How the cockpit manages anomalies: revisiting the dynamic fault management model for aviation

Guido C. Carim Jr¹, Tarcisio A. Saurin ², Sidney W.A. Dekker¹

¹Griffith University, 170 Kessels Rd, Nathan QLD 4111

²Federal University of Rio Grande do Sul, Av. Paulo Gama, 110 - Farroupilha, Porto Alegre -
RS, 90040-060, Brazil

Corresponding author:

Guido Carim Júnior,

E-mail: g.carimjunior@griffith.edu.au,

Tel: +61 7 37355573

ORCID: 0000-0001-5258-3912

Abstract

More than 20 years ago, Woods proposed a model that accounts for the inherent complexity faced by operators when managing abnormal and emergency situations in highly complex sociotechnical systems. The model was reviewed a decade later and only a few studies have applied it to aviation. This paper proposes adjustments to the original model, based on recent theoretical developments and empirical evidence on the anomaly management activity in aviation. The model was divided into five components; three of which – activity, types of reasoning involved, and resources – were revisited and further developed. The two other components – fault behaviour and unit of analysis – were not updated and only discussed in the aviation context. As a result, the revisited model descriptively clarifies how the activity of anomaly management emerges from the use of a wide repertoire of strategies, involving a spectrum of types of reasoning and a set of resources for action, which are not limited to those anticipated by designers, such as checklists and the warning system. An instantiation of the revisited model highlights the implications of false alarms, which trigger a cascade of disturbances that, in turn, requires adaptive strategies based on heuristics and analogies and supported by pilot's experience. The revisited model can support a more accurate analysis of anomalous situations and the redesign of work systems to achieve a better performance.

Keywords: resources for action, dynamic fault management, Quick Reference Handbook, checklist, procedures, aviation.

1. Introduction

The dynamic fault management model proposed by Woods (1994) and Woods and Hollnagel (2006) supports the description of the inherent complexity that operators face when dealing with abnormal and emergency situations in complex sociotechnical systems, such as cockpits, space missions, nuclear plants, and anaesthetic management under surgery (Watts et al. 1996; Watts-Perotti and Woods 2007). The model, also known as the anomaly management, explains how operators make sense of the situation, diagnose and act under ambiguity and uncertainty while managing the ongoing process (Johannesen and Woods 1991).

According to the model, a fault can be perceived only through its consequences, or disturbances, because faults and symptoms rarely have clear cause-and-effect links. Indeed, disturbances impose additional cognitive demands on operators, who need to cope with them while maintaining the monitored process integrity (Christoffersen and Woods 2006).

Therefore, operators manage the situation based on three iterative and concurrent event-driven cognitive processes influenced by abductive reasoning: anomaly recognition and assessment, diagnosis, and responses or courses of action (Woods 1994; Watts et al. 1996).

Based on these premises, the model criticizes modern alarm systems for their failure both to precisely diagnose the problem and to distinguish the important signals against a noisy background (Woods 1995). Also, the model proposes that there are some patterns that might hinder a proper situation management, such as the failure to re-assess the fault or biases that may affect attention control (De Keyser and Woods 1990; Woods and Sarter 2010).

Only a few studies, such as Singer and Dekker (2000) and Carim Jr. et al. (2016), have applied the original model to practical situations in aviation. Despite their contributions, none of them has discussed its theoretical suitability to aviation, even though Woods (1994) argued that the model is generic and is partially based on studies of commercial aircraft (e.g.,

Abbott 1991). Moreover, a review of the model by Woods and Hollnagel (2006) did not add new evidence or concepts, thus highlighting the need for an update.

This paper aims to revisit the dynamic fault management model for application in the aviation domain based on recent developments in the literature and on the previous study conducted by Carim Jr. et al. (2016). The model was revisited and adapted to aviation to answer two research questions (RQs): RQ1: What are the implications of recent theoretical developments for the dynamic fault management model? RQ2: How does the cockpit manage anomalies and emergencies?

The revisited model contributes to the cognitive systems engineering (CSE) literature, more specifically to a series of studies started by Hutchins (1995) and Hutchins and Klausen (1996) and followed by Henriqson et al. (2011), and Roth et al. (2014) under titles that begin ‘How a cockpit...’. These works have advanced cognitive studies in real-world situations by taking the cockpit as the unit of analysis and assuming that cognitive functions are distributed among material and social worlds.

We propose three adjustments to the original model. The first adjustment combines the three aforementioned cognitive processes proposed by Woods (1994) and describes how these can be operationalized through strategies. Based on Rasmussen and Jensen (1974), the cockpit is viewed as possessing a repertoire of strategies to address the variability of contextual factors based on the operator’s expertise and other resources. The second adjustment proposes that strategies are driven not only by abductive reasoning but also by a spectrum of reasoning types, ranging from heuristic and analogy (Klein 1993, 2015b; Kahneman and Frederick 2005) to abductive (Woods 1994) and analytical (Rasmussen 1993b). Lastly, the third adjustment recognizes that, when coping with anomalies, operators deploy more than just the checklists and do not rely exclusively on the warning system. This

adjustment is based on the ‘resources for action’ concept from Suchman (1985), further developed by Wright et al. (1996, 1998, 2000).

To highlight the changes made to the model and its applicability to aviation, a case originally reported by Carim Jr et al. (2016) was analysed. The findings from the case analysis provide insights into how the cockpit manages false alarms and which design changes could improve its performance.

The paper is organized into six sections. Following the introduction, section 2 presents the research design and its rationale. Section 3 decomposes the original model into five components and describes each one. Section 4 introduces the three adjustments made to the original model. Section 5 adapts the original model for aviation use and describes an instantiation. In section 6, the conclusion, limitations and suggestions for future studies are presented.

2. Research design

This study consisted of three steps. The first step aimed to delineate the model by organizing its components. This was necessary because the model was originally presented in two book chapters as a narrative with no explicit boundaries among the constructs (Woods 1994; Woods and Hollnagel 2006). The second step brought together theories from different areas and empirical evidence to improve the original model. Finally, an analysis was carried out of what the model looks like in aviation, based on a case study.

In Step 1, we decomposed the model according to five constructs: fault behaviour (construct 1), unit of analysis (construct 2); activity (construct 3), type of reasoning (construct 4), and resources (construct 5). Although the original model had a sixth construct (patterns of failure during the activity), it was excluded from the revisited model since the objective was

to develop a descriptive model rather than a normative reference (Vicente 1999) of what should count as failure or success.

Two main studies were the core references to complete the first step: Woods (1994), who first introduced the model, and Woods and Hollnagel (2006), who reviewed and reorganized it. We also reviewed papers that explicitly addressed ‘anomaly management’, ‘dynamic fault management’ or one of the model’s components in the title, abstract or content, and made contributions to the original model independent of their field or domain of research (Table 1). These studies further clarified the constructs and their interactions, which resulted in a model with clearer boundaries and relationships among them (Wartofsky 1979).

Table 1 The references used to describe the original model organised chronologically

Study		Contribution
1	Woods (1984)	Early results on experiments performed with nuclear plant operators on how they recognise, assess and use procedures to correct operational problems.
2	Keyser et al. (1990)	Describes the attentional control mechanism.
3	Woods et al. (1991)	Literature review on theoretical and empirical studies on human-AI system cooperation during fault management activity.
4	Johannesen and Woods (1991)	Discusses problems in the interaction and interface design of several intelligent fault management systems in a space mission control room that make it difficult for the operator to cope.
5	Potter (1994)	Proposes temporal and functional displays to support anomaly management during the cascade of disturbances.
6	Woods (1994)	First proposal of the model, describing the main constructs and calling it as dynamic fault management.
7	Woods (1995)	Reflects on the problems with warning system functions and the control of attention.
8	Watts et al. (1996)	Discusses how the dynamic fault management activity is distributed among functionally distinct teams and how they cope very successfully with the demands imposed during this activity.
9	Woods and Patterson (2000)	Describes the technology-induced complexity and how it produces an escalation of cognitive and coordinative demands on operators.
10	Singer and Dekker (2000)	Analyses pilots performance when dealing with anomalies according to four different warning systems.

11	Christoffersen and Woods (2003)	Discusses how people perceive meaningful events in a monitored process and how different methods of displaying the information may help or hinder those perceptions.
12	Christoffersen and Woods (2006)	Describes how operators make sense of events based on stream of raw data by allocating attention.
13	Woods and Hollnagel (2006)	Revises the original model, describes the constructs more clearly and renames the model to anomaly management.
14	Watts-Perotti and Woods (2007)	Analyses how coordinated activities across multiple agents contribute to the anomaly management at the team level.
15	Christoffersen et al. (2007)	Identifies different techniques applied by operators in space missions to identify meaningful events in a stream of dynamic data.
16	Woods and Sarter (2010)	Synthesises the control of attention and the use of new perspectives to guide the design of new technologies.

The second step consisted in reviewing the constructs based on recent advances in the literature and on empirical data. The studies were derived from a broad range of research areas, from cognitive system engineering, distributed cognition and diagnostic reasoning to naturalistic decision making, reasoning and thinking, and situated action. Empirical findings from the study conducted by Carim Jr. et al. (2016) also supported the theoretical changes. As a result, this step improved the model representation, feasibility and practicability (Stefanov 2012) by addressing issues not covered in the original proposal.

The study conducted by Carim Jr et al (2016) investigated, through cognitive ethnography (Hollan et al. 2000) and phenomenology (Cerbone 2012), how airline pilots for a specific aircraft model used fragments of different checklists contained in the Quick Reference Handbook (QRH) and additional resources for action to solve anomalies for which the checklist did not offer a complete solution. In the former, data were collected from the first author's experiences as an airline pilot, during which he experienced five situations on five hundred and sixty-eight flights. In the latter, the critical decision method (CDM; Hoffman et al. 1998; Klein et al. 1989) and semi-structured interviews were used with twelve pilots, who shared fifteen stories involving in-flight technical faults that could not be solved by actioning the QRH. These interviews focused on the pilots' perception of the usability of

1 the warning system, QRH organization, checklist layout and typography. Secondary data
2 from the company's safety report database were used to support the findings from the shared
3 stories.
4
5

6
7 The study confirmed that most of the situations faced by pilots are simple problems
8 that are clearly addressed by the warning system and easily solved using the checklists
9 contained in the QRH. However, occasions such as false alarms, multiple messages and faults
10 that occur repeatedly in a sequence of flights are not fully comprehensible or anticipated by
11 procedures. These ill-structured problems are far more complicated than procedures can
12 anticipate and force pilots to improvise strategies to address them. In turn, these strategies are
13 supported by different resources for action, ranging from fragments of the QRH checklists
14 and documents designed for other purposes to previous experience, rules of thumb and stories
15 informally shared by pilots.
16
17
18
19
20
21
22
23
24
25
26
27

28
29 The third step expands and conducts an in-depth analysis of a case study that was
30 originally (and briefly) presented by Carim Jr. et al. (2016). The objective was to highlight
31 the differences between the original model and an instantiation, aiming to improve its
32 representational and inferential features in the aviation domain (Stefanov 2012). In particular,
33 the analysis enabled the representation of what a cascade of disturbances looks like inside a
34 cockpit, how the cockpit should be delimited as the unit of analysis and how the cockpit uses
35 adaptative strategies driven by different types of reasoning and supported by resources for
36 action to cope with a problem outside of the scope of procedures.
37
38
39
40
41
42
43
44
45
46
47
48
49
50

51 **3. Dynamic fault management: the original model**

52 **3.1. Construct 1: Cascade of disturbances (fault behaviour)**

53
54
55 Some faults in monitored processes should be regarded as malfunctions or anomalous
56 behaviour of important components and systems that may evolve over time (Woods 1995;
57
58
59
60
61
62
63
64
65

Christoffersen and Woods 2006). These faults disturb the system in a non-linear way, affecting other processes, parts, sensors and indications. Under these circumstances, symptoms, which are generally represented by indicators, cannot be traced back to a single fault, making it difficult to precisely diagnose the root cause(s) (Christoffersen et al. 2007).

Disturbance is a concept used throughout the original model to refer to changes in the process that are not directly linked to symptoms or causes. Woods (1994, p. 71) defined it as ‘abnormal conditions or malfunctions where the actual process state deviates from the desired function for a relevant operating context’.

Because the functions in a monitored process are interconnected, most faults, even single ones, promote a time-dependent cascade of disturbances while the fault develops or even after it has ceased to do so (Potter 1994). The situation becomes more complicated when automatic systems and operational personnel intervene to counter the disturbances and to maintain core goals, such as safety, integrity, or fault correction. Ultimately, the cascade of disturbances might be a mix of influences produced by both the fault itself and the intervention(s), thus masking the symptomatic indications (Woods and Hollnagel 2006).

The situation might be worsened either by the advent of multiple faults or when a single fault affects different parts of the system or other systems, such as electrical controllers and sensors (Potter 1994). In the first scenario, the operator may not have a clear cue about whether the faults are interrelated or independent, since the disturbances and symptoms are mixed. In the second scenario, the disturbance may escalate rapidly, triggering so many lights and messages that the alarm system might resemble a ‘Christmas tree’ (Woods 1995).

3.2. Construct 2: Joint cognitive system (unit of analysis)

Since the beginning, the dynamic fault management model has recognized the unit of analysis is neither the operator nor the technology but the joint cognitive system (JCS) that

emerges from the interaction between them (Hollnagel and Woods 2005). Woods (1994) argued that managing dynamic faults is about cognitive systems since the emergent properties of the activity cannot be reduced to its elements.

According to Hollan et al. (2000), instead of merely processing information, a JCS manipulates the symbols and uses knowledge about itself and the social and material world as a guide for achieving its objective. The environment also plays an important role in the JCS performance and is defined as everything outside the direct control of the system's agents, but influences the cognitive system behaviour (Hollnagel and Woods 2005).

From the dynamic fault management standpoint, studies from Watts et al. (1996), Patterson et al. (1998), Patterson and Woods (2001) and Watts-Perotti and Woods (2007) have defined the mission control centre as the JCS and, thus, as the unit of analysis during space shuttle missions. The boundaries were drawn around multilevel set of teams, real-time telemetry data downlinked from the shuttle subsystems and procedures for certain distinctive situations. The reason is these elements contain and coordinate information, knowledge, strategies and priorities needed to manage technical problems that arise in the launch, orbit and re-entry phases.

3.3. Construct 3: three interwoven cognitive processes (activity)

Based on Neisser's perceptual cycle, Woods (1994) proposed that operators perform three cognitive processes that mutually influence each other and might occur simultaneously to address more complicated faults. The processes are as follows: (a) anomaly recognition and assessment, (b) diagnosis of the cause, and (c) planning and executing a course of action (Fig. 1).

These three processes describe how operators make initial assessments, create expectations, provide explanations, act based on partial and uncertain data, and constantly

1 revise their hypothesis as new evidence and symptoms emerge. Rather than distinct
2 sequential steps, they are interwoven, with one process occurring concurrently with others
3 depending on the goal, the local constraints and the demands posed by the context
4
5 (Christoffersen and Woods 2006; Woods and Hollnagel 2006).
6
7
8
9

10 11 12 **3.3.1. Construct 3: recognizing and assessing anomalies** 13

14 According to Woods (1995), operational settings are a mixture of relevant elements
15 and noise. Many different objects, events and activities are embedded in the monitored
16 process, leading operators to constantly shift their attention across elements, ongoing
17 activities, plans and goals (Woods and Sarter 2010). Unlike traditional models of diagnosis,
18 the dynamic fault management frames fault identification as the identification of events
19 through the attention control process, violations of expectations, and re-assessment (Woods
20 1995; Christoffersen and Woods 2006).
21
22
23
24
25
26
27
28
29
30

31 Experts are highly sensitive to meaningful events because they are constantly making
32 sense of raw data, system status and the physical environment (Christoffersen and Woods
33 2003; Woods and Sarter 2010). Instead of merely reading the data spread over different
34 gauges and displays, operators gather them together to build events, which are meaningful
35 changes in the process parameters. What counts as an event depends on data behaviour in a
36 temporal interval, on data availability, operators' knowledge and expectations, and on the
37 past and the future (Christoffersen et al. 2007). All these factors might be interpreted
38 differently by different operators in different operational contexts. An event that is desirable
39 in one context may be perceived as undesirable in another (Christoffersen and Woods 2006).
40
41
42
43
44
45
46
47
48
49
50

51 The control of attention helps operators to constantly shift attention to explore and
52 track the world for relevant changes, or even the lack of them, based on goals, plans and
53 activities (Christoffersen et al. 2007). The perceived anomaly is thus the result of a mismatch
54
55
56
57
58
59
60
61
62
63
64
65

1 between what is observed and what is expected, which is known as the violation of
2 expectation (Christoffersen and Woods 2003). Both the control of attention and the violation
3 of expectation are mechanisms that avoid data overload (Woods and Sarter 2010).
4
5

6
7 Another feature that differentiates the anomaly management from traditional
8 diagnostic models is the role played by re-assessments. The initial explanation of the fault
9 can be either correct or plausible given the evidence available at that point. As the situation
10 unfolds and new disturbances and evidence emerge, operators re-assess the situation, develop
11 another explanation for the problem and re-plan their actions many times as necessary
12 (Woods 1994).
13
14
15
16
17
18
19
20
21
22
23

24 3.3.2. Construct 3: *planning and implementing a course of action*

25
26 Woods (1994) argued that operators deploy three typical courses of action when
27 managing dynamic faults. Therapeutic interventions aim either to mitigate, cope with
28 symptoms and disturbances or to break the disturbance propagation path. Under typical
29 circumstances of critical faults and time pressure, the objective is to counteract the
30 consequences instead of seeking explanations for what caused the disturbances.
31
32
33
34
35
36
37

38
39 The second course of action, regarded as diagnostic responses, attempts to generate
40 more information about the nature and the source of the fault. The aim is to verify or confirm
41 the initial hypothesis commonly performed through tests of the faulty component (Singer and
42 Dekker 2000). Sometimes, the therapeutic intervention ends up producing more evidence
43 about the source of the fault and, thus, acting as a diagnostic response (Watts et al. 1996).
44
45
46
47
48
49
50

51 One common pathway of this course of action is to verify the control influence currently
52 acting or acted before the disturbance occurred, regardless whether was human or automatic
53 system intervention (Woods and Hollnagel 2006).
54
55
56
57
58
59
60
61
62
63
64
65

1 Finally, actions intended to terminate the source of the fault require an operator's
2 deep knowledge of the causes and the nature of the fault and solving the fault itself and
3 include such fault messages or components or systems that are automatically disabled by the
4 monitored process (Woods, 1994). This approach includes both cleaning up the after-effects
5 of the failure, when symptoms persist even after the source of the fault has been terminated
6 (Christoffersen and Woods 2003).
7
8
9
10
11
12
13
14
15
16

17 3.3.3. Construct 3: *diagnosis*

18
19 Woods and Hollnagel (2006) defined diagnosis as the ability of the cognitive system
20 to generate plausible hypotheses that might account for and explain most of the evidence. In
21 addition to and at the same time as generating hypotheses, this process begins a knowledge-
22 driven search to evaluate the adequacy of those possible explanations. Rather than being
23 immutable, a hypothesis shifts according to the context, new evidence, and post-action
24 monitored process behaviour. The definition also emphasizes the active role of the diagnostic
25 process, driving the search for additional evidence to assess and re-assess the nature of the
26 failure.
27
28
29
30
31
32
33
34
35
36
37

38
39 Multiple faults, multiple messages and multiple disturbances are likely to occur in
40 highly tight-couple monitored processes. These situations may complicate the hypothesis
41 generation and the revision of assessments because they can produce numerous varieties of
42 disturbances (Woods 1994). Eventually, the assessment may suggest a single fault even when
43 the disturbance arises out of multiple faults. The opposite is also true: multiple disturbances
44 may represent the consequences of a single fault.
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

3.4 Construct 4: *abductive reasoning (type of reasoning)*

Originally, Woods (1994) proposed abduction as the prevalent reasoning in anomaly management. Reasoning, in this sense, is defined as the nature of the systematic manipulation of mental representations to achieve a desired goal (Holyoak and Morrison 2005). This characterization was particularly important for operators who must draw inferences from a representation under uncertainty and unexpected process behaviours.

Abduction is an attempt to explain facts for which we already have a hypothesis and then to test that hypothesis against a set of available evidence (Burks 1946; Råholm 2010). This type of thinking differs from deductive and inductive reasoning because it implies the search for a more suitable explanation that covers most of the relevant evidence at hand, and not all of them. Furthermore, it is the only mode of inference able to introduce a new idea (Upshur 1997; Peirce and Turrisi 1997).

Instead of static and linear thinking, abductive reasoning involves a dynamic and constant re-evaluation as the situation unfolds and new evidence emerges. The search for a reasonable explanation is a continuum along the activity (Woods 1994). Multiple hypotheses are proposed and discarded as long as the context presents new evidence, the disturbance evolves, and the operator interacts with the faulty process (Woods and Hollnagel 2006).

3.5. Construct 5: *functions of a warning system (resources)*

Woods (1995) noted that alarm and warning systems should be viewed as representative aiding devices that attempt to support the human attention control and the violation of expectations in two ways. First, it discriminates abnormal conditions among important features, supporting the attention control. Second, it draws attention to an imminent danger, aiding the violation of expectation. However, according to Woods (ibid.), most systems rarely accomplish these functions and fail to effectively re-direct attention to meaningful problems.

To overcome these problems and enhance the human ability to cope with anomalies, Woods (1994) suggested that warning systems should incorporate three functions. First, the representation function might help the operator distinguish anomalous behaviour from irrelevant cues by highlighting the temporally unfolding pattern of disturbance and separately representing the multiple factors that influence the disturbances over time (human intervention, automatic system response, another fault or faults). In this regard, Potter (1994) proposes displaying clear information about single and multiple faults and providing future system status, trends and meaningful information instead of raw data. Potter (ibid.) also suggests incorporating indications of whether the system goals have been met.

The second function, hypothesis generation, can support a better diagnosis by generating as many alternative hypotheses as possible given the evidence. It may also highlight the set of evidence covered by each candidate hypothesis (Potter 1994; Watts-Perotti and Woods 2007). The third function, the support actions, should aid the operator in the trade-off between acting under great uncertainty or waiting for more evidence even in the face of undesirable consequences (Woods et al. 1994; Singer and Dekker 2000).

4. Proposed adjustments to the original model

4.1. construct 3: repertoire of strategies (activity)

Woods (1994) and Woods and Hollnagel (2006) did not make clear how the three cognitive processes — anomaly recognition, diagnosis and course of action — relate to practices used by operators in real-world situations except for their responses. To address this gap, in line with Rasmussen (1993a) and Rasmussen and Jensen (1974), we argue that strategies are proxies of cognitive processes.

By strategy, we mean the possible patterns into which the JCS organizes the three cognitive processes according to the type of reasoning involved, the resources available and

1 the goal. These strategies are created, learned, stored and retrieved according to the
2 familiarity with the situation, the viability of the strategy and the availability of resources to
3 implement the strategy. As long as the JCS is exposed to many different situations, it
4 embodies numerous strategies to cope with the contextual factors (Rasmussen 1993a), thus
5 increasing its ability to cope with a wide variety of circumstances. For this reason, we
6
7 propose to use the concept 'repertoire of strategies' to address all possible strategies that a
8
9 JCS may deploy based on the situation. Fig. 2 presents a graphical representation of this
10
11 concept.
12
13
14
15
16
17
18

19 These strategies can shift many times during the activity because (Rasmussen 1993b;
20 Rasmussen and Jensen 1974) the cues indicate so; each strategy requires different time, tools,
21 procedures, information and previous knowledge; the goal changes as the situation unfolds;
22 and operators need to circumvent local difficulties. The basic rule is that a JCS begins with
23 simple and effortless strategies and evolves to more intricate and effortful ones as long as the
24 response does not produce desirable effects (Rasmussen 1993a). If the situation is completely
25 new and the strategies that have been tried cannot solve the problem, the JCS might create a
26 new strategy that, depending on the outcome, will be stored in the repertoire of strategies for
27 future use. Hence, the more a JCS is exposed to abnormal and emergency situations, the
28 richer its repertoire of strategies is, and the more expert the practitioner becomes (Dreyfus
29 and Dreyfus 1986, 2005).
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45

46 Carim Jr. et al. (2016) described the cognitive processes through strategies employed
47 by the cockpit to cope with anomalies. In one of the examples reported, an aural alarm and
48 warning system fault message indicated that the passenger front door had opened during the
49 flight and triggered a set of actions by the crew. Since the alarm indicated a critical situation
50 (assessment), the pilot in command immediately turned the seat-belt signs on and checked the
51 cabin pressurization status (therapeutic response) before diagnosing or retrieving any
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 checklist. These actions, recorded recorded as the strategy of acting before retrieving a
2 checklist, indicated that the assessment related the alarm to a possible pressurization problem,
3
4 and the response aimed to bring everyone, including the flight attendants, to their seats in
5
6 case the situation evolved into depressurization and they needed oxygen masks.
7
8

9
10 Later, after checklist completion, which implied performing some tests (diagnostic
11 responses), the evidence suggested that a false alarm had occurred (assessment), and the
12 pilots diagnosed the cause as a fault in the door lock sensor (diagnosis); all of these actions
13
14 can be framed as a second strategy. Even after this, the pilots deployed a third strategy: an
15
16 early descent for landing at the destination airport (therapeutic response) to reduce the
17
18 likelihood of a depressurization, even though an early descent consumes more fuel. In
19
20 addition, they continued to monitor the system status and followed up by checking the
21
22 situation more thoroughly after they were on the ground.
23
24
25
26
27
28
29
30

31 *4.2. Construct 4: spectrum of reasoning (types of reasoning)*

32
33

34 Whereas abductive reasoning prevailed in the original model, we propose to include a
35
36 spectrum of reasoning types, ranging from the effortless, rapid cognitive process to slower,
37
38 more in-depth thinking. Thus, in addition to abduction, heuristic, analogy and analytical
39
40 reasoning may be prevalent in some strategies.
41
42

43
44 Carim Jr. et al. (2016) found evidence that the JCS also employs strategies requiring
45
46 more analytical thinking whenever the situation is unfamiliar, does not impose imminent risk
47
48 or time pressure, the fault is complicated but expected, and the performed action fails to solve
49
50 the problem. This is consistent with the predictions from Rasmussen (1993a).
51
52

53
54 In general, analytical reasoning requires the use of formal textbooks and decision-tree
55
56 methods (Rasmussen 1993b), such as the QRH and the checklist, and it is especially useful
57
58 for multiple fault conditions (Carim Jr. et al. 2016). In such situations, the first thing pilots
59
60
61
62
63
64
65

1 tend to do is to relate the disturbances to a common cause and to use checklists and other
2 manuals to perform tests over the faulty system. If the test fails to point out a single root
3 cause, then pilots tend to link each disturbance to a specific root cause and assume that
4 multiple unrelated faults occurred simultaneously. Both hypotheses are based on analytical
5 thinking, in which the problem is decomposed into small units of analysis and tests are
6 performed (Rasmussen and Jensen 1974).
7

8
9 Furthermore, Carim Jr. et al. (2016) found that pilots deferred to their expertise under
10 uncertainty, especially for problems laying out of the QRH, checklist and training scopes.
11 Pilots acted rapidly and with very little conscious efforts by either using simple and generic
12 rules or making comparisons to prototypical situations. Carim Jr et al. (ibid.) reported that
13 some pilots incorporated the simple rule of turning the seat-belt signs on whenever the
14 perceived problem could impact cabin pressurization, even though the sign is formally used
15 to advise the cabin crew of turbulence and an imminent take-off or landing. According to the
16 study, one of the interviewees learned this strategy from his flight instructor during his initial
17 training with the airline and has been using it even since.
18

19 In another example, the study (Carim Jr et al. 2016) describes some strategies based
20 on comparisons to past experiences and shared stories. While on the final approach to landing
21 at an airport with a short runway surrounded by complex geography, a crew faced two fault
22 messages when the landing gear was lowered. The messages initially indicated that the
23 brakes on both sides could have failed, but seconds later, the messages disappeared. Although
24 the crew was not sure whether the problem was real or a false alarm, they decided to divert
25 because the pilot in command remembered a story shared by a colleague who had been
26 through the same situation and decided to land. His colleague had noticed that the brakes
27 were not working properly only during the landing roll, which was not a problem because
28 they had just landed on a very long runway. Although the airplane was diverted, the crew did
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 not notice any anomaly with the brakes during the landing, suggesting that the fault messages
2 were false.
3

4 Many studies from different fields have incorporated elements of heuristic, bias,
5 intuition and analogy to explain how practitioners use their expertise and experience to
6 quickly resolve situations in the field settings despite high uncertainty (Klein et al. 1986,
7 1989; Rasmussen et al. 1990; Rasmussen 1993b; Klein 1993; Patel et al. 1994; Rajkomar and
8 Dhaliwal 2011). Dual-process theories are now widely accepted and distinguish quick,
9 effortless cognitive processes from slower, rule-oriented ones (Kahneman and Frederick
10 2005). They explain that people make intuitive judgment about problems in familiar but
11 critical contexts. Sometimes they seem to know how to act even before any kind of diagnosis
12 takes place (Kahneman and Klein 2009). At other times, they make plausible inferences
13 about the current situation based on elements linked to a representation of the situation
14 (Holyoak 2005). It is the ability to make rapid judgments through heuristics and analogies that
15 differentiate experts from novices, in which the former have a richer repertoire developed
16 along years of deliberate practice (Dreyfus and Dreyfus 2005).
17

18 More specifically, the recognition-primed model (Klein et al. 1988, 2010) recognises
19 how people defer to their expertise and heuristic to make good decisions in applied settings
20 (Klein 2015a, b). This fast thinking process occurs through three common paths (Klein 2009).
21 The first path is the ability to assess if the situation is functionally similar to a prototype, a
22 typical or representative case and generate a reasonable single course of action from a
23 repertoire of patterns. The second path is the ability to create coherent stories from a set of
24 evidence, tailored using heuristics, to diagnose system malfunctions and equipment
25 anomalous behaviours. The third path recognises that operators use mental simulation to
26 predict the process and consequences to carry out one course of action at a time. If the
27

simulation identifies any problem with one option, they may adjust the course of action or switch to another plausible one.

As argued by Rasmussen (1993a), troubleshooting involves a repertoire of strategies directed by different types of reasoning, depending on the operator's familiarity with the situation, previous experience and time spent on the activity. The more time the operator takes to resolve the fault, the less familiarity and less experience with the situation, the more abductive, analytical and time consuming the strategy is (Rasmussen and Jensen 1974; Rasmussen 1993a). However, the operator tends to use strategies based on heuristic and analogy under familiar and non-time-constrained contexts.

4.3. Construct 5: a variety of resources for action (resources)

Originally, the dynamic fault management model discussed only how warning systems should support operators assessing the problem, diagnosing the cause, and planning and implementing a course of action. However, Carim Jr. et al. (2016) found that pilots employ a broader set of resources to cope with problems than just the warning system, checklists or QRH.

According to Fields et al. (1997), resources for action (RfAs) are characterized as abstract information structures activated by the situation feature that constrain or determine the course of action. When applied to abnormal and emergency situations, for example, different fragments of procedures and checklists support the course of action in interwoven ways (Wright et al. 1998) so that operators can either cope with or avoid unanticipated demands (Suchman 1985).

The empirical evidence from Carim Jr. et al. (2016) suggests that more than RfAs, procedures and checklists are useful for the entire activity because they constrain and guide not only the action but also the cognitive processes involved in assessing and diagnosing the

1 fault. Reading a fragment of the checklist to understand its objective and assumptions (De
2 Brito, 2002), for example, is a way to gather more information about the fault, especially
3 when it is unclear, unfamiliar, or unexpected. Another example is to use procedures to aid the
4 diagnosis. When a pilot uses a fragment of a checklist merely to perform a system reset, even
5 knowing that the system will not be restored, s/he intends to understand the precise
6 circumstances in which the system failed instead of trying to recover it.
7
8
9
10
11
12
13

14 The concept of resources encompasses the QRH, procedures and checklists, and any
15 source of information required to accomplish the activity goal and support a strategy
16 (McCarthy et al. 1998; Wright et al. 1998, 2000; Wright and McCarthy 2003). Considering
17 that cockpits have extensive social and technical resources, Carim Jr. et al. (2016) highlighted
18 how pilots employ different resources available to them at the time to provide complementary
19 information and courses of action that are not contained in the QRH. The more ill-structured
20 the fault is, the more resources are employed.
21
22
23
24
25
26
27
28
29
30

31 The resources shown in Table 2 can be merged into four types: (1) documents, (2)
32 representation technologies, (3) previous experience, and (4) social. Each of these categories
33 plays an important role in the activity according to the locally presented contextual factor.
34 For example, a set of faults regularly identified by the warning system is likely to be a false
35 alarm. Knowing this, pilots generally skim the Technical Logbook (TLB; document) for any
36 reports of faults that occurred in the past few days as soon as they arrive at the cockpit. They
37 look for situations that occurred more than once, were resolved by resetting the system or by
38 postponing maintenance actions. The aim is for the pilots to prepare themselves for future
39 problems and avoid surprises. The crew also knows that most of the checklists (document)
40 contain groups of actions intended to reset the system or a component of it, which means
41 deactivating and then re-activating it after a while. These actions normally avoid shutting
42 down the system or deactivating its components until the flight finishes.
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

Table 2 Description of the main categories of resources adapted from Carim Jr et al. (2016)

Resources for action (RfAs)	Relevance
1. QRH and the checklist(s)	Helps pilots to elucidate and solve well-structured problems, such as single fault messages and a group of fault messages with an indication of the root cause.
2. Fragment of the checklist 2.1. Description of the failure	Provides more information about the conditions for the fault occurrence.
2. Fragment of the checklist 2.2. Action or questions to verify the extent of the fault or to reset the system	Helps pilots to gather more information about the system and eventually re-establish the faulty system.
2. Fragment of the checklist 2.3. Landing configuration and performance calculation	Useful for faults that compromises the aircraft ability to stop on the runway or that requires a specific landing configuration (flaps, slats and speed).
2. Fragment of the checklist 2.4. Inoperative items list	Advises about additional faults derived from a main fault or the actions performed to contain that fault. Especially useful for multiple faults.
2. Fragment of the checklist 2.5. Secure the system (uncouple or turn off) or Critical actions to minimize the consequences of the failure	Advises when it is secure to shut down or decouple the system and the consequences of that action.
3. Warning system	Alerts pilots to a problem and its severity or for a mere change in system status.
4. System Synoptic Page	Dynamically displays all aircraft systems, operation, status and components faults.
5. Past Experience	Used as a reference to decisions made in similar situations, regardless of whether the situation was personal or shared by a colleague.
6. Maintenance Personnel	Whether a maintenance technician or the troubleshooting team is available at the maintenance control centre (MCC), helps assess, diagnose and act on faults either not covered by the QRH or for which the QRH cannot solve.
7. Technical Logbook (TLB)	Because all faults and maintenance actions performed in the aircraft in the last two days are recorded in the TLB, it provides an overview of the aircraft's faults and what fault might appear next.
8. Minimum Equipment List (MEL)	Useful to provide more information about the fault and whether the aircraft, after landing, can take-off again before receiving major maintenance actions.

More specifically, RfAs should better support anomaly recognition, fault diagnosis and response. As suggested by Woods (1994), anomaly recognition can be improved by resources that draw attention to a real problem against a noisy background and provide meaningful information about the disturbance, the fault and the system status (Christoffersen et al. 2007; Wright et al. 1996).

The diagnostic process can then be enhanced by warning systems that broaden the set of possible hypotheses for the disturbances and faults (Woods 1994). However, the findings of Carim Jr. et al. (2016) reveal that pilots seem to use fragments of different checklists, minimum equipment lists (MEL), previous experience and contacts with the maintenance

control centre (MCC) and local maintenance engineers in an attempt to diagnose and cope with ill-structured problems. These resources were valuable during avalanches of messages and false alarms (Woods 1995), particularly the MCC, which has access to the entire history of faults for any given aircraft, and the experienced engineers who have additional knowledge not described in the manuals. Carim Jr. et al. (2016) also noticed that the QRH and the synoptic page were used together to build a new course of action based mostly on a trial-and-error approach and as a means to gather more data about the problem.

Finally, Rasmussen and Jensen (1974) and Rasmussen (1993b) suggested that some RfAs are better suited to support some types of reasoning involved in anomaly management than others. Analytical thinking, for example, is better supported by procedures and checklists, while resources that present ready-to-be-used information can enhance heuristics, such as rules of thumb and informal training. Additionally, stories shared informally by colleagues and past experiences, whether or not in the same company, aircraft model or role, contributed to strategies based on the analogical reasoning (Carim Jr. et al. 2016).

4.4. Contrasting the models

A comparison between the original and the revisited model is shown in Table 3. The revisited model is based on empirical evidence highlighting cognitive demands imposed by the cascade of disturbance on operators, how the JCS uses the repertoire of strategies based on different reasoning types to cope with the problem, and how these strategies are supported by a variety of resources for action. As argued by Rasmussen (1993b), and described by Carim Jr. et al. (2016), the strategies and resources are intimately related in the sense that the resources constrain the strategies, and the strategies need to be put into practice through RfAs.

Table 3 Comparison between the original and the revisited model

Construct	Original Model	Revisited Model
(1) Fault behaviour	Faults as dynamic events that produce a cascade of disturbances.	
(2) Unit of Analysis	JCS, emphasizing interactions between technological, human, and organizational agents.	
(3) Activity	Anomaly assessment, diagnosis, course of action.	A wide repertoire of strategies operationalizes anomaly assessment, diagnosis, course of action.
(4) Type of Reasoning	Abductive reasoning.	Spectrum of reasoning types, from heuristic and analogical to abductive and analytical.
(5) Resources	Functions of the warning system.	A variety of resources for action (RfAs), including procedures, documents, systems diagrams, warning system, past experiences and social.

Using the concept of strategy, we operationalized the three cognitive processes proposed by Woods (1994), which was not clear in the original model. The revised model also argues that the JCS has a pool of strategies influenced by many factors, including the available RfAs. The assessment, diagnosis and course of action, encompassed as strategies, are also operationalized through different types of reasoning according to the nature of the disturbances.

Finally, more than the warning system and the QRH, pilots employed a variety of RfAs to support their anomaly assessment, diagnosis and course of action. Procedures, fragments of the checklist, documents, system diagrams, maintenance personnel and past experiences helped pilots cope with the demands imposed by ill-defined problems. Most of these resources were not designed to help them cope with faults but were opportunistically used with purpose.

5. Applying the revisited dynamic fault management model to cockpits

5.1. Description of the case

In one of the events identified by Carim Jr et al. (2016), pilots faced a critical situation immediately after departure. During the climb, the warning system displayed several

1 visual and aural alarms in a sequence. The system indicated fire in both engines, the auxiliary
2 power unit (APU), both cargo compartments (the sensors can only detect smoke) and the two
3 lavatories (the smoke detectors; **construct 1, fault behavior**). As an immediate reaction, the
4 first officer reached the QRH to read the checklist, but the pilot in command did not permit
5 him to do so, because he was certain the situation was a false alarm.
6
7

8
9
10
11 Despite the assessment of a false alarm, the pilots managed the situation as if it was
12 real, except for the checklist and QRH that were not used. They issued a mayday call and
13 requested an immediate return to the departure airport under visual references and the support
14 of fire fighters and ambulance once they had stopped on the runway. They also briefed the
15 cabin crew, requested them to follow the procedures for an emergency landing and addressed
16 the situation with the passengers. The landing was uneventful and, as soon as the airplane had
17 stopped on the runway, fire trucks approached it and visually inspected for any signs of fire.
18 Since nothing was found, the aircraft was released, proceeded to the gate and the passenger
19 disembarked as normal.
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35

36 5.2. Analysis

37
38 The **unit of analysis (construct 2)** in this case was the joint cognitive system
39 involving the cockpit and its functional and structural boundaries (Hutchins 1995; Hutchins
40 and Klausen 1996; Henriqson et al. 2011; Roth et al. 2014; Soo et al. 2016). These
41 boundaries encompass everything that helps pilots to cope with the fault and is located both
42 inside the physical cockpit, including the procedures, warning systems and controller, and
43 outside, such as the cabin crew and passengers, air traffic control and the company's support
44 centre (Carim Jr et al. 2016). The interactions between these elements correspond to the
45 functional boundaries (Hollnagel and Woods 1999).
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 Among the artefacts available, the aircraft warning system and the abnormal and
2 emergency checklists played important roles in this situation (**construct 5; resource**). The
3
4 warning system has more than two thousand fault messages categorized in different levels of
5
6 risk based on a fault-tree analysis (Heymann et al. 2007). Its sensitiveness attempts to balance
7
8 the risk of triggering alarms all the time, including false alarms (Bliss and Gilson 1998; Bliss
9
10 et al. 1999; Bliss and Dunn 2000), and detecting a situation before it becomes irreversible
11
12 (Papastavrou and Lehto 1996; Woods 2015). In the event of multiple faults, the system
13
14 indicates the root cause(s), which is often related to electrical system malfunctions (Carim Jr
15
16 et al. 2016).

17
18 According to their procedures, pilots should retrieve the checklist available in the
19
20 QRH corresponding to the fault message, or messages in the case of multiple faults (Degani
21
22 and Wiener 1990, 1994, 1997; De Brito 2002). The objective is to stabilise the fault
23
24 propagation, recover the faulty system or component and to continue the flight with the
25
26 inoperative system or component (Degani et al. 2005).

27
28 According to the pilot in command, who had more than 10,000 hours in command
29
30 and had flown most of the commercial airplanes models available in the market, assessing
31
32 whether the situation was or not a false alarm was the first and only strategy he could think
33
34 of, particularly because similar occasions had occurred in the past (**construct 3, activity**). He
35
36 recalled that the displayed fault messages were identical to those displayed during the fire
37
38 detection system integrity check, except the fire indication in the lavatory. He also
39
40 remembered a story shared by a colleague, who had been through a similar false alarm, in
41
42 that case, however, the airplane had been on the ground. And this was important because
43
44 reinforced his assessment, signalling a real possibility of false alarm with the fire detection
45
46 sytem.

1 The pilot in command also identified other pieces of evidence that supported his
2 perception (**construct 3, activity**): (a) it is highly unlikely that fire and smoke will appear
3 simultaneously in different systems that are only loosely coupled; (b) there was no visual
4 indication of fire, smoke or smell, neither inside the cockpit nor reported by flight attendants
5 or passengers; and (c) there was no report in the technical logbook that related similar
6 problems in the past or any indications suggesting that a fire would commence, especially in
7 the engines and APU.
8

9 The fire checklist contained in the QRH was not even considered as an option
10 (**construct 5; resources**). The pilot in command argued that the checklist does not consider
11 false alarm scenarios. Thus, reading the fire checklist would have not provided any new
12 evidence. Eventually, it would have led to shutting down the engines and APU. In constrast,
13 the first officer considered using the fire checklists both to avoid “violating” the company’s
14 procedures and in the hope of finding useful information.
15

16 While the rapid diagnostic of a malfunction in the fire detection system test occurred
17 through the comparison among the present scenario, the typical features of the fire detection
18 system test and the story shared by a colleague, the rapid assessment of the situation as a
19 false alarm was predominantly based on simple heuristics. In addition, heuristics were
20 responsible for supporting the pilot’s decision to disregard the checklists and the QRH
21 (**construct 4, types of reasoning**).
22

23 The strategy of managing the false alarm as through it was real (**construct 3,**
24 **activity**), except for the critical and irreversible actions, meant requesting to the air traffic
25 controllers assistance services upon arrival, avoiding shutting down the engines and APU and
26 avoiding discharging the fire extinguisher bottles and landing as soon as possible. According
27 to the pilot in command, the fastest way to return to the airport and land was to request a
28 visual approach to the only one of the four runways not surrounded by mountains.
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1 The pilots also acknowledge that this strategy was necessary, because they are
2 accountable for the flight regardless of the outcome. If they had disregarded the warning
3 system there had been an undesired outcome, even one not directly related to the situation,
4 such as the death of a passenger after a burst tyre or bird strike, they would have been blamed
5 and sued for negligent and reckless behaviour. Additionally, they argued, the fire detection
6 was potentially compromised, which reduces the system's ability to detect fire and smoke in
7 the relevant parts and requires an immediate landing. All these considerations make it explicit
8 that operators not only simulate the practical consequences of situation management but also
9 the ethical ones (**construct 4, types of reasoning**).

10 In regards to the resource employed (**construct 5, resources**), the pilot in command's
11 large experience was built on knowledge, stories and prototypical situations accumulated
12 through years of practice. His knowledge on the airport and surrounding geography was
13 formed along decades, flying to and from this particular airport. Similarly, his familiarity
14 with the fire checklist content and a prototypical situation of a fire alarm system test come
15 from the recurrent simulator training on fire emergencies and the routine of performing the
16 test every first flight of the day. On the other hand, the story about a similar situation shared
17 by a colleague occurred informally when both met in an airport.

18 In sum, the case study highlighted the difference between the original model and an
19 instantiation of the revisited dynamic fault management model, that is graphically contrasted
20 in a conceptual map presented in Fig 3. The analysis evidenced the lack of formal support for
21 coping with false alarms and showed that pilots disregarded the checklists and used their
22 experience to employ adaptative strategies that are neither taught nor developed in training.
23 The heuristics, prototypical situations and knowledge involved in the adaptative strategies
24 may help designers reconceptualise the warning system and the checklist to reduce false
25 alarms and support the crew in coping with those problems, respectively.

6. Conclusion

This paper aimed to revisit the dynamic fault management model for aviation applications and proposed two questions. RQ1: What are the recent developments that contribute to the dynamic fault management model? RQ2: How does the cockpit manage anomalies and emergencies?

The first question was answered by updating three of the five components of the original model using concepts, models and theories derived from cognitive system theory, diagnostic reasoning, naturalistic decision making, reasoning and thinking, situated action and empirical evidence from aviation.

Answering the second question required an instantiation of the revisited model, in which a case was analysed. The case revealed that instead of using the checklist based on the messages presented by the warning system, the false alarm forced pilots to implement adaptative strategies based on heuristics and analogy and supported by their experience. Even though the case was successfully managed, the descriptive nature of the revisited model enabled insights into the anomaly management activity.

Although the empirical data were restricted to one study that researched pilots from a specific airline flying a particular aircraft model, the new model can be further developed through applications to other aircraft models and companies. Furthermore, the study did not assess the model validity, which future experiments conducted in simulators could do. The applicability of the model to contexts other than aviation, such as oil and gas, power plants and transport systems in general, is also a subject for future studies.

Acknowledgements

The first author would like to thank Captain Nicholas Carpenter for insightful contributions.

Funding

This study was funded by Capes (Brazil) in a format of PhD scholarship awarded to the first author while he was conducting this study as part of his PhD research project at the Safety Innovation Laboratory, Griffith University.

Conflict of interest

The authors declare that they have no conflict of interest.

REFERENCES

- Abbott KH (1991) Robust Fault Diagnosis of Physical System in Operation. Phd Dissertation, State University of New Jersey.
- Bliss JP, Dunn MC (2000) Behavioural implications of alarm mistrust as a function of task workload. *Ergonomics*, 43:1283–1300. <https://doi.org/10.1080/001401300421743>
- Bliss JP, Freeland MJ, Millard JC (1999) Alarm related incidents in aviation: A survey of the aviation safety reporting System Database. In: *Proc Hum Factors Ergon Soc Annu Meet* 43:6–10. <https://doi.org/10.1177/154193129904300102>.
- Bliss JP, Gilson RD (1998) Emergency signal failure: implications and recommendations. *Ergonomics* 41:57–72. <https://doi.org/10.1080/001401398187323>
- Burks AW (1946) Peirce's Theory of Abduction. *Phil Sci* 13:301-306. <https://doi.org/10.1086/286904>
- Carim Jr GC, Saurin TA, Havinga J, Rae A, Dekker SWA, Henriqson E (2016) Using a procedure doesn't mean following it: A cognitive systems approach to how a cockpit manages emergencies. *Saf Sci* 89:147–157. <https://doi.org/10.1016/j.ssci.2016.06.008>
- Cerbone DR (2012) Understanding phenomenology. Acumen Publishing Limited, Durham. <https://doi.org/10.1017/UPO9781844653737>
- Christoffersen K, Woods DD, Blike GT (2007) Discovering the events expert practitioners extract from dynamic data streams: the modified unit marking technique. *Cogn Technol Work* 9:81–98. <https://doi.org/10.1007/s10111-006-0043-y>.
- Christoffersen, K, Woods, DD (2003). Making Sense of Change: The Challenge of Events in Operations Environments. Technical Report, The Ohio State University, Columbus, OH.
- Christoffersen, K, Woods, DD (2006). Making Sense of Change: Why Recognizing Events is Special in Cognitive Work. Technical Report, The Ohio State University, Columbus,

OH.

De Brito G. (2002) Towards a model for the study of written procedure following in dynamic environments. *Reliab Eng Syst Safe*, 75:233–244. [https://doi.org/10.1016/S0951-8320\(01\)00097-7](https://doi.org/10.1016/S0951-8320(01)00097-7).

De Keyser V, Woods DD (1990) Fixation errors: failures to revise situation assessment in dynamic and risky systems. In: Colombo AG, de Bustamante AS (eds) *Systems reliability assessment*. Springer Netherlands, Dordrecht, pp 231–251. <https://doi.org/10.1007/978-94-009-0649-5>.

Degani A, Heymann M, Barshi I (2005) A formal methodology, tools, and algorithm for the analysis, verification, and design of emergency procedures and recover. Nasa internal white paper, Nasa Ames Research Centre, Moffett Field, CA.

Degani A, Wiener EL (1990) Human factors of flight-deck checklists: the normal checklist. Nasa contractor report, Nasa Ames Research Centre, Moffett Field, CA.

Degani A, Wiener EL (1994) On the design of flight-deck procedures. Nasa contractor report, Nasa Ames Research Centre, Moffett Field, CA.

Degani A, Wiener EL (1997) Procedures in complex systems: the airline cockpit. *IEEE Trans Syst Man Cybern A Syst Hum Publ IEEE Syst Man Cybern Soc* 27:302–312. <https://doi.org/10.1109/3468.568739>

Dreyfus HL, Dreyfus SE (1986) *Mind over machine: the power of human intuition and expertise in the era of computer*. Free Press, New York, NY.

Dreyfus HL, Dreyfus SE (2005) Peripheral vision. *Organ Stud* 26:779–792. <https://doi.org/10.1177/0170840605053102>

Fields B, Wright P, Harrison M (1997) Objectives, strategies and resources as design drivers. In: Steve H, Judy H, Gitte L (eds) *Human-computer interaction InterAct '97*. IFIP — the International Federation for Information Processing. Springer, Boston, MA, pp

- 164–171. https://doi.org/10.1007/978-0-387-35175-9_31.
- Henriqson E, van Winsen R, Saurin TA, Dekker SWA (2011) How a cockpit calculates its speeds and why errors while doing this are so hard to detect. *Cogn Technol Work* 13:217–231. <https://doi.org/10.1007/s10111-010-0161-4>.
- Heymann M, Degani A, Barshi I (2007) Generating procedures and recovery sequences: a formal approach. In: *Proceedings of the 14th International Symposium on Aviation Psychology*, The Ohio State University, Columbus, OH.
- Hoffman RR, Crandall B, Shadbolt N (1998) Use of the critical decision method to elicit expert knowledge: A case study in the methodology of cognitive task analysis. *Hum Factors* 40:254–276. <https://doi.org/10.1518/001872098779480442>.
- Hollan J, Hutchins E, Kirsh D (2000) Distributed cognition: toward a new foundation for human-computer interaction research. *ACM Trans Comput-Hum Interact ACM Transactions on Computer-Human Interaction* 7:174–196. <https://doi.org/10.1145/353485.353487>.
- Hollnagel E, Woods DD (1999) Cognitive systems engineering: new wine in new bottles. *Int J Hum Comput Stud* 51(2):339–356. <https://doi.org/10.1006/ijhc.1982.0313>
- Hollnagel E, Woods DD (2005) *Joint Cognitive Systems: foundations of cognitive systems engineering*. CRC Press, Boca Raton. FL.
- Holyoak KJ (2005) Analogy. In: Holyoak KJ, Morrison RG (ed) *The Cambridge Handbook of Thinking and Reasoning*. Cambridge University Press, Cambridge, pp.117-142.
- Holyoak KJ, Morrison RG (2005) Thinking and reasoning: a reader's guide. In: Holyoak KJ, Morrison RG (ed) *The Cambridge Handbook of Thinking and Reasoning*. Cambridge University Press, Cambridge, pp.1-9.
- Hutchins E (1995) How a cockpit remembers its speeds. *Cogn Sci* 19:265–288. https://doi.org/10.1207/s15516709cog1903_1

- Hutchins E, Klausen T (1996) Distributed cognition in an airline cockpit. In: Engestrom Y, Middleton D (eds) *Cognition and communication at work*. Cambridge University Press, Cambridge, pp 15–34. <https://doi.org/10.1017/CBO9781139174077.002>
- Johannesen L, Woods DD (1991) Human interaction with intelligent systems: trends, problems and new directions. In: *Proceedings of the 1991 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, Charlottesville, pp 1337–1341. <https://doi.org/10.1109/ICSMC.1991.169874>
- Kahneman D, Frederick S (2005) A model of heuristic judgment. In: Holyoak KJ, Morrison RG (eds) *The Cambridge Handbook of Thinking and Reasoning*. Cambridge University Press, Cambridge, pp. 267-293.
- Kahneman D, Klein GA (2009) Conditions for Intuitive Expertise: A Failure to Disagree. *Am Psychol* 64:515–526. <https://doi.org/10.1037/a0016755>.
- De Keyser, V., & Woods, D. D. (1990). Fixation Errors: Failures to Revise Situation Assessment in Dynamic and Risky Systems. In: Colombo AG, Bustamante AS (eds), *Systems Reliability Assessment* (pp. 231–251). Springer Netherlands, Dordrecht. <https://doi.org/10.1007/978-94-009-0649-5>.
- Klein GA (1993) A recognition-primed decision (RPD) model of rapid decision making. In: Klein GA, Orasanu J, Calderwood R, Zsombok CE (eds) *Decision Making in Action: Models and Methods*, Ablex, Norwood, pp 138–147. <https://doi.org/10.1002/bdm.3960080307>.
- Klein GA (2009) How Can We Train pilots to make Better Decisions? In: O’Neil Jr HF, Andrews DH (ed) *Aircrew training and assessment*. Lawrence Erlbaum Associates, London, pp. 165–195. <https://doi.org/10.1038/nrn1806>
- Klein GA (2015a) A naturalistic decision making perspective on studying intuitive decision making. *J Appl Res Mem Cogn* 4:164–168.

<https://doi.org/10.1016/j.jarmac.2015.07.001>.

Klein GA (2015b) Reflections on applications of naturalistic decision making. *J Occup Organ Psychol* 88:382–386. <https://doi.org/10.1111/joop.12122>.

Klein GA, Calderwood R, Clinton-Cirocco A (1986) Rapid decision making on the fireground. *Proceedings of the 30th Annual Human Factors Society, HFES*, Santa Monica, CA, pp. 576–580.

Klein GA, Calderwood R, Clinton-Cirocco A (1988) Rapid decision making on the fire ground. Technical Report 796, Army Research Institute for the Behavioral and Social Sciences, Alexandria.

Klein GA, Calderwood R, Clinton-Cirocco A (2010) Rapid decision making on the fire ground: the Original Study Plus a postscript. *J Cogn Eng Decis Mak* 4:186–209. <https://doi.org/10.1518/155534310X12844000801203>.

Klein GA, Calderwood R, MacGregor D (1989) Critical decision method for eliciting knowledge. *IEEE Trans Syst, Man, Cybern* 19:462–472. <https://doi.org/10.1109/21.31053>

McCarthy J, Wright P, Monk A, Watts L (1998) Concerns at work: designing useful procedures. *Hum Comp Interaction* 13:433–457. https://doi.org/10.1207/s15327051hci1304_3.

Papastavrou JD, Lehto MR (1996) Improving the effectiveness of warnings by increasing the appropriateness of their information content: Some hypotheses about human compliance. *Saf Sci*, 21:175–189. [https://doi.org/10.1016/0925-7535\(95\)00060-7](https://doi.org/10.1016/0925-7535(95)00060-7)

Patel VL, Arocha JF, Kaufman DR (1994) Diagnostic reasoning and medical expertise. *Psychology of Learning and Motivation* 3:187–252. [https://doi.org/10.1016/S0079-7421\(08\)60411-9](https://doi.org/10.1016/S0079-7421(08)60411-9)

Patterson ES, Watts-Perotti J, Smith PJ, Woods DD, Shattuck LG, Klein GA, Jones PM

- (1998) Patterns in cooperative cognition. In: Proc Hum Factors Ergon Soc Annu Meet 42:263–266. <https://doi.org/10.1177/154193129804200317>.
- Patterson ES, Woods DD (2001) Shift changes, updates, and the on-call architecture in space shuttle mission control. *Comput Support Coop Work* 10:317–346. <https://doi.org/10.1023/A:1012705926828>.
- Peirce CS, Turrisi PA (1997) *Pragmatism as a principle and method of right thinking: the 1903 Harvard lectures on pragmatism*. State University of New York Press, Albany.
- Potter, SS (1994). *The development of temporal and functional information displays to support cooperative fault management*. The Ohio State University.
- Råholm, M. B. (2010). Abductive reasoning and the formation of scientific knowledge within nursing research. *Nurs Philo*, 11:260–270. <https://doi.org/10.1111/j.1466-769X.2010.00457.x>
- Rajkomar A, Dhaliwal G (2011) Improving diagnostic reasoning to improve patient safety. *Permanente J* 15:68–73. <http://dx.doi.org/10.7812/TPP/11-098>
- Rasmussen J (1993a) Analysis of tasks, activities and work in the field and in laboratories. *Trav Hum* 56:133–155.
- Rasmussen J (1993b) Diagnostic reasoning in action. *IEEE Trans Syst, Man, Cybern* 23:981–992. <https://doi.org/10.1109/21.247883>.
- Rasmussen J, Jensen A (1974) Mental procedures in real-life tasks: a case study of electronic trouble shooting. *Ergonomics* 17:293–307.
- Rasmussen J, Nixon P, Warner F (1990) Human error and the problem of causality in analysis of accidents. *Philos Trans R Soc Lond. B, Biol Sci*, 327: 449–460,460-462. <https://doi.org/10.1098/rstb.1990.0088>
- Roth W-M, Mavin TJ, Munro I (2014) How a cockpit forgets speeds (and speed-related events): toward a kinetic description of joint cognitive systems. *Cogn Technol Work*

17:279–299. <https://doi.org/10.1007/s10111-014-0292-0>

Singer G, Dekker SWA (2000) Pilot performance During multiple failures: an empirical study of different warning systems. *Transp Hum Factors* 2:63–76.

https://doi.org/10.1207/STHF0201_8

Soo K, Mavin TJ, Roth W-M (2016) Mixed-fleet flying in commercial aviation: a joint cognitive systems perspective. *Cogn Technol Work* 18:449–463.

<https://doi.org/10.1007/s10111-016-0381-3>.

Stefanov A (2012) Theoretical models as representations. *J Gen Philos Sci* 43:67–76.

<https://doi.org/10.1007/s10838-012-9178-0>.

Suchman LA (1985) Plans and situated actions: the problem of human machine communication. Final Report, Xerox Company, Palo Alto Research Centre, Palo Alto, CA.

Upshur R (1997) Certainty, probability and abduction: Why we should look to C.S. Peirce rather than Gödel for a theory of clinical reasoning. *J Eval Clin Pract* 3:201–206.

<https://doi.org/10.1046/j.1365-2753.1997.00004.x>

Vicente KJ (1999) Cognitive work analysis: Toward safe, productive, and healthy computer-based work. Erlbaum, Mahwah, NJ.

Wartofsky MW (1979). Models: representation and the scientific understanding. Boston studies in the philosophy of science, Vol. XLVIII. Springer Netherlands, Dordrecht.

<https://doi.org/10.1007/978-94-009-9357-0>.

Watts JC, Woods DD, Patterson ES (1996) Functionally distributed coordination during anomaly response in space shuttle mission control. In: Proceedings 3rd Annual Symposium on Human Interaction with Complex Systems, HICS '96, IEEE, Dayton, OH. <https://doi.org/10.1109/HUICS.1996.549494>

Watts-Perotti J, Woods DD (2007) How anomaly response is distributed Across functionally

distinct teams in space shuttle mission control. *J Cogn Eng Decis Mak* 1:405–433.

<https://doi.org/10.1518/155534307X264889>.

Woods DD (1984) Some results on operator performance in emergency events. In: The Institution of Chemical Engineers (ed.) *Ergonomics Problems in Process Operations*, Pergamon Press, Warks, pp. 21–32. <https://doi.org/10.1016/B978-0-85295-172-9.50006-8>.

Woods DD, Johannesen L, Potter SS (1991) Human Interaction with Intelligent Systems: An Overview and Bibliography. *ACM SIGART Bulletin*, 2:39–50. <https://doi.org/10.1145/122570.122571>.

Woods DD (1994) Cognitive demands and activities in dynamic fault management: abductive reasoning and disturbance management. In: Stanton N (ed) *Human factors in alarm design*. vol. 7, Taylor & Francis, Bristol, pp. 63-92.

Woods DD (1995) The alarm problem and directed attention in dynamic fault management. *Ergonomics* 38:2371–2393. <https://doi.org/10.1080/00140139508925274>.

Woods DD (2015) Four concepts for resilience and the implications for the future of resilience engineering. *Reliab Eng System Saf* 141:5–9. <https://doi.org/10.1016/j.ress.2015.03.018>.

Woods DD, Hollnagel E (2006) *Joint Cognitive Systems: patters in cognitive systems engineering*. CRC Press, Boca Raton, FL.

Woods DD, Johannesen L, Cook RI, Sarter N (1994). *Behind human error: cognitive systems, computers and hindsight*. Crew Systems Ergonomic Information and Analysis Center, WPAFB, Dayton OH

Woods DD, Patterson ES (2000) how unexpected events produce an escalation of cognitive and coordinative demands. In: Hancock PA, Desmond PA (eds) *stress workload and fatigue*, Lawrence Erlbaum, Hillsdale, NJ, pp. 1–15.

<https://doi.org/10.1097/ACM.0b013e3181ea3831>.

Woods DD, Sarter NB (2010) Capturing the dynamics of attention control from individual to distributed systems: the shape of models to come. *Theor Issues Ergon Sci* 11:7–28.

<https://doi.org/10.1080/14639220903009896>.

Wright P, Fields B, Harrison MD (1996) Distributed information resources: A new approach to interaction modelling. In: *Proceedings of the 8th European Conference on Cognitive Ergonomics*, 10-13 September 1996, European Association of Cognitive Ergonomics, Granada, Spain, pp. 5–10.

Wright P, Fields B, Harrison MD (2000) Analysing human-computer interaction as distributed cognition: the resources model. *HumComput Interaction* 51:1–41.

https://doi.org/10.1207/S15327051HCI1501_01

Wright P, McCarthy J (2003) Analysis of procedure following as concerned work. *Human Factors and Ergonomics*. In: Hollnagel E (ed) *Handbook of cognitive task design*. Lawrence Erlbaum Associates, Mahwah, NJ, pp. 679–700.

<http://dx.doi.org/10.1201/9781410607775.ch28>

Wright P, Pocock S, Fields B (1998) The prescription and practice of work on the flight deck In: *Proceedings of the 9th European Conference on Cognitive Ergonomics*, 24-26 August 1998, European Association of Cognitive Ergonomics, Limerick, Ireland, pp 37–42.

Figure captions

Fig. 1 The original representation of the three cognitive processes proposed by Woods (1994)

Fig. 2 Representation of the strategies described by Carim Jr. et al. (2016) and based on Woods (1994)

Fig. 3 Conceptual map of the original and revisited models

Dr. Guido Carim Junior
Griffith University
170 Kessels Rd, Nathan,
Brisbane, Australia, QLD 4111
+61 7 3735-5573
g.carimjunior@griffith.edu.au

Dr Oliver Carsten and Dr Frédéric Vanderhagen,
Editors-in-Chief
Cognition, Technology and Work

06nd of January 2019

Dear Dr Carsten and Dr Vanderhagen:

I am pleased to resubmit the original research article entitled “How the cockpit manages anomalies: Revisiting the dynamic fault management model for aviation” by me, Dr Guido Carim Junior (first author), A/Prof Tarcisio Abreu Saurin and Prof Sydney Dekker. We appreciate the reviewers’ comments and incorporated most of the suggestions, which we believe improved the paper quality and readability. All the changes are highlighted in yellow in the manuscript and on the following lines we address each comment.

- 1) **Reviewer #1:** “[The paper] discusses how cognitive and social structures are involved in analysis and decision-making including representation technologies, previous experience and social experiences such as shared stories. This concept is less easy to define in analytical terms but is well researched and described by other authors such as Klein, Lehrer and Kahneman. A little more reference to the powers of intuition (essentially split second decision making without thought) in unexpected events would have enhanced the paper...”

Response: We included references from Klein, Kahneman and Holyoak and further developed the section 4.2 (old section 4.4) “Construct 4: Spectrum of reasoning (types of reasoning)”. We also reviewed the theories available and decided to consider heuristics and analogy as part of intuition and not include Lehrer’s notion of gut feelings or emotion-driven intuition because our empirical data do not support them. This limitation was included in the conclusion.

- 2) **Reviewer #2:** “[...] just revising the DFMM, you’ve done very well, but for those ‘revision’ 4.2 falls short of the mark to really be a revision. And 4.1 is also not persuasive that it is really needed. However, the last 3 revisions are nicely argued and seem to be real contributions. But as far as explaining how a cockpit manages anomalies, I feel that you’re missing a section which brings all the stuff about cockpits together. I’d really like to see a few case studies or reinterpretations of prior case studies of accidents or incidents where you show how your model provides real description and additional insight can be gained”. Then, reviewer #2 proposes “add Section 5: Applying the DFMM for Cockpits. Here’s where I’d introduce section 4.2 - it isn’t really a revision, so much as a specialization or specification when dealing with cockpits (or make a separate category of specializations after your revisions). If you decide to keep 4.1, then begin it the way you begin 4.3 by stating how it differs plainly from the original model in 3.1. I reread these sections a few times and was not convinced 4.1 was a real revision. If not a revision, but just a specialization for cockpits - then move to the new Section 5 (or make a separate category of specializations after your revisions)”.

Response: We agree that sections 4.1 and 4.2 are specifications of the model when applied to aviation. Thus, we created the section 5 “Applying the revisited anomaly management model to cockpits” as suggested, where we present a real case (section 5.1), originally discussed by Carim Jr et al. (2016), and then analyse it (section 5.2). Both old sections 4.1 and 4.2 were substantially reduced and incorporated as parts of the analysis.

- 3) **Reviewer #2:** “The only other outstanding question I had was the change in reasoning to include both heuristic and analytic reasoning in addition to abductive. I'm a bit confused now, because when I think about all reasoning types, I think of different dimensions and one dimension runs from heuristic on one end to analytic on the other. And you could do abductive, inductive or deductive reasoning anywhere along the spectrum. So, I think it would be good to define your reasoning better.”
Response: We agree and decided to review the definition of reasoning in section 3.7 “Construct 4: Abductive reasoning (type of reasoning)” and the definition of heuristics, analogy and analytical reasoning in section 4.2 “Revised Construct 4: Spectrum of reasoning (types of reasoning)”. We tried to make clear the model should account for heuristics, analogy and analytics in addition to abductive. We also defined them based on two dimensions, as suggested by Klein, Kahneman and Holyoak: speed of the logical manipulation and the conscious effort required. We decided not to include inductive and deductive reasoning because our empirical data do not support them.
- 4) **Reviewer #2:** “[...] decide if you really need to keep RfA as acronym you introduce it on Pg. 8, but then don't use it again until Page 26. I was completely lost when re-encountering it. Maybe just wait until page 26”.
Response: We agree with the reviewer and the acronym was first introduced on page 22, section 4.3 “Revised Construct 5: A variety of resources for action (resources)”, when the resource for action theory is first introduced in the manuscript.
- 5) **Reviewer #2:** “I'd consider moving Table 3 forward to the beginning of Section 4”.
Response: The table 3 is already in section 4. Even so, we revised the figures and tables to adequate to the reviewed text and decided to relocate Fig 1 at the end of section 5 (Fig 3).
- 6) **Reviewer #2:** “section 3.2 is very well known and could probably be shortened to be more inline with the lengths of the other sections”.
Response: We agree and shortened the section. We tried to condense the description of a joint cognitive system and make explicit its relation to the anomaly management activity.
- 7) **Reviewer #2:** However, if you'd happily just propose a revision to the DFMM - then you can just remove a lot of the cockpit stuff and have a shorter, but still impactful paper.
Response: We appreciate the comment. However, we still think the paper only makes sense if the reviewed dynamic fault management model is combined with application to aviation, particularly because of the context-dependent empirical data.

We still ensure this manuscript has not been published, is not under consideration for publication elsewhere and its content has been approved by the co-authors.

Thank you again for your consideration.
Sincerely,

Guido Carim Junior, PhD
Senior Lecturer, Griffith Aviation
Griffith University