USING A FORMAL LANGUAGE TO SUPPORT NATURAL LANGUAGE IN ACCIDENT REPORTS

C.W. Johnson [1], *J.C. McCarthy* [2] *and P.C. Wright* [3]

[1] The Human-Computer Interaction Group,
The Department of Computer Science,
The University of York, Heslington,The United Kingdom, YO1 5DD.
E-mail: johnson@minster.york.ac.uk, Telephone: + 0904 433376.

[2] The Department of Applied Psychology,
University College Cork, Ireland.

[3] British Aerospace's Dependable Computing Systems Centre,
The University of York, The United Kingdom.

ABSTRACT

Accident reports written by official bodies, such as the Air Accident Investigation Branch of the United Kingdom's Department of Transport, are produced in response to all major civil aircraft accidents or incidents. There are many statutory, legal and commercial implications that rest on the analysis, conclusions and recommendations that these reports contain. Air accident reports usually follow a standard format of synopsis followed by factual information, including history of flight and the systems involved, followed by analysis and conclusions. Finally, there are safety recommendations aimed at preventing a recurrence of the accident. Natural language is the primary means of communicating all of these findings. In requirements engineering there is an increasing recognition that natural language is not always an adequate means of expressing some of the detailed reasoning associated with the causal analysis of complex systems. Recent work in software engineering has explored the use of formal, mathematically based, techniques to help gain the required level of clarity and precision. We argue that accident reports, like requirements documents could benefit by the use of formal techniques to complement the usual natural language descriptions. In this paper we consider one specific accident report. The limitations of its natural language descriptions are examined and we explore the use of a Petri Net notation to help elucidate its ambiguities.

Keywords: Safety Critical Systems; Petri Nets; Accident Reports; Natural Language.

1 Introduction

This paper argues that formal, mathematically based notations can be recruited to support natural language descriptions of accidents. In particular, Petri Nets are advocated as a means of representing findings that can be used to guide the development of safety critical systems.

1.1 Safety Critical Systems

The term 'safety critical systems' is used in the engineering industry to refer to applications where system failure may result in injury, loss of life, severe environmental damage or loss of the system itself. Nuclear power stations, chemical production plants, commercial shipping and aircraft are examples of safety critical systems. Every effort is made in the design of these applications to avoid catastrophic system failure. In many domains there are regulatory bodies, such as the United Kingdom's Civil Aviation Authority or the United State's Federal Aviation Administration, to whom manufacturers must prove that their products are safe. As a result, catastrophic accidents are extremely rare events. For example, Nagel (1988) reports that the accident rate for commercial aircraft, defined as a hull loss or a fatality, is approximately two in every million departures. This represents a significant reduction over the last twenty years, although with such small figures there is considerable variation from year to year. The rate in 1960 was over forty-five per million departures.

1.2 Accident Investigations

The rarity of aircraft accidents makes it important that as much information as possible is gained from such events. This information can be used to improve operating procedures, operator training, system design, system maintenance and system management. In the United Kingdom, the Air Accident Investigation Branch of the Department of Trade and Industry (AAIB) is responsible for investigating all aircraft accidents and major incidents. In the United States, this responsibility rests with the National Transportation Safety Board. Our analysis will focus upon the United Kingdom's air accident reporting procedure because this is the system which the authors are most familiar with. We believe, however, that many of our findings are applicable to the reporting procedures used in other domains and by other countries. A feature shared by all accident investigations is that they are lengthy processes. They involve analysis by specialists who are drawn from many different technical disciplines: human factors; forensic investigation; engineering reconstruction; computer simulation; etc. The result of such investigations are presented in official accident reports. These usually follow a standard format: synopsis; history of flight; analysis; conclusions and recommendations for preventing further accidents. The recommendations made in these reports are intended to influence the working practices of operating companies. If adopted by the Civil Aviation Authority, they may eventually be reinforced by statutory powers. Interim recommendations can also be made directly by the AAIB. For example, they recommend immediate modifications to a particular aircraft type. It is, therefore, of great importance that the analysis, conclusions and recommendations are as clear, unambiguous and precise as possible.

This paper focuses upon techniques which can be used to improve the clarity and precision of one part of an accident report; the history of flight. This part of the document describes the actual events that lead up to the accident. It is the data on which further analysis rests. It is consequently very important to ensure that this description is correct and complete. Most reports use natural language to describe the events, such as aircraft manouvers, radio communications and system failures, which contribute towards an accident. The history of flight information also describes how the various 'actors' or 'agents', including pilots, co-pilots and air traffic controllers, respond to these events. Such descriptions are inherently temporal. There is often a great deal of detail describing precisely when an event took place and what else was happening at that time. As a descriptive narrative, the text associated with the history of flight information is rich in terms such as "meanwhile", "then", "at time x", "after x then y",

" while x then y" and so on. A particular thread, such as what the co-pilot was doing, will be pursued through a period of time. Subsequent paragraphs will then follow another thread extending over the same period and so on through the various streams of activity that contribute to the accident. Forming a global picture of the accident can, therefore, be quite difficult for the reader. Time lines, track plots and other graphical techniques can help in forming this global picture. Unfortunately, many of these notations are ad hoc in that they lack any standard format. They may only represent one aspect of an accident; readers must consider ways in which pilot actions can be integrated onto time-lines that represent the behaviour of a particular engine or avionics system. A further problem is that these techniques do not help the reader think about the causal relations that may or may not exist between various events. The remainder of this paper argues that Petri Nets can be used to avoid these limitations.

1.3 Outline Of The Paper

A 'real-life' case study is used to demonstrate the utility of Petri Nets as a means of supporting accident reports. The next section provides a resumé of the events which led to the crash of a Boeing 737-400. Following this we highlight limitations of the textual description of the *History of the Flight* section in the accident report. The Petri Net notation is then introduced. This formalism is used to analyse our case study. In particular, we show how Petri Nets can be used to avoid some of the limitations which restrict the utility of natural language descriptions. The final section identifies the conclusions that can be drawn from this research and proposes directions for further research.

2 Resumé Of The Kegworth Accident

A British Midlands Boeing 737-400 took off from Gatwick headed for Belfast. Approximately thirteen minutes into the flight the turbofan on the number one (left) engine fractured causing a series of compressor stalls in that engine. The pilots did not know what had happened. There were excessive vibrations throughout the airframe. Loud noises and a smell of fire could also be detected in the cockpit. There were transitory fluctuations on the primary instrument displays and a maximum reading on the airborne vibration meter (AVM) for the left engine. The crew's initial reaction was to diagnose a fire. The First Officer commented:

> "It's a fire Kevin. It's a fire coming through."

In response the commander dis-engaged the auto throttle and said:

> "Which one is it though?"

The 1st officer replied:

> "Its the le, its the right one."

The commander then requested the First Officer to throttle the right engine back. In fact it was the left hand engine that was faulty; the First Officer had identified the wrong engine. It was a perfectly healthy right engine that was throttled back. Surprisingly, when the First Officer did this all indications of trouble in the left engine went away except for a maximum reading on the AVM for the left engine. The pilots did not notice this indication. The right hand engine was throttled back twenty-two seconds after the vibration, shuddering and smell of smoke first occurred. In the ensuing two and a half minutes the smoke cleared and the commander ordered the right engine to be shut-down. During this period the AVM reading for the left engine dropped from a maximum of five to two units, slightly above normal. All indication suggested that the pilots had solved the problem. It was decided to divert the aircraft to East Midlands Airport. This activity engaged the First Officer for some time since he had difficulty in re-programming the flight management system with the diversion route. The aeroplane appeared

to be flying normally and there was no reason to suspect that the wrong engine had been shut down. Passengers and cabin crew had seen smoke and sparks emanating form the left engine and smoke entered the passenger cabins. The cabin steward went forward to the flight deck and reported that the passengers were panicky. The commander then used the intercom to reassure the passengers. He said that they had experienced trouble with their right hand engine but that the problem had been solved by shutting it down. Survivors of the accident reported noticing the discrepancy between what they had witnessed happening to the left engine and the Captain's solution which involved the right engine. Approximately fifteen minutes later, as the aircraft was being manouvered for its final approach to runway twenty-seven at East Midlands Airport, there was an abrupt decrease in power in the left engine. Attempts to re-start the right engine failed. The commander then tried to stretch the glide of the aircraft but he failed and the aircraft crashed on the embankment of the M1 motorway two hundred yards short of the start of the runway. A total of forty-six passengers died and a further seventy-four suffered serious injury.

3 The Limitations Of Natural Language

Although plans, diagrams, photographs, and schematics are included in air accident investigation reports, the medium of the accident report is predominantly natural language. One of the advantages of natural language is its accessibility. This is an advantage because these reports are intended to be read by people from a wide range of disciplinary backgrounds: safety specialists; engineers; computer scientists; human factors specialists etc. Natural language descriptions also suffer from a number of limitations. It is important that the readers of accident reports are aware of these problems. The limitations noted in this section derive from an analysis of Section 1.1 of the AAIB Report into the Kegworth accident (AAIB, 1990).

3.1 Incompleteness

Some sequencing information was not present in the report and could not be inferred. It is stated that:

> "throughout the descent there were distractions from a small number of other aircraft making radio calls on the same frequency as that being used by G-OBME".

Not only can we not tell the times of these "distractions" from the report but we cannot even be sure that they were "distractions", given the lack of information on what the crew were doing when these radio calls were heard.

3.2 Inconsistent Temporal Referencing

As well as important timing information being omitted, there is the added problem that when timing information is given it is not always given in the same form. For example, absolute times are used:

> "At 2024.33hrs the commander broadcast a crash warning".

Relative times are also used:

> "Seven seconds later the ground proximity warning system (GPWS) glide-slope warning system sounded."

The aircraft's position in space is also used to fix events:

> "When the aircraft was 13 nm from touchdown on this new heading and descending to 3,000 ft AMSL, ATC advised a right turn".

Imprecise temporal intervals are also used:

"The commander called immediately for the First Officer to relight (i.e., restart) the other engine."

3.3 Inconsistent Object Referencing

Inconsistent references are made in the Kegworth report to many objects that were involved in the events leading to the accident. Together with the the temporal inconsistencies, described in the previous section, these object reference inconsistencies result in a great deal of ambiguity. For example, the engines are referred to by their numbers; 1 and 2. Elsewhere they are referred to as the left and right engines. Some of these inconsistencies arise from the verbatim reporting of witnesses. Others have no such justification. This creates considerable confusion and doubt; the reader of the report is drawn into continual cross referencing to ensure that they understand the natural language description.

3.4 Lack Of Precise Definitions

One of the reasons that natural language is so accessible is the facility it affords to use words flexibly. The intended meaning of a word may not be quite the same every time it is used. In many domains this need not be a problem; the specification of meaning is facilitated by the context in which a word is used. Such flexibility does, however, cause problems for accident investigations where a higher degree of precision is required. The Kegworth report suggests that the Captain's decision to divert increased the crew's workload so that there was little scope for checking their diagnosis:

"Whilst the commander's decision to revert to East Midland's Airport to land with the minimum delay was correct, he thereby incurred a high cockpit workload which precluded any effective review of the emergency or the actions he had taken."

This contains many assumptions about the source and consequences of workload that are not made explicit. Nowhere in the report is 'workload' defined even though the Human Factors literature contains many potential definitions. For an overview of alternative approaches see Moray (1988). This lack of precision can have important consequences. 'Common sense' meanings of these terms may differ from reader to reader; conclusions based upon personal interpretations may be ill-founded.

3.5 Cause-Effect Assumptions

The AAIB report states that:

"Immediately after throttling back the No. 2 engine, the First Officer advised London Air Traffic Control (LATCC) that they had an emergency situation which looked like an engine fire. The commander then ordered the First Officer, "SHUT IT DOWN"."

Engine shut down is the required operating procedure in the event of an engine fire. But in this case there was no fire and there was no fire alarm. In fact, the crew had indications of excessive engine vibration and the required operating procedure for this is to idle the engine. It could be argued that the natural language description contains the implicit assumption that the commander's decision to shut down the engine was influenced by the First Officer's diagnostic report to air traffic control.

There are two problems with implicit assumptions like this. First, it is not at all clear whether the report writer intended the reader to infer the 'causal' link between the commander's command and the First Officer's report. Our interpretation is prompted by the juxtaposition of the two sentences in the text. If our inference is incorrect then this property of natural language renders it open to misinterpretation. Second, if the report writer did intend the reader to conclude such a causal link, it is not clear whether this intention is based upon an assumption made by the writer or upon some evidence gleaned from interviewing the commander during the investigation.

3.6 Assumptions About Domain Specific Knowledge

The Kegworth accident report often assumes that readers are aware of the normal and emergency operating procedures that are followed by the crews of commercial aircraft. Actions are often described without explicit reference to the agent who carried them out. For example, in order to know who actually throttled back the engine the reader has to know that it is the First Officer's responsibility to throttle back the engine when carrying out an emergency procedure.

3.7 Representing Concurrent Activity

Natural language descriptions are not ideally suited to representing concurrent streams of activity. The natural language description of the history of flight in the Kegworth report first focuses upon the interaction between members of the crew on the flight deck. This continues for six paragraphs and takes the reader through the initial engine failure to the engine shut down and diversion. The focus then reverts to the experiences of the cabin crew and passengers during the initial engine failure. The natural language description does not, therefore, lend itself to the construction of an ordered sequence of events relating the experiences and actions of all participants.

3.8 Volume

Natural language descriptions can be quite 'wordy'. The section that forms the basis of the current analysis is four pages long but the whole report extends over one hundred and seventy pages. There is a danger in such a voluminous and dense document that important details are missed by the reader. For instance, after a number of passes we identified the possibility that the commander had two independent information sources confirming the 'erroneous' diagnosis: direct experience of smoke which appeared to enter from right side ventilation and the First Officer's remark about the source of the failure. This is not immediately apparent from an initial reading of the natural language report.

Larkin and Simon (1987) argue that two representations may be informationally equivalent but that their computational efficiency may differ. Diagrammatic representations may, therefore, be more computationally efficient than natural language descriptions. Larkin and Simon point out that diagrammatic representations are organised by location. This affords efficiencies when spatial organisations are best suited to the readers' tasks. If a task requires access to related items of information then it can be beneficial to group data under a single node in a diagram. Semantic relations can be represented by the distance between nodes. Diagrammatic representations can, therefore, complement the usual natural language descriptions in accident reports.

4 A Brief Introduction To Petri Nets

Petri Nets have been used to support the engineering of concurrent systems (Kramer, 1991). Chretienne (1986) shows how they can be exploited to represent and reason about timing properties of system events. Hura and Attwood (1988) have used Petri Nets to support accident analysis from the perspective of systems engineering. They have also been used to represent human factors requirements. Van Biljon (1988) and Bastide and Palanque (1990) exploit Petri Nets to derive formal specifications of interactive systems at a very high level of abstraction. Johnson (1993) has shown that Petri Nets can be used to represent the operator-system interaction which can lead to accidents. This section builds upon this work and shows how Petri Nets can be used as an adjunct to natural language in accident reports.

Petri Nets can be used to represent the state of a human-machine system in terms of the conditions that are satisfied during intervals of interaction (Peterson, 1977). When particular conditions hold, certain events can occur. If an event takes place then it can alter the state of the human-machine system. Changes in state are represented by the new conditions that hold after an event has occurred.

These new conditions enable further events to take place. More formally, Petri Nets are directed graphs; $PN = (P, T, E, M)$. They consist of a set of places, P, transitions, T, edges, E and markings, M.

Places can be used to describe the conditions which hold for operators and their systems during the course of an accident. In particular, they can be used to represent the pre-conditions for disaster. In our case study, accident analysts can use a place to represent the fact that vibrations are emanating from engine number one. Places can also be used to represent causes which are specifically related to the human factors or systems engineering of an application. Places can be used to represent human factors observations about the behaviour of individual operators; the Captain believes that the fault is in engine number two. Places can also represent the behaviour of individual systems; the AVM is displaying an 'out of range' warning.

Transitions can be used to represent the events that cause accidents. They can represent events initiated by both systems and their operators. In our case study, the initiating event leading to the accident can be identified as the fracturing of the fan blade in engine number one. This systems engineering event can be represented as a transition which changes the state of the human-machine system into one in which smoke and vibrations are emanating from the engine. Similarly, human factors observations indicate that the First Officer's remark about the source of the fault was a critical transition in the human-machine system. Isolating these critical transitions provides a focus for subsequent human factors and systems analysis. The Captain could have been provided with additional information to help him to correctly diagnose the source of the failure. Design resources might have been allocated to determine whether it was possible to directly report the fan blade fracture as a problem in engine number one.

Edges connect places to transitions: $E \subseteq \{P \times T\} \cup \{T \times P\}$. They can be used to form the chains of events and conditions that lead to an accident. They can be described in terms of two functions. The function Op maps from each transition to its set of output places. The output places of a transition represent the conditions which hold after an event has occurred. For example, an output place can be used to represent the systems engineering observation that the detection of vibrations in number one engine causes the out of range reading on the AVM display. An input place function, Ip, maps from each transition to the set of input places for that transition. The input places of a transition specify the conditions which must hold for an event to occur. The input place of a transition can be used to represent the human factors observation that the First Officer's guess as to which engine was failing led him to remark: "Its the le, its the right one.".

4.1 Graphical Notation

Petri Nets can be represented graphically. Events, or transitions, are shown as bars (–). Conditions, or places, are denoted by unfilled circles (◯). Edges are shown as arrows linking places and transitions. Figure 1 shows a simplified graphical Petri Net representation of the Kegworth accident.

In order to model the dynamic behaviour of a human-machine system, tokens are used to mark those places in a Petri Net which are enabled. A place is enabled if its conditions hold. The tokens in a net are said to characterise a marking state and are denoted graphically by filled dots (•). For instance, Figure 2 is marked to show that there is smoke and that the AVM is displaying an out of range reading. Analysts can alter the marking of a Petri Net to indicate the different conditions that hold for operators and their systems. These walk-throughs can be used to simulate the sequences of events and states that are identified during accident investigations. A transition can fire if all of its input places contain at least one token. After firing, a token is deposited in each of the output places of a transition. In Figure 2 it is possible for the transition indicating that the Captain notices the smoke to fire. The transition representing the First Officer's remark about the source of the problem can also fire. If these transitions fired then the places indicating that the Captain believes it is engine number two and that the First Officer is committed to his decision would be marked with tokens.

The graphical Petri Net notation can be used to provide a high-level representation of the hundreds of pages of analysis that are contained in accident reports. Figure 3 illustrates the sequence of events

that led to the fatal decision to shut-down the functioning engine. It also represents some of the critical factors that could have prevented the accident. These are represented using inhibitor arcs. Transitions which are linked by an inhibitor can only fire if the place from which the inhibitor comes is not marked. Inhibitors are represented graphically as an edge with a small empty circle on one end. In Figure 3 an inhibitor arc is shown running from the place labelled `Display layout is poor` to the transition marked `1st Officer correctly polls AVM`. In our example, the place is marked and so the transition cannot be enabled. Poor display layout, therefore, prevents the 1st Officer from correctly polling the AVM. Similarly, an inhibitor arc is used to link the place stating that the Captain is unfamiliar with the ventilation system and the transition labelled `Captain correctly diagnoses engine #1`. The place is also marked to indicate that the pilot's lack of information about the ventilation inhibited a correct diagnosis.

5 Using Petri Nets To Support Natural Language

Having introduced the Petri Net notation, this section demonstrates ways in which this formalism can be recruited to avoid some of the limitations of natural language descriptions in accident reports. The intention is not to advocate Petri Nets as a substitute for natural language descriptions but as an adjunct to conventional reporting techniques.

5.1 Incompleteness

The first criticism raised against natural language accident reports was that they are often incomplete. It can be hard to determine the scope of an accident investigation. It may not be clear which events actually contribute to an accident. Petri Nets can be used to overcome this problem; they provide a graphical means of defining the scope of an accident investigation. Analysts must identify a place or transition which marks the starting point of an accident. This is illustrated by the place labelled `There is fatigue in fan blade #17` in Figure 3. From this place or transition, human factors and systems engineers must trace the sequences of events that lead to the final outcome of the accident. This analysis would produce a network which could act as a reference point for subsequent analysis. The advantage of this approach is that the scope of the analysis is explicitly represented in an accessible form and is not implicitly embedded within many dozens of pages of natural language analysis.

5.2 Inconsistent Temporal Referencing

Petri Nets represent sequences of events as successive transitions linked by a series of edges and places. Analysts are restricted to a single and, therefore, consistent means of representing temporal information. This has the advantage that readers are not then forced to extract many different real and interval time references in order to re-construct the ordering of events leading to an accident. Figure 4 shows how a Petri Net can be used to provide consistent representation for the many different temporal references that were used in the natural language excerpts of Section 3.2.

One of the problems with the notation exploited in this paper is that it loses some of the real-time information that is captured in an accident report. This is illustrated by the following passage from the Kegworth report:

> "17 seconds after the power loss the fire warning system operated on the number 1 engine."

The lack of real-time references need not be a significant limitation for our application of Petri Nets. Accident reports are intended to guide the development and operation of subsequent systems. It is unlikely that the delay between the two events, described above, will be exactly replicated in future accidents. The absence of real-time information, therefore, increases the genericity of the information

represented by a Petri Net. It should be noted, however, that some real-time properties are significant for subsequent systems. The following quotation describes a critical delay in the crew's response to the developing emergency on G-OBME. This real-time interval is significant because future flight management systems could be designed to support airborne re-programming in under two minutes:

> "Flight deck workload remained high as the First Officer obtained details of the actual weather at East Midlands and attempted without success to program the flight management system to display the landing pattern at East Midlands. This last activity engaged the First Officer's attention for two minutes."

It is possible to represent such real-time delays by extending the Petri Net notation. Figure 5 shows how this can be done. Transitions are assumed to be instantaneous, they mark the beginning and end of the conditions described by the places. Non-negative time values are associated with places, such as `1st Officer is reprogramming Flight Management System`. Previous applications of real-time Petri Nets have associated durations with all places (Levi and Agrawala, 1990). The net shown in Figure 5 does not do this because, typically, it is not possible to derive accurate timings for all of the events leading to an accident. For example, not all of the interaction between the cabin crew and the Captain were registered on the flight recorder. In other scenarios, timing information has been lost when recordings have been lost or corrupted (AAIB, 1989).

5.3 Inconsistent Object Referencing

The use of the Petri Net notation does not, in itself, ensure that human factors and systems engineers will exploit a consistent object reference scheme. It is possible to label places and transitions with references to both "the left engine" and "engine number one". Petri nets do, however, provide a means of reducing the likelihood of such inconsistency. The process of constructing a network helps to strip out the verbiage that can disguise inconsistent references in natural language descriptions. Figure 3 adopts the convention of referring to the engines by their number; the right engine is referred to as #2 and the left engine is referred to as #1. This reduces the degree of inconsistency but it does not eliminate it. The 1st Officer observes "It's the le... it's the right one". The transition which represents this utterance is, therefore, inconsistent with the more general naming scheme for G-OBME's engines. Such problems are unavoidable if the exact words of crew members and air traffic controllers are to be represented in the network descriptions of an accident. It is impossible to constrain the vocabulary of all of the parties involved in an accident after it has occurred! One means of reducing this problem would be to maintain a glossary of terms used in each Petri Net. For example, the following excerpts describe terms used in Figure 3:

> *Engine #1*:
> The left engine on G-OBME. Site of the original fracture in fan blade number 17, increasing load on the engine led to loss of power which brought the aircraft below its glidepath.
> *Engine #2*:
> The right engine on G-OBME. Incorrectly diagnosed as the mal-functioning engine, throttled back and then shut down during the accident.

The Kegworth report only contains a brief glossary of abbreviations. Extending such descriptions could increase the general accessibility of accident reports.

5.4 Lack Of Precise Definitions

Section 3.4 argued that the semantic richness of natural language makes it difficult to avoid the imprecise use of certain words and phrases. Petri Nets can be used to reduce the impact of this problem because

they could provide a focus for different analytical techniques. For example, human factors specialists could advise other experts about the use of terms such as 'workload' within networks. Where experts disagree, for instance over the definition of workload (Kantowitz and Casper, 1988), pragmatic decisions must be made to ensure that different analysts do not assume different definitions of the term. These standard definitions can be incorporated into a glossary like that proposed in the previous section.

Structural properties of Petri Nets provide graphical representations of certain terms that are used in the natural language sections of accident reports. High workload situations are those in which operators are engaged in more than one simultaneous task. In terms of a Petri Net these would be represented as multiple places which are marked and which relate to a particular individual. For example, in Figure 6 the places labelled `Captain is aware of smoke on flight deck` and `Captain is distracted` by the call of other aircraft can both be marked at the same time. High workload can be assumed to occur because the Captain must diagnose the cause of the smoke whilst monitoring the messages from the other aircraft. A limitation of this approach is that it does not differentiate between the cognitive and perceptual demands imposed by particular tasks. It is important to emphasise that such Petri Nets are intended to augment rather than replace natural language descriptions. Such details can more easily be incorporated into traditional forms of analysis. This process would be aided by the techniques advocated in this paper because the framework of the analysis would be explicitly represented by the Petri Nets. Definitions of particular terms would be explicitly represented within natural language glossaries.

5.5 Cause-Effect Assumptions

Section 3.5 has argued that natural language descriptions of accident reports can contain implicit assumptions about the causal sequences of events that lead to accidents. In particular, it was argued that the Kegworth report assumes the Captain's decision to shut engine number two down was influenced by the First Officer's report of an engine fire to London air traffic control. It can be argued that the Petri Net in Figure 7 represents this causal relationships. The transition labelled `1st Officer reports to London Air Traffic Control that it looked like an engine fire` is linked by a chain of edges to the transition labelled `Captain: Shut it down`. It is important to emphasise, however, that transitions and places represent sequences of states and events during an accident. They indicate a temporal rather than a causal ordering which must be inferred by the reader. This emphasises the importance of integrating Petri Nets into natural language accounts within accident reports. Such inferences can be supported by textual descriptions.

5.6 Assumptions About Domain Specific Knowledge

The amount of domain specific knowledge that is often assumed in accident reports can be reduced if designers can identify the informational requirements of potential readers. It would be extremely time consuming to describe all of the contextual information relating to the normal operation of a complex system. For instance, many volumes of natural language analysis would be necessary in order to describe the many hundreds of tasks performed by the Captain and his crew during the Kegworth accident. Much of this domain specific detail will be irrelevant for the causes of an accident. The process of constructing a Petri Net can help to filter out this mass of contextual information. For instance, analysis of the causal relationship between the 1st Officer's comments and the Captain's commands in Figure 7 might encourage analysts to explicitly represent information about normal operating procedures. Readers can only explain the Captain's command to shut down engine number two if they know that the crew are required to shut down an engine which is on fire. In other words, the causal link can only fully be explained by including details about the steps that are taken against engine fires. Figure 8 shows how the Petri Net of Figure 7 can be extended to represent this additional information. It should be noted that the introduction of this information forces minimal changes to the existing network.

Section 3.6 argued that natural language reports often assume their readers are familiar with the allocation of tasks within a particular working context. This complaint is a more specific form of the general problem of domain specific assumptions, described above. The networks presented in this paper have countered this problem by explicitly associating places and transitions with the different 'agents' involved in the accident. For example, Figure 7 associated the `Shut it down` transition with the Captain. The report to London Air Traffic Control is associated with the First Officer. Such attributions do not form a necessary component of the Petri Net notation and they are dependent upon the self-discipline of the individual analyst. It is hypothesised, however, that necessary information about task allocations may be more readily identified and represented in networks which provide a common communication medium between all of the parties involved in an accident investigation.

5.7 Representing Concurrent Activity

Petri Nets were first developed to represent concurrent behaviour in complex systems (Peterson, 1977). Section 3.7, in contrast, argues that natural language is ill-suited to the description of concurrent events in accident reports. For example, the *History of the Flight* section in the AAIB report describes the events leading up to the decision to shut down the number two engine. This is done from the perspective of the Captain and the First Officer. The report then goes on to detail the events from the perspective of the cabin crew. This sequential style of presentation makes it difficult to identify possible interactions between such concurrent strands of activity. It is difficult to assess whether the passengers' correct observations about the source of the smoke could have been passed to the Captain in time to prevent the wrong engine from being shut down. Figure 3 shows how the concurrent behaviour of the pilot and his passengers can be woven into the overall structure of a Petri Net. This is illustrated by the two separate sequences of places and transitions which stem from `Smoke enters ventilation`. This transition triggers the passenger's observation of the fault with the number two engine. It also triggers the Captain's observation of smoke on the flight deck.

5.8 Volume

One of the criticisms raised against natural language descriptions of accidents is that they can be extremely lengthy. This, in turn, can dissuade designers from devoting the time that is required to plough through the many different analyses presented in accident reports. It can also be difficult to identify important sequences of events during the course of an accident. Such details may be obscured by the volume of data contained in many reports. It has been argued that the use of a graphical notation can reduce this problem by stripping out important events so that they can be presented in a more accessible form.

Unfortunately, there are a number of costs associated with the use of a graphical notation. In particular, it is important that human factors and systems engineers have a clear understanding of the behaviour of the systems represented by Petri Nets. It can be difficult to trace the likely passage of tokens through the many places and transitions that make up complex networks. Elsewhere we describe how hierarchical networks can be used to reduce this problem (Johnson, 1993). Tools can also be recruited to support the development of Petri Nets. They can animate the enabling and firing of transitions as tokens pass from place to place in a network. For instance, Chiola's GreatSPN can be used to view tokens as they pass through a Petri Net:

> "The possibility of playing (such) token games highly simplifies the development of correct models, thus eliminating the need for more complex 'net debugging'." (Chiola, 1987).

The resulting animations provide powerful communications tools which can be shown to the many different teams that must collaborate during an accident analysis. Such facilities are vital if complex networks are to represent accident scenarios.

6 Conclusions And Further Research

In this paper we have argued that accident reports are an extremely valuable source of information for the design of future generations of safety critical systems. They can be used to direct maintenance activities and can guide operator training for existing systems. The statutory bodies which are commissioned to produce these reports have wide ranging powers; they can recommend changes to improve system safety. It is, therefore, important that accident reports are correct and complete. It is also vital that this information is communicated in a form which is understandable by a wide range of interested parties.

Natural language provides an accessible and understandable medium for accident reports. It does, however, suffer from a number of limitations. The power and flexibility of natural language is bought at the expense of precision and clarity. This is a problem not only in accident reporting but also in requirements definition and in legal documentation. Within the legal profession great lengths are taken to avoid ambiguity by the use of specialist and erudite phraseology. This solution increases precision but reduces accessibility for non-specialists. Further problems limit the utility of natural language as a means of representing the findings of accident analyses. It can be difficult to represent sequences of events that unfold in time either concurrently or sequentially. Similarly, it can be difficult to represent the ways in which many different events interact to cause accidents in complex systems. Such problems can be reduced by the incorporation of graphs and diagrams, such as track-plots, into accident reports. These illustrations cannot represent alternative courses of events nor can they capture detailed interactions between different agents.

In this paper we have examined the value of a mathematically-based notation as an adjunct to natural language. Petri Nets have both a graphical and a textual form. We have focussed upon the use of the graphical form to represent various alternative courses of events that could have occurred during an accident. We have argued that these networks can help accident analysts to visualise the relationships between various events. This, in turn, can support informal reasoning about causation and information flow during an accident. In order to illustrate our argument, we have highlighted the shortcomings of a natural language description of the Kegworth accident. We have described ways in which Petri Nets can help to overcome each of these limitations. One important advantage is that concurrent activity can be represented in a very straightforward way. Another is that tool support can be recruited to simulate the sequences of events that are described in accident reports. Animations can be used to assess the completeness of a textual description and provide powerful tools for communication.

In conclusion, we feel that the use of Petri Nets provides a valuable adjunct to conventional accident analysis. It provides a means of expressing the results of an accident investigation in a clear and precise manner without incurring the associated overhead of more rigorous formal techniques, such as full algebraic specification.

7 Acknowledgements

This research was supported by British Council/EOLAS grant number 9284(1992).

8 References

Air Accidents Investigations Branch, Department of Transport. *Report On The Incident Involving BAC 1-11 G-AYWB and Boeing 737 EI-BTZ On 12 April 1988 At Gatwick Airport*, number 2/89, Her Majesty's Stationery Office, London, United Kingdom, 1989.

Air Accidents Investigations Branch, Department of Transport. *Report On The Accident To Boeing 737-400 G-OBME Near Kegworth, Leicestershire on 8th January 1989*, number 4/90, Her Majesty's Stationery Office, London, United Kingdom, 1990.

R. Bastide and P. Palanque. Petri net objects for the design, validation and prototyping of user-driven interfaces. In D. Diaper, D. Gilmore, G. Cockton, and B. Shackel, editors, *Human-Computer Interaction—INTERACT'90*, pages 625–631. Elsevier Science Publications, North Holland, Netherlands, 1990.

W.R. Van Biljon. Extending Petri nets for specifying man-machine dialogues. *International Journal of Man-Machine Studies*, 28(4):437–455, 1988.

G. Chiola. GreatSPN users' manual. Technical report, Departmento di Informatica, Universita' delgi Studi di Turino, Turino, Italy, 1987.

P. Chretienne. Timed Petri nets: A solution to the minimum-time-reachability problem between two states of a timed-event graph. *Journal of Systems and Software*, 6(1-2):95–101, 1986.

G.S. Hura and J.W. Attwood. The use of Petri nets to analyse coherent fault trees. *IEEE Transactions On Reliability*, 37(5):469–473, 1988.

C.W. Johnson. The application of Petri Nets to represent and reason about human factors problems during accident analyses. To appear in M. Jones and L. Brooks (eds.), Requirements Capture For Multi-User Systems, Elsevier, North Holland, 1993.

B.H. Kantowitz and P.A. Casper. Human workload in aviation. In E.L. Wiener and D.C. Nagel, editors, *Human Factors In Aviation*, pages 157–187. Academic Press, London, United Kingdom, 1988.

B. Kramer. Introducing the GRASPIN specification language SEGRAS. *Journal of Systems and Software*, 15(1):17–31, 1991.

J.H. Larkin and H.A. Simon. Why a diagram is (sometimes) worth ten thousand words. *Cognitive Science*, 11, 1987.

S.-T. Levi and A.K. Agrawala. *Real-Time Systems Design.* Mc Graw Hill, New York, United States of America, 1990.

N. Moray. Mental workload since 1979. *International Reviews Of Ergonomics*, 2:123–150, 1988.

D.C. Nagel. Human error in aviation operations. In E.L. Wiener and D.C. Nagel, editors, *Human Factors In Aviation*, pages 263–303. Academic Press, London, United Kingdom, 1988.

J.L. Peterson. Petri nets. *Computing Surveys*, 9(3):223 – 252, 1977.

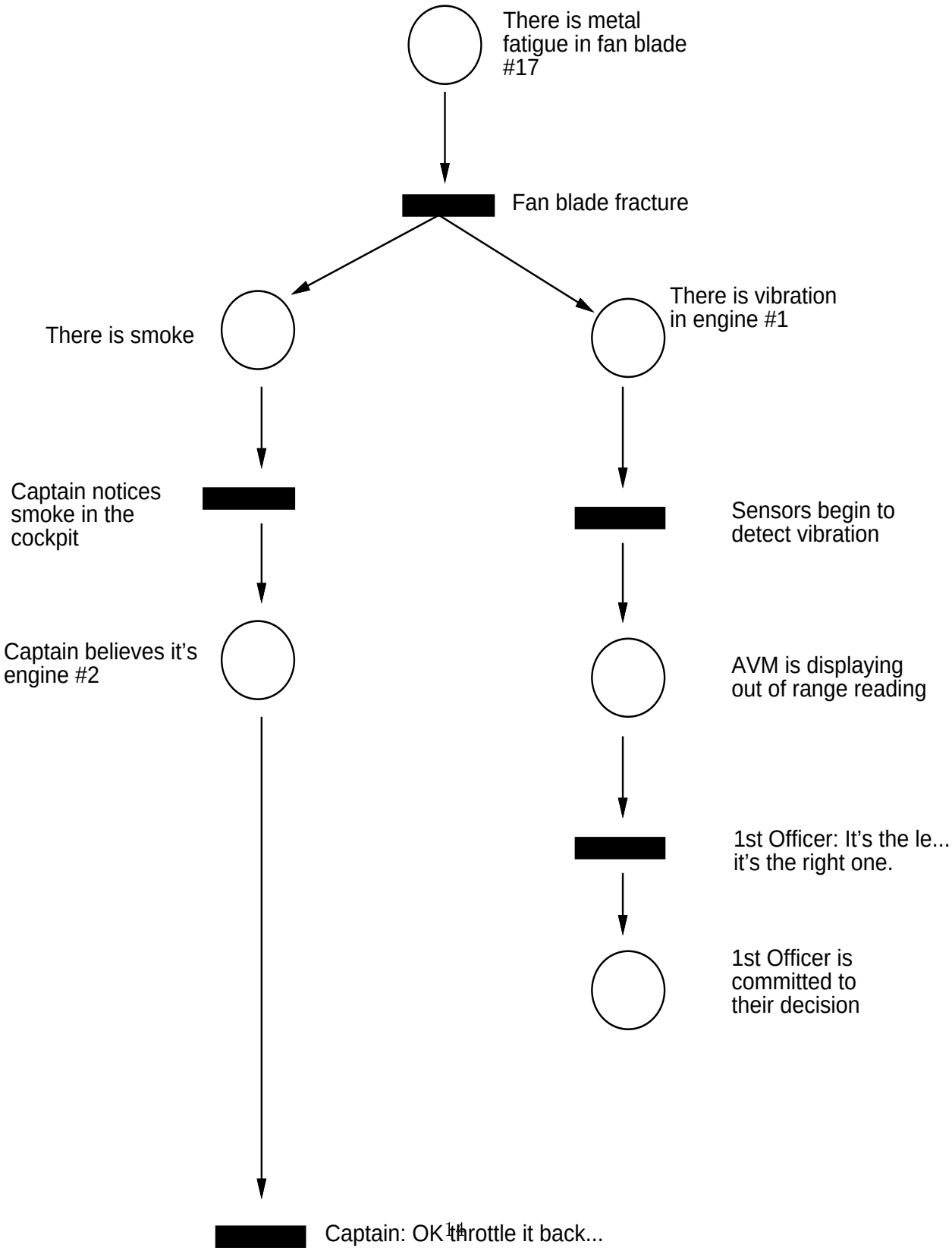

Figure 1: A Simple Petri Net.

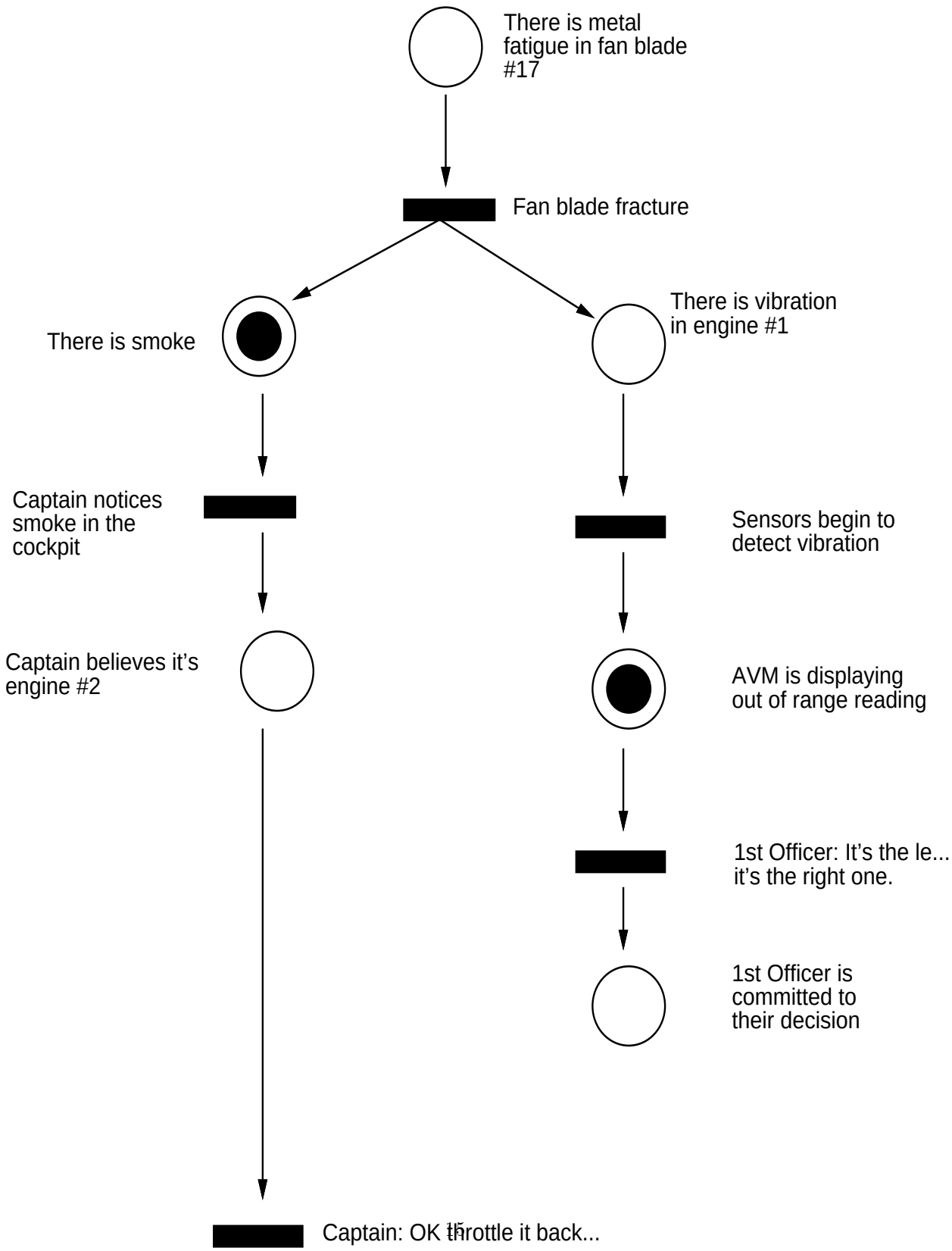

Figure 2: A Simple Marked Petri Net.

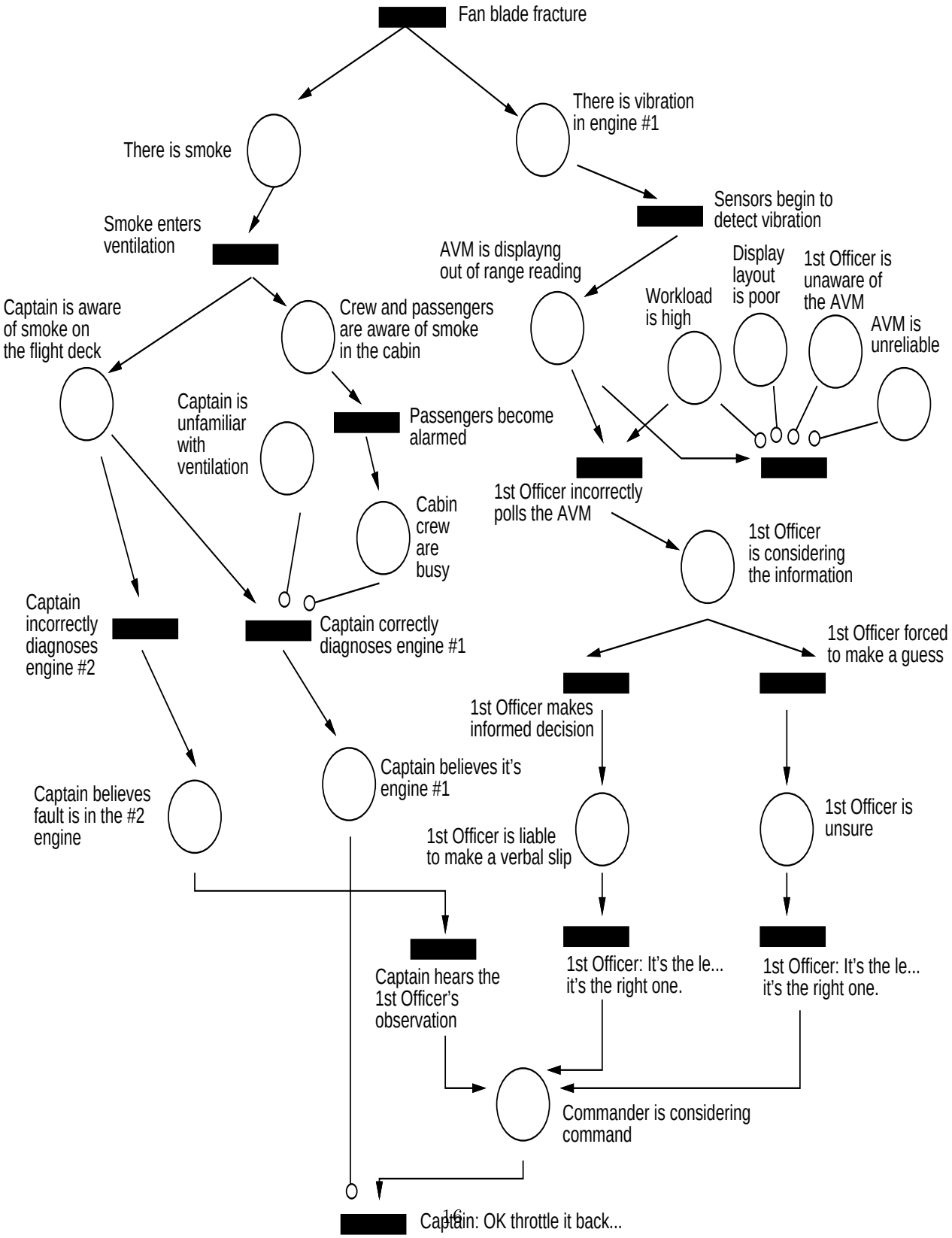

Figure 3: A Petri Net Representing Initial Events In The Kegworth Accident.

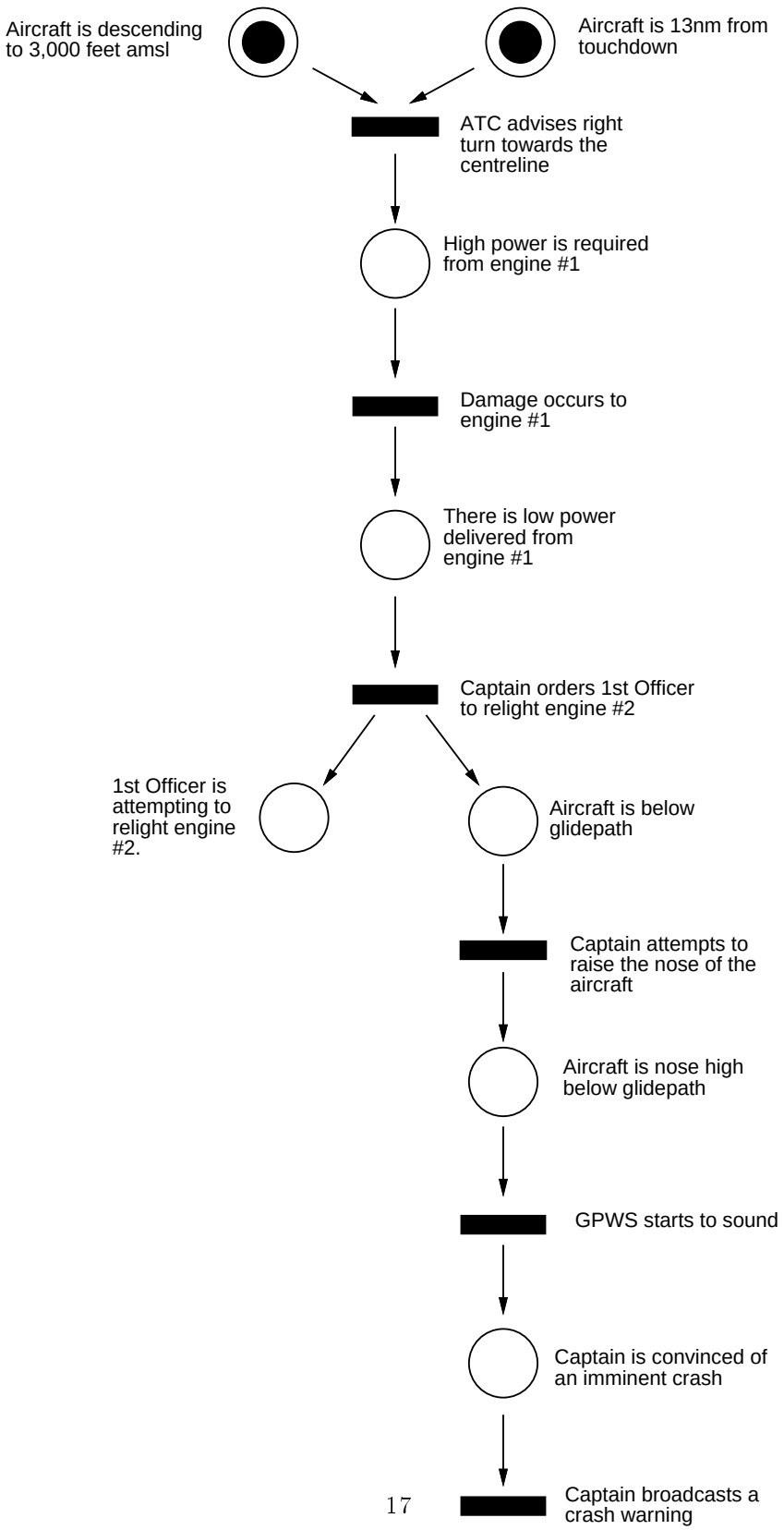

Figure 4: A Petri Net With A Single Temporal Reference Scheme.

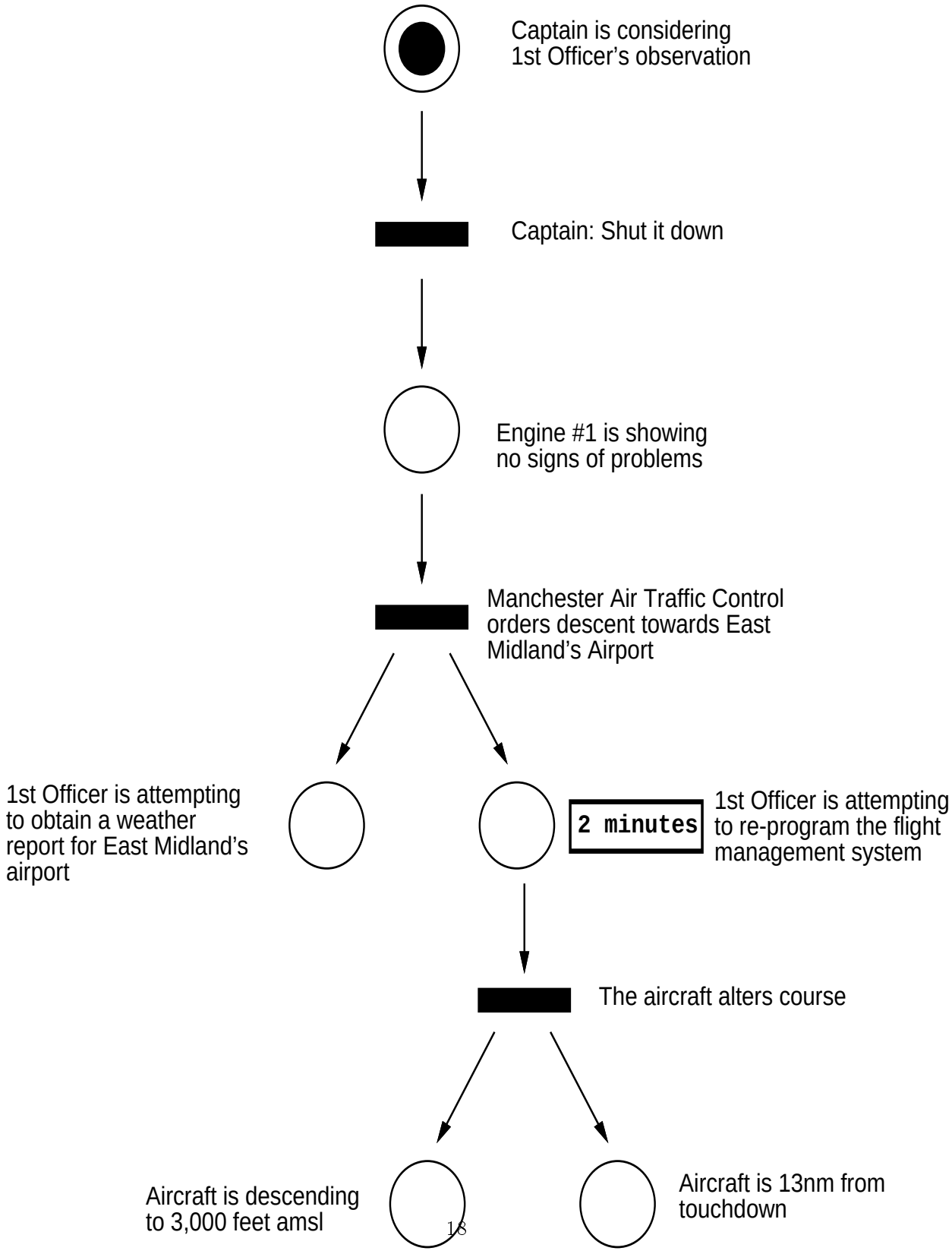

Figure 5: A Petri Net Representing A Real-Time Delay.

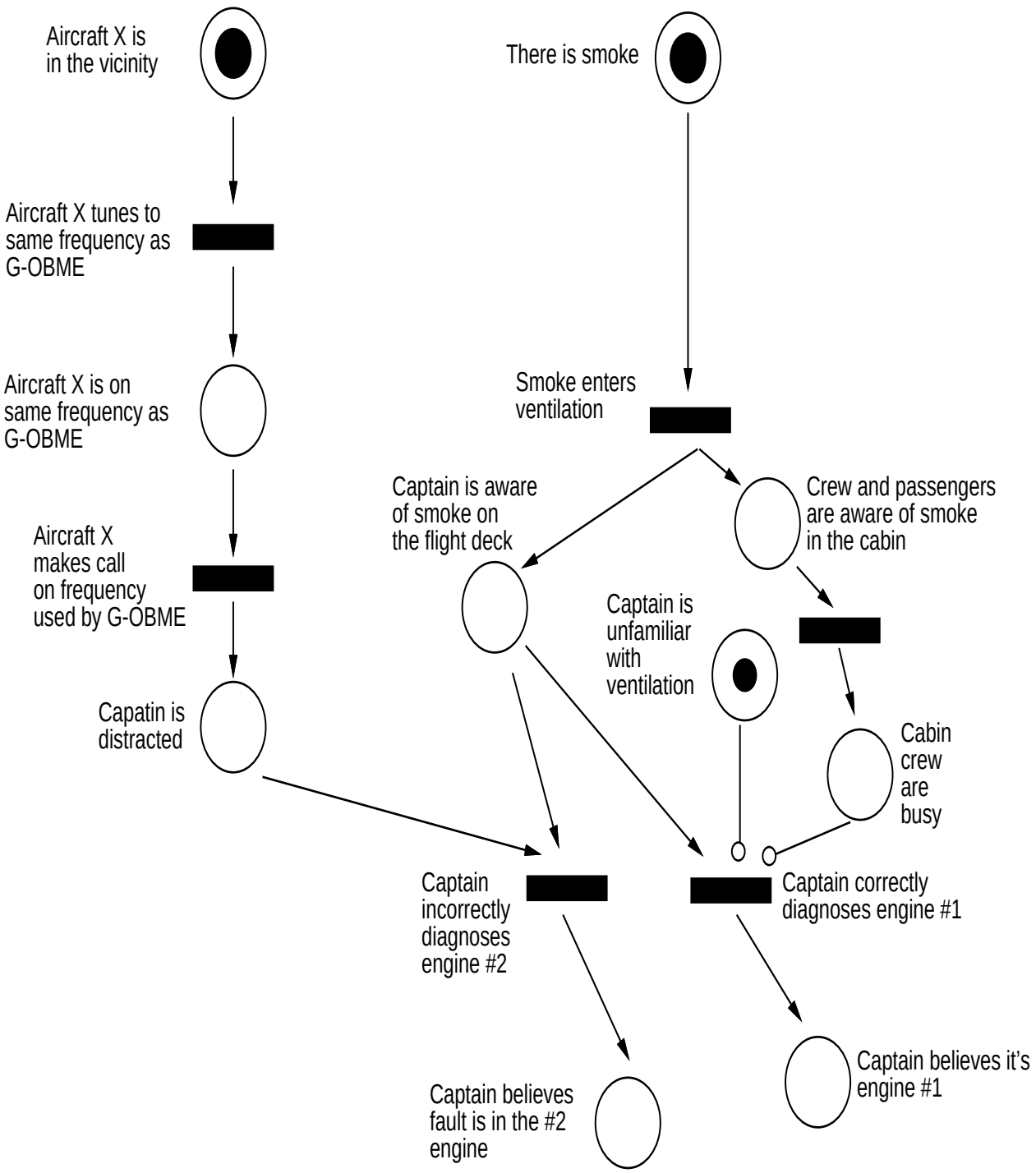

Figure 6: A Petri Net Representing Potential For High Workload.

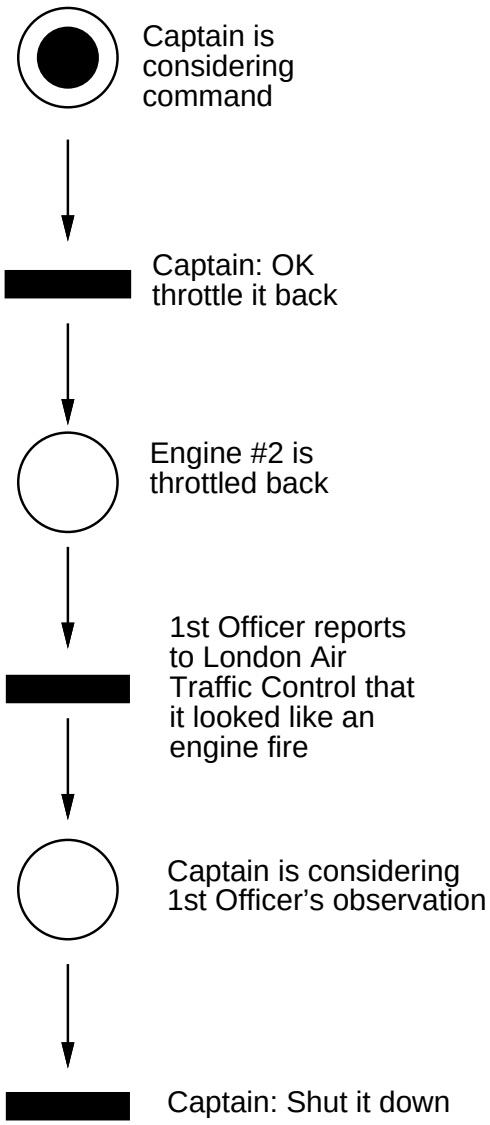

Figure 7: A Petri Net Representing A Causal Relationship.

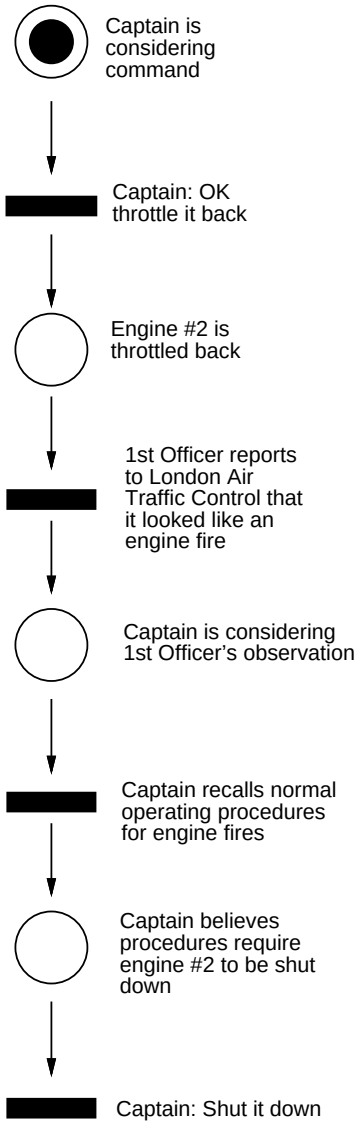

Figure 8: A Petri Net Representing Domain Specific Knowledge.