Chapter 7

Secondary Investigation

This chapter looks at the immediate follow-up to a preliminary report. It begins by examining the role of specialist incident investigators who may be called in to supplement the work of the primary recipient. In particular, it looks as the way in which they must define the scope of any inquiry. Subsequent sections describe ways in which further evidence is gathered about an incident. This is then used in Chapters 7.3 and 8.3 to reconstruct the events that contributed to an adverse occurrence.

In some cases, it may be decided that the investigation of an incident should be terminated after the publication of a preliminary report. Such a decision could be based on a preliminary risk assessment; the apparent criticality of the incident does not justify the expenditure involved in additional investigatory resources. Alternatively, such a decision could be based on the workload that must be supported by investigation teams. An incident that might receive further consideration under 'normal' circumstances might be neglected through pressure of work with other adverse occurrences. As a result, it is important to document the reasons why an investigation is stopped:

> "The reporting officer will ordinarily decide whether or not an incident is accountable or reportable. This decision cannot be an arbitrary one, but must be based on a thorough review of all evidence, as opposed to speculation, related to the incident in question and be in accordance with the requirements of the accident reports statute and the guidelines provided in this Guide. If you are certain that a particular situation is outside the scope of the reporting requirements, then the basis on which this determination was made must be thoroughly documented before the case may be omitted from the monthly submission. If there is any uncertainty as to whether or not to report an incident, it is recommended that a report be made." [235]

Clearly the decision to terminate an investigation must be monitored to ensure that it does not jeopardise an important 'learning opportunity'. Typically, the documentation that justifies such a decision should be forwarded to regional or national safety management groups for further analysis [423]. For instance, certain units might consistently assign relatively low risk levels to incidents that have the potential to cause more serious failures if any available protection measures are compromised [702].

The secondary investigation takes place after the primary recipient of an incident report has drafted their preliminary account. This document is based on initial witness statements and a cursory examination of any physical evidence. However, it is unlikely to be complete. The timelimits, mentioned in Chapter 5.4, that govern the production of these reports typically imply that these initial accounts will be based on partial evidence. For instance, it can take some time to extract information from automated logging systems. Similarly, lab-tests on metallurgical failures can take weeks or months to complete. It is, therefore, important that procedures are specified to coordinate any subsequent investigations.

The simplest approach to any secondary investigation is to allow the primary recipient to continue with an investigation. This has numerous potential benefits. In particular, it is likely that they will understand the local context in which an incident occurred. This is important because it can be difficult for external investigators to quickly come to terms with this situation. The primary recipient is also likely to be a trusted individual. For instance, we have described how they are often 'local champions' for the reporting system. The primary recipient may also have been nominated to perform this role by their per group. There are, however, a number of potential problems with this approach.

Some of these problems inspired the writing of this book. Later sections of this chapter will provide primary recipients with a number of techniques that can be used to support the secondary investigation of adverse occurrences. Subsequent chapters introduce analytical techniques that support more detailed causal analyses. Such written material can be supported by training courses that provide primary recipients with this information in a manner that can be tailored to the particular needs of their organisation. For example, Section 4.7 of the US Lawrence Livermore Laboratory's Health and Safety Manual states that "Training course EM2010 (Occurrence Reporting) is required for managers, supervisors, and others involved in occurrence reporting activities" [478]. The problem with this approach is that it can be extremely expensive to sustain an in-house training capability in incident investigation. In particular, it can be difficult to ensure that such guidance continues to conform with national and international guidelines. As a result, a number of organisations offer training courses that are intended to provide staff with the information and skills that are required during a secondary investigation. For instance, the American Institute of Chemical Engineers offers a course on Investigating Process Safety Incidents:

> "*You should attend if:* You are a technical professional who wants to be a team leader in critical process safety investigation situations. Process engineers, superintendents, managers, operating supervision personnel and Process Safety Management program coordinators have all found this course to be a valuable resource for developing a solid system for investigations.
>
> *You can expect to:* Learn how to be an effective process incident investigation team member or team leader. Focus on the structure and function of the investigation management system but not on root cause analysis techniques. Discover how to create a turn-key investigative management system tailored to your organisation's needs. Gain a comprehensive view spanning the scope of the investigation management system ranging from pre-planning to report generation...from structure to function. Broaden your knowledge of process related incidents, specifically vs. personnel injuries. Apply practical techniques based on up-to-the-minute reports like the AIChE/CCPS Incident Investigation Guidelines. Utilise key principles and practical skills in two stimulating workshops intended to reinforce your knowledge.
>
> *Content you can count on:* Multiple Root Cause Concept and Investigation
>
> *Methods:* Management System Development, Evidence Gathering and Analysing, Witness Interviewing, Determining Root Causes, Forming and Evaluating Recommendations, Preparing Written Reports.
>
> *Interactive Workshops:* Witness interview; Incident investigation." [24]

The use of such professional courses helps to ensure that staff are kept up to date with regulatory reporting requirements without incurring the costs associated with maintaining local training provision. However, professional courses can also incur significant costs for organisations that want to train primary recipients in secondary investigation techniques. As a result, many organisations only send regional or national investigators to these training sessions. There are also a number of further pragmatic issues that limit the use of local, primary recipients during subsequent stages of incident investigation. As mentioned, it is likely that the employee representatives, supervisors and local managers who initially receive incident reports will have a good grasp of the environmental and contextual factors that contribute to adverse occurrences. However, they may lack an awareness of regional or national safety priorities. In particular, it can be difficult for these individuals to find out about whether or not a particular incident forms part of a wider pattern of similar failures. There are also concerns that the standard of skill, training and commitment to secondary investigations will not be consistent across all branches of an organisation. As a result of these concerns, many organisations allocate subsequent investigation tasks to a small group of regional or national investigators. For example, the US Army specifies a number of detailed training requirements that must be satisfied by the relatively small number of individuals who can lead aviation incident and accident investigations [804]. These fall into two phases. In the first phase, they must complete the Aviation Safety Officer Course, they may additionally have to sit a Chemical Accident Investigator Class. They must complete classes on Blood-borne Pathogen and Hazardous Materials and Human Factors in Accident Investigations. They must also display a knowledge of the relevant military investigation guidance; AR 385-95, AR 385-40, AR 385-10, DA Pam 385-40 and USASC Investigations Handbook. Finally, they must have participated in an aircraft accident investigation orientation. The second phase of training for these 'professional' investigators includes courses on Aircraft Accident Investigation, Rotorcraft Accident Investigation, Basic Crash Survivability Investigation and on Advanced Crash Survivability Investigation. Investigators must also demonstrate proficiency in investigative and briefing skills to a board of peers and group commanders. Additionally, these individuals must ensure that they maintain 'accident investigation currency'. if more than six months passes between investigations then officers can be required to participate in a subsequent accident investigation orientation. The Chief, Aviation Systems and Accident Investigation must ensure that investigators continue to satisfy these various requirements.

As can be seen from the previous paragraph, 'professional' investigators will be better trained in incident investigation techniques than the primary recipients who initially pass on information about an adverse occurrence. However, as noted, there is a danger that national and regional inspectors will lack important local knowledge. There is also a danger that, over time, they may become isolated from the practical experience of performing the functions whose failure they must subsequently investigate. For example, many European air traffic service providers require that incident investigators have a minimum of ten years active service as controllers. However, their appointment as investigators necessarily places demands on their time that can prevent them from acting as controllers. After a relatively short period of time they must be re-trained not simply in investigation techniques but in the revised procedures and new systems that their colleagues must exploit to support their everyday tasks.

It is important to emphasise that the use of highly trained and well motivate personnel will not guarantee the overall success of an investigation. Even though a secondary investigation is performed in a reliable and consistent manner, it is still possible for the recommendations not to be acted upon. For example, incident investigators who work for the Train Operating Companies (TOC) on UK railways must satisfy the following regulatory requirement:

1. preservation and collection of evidence, including securing the scene of an accident;
2. accident investigation;
3. maintenance of confidentiality;
4. forensic and interview techniques;
5. human performance assessment; and
6. root cause analysis. [352]

However, Her Majesty's Railway Inspectorate (HMRI) enquiry into the investigation of incidents involving 'Signals Passed at Danger' (SPADs) found that "in some cases greater emphasis was placed on completing a multi-page form than getting to the root cause of the SPAD incident". This was apparent even though the actions of regional investigators were governed by railway group standard GO/RT3252 'Signals Passed at Danger':

> "Inspectors identified shortcomings in the competence of those charged with investigating SPAD incidents in some Train Operating Companies, whereas others were seeking to address this by suitable training in root cause analysis in order to ensure greater competency in root cause investigation techniques."[351]

The consequences of this were identified in a recent internal report that examine the failure of the HMRI to respond adequately to previous problems at the signals which were involved in the Ladbroke Grove rail crash:

> "During the almost five years preceding the Ladbroke Grove accident, there had been at least three occasions when some form of risk assessment analysis on the signaling in the Ladbroke Grove area has been suggested or proposed. The requests were: the Head of Technical Division's letter of 11 November 1996 which requested a layout risk assessment of the re-signaling (paragraph 43); the Field Inspector's letter of 16 March 1998 to Railtrack (paragraph 64); and the Railtrack Formal Inquiry of 1 July 1998 (paragraph 66). In addition there was an earlier request for details of measures taken to reduce the level of SPADs in the area around SN109 recorded in the Head of Technical Division's letter of 1st March 1995 (paragraph 39). None of these requests appear to have been pursued effectively by HMRI." [353]

These quotations illustrate systemic failures in the conduct and monitoring of the secondary investigations that are the focus for this section of the book. Local TOC inspectors were expected to investigate and report on any SPADs that were reported. However, the enquiry showed that these primary recipients had not received sufficient training to perform their duties. The HMRI inspectors were supposed to ensure that TOC inspectors investigated and acted upon those reports. However, the internal report argues that they failed to respond to the shortcomings of the TOC inspectors. In consequence, the root causes of many SPADs were not addressed before the Ladbroke Grove accident.

7.1 Gathering Evidence about Causation

Previous paragraphs have argued that the primary recipient of an incident report must be trained in investigation and analysis techniques if they are to follow-up on the information that is contained in a preliminary report. However, training courses and their supporting documentation provide no guarantees either that a secondary analysis will be performed in a rigorous and consistent manner or that any consequent recommendations will be acted upon. This chapter looks at some of the reasons why it is so difficult to build on the primary report of an incident. Subsequent chapters present a range of techniques that can be used to address these barriers to the secondary investigation of adverse occurrences

7.1.1 Framing an Investigation

One of the main decisions to be made during any subsequent investigation of an incident is to determine the scope of the analysis. This raises a number of theoretical and pragmatic problems. For example, some authors have suggested that it is possible to separate an analysis of *what* happened from the more causal investigation of *why* those events occurred [414]. This provides considerable analytical benefits. Later sections will describe how it is possible to build mathematical models of causation that link the events identified during an investigation to explain the reasons why an incident occurred. However, this division of *what* and *why* creates pragmatic difficulties for the incident investigator. For example, without some preliminary ideas about the probable causes of an adverse occurrence, it can be difficult to determine what evidence should be gathered. It is often infeasible to gather every possible item of evidence in response to a preliminary report. For example, the previous chapter cited instances in which investigators choose not to gather CVR data, because they believed that it would not make any contribution to the overall understanding of the incident. Initial informal ideas of causation, therefore, seem to play a critical role in guiding the initial investigatory process. Several of the mathematical techniques that support the causal analysis of accidents and incidents now recognise the importance of this iterative process [469]. Evidence that is obtained about the course of an incident can force investigators to revise their initial ideas about the causation of an adverse occurrence. This iterative loop is illustrated between the various phases of data gathering, reconstruction and analysis in Figure 5.1.

This chapter focuses on reconstruction techniques that help investigators to determine what happened. In consequence, we postpone an analysis of tools that can be used to support the causal modelling of *why* an event occurred until Chapter 9.3. As notes in the previous paragraph, however, it is difficult in practice to separate the causal analysis from the process of gathering evidence. As a result the remainder of this section introduces the notion of root cause analysis that motivates many of the techniques that we shall introduce in subsequent chapters. This is justified by the observation that any secondary investigation must uncover sufficient evidence to identify there root causes.

The US Department of Energy argues that investigations must help line management to avoid future failures by identifying the causal factors of previous incidents [208]. This implies that any investigation must detect and remove any local factors that, if corrected, might help to prevent a future failure. Investigatory boards must also identifying and describing any failures in management systems and oversight processes that allow hazards to exist:

> "Modern accident investigation theory indicates that generally the root causes of accidents are found in management system failures, not in the most directly related causal factor(s) in terms of time, location, and place. Generally, the higher the level in the management and oversight chain at which a root cause is found, the broader the scope of the activities that the root cause can affect. Because these higher-level root causes, if not corrected, have the largest potential to cause other accidents, it is incumbent on a board to ensure that the investigation is not ended until the root causes are identified. If a board cannot identify root causes, this should be stated clearly in the investigation report, along with an explanation." [208]

A key question that emerges from this analysis is; what exactly is a root cause and how does it differ from other contributory causes? Not only is this subject of considerable practical significance for incident investigators but it has also been the focus of philosophical debate for many years. Brevity prevents a thorough explanation of the various positions within this debate but it is worth reviewing two different stand-points because they have been used to guide a number of different incident and accident investigation techniques. The first of these philosophical approaches to causation was initially stated by Hume [378] and then developed by David Lewis [490, 491]. It has recently been developed into a causal reasoning tool by Peter Ladkin [470, 469], see Chapter 9.3, and hence is introduced in this section. Hume's contribution can be summarised in the following two definitions where objects can refer both to events and to states in a system:

> "...we may define cause to be an object, followed by another, and where all the objects similar to the first are followed by objects similar to the second. Or in other words where, if the first object had not been there, the second never had existed."

These definitions characterise what has become known as *counterfactual* reasoning. The general form of this argument is that if some event had not occurred as it did then the accident would never have occurred. This provides useful leverage because incident investigations must identify those events that we can eliminate to prevent future accidents from occurring. Lewis' contribution was to provide a mathematical model to support counterfactual reasoning; this model lies at the heart of Ladkin's Why-Because Analysis (WBA) that will be discussed in subsequent chapters. Lewis argues that *necessary causal factors* can be distinguished using a particular form of counterfactual argument. If A and B are states or events, then A is a necessary causal factor of B if and only if it is the case that if A had not occurred then B would not have occurred either. Lewis builds on this to consider alternative scenarios in which A did not occur and neither did B. In mathematical terms, he exploits a Kripke structure to define a nearness relationship between possible worlds. This enables us to reason about the nearest possible world in which A and hence B did not occur. All of this would be of only academic interest if it were not for the strong parallels between Lewis' philosophical approach and the activities of secondary incident investigation. For instance, there is a very real sense in which investigators are look for the closest possible world, i.e. the minimal system change, that would prevent an accident from being caused. The importance of the counterfactual approach is also illustrated by the US Air Force's definition of a causal factor:

> "A cause is a deficiency the correction, elimination, or avoidance of which would likely have prevented or mitigated the mishap damage or significant injury." [795]

The second line of theoretical thought on causation stems from Mackie's work on singular causality [508]. This is included within our analysis because Johannes Petersen has recently extended Mackie's work to analyse the ways in which operators respond to incidents and accidents [678]. Mackie argues that a cause (in the singular) is a non-redundant factor which forms part of a more elaborate *causal complex*. It is the conjunction of singular causes within the causal complex that leads to a particular outcome. Crucially, the causal complex is sufficient for the result to occur but it is not necessary. There can be other causal complexes. If any of the necessary causal factors within a causal complex are not present then the effect will not be produced. However, Mackie argues that it is a subjective decision by the investigator if they attempt to identify a single cause within the collection of necessary causes of a causal complex. He goes on to develop the notion of a causal field that describes the normal state of affairs prior to any incident. Investigators try to identify the causes of an incident by looking for disturbances or anomalies within the causal field. This causal field is, therefore, a subjective frame of reference that individuals use when trying to explain what has happened in a particular situation. If a cause does not manifest itself within the causal field then its influence is unlikely to be detected. This is important because Russell points to the uncertainty of any causal analysis that is based on partial observations of 'causal' sequences [717]. He argues that if we see a stone beside a broken window then we can never be absolutely sure that the stone caused the window to break; a bird may have flown into the glass or there may have been an inherent weakness in the material etc. Mackie's work explains this by suggesting that an individual's interpretation of cause depends upon the subjective frame of reference determined by their causal field. As before, this analysis would not be particularly significant if it had not been used to guide the causal analysis of incidents and accidents. For instance, Petersen's work builds on previous studies by Rasmussen [696] and Lind [493] in which they advocated that any analysis of system failure must be grounded on the functional structure of the system because this provides what Mackie describes as the causal field. The notion of a causal field also has strong implications for our previous discussion about the iterative nature of evidence gathering and causal analysis. For example, if an investigator develops an initial view about the causes of an incident then they may restrict their view of the causal field only to those system behaviours that provide evidence about those causes. Several of Mackie's ideas are reflected in the UK Health and Safety Executive's guidance on the incident and accident analysis that support railway safety cases:

> "There is much evidence that major accidents are seldom caused by the single direct action (or failure to act) by an individual. There may be many contributing factors that may not be geographically or managerially close to the accident or incident. There might also be environmental factors arising from or giving rise to physical or work-induced pressures. There is often evidence during an investigation that some of the contributory factors have been observed before in events that have been less serious. Accident and incident investigation procedures need to be sufficiently thorough and comprehensive to ensure that the deep-rooted underlying causes are clearly identified and that actions to rectify problems are carried through effectively. For such arrangements to be adequate under the Regulations, it is essential that incidents that have a potential to endanger people are examined effectively and that those that could lead to more serious consequences are treated with similar rigour to accidents that actually do cause harm." [352]

The idea that accidents and incidents are not caused by single factors has strong parallels with Mackie's causal complexes. The argument that accident and incident investigation must be thorough and comprehensive enough to identify possible causal factors also reflects Mackie's work on causal fields.

There are strong similarities between the work of Lewis and Mackie. However, Lewis' work focuses on more narrowly on necessary causal factors while Mackie's work on causal complexes focuses on conditions that are sufficient for an outcome but which are not necessary. The same effect may be achieved by several other causal complexes. This difference has profound practical implications. Lewis suggests that it is possible to avoid incidents by blocking the necessary and sufficient causes of failure. Mackie suggests that the best that we can do is to expand the scope of our causal field to provide a better view of a causal complex. There can, however, be little assurance that the same incident will not recur in ways that we have not been able to predict from our examination of a single causal complex. This debate, therefore, has strong similarities with the different positions adopted by Sagan and Perrow. As we have seen in Chapter , Perrow's work on normal accidents suggests that it is impossible to entirely engineer out certain forms of failure that are inherent in complex, tightly coupled systems [677]. In contrast, Sagan's initial position has been to argue that high-reliability organisations can systematically address the causes of failure in complex, technological systems [719].

Part of the motivation for introducing this theoretical material has been to try to clarify the underlying distinctions that often become lost in the plethora of competing definitions that have been proposed for everyday terms such as 'root cause' or 'contributory factor'. It is also important to stress that many incident investigators introduce further distinctions that build on, or arguably confuse, the concepts introduced by Lewis and Mackie. For example, the US Department of Energy introduces the concept of direct causes [208]. A direct cause is the immediate events or conditions that led to the accident. An example might be the contact between the chisel bit of the air-powered jackhammer and the 13.2 kV energised electrical cable in a sump pit that is being excavated. The US Department of Energy argues that "while it may not be necessary to identify the direct cause in order to complete the causal factors analysis, the direct cause should be identified when it facilitates understanding why the accident occurred or when it is useful in developing lessons learned from the accident" [208]. This notion of directness is a recurrent theme in many investigatory handbooks and manuals. It is also often referred to in the distinction between proximal and distal causes [486]. However, it can be difficult to explain this notion of directness in terms of the models developed by Lewis and Mackie. In some respects these proximal, direct causes are both necessary and sufficient. Using a counterfactual argument, if the chisel bit had not hit the 13.2 kV energised electrical cable then the accident would not have occurred. However, a counterfactual argument at this level provides few insights for the secondary analysis of an adverse occurrence. It can also be argued that from the point of view of the outcome, a direct cause is sufficient but not necessary. There may be a number of other direct causes for the resulting shock that was delivered to the jackhammer operator. In order to account for such paradoxes, several authors have introduced a distinction between general and singular causality [678]. Singular causality refers to relations between the particular set of events that were observed during an incident. In the case of the Department of Energy example, the direct causes were singularly necessary and sufficient for that particular adverse occurrence. General causality refers to relations between more abstract types of events that could lead to several different instances of the same failure. In the previous example, the direct causes of the particular failure were sufficient for the incident to occur but were not necessary in terms of the general outcome. There may have been several different ways in which the accident could have occurred. Clearly, incident investigation must focus on general causality if it is to prevent the outcome from recurring. Experience shows, however, that many accidents occur because safety managers focussed on the singular causes of particular failures [702].

Secondary analysis, typically, proceeds by the iterative formation and validation of various hypotheses about the causes of an incident. This validation, in turn, depends upon gathering evidence that is then used to reconstruct the events leading to an adverse occurrence. Three classes of causal factors can be identified amongst these 'events':

- *Contextual Factors: neither necessary not sufficient.* Contextual factors are events or conditions that did not directly contribute to an incident. There are many reasons why these events are considered during an incident investigation and why they can be included in the synopses that often support final reports about the causes of an incident. Firstly, they help to set the scene and establish the context in which an adverse occurrence took place. Secondly, they can help to establish that certain factors were NOT significant in the events leading to failure. For instance, incident reports often state that meteorological conditions were favourable. Adverse weather conditions might then be excluded as potential causal factors. Thirdly, although contextual factors may not have contributed to the particular view of an incident, they may play a more active role within a general analysis of alternative causes of an incident. For example, the fact that a platform was wet may not have contributed to a particular fall, however, it remains a potential cause of future slips.

- *Contributory Factors: necessary but not sufficient.* Contributory factors are events or conditions that collectively increase the likelihood of an accident but that individually would not lead to an adverse occurrence. These are the 'banal factors' in Reason's observation that "... a detailed examination of the causes of these accidents reveals the insidious concatenation of often relatively banal factors, hardly significant in themselves, but devastating in their combination" [701]. Contributing causes can be thought of as latent conditions that, alone, are insufficient to cause a failure but which were necessary for it to occur. For example, disabling a necessary protection mechanism can create the potential for a triggering event to have more serious consequences. Similarly, the failure to erect barriers or to post warning signs can contribute to an adverse occurrence. It is important not to underestimate the importance of these contributory factors as they often have the greatest general significance for future failures. It may be difficult or impossible to predict all of the catalytic events that can lead to a failure. However, the consequences can be reduced by ensuring that contributory factors are adequately dealt with in the aftermath of an incident.

- *Root Cause: necessary and sufficient.* Root causes capture Lewis' notion of causation established by counterfactual reasoning. If a root cause had not occurred in the singular causes of an incident then the incident would not have occurred. If a root causes were corrected then that the same incident would not recurr. However, as noted above, we can also introduce the stronger notion of a general root cause. These are causes that represent the globally necessary and sufficient causes that go beyond the immediate direct causes of an incident, as defined by the US Department of Energy. It is important also to emphasise that root causes can be formed from several contributing causes. This captures part of Mackie's vision of a causal complex. They are higher-order, fundamental causal factors that address classes of deficiencies, rather than single problems or faults. For example, the HSE stress that:

  > "In these criteria the term 'root causes' includes consideration of management's real and perceived messages to workers, environmental and human factors, as well as plant failures and inadequate procedures. Human errors arising from poor operating conditions, procedures, management expectations or plant design are not root causes; the predisposing factors are." [352]

  The root causes of an incident might, therefore, include the failure to implement a safety management system. Individual contributory causes might then involve failures to: define clear roles and responsibilities for safety; ensure that staff are competent to perform their responsibilities; ensure that resource use is balanced to meet critical mission and safety goals; ensure that safety standards and requirements are known and applied to work activities; ensure that hazard controls are tailored to the work being performed; ensure that work is properly reviewed and authorised [208].

It is important to notice that the 'exacerbating factors' introduced in Chapter 8.3 does not fit naturally within these distinctions. Having raised this caveat, it is important to note the significance of the final point in this list, which focusses on managerial root causes. Safety-critical systems are, typically, designed with defences that are based upon the premise of causal independence. In order for an accident to occur any technical failure or human error involving a production systems would have to 'circumvent' the available automated protection systems. It would also have to breach the numerous physical barriers that are usually erected to protect personnel and equipment. However, the managerial root causes of many incidents often conspire to overcome these 'independent' defences.

As Reason notes, the Bhopal disaster showed that "three supposedly independent defences failed simultaneously: a flare tower to burn off the deadly methocyanate gas; a scrubber to clean air emissions and a water sprinkler system to neutralise the remaining fumes" [702].

7.1.2 Commissioning Expert Witnesses

The previous sections has argued that the scope of a secondary investigation is defined by an iterative process in which investigators form hypotheses about the root causes of an incident. These hypotheses are then validated by gathering relevant evidence. However, this evidence may reveal inconsistencies that force the investigator to revise their initial hypotheses. They must then, in turn, seek further evidence to validate their new ideas about the causes of an incident.

Chapter 5.4 introduced some of the problems of evidence gathering that effect the initial investigation of an adverse occurrence. Many of these problems, such as the difficulty of gathering and interpreting eye witness statements, also affect subsequent enquiries by trained investigators. Other problems stem from the iterative process of formatting and validating hypotheses. For instance, previous chapters have introduced the *confirmation bias* that makes individuals more likely to accept evidence that supports a hypothesis. It also makes them more likely to ignore evidence that is inconsistent with their initial views. Other forms of bias effect the secondary analysis of incidents by individuals working within the organisations that are under investigation. For example, attribution errors occur because individuals are more likely to attribute the causes of failure to situational aspects if they are potentially implicated in that failure. However, if they are not themselves implicated then they are more likely to look for evidence that others were to blame rather than look for wider contextual factors [121]. It is difficult to avoid what are often implicit biases. Investigators may not be aware that such factors influence their behaviour. These biases are often exacerbated by their omission from many of the courses that are intended to train incident investigators.

Further problems complicate the secondary investigation of adverse occurrences. For example, the primary recipient of an incident report usually does not have time to call for specialist reports in the immediate aftermath of an adverse occurrence. However, expert witnesses are often solicited after a preliminary report has been published. In most cases, these witnesses help to mitigate the biases mentioned above. Attribution errors can be addressed because expert witnesses may take an independent view of the investigatory agencies role in any incident. Confirmation biases are resolved because expert witnesses can use their experience to look beyond the initial hypotheses being proposed by incident investigators. Of course, a more cynical view is that these sources of additional evidence may do little more than to bolster or confirm these preliminary judgements about the causes of an incident [412]. Such cynicism contrasts sharply with the guidelines that determine the role of expert witnesses within boards of inquiry:

> "Expert witnesses also may be called to testify on selected topics to assist the Chemical Safety and Hazard Investigation Board in its investigation. The testimony is intended to expand a public record and to assure the public that a complete, open objective investigation is being conducted. The witnesses who are called to testify have been selected because of their ability to provide the best available information on the issues related to the chemical incident, or who had direct knowledge of the events leading up to the incident." [161]

This quotation stresses the positive role of expert witnesses in helping to determine the causes of incidents and accidents. However, things are not always so clear cut. For instance, the evidence of one group of experts can often be rebutted by evidence from their colleagues. As a result, regulatory organisations often publish explicit advice about the role of scientific evidence in safety assessments and risk analysis. For example, the UK Health and Safety Executive have considered this issue in a number of recent studies [332]. Although the remit of these enquiried has extended well beyond the scope of secondary incident investigation, some of the interim findings are applicable within this context:

> "Identify trusted, independent parties who your audience are likely to turn to for

> advice, or from whom they will form their opinions. Get them on board early. Conflict among experts will always damage credibility." [330]

If such advice is not heeded then the consequences for any incident investigation can be profound. Any subsequent litigation will be reduced to a dispute between the relative credibility of expert witnesses. In such circumstances, courts rule on the weight of the scientific and technical evidence that is presented to them. They must assess the credibility of expert evidence.

> "The administrative law judge who heard the case decided that Dr. Hochman's 'opinion is entitled to considerable weight'; nevertheless, he further decided that the opinion testimony of the Secretary's three experts about breaks before the rope snapped is of 'greater value'." [645]

If outside opinion is to be relied upon, it is therefore essential that incident investigators seek advice from a well qualified source. Most expert witnesses gain a reputation for their work within a particular area of technical expertise. As a result, information about their particular skills is often exchanged by incident investigators who need particular services. However, if investigators cannot find an expert witness through the recommendations of their peers then there are a number of alternative techniques that can be used. For example, some experts advertise their services in trade publications or directly through promotional flyers that are sent to lawyers and investigators. There is an obvious concern to validate the credentials of such individuals. One of the main means of achieving this is to consult the national professional association of the discipline concerned. However, this does not provide a guarantee of competence.

It is important to emphasise that expert witnesses do not simply need to be skilled within their own domain. There is an obvious requirement that they have some understanding of the legal framework that supports their role within a safety system. This is not always as straightforward as it might appear. For example, some aspects of the English and Welsh legal system can appear 'surprising' to potential witnesses:

> "The Royal Commission on Criminal Justice was concerned that because of the rules on hearsay evidence, an expert witness may not, strictly speaking, be permitted to give an opinion in court based on scientific tests run by assistants unless all those assistants are called upon to give supporting evidence in court. It seems to us that this rule is badly in need of change. The Law Commission agrees, and recommends that the prosecution and the defence should give advance notice of the names of anyone who has supplied information on which an expert will rely, and the nature of that information. The expert could then base any opinion or inference on the information supplied by any such person, without the party having to call that person, unless the court directs otherwise on application by any other party to the proceedings. This should result in a reduction in pointless cross-examination of experts' assistants." [477]

It may seem paradoxical to stress this issue again, when many of the reporting systems that we have considered are both voluntary and non-punitive. However, expert witnesses are most typically called to support the analysis of incidents within 'proportionate blame' systems. It is also important to remember that even 'no blame' systems must operate within the law.

Expert witnesses must possess a range of further skills in addition to their domain expertise. They must also be able to explain their insights to the many different groups who can have a stake in the results of an incident investigation. Spohrer and Maciejewski [755] illustrate this point when they stipulate ten commandments for expert witnesses. They focus on the role of expert chemists during litigation. However, their advice is generic. The following guidelines re-interpret them for incident reporting:

1. *Know the proper standard for admissibility of your testimony.* In certain areas, there are standard tests for establishing particular hypotheses. For example, in the United States post-incident examinations of trucks and buses are, typically, based around the Commercial Vehicle Safety Alliance (CVSA) criteria. There are also Office of Motor Carrier (OMC) inspection

guidelines that must be followed by any independent expert. These guidelines provide a set of standards that can be used to determine whether, for example, the brakes on a commercial vehicle were satisfactorily maintained before an incident. In other areas, things are less clear cut. For example, there are several competing theories about the impact of workload on human decision making [864]. As a result, experts may use one of several approaches to determine whether or not this was a factor in a particular incident.

2. *Do your homework.* There is a legal trick which goes as follows. The lawyer asks the expert witness if they agree that some standard text is an authoritative source on a particular topic. If the expert witness agrees then the lawyer takes them carefully through the paragraphs that rebut their evidence. The standard response to this ploy is to claim that no published source can ever be authoritative because by the time that they are published there will usually be more advanced research that could not be included. In consequence, it is important for expert witnesses to keep up to date with recent developments. For instance, the tests mentioned in the previous bullet point have recently been reviewed by the NTSB following a number of incidents in which vehicles brakes failed even though they were OMC certified [609]. Any evidence that is based on the OMC certification would have to be re-interpreted in the light of this NTSB study.

3. *Always maintain your "cool" during a deposition and at trial.* This commandment relates narrowly to the role of the expert witness within litigation and so it more difficulty to apply more generally in the secondary analysis of safety-critical incidents. However, Spohrer and Maciejewski introduce a number of important pitfalls that witnesses should be aware of [755]. For instance, they warn against the negative effects of cross-examinations that include questions such as "Have you stopped beating your wife?". These 'no-win' questions could be phrased as "Dr. Engineer, is your company still manufacturing these defective widgets?" or "Doctor, are you still performing this discredited surgical procedure?". Spohrer and Maciejewski procedure recommend that experts should never give a 'yes' or 'no' answer to such questions but should use the opportunity to restate their opinion. For instance, "I disagree with your assumption. Our widgets are among the safest in the marketplace and have been used by millions of customers without an incident..."

4. *Be an expert, not a "hired gun".* The Chemical Safety and Hazard Investigation Board's terms of reference for expert witnesses, cited above, emphasised that they are intended to convince the public that an investigation is 'complete', 'open' and 'objective' [161]. In other words, they must not simply support the existing hypotheses proposed by an investigator. Fortunately, it is relatively common to find experts who are willing to act in this independent manner. For instance, the following excerpt comes from a US Coast Guard judgement in which even the government's expert witnesses agreed with the appellant:

   > "The only testimony to be found in the record on this issue is favorable to Appellant. The sole expert witness to testify stated that he approved of Appellant's decision (Tr. 194-195). The Marine Superintendent for Ecological Shipping Corp., called by the government, testified on cross examination that he thought Appellant had made the right choice (Tr. 124-126)." [826]

   It is also important to emphasise the any initial discussions between an expert witness and an incident investigator must consider the ways in which they are to be paid for their work. It is clearly unethical to make such payments contingent on the outcome of any analysis.

5. *Request a thorough briefing.* Incident investigators must provide expert witnesses with information about the general scope of an investigation. In particular, they must provide experts with access to any necessary data. It is also important that investigators explain their reasons for engaging the services of an expert witness. The expert, in turn, must determine whether they are able to provide the evidence that is expected by the investigator.

6. *Know when and when not to 'blow your own horn'.* It is important for experts to provide the information that establishes their credibility. For instance, the following quotation comes from an NTSB investigation into a non-fatal aviation incident. Although the information seems very plausible, it is impossible to know the basis of this analysis from the report alone:

   > "According to an expert on the Long-EZ, following a loss of engine power, you must maintain flying airspeed just like a regular airplane, otherwise the canard will stall. When the canard stalls the aircraft's nose will drop 10 to 30 degrees. After the canard stalls, if the control stick is kept fully aft and flying airspeed is regained, the nose of the aircraft will rise." [597]

   It would have been far better to state the level of expertise that backs such an assessment. This does not necessarily imply that every expert ought to be named even in minor incident reports, although this is good practice. In this case, it might have been sufficient to state the number of hours that the expert had completed on this type of aircraft.

7. *Don't guess or go out on a limb.* It is important for expert witnesses to remember that some questions defy simplistic answers. In particular, many investigations rely upon evidence derived from tests that do not provide definitive answers. The majority of scientific test provide results that are based on confidence intervals. This is illustrated by the US Occupational Safety and Health Administration's (OSHA) use of expert witnesses in assessing the risks of exposure to 1,3-Butadiene (BD). The witnesses provided the following analysis:

   > "In the Downs study (Ex. 34-4, Vol. III, H-2) the standardised mortality ratio (SMR) for all causes of death in the entire study cohort was low (SMR 80; p ¡ .05) when compared to national population rates. However, a statistically significant excess of deaths was observed for lymphosarcoma and reticulum cell sarcoma combined (SMR 235; 95(The issue of reference population selection is discussed below in paragraph (viii).) When analysed by duration of employment, the SMR for the category of all LH neoplasms was higher in workers with less than five years employment (SMR = 167) than for those with more than five years employment (SMR = 127). However, neither of these findings was statistically significant." [652]

   As can be seen, the experts are carefully to note both the problems of determining a reference population for their epidemiological study. They also state which of their findings were statistically significant and which were not.

8. *Don't talk down to the investigator or other colleagues in the investigation.* It is important to note the language that was used by the experts that are cited above. This excerpt assumes that the readers can correctly interpret the use of statistics and will be aware of some of the control issues involved in such a study. The tone is of one scientist or engineer talking to another. Although the previous citation does not show them, it also included numerous footnotes so that additional details could be obtained if the reader failed to understand some of the points that were being made. However, such references in turn assume a certain technical background and scientific expertise. This is completely appropriate given the nature of the report. However, considerable additional care is required when expert witnesses must communicate their findings to groups without more diverse backgrounds. Chapter 13.5 will introduce a range of techniques that are intended to address these communications issues.

9. *Don't try to be an expert on everything.* It is important that expert witnesses know the limits or bounds of their expertise. Investigators are, typically, aware of the limitations in their own expertise. This often a primary reason for the use of expert witnesses. It is also illustrated by the way in which many investigatory agencies deliberately partition the skills that they require into a number of specialist areas. Staff develop skills in a subset of those areas. For instance, the Federal Railroad Administration employs railroad inspectors who investigate possible breaches of Federal laws, regulations, rules and standards and to conduct and report on incidents or accidents.

> "The Inspector writes reports of findings and seeks correction of unsafe conditions and may be called upon to testify as an expert witness in civil suits. The demands of these jobs are many, requiring skill in evaluation, fact-finding, report writing; comprehension and application of technical and regulatory standards; the ability to gain the cooperation of individuals and organisations; and knowledge of methods used in installation, operation, maintenance or manufacturing of railroad equipment and systems." [238]

As a result, inspectors are groups around a number of specialisations including track inspectors; motive power and equipment inspectors; hazardous materials inspectors; operating practices inspectors. As can be seen, each of these divisions carefully defines the scope of expertise for each of these 'professional expert witnesses'. It is important that a similar degree of care is taken when recruiting free-lance expert witnesses.

10. *Never sacrifice your credibility.* This might seem like little more than common sense. However, it is instructive to spend a little time reviewing the way in which a court treats expert testimony during subsequent litigation about the course of an incident. For example, the following excerpt comes from the OSHA review Commission's judgement on an appeal against a decision that went in favour of the US Secretary of Labour and against the expert opinion:

> "Keco's argument against classifying its facility as a 'blast-cleaning room' is based primarily on the opinion testimony of its expert witness, Nicholas Corbo. We conclude, however, that that testimony is entitled to little weight... In essence, therefore, Mr. Corbo concluded that Keco's facility was not a 'blast-cleaning room' because it did not have a forced-draft ventilation system. This is not, however, how the standard defines the term. The definition in section 1910.94(a)(1)(iv) says nothing about a forced-draft ventilation system. The standard's definition is controlling here. Moreover, adopting Mr. Corbo's definition would create an absurdity in the standard. Section 1910.94(a)(3)(i) sets forth a requirement that '[b]last-cleaning enclosures [including blast-cleaning rooms] shall be exhaust ventilated in such a way that a continuous inward flow of air will be maintained at all openings in the enclosure during the blasting operation'. Yet, this standard would be rendered inapplicable to the unventilated enclosures it forbids if we were to define 'blast-cleaning enclosures' as ventilated enclosures." [646]

Such decisions illustrate the consequences when expert witnesses lose their credibility either through a failure to apply the relevant standard or through apparent contradictions within the arguments that they present.

It is possible to add a further requirement that all expert witnesses should "keep a written record of the supporting analysis that helped in forming particular conclusions". Without this information it is impossible both to assess the validity of the witnesses conclusions or to replicate their method. This is a particular problem for the human factors analyses that frequently form part of the secondary investigation of an adverse occurrence [410]. For example, the following excerpt emphasizes the problems that high workload can create for aircrews during adverse situations. Here the term is used colloquially even though there are many more technical definitions of the concept [864]

> "There can be little doubt, however, that the high workload in the cockpit contributed to the failure of the crew to notice the abnormally high reading on the No 1 engine vibration indicator that was evident for nearly four minutes after the initial vibration. It is, therefore, recommended that the CAA should review the current guidance to air traffic controllers on the subject of offering a discrete RT frequency to the commander of a public transport aircraft in an emergency situation, with a view towards assessing the merits of positively offering this important option." [8]

In contrast, the following excerpt from a far less severe incident illustrates how expert evidence can be backed-up with information about the reconstruction techniques that support particular conclusions. Here the pilot's workload was assessed in terms of direct observations about what could and what could not be seen in a similar cockpit under similar lighting conditions. Although it is possible to argue with the interpretation of 'workload' that is being used in this incident report, the documentation of supporting evidence does provide the reader with a clear interpretation of what was meant by the human factors analysis in this context:

> "Pilot workload was evaluated whilst flying an AS 355 along a low-level route at night in full moonlight conditions. One hour was spent simulating the VFR mode whilst navigating with a half-million topographical chart and stopwatch at between 1,200 and 2,000 feet altitude. This phase also included an assessment of the ground lighting conditions in the accident area. A further 30 minutes was spent evaluating handling and navigation in the IFR mode at 3,500 feet altitude. The following observations were noted. The flight instruments were well lit, although a variety of lighting installations exist and no comparison was possible with the accident aircraft. The cabin dome lighting was too weak for easy chart reading. (The primary function of these lights is to provide back-up illumination of the flight instruments; they were not intended for use as chart reading lights). When dimmed the dome lights had a yellow tint and the yellow coloured towns on a 1:500,000 topographical chart could not be easily identified. Minor terrain features on the chart, depicted in yellow, could not be seen in flight due to the yellow tinted light. The cabin dome light eyeball could be vectored far enough forward to shine on the pilot's left knee..." [13]

The key point here is that without such supporting information about the analytical methods that scientific and technical experts use during the secondary stages of an incident investigation then it is highly likely that their findings may be questioned during the later stages of analysis. In the worst case, their results may stand until they are examined during subsequent litigation. Without necessary information about the method and scope of the expert's techniques then it is highly likely that their insights will be discredited or rebutted by the evidence of other, equally qualified, professionals.

7.1.3 Replaying Automated Logs

Chapter 5.4 introduced the problems that arise when attempting to safeguard the automated logs that are increasingly being used as evidence in the subsequent investigation of adverse occurrences. This section builds on the previous introduction and goes on to consider the use of these data sources to yield important insights into the causes of near miss incidents.

It is important to emphasise that the use of data recorders to support incident investigation is not a new phenomena. The maritime industry has for a long time exploited log books, navigation charts, bell and engine order logs, course recorders and hull stress meters. However, these traditional sources of information are being supplemented by more recent developments. These include propulsion and auxiliary engine computer logs, vessel traffic service systems, Rescue Coordination Center radio transmission tapes and Automatic Identification System logs [114]. As mentioned in Chapter 5.4, this creates logistical problems for the primary recipients of an incident report. They must safeguard these diverse information sources and coordinate their collection for later analysis. Fortunately, a range of marine voyage data recorders have been developed to collate the various measurements that can be taken on board a vessel. These systems also ensure that they are recorded and protected in one data store so that they can be retrieved for later analysis. As Brown notes, the usefulness of these systems goes beyond their role in incident investigation; " Many companies have already taken the initiative of installing Voyage Data Recorders (VDRs) not only to obtain data in the event of an accident or incident, but also to assist in managing their fleets" [114]. The following paragraphs summarise the benefits of automated logging systems. Particular emphasis is placed on their role in incident investigation, however, we also consider some of the wider benefits that these logging systems can provide.

Most automated logging systems are introduced to provide investigators with the data that is necessary during the subsequent reconstruction of adverse occurrences. These devices were initially deployed to support air accident investigations. However, they have since been installed in a wide, and ever expanding, range og safety-critical systems. For instance, tachographs are now routinely used during the investigation of road traffic incidents:

> "(Vehicles) with the electronic tachograph capability graphically show simultaneous engine and vehicle speed, and show how a vehicle was driven for a 24-hour period. This function identifies driver compliance with speed limit changes along routes. It also profiles basic driving habits. For example, if the graph shows that the vehicles speed decreased suddenly but the engine speed did not, the driver may have been tailgating and had to slam on the brakes to avoid an accident." [216]

Information from such sources is not simply used to analyse human and system performance immediately before an incident. Records can also be kept to determine whether or not there is evidence of similar failures over a much longer period of time. They can also be used more pro-actively. For example, tachograph records can be used to trigger US Department of Transport violation reports if drivers exceed certain operational limits [216].

As mentioned, automated logging systems have a number of uses. Not only do they record information about system performance during potential failures, many of the applications also provide live output that can be monitored. This provides potential rescuers with direct information about the events that contribute to an incident:

> "Current generation recorders now permit a watchman monitoring distress channels to instantly play back a distress call without interrupting the recording process, even as additional voice or data signals are received. Weak, unintelligible signals can be enhanced and amplified by signal processing. This allows search and rescue workers to save lives that might otherwise be lost. Tapeless magneto-optical drive systems provide immediate playback of data when there is uncertainty concerning the exact message that was received or transmitted." [223]

This illustrates how automated logging equipment can support secondary investigations long before the analysis actually begins. By providing potential eye-witnesses with important and accurate information about the the state of an application, these systems can help observers to more accurately recall the events leading to a failure. Arguably the most obvious use of automated logging systems is to validate the testimonies of people who are involved in an incident. The following excerpt cites an NTSB summary of cases in which rail recording systems were either available to validate the crew's interpretation of events or were unavailable and the subsequent investigation had to rely on witness testimony alone. Chapter 5.4 has summarised the many biases that complicate the task of interpreting such evidence derived from those who are involved in an incident:

> "After reviewing the information from the trains event recorders the Safety Board investigators determined that the St. Louis Southwestern Railway Company (Cotton Belt) was lax in enforcing speed restrictions. In the investigation of a 1985 head-on collision between two Amtrak trains at Astoria, Queens, New York, Safety Board investigators performed a comparative analysis of the data from the recorders. The recorded train operator activity data was compared to crewmember statements for cab signal indications and applicable wayside signal indications to develop findings in the investigation... The investigation of a 1989 derailment with the release of hazardous materials from a freight train near Freeland, Michigan was noted as being hindered by the absence of multi-event-recorder data. The Safety Boards report stated that train-handling information was derived from what the train crew stated. The paper-tape-recorded train speed was of limited usefulness since the manner in which the train was controlled was more important than its speed. Vital information, such as quantified braking, throttle manipulation, and the chronological relationship between power-to-braking and braking-to-power, was not available". [215]

It is important not to underestimate the practical difficulties that are involved in using automated logs to validate eye-witness testimonies. As the previous citation shows, these systems do not always provide the evidence that is necessary to prove or disprove key aspects of their statements. Simply recording more data does not always provide straightforward solution. Later sections will identify some of the problems that can arise in both filtering and in interpreting the mass of data that these systems can record. You may be able to determine that the operator did issue a particular command at a particular moment in time, but no logging system will currently tell you why that command was selected.

The positive side of automated logging focuses on the use of these records to encourage future improvements in operator performance and system reliability. This provides another aspect to the way in which some organisations blur the distinction between a safety-critical incident reporting system and a more general approach to quality improvement:

> "The Navy uses recording devices as training tools to improve air traffic control operations for both ship and shore-based facilities. Operators are given the opportunity to hear themselves and see the consequences of their actions in replicated scenarios. This enhances readiness by allowing total system simulation, and by providing both individual and team training. Managers and commanders can better measure readiness, identify whether proper operational procedures are being used, and evaluate the outcome of using those procedures. Recorders offer the opportunity for students to safely learn from their mistakes in an unbiased, objective mode."[223]

The same techniques of replay and simulation that are described in this citation can also be used more directly to support the secondary investigation of an incident. Showing automated logs to an operator or eye-witness can trigger recollections that might otherwise not form part of their testimony. There is, however, a danger that such an approach may evoke a form of false memory syndrome. This is particularly apparent when the automated logs are presented through sophisticated, three-dimensional simulations. For this reason, several organisations have moved to limit the use of such reconstruction techniques during some stages of incident investigation [423]. Witnesses should only be shown replays on the equipment that they actually had available to them during the incident itself. It can be argued that this is an unnecessary restriction. Further work is urgently needed to determine whether these are valid concerns during the subsequent investigation of an adverse occurrence. However, there is often a justifiable fear that automated logging systems will not primarily be used as a safety tool. Instead they will be used to monitor employee compliance with organisational objectives and performance criteria. Later sections will describe how many automated monitoring systems are deliberately developed so that they can be customised to the requirements of the companys that buy them. The previous positive comments about the use of these systems must, therefore, be balanced against their more sinister application:

> "Competent personnel love them, while incompetent personnel loathe them. What better documentation for management to have in an incident than an exact record of actions that were (or were not) taken. Multi-tiered security systems embedded in the design of todays naval recorders prevent unauthorised access to the recorded information, thus preserving the integrity of the data for use in accident investigations or analyses. Additional features prevent the overwriting of data previously recorded on another machine. Modern recorders can also be synchronised to a universal time standard such as global positioning system (e.g., Havequick time). This allows platform-unique data to be recorded and played back in synchronisation with recording systems in other locations, thereby improving time-sensitive accident investigations." [223]

The previous paragraphs describe some of the benefits that can be obtained both for the secondary analysis of an adverse occurrence and also more widely in the operation of safety-critical systems. However, all of these benefits depend upon the deployment of the monitoring equipment. Typically, in spite of the claimed commercial benefits, there systems are not widely used unless they are backed by regulatory requirements. There are notable exceptions, however as usual, these tend to be companies that already have a high reputation for their safety management systems. The problems that arise when attempting to introduce reporting systems can be illustrated by the complex negotiations within the International Maritime Organisation (IMO). The 44th session of the IMO Sub-Committee on Safety of Navigation considered the adoption of Voyage Data Recorders (VDR). Several options were considered during this meeting:

> "The proposed options include a provision limiting the new requirement for VDRs to Ro-Ro (roll on-roll off) passenger ships on international voyages. Other options, which were submitted by the United Kingdom and supported by the European community, the United States, Canada, Australia, and New Zealand, require that all new vessels built by a certain date have a VDR and that all existing vessels install a VDR during a phase-in period, which will be at a later date... Some countries opposed the VDR requirement for all vessels. Japan and others stated that the carriage requirement should apply only to vessels on international voyages; Panama maintained that the VDR should only be required on self-propelled vessels." [114]

Coordinating the adoption of automated monitoring equipment is simpler when a single national regulator has jurisdiction over an industry. However, regulators must still address the problems of gaining employee trust and of convincing industry that such systems are not an unnecessary burden. Even once automated logging systems are widely deployed, a host of further problems complicate their use within the secondary investigation of adverse occurrences. These problems range from design limitations through to installation issues and the difficulty of maintaining often complex digital equipment in potentially 'hostile' environments:

> "There are no (Federal Railroad Administration) requirements for records to be kept about recorder system specifications, or applicable readout software... While a readout of the data is required every 92 days for tape-based recorders only, there is no requirement (for any type of recorder) to test the sensors or other system components or to verify that accurate data is actually being recorded. Furthermore, under current FRA regulations, microprocessor based recorders are not required to be readout, tested, or examined unless the recorder itself indicates a fault from its self-diagnostic test... (These tests) detect the presence of certain sensors, they cannot test the validity of the signals coming from the sensors. If an errant axle generator continuously sends a signal representing 0 mph, the self-test feature will not detect a malfunction. Failures such as this one may never be detected, because there are no requirements to ever read out, test, or evaluate this type of recorder. Additionally, self-test features can not detect improper programming or set-up of the recording system." [215]

The following list builds on this analysis and identifies a number of more detailed barriers to the effective use of automated logs in the secondary analysis of adverse occurrences. A common thread running through each of these items is that the installation of particular devices and the protection of their data in the aftermath of an incident do not provide any guarantee that reliable information will be obtained about the causes of failure.

Automated recording devices may simply fail to operate. In some ways this simplifies the investigators task because they do not have to piece together partially corrupted data. On the other hand, they are left to determine the reasons why such critical equipment was not being operated. Chapter 5.4 provided a number of examples in which data recorders were either sabotaged. It also described some comparatively rare incidents in which equipment was lost as the result of extreme forces in the aftermath of an incident or accident. The failure of most data recorders, however, often stems from more complex causes:

> "During normal operation of the system, when aircraft power was applied, the tape transport would run for 1 minute without recording data to enable different flight sectors to be separated upon replay. The system would then enter standby mode with no tape motion and the mechanical indicator on the control panel indicating 'STBY'. Once the crew had started both engines, as part of the startup procedure, they would select the aircraft generators to 'ON'. This action would switch the tape transport on, initiating the recording of data and setting the control panel indicator to 'RUN'. From this point a further 2 minute period was required to allow the Built-In Test Equipment (BITE)

> to detect and indicate a system fault. A later item in the checklist required the crew to ensure that the control panel mechanical indicator was showing 'RUN' and that the BITE fault indication was extinguished. A fault in the track change sensing of the tape transport of G-ATMI's recorder had allowed the tape to run off the end of one reel, become stuck to the tape drive capstan and then wind backwards around the capstan until it had jammed. Following the engine starts, prior to the accident take-off, the crew had selected the generators to 'ON', thus setting the FDR system to 'RUN'. However, the CVR recording showed that the checklist item to ensure normal operation of the FDR system had been carried out within 1 minute of switching the generators, which did not allow sufficient time for the system BITE to detect and indicate the fault in the tape transport. The position of the control panel on the flight deck was such that neither crew member would have been able to see the fault indication without turning to look over their shoulder." [17]"

The previous quotation illustrates the care with which incident investigators must investigate the sources of such failures. Although automated logging systems do not directly contribute to the causes of an adverse occurrence, their failure jeopardises the investigators ability to accurately identify those causes.

There are many ways in which automated recording equipment can fail to provide necessary information about the course of an incident. As we have seen, the design of the equipment may not record all of the parameters that are necessary during any subsequent investigation. Such problems are being addressed by the development of an increasingly sophisticated range of digital recording devices. There are also a number of common technological problems that can affect the analysis of flight data recorders. For example, many recorders fail to deal adequately with information that is buffered in a volatile store immediately prior to any adverse occurrence:

> "The Universal Flight Data Recorder (UFDR) takes flight data into one of two internal memory stores, each holding about one second of data. When one memory store is full, the data flow is switched to the other store. While the data is being fed to this other store, the tape is rewound and the previous second of data is checked. A gap is left on the tape and the data in the first store is then written to the tape, and the first memory store emptied. This whole 'checkstroke' operation takes much less than one second to complete... Thus the UFDR tape is not running continuously. The tape first accelerates from stationary to 6 inches per second to read the previous data block, leaves an inter-record gap and then writes the new data block. The tape then slows and rewinds ready to begin the next 'checkstroke' operation. A total of 0.48 inches of tape is used to record one block of data and inter-record gap... When power is lost from the recorder, the data held in the volatile memory which has not been recorded on the tape is lost. As can be seen from the way in which data is temporarily stored on this UFDR and then recorded, this can mean that up to 1.2 seconds of data may be lost just before impact." [8]

The AAIB continue to report similar problems. For instance, the buffering of data by a digital flight data recorder led to significant problems for the investigators of a recent loss of control incident [18]. The data buffer was not crash protected and required electrical power to retain the contents. When it was replayed, it was also found that the recorder had an undetected fault which resulted in the random corruption of all parameters over the duration of the recording. The recorder's built-in test circuitry was incapable of warning the operators about the presence of this particular fault.

Secondary investigations must make the best use of data that is provided by automated monitoring equipment. However, experience with failures in this equipment varies considerably from industry to industry. The previous problems noted with flight data recorders do not seem to have been such a concern in the railway industry. For example, the following citation describes the NTSB's experience with these systems:

> "The actual recording device itself is seldom, if ever, at fault. In fact, none of the microprocessor recorders that the NTSB has had tested thus far has ever been found to have failed, be out of tolerance, or to have malfunctioned." [215]

In contrast, most problems seem to arise from the data supplied to the recording device. Anomalous or missing data often results from inoperative, incorrectly installed, or out-of-calibration sensors. Many of the NTSB's concerns about this class of recording system focus upon the quality of maintenance that these devices receive.

> "The event recorders maintenance and its location within a locomotive were addressed in the Safety Boards report of the 1996 freight train derailment near Cajon, California. The post-accident testing of the microprocessor type of event recorder showed that one event recorder had a broken wire in the axle generator, as a result of an improper modification, and that another was improperly programmed. In addition, the self-diagnostic indicators were insufficient to fully examine the recording status of the units. The pre-accident inspections had been inadequate." [215]

Such concerns have complex organisational and regulatory causes. It is unclear whether substandard maintenance and inspection stem from a perception that these devices are not 'essential' for the actual operation of the railroad. It could also be argued that maintenance problems also stem from the inherent complexity of the monitoring devices and the relatively fragile nature of some sensors. Alternatively, better self-test functions could provide operators with a clearer indication that equipment is not functioning as intended. Further work is urgently required to resolve some of these outstanding issues.

Current generations of automated data recorders offer great flexibility. For example, in the rail and maritime industries it is possible to configure or progam these devices to monitor and record information about events that are of specific interests to the companies that operate them. In aviation this has led to the growth of Flight Data Monitoring (FDM) and Flight Operational Quality Assurance (FOQA) programs. The growth in the scale and complexity of the devices that support these initiatives can be illustrated by the increasing number of parameters that are simultaneously recorded. The first generation systems read from 5 to 30 parameters from metal foil storage. More recent versions of what have become known as Quick Access Recorders, to distinguish them from accident recorders, now sample from 200-300 parameters [92]. It is hard to underestimate the technical challenges that these systems can pose. As mentioned, microprocessor recording systems are typically configured to meet the customers specific requirements. As a result, it is likely that one operators requirements will be different form anothers. Additional problems arise because an individual operator can change their own requirements over time. Recorder manufacturers also update and revise system configurations as new technology is introduced. Incorrect setup or programming can lead to certain parameters being recorded incorrectly or not being recorded at all [215].

Problems can still arise even if sensor signals are reliably received by a recording system and the system is correctly configured to receive those signals. In particular, a significant amount of incident data has been lost in recent years by improper or incorrect handling procedures while the data is being prepared for analysis. These handling problems take a variety of forms. For example, recording media have been placed too close to strong electro-magnetic sources. They have also been placed in direct sunlight and even accidentally immersed in water so that even relatively resilient housings have been compromised after the equipment has been removed from the system that is being monitored. Further problems have arisen during the process of transferring data from a primary recording medium to a secondary or back-up source:

> "When the copy tape was first replayed it yielded 60% bad data, making analysis of the readout difficult, and it was not possible to determine whether this data contained the landing. This copy tape was then replayed by AAIB using both the original Copy Recorder and the AAIB replay facilities, and this yielded 95% good data for the incident. Analysis showed that this data ended when the aircraft touched down, giving incident data for 116 seconds additional to that recovered directly from the Universal Flight Data Recorder (UFDR). The copying process appeared to have repositioned the tape in the UFDR incorrectly after the down load, allowing the final approach data to be overwritten by the engine ground runs." [12]

Fortunately in this incident, the primary source was uncorrupted and the analysis could proceed as planned. However, such incidents reinforce the point that simply gathering and recording data does not guarantee that it will survive in an uncorrupted form until an eventual analysis.

The increasing flexibility and capacity of the recording systems that can support incident analysis also raises further problems for the interpretation of the data that they collect. Increasingly, these problems are being addressed by a range of sophisticated reading tools that provide and visualisation capabilities:

> "The Decision Support System is a uniquely designed relational database system that allows for extraction of information such as what-if and queries of a large number of events stored in the system. FOQA II uses high fidelity visualisation and simulation whenever feasible, to display a situation or an analysis. Visualisation is 3-dimensional. The Visualisation and Simulation can be used to display and replay Allied Signal Enhanced Ground Proximity Warning events using a photo realistic terrain database." [92]

Later sections will consider the use of simulation and visualisation techniques to support incident analysis. For now it is sufficient to realise that different configurations will be required so that any reader can correctly interpret the different configurations of recording devices: As a result; "a recording system installed on a particular operators locomotive requires a readout program that is unique to that operator" [215]. If a similar recording system were to be installed on another operator's rolling stock then there is a good chance that it would require a different readout program. Some rail recorder manufacturer support more then 50 different configurations, each requiring different software to properly extract the data. If a recorder is analysed using an incorrect or outdated reader then it is likely that some of the resulting data will be corrupted.

Chapter 4.3 briefly outlines the benefits of automated logging systems as a means of monitoring performance and, thereby, detecting potential incidents. This chapter also described the personal, social and organisational barriers to the introduction of these devices. Chapter 5.4 went on to identify the problems that occur when primary recipients have to safeguard automated logs in the aftermath of an incident. They must protect systems from deliberate sabotage. They must also prevent the inadvertent damage to logs when there are considerable pressures to resume operation. On looped recording devices, they must intervene ensure that critical data is not over-written. This section has focussed on the challenges that arise once data has been retrieved in the aftermath of an incident. Technical problems in the configuration of sensors, of the recording media or of playback devices can corrupt automated logs. In particular, installation and maintenance problems can reduce the effectiveness of these devices as reliable sources of information about the causal factors behind adverse occurrences .

7.2 Gathering Evidence about Consequences

The previous section argued that these are mutual dependencies between the search for evidence and the formation of causal hypotheses. The search for evidence is often guided by hypotheses about the root causes of an incident. This evidence, in turn, helps to refine preliminary hypotheses. This is only on aspect of the situation that confronts many incident investigators. The previous definitions of contextual factors, contributory factors and root causes looked at the events which occur before an incident. However, evidence about these events can often only be obtained by looking at the events immediately after an adverse occurrence. From the previous argument, this implies that causal hypotheses are effected both by evidence about those events that *contributed* to an incident and by those events that occurred as a consequence of an incident. For example, a recent NTSB report found that metal fractures could only have been caused by a container being loaded on top of a 'foreign object' as it was installed on a railcar. There was no direct evidence of the foreign object but it was argued that such a cause is the only explanation for the consequences that were observed:

> "Investigators found that the cracks discovered in Thrall cars were not related to car age, mileage, service pattern, maintenance, or previous repairs but to stress forces caused by the presence of a foreign object on the floor of these cars. The UP inspections

> of Thrall cars that ultimately prompted EW-161 provide additional evidence of this phenomenon. Further, inspections of 1,653 cars still in service since EW-161 was issued, in December 1997, have resulted in the repairs of 27 Thrall double-stack container cars, all of which had damage due to foreign objects. No evidence suggests that any of the weld failures found by the FRA or during the EW-161 inspections were the result of any other condition or phenomenon. Therefore, the Safety Board concludes that a direct causal relationship exists between the misloading of a loaded container on top of a hard foreign object and the weld failures at the floor shear plate to bulkhead bottom angle on Thrall 125-ton deep-well double-stack cars." [614]

This quotation illustrates many of the complexities that arise during the secondary investigation of adverse occurrences. Firstly, the lack of direct evidence for the foreign object forces the investigator to form and test a number of alternative hypotheses. The report tells us that the cracks were not related to car age, mileage, service pattern, maintenance etc. Although the report does not inform us of the techniques that were used, the reader must assumed that considerable efforts were made to obtain the necessary evidence to eliminate these possible alternatives. We are then left with the hypothesis that a foreign object caused the weld failures. This illustrates another form of causal reasoning which is similar to the counterfactual approach of Lewis. The previous quotation provides an example of a more general form of argument known as 'reductio ad absurdum'. This proceeds by assuming the opposite of the thing that you want to prove. In this case, we assume that the fractures were caused by the age of the car or by mileage. The investigator then looks for evidence to show that it is impossible or irrational to believe these alternative hypotheses. For example, by showing that the car was only three years old or that it had done significantly less miles than other comparable cars. By eliminating all of the alternatives and by proving that it is incorrect to assume otherwise, you indirectly provide support for the thing that you want to establish.

7.2.1 Tracing Immediate and Long-Term Effects

The secondary investigation of the consequences of an incident is not simply intended to gather clues about the root causes of an adverse occurrence. In many cases, this information is used to assess the severity of the incident. Chapters and 1.3 have introduced the problems associated with any estimate of the potential 'cost' of an incident. However, a qualitative estimate of the consequences of an incident can be given by some (qualitative) function of the proximity to a particular event and the losses associated with that event. The severity of an incident is most easily assessed when there are objective physical measures these values. For example, the nearness to a airspace collision can be measured in Cartesian space. The consequent loss associated with that event can be represented by the number of lives that are threatened by such a collision. These criteria were used to calculate that the following incident should be ranked as a category C air proximity violation:

> "Shortly afterwards, the Mentor heard the Air Arrivals controller announcing that he had turned SAB 603 onto 310 degrees and immediately informed him that a British Airways aircraft, callsign BAW 818, was also airborne on a 'Brookmans Park' SID. The two controllers then instructed their respective aircraft to alter heading and noted from their Air Traffic Monitor (ATM) screens that the two aircraft symbols were very close. Subsequent calculations revealed that the minimum separation was 200 feet vertically and 0.16 nm horizontally when the highest aircraft was at 2,400 feet agl. All the flight crews involved in the incident complied fully and correctly with ATC instructions. At the time of the incident, both SAB 603 and BAW 818 were in cloud and none of the crew members in either aircraft saw the other." [15]

This incident is relatively straightforward. The air traffic controllers' who contributed to the incident were almost immediately made aware of the consequences of their actions. This simplifies any secondary investigation because the individuals who are involved in an incident can help to piece together the events both before and after an adverse occurrence. This task is made far more difficult when the individuals and teams that contribute to the causes of an incident, have little or no idea about the impact of their actions. Such incidents are particularly incidious. There is a danger that the groups who contribute to an initial failure will not alter their behaviour unless they are made aware of the consequences of their actions. These sorts of failures are typified by maintenance incidents. Two frequent scenarios reappear in the incident reports that are submitted in many different industries. In the first scenario, engineers fail to correctly reassemble some sub-component that is then placed in service for a prolonged period of time. This component might fail at any time given the presence of some catalytic event. The maintenance problem is only identified during the next scheduled maintenance interval when the original engineer might have incorrectly assembled many other devices [502]. The second scenario is illustrated by the following example. In this incident, maintenance procedures are not completed. As a result, there is a system failure and an accident is only avoided by a number of fortuitous circumstance:

> "Following an indicated loss of oil quantity and subsequently oil pressure on both engines, the crew diverted to Luton Airport; both engines were shut down during the landing roll... The investigation identified the following causal factors: 1.The aircraft was presented for service following Borescope Inspections of both engines which had been signed off as complete in the Aircraft Technical Log although the HP rotor drive covers had not been refitted. 2.During the Borescope Inspections, compliance with the requirements of the Aircraft Maintenance Manual was not achieved in a number of areas, most importantly the HP rotor drive covers were not refitted and ground idle engine runs were not conducted after the inspections. 3.The Operator's Quality Assurance Department had not identified the non-procedural conduct of Borescope Inspections prevalent amongst Company engineers over a significant period of time." [12]

This separation of causes from consequences creates considerable problems for investigators. They must work backwards from the aftermath of an incident to assemble the evidence that will eventually identify and explain the root causes of failure. The following quotation provides a further example in which the causes of an incident are separated from its consequences. In this case, medical staff initially had no idea that a syringe had been filled with the wrong drug. Only 'in retrospect' were they able to test the device and piece together the causal sequence that caused the problem. This example also illustrates how such a separation also creates immediate problems for the staff who must respond to the consequences of any failure:

> "Unknown nurse prepared 'ephedrine' labelled syringe the day before and left in OB operating room for emergency use, as was the usual practice at this hospital. On day of surgery patient had hypotension after spinal, we gave 'ephedrine' syringe and had intermittent unusual responses of severe ectopy, tachydysrhythmia, hyper and hypotension. There was delayed recognition that the 'ephedrine' syringe may have been the problem because patient had some more benign ectopy and tachycardia prior to giving 'ephedrine' and after giving 'ephedrine' the response was intermittent not immediate and lasting. Post op patient had small MI but is in no way impaired and otherwise fine and baby is fine. In retrospect the syringe became suspect and was tested and found to contain epinephrine rather than ephedrine." [756]

It is important to realise the impact that such situations can have upon the individuals who are involved. The nurse may well have realised that they could be implicated in any subsequent investigation. This can create considerable personal distress. An individual sense of guilt can be exacerbated when the staff who are involved in the causes of an incident cannot help to mitigate its consequences [7]. Instead, they must rely upon the skill and knowledge of their colleagues to rectify an adverse situation. Previous chapters have emphasised the complex, systemic causes of failure. It is interesting to note, therefore, that this voluntary, anonymous incident report focuses on the actions of a single nurse. It ignores the managerial and organisation issues surrounding the preparation of a labelled syringe on the day before the procedure. These issues were, however, commented on by a number of anaesthetists who responded to the original incident report. The separation between causes and consequences also raises a number of more complex organisational issues. There can be a delay while investigators attempt to re-establish the causal chain that links the consequences of an incident to its root causes. This creates an interregnum in which organisations can suppress or destroy evidence. They can prepare a legal defence or may even take precipitous action to forestall legal action, such as sacking individual members of staff [702].

The secondary investigation of an incident must monitor and record the consequences of any adversed occurrences. These consequences help to assess the criticality of the event. They can help to identify causal factors. This, in turn, helps investigators to ensure that the individuals, systems and organisations who are involved in a failure are ultimately informed on the consequences of their interaction. However, the investigator's tasks are further exacerbated when the consequences of an incident develop over a prolonged period of time. Air proximity incidents are relatively simple; any consequent loss of separation can be measured relatively quickly after it has occurred. Other incidents are far more complex. In particular, it can be extremely difficult to predict the long term consequences of medical incidents in which quality of life must also be considered:

> "We performed continuous spinal anaesthesia for femoro-crural bypass surgery. During the operation the patient had no pain, but was still able to move her legs... Towards the end of the operation, with regard to postoperative analgesia, we wanted to give intrathecal morphine. But instead of 0,1mg as intended, an overdose of 1,0mg morphine was injected together with another 5 mg of hyperbaric bupivacaine. The error was immediately detected. SpO2 remained at 98% with 4l/min nasal O2. Naloxone 0,08mg IV was given, followed by a continuous infusion (initially 0,2mg /h, then decreased according to clinical symptoms). The patient stayed in the Post-Anaesthesia Care Unit for the next 18 hours. During this time there occurred no respiratory complications. A slight pruritus and a 12 hour amnesia, were the symptoms experienced by the patient. She was informed about the incident and satisfied with the outcome." [756]

The causes of this adverse occurrence were determined 'immediately'. However the consequences required careful monitoring for at least eighteen hours after the event. It is difficult to underemphasise the importance of such incidents for the medical community. Recent recommendations, such as those contained in the Institute of Medicine report [453], make it clear that there must be longer-term monitoring of the clinical outcomes of adverse occurrences. In particular, the point has been made that it may not be possible to predict the long term outcome on the basis of an initial post-operative assessment. Such arguments have also been expended into more general suggestions to expand the scope of clinical monitoring to increase the detection of clinical incidents. Not only must we assess the outcome of adverse occurrences on those patients that we know have suffered from inadequate care but we must also monitor the outcomes for a wider group of patients in order to improve our detection of those incidents.

This section has focussed on the geographical and temporal distances that separate the causes of some incidents from their consequences. It has been argued that this complicates the secondary investigations that must trace the complex relationships between precursors and outcomes. However, the previous examples have illustrated relatively simple cases. There are further pathological incidents in which causal events have occurred years before other organisations have suffered the consequences of failure. For example, the Watford Junction railcrash took place in August of 1996 [350]. The original signaling that was a contributory cause to the accident had been completed and commissioned between May and June 1993. Between November 1994 and the time of the accident, the HMRI made a number of attempts to arrange an inspection of the site without success [421]. The wording of a Railway Signaling Standard (SSP 20) was imprecise. This led to a speed restriction sign being placed in an inappropriate position, which gave confusing information to the train driver. This standard had been drafted and reviewed long before the accident occurred or the signaling was installed. Such a timespan creates incredible problems for secondary investigations. The companies and individuals who contributed to the design, development and maintenance of particular components may no longer be employed to support existing systems. Documentary evidence about those components may only exist in fragmentary form. As the interval between the root causes of an incident and its eventual consequences increases, there is a corresponding increase in the importance of poor safety management and weak regulation as contributory causes. These organisations, in theory, should have had ample time to detect a problem and resolve it before the incident occurred.

This is not as easy as it might seem, especially if regulatory organisations are involved in the initial decisions that create the root causes of an incident. For example, the following citation described how federal authorities partly financed a signaling system that was not ultimately supported by an adequate safety case:

> "The CSX Transportation (CSXT) and Maryland Rail Commuter (MARC) had operational reasons to modify the Brunswick Line signal system: improve passenger safety and freight train operations by changing the method that CSXT dispatched and monitored trains, upgrade the system capacity to operate more trains with increased peak and midday service, increase the MARC labor and equipment productivity, and reduce the CSXT operating costs. Identifiable improvements, such as total trains, traincrew use, cost savings, and Centralised Traffic Control (CTC) operations, could be quantified and measured; however, the signal system modifications did not address the overall safety of the signal system for traincrew use... The Safety Board concludes that Federal funds granted for the signal modifications on the CSXT Brunswick Line to accommodate an increase in the number of MARC trains did not ensure that the safety of the public was adequately addressed. Therefore, the Safety Board believes that the Federal Railroad Administration (FRA) should require comprehensive failure modes and effects analyses, including a human factors analysis, for all signal system modifications and that the Federal Transport Administration (FTA) should revise the grant application process to require the same such analyses be provided for all federally funded transit projects that are directly related to the transport of passengers." [598]

The previous paragraphs have described how it is important for the secondary investigation not only to gather evidence about the causes of an incident but also to monitor the consequences of any failure. The outcome of an adverse occurrence provides investigators with important information about its criticality. It can also help to ensure that all of the parties who contribute to an adverse occurrence are identified and informed about its impact upon application processes. Finally, it is important to investigate the consequences of an incident because this helps to determine its criticality. There is an important caveat to this last point that we have not raised in this chapter. In particular, we will see in Chapter 9.3 that the risk assessments that are derived from particular incidents need not mirror the actual consequences of an adverse occurrence. For example, some organisations adopt the policy of assuming the 'worst plausible outcome' . As a result, some Air Traffic Management providers assume that if aircrews detect and resolve an air proximity violation then that incident should be treated as if the aircraft had collided because controllers failed to actively intervene to prevent a potential accident [423].

7.2.2 Detecting Mitigating Factors

The previous section has described how some of the consequences of an incident can be separated in time and place from the immediate events that lead to an incident. As a result, it can be difficult for investigators to fully assess the outcome of an adverse event until some time after it has occurred. This section investigates a number of further complications that frustrate secondary investigations. In particular, it identifies ways in which the intervention of operators and automated systems force investigators to consider alternate hypotheses about the consequences of an incident without these mitigating factors. This represents a particular extension of Lewis' counterfactual arguments [490]. We summarised his approach to causation by stating that that 'if some event had not occurred as it did then the accident would never have occurred'. Consequence analysis often takes the form of 'if some mitigating event had not occurred as it did then the accident would have been far worse'. As can be seen, therefore, mitigating actions can be though of as a form of complement to the causal actions that lead to incidents and accident.

The following incident illustrates the way in which staff and automated systems often have the opportunity to detect an adverse occurrence and intervene to mitigate its effects. If the staff had monitored the set up of the heating blanket or if they had inspected the patient's legs during the operation then the burns might have been avoided. This form of incident represents the simplest case for consequence analysis because it is difficult to see how the outcome could have plausibly been much worse given the particular heating system that was involved:

> "After surgery, burns on the foot, posterior calf, and posterior medial thigh were noted. Surgery was lengthy. Burns are second degree, requiring at this point, topical treatment. Blistered areas are 1 X 2 cm. (foot), 4 x 8 cm. (calf) and 3 x 5 cm. (thigh). Due to the size of child, he was placed on top of the blanket with the nozzle between his legs. The company believes the leg was too close to the nozzle, which protrudes 10 cm. into the blanket, and the hot nozzle/hot air burned the skin." ([270], Report Number 9681384-1997-00016).

As mentioned, however, the identification and analysis of the potential consequences of any incident can be complicated by the ways in which operators or safety systems intervene to mitigate the worst effects of any failure. Of course, these fortunate interventions help to avoid accidents and more serious incidents. However, they force investigators to consider a large number of hypothetical worse case scenarios in which operators and systems did not intervene to mitigate the failure. Again, there are many incidents in which this is can be relatively straightforward. For example, the worst case in the following incident is clearly that the patient could have died if the staff had not been able to offer effective cardio-pulmonary resuscitation (CPR) in time:

> "At 12:50 pm Charge Nurse entered patient's room. Patient was dusky in colour and without vital signs. Ventilator and alarms not sounding. Ventilator circuit observed to be disconnected from TRACH, ventilator producing air however pressure alarm did not sound. Circuit reconnected to TRACH, then removed to initiate manual ventilation and CPR. After circuit disconnected for CPR alarms sounded in approx 5 seconds." ([270], Report Number 221768)

The potential consequences of many incidents are, however, often less clear-cut than this example. At the extreme, an investigator might consider that an apparently minor incidents could have 'snow-balled' into a major accident involving a significant loss of life. Although this might seem to be nonsensical, it is important to remember that many major catastrophes have apparently simple root causes. The match that triggered the Kings Cross fire [249] provides an example of this. Several investigations into previous fires on the London Underground failed to understand the potentially disastrous consequences of such events. Partially as a result, safety managers focussed on putting out those fires that did occur rather than trying to eliminate the potential for a fire to start. The following incident provides a further example of this problem. The ingestion of flying insects into a vent tube forced the crew of a commercial airliner to glide towards the nearest runway. This relatively simple problem could have had disastrous consequences. The key point here is that the organisation concerned, like the London Underground, still failed to predict these consequences even though a number of similar failures had previously been reported:

> Fuel at time of departure was 56 gallons, of which 40 was in the tip tanks... Climbed to cruise altitude of 5,500 feet MSL, leveled off, turned off boost pump. Engine lost power about 1-1/2 minutes (estimated) after changing tanks... Established glide to nearest airport and commenced restart procedure...and declared emergency. Engine restarted at 500 feet AGL on short final... Landed without incident, with full power available... Cause of engine-out was determined by mechanic at FBO to be "leaf roller" (flying insect) debris packed into right tip tank vent tube, totally obstructing air flow in the vent. Tank vents...open to air at a point under the wing attachment point. There are no screens on the vent openings. The vent was cleared, and the left vent checked and also cleared of similar debris (although not completely closed), and the aircraft was returned to service..." [61]

There are many reasons why the secondary investigation of an incident report must gather evidence about mitigating events. Not only does this provide important information about potential 'worst case' scenarios using an extension of Lewis' counterfactual arguments, evidence about the defences that protect safety-critical systems. As we have seen, human operators and automated systems are often designed to provide 'defence in depth' so that if one fails to protect an application then another may successfully intervene. However, Reason argues that many incident have multiple root causes that together may combine to defeat safety measures [702]. As a result, it is imperative that we learn as much as possible both not only about those defences that succeed but also about those defences that fail to offer the intended protection during particular incidents. For example, the following incident illustrates a situation in which a warning display in the cockpit was able to back-up the human surveillance of the cabin staff. It also illustrates how fortuitous circumstances, in particular the availability of additional company personnel on-board, often help retrieve adverse situations:

> "At FL330 had momentary [warning] message 'Door Left Aft Cabin,' meaning door 2L was not fully latched. Message cleared itself, then reappeared. (Got message a total of 4 times.) Contacted purser to have her ensure no one was tampering with door. She said there was a female passenger who had been acting very strangely since leaving [airport]... Through an interpreter...passenger admitted to having attempted to open door. [Crew] found 2 [company] pass-riders and had them sit with/watch over passenger for remainder of flight. Contacted company and asked for flight to be met by the FBI." [58] .

This section has used examples of a number of mitigating factors to illustrate the problems that can arise if investigators are both to assess the potential consequences of an incident and determine what factors combined to preserve the safety of an application. These accounts have been selected because they are each relatively simple. However, the investigators task can become considerably more complicated. For example, the following quotations describe a situation in which the crew of a merchant ship actively intervene to prevent an accident. However, by gathering evidence about the ship and their actions the investigator concludes that their immediate actions had the potential to exacerbate rather than mitigate the incident. This assessment is made even more complex by the fact that the ship and its crew survived both the initial incident and the immediate intervention. The incident began when a load of nickel ore became saturated, settled and started to shift to port.

> "At 2200, or a little before, Padang Hawk suddenly developed a 15 degree list to port. The master, who was in his cabin, immediately went to the bridge and joined the second mate and lookout. The master altered course from 265 degrees to 295 degrees to bring the wind and sea on to the port quarter and reduced the engine revolutions from 110 RPM to 100 RPM... The master decided to ballast starboard side tanks to correct the list. Numbers 3 and 5 starboard topside tanks were filled... At 0145, the master received a reply from the vessels owners advising him to use double bottom tanks to correct the list. The message noted that countering lists by using topside tanks had caused vessels to capsize and it continued: 'Although your vessel is having very high GM due to dense cargo, still high risk of cargo shifting to one side with the roll is high'... The cargo hold bilges were pumped at regular intervals throughout the day. The disposition of ballast was adjusted in accordance with the advice from the owners...
> [Investigators analysis] While recognising the circumstances and the imperative to right the ships list, the master took a significant risk in ballasting the vessel, by adding weight centred high and outboard with an accompanying free surface, without first checking the likely effect on the vessels stability. Although the master was correct in his assessment of the stability, there was a risk of far worse consequences for the vessel and crew, should his intuitive judgement have been faulty. It would have been prudent to use the available resources to calculate the stability of the vessel for all of the conditions prior to transferring any ballast."

This incident begins to illustrate the full complexity involved in both collecting and interpreting evidence about the mitigating factors that influence the development of any incident. The crew intervened in numerous ways to reduce the likelihood that their vessel would be lost. Some of those actions were correct, such as altering the course of the vessel to bring the wind and waves on the port quarter. Other actions were incorrect, most notably the decision to move ballast without first ensuring the stability of the ship. These distinctions reflect what Mackie calls the singular causes of conditions that characterise particular events [508]. Difficulties arise when investigators must move beyond these specific observations to assess the potential severity of an incident without such interventions. Similarly, it is far from simple to determine what might have happen in future situations in which the crew did not perform in the manner described above. One means of reducing this uncertainty, and of supporting other aspects of secondary investigation, is to draw upon evidence from a number of similar incidents.

7.2.3 Identifying Related Incidents

This chapter has described a number of complex tasks that must be performed during the secondary investigation of an adverse occurrence or near miss incident. Many of these tasks are intended to help gather the evidence that will eventually support a causal analysis of 'failure'. Previous sections have argued that ultimately this analysis must look beyond the singular causal factors that contribute to a particular occurrence. Any recommendations should ideally address the more general causes that might lead to similar consequences. In order to do this it is important that investigators gather evidence about similar incidents that may have already occurred. In particular, they must determine whether the singular causes of an adverse occurrence now form part of a wider pattern of failure.

Unfortunately, it can often be difficult to identify common trends in incident reports. Issues of confidentiality and privacy often make organisations reluctant to share information about incidents and accidents. For example, a recent meeting of European air traffic service providers identified a number of common concerns over the impact of that TCAS advisories have upon their ability to sustain safe separations in congested airspace. Aircrews have over-reacted to TCAS warnings; by performing sudden ascents or descents that have infringed on the airspace of other aircraft creating a knock-on effect that can be difficult to counter. Information about a range of similar incidents was passed informally amongst a group of friends from different national providers during a break rather than through any systematic exchange programme. There may of course be information about other similar incidents that is never passed on and so cannot inform the secondary investigation of future adverse occurrences. If anyone is in doubt about this it is instructive to compare the NTSB's report in the collision between a Maryland Rail Commuter and an AMTRAK train [598] with the events leading to the Watford Junction [350] and Ladbroke Grove accidents [353].

A range of further problems prevent investigators from establishing whether an incident forms part of a wider trend. For instance, it can be difficult to ensure that similar events are investigated, analysed and documented in a consistent manner. This is confirmed by both empirical studies and by the more theoretical models of causal analysis. Mackie's notion of a causal field, mentioned above, implies that different investigators may identify different disturbances in the normal state of affairs [508]. This, in turn, can lead them to recognise and diagnose different elements of a causal complex as being salient to a particular incident [508]. Empirical work to back-up this analysis is provided by Lekberg's study of investigator 'biases' [484]. As mentioned in Chapter 2.3, she showed that different investigators will identify different causal factors within the same incident depending on their previous training and experience. This has profound consequences. If, for example, an investigator were looking for similar incidents in which crew coordination were a causal factor then there is no guarantee that other investigators would have diagnosed this as being significant even if it had indeed taken place. Chapter 9.3 will introduce a range of analytical techniques that have been proposed to reduce the impact of this problem. For now it is sufficient to understand that such individual differences between investigators may compromise their ability to determine whether or not a particular incident forms part of a more general pattern.

Problems of scale also complicate the task of identifying similar incidents. As mentioned in previous chapters, the ASRS was established in 1976 and now receives an average of more than 2,600 reports per month. The cumulative total is now approaching half a million reports from pilots, air traffic controllers, flight attendants, mechanics etc. Similarly, the FDA's Centre for Devices and Radiological Health's Medical Device Reporting program forms part of a collection of well over 700,000 incidents. Later chapters will introduce a range of innovative technological solutions that are being recruited to support these tasks. In contrast, the remainder of this section looks at a range of more straightforward organisational and managerial techniques that can help investigators to identify similar incidents and common concerns. Fortunately, in some cases it is relatively easy for investigators to determine a pattern of failure. Similar incidents may occur in the same place and within a relatively short-period of time. Under such circumstances, it is readily apparent to many of the individuals who are involved in operating a systems that they may have to address common problems in two or more incidents:

> "Two similar serious incidents were notified to the Air Accidents Investigation Branch (AAIB) at 0630 hrs and 0740 hrs respectively on 6 June 1998, and the investigation commenced the same day... The two serious incidents occurred as each aircraft was making an instrument approach to Runway 08 at Ronaldsway Airport, Isle of Man. Both aircraft were using the Isle of Man VHF Omni-Directional Radio Range beacon and associated Distance Measuring Equipment for lateral navigation and distance information respectively. During the course of each of the approaches, each aircraft descended very significantly below the specified descent profile while over the sea to the west of high ground at the Calf of Man and Spanish Head. There was extensive low cloud in the area at these times and in both cases initiation of a climb to avoid possible collision with the high ground occurred once the surface and coastline had been sighted by the pilots involved." [19]

In other cases, organisations may take specific measures to monitor incidents that occur in the same physical location over a more prolonged period of time. This approach has been actively exploited by a number of road traffic management organisations. Sections of road are categorised according to the number and severity of accidents that occur over them in a fixed period of time. Those sections with the worst record are then subjected to an additional level of scrutiny. For example, there may be a detailed analysis of the causal factors behind those incidents that occur on that stretch of road. This analysis and the record of previous incidents help to direct and justify subsequent expenditure on additional safety measures:

> "The junction, near the Lincolnshire Showground, has one of the worst accident records on the A15 between Lincoln and the county boundary. Options for its improvement include a roundabout or staggered junction. It is hoped work could start next financial year. The recommendation for the scheme was made in a safety study commissioned by the Highways Agency in response to the considerable number of road traffic accidents on the A15 in recent years... In the three year period up to 31 May 1998, there were six fatalities on the stretch of A15 covered by the report, 10 serious injuries and 39 slight injuries." [360]

By identifying common causes behind particular incidents, it is possible to justify additional expenditure on more detailed, comparative studies. These investigations might be harded to justify on the basis of individual failures. This approach is exploited by the NTSB. Special investigations are commissioned if investigators identify common causes or consequences in the incidents that they report on. In many instances, these reports simply confirm the initial suspicions that were raised during the initial investigations. However, the additional resources that are invested in these more detailed studies can also reveal more unexpected findings about the potential consequences of a failure. For instance, a recent report demonstrated that cable breakages caused by excavation activities threatened safety in a number of different industries. This was not an unusual finding. However, the potential impact on US air traffic management was not previously appreciated by many other service providers:

> "Network reliability data, compiled since 1993 by NRSC, show that more than half of all facility outages are the result of excavation damage (53 percent), and in more than half of those cases (51 percent), the excavator failed to notify the facility owner or provided inadequate notification... The Federal Aviation Administrations (FAA) study of cable cuts in 1993 documented 1,444 equipment outages or communications service disruptions resulting from 590 cable cuts nationwide over a 2-year period. The majority of cable cuts were related to construction and excavation activities. For 1995, the FAA's

> National Maintenance Control Center documented cable cuts that affected 32 air traffic control facilities, including five en route control centers. Cable cuts for the first 8 months of 1997 affected air traffic control operations for a total of 158 hours." [600]

Previous quotation have shown how regulators, such as the UK Highways Agency, and investigatory agencies, such as the NTSB, will monitor the common causes and consequences of adverse occurrences. The independent reporting agencies that operate many voluntary reporting systems will also undertake this form of analysis. For example, the ASRS uses three distinct publications to communicate the concerns that are raised within the aviation community. More than 85,000 copies of the CALLBACK newsletter are distributed directly to employees within the aviation community. This includes excerpts from ASRS incident reports with associated editorial comments. It can also contain summaries of ASRS research studies and related aviation safety information. In contrast, DirectLine and the Operation Issues Bulletins are entirely devoted to more sustained investigation about the common causes of adverse occurrences. Although the distinction becomes slightly blurred, the Bulletins cover more immediate concerns whereas DirectLine focuses on incidents that may have arisen over a longer period of time. For instance, the following excerpt shows how DirectLine provides explicit information about common causes, and consequences, in communications failures involving General Aviation (i.e., private pilots):

> "A recent survey of the Aviation Safety Reporting System (ASRS) database on incidents involving General Aviation (GA) aircraft revealed that one third of the GA incidents were associated with communications difficulties... Confusing, erroneous, or misleading statements were the leading type of instructor communications anomaly (30 percent of citations). Delayed or withheld communications by instructors were the next most frequent instructor anomaly (16 percent of citations), and a leading cause of delayed or inappropriate actions on the part of trainees. It is a common technique of flight instructors to allow the trainee to make mistakes in an attempt to develop independent actions and observe the trainee's level of awareness. However, especially during IFR operations, or when compliance with an ATC directive is doubtful, corrective verbal comments by the instructor have a significant impact on flight safety." [229]

Previous sections have argued that investigators gather evidence to help validate their initial hypotheses about the causes of an incident. Information about previous events can provide additional information to guide this validation process. However, there is a danger that beliefs about the causes of a particular incident will be biased by preconceptions about similar incidents. There is also a danger that investigators may diagnose common causes even if two incidents have similar consequences. This is problematic because many different causes can potentially contribute to the same set of outcomes. In spite of these dangers there are, however, considerable benefits if investigators are encouraged to identify common causal factors between similar incidents. This can help to increase the consistency of analysis between investigators. It can help to ensure that similar measures are taken to address the common causes of failure. This, in turn, helps regulatory agencies to determine the success or failure of remedial measures. Such monitoring becomes far more complex if each incident is treated as an individual instance of failure. As a result, many regulatory agencies explicitly encourage these generalisations by publicising common causes and remedies for incidents and accidents:

> "THE PROBLEM:
> Drivers too close to the vehicle in front. 2000 'shunt' type accidents per year on British motorways. Cost of 'shunt' £60 million/year (1989 prices).
> THE SOLUTION:
> Chevron road markings at 40m intervals at problem locations. Signs instructing drivers to keep 2 chevrons from the vehicle in front. Require authorisation.
> THE BENEFITS:
> Study results showed: A reduction of about 15% of drivers 'close-following'. Fewer accidents as driver awareness increased over the site. 56% fewer injury accidents, 89%

> fewer single vehicle accidents, 40% fewer multiple vehicle accidents, £0.8m/year accident savings (1993 prices). The effect can last at least 18km." [361]

This quotation illustrates how the UK Highways Agency has identified that drivers being too close to the vehicle in front is a common cause in road traffic accidents. They have also gone on to propose chevron road markings as a general solution to this problem and have then gone on to measure the impact of this remedial action. This analysis and the supporting statistics are published in a national compendium of 'techniques and innovative ideas for the better management of the trunk road network' [361]. The success of this document is illustrated by the fact that it has inspired similar initiatives in countries ranging from the Netherlands to Japan. However, there is a danger that such documents will focus the attention of investigators on particular areas of a causal field and that, as a result, on a small subset of possible remedial actions will be taken. This is a particular concern where those remedial actions that are recommended within such a publication are selected for political acceptability rather than effectiveness. Fortunately, the Highways Agency avoids this criticism by publishing statistical evidence to demonstrate the impact of the measures that it advocates. Other organisations have avoided these concerns by adopting a slightly simpler approach. The NTSB does not explicitly identify common causes and general solutions. In contrast, it surveys the recommendations made in incident reports, irrespective of the causes, and then publishes a 'most wanted list'. This, at least publically, avoids any suggestion that all events with particular causal factors can be resolved by the same set of remedial actions. For example, the most wanted safety improvements for highway vehicle occupant protection include the enforcement of state seat-belt laws and an evaluation of whether higher thresholds could safely be allowed for air bag deployment. The corresponding list of commercial truck and bus safety improvements includes general measures to enhance occupant safety, modifications to hours-of-service regulations and higher vehicle maintenance standards.

7.3 Summary

This chapter has focussed on the secondary investigation that, typically, takes place after the primary recipient of an incident report has completed a preliminary report. This phase of an investigation is primarily focussed on securing further evidence about the course of an incident. However, we have argued that this task is guided by a succession of hypotheses about the potential causes of an incident. Evidence is gathered to validate these initial ideas. If necessary, the investigators' causal hypotheses may have to be revised as more evidence becomes available.

It is important to understand some of the distinctions that have been made between the causal factors that contribute to accidents and incidents. For example, Mackie introduced the idea of a causal field, of particular and general causality , of causal complexes [508]. Lewis has pioneered the use of counterfactuals in causal explanations. This work is relevant and significant because it has been integrated into a number of incident analysis techniques that will be introduced in subsequent chapters. Based on this work, we have distinguished between contextual factors, contributory factors and root causes. Contextual Factor are neither necessary not sufficient They are events or conditions that did not directly contribute to the causes of an incident. However, they help to set the scene and establish the context in which an adverse occurrence took place. They may also help to establish that certain factors were NOT significant in the events leading to failure. Contributory Factors are necessary but not sufficient. They are events or conditions that collectively increase the likelihood of an incident but that individually would not lead to an adverse occurrence. These are the 'banal factors' in Reason's observation that "... a detailed examination of the causes of these accidents reveals the insidious concatenation of often relatively banal factors, hardly significant in themselves, but devastating in their combination" [701]. Root causes are both necessary and sufficient. They capture Lewis' notion of causation established by counterfactual reasoning. If a root cause had not occurred in the singular causes of an incident then the incident would not have occurred.

Later sections went on to examine sources of evidence that can be used to identify contextual factors, contributory factors and root causes. It was argued that the use of independent expert witnesses can help to combat the natural biases that can persuade investigators to favour particular causal hypotheses. However, there is also a danger that such witnesses may themselves be biased. In order to address this problem, we developed Spohrer and Maciejewski's [755] ten commandments for Chemists acting as expert witnesses during criminal investigations. We presented a more general set of guidelines based on these heuristics so that they might support the wide range of experts who are called upon to support incident investigations.

Evidence about the causes of an incident can also be extracted from the automatic monitoring devices whose logs are preserved during the initial response to an incident. However, this chapter has reviewed the considerable managerial and technical problems that continue to affect the use of these critical data sources in many industries. For example, it can be difficult to ensure that these devices are correctly maintained. There have also been instances where monitoring devices are incorrectly configured to the individual standards that many commercial organisations are creating. Even if data is correctly recorded, problems can arise when duplicating data or in finding a correctly configured reader. Although many of these problems are being addressed both by regulators and manufacturers, they continue to be document in incident reports that lament the lack of automated logs.

The second half of this chapter focussed on the importance of gathering evidence about the consequences, as well as the causes of adverse occurrences. In some situations this can be relatively straightforward. The effects of any failure can be directly witnessed by those involved in the immediate precursors to an incident. In other contexts, the individuals who contribute to a failure may have no idea of the impact that their actions have had. For example in transportation systems, problems can occur many miles away from the maintenance facility that contributed to the failure. In medical systems, the consequences of an incident may not manifest themselves until years later when the patient's physical well-being and quality of life may be seriously compromised.

The problems of gathering evidence about the consequences of an incident are further complicated by the fact that investigators may have to account for mitigating factors. These interventions can reduce the consequences of a particular incident. As a result, investigators may choose to treat the occurrence as if the intervention had not taken place. This approach exploits the notion of a worst plausible outcome . However, a limitation with this technique is that it can be difficult to predict the ways in which apparently trivial failures can quickly escalate into major accidents. Further problems are created by the difficulty of establishing possible combinations of contributory and mitigating factors that are likely during any future failure.

One means of addressing the uncertainty that arises during the secondary analysis of any incident is to gather as much information as possible about similar incidents. This can be done by investigating records of previous failure in the same location or within a similar period of time. It can also be done by examining regulatory and investigatory 'hit lists' of common causal factors in adverse occurrences. Incident reporting systems may also provid information about previous problems. These alternative sources of evidence help to increase the investigators confidence in any generalisations that may be made about the causes and consequences of particular incidents. However, there is also a danger that they may inadvertently bias any investigation towards the findings of previous investigations. Rather than looking at each incident as a potentially unique occurrence, investigators might simply attempt to place it within pre-existing categories of superficially similar incidents.

To summarise, this chapter has stressed the importance of gathering evidence about the causes and consequences of adverse occurrences. It has also explained why it can be so difficult to achieve this. Technical difficulties continue to frustrate automated logging techniques. The problems of determining a plausible worst case scenario frustrate attempts to gather evidence about possible consequences of previous incidents. The following chapters, therefore, present a range of techniques that are intended to address these problems.