Chapter 4

The Anatomy of Incident Reporting

The following incident report was recently published by the Australian Transportation Safety Board (ATSB). It describes an incident that was initially notified by a member of the public and which was subsequently investigated by ATSB staff:

> "A member of the public reported seeing a single engine aircraft manouevre suddenly to avoid another aircraft, on an intersecting track, while the aircraft were over Brisbane.
>
> An investigation reviewed radar data and air traffic control automatic voice recordings to establish the sequence of events. The investigation found that VH-OXF, a Beech 300, was tracking for a left base to runway 01 at Brisbane Airport at 2,500 ft, while a Cessna 172, VH-IGA, was tracking north over the suburbs at 1,500 ft. The Brisbane departures controller established that the pilot of the Beech could see and was able to avoid the Cessna before reducing the vertical spacing between the aircraft to less than the vertical separation standard of 1,000 ft. The Beech pilot reported seeing and passing over the top of the Cessna and ready for further descent. The controller issued a clearance for a visual approach. The recorded radar data indicated that the Beech began a steady descent from about the intersection of the aircraft tracks.
>
> The controller's options in relation to ensuring separation between the aircraft were either to: maintain the Beech at 2,500 ft until there was more than 3 NM lateral separation with the Cessna; or use visual separation procedures by having a pilot report seeing the other aircraft and then instructing that pilot to avoid the sighted aircraft. To enable the Beech to descend in preparation for landing, the controller used the second option. Examination of the radar data indicated there was no infringement of separation standards.
>
> The recorded radar data indicated that during the period when the Beech was assigned 2,500 ft, the Mode C altitude intermittently indicated 2,300 ft and 2,400 ft. Mode C altitude has a tolerance of plus or minus 200 ft. The pilot was therefore complying with the air traffic control clearance." [50]

This report illustrates some of the tasks that must be performed during any incident investigation. The incident must be reported to the appropriate authorities. The people who initially receive a notification must take any immediate action and pass it on for further investigation. The conclusions and findings of any investigation must be published. Although there were no immediate recommendations from the incident cited above, if there had been then these must be implemented and monitored. The following sections take each of these tasks or roles and considers how they contribute to the successful implementation of an incident reporting system.

4.1 Different Roles

It is important to emphasise that the following paragraphs identify tasks or roles. Any individual or group can perform several of these roles depending on the organisational needs of the reporting system. For example, in a local system the same individual may both receive a report and conduct any subsequent analysis or investigation. In a national or international system, it is more likely that specialist analytical expertise might be called upon to support the local officers who receive an initial notification.

Section 4.2 builds on this analysis and describes a number of different organisational models that can be used to manage these different roles or tasks within specific working environments.

4.1.1 Reporters

This is the person who contributes the initial incident report that triggers any occurrence investigation. The organisation running the scheme may employ them, they may be subcontractors or they may be employed by other organisations that must co-operate with the organisation running the scheme. For example, a member of an aircrew might report an air traffic control incident. Alternatively, members of the public who have witnessed or been involved in an occurrence report some incidents, as was the case in the incident cited above. The following paragraphs identify some of the issues that must be considered when encouraging such contributions to occurrence reporting schemes.

Am I Protected?

Previous chapters have argued that incident reporting systems depend upon the trust of those who contribute to them. If individuals are concerned about punitive actions or about the confidentiality of their submissions then they are unlikely to participate in such a system. One means of preserving this sense of trust is to publish a summary of the rights that protect workers who contribute to a reporting scheme. These rights are partly built on legislative protection, they also rely upon the procedural safeguards that support their participation during the investigation and analysis of an incident.

It is important that the individuals who contribute to an incident reporting system are aware both of their rights and responsibilities when contributing information about adverse occurrences. For instance, in some industries it may be assumed that operators have the right to be excused from further duties in the aftermath of an incident until they are physically or psychologically fit. It is important that such actions should not be interpreted as an admission of guilt or responsibility for an incident. Some systems also offer various forms of counselling to support individuals int he aftermath of an adverse occurrence.

Operators often have the right to a representative of their choice during subsequent interviews or hearings. These representatives can be colleagues, lawyers or a trades union officials. Their presence can have a profound impact both on the individual's participation in a system but also on wider perceptions about the efficacy of incident reporting. There are also practical implications. It can be difficult to schedule investigatory meetings if workers' representatives are unavailable when investigators must compile evidence about an occurrence.

Many national legal systems preserve an individual's right to silence during criminal investigations. Incident reporting systems are not concerned with such criminal acts. However, many systems do offer individuals the opportunity not to 'incriminate' themselves. Operators are not obliged to make written statements. Other systems do not go this far but do ensure that individuals can consult with their chosen representatives before submitting written material.

After the initial information has been gathered about an incident, it is important that workers are aware of their rights during any subsequent analysis. For instance, workers and their representatives may have the right to pose questions to the investigation team. They may also be entitled to review any relevant documents, data recordings or transcripts before appearing in front of any enquiry. Finally, it is also possible for contributors to review the contents of a final report and offer a written response that may be appended to the initial document.

It can, of course, be argued that these various arrangements add greater administrative complexity to incident investigation. Worker representation and participation may also 'tie the hands' of incident investigators. However, such arguments must be balanced against the primary importance of ensuring participation and consensus. Unless individuals feel confident of equitable treatment then they will not contribute. Unless groups of workers are confident in the findings of an investigation then they may oppose the implementation of controversial findings and recommendations.

Should I Report?

A key issue here is that potential contributors must know about the scheme and know how to submit a report. The scale of this task can be illustrated by the distribution list associated with the UK Medical Devices Agency's (MDA) reporting scheme for Adverse Incidents and Disseminating Safety Warnings. This list describes those who must pass on information about this scheme to the people on a far larger list of potential contributors:

> "Please bring this notice to the attention of all who need to know or be aware of it. This will include distribution by:
> TRUSTS to:
> Liaison Officers (for onward distribution), All relevant staff including: Risk Managers, Safety Officers, Medical Directors, Clinical Directors, Nurse Executive Directors, Medical, Dental and Nursing staff, Medical Physics/EBME, Operating Theatres, Intensive Care Units, Intensive Therapy Units, Ambulance staff and Paramedics.
> HEALTH AUTHORITIES to:
> Liaison Officers (for onward distribution), Chief Executives of Primary, Care Groups, Registration Inspection Units, General Medical Practitioners, General Dental Practitioners, Opticians, Pharmacists, Practice Nurses, Nursing Homes, Hospices, Private Hospitals.
> SOCIAL SERVICES to:
> Liaison Officers (for onward distribution), Registration Inspection Units, Residential Care Homes, Occupational Therapists, Special Schools." [536]

The scale of this task should not be underestimated. These distributors must ensure that induction courses and periodic retraining reminds staff about the importance of reporting. They must also perform more prosaic duties. For example, they must ensure that staff are providing with access to reporting forms at all times. The logistics involved in disseminating information about incident reporting systems are not the only challenge

It is not enough simply to inform potential respondents about reporting procedures, they must also be able to provide the necessary details that are requested by forms or other elicitation documents. This is a non-trivial task. it can be difficult to draft a form that will elicit sufficient information from all of the many different groups listed above. If respondents do not understand a question then they may fail to provide necessary information. If they misinterpret a question then they may provide erroneous or misleading responses. All of these issues have been compounded by the increasing use of electronic submission forms based on Internet technology. The design of these submission procedures will be discussed in greater detail in Chapter 4.3.

Will Everyone Participate?

This will be a continuing theme throughout much of this book. Previous chapters have cited the relatively low participation rate in voluntary aviation reporting schemes by general aviation and the military in contrast to commercial aviation. It should also be noted that such comparisons are compounded by the difficulty of estimating what the anticipated reporting rate ought to be. It can be difficult to assess whether each of these groups has a comparative exposure to hazardous occurrences etc. For example, in one local incident reporting system within a UK intensive care unit, approximately 90% of all reports were submitted by nursing staff over a ten year period. 621 reports were submitted by nurses compared with 77 reports by medical staff. However, these figures must be interpreted in terms of the number of staff on the ward. Usually the team consisted of three medical staff, one consultant, and up to eight nurses per shift. The analysis is further complicated by the fact that nursing staff had the most direct contact with the patients who remain the focus of the reporting system and hence may have had proportionately greater opportunity to witness adverse events [119]. Each of these factors must be considered before concluding that there is a systematic under-reporting by medical staff.

What Did I Really See?

There are clear problems in interpreting the evidence provided by an initial report of an incident. For example, the testimony of one eye witness to the Concorde crash was initially interpreted an being consistent with the illumination caused by afterburners rather than a fire involving the fuel tanks. Statements that indicated the true extent of the damage to the aircraft on take-off were dismissed as the exaggerated claims of uninformed observers. The problems of interpreting eye witness statements are not simply related to the difficulty of assessing non-technical accounts of system failures. They can also arise when qualified personnel attempt to provide immediate causal explanations. As mentioned in previous chapters, witnessing an accident can often have the effect of confirming previous concerns about particular operational problems. This confirmation bias can dissuade technical witnesses from considering alternative hypotheses in the immediate aftermath of an incident or accident. A feeling of direct personal responsibility or of physical threat during an accident can lead witnesses to either minimise of maximise the implications of the incidents that they report. Conversely, as mentioned in previous chapters, reports may be contributed by individuals who are more concerned with a perceived grievance than with the overall objectives of addressing safety issues. Reports may also be biased in order to protect themselves, their co-workers or their employers. This final point is illustrated by the findings of an enquiry into a trench collapse that was reported by the US Occupational Safety and Health Administration (OSHA). This refers to witness testimony in the investigation of an incident rather than the initial report of an incident. However, the following quotation does illustrate the potential problems of interpreting bias in eye-witness statements:

> "The judge based his finding that the trench walls had no significant slope on the testimony of 'three disinterested on-the-scene eyewitnesses' (two paramedics and a volunteer fireman), who entered the trench that collapsed. All three reported seeing identical conditions. The judge found the testimony of two corporate officers and two other employees of Zunker regarding the trench dimensions and sloping to be 'unreliable and indeed untruthful,' stating as follows:
>
> The testimony of all these witnesses, each of whom had an interest in the results of these proceedings, was at total odds with the testimony of the [paramedics and fireman] who were disinterested and who truthfully reported their observations at the work site, and in particular at the site of the cave-in. The demeanor of [Zunker's witnesses] as well as their sworn testimony, leaves much to be desired as having any probative value in determining the factual issues in this case.... What element of truth we do attribute to these witnesses comes from Respondent's backhoe operator who indicated that it took him 20 minutes to dig the trench.... [I]t would be virtually impossible to excavate a trench in accordance with the dimensions testified to by [Zunker's president] within a 20-minute period." [648]

The problems that arise immediately after the reporting of an incident are compounded in anonymous systems. This is best illustrated by US guidelines that provide recommended practices for small businesses following the notification of any incident:

> "Gather evidence from many sources during an investigation. Get information from witnesses and reports as well as by observation. Interview witnesses as soon as possible after an accident. Inspect the accident site before any changes occur. Take photographs and make sketches of the accident scene. Record all pertinent data on maps. Get copies of all reports. Documents containing normal operating procedures, flow diagrams,

> maintenance charts, or reports of difficulties or abnormalities are particularly useful. Keep complete and accurate notes in a bound notebook. Record pre-accident conditions, the accident sequence, and post-accident conditions. In addition, document the location of victims, witnesses, machinery, energy sources, and hazardous materials." [651]

These guidelines are generic; they are applicable to a wide range of industries. They also cover what we have termed 'local' reporting systems because they are specifically intended for small businesses. However, these guidelines also illustrate the problems of responding to an anonymous report of an incident. It can be difficult to know where to begin gathering evidence if a report is anonymous. As mentioned in previous chapters, this initial investigation may itself be enough to sacrifice the trust of the contributor and compromise their anonymity. Without the active participation of a known reporter it can be difficult to obtain the additional information that may be necessary to accurately record pre-accident conditions, as they saw them.

Chapter 4.3 will address these concerns in greater detail. In contrast, the following paragraphs look beyond those individuals who contribute occurrence reports to look at the people who must initially respond to their notifications.

4.1.2 Initial Receivers

The reporter sends their submission to an 'initial receiver'. In most company's incident reports are made to line supervisors unless they are directly implicated in an incident. This has the advantage that supervisors will be familiar with working practices and can take immediate remedial actions to mitigate any adverse consequences. However, these initial receivers need not be directly connected with the reporter's organisation or company. In particular, national systems often rely upon independent reporting agencies. For example, NASA is responsible for administering the Aviation Safety Reporting System (ASRS) on behalf of the FAA. Such organisations protect the notifier's anonymity whilst still enabling investigators to perform subsequent data collection.

The receivers of an incident report are responsible for making an initial criticality assessment. 'Triage' is an important task during the operations of many incident reporting systems. The individual who detects a potential incident must first decide whether or not it is worth reporting. The individual who receives an initial report must then decide whether to pass it on. If they decide that it should be acted on then they must determine who is best placed to act on the report. The group or individual who must act on a report has further more detailed technical judgements to make about the best way in which to investigate and resolve any safety concerns. These decisions depend upon assessments of the importance or priority associated with an incident. Such assessments must be documented and justified in order to support the external inspections that help to ensure consistent responses to similar incidents. The initial receiver also plays an important role in taking any immediate actions that is necessary to safeguard services following an incident. The following paragraphs consider these issues in more detail.

How to Safeguard the System?

The most important task facing the individual who receives an incident report is to coordinate the immediate response to an adverse occurrence. Typically, such actions cannot be delayed until after a full investigation has been instigated or a final report has been delivered. Operators may have to be removed from their working positions. Faulty equipment must be disconnected. Alternative systems or manual back-ups must be set-up. All of this relies upon individuals making a rapid assessment of the context in which an incident occurred. It also relies upon their ability and willingness to instigate immediate corrective actions. Such a response relies upon both a number of factors. The individuals who assume this role must be training to enable them to perform an accurate initial response. They must be familiar with the relevant procedures involved in instigating immediate corrective actions and must feel comfortable with the responsibilities that are associated with such actions. There are clear safety implications if these individuals feel that they lack the appropriate authority or responsibility for taking immediate corrective actions.

It is important to emphasise that operators should not, typically, be withdrawn from their working positions for disciplinary reasons in the aftermath of an occurrence. This would create a strong disincentive to further participation in any such system. In contrast, the purpose behind their removal is to act in the operator's own interest and to preserve the continued safety of their system. In some industries, the knock-on effects of such actions may have relatively minor implications for the operation of the system as a whole. In other industries, the removal of key personnel can impose considerable practical burdens on their colleagues who must continue to operate their systems. These problems are likely to be exacerbated by the fact that many incidents occur during periods of peak workload. As a result, incident reporting systems are often integrated into more general techniques for contingency planning during safety-related failures. The removal of key members of staff can, of course, have further safety implications if their replacements are less well trained, fatigued or nervous about stepping into their roles in the aftermath of an incident. Irrespective of the immediate decision, it must also be determined whether or not an operator should be allowed to return to normal operations or should be relieved for an extended period. This decision has important implications if an investigation determines that inadequate training was a contributory factor to any incident. Clearly such decisions should not be devolved to the person receiving an initial report but must be the shared responsibility of operational and safety managers within the organisation.

It may not be possible for operators to be removed from their duties in confidential or anonymous schemes without raising the suspicion of their colleagues and supervisors. In an open system, however, the removal of staff involved in an incident helps to reduce the likelihood of further failures in the aftermath of an adverse occurrence. It also provide a number of additional benefits. For instance, it can provide an opportunity for those individuals to complete reporting forms while the details of an incident are still 'fresh' in their mind. It also creates an opportunity for the stress management and peer counselling services that are increasingly being introduced in safety-critical industries. These activities are intended to combat the sense of guilt and blame that often arise in the aftermath of an incident. Wu provides a direct impression of the problems that these feelings can cause in the medical domain:

> "In the absence of mechanisms for healing, physicians find dysfunctional ways to protect themselves. They often respond to their own mistakes with anger and projection of blame, and may act defensively or callously and blame or scold the patient or other members of the healthcare team. Distress escalates in the face of a malpractice suit. In the long run some physicians are deeply wounded, lose their nerve, burn out, or seek solace in alcohol or drugs. My observation is that this number includes some of our most reflective and sensitive colleagues, perhaps most susceptible to injury from their own mistakes.
>
> What should we do when a colleague makes a mistake? How would we like others to react to our mistakes? How can we make it feel safe to talk about mistakes? In the case of an individual colleague it is important to encourage a description of what happened, and to begin by accepting this assessment and not minimising the importance of the mistake. Disclosing one's own experience of mistakes can reduce the colleague's sense of isolation. It is helpful to ask about and acknowledge the emotional impact of the mistake and ask how the colleague is coping." [878]

Such counselling helps to maintain valuable human resources, for example, by reducing the likelihood of needing the additional costs of staff replacement. Many organisations provide these services through a peers group who are chosen by the workers themselves and who complete an appropriate training course.

Is the Report Relevant?

As mentioned above, the person or group who initially receives an incident report must determine whether or not the incident falls with in the scope of the system Two different sets of problems are created depending on whether the incident is considered 'appropriate' or not.

If the initial receivers of an incident report believe that it does not fall within the scope of the system then they must reject it. This creates the possibility that important lessons about previous failures will be excluded from the system. In national and international systems, it is also possible that different regional definitions of relevance will lead to inconsistency and bias in the information that is collected. As a result, many organisations publish exhaustive lists of those sorts of incidents that fall within the scope of the system. Some of these lists were considered in the opening chapter of this book when it was argued that it can be extremely difficult to support such exhaustive definitions in complex and dynamic industries where the nature of those failure that are observed will change over time. The problems of determining whether or not an incident falls within the scope of the system are not simply related to technological change. They also relate to the political and organisational environment that support the reporting system. For example, the US Federal Railways Administration published the following exemptions in response to industry objections to the burdens imposed by an occupational injury reporting system:

> Partial relief to certain small railroads generally covered by Part 225. FRA recognises that small operations are concerned with the burdens, both in terms of time and expense, associated with full implementation of the amendments to Part 225 issued in 1996. Based on additional analyses, FRA concludes that it can grant partial relief to certain small operations without compromising the accuracy of its accident reporting data base. These operations are: 1. Railroads that operate or own track on the general railroad system of transportation that have 15 or fewer employees covered by the hours of service law ... and 2. Railroads that operate or own track exclusively off the general system... If your railroad is subject to Part 225 at all and falls in either of the above categories, then you need not adopt and comply with components 3 through 10 of the Internal Control Plan requirements in Section 225.33. See Section 225.33(a)(3)-(10). However, you must fulfill the requirements of components 1 and 2, which require a stated policy dealing with harassment and intimidation. See Section 225.33(a)(1)-(2). To assist railroads in developing this policy, the FRA has provided suggested language, found in Appendix I to this Guide, that may be used. A railroad in either of these two categories is also exempted from the requirements in Section 225.25(a)-(g) to record accountable injuries and illnesses and accountable rail equipment accidents. (See Chapter 2 for definition of accountable events.) You must also, however, maintain a Railroad Employee Injury and/or Illness Record of any reportable condition of one of your employees. (See Chapter 4.) Additionally, a railroad that is generally subject to Part 225 but that operates exclusively off the general system (including off-the-general-system museum and tourist railroads) is not required to report or record an injury or illness of any person that results from a non-train incident, unless the non-train incident involves in-service railroad equipment. See definition of non-train incident in Chapter 2. Railroads that are subject to Part 225 in the first place and that operate exclusively off the general system must, however, continue to comply with Part 225 requirements regarding reporting and recording injuries and illnesses incurred by any person that result from a train accident, train incident, or a small subset of non-train incidents that involve railroad equipment in operation but not moving." [235]

If the person receiving a report can interpret such exceptions and, nevertheless, determines that the incident does fall with the scope of the system then this raises further problems. For example, they must ensure a consistent response to an incident. This is particularly important during the immediate aftermath of an incident when effective action can be taken to mitigate adverse consequences. As we shall see, if these actions are delayed or if 'inappropriate' actions are taken then the net result can be to exacerbate an already serious situation. If the entire decision to investigate an occurrence report is incorrect then this can waster scarce resources and may ultimately convince higher levels of management that the benefits that are derived from the system may not meet the expenditure that is required by the 'false alarms'.

How to Provide Immediate Feedback?

The person who initially receives an incident report must, as mentioned previously, assess its criticality and, if appropriate, must pass it on for further consideration and analysis. If the incident has clear implications for the continued safety of the system then the individual receiving the initial report must directly inform their safety managers so that interim corrective actions can be immediately instigated throughout the organisation. Such notifications have other benefits. While compiling material for this book, I learned of several occasions during which safety managers first learned of critical incidents when a member of the television or press contacted them for their reactions. The notifications of that incident were slowly being passed through the intervening managerment structures of the organisation concerned. Such communications failures have important implications not only for public relations but also for the effective response to incidents and accidents.

Whether or not the immediate recipient of an incident report decides that it falls within the scope of a reporting system, there are two further duties that must be performed in most reporting systems. The first is to inform the contributors, in open or confidential systems, that their reports are being dealt with. This is critical to preserve the trust and coincidence of the participants in the scheme. In the past, completed incident reporting forms have been found in the bottom of supervisors' desks, in pending trays over a month after submission and even in waste paper baskets. One means of avoiding such problems is to develop an auditable paper trail of receipts from the point of submission. This enables those who are responsible for administering a system to trace any potential 'bottle necks'. Many of the organisations, such as the Swedish Air Traffic Control organisation, that exploit these systems have recently turned to electronic implementations that automate the monitoring process and provide staff with feedback on the handling of a report at all stages of the process.

The second documentary obligation on staff receiving an incident report is to provide a written justification of their decision either to proceed with the report, or arguably more importantly, to explain why they decided to drop it. The former is important if incident investigators are to understand why an initial report was passed on for consideration. The later is critical if internal quality control bodies or external regulators are to monitor and approve of decisions that remove potentially critical reports from any subsequent investigation. The importance of this documentation cannot be underestimated. The disclosure laws in several countries make it imperative that such explanations are available. If an initial occurrence report is not investigated and the circumstances of that incident are later replicated by an accident then the potential legal consequences are considerable.

4.1.3 Incident Investigators

Incident investigators conduct the detailed analysis that follows an occurrence report. Rasmussen identified three different diagnostic roles that can be associated with this analysis: analyst, attorney or repairman [697]. These different roles, in part, reflect the difficult of their task. Diagnosis is, however, one one aspect of their duties. They must determine whether any further data acquisition is required, for instance by interviewing more contributors or by examining records from automated logging equipment. Ideally, there investigators work in teams of two or three. This helps to promote the necessary mix of domain-specific, human factors and technical skills. There are also benefits in conducting various interview and elicitation procedures with more than one investigator. The additional expense of forming such groups is, however, beyond the means that are available to many incident reporting systems.

Investigators operate at a local, regional or national level. Given that most reporting systems have a relatively low number of high criticality incidents, many schemes rely upon a small number of highly-skilled investigators. These individuals operate from national or regional centres. However, the additional skills and expertise of such investigators must be balanced against the potential problems of sending 'strangers' to investigate the circumstances of particular incidents in local units. In contrast, other systems have trained larger numbers of investigators who can be appointed from the staff within individual units. This reduces the problems that individuals experience when attempting to understand the working practices of teams that they have not previously met or interacted with. The limitations with this approach are, however, that any investigation can be compromised if the divide between operational and investigatory roles becomes blurred. Investigators may be unwilling to implicate their friends and colleagues. ICAO Annex 13, paragraph 3.1 states that incident investigation is part of the safety improvement process and not part of the operational management of an organisation [386].

What Training do I Need?

The coherent and consistent analysis of occurrences depends upon the careful selection of investigators. They are responsible for drafting the final occurrence report and for submitting it to the appropriate regulatory authority. Recruitment must, therefore, focus on appropriate personality traits. They must be well-organised, meticulous, unbiased, effective communicators etc. These attributes cannot simply be assessed a priori but must be measured and inspected throughout their careers as incident investigators. For example, it is important to determine whether investigators are biased towards certain causal factors in their analysis and interpretation of incidents. It is also important to determine whether investigators continue to consider an appropriate range of recommended remedial actions.

The quality control measures, proposed in the previous paragraph, provide insights into the effectiveness of the training that is provided for incident investigators. Specialised training into the nature and causes of incidents must build upon a detailed knowledge of the working domain. The following list identifies a number of more detailed training requirements:

- *Domain expertise.* Any investigation team must be led by a manager who is competent in the application domain. For instance, it is anticipated that incident investigators will have between five and ten years experience within an Air Traffic Control centre before they are qualified to perform such a role. The meta-level requirement for domain expertise hides a number of more detailed issues. They should understand the working practices of the team that noted the occurrence. They should have a clear view of relevant legislation, regulation and protocols. Their expertise should also be recognised and trusted by employee representatives.

- *Incident investigation expertise.* Chapter 2.3 has reviewed a number of competing theories and models that describe the ways in which incidents and accidents can occur. The ideas presented in this chapter have different degrees of importance in the training of incident investigators. For instance the previous chapter contrasted Sagan's ideas about high reliability organisations with Perrow's work on normal accidents. It is important for accident investigators to have at least a superficial understanding of these different positions. However, it is essential that accident investigators understand the practical implications of the 'systems approach' to accidents. Similarly, Reason's work on the latent and catalytic causes of failure underpins most recent work in incident investigation.

- *Technical and engineering expertise.* Incident investigators must either posses or have access to specialist knowledge about potential hardware and software failure 'modes'. This is increasingly important as automation enduced failures, typically, emerge from the interaction between a number of component subsystems. It is difficult to under-emphasise the technical challenges that are posed by an investigation and analysis of these incidents. For instance, the integration of application processes can lead to a number of failures that have little superficial connection but which share a number of common causes. Such similarities can only be detected if investigators have considerable technical and engineering skills [416].

- *Human factors expertise.* Given the prominence of human factors in the causation, detection and mitigation of many occurrences, it is necessary to identify a source of human factors expertise for investigators to call upon. This raises a number of pragmatic difficulties. In particular, it is important to emphasise that the analysis of human factors in incident investigation is typically a complex and skilled task. Just as technical and engineering analysis requires competent, specialist training, so does the analysis of human failure. For example, it is often difficult to categorise an error according to a predetermined category. It is critically important to identify and understand those factors that contributed to the error and that helped to shape the operators response to any initial failure.

This is a partial list. More detailed requirements can be identified for particular industries. Additional training requirements can also be identified if investigators must work at the interface between different industries or professions. Air traffic control investigator must understand not the working practices of other controllers but also of pilots. Medical investigators may have to understand the priorities and concerns of several different clinical disciplines.

What Are My Duties?

In order for investigators to complete any analysis of an incident it is important that they have the necessary authority to access all relevant sources of information. This includes immediate access to logs from automated data sources. Investigators must be able to make copies of this information and be able to protect the original logs. They must also have the right to interview key personnel in the aftermath of an adverse occurrence. This can lead to conflict if those members of staff are required for other duties or if they have been excused from duty for psychological or physiological reasons.

Along with these rights, investigators must also fulfill a number of general and specific obligations both to the staff members involved in an incident and to the rest of the safety management structures within their organisation [68]. These general duties include an obligation to ensure a full, independent and objective investigation. To ensure that any investigation and analysis is conducted with the knowledge and participation of operational staff; within the bounds defined by the confidentiality policy that is being used. Investigators must ensure that all relevant documentation is identified, compiled and protected so that subsequent reviews can re-trace the arguments that support their findings. They must also assess the validity and integrity of data that is gathered during any analysis. They must interview all staff who are involved in an occurrenc, again within tbounds specified by the confidentiality policy. They must compile and submit both an initial assessment of the occurrence, typically within 3-10 days of the event, and a final report to their organisation's safety managers. These documents must at a minimum contain an analysis of the occurrence and either interim or final recommendations. They must also ensure that these reports, or a digest, are made available to operational staff so that they can both learn of the outcome of the investigation and see what actions have been identified following from a report.

As mentioned above, investigators must also fulfill a number of obligations that relate more narrowly to the treatment of data that is gathered during any investigation. In particular, access to this data should be restricted to a relatively small number of authorised personnel. If this policy is not enforced then there are strong dangers that data may be lost, corrupted or challenged during any subsequent analysis. It is also important to clearly define permissable uses for the data. For instance, it may only be used for investigating the specific occurrence for which it was gathered. Alternatively, personnel may be told that data will be retained and used to spot emerging trends. In either case, there may be considerable consequences if staff feel that information is retained to monitor individual performance rather than to support more general safety improvements.

4.1.4 Safety Managers

As mentioned previously, each of the roles in this section is generic in the sense that they do not refer to specific posts within a management structure. Instead, they refer to a set of duties or obligations that must be fulfilled in order for an incident reporting system to be effective within an organisation. Safety Managers are ultimately responsible for the operation of the reporting system. They oversee that appointment and working activities of investigators. Together with the regulator, they must also ensure that the recommendations in an occurrence report are acted upon.

How to Resist the Pressure?

Safety managers act as the interface between the investigatory process and many other groups both inside and outside their own organisation. They must propagate information from incident investigators to higher levels of management. This may liaise with training 'departments', with operational staff and with acquisitions groups to ensure that recommendations are implemented throughout the organisation. They must liaise with regulatory authorities and, in more severe incidents, with external investigatory bodies. They may also be expected to liaise either directly with the media or indirectly through public relations organisations. These multiple roles create demands that cannot be underestimated. As noted in previous chapters, they help to account for the way in which local systems are often heavily dependent upon the support of the key individuals that perform this role. In national and regional systems, these pressures can lead to considerable personal stress that may ultimately threaten the success of any incident reporting system. In preparing this book, I interviewed several safety managers who emphasised the invidious nature of their task. They argued cogently that responsibility for the performance of their duties ultimately rested both personally with themselves but also corporately with the directors and managers who must support their actions.

It is very important that safety managers receive adequate protection from the influences that can be exerted on them. For example, it is difficult or impossible to sustain incident reporting functions without a stable budget. This does not imply that infinite resources are required to support the system. It does, however, suggest that frequent cuts without careful planning can and do send inappropriate messages to the staff who must participate in the system. It remains to be seen whether the recent decision to reduce the number of publications of the ASRS' DirectLine journal will have an impact upon the submissions that are made to this system.

Safety managers have further responsibilities. They must protect investigators from undue pressure. External and internal sources can seek to influence the course of an investigation in the hope of having some effect both on the analysis and the recommendations. These pressures can be introduced in covert and discrete ways, through informal meetings, through hints or second-hand reports of the opinions of others within an organisation. In practice, it is difficult or impossible to isolate investigators from these factors. All that safety managers can realistically hope to achieve is to provide investigators with the necessary support so that they can resist the more pernicious influences.

Who Do I Report To?

As mentioned above, safety managers must establish and preserve the communications channels that disseminate lessons from previous incidents. They help to ensure that other groups within the organisation are warned about the potential for similar incidents. This can be done through team briefings, through internal journals or newsletters and increasingly through the electronic media provided by intranets. In practice, however, many of these duties are delegated to incident investigation teams. The safety manager is ultimately responsible for the adequate completion of these tasks.

Safety managers are also responsible for monitoring trend information. For instance, they must encourage participation in an incident reporting system across all geographical regions and managerial groups. They must not only monitor participation rates but must also look for trends of similar incidents that can emerge over time. This task may also involve collaboration with managers of other organisations within the same industry. Of course, this can only be achieved where safety considerations are perceived to be more important than any competitive advantage that might be lost through the exchange of data.

Safety managers must also assess the recommendations that are made by their investigators. Together with operational staff, they can be required to prioritise those recommendations and justify decisions to wither adopt or reject particular findings. They must monitor the implementation of those recommendations that are accepted. They must also monitor the effectiveness of any remedial actions to ensure that they have adequately protected the system against future failures.

Safety managers must prepare briefing documents that are passed to the highest level of management within their organisation. It is, therefore, critical that they have a right of access to upper management. Incident reporting systems are often introduced as a means of improving communication about potential failures within an organisation. The effectiveness of this role will be impaired if all such communication stops with the safety manager. There is also a danger that under such circumstances, managers will only accept recommendations that are amenable to short term fixes [411]. Additional board level support is often required to approve longer term operational changes.

Safety managers must also communicate potential hazards to other groups outside of their own organisations. This can be achieved via a regulatory body. It is important that safety managers have means of communicating directly with the groups or individuals who must intervene to regulate their market. As mentioned in previous chapters, safety managers are, typically, required to provide them with incident statistics. Again, however, safety managers often supplement this information with more pro-active information about wider safety concerns based on their operation experience. A Machiavellian interpretation of this would be that safety managers may predispose the regulator to a positive view of their safety culture. A less cynical interpretation is that this encourages the regulator to fulfill their role as a medium of exchange for safety-related information across an industry.

4.1.5 Regulators

Section 3.1 introduced the role of the regulator by focusing on the ultimate responsibility that they, arguably, hold for failures within an industry. In contrast, this section focuses on the role of the regulator in creating the necessary preconditions for the effective exchange of information through incident reporting. The regulator monitors the performance of the occurrence reporting system as part of the wider safety management processes that are adopted by the management. They often receive copies of all final reports into occurrences as well as reports from the safety managers that describe the measures that have been taken to implement any safety recommendations. Regulators may initiate periodic investigations into particular problems should they continue to receive occurrence reports about similar incidents.

When Do We Regulate?

At a more detailed level, regulators are typically involved in encouraging organisations to establish incident reporting systems. This is often perceived to be part of a wider requirement to encourage safety management programs within their industry. In some sectors, regulators must ensure that organisations meet international obligations:

> “(The assembly) urges all Contracting States to ensure that their aircraft oper ators, providers of air navigation services and equipment, and maintenance organisations have the necessary procedures and policies for voluntary reporting of events that could affect aviation safety” (ICAO Resolution A32-15: ICAO Global Aviation Safety Plan)

However, there are many constraints on the ways in which regulators can intervene to achieve these objectives. As we have seen, OSHA’s Cooperative Compliance Programme failed to establish incident reporting as a means of improving safety culture. Employers groups opposed this initiative because it may have placed undue burdens in competitive markets and potentially increased the influence of Federal organisations.

It is again important to emphasise that this section deals with the role and not the office of the regulator. The duties that are associated with regulatory bodies in some industries may, in other industries, be distributed across many organisations. Similarly, they may not be performed at all owing to the nature of the markets that are involved. Healthcare provides an important example of this point. Although some elements of regulation can be associated with the US Food and Drug Administration, there role is primarily focussed on the safety of devices, pharmaceuticals and other products utilised by the medical sector. They do not and have not, typically, been involved in monitoring other adverse occurrences. As a result, the Institute of Medicine report led to the drafting of the Patient Safety and Errors Reduction Act, S.2738, that was introduced into the Senate in 2000. This seeks to establish a national Center for Quality Improvement and Patient Safety under the leadership of a Director who must:

> '(D) develop a confidential national safety database of medical errors reports;
>
> (E) conduct and support research, using the database developed under subparagraph (D), into the causes and potential interventions to decrease the incidence of medical errors and close calls; and
>
> (F) ensure that information contained in the national database developed under subparagraph (D) does not include specific patient, health care provider, or provider of service identifiers.
>
> (2) NATIONAL PATIENT SAFETY DATABASE- The Director shall, in accordance with paragraph (D), establish a confidential national safety database (to be known as the National Patient Safety Database) of reports of medical errors and close calls that can be used only for research to improve the quality and safety of patient care. In developing and managing the National Patient Safety Database, the Director shall–
>
> (A) ensure that the database can only be used for its intended purpose;
>
> (B) ensure that the database is as comprehensive as possible by aggregating data from Federal, State, and private sector patient safety reporting systems;
>
> (C) conduct and support research on the most common medical errors and close calls, their causes, and potential interventions to reduce medical errors and improve the quality and safety of patient care;
>
> (D) report findings made by the Director, based on the data in the database, to clinicians, individuals who manage health care facilities, systems, and plans, patients, and other individuals who can act appropriately to improve patient safety; and
>
> (E) develop a rapid response capacity to provide alerts when specific health care practices pose an imminent threat to patients or health care workers.
>
> (3) CONFIDENTIALITY AND PEER REVIEW PROTECTIONS- Notwithstanding any other provision of law any information (including any data, reports, records, memoranda, analyses, statements, and other communications) developed by or on behalf of a health care provider or provider of services with respect to a medical event, that is contained in the National Patient Safety Database shall be confidential in accordance with section 925.
>
> (4) PATIENT SAFETY REPORTING SYSTEMS- The Director shall identify public and private sector patient safety reporting systems and build scientific knowledge and understanding regarding the most effective–
>
> (A) components of patient safety reporting systems; (B) incentives intended to increase the rate of error reporting; (C) approaches for undertaking root cause analyses; (D) ways to provide feedback to those filing error reports; (E) techniques and tools for collecting, integrating, and analysing patient safety data; and (F) ways to provide meaningful information to patients, consumers, and purchasers'

I view this as a form of regulation because it is an attempt to intervene in the existing market place in a manner that is intended to improve the safety of patients (and staff) within the US healthcare system. In some countries, 'regulation' is a pejorative term that is often associated with ideas of government 'over-regulation'. Those who read the Institute of Medicine report can, however, see that it's authors were careful to balance this fear of intrusion in the marketplace against the need to address the consequences of human error in medicine [481]. Those same concerns are apparent in this draft of the Act.

Not only must regulators help to establish incident reporting systems, they must also monitor their operation. As we shall see, this is a non-trivial exercise. There is the obvious paradox that a relatively low number of reported incidents may indicate a high degree of safety within an organisation or a relatively low participation rate. Similarly, it can be difficult to determine whether the investigatory procedures that lead to a criticality assessment of each incident are implemented in the same manner across different organisations. For instance, some European Air Traffic Service provides classify the severity of an incident according to its worst plausible outcome . An air proximity violation that was resolved by the actions of the crew might, therefore, be treated as if a collision had occurred because ATS personnel had not intervened to avoid the incident from become more serious. Other organisations within the same industry would treat this as a far less serious incident. Under this vew, the aircrew are perceived to form part of the wider safety system. A collision was avoided and hence that system functioned as intended.

Regulators must intervene to support the exchange of safety-related information throughout an industry. This responsibility is a repeated theme in the Patient Safety and Errors Reduction Act cited above. However, it can also be seen in the regulatory structures that govern other industries. For instance, the regulatory safety functions of the UK rail industry are performed by the Railways Inspectorate within the Health and Safety Commission of the Health and Safety Executive. In contrast, the economic functions associated with performance measurement, standard setting and price monitoring are performed by the office of the Rail Regulator. The regulatory role of the Health and Safety Commission in establishing confidential incident reporting schemes can be seen in their action plan to implement the recommendations of the recent inquiry into the Southall rail crash:

> "All parties in the rail industry should co-operate in the collection of evidence to support reliable research into human behaviour studies relating to driver performance. Railtrack should co-ordinate this work and TOCs (Train Operating Companies) incorporate the results into training programmes (paras 1.25, 7.16, 16.2).
>
> Evidence should include that to be provided by CIRAS (Confidential Incident and Reporting System) and from On-Train Data Recorders used to monitor driver behaviour. ASLEF (Associated Society of Locomotive Engineers and Firemen) in particular should give their full support to such an initiative (paras 14.23, 14.25, 15.15, 16.3).
>
> Comment: Much of the information required for the human factors work on driver behaviour (Recommendation 1) will be provided by train operators. Most TOCs have already agreed to enroll their drivers in CIRAS (or equivalent confidential reporting systems) following the Rail Summit; coverage should be complete nationally with all staff briefed by 1 April 2001. Individual TOCs agree to interrogate and provide data analysis of on-train data recorders or from other available means of recording driver activity. ASLEF and RMT (National Union of Rail, Maritime and Transport workers) support approach, subject to confidentiality reassurances. HSC (Health and Safety Commission) agrees that this action should be on individual train (both passenger and freight) operators. Action: Individual TOCs to submit a progress report to HSC confirming their active participation in providing human factors data to Railtrack and enrollment of driver in CIRAS. ATOC (Association of Train Operating Companies) to set up a system to identify good practice on how driver behaviour is to be monitored using OTDRs (On train data recorders). Progress report to be submitted to the HSC." [319].

The Health and Safety Commission are intervening to ensure that all parties in the rail industry cooperate to collect evidence about the human factors problems that affect driver performance. All train operating companies must establish a confidential incident reporting system, similar to CIRAS mentioned in previous chapters. These companies must, in turn, agree to provide access to the data that is obtained by these systems.

The previous paragraph has argued that regulators play a role in the collection and dissemination of information within an industry. This may clearly involve a delicate balance between the promotion of safety and the exchange of commercially sensitive information. This balancing act becomes even more complex when regulators attempt to promote the exchange of information across national boundaries:

> "The Board's focus extends beyond the United States' borders. Realizing that chemical accidents may have global health, environmental and economic effects, Congress encouraged the Board to offer investigative assistance to other countries, both as a means of helping and as a method of learning. Through its international outreach efforts to

> government and industry, the Board can ensure its safety research program, professional services and technical information accurately and adequately address the world's chemical safety needs". [163]

The sensitivity of the information that is often provided by incident reporting systems perhaps accounts for the notable lack of success in achieving the international collaboration that many regulators envisage. However, this view is being challenged by recent commercial initiatives to encourage the exchange of occurrence data within the aviation industry [310]. The GAIN system, introduced in Chapter 1.3 has over the last three years been transferred away from the FAA to the airline industry itself [681]. At present, GAIN simply acts as a clearing house for data gathered by other public sources including the ASRS and FAA incident reporting schemes. In the future, however, it may provide greater opportunities for the exchange of data directly between aviation operating companies even though that data is unlikely to be publically accessible to the same extent as the ASRS sources.

What Information Do We Need?

The previous section described the role of the regulator in setting up and monitoring incident reporting systems. They must also ensure that the output from these systems is collated, analysed and effectively used to address safety-related problems that arise across an industry or between several industries. This duty can be stated relatively simply. However, it is far harder to achieve. This difficulty of performing this task can be illustrated by the FDA's Manufacturer and User Facility Device Experience Database (MAUDE) [270]. This tool represents a significant advance on many existing regulatory incident reporting systems because it provides manufacturers and operators with an accessible means of looking for information about previous incidents. Techncial details about this system will be provided in Chapter 13.5 and the interface to this system is illustrated in Figure 14.4. Users can access incident data in the MAUDE database by selecting a number of predefined categories or by entering a free-text search. The following quotation illustrates the types of data that can be retrieved using this system:

> "Adverse event or product problem description: A susceptibility report message, which the microbiology lab uses as an indicator for verifying oxacillin results did not print on a pt lab report from the ... instrument. The lab did not verify ... results on this pt's blood culture report. The pt's physician has stated that as a result of a lab error, a treatment error occurred leading to development of an abscess. This abscess has put pressure on the pt's spinal cord causing paralysis of the legs.
>
> Additional manufacturer narrative: An investigation into the customer complaint determined that a message, which previously printed on the instrument lab report, no longer prints with the release of a new software version.
>
> ...[It could not be concluded] that lack of this message caused or contributed any negative effects to the pts condition ased on the following points: 1. subsequent blood cultures were negative after treatment with oxacillin. 2. the lab did not save the original isolate from the blood culture used for testing on the system. 3. this pt had a previous history of a oxacillin resistant staph aureus infection. 4. treatment of an abscess, regardless of culture and susceptibility results, routinely requires more intervention than simply administering antibiotics. The message for oxacillin will be added to the lab reports with the next software release. All customers will be notified immediately by letter concerning the missing message when the oxacillin indicator antibiotics are resistant"

The MAUDE system is important because it illustrates the ways in which regulators can intervene to act as a clearing-house for incident data. The development of search engines, for the first time, provides users with the opportunity to identify common trends across an industry. However, the previous examples also illustrate some of the challenges that are facing such regulatory action. In particular, the previous search for software related incidents yielded five hundred hits amongst the MAUDE collection. At this point the system halted its search and prompted me to refine my search because there was too much relevant data. In some senses this reflects the way in which incident reporting systems can become victims of their own success. For instance, the ASRS system know holds over 500,000 records. Later section will describe software engineering and information management tools that can be used to address these problems and still enable users to identify common trends amongst a growing mass of incident data.

4.2 Different Anatomies

The previous section has summarised a number of the key roles that support incident reporting. In contrast, however, this section goes beyond these roles to look at a number of different reporting architectures. These architectures reflect the organisation that is necessary to collect incident reports, analyse them and then make recommendations. Clearly, the managerial structures that are necessary to support large national and international systems are unlikely to be appropriate or even necessary in smaller scale local and regional systems. This section, therefore, provides a brief overview of a number of different ways in which incident reporting systems can be managed.

4.2.1 Simple Monitoring Architectures

Figure 4.1 represents the simplest architecture for an incident reporting system. A contributor submits a report based on the occurrence that they have witnessed or are concerned about. This submission process can be implemented using printed forms, by telephone calls, or increasingly using computer-based techniques. An external agency received the report and after assessing whether or not it falls within the scope of the system they will decide whether or not to publish information about the occurrence. The contributor and others with the same industry can then read the report and any related analysis before taking appropriate corrective actions.

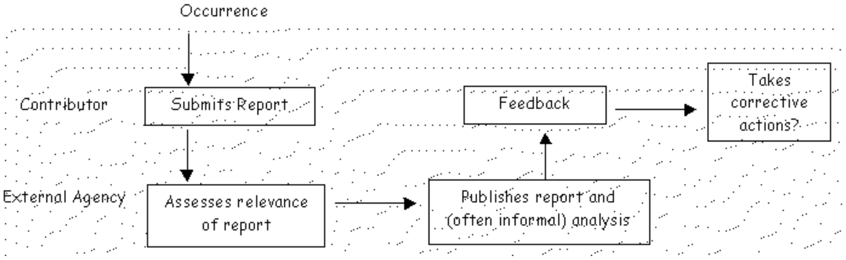
Occurrence
Contributor
Submits Report
Feedback
Takes corrective actions?
External Agency
Assesses relevance of report
Publishes report and (often informal) analysis

Figure 4.1: A Simple Monitoring Architecture

This approach is typified by the Swiss Confidential Incident Reporting in Anaesthesia system (CIRS) [756]. A web-based form is used to submit an incident report to the managers of the system. Given the sensitive nature of these incidents, this is an anonymous scheme. The managers cannot, therefore, conduct follow-up investigations. However, they do perform a high-level analysis of this and similar events before publishing a summary on their web site.

There are a number of limitations with the architecture shown in Figure 4.1. In particular, this simple monitoring approach simply provides a means of disseminating information about previous failures. There are no guarantees that individual organisations will take any necessary corrective actions. Similarly, there is a danger that different institutions will respond to the same incident in different ways. This inconsistency creates the opportunity for future failures if an organisation fails to correctly safeguard the system. A further problem is that this approach does not provide any means of determining whether reports were accurate or not. This creates potential dangers because a report may omit necessary information about the causes of an incident. As a result, other organisations might respond to the symptoms rather than the underlying problems that lead to an occurrence. As most of these systems are truly anonymous, it can be difficult or impossible for the managers of the scheme to identify whether any local, contextual factors contributed to an incident.

As with all of the architectures presented in this section, there exist a number of variations that have been used to structure existing systems. For instance, the US Food and Drug Administration's MAUDE system, mentioned above, cuts out the external agency and enables individuals to report directly to the regulator. These reports are then posted on the FDA's web site. If the incident is considered serious enough then the regulator may intervene through a product recall or amendment notice.

4.2.2 Regulated Monitoring Architectures

Figure 4.2 provides a high-level view of what we have termed the 'regulated monitoring' architecture for incident reporting. This is very similar to the approach described in the previous section. However, in this approach the external agency that received the contribution can go back and ask further questions to refine their understanding of an occurrence. Once they are clear about what has taken place, they produce a summary report that, typically, does not reveal the identity of their contributor. This summary is then placed before management and regulators who are responsible for identifying corrective actions. They must also determine whether those corrective actions can be implemented. The reporting agency will then receive a report on corrective actions that can then be communicated back to the original contributors and their colleagues through journal or newletter publications.

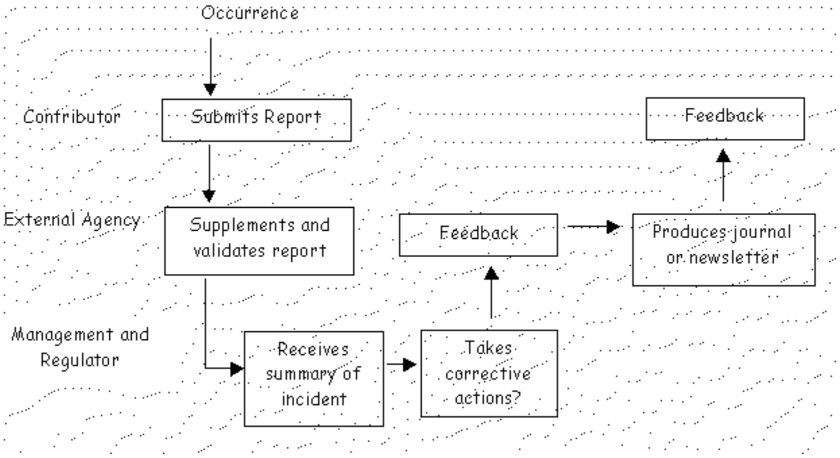
Occurrence
Contributor
Submits Report
Feedback
External Agency
Supplements and validates report
Feedback
Produces journal or newsletter
Management and Regulator
Receives summary of incident
Takes corrective actions?

Figure 4.2: Regulated Monitoring Reporting System

The Confidential Incident Reporting and Analysis System (CIRAS) is a good example of an incident reporting scheme that implements the high-level architecture illustrated in Figure 4.2. This receives paper-based forms from Scottish train drivers, maintenance engineers and other rail staff. A limited number of personnel are responsible for processing these forms. They will conduct follow-up interviews in-person or over the telephone. These calls are not made to the contributor's workplace for obvious reasons. The original report form is then returned to the employee. No copies are made. CIRAS staff type-up a record of the incident and conduct a preliminary analysis. However, all identifying information is removed from the report before it is submitted for further analysis. From this point it is impossible to link a particular report to a particular employee. The records are held on a non-networked and 'protected' database. This data itself is not revealed to industry management. However, summary reports are provided to management at three monthly intervals. This concern to preserve trust and protect confidentiality is emphasised by the fact that a unit within Strathclyde University employs the personnel who process the reports rather than the rail operators.

The FAA's ASRS provides a further example of the architecture illustrated in Figure 4.2. NASA plays the role of the external reporting agency. Feedback is provided through a number of publications, such as the Callback newsletter and the DirectLine journal. An important strength of the publications produced by this approach is that it provides a measures assessment of several incidents through the editors' analysis. It also enables staff to read an explanation of an incident through the words of their colleagues.

Again there are a number of limitation with the high-level architecture shown in Figure 4.2. These do not stem principally from the problems of accessing more detailed causal information, as was the case with simple monitoring architectures. In contrast, they stem from the additional costs and complexities that are introduced by external reporting agencies. In particular, it can be difficult to preserve an independent but co-operative relationship between the organisation's management and a reporting agency. This relationship can become particularly strained when the agency is responsible for identifying corrective or remedial actions that the management must then implement. The ALARP (as low as reasonably practicable) principle is often used to justify resource allocation. The subjective nature of this approach can lead to conflicts over the priority allocated to many remedial actions. There is also a danger that these schemes will resort to low-cost reminders [411]. In consequence, many schemes operate on a smaller-scale, more local level. These schemes rely upon the same individuals to both collect the data and take immediate remedial actions.

4.2.3 Local Oversight Architectures

Figure4.3 illustrates the architecture that typifies many locally operated, incident-reporting systems. In many ways, these schemes were the pioneers of the larger more elaborate systems that have been mentioned in the previous sections. Individual sponsors either witness other schemes or independently decide to set up their own. Staff are encouraged to pass on incident reports to them. Typically, this is in a confidential rather than an anonymous fashion. Even if the forms do not ask for identification information it is often possible for the sponsors to infer who is likely to have submitted a form given their local knowledge of shift patterns and working activities. The sponsors can supplement the reports from their own knowledge of the procedures and practices within a unit. This enables them to analyse and validate the submission before passing a summary to their management. In contrast to other architectures, however, they are in a position to take direct remedial action. This is, typically, published in a newsletter. These publications not only provide feedback, they are also intended to encourage further submissions.

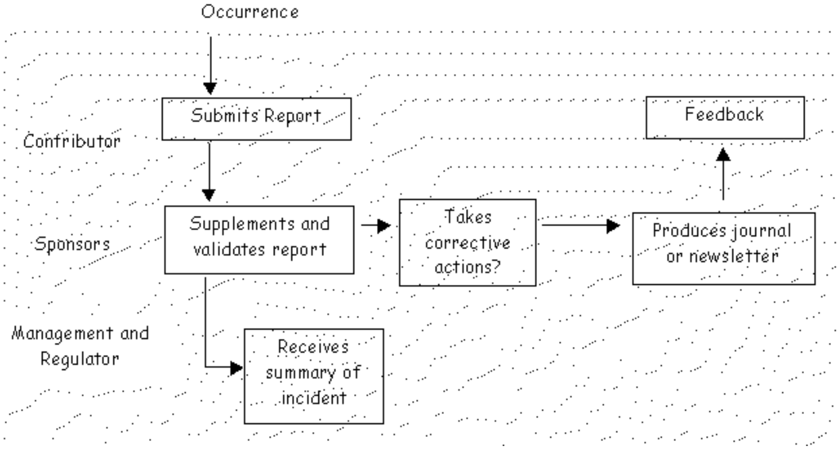
Occurrence
Submits Report
Feedback
Contributor
Supplements and validates report
Takes corrective actions?
Produces journal or newsletter
Sponsors
Management and Regulator
Receives summary of incident

Figure 4.3: Local Oversight Reporting System

Local oversight architectures are illustrated by one of the longest running medical incident reporting systems. David Wright, a consultant within the Intensive Care Unit of an Edinburgh hospital, established this system over ten years ago [119]. The unit has eight beds at its disposal with approximately three medical staff, one consultant, and up to eight nurses per shift on the ward. David Wright receives each report. They are then analysed with the help of a senior nurse. Any necessary corrective actions are instigated by them. Trust in the sponsor of this system is a primary concern, given the relatively close-knit working environment of an intensive care unit. The success of the system depends upon their reputation and enthusiasm. The extent of his role is indicated by the fact that less reports are submitted when David Wright is not personally running the system. The reports from these systems provide a valuable insight into problems in the particular practices and procedures that are followed within an organisation.

The strengths and weaknesses of such local systems are readily apparent. The intimate local knowledge and direct involvement with the contributors makes the interpretation and analysis of incident reports far easier than in other systems. However, it can be difficult to replace key personnel and sustain confidence in the system. It can also be difficult to drive through deeper structural or managerial changes from local systems. Individual sponsors often lack the necessary authority (or resources) to instigate such responses. As a result they often 'target the doable'. Similarly, it can be difficult to co-ordinate the efficient exchange of date between local systems to get a clearer overview of regional, national and even international trends.

4.2.4 Gatekeeper Architecture

Figure4.4 illustrates the architecture of several national incident-reporting systems. The increased scale of such systems usually implies the greater degree of managerial complexity apparent in this framework. The contributor submits a report to their local manager. They may then take some initial remedial actions and then passes the form to a 'gatekeeper'. They register the report; in any national system there is a danger that individual contributions may be lost or delayed. The gatekeeper has this name because they must determine whether the occurrence is important enough to allocate further analytical and investigatory resources. If this decision is made then they will delegate the report to another unit within the organisation that is responsible for the aspect of the system that was most directly affected by the occurrence. The report is passed to a handler within this service department and they attempt to identify means of resolving any potential problems. Feedback is then provided to the contributor via their local manager. This approach is, typically, confidential or open rather than anonymous.

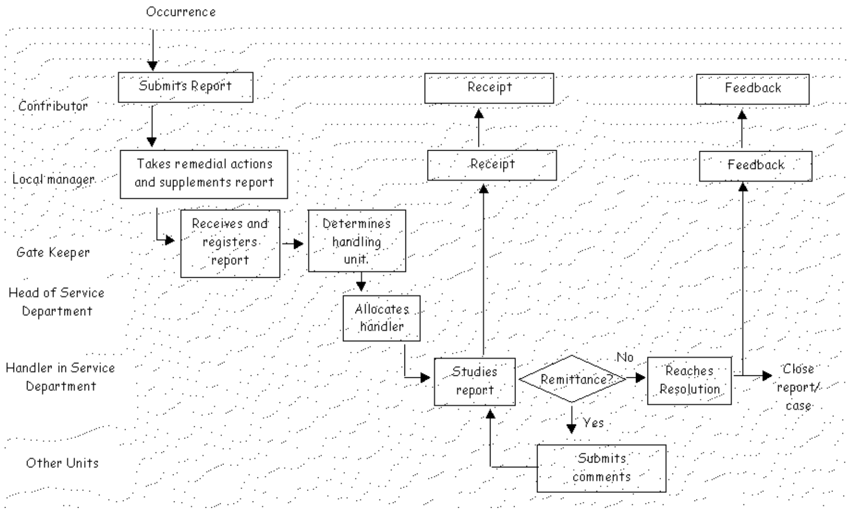

Figure 4.4: Gatekeeper Reporting System

This approach is exploited by the Swedish Air Traffic Control system. It is unusual in that it encourages the open reporting of a wide range of potential and observed failures. The definition of an 'occurrence' includes all forms of human, operational and technical failures even including incidents such as a failure of a light bulb. All reports are handled centrally by a number of specially trained gatekeepers who are responsible for filtering the reports and then passing them on to the relevant departments for action.

These individuals must be highly trained both in the application domain of air traffic control but also in the technical problems that lead to system failures. However, because all occurrence reports pass through their offices they gain a detailed understanding of both operator behaviour and system performance. The gatekeepers, therefore, are in a position to provide valuable information both to training directors but also to the risk assessments that guide future investment decisions.

The gatekeepers are an important strength of the system shown in Figure4.4. They are responsible for filtering reports and allocating remedial actions. This centralisation ensures a consistent analysis and response. However, they are a critical resource. There is a risk that they may act as a bottleneck if incidents are not handled promptly. This is particularly important because delays can occur while reports are sent from outlying areas to the gatekeeper's central offices. The Swedish system has addressed many of these criticisms by adopting a range of computer-based systems that keep safety managers and contributors constantly informed about the progress of every incident report. However, there remains the danger for many of these systems that any omissions in the training of a gatekeeper can result in incorrect decisions being made consistently at a national level.

4.2.5 Devolved Architecture

Figure4.5 provides an overview of an alternative architecture for a national system. Rather than have a central gatekeeper who decides whether an incident falls within the scope of the system, this approach relies upon a more decentralised policy. Any of the personnel involved in the system can decide to suspend an investigation providing that they justify their decision in writing and pass their analysis to the safety management group who monitors the scheme. As can be seen, contributors pass their reports to their supervisors. This is important because in many industries, such as air traffic control, the individuals who are involved in an incident will often be relieved of their duties. A sense of guilt can often affect their subsequent performance and this can endanger further lives. In national systems, it is often common to provide an alternative submission route through an independent agency in case a report is critical of the actions taken by a supervisor.

The supervisor takes any immediate actions that are necessary to safeguard the system and informs the safety management group if the incident is sufficiently serious. The safety management group may then commission an initial report from a specialist investigation unit. They may also decide to provide an immediate notification to other personnel about a potential problem under investigation. These investigators may call upon external experts. Depending on the conclusions of this initial report they may also be requested to produce a final report that will be communicated back to the safety management group. In a number of these systems, final reports are issued to the original contributors who can append any points of further clarification. The safety management group is then responsible for communicating the findings and for implementing any recommendations following discussions with the regulatory authorities.

Figure4.5 illustrates the complexities involved in organising nation and international reporting systems. It depends upon the co-ordination and co-operation of many different individuals and groups. However, such architectures are necessary when the problems of scale threaten to overwhelm systems based on the approach illustrated in Figure4.4. The problem with this system is that there is a greater chance of inconsistency because different staff determine how an occurrence is to be reported and investigated. Different supervisors may have different criteria for what constitutes an occurrence that should be passed on for further investigation. Most European air traffic control service providers have tackled this problem by publishing exhaustive guidelines on what should be reported. These guidelines are distributed to all personnel and are addressed during the training of control staff.

It is important to emphasise that this section has avoided normative arguments about the absolute value of the different architectures that have been presented. This is entirely deliberate. As suggested in the previous paragraph, we know very little about the impact of these different man-

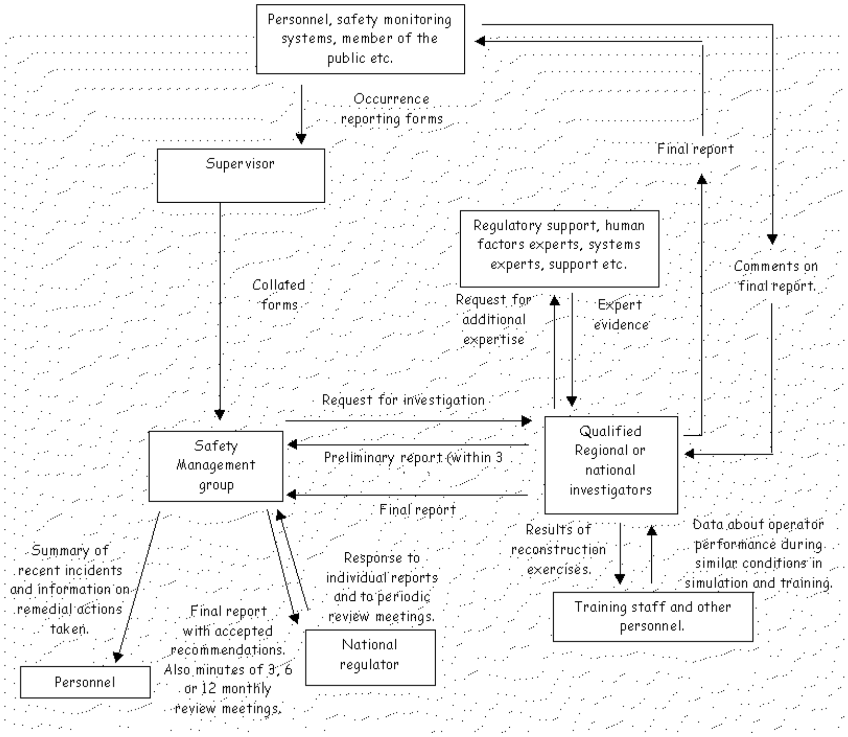
Personnel, safety monitoring systems, member of the public etc.
Occurrence reporting forms
Supervisor
Final report
Regulatory support, human factors experts, systems experts, support etc.
Comments on final report.
Collated forms
Request for additional expertise
Expert evidence
Request for investigation
Safety Management group
Preliminary report (within 3
Qualified Regional or national investigators
Final report
Results of reconstruction exercises.
Data about operator performance during similar conditions in simulation and training.
Summary of recent incidents and information on remedial actions taken.
Response to individual reports and to periodic review meetings.
Training staff and other personnel.
Final report with accepted recommendations. Also minutes of 3, 6 or 12 monthly review meetings.
National regulator
Personnel

Figure 4.5: Devolved Reporting System

agement structures. In consequence, it is difficult to be confident in any comparative analysis. Tools and techniques for performing such comparisons are urgently needed as incident reporting systems continue to proliferate in many different industries.

4.3 Summary

This chapter began by considering a number of different roles that together contribute to the successful operation of many incident reporting systems. These roles are generic in the sense that they represent key activities during the reporting, analysis and subsequent implementation of safety recommendations. These activities may be associated with particular individuals or with teams depending upon the scale and the organisation of the reporting scheme.

This chapter initially focussed on the reporting of adverse occurrences by individuals and groups in the workforce. The opening sections focussed on the rights and duties of these contributors. The next chapter will provide a greater consideration of the ways in which automated monitoring equipment can be used in the detection of adverse occurrences.

The following sections went on to consider the triage that is required when a report is initially received. Line managers and supervisors are, typically, required to secure the short term safety of the system in the aftermath of an incident. They must also pass on reports so that they can be processed in a prompt and efficient manner.

This chapter also looked at how information must be passed to incident investigators. We considered the powers that investigators must have if they are to elicit relevant information about an occurrence. Later sections also considered the training requirements and professional obligations that must be met by these individuals.

We went on to consider what we have described as the ‘invidious’ role of the safety manager. They act as a conduit of safety information from the workforce to higher management. They must also effectively communicate safety objectives from higher levels of management down to the workforce.

It was stressed that they must communicate effectively not only within their organisation but also to external bodies including industry regulators.

Regulators have been defined as organisations that intervene in the normal operation of the market to achieve economic and social objectives, such as improved safety, that might otherwise be overlooked. This chapter examined the tensions that arise when regulatory actions must balance the need to exchange safety information against the danger of forcing companies to pass on what might be commercially sensitive data. We also briefly considered nascent attempts by a commercial consortium to encourage the global exchange of incident information.

The second half of this chapter then went on to look at how these different roles contributed to different types of incident reporting system. Simple monitoring architectures simply provide a common point of access to incident reports. They are, typically, anonymous and so only a cursory validation can be performed. There are a number of limitations that restrict the utility of these systems, although they are simple to operate and can be established at low-cost. In particular, there is no guarantee that the submissions are genuine nor is there typically any guarantee that different institutions or investigators will arrive at a consistent interpretation of the events that are described.

Regulated monitoring architectures extend simple monitoring architectures by introducing an external agency that intervenes to validate and supplement any initial report. This additional validation increases the range of evidence that is available within the system and also helps to support any subsequent analysis of an adverse occurrence. However, the costs of maintaining such an external investigatory body are typically beyond the resources of most local systems.

Local oversight architectures rely upon key individuals or sponsors who can use their knowledge of a working environment to interpret and assess the reports that they receive. These individuals may perform additional validation and investigation but this need not always be necessary depending in their involvement in the target system. However, there is a danger that such systems are susceptible to the personal biases and training of these key sponsors. It can also be difficult to reestablish staff trust in any system when these individuals leave or take up other duties.

Gatekeeper architectures represent a more complex architecture in which a number of key individuals together perform the triage that might otherwise have been performed by a single individual within a local system. These individuals are trained to identify the severity of a report and to allocate a handling unit that is tasked to respond to that incident. However, in national and regional systems there is a danger that they may act as a bottleneck if incidents are not handled promptly. This is particularly important because delays can occur while reports are sent from outlying areas to the gatekeeper's central offices.

Finally, devolved architectures are intended to support large-scale national and international incident reporting systems. Information is passed through the different levels of an organisation up to a body of 'professional' incident investigators. These investigators report to the safety managers, mentioned above. Elaborations on this approach include several feedback mechanisms so that contributors are continually involved in the investigation and analysis process. Again, however, the costs associated with such a system would dissuade many industries from adopting every aspect of this approach.

As mentioned, the intention in this chapter has not been to recommend any particular architectures. In contrast, the intention has been, for the first time, to provide an overview of the different approaches that are currently being used within individual reporting systems. The following chapter builds on this analysis and begins to look in detail at key stages in the operation of an incident reporting system. These include: detection and notification; data gathering; reconstruction; analysis; recommendation and monitoring; reporting and exchange. As before, the intention is to provide a generic analysis of activities that are common to many different types of system. It is also intended the analysis provide pragmatic advice and guidance based on comparative studies of systems in several different industries.