palmer, E.: An automated method to detect mode confusions. *18th Digital Avionics Systems Conference Proceedings* **1** (1999)
28. Simpson, C.W., Prusak, L.: Troubles with information overload - moving from quantity to quality in information provision. *International Journal of Information Management* **15**, 413–425 (1995)
29. Van Benthem, J.: *Modal Logic for Open Minds*. CSLI lecture notes. Center for the Study of Language and Information (2010)