Chapter 9

Modelling Notations

The previous chapter has introduced the growing number of computer-based simulation tools that can be used to reconstruct and replay the events leading to failure. As we have seen, however, these tools can be costly both to purchase and to apply to particular incidents. There is also the significant danger that they may bias investigators towards particular conclusions. For example, it is far easier to simulate the direct physical failure of component hardware than it is to model the managerial or regulatory failures that created the latent conditions for an incident. In consequence, this chapter introduces a number of notations that can be used to reconstruct the events leading to adverse occurrences. These techniques range from relatively 'intuitive' extensions to text-based time-lines through more complex graphical notations, such as Petri Nets, to mathematical logic. The intention is not to advocate a particular technique but to illustrate the costs and benefits of each approach. The final sections build on this analysis by presenting a list of requirements to be satisfied by any abstract notation for incident reconstruction.

9.1 Reconstruction Techniques

As we have seen, incidents may take many days, weeks or even years to develop [700]. As a result, a range of reconstruction techniques have been developed to help investigators represent and reason about the events that contribute to adverse occurrences. The following paragraphs briefly introduce a number of these approaches. These include graphical time-lines which provide a sketch of the events leading to an incident. We also consider the application of Fault trees to support the reconstruction of adverse occurrences. This diagrammatic techniques has been widely applied to support systems development and is, therefore, accessible to many engineers and investigators. Later sections also explore the use of Petri Nets reconstructions. This graphical notation is specifically intended to represent and reason about the complex temporal properties that characterise many incidents. A textual logic is then considered. This approach lacks the visual appeal of the graphical notations but has well-developed proof techniques that enable investigators to establish key properties of any reconstruction.

In order to illustrate the application of these different reconstruction techniques, the following sections analyse an incident involving the rupture of a natural gas distribution pipeline [589]. A 2-inch-diameter steel gas service line had been exposed during the excavation that was intended to help the with the removal of a 8,000 gallon buried fuel tank. The exposed pipeline separated at a compression coupling about 5 feet from the wall of a retirement home in Allentown, Pennsylvania. The escaping gas flowed underground, passed through openings in the building foundation. It then migrated to other floors in the retirement home before it exploded. The Allentown incident resulted in one fatality. The consequence criteria that were introduced in the opening chapters could, therefore, be used to argue that this is an accident and not a 'near-miss' incident. However, pragmatic and theoretical justifications support the decision to use this case study. The pragmatic explanation is that the subsequent National Transportation Safety Board (NTSB) report provides detailed information about the secondary investigation of this explosion. This provides public access to the sorts of details that often remain confidential within many commercial reporting systems. The theoretical justification for using this incident is that its consequences could have been very much worse. Many of the elderly residents of the retirement home were not in the building at the time of the explosion. A final motivation for using this incident is that it represents one of a number of similar incidents, the causes of which had arguably not been properly addressed by the pipeline and construction industries or their regulators.

9.1.1 Graphical Time Lines

Time-lines are one of the simplest means of representing the flow of events during major accidents. They simply translate the events on the text-based time-lines, which have been presented in previous paragraphs, onto a horizontal or vertical axis. Each event is mapped to a point on a line which stretches from the earliest to the lastest moment that is considered to be important to the analysis. For example, Figure 9.1 examines the regulatory environment in which the Allentown incident took place. In particular, this diagram provides a high-level overview of Appendix B of the NTSB's report. This natural language account is over twenty pages long. The graphical time-line does not replace the more detailed prose, however, it does provide an overview of the information that it contains. It focuses on the way in which the NTSB and groups within the Department of Transportation (DOT), in particular the Office of Pipeline Safety (OPS) within the Research and Special Programs Administration (RSPA), responded to previous incidents. In particular, it looks at the way in which recommendations to introduce Excess Flow Valves (EFVs) had limited uptake in the industry. The NTSB report argues that these devices could have mitigated the consequences of the Allentown incident. As can be seen, EFV devices were initially pioneered in the late 1960s. Incidents in 1968 and in 1972 had led the NTSB to recommend that the OPS develop standards for the use of protection devices such as EFVs. As a result, OPS recommend the installation of Excess Flow Valves (EFVs) in all new gas service lines and lines undergoing repair in 1974. Incidents continued to occur and later the same year, a Department of Transportation report recommended that EFVs be extended to customer lines. In 1976 the NTSB recommended their use in commercial premises. However, the Office of Pipeline Safety argued that the results of tests on these devices had proved to be inconclusive.

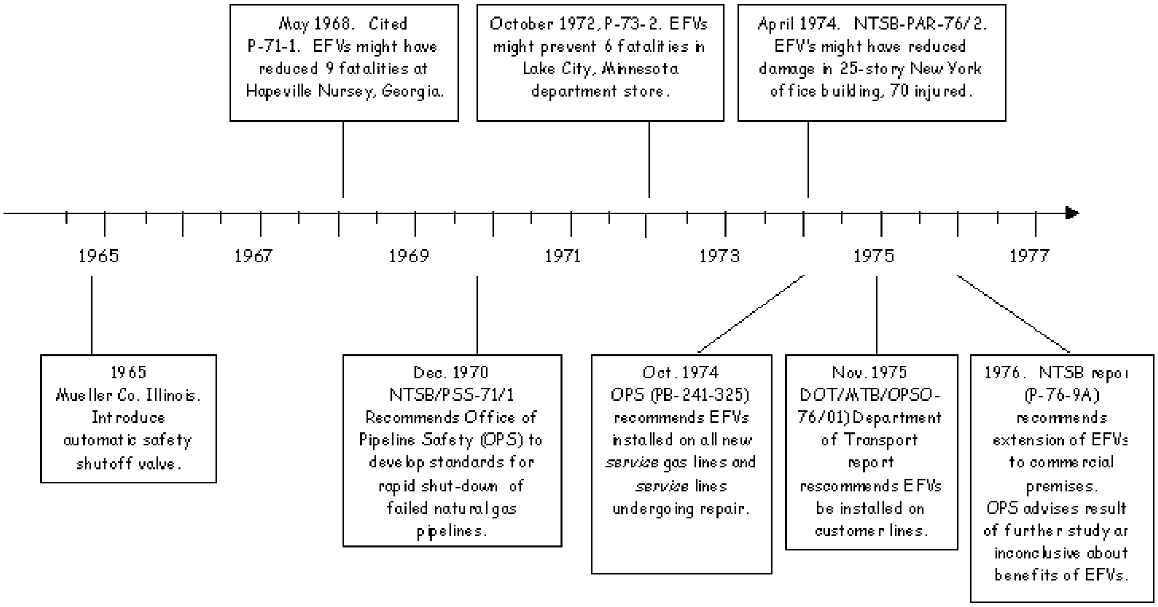

May 1968. Cited P-71-1. EFVs might have reduced 9 fatalities at Hapeville Nursey, Georgia.
October 1972, P-73-2. EFVs might prevent 6 fatalities in Lake City, Minnesota department store.
April 1974. NTSB-PAR-76/2. EFV's might have reduced damage in 25-story New York office building, 70 injured.
1965
1967
1969
1971
1973
1975
1977
1965 Mueller Co. Illinois. Introduce automatic safety shutoff valve.
Dec. 1970 NTSB/PSS-71/1 Recommends Office of Pipeline Safety (OPS) to develop standards for rapid shut-down of failed natural gas pipelines.
Oct. 1974 OPS (PB-241-325) recommends EFVs installed on all new *service* gas lines and *service* lines undergoing repair.
Nov. 1975 DOT/MTB/OPSO-76/01) Department of Transport report rescommends EFVs be installed on customer lines.
1976. NTSB repo (P-76-9A) recommends extension of EFVs to commercial premises. OPS advises result of further study ar inconclusive about benefits of EFVs.

Figure 9.1: Graphical Time-line Showing Initial Regulatory Background.

The spatial layout of this time-line is not simply used to indicate the flow of events over time. In

Figure 9.1 previous incidents are grouped above the line. The regulatory responses to those events are grouped below the line. This format is intended to show the impact the previous failures had on wider aspects of safety management within the pipeline and construction industries. Figure 9.1.1 builds on this approach by extending the time-line closer to the Allentown incident. As can be seen, a number of further incidents occurred that either had similar causes to the Allentown incident, such as the Green County incident, or in which the NTSB again recommended the use of EFVs. Again, the labels below the time-line are used to chart the progress of regulatory studies and recommendations about the use of EFVs. This diagram shows the NTSB's continuing support for the wider introduction of these devices, for example in the 1981 study of 14 previous accidents. It also illustrates concerns about the reliability and utility of these devices within the Department of Transportation. These concerns lead to a study by the Gas Research Institute in 1985. The NTSB concludes that this report is seriously flawed in 1987-88 in that it under-estimates the utility of EPVs.

Figure 9.1.1 further extends the previous two time-lines beyond the Allentown explosion. It illustrates the continuing debate between the regulator, the Department of Transportation, and the investigatory agency, the NTSB. Following the Allentown explosion, a group of seventeen congressional representatives signed a letter that was sent to the Department of Transportation. This criticised the lack of progress that had been made in improving pipeline safety. However, the Office of Pipeline Safety still deferred any final ruling on the widespread introduction of EFVs.

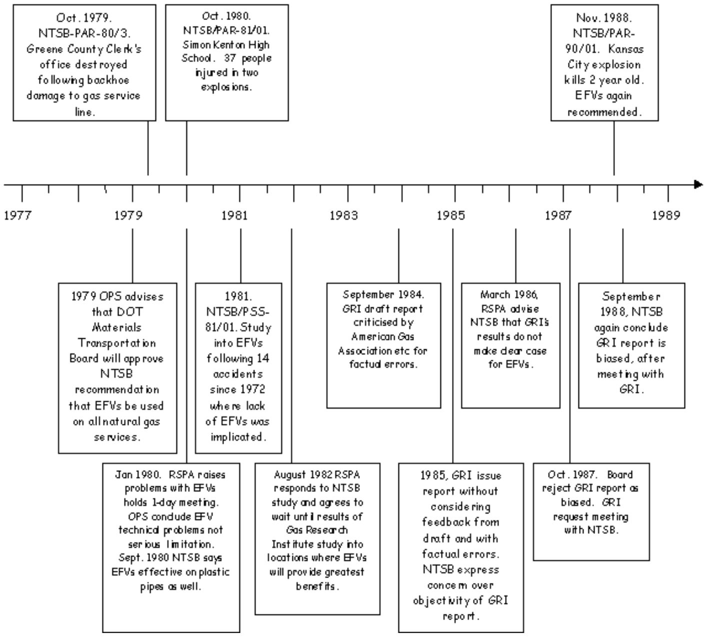

Oct. 1979. NTSB-PAR-80/3. Greene County Clerk's office destroyed following backhoe damage to gas service line.
Oct. 1980. NTSB/PAR-81/01. Simon Kenton High School. 37 people injured in two explosions.
Nov. 1988. NTSB/PAR-90/01. Kansas City explosion kills 2 year old. EFVs again recommended.
1977
1979
1981
1983
1985
1987
1989
1979 OPS advises that DOT Materials Transportation Board will approve NTSB recommendation that EFVs be used on all natural gas services.
1981. NTSB/PSS-81/01. Study into EFVs following 14 accidents since 1972 where lack of EFVs was implicated.
September 1984. GRI draft report criticised by American Gas Association etc for factual errors.
March 1986, RSPA advise NTSB that GRI's results do not make clear case for EFVs.
September 1988, NTSB again conclude GRI report is biased, after meeting with GRI.
Jan 1980. RSPA raises problems with EFVs holds 1-day meeting. OPS conclude EFV technical problems not serious limitation. Sept. 1980 NTSB says EFVs effective on plastic pipes as well.
August 1982 RSPA responds to NTSB study and agrees to wait until results of Gas Research Institute study into locations where EFVs will provide greatest benefits.
1985, GRI issue report without considering feedback from draft and with factual errors. NTSB express concern over objectivity of GRI report.
Oct. 1987. Board reject GRI report as biased. GRI request meeting with NTSB.

Figure 9.2: Graphical Time-line Showing Intermediate Regulatory Background.

As has been mentioned in previous paragraphs, the graphical time-lines provide a framework or overview of the events that contribute to an incident or accident. Each entry can be thought of as an index into the more detailed evidence that is gathered during a secondary investigation. It also follows that not all of this evidence may be shown on a graphical time-line. Reconstruction, typically, involves a process of abstraction that is implied by our use of terms such as 'overview' or 'model' in the previous paragraphs. Investigators must use their judgement to determine what is, and what is not, included in a time-line. For instance, the previous diagrams have not included the letter that Jim Hall, Chairman of the NTSB, sent on the 28th September 1995 to the administrator of the Research and Special Programs Administration in the Department of Transport. The recipient of this letter was responsible for managing the Office of Pipeline Safety. Chairman Hall's letter expressed disappointment at the RSPA's response to House and Senate committees when they failed

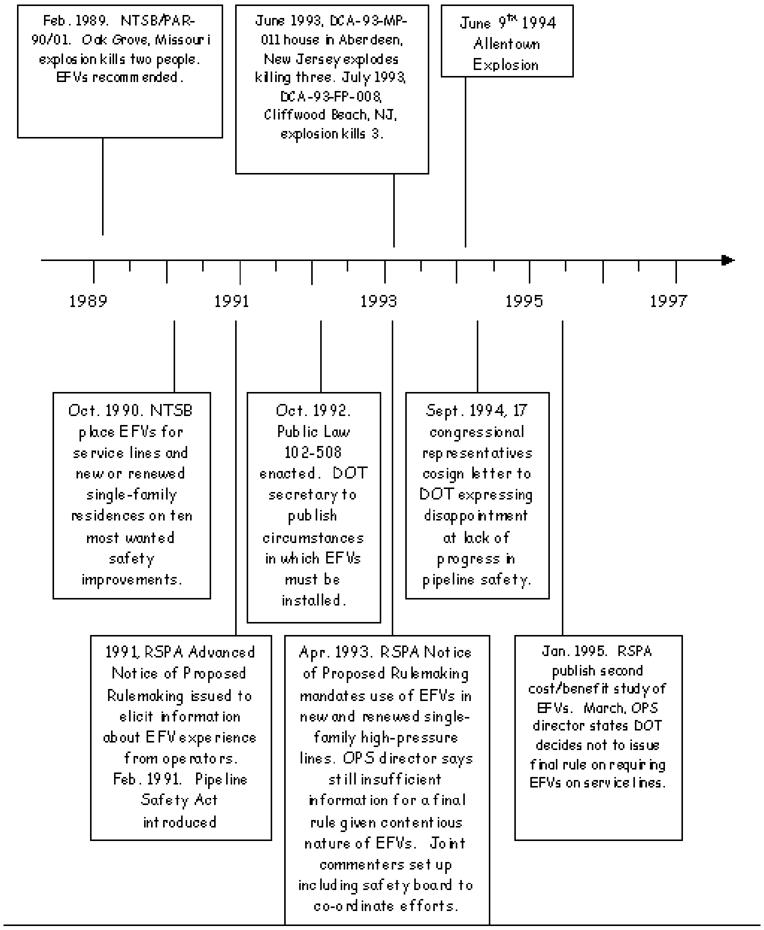

Feb. 1989. NTSB/PAR-90/01. Oak Grove, Missouri explosion kills two people. EFVs recommended.
June 1993, DCA-93-MP-011 house in Aberdeen, New Jersey explodes killing three. July 1993, DCA-93-FP-008, Cliffwood Beach, NJ, explosion kills 3.
June 9th 1994 Allentown Explosion
1989
1991
1993
1995
1997
Oct. 1990. NTSB place EFVs for service lines and new or renewed single-family residences on ten most wanted safety improvements.
Oct. 1992. Public Law 102-508 enacted. DOT secretary to publish circumstances in which EFVs must be installed.
Sept. 1994, 17 congressional representatives cosign letter to DOT expressing disappointment at lack of progress in pipeline safety.
1991, RSPA Advanced Notice of Proposed Rulemaking issued to elicit information about EFV experience from operators. Feb. 1991. Pipeline Safety Act introduced
Apr. 1993. RSPA Notice of Proposed Rulemaking mandates use of EFVs in new and renewed single-family high-pressure lines. OPS director says still insufficient information for a final rule given contentious nature of EFVs. Joint commenters set up including safety board to co-ordinate efforts.
Jan. 1995. RSPA publish second cost/benefit study of EFVs. March, OPS director states DOT decides not to issue final rule on requiring EFVs on service lines.

Figure 9.3: Graphical Time-line Showing Immediate Regulatory Background.

to identify any circumstances that might mandate the use of EFVs. The Chairman of the NTSB continued:

> "The Safety Board is extremely disappointed in your decision. For more than 20 years, RSPA has failed to objectively assess the benefits of EFVs, and we believe RSPA has again lost an excellent opportunity to provide increased safety for gas customers and the public... In our investigations of distribution pipeline accidents, the Safety Board continues to find strong evidence that supports requiring a means to rapidly shut off gas flow to failed pipe segments. While such a requirement would not prevent accidents, it would significantly reduce their consequences." [589]

The previous time-lines illustrate some of the production problems that limit the tractability of this approach. Initially, Figure 9.1 9.1.1 and 9.1.1 formed part of a single time-line. However, it proved to be impossible to reproduce this within the format and pagination of this book. As a result, the simple spatial relationship between layout and time had to be broken, in part, by splitting a single linear diagram into several different figures. Later paragraphs will show how hierarchical time-lines can be used to avoid this potential limitation.

The high-level time-lines shown in Figures 9.1, 9.1.1 and 9.1.1 illustrate many of the strengths of this reconstruction or modelling technique. The simple relationship between spatial locations on the diagrams and temporal locations during an incident has already been noted. The practical consequence of this is that analysts need minimal training to use these models. They can be used

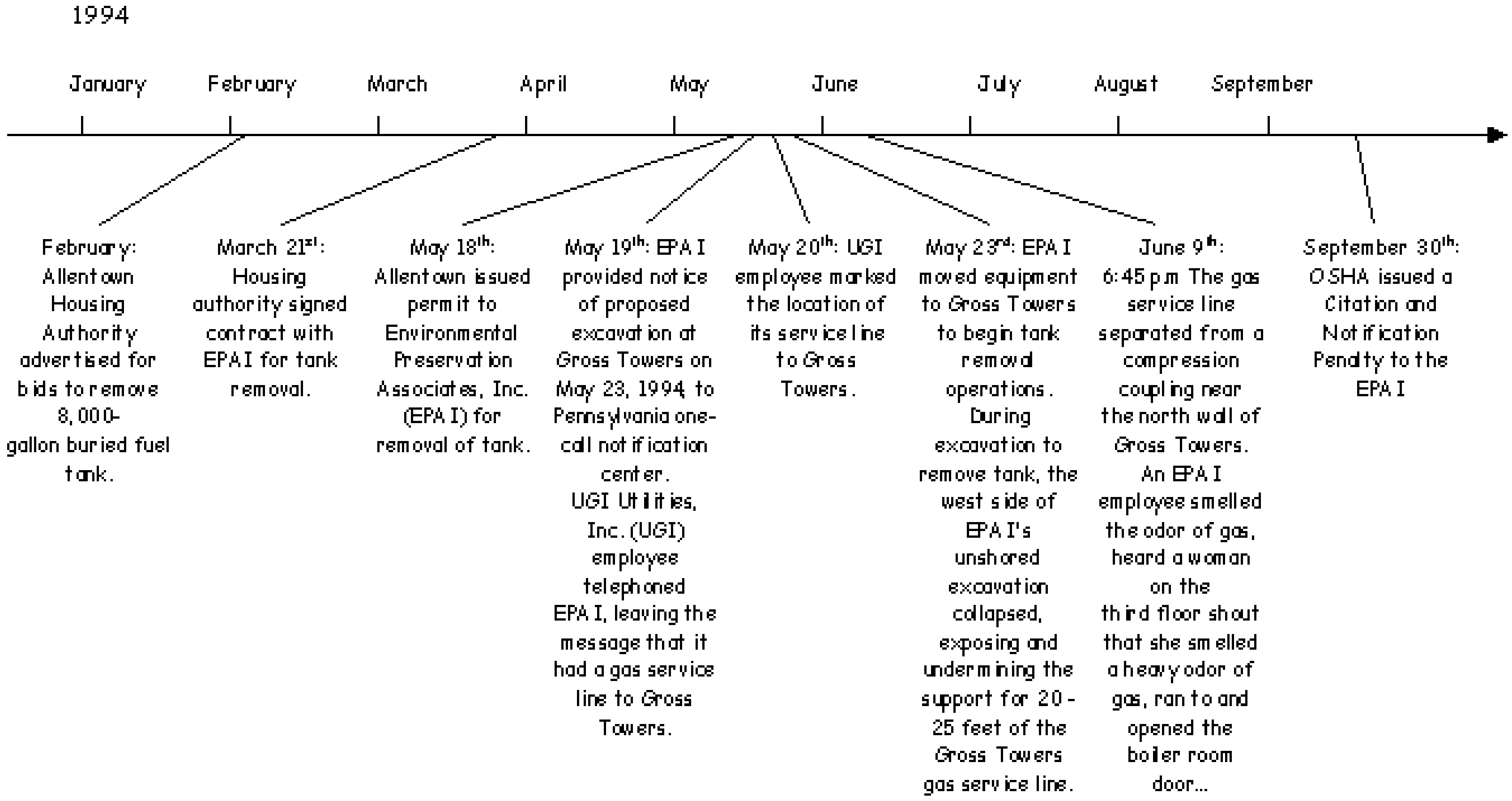

1994
January
February
March
April
May
June
July
August
September
February: Allentown Housing Authority advertised for bids to remove 8,000-gallon buried fuel tank.
March 21st: Housing authority signed contract with EPAI for tank removal.
May 18th: Allentown issued permit to Environmental Preservation Associates, Inc. (EPA I) for removal of tank.
May 19th: EPA I provided notice of proposed excavation at Gross Towers on May 23, 1994 to Pennsylvania one-call notification center. UGI Utilities, Inc. (UGI) employee telephoned EPA I, leaving the message that it had a gas service line to Gross Towers.
May 20th: UGI employee marked the location of its service line to Gross Towers.
May 23rd: EPA I moved equipment to Gross Towers to begin tank removal operations. During excavation to remove tank, the west side of EPA I's unshored excavation collapsed, exposing and undermining the support for 20 - 25 feet of the Gross Towers gas service line.
June 9th: 6:45 p.m The gas service line separated from a compression coupling near the north wall of Gross Towers. An EPA I employee smelled the odor of gas, heard a woman on the third floor shout that she smelled a heavy odor of gas, ran to and opened the boiler room door...
September 30th: OSHA issued a Citation and Notification Penalty to the EPA I

Figure 9.4: Graphical Time-line of Events Surrounding the Allentown Explosion.

as a common medium of communication between the diverse disciplines involved in incident investigations. Figure 9.4 extends this approach by presenting a time-line for some of the events that relate more directly to the Allentown case study, rather than to a more general class of pipeline failures. Here we can see the strong visual appeal of this linear notation. Readers can easily gauge the intervals between events because there is a simple relationship between linear distance and the temporal intervals between events. In other words, standard units of distance are used to represent standard units of time. In Figure 9.4, this is used to indicate the interval between the date at which the Allentown Housing Association put the removal of the buried fuel tank out to tender and the date when Occupational Safety and Health Administration (OSHA) cited EPAI for a range of health and safety deficiencies. As can be seen, this diagram shows both the events leading to the gas line separation on the 9th June as well as events after the incident, such as the OSHA citation. This satisfies the reconstruction requirement that it should be possible to represent the consequent actions following any adverse occurrence. However, this graphical time-line illustrates events at an extremely high level of granularity. In contrast, Figure 9.5 shows how the same approach can be applied to the more detailed proximal events 'on the day of the incident' rather than the more distal causes shown in Figures 9.4, 9.1, 9.1.1. Unfortunately, Figure 9.5 illustrates further limitations with this reconstruction technique. In particular, it is necessary to position all events at some time during the incident. This is not always possible. For instance, the it was never possible to determine the exact time at which the foreman asked his team to trace the gas line back towards Utica street so that they could shut-off the gas valve. As a result this is labelled as occurring at 18:?? in Figure 9.5 and no connection can be made to the intervals illustrated on the time-line.

It is also possible to see an 'uneven' distribution of events over time in the clustering between 18:40 and 18:50. Nothing significant is shown to happen between the EPAI foreman's warning to the Housing Association Official that the gas line needed to be supported and the arrival of the backhoe at Gross Towers. Conversely, a large number of critical events take place in the interval between the moment when the backhoe was driven across the buried section of pipe and the moment when the foreman rang UGI to inform them that they had definitely hit the gas line. The concentration of critical events crams many different annotations into a small area of the line. This reduces the tractability of the resulting time-line.

This uneven distribution of events over time partially explains the decision to use two different scales in Figures 9.4 and 9.5. The former divides the line into months while the latter uses hours. If the same hour-based scale were used then the tendering process in February would have to be drawn many meters away from the events in May or June. Most of this line would have no significant annotations until the contract was signed in March. Although our use of different temporal scales helps to avoid this problem, it also introduce further concerns. In particular, investigators now have to maintain multiple diagrams of the same incident. Extensive cross references have to made in order to get a coherent overview of these different aspects of the same reconstruction. Figure 9.6 addresses this concern by using different axes to link the previous two graphical time-lines. This represents one of the hierarchical approaches mentioned in previous paragraphs . The higher-level intervals that are represented on one axis can be broken down into more fine grained intervals that are represented on an orthogonal axis. Unfortunately, this approach introduces further problems. In particular, it can be argued that Figure 9.6 destroys the simple, linear relationship between space and time that is claimed to be the key strength of the time-line notation. The following sections, therefore, describe a number of further reconstruction techniques that can be used to address these limitations of graphical time-lines.

9.1.2 Fault Trees

Fault trees provide an alternative means of reconstructing the events that contribute to incidents and accidents [502, 409]. This notation provides a simple graphical syntax based around circuit diagrams. Figure 9.7 presents a brief overview of the syntactic elements that support this approach. These elements are used to construct a diagram that connects basic events to higher-level faults. AND gates can be used to represent that a particular fault or intermediate event is caused by the combination of two or more basic events. Similarly, OR gates can be used to represent that a par-

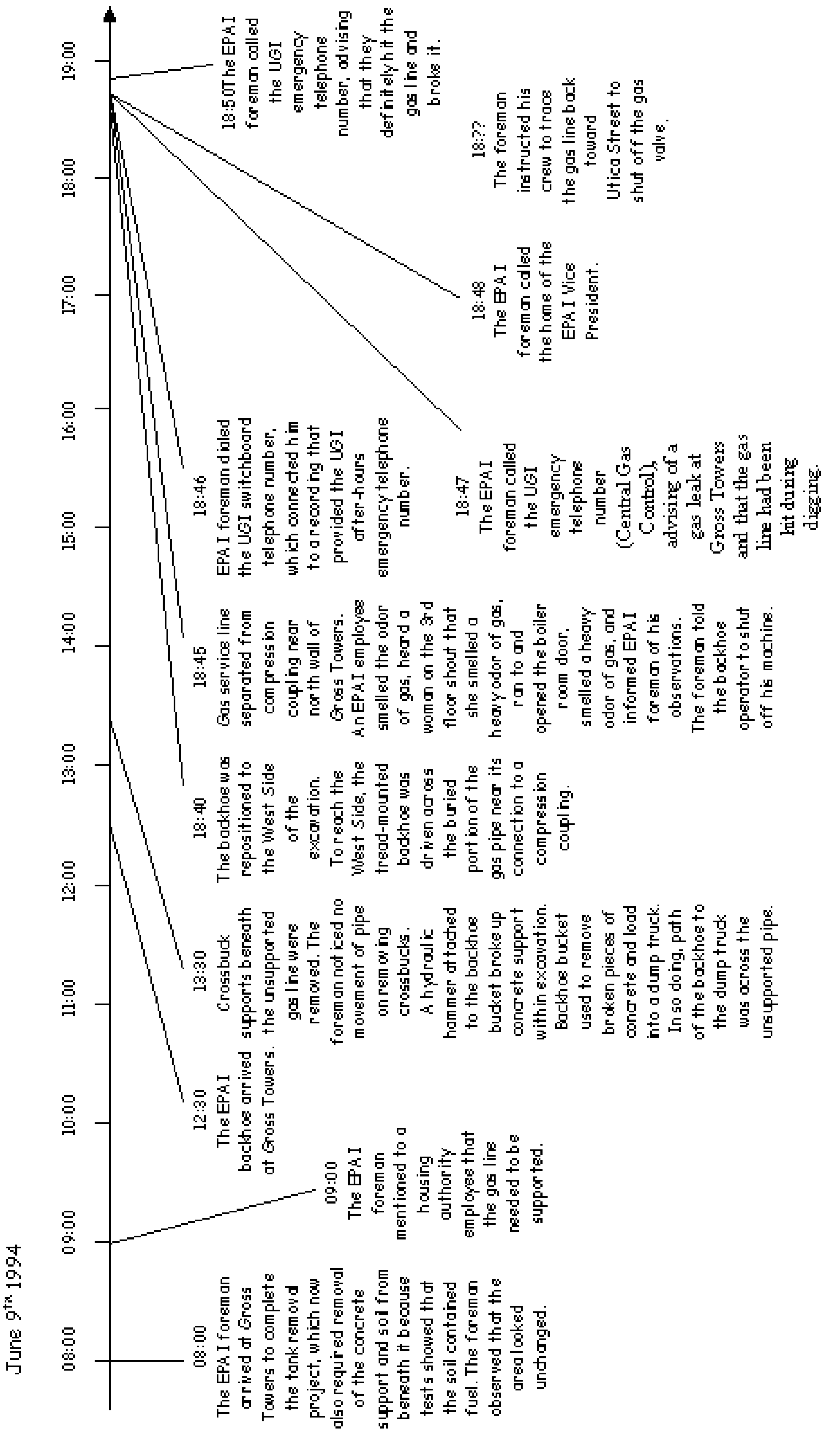
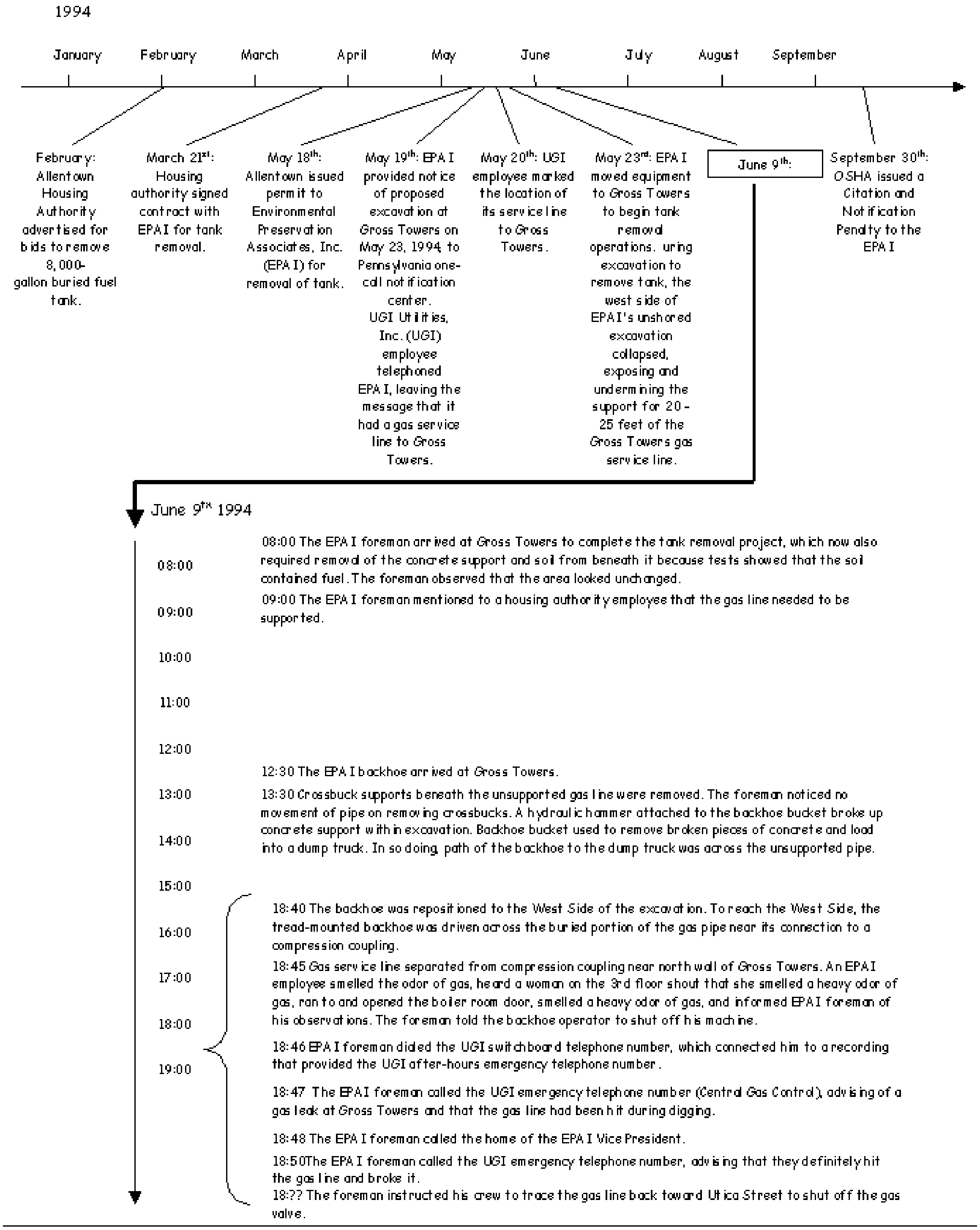

June 9th 1994
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
08:00 The EPA I foreman arrived at Gross Towers to complete the tank removal project, which now also required removal of the concrete support and soil from beneath it because tests showed that the soil contained fuel. The foreman observed that the area looked unchanged.
09:00 The EPA I foreman mentioned to a housing authority employee that the gas line needed to be supported.
12:30 The EPA I backhoe arrived at Gross Towers.
13:30 Crossbuck supports beneath the unsupported gas line were removed. The foreman noticed no movement of pipe on removing crossbucks. A hydraulic hammer attached to the backhoe bucket broke up concrete support within excavation. Backhoe bucket used to remove broken pieces of concrete and load into a dump truck. In so doing, path of the backhoe to the dump truck was across the unsupported pipe.
18:40 The backhoe was repositioned to the West Side of the excavation. To reach the West Side, the tread-mounted backhoe was driven across the buried portion of the gas pipe near its connection to a compression coupling.
18:45 Gas service line separated from compression coupling near north wall of Gross Towers. An EPA I employee smelled the odor of gas, heard a woman on the 3rd floor shout that she smelled a heavy odor of gas, ran to and opened the boiler room door, smelled a heavy odor of gas, and informed EPA I foreman of his observations. The foreman told the backhoe operator to shut off his machine.
18:46 EPA I foreman dialed the UGI switchboard telephone number, which connected him to a recording that provided the UGI after-hours emergency telephone number.
18:47 The EPA I foreman called the UGI emergency telephone number (Central Gas Control), advising of a gas leak at Gross Towers and that the gas line had been hit during digging.
18:48 The EPA I foreman called the home of the EPA I Vice President.
18:?? The foreman instructed his crew to trace the gas line back toward Utica Street to shut off the gas valve.
18:50 The EPA I foreman called the UGI emergency telephone number, advising that they definitely hit the gas line and broke it.

Figure 9.5: Graphical Time-line of the Allentown Explosion.



February: Allentown Housing Authority advertised for bids to remove 8,000-gallon buried fuel tank.

March 21st: Housing authority signed contract with EPAI for tank removal.

May 18th: Allentown issued permit to Environmental Preservation Associates, Inc. (EPA I) for removal of tank.

May 19th: EPA I provided notice of proposed excavation at *Gross Towers* on May 23, 1994 to Pennsylvania one-call notification center. UGI Utilities, Inc. (UGI) employee telephoned EPA I, leaving the message that it had a gas service line to *Gross* Towers.

May 20th: UGI employee marked the location of its service line to *Gross* Towers.

May 23rd: EPA I moved equipment to *Gross* Towers to begin tank removal operations. uring excavation to remove tank, the west side of EPAI's unshored excavation collapsed, exposing and undermining the support for 20 - 25 feet of the *Gross* Towers gas service line.

September 30th: OSHA issued a Citation and Notification Penalty to the EPA I

08:00 The EPA I foreman arrived at *Gross* Towers to complete the tank removal project, which now also required removal of the concrete support and soil from beneath it because tests showed that the soil contained fuel. The foreman observed that the area looked unchanged.

09:00 The EPA I foreman mentioned to a housing authority employee that the gas line needed to be supported.

12:30 The EPA I backhoe arrived at *Gross* Towers.

13:30 Crossbuck supports beneath the unsupported gas line were removed. The foreman noticed no movement of pipe on removing crossbucks. A hydraulic hammer attached to the backhoe bucket broke up concrete support within excavation. Backhoe bucket used to remove broken pieces of concrete and load into a dump truck. In so doing, path of the backhoe to the dump truck was across the unsupported pipe.

18:40 The backhoe was repositioned to the West *Side* of the excavation. To reach the West *Side*, the tread-mounted backhoe was driven across the buried portion of the gas pipe near its connection to a compression coupling.

18:45 *Gas* service line separated from compression coupling near north wall of *Gross* Towers. An EPAI employee smelled the odor of gas, heard a woman on the 3rd floor shout that she smelled a heavy odor of gas, ran to and opened the boiler room door, smelled a heavy odor of gas, and informed EPAI foreman of his observations. The foreman told the backhoe operator to shut off his machine.

18:46 EPA I foreman dialed the UGI switchboard telephone number, which connected him to a recording that provided the UGI after-hours emergency telephone number.

18:47 The EPAI foreman called the UGI emergency telephone number (Central *Gas* Control), advising of a gas leak at *Gross* Towers and that the gas line had been hit during digging.

18:48 The EPA I foreman called the home of the EPA I Vice President.

18:50The EPA I foreman called the UGI emergency telephone number, advising that they definitely hit the gas line and broke it.

18:?? The foreman instructed his crew to trace the gas line back toward Utica Street to shut off the gas valve.

Figure 9.6: Two-Axis Time-line of the Allentown Explosion.

ticular fault or intermediate event is caused by some subset of the more basic events that are linked to it. An exclusive-OR gate can be used to further restrict this representation so that a particular fault or intermediate event is caused by one of a number of more basic events. Andrews and Moss [27] provide a more detailed introduction to the fault tree notation. However, the following paragraphs will introduce the basic concepts as they are used. Fault trees are, typically, used to

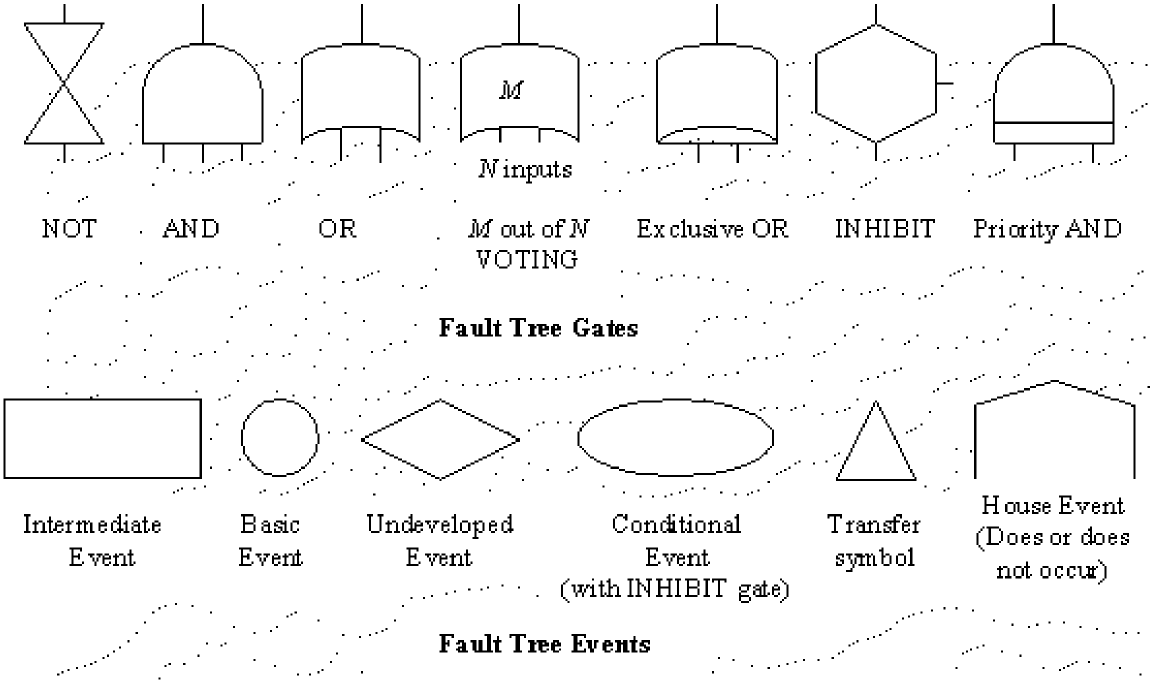


Figure 9.7: Fault tree components.

analyse potential errors in a design. This is illustrated by the simplified tree shown in figure 9.8. An operator injury occurs if three conditions are met. The protective guard must fail and a command to initiate the press must be given and the operator's hand must be under the protective guard. As can be seen, the conjunction between all of these three conditions is denoted by the graphical symbol that represents an AND operation within a circuit diagram. The left hand sub-branch of Figure 9.8 shows two ways in which the guard can fail. There may be a physical obstruction that prevents the guard from closing or an electrical failure of the guard motor may occur while it is still in the open position. Here the disjunction between these two conditions is denoted by the graphical symbol that represents an OR operation within a circuit diagram. There are numerous design benefit for this, typical, application of fault trees. For instance, they can be used to identify what is known as the minimal cut set. In order to explain this concept it is first necessary to explain that a basic event is one which cannot be decomposed any further. In figure 9.8 'Physical obstruction blocks guard at open' is a basic event. In contrast, 'guard fails' is an intermediate or higher level event. A minimal cut set is defined to be the smallest possible conjunction of events in which if any basic event is removed then the top condition will not occur [27]. For our example, there are two minimal cut sets. Operator injury will occur if:

```
Physical obstruction blocks guard AND
Pressing initiated AND
Operator's hand is under guard

OR
```

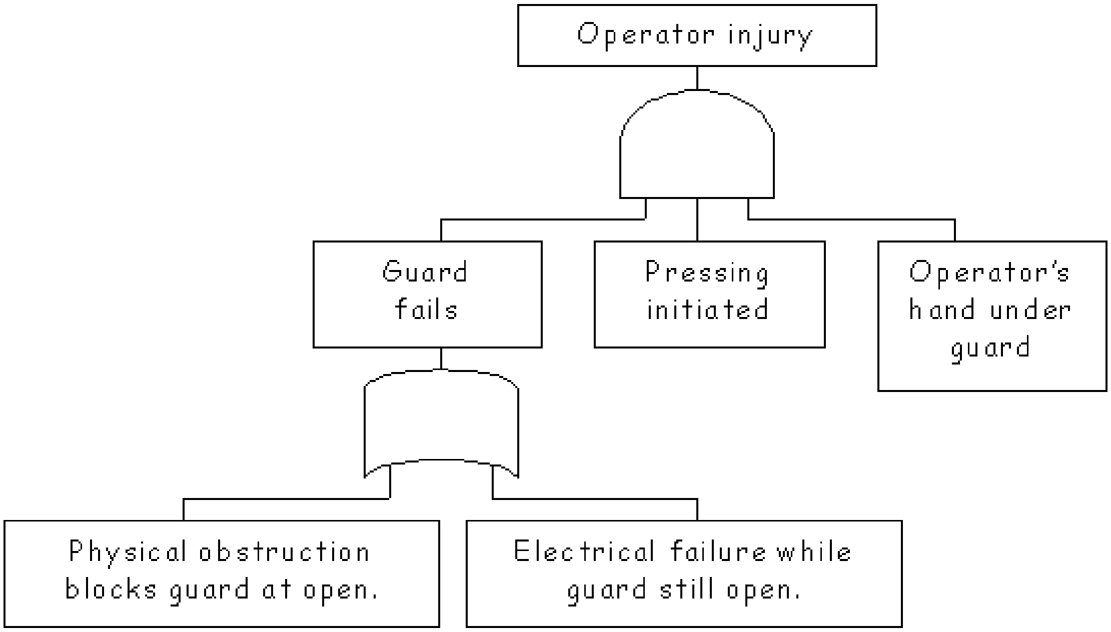

Operator injury
Guard fails
Pressing initiated
Operator's hand under guard
Physical obstruction blocks guard at open.
Electrical failure while guard still open.

Figure 9.8: A Simple Fault Tree for Design.

```
Electrical failure while guard at open AND
Pressing initiated AND
Operator's hand is under guard
```

The importance of a minimal cut set is that it can be used to identify where to focus finite development resources. If there is a basic event that is common to all minimal cut sets and it is possible to prevent that event from occurring then, by definition, the top event cannot also occur. This assumes that the fault tree accurately reflects all of the possible ways in which an adverse occurrence can take place. Conversely, if it is only possible to prevent basic events that occur in some proportion of the minimal cut sets then there will continue to be other ways in which the incident may occur. Extensions of this basic approach can also be used to analyse the probability of a top level event if designers know the probability of the basic events that contribute to it. For instance, if observations of previous operations suggest that a physical obstruction blocks the guard once every hundred days then we assign a probability of it failing in the next day of 0.01. Similarly if observations suggest an electrical failure once every 1,000 days then the probability would be 0.001. The probability of the disjunction of an electrical failure, shown as event A, or of an obstruction, shown as event B, is derived by applying the following formula. The final term accounts for the situation in which both the electrical failure and the physical obstruction occur together.

$$Pr(A\ or\ B) = Pr(A) + Pr(B) - Pr(A\ and\ B) \tag{9.1}$$

If these events were mutually exclusive, in other words the physical obstruction and the electrical failure could not occur together, then this term could be omitted. In similar fashion, the probability of a conjunction can, most simply, be given as the product of the probabilities of its child events. There are, however, a number of technical and practical limitations. For example, it can be difficult to obtain reliable statistical data to validate the probabilities that are included in the tree. There are also a number of limitating assumptions, such as event independence. If these assumptions are violated then more complex mathematical procedures must be used to calculate conditional probabilities [27].

As mentioned, fault trees have traditionally been used to support the design of safety-critical systems. This notation can, however, offer considerable benefits as a means of supporting the reconstruction of adverse occurrences. The leaves of the tree represent the initial causes of an incident [485]. Basic events can be used to represent the underlying failures that lead to an accident [363]. Logic gates can be used to represent the ways in which those causes combine. For example, the combination of operator mistakes, hardware/software failures and managerial problems might be represented using an AND gate. Conversely, a lack of evidence about user behaviour or system performance might be represented using an OR gate. For instance, Figure 9.9 uses a fault tree to reconstruct part of the NTSB case study:

> "By reducing the soils capacity to restrain the movement of the pipe and by exerting forces on the service line that resulted in excessive longitudinal stress, the excavator caused the line to separate at a compression coupling. "
> "The gas company lost the opportunity to preserve the integrity of the service line because its procedures did not require a review of any unusual excavation near a gas service line that might damage the line and threaten public safety."
> "The likely reason the fire inspectors did not notify the gas company that its service line was damaged was because the inspectors did not understand the importance of notifying operators so the effects on a facility could be assessed by the operators and necessary action taken." [589]

As can be seen, the subtree on the right of Figure 9.9 represents the conjunction of events that are identified as causes for the line separation at the compression coupling: the soils capacity to restrain the movement of the pipe was reduced and undue forces were exerted on the line and gas company procedures did not require a thorough review of unusual excavations. Had any one of these events not taken place then the incident would not have occurred in the manner described by the NTSB. The counterfactual reasoning in the previous sentence illustrates the important point that the elements of a minimal cut-set within an accident fault tree are root causes of the ultimate failure that (paradoxically) is at the root, or top, of the entire tree structure. The events that contribute to the line separation, labelled Conclusion 3 and 6, and the failure of the fire inspectors to notify the company, labelled Conclusion 7, are all members of the minimal cut set and are, therefore, root causes of the gas explosion.

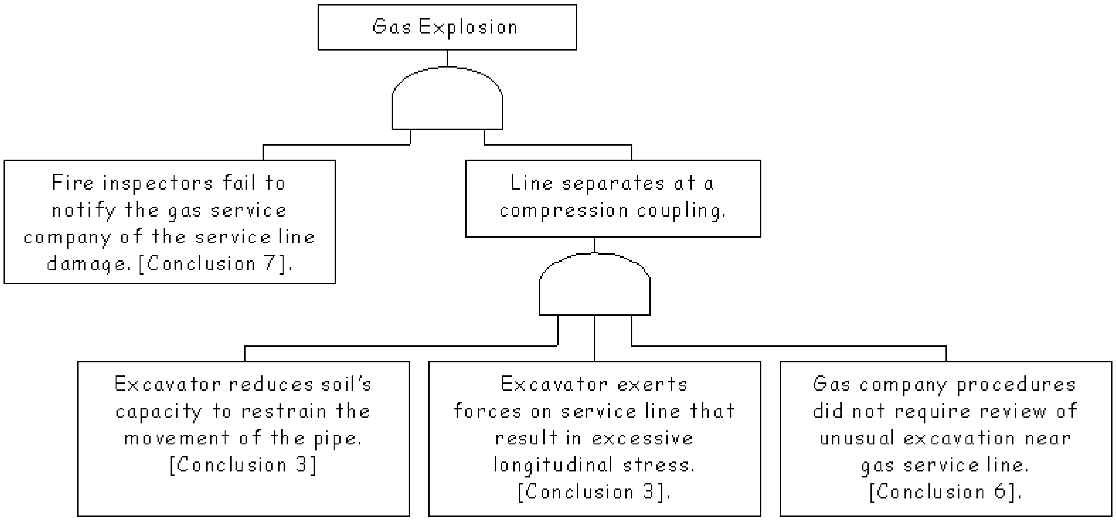

Gas Explosion
Fire inspectors fail to notify the gas service company of the service line damage. [Conclusion 7].
Line separates at a compression coupling.
Excavator reduces soil's capacity to restrain the movement of the pipe. [Conclusion 3]
Excavator exerts forces on service line that result in excessive longitudinal stress. [Conclusion 3].
Gas company procedures did not require review of unusual excavation near gas service line. [Conclusion 6].

Figure 9.9: Simplified Fault Tree Representing Part of the Allentown Incident.

The previous paragraph has shown how fault trees can be used to represent the root causes that are identified by counter factual reasoning. Unfortunately, this raises a number of practical and theoretical problems. As we have seen, our counter factual reasoning relies on that fact that the intermediate events described by an AND gate will only occur if all of its inputs are true. The gas explosion in Figure 9.9 would not have occurred if any of the four basic events were prevented from happening. This is an extremely strong assumption. How confident can we be that an explosion would actually have been avoided if the Fire inspectors had intervened? It is difficult to be certain that an incident would have been avoided under such circumstances. A number of complex reasoning techniques, based around modal logic, can be used to address this apparent limitation [470]. It is also possible to recruit additional forms of secondary investigation to increase our confidence in the elements of a reconstruction. In the previous example, this could involve further studies of the interaction between Fire inspectors and gas service companies. These studies might demonstrate that inspectors routinely intervene to prevent similar incidents from occurring. However, if there was strong evidence that such interventions have not been effective in avoiding gas explosions then the tree must be redrawn.

Immediate Causes

Figure 9.9 provides a high-level overview of some of the causes that led to the Allentown explosion. However, such abstract fault trees provide few insights into the more detailed patterns of events that contribute to major incidents. For example, Figure 9.9 abstracts away from the particular way in which the excavators' actions led to undue forces being exerted on the exposed gas line. Similarly, it does not identify the contextual or motivating factors that prevented the fire inspectors from notifying the damage that they observed to the gas company's line. Figure 9.10, therefore, shows how a fault tree can be used to provide a more detailed overview of the events leading to an adverse occurrence. This diagram is significantly more complex than its predecessors. It is also important to note that the triangular continuation symbol, labelled A1, is used to denote the fact that further details about the exposure of the gas line are provided in an additional sub-tree that is not shown here.

In Peterson's terms, Figure 9.9 shows how fault trees can be used to provide a general view of causality [678]. It provides some indication of the high-level failures that led to the incident. However, it is also ambiguous in the sense that there are many different reasons for the inspectors failure to report the damage to the gas line or the failure of the gas company's procedures. In contrast to Figure 9.9, Figure 9.10 provides a more singular view of the adverse occurrence. For example, it refines the abstract information in Figure 9.9 by representing the ways in which the incident developed over time. The moment at which the line coupling broke is shown to be [18:45]. Similarly, the initial UGI response is shown to have occurred during the interval between [18:50-18:58] which was too late to prevent the explosion. This representation of temporal information introduces further distinctions between our use of fault trees to support incident reconstruction and their more conventional design applications. Our approach looks at the way in which particular events actually occurred in the past rather than the probability of those events occurring again in the future. There are further complications. For example, the events in conventional fault trees tend to occur at particular instants in time. This is reflected by the way in which the developers of fault trees are encouraged to label their diagrams with 'trigger events' rather than conditions that emerge over time. For example, Andrews and Moss [27] advise that:

> "Trigger events should be coupled with 'no protective action taken', i.e. 'overheating' could be 'loss of colling' and 'no emergency shutdown'." [27]

This advise is important because it simplifies the probabilistic failure analysis that is used to guide system development. However, our application of the fault tree notation does not exploit the stochastic models that support design. As a result, it is possible to move away from any requirement for instantaneous events. For example, the Foreman's response to the initial rupture of the gas pipe took place from 18:45 to 18:54. This flexibility comes at a cost. The semantics of both the temporal information and the events in the tree become a cause for concern. For instance, Figure 9.10 uses [18:45-18:54] to denote that the Foreman coordinated a partial response to the emergency between 6.45pm and 6.54pm. In contrast, [18:58 and 19:03 approx] is used to denote the fact that two separate

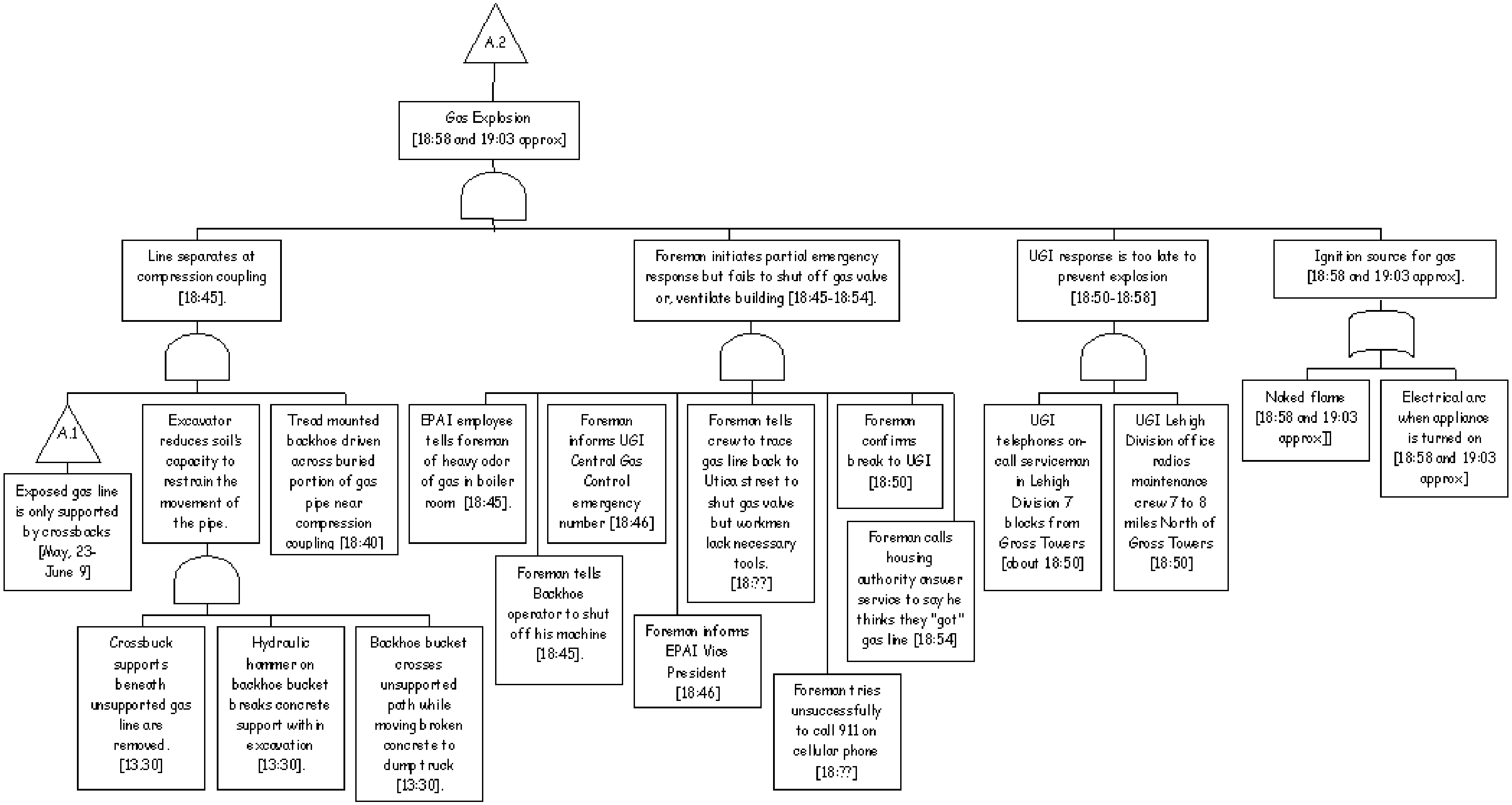

A.2
Gas Explosion [18:58 and 19:03 approx]
Line separates at compression coupling [18:45].
Foreman initiates partial emergency response but fails to shut off gas valve or, ventilate building [18:45-18:54].
UGI response is too late to prevent explosion [18:50-18:58]
Ignition source for gas [18:58 and 19:03 approx].
A.1
Exposed gas line is only supported by crossbacks [May, 23-June 9]
Excavator reduces soil's capacity to restrain the movement of the pipe.
Tread mounted backhoe driven across buried portion of gas pipe near compression coupling [18:40]
Crossbuck supports beneath unsupported gas line are removed. [13:30]
Hydraulic hammer on backhoe bucket breaks concrete support with in excavation [13:30].
Backhoe bucket crosses unsupported path while moving broken concrete to dump truck [13:30].
EPAI employee tells foreman of heavy odor of gas in boiler room [18:45].
Foreman tells Backhoe operator to shut off his machine [18:45].
Foreman informs UGI Central Gas Control emergency number [18:46]
Foreman informs EPAI Vice President [18:46]
Foreman tells crew to trace gas line back to Utica street to shut gas valve but workmen lack necessary tools. [18:??]
Foreman tries unsuccessfully to call 911 on cellular phone [18:??]
Foreman confirms break to UGI [18:50]
Foreman calls housing authority answer service to say he thinks they "got" gas line [18:54]
UGI telephones on-call serviceman in Lehigh Division 7 blocks from Gross Towers [about 18:50]
UGI Lehigh Division office radios maintenance crew 7 to 8 miles North of Gross Towers [18:50]
Naked flame [18:58 and 19:03 approx]]
Electrical arc when appliance is turned on [18:58 and 19:03 approx]

Figure 9.10: Fault Tree Showing Events Leading to Allentown Explosion

explosions occurred at 6.58pm and at approximately 7.03pm. [18:??] denotes that the exact time when the foreman attempted to call 911 is not known. These examples illustrate particular forms of temporal relationship within our case study. They are not complete in the sense that there will be temporal relationships that we cannot describe in terms of these annotations. Analysts must develop similar conventions to describe more complex timing information.

Like the graphical time-lines of the previous section, this diagram represents the passage of time flowing from left to right. For example, the lest-most sub-branch represents the events that led to the separation of the gas pipeline at 18:45. An examination of the intermediate and basic events that led to this failure shows that some, such as the initial exposure of the line, took place days before the actual failure. Other contributory events, such as the movement of the backhoe over the line occurred only minutes before the separation of the coupling. Unlike the graphical time-lines, however, this representation loosens some of the restrictions that are implied by a strict left to right ordering for events over time. It is possible to denote events that contribute to a higher level failure but for which there is little or no timing information. This is illustrated by the ambiguity that surrounds the Foreman's unsuccessful attempts to contact the emergency services by dialing '911' on his cellular telephone. No timing information is available to confirm this event because he could not raise a signal and the call was never completed.

The left to right temporal ordering of Figure 9.10 only applies to events at the same level in the tree. For instance, the basic events of the second sub-tree from the left denote that EPAI employees tell the foreman about the odour of gas and tells the Backhoe operator to stop work at 18:45. These are shown to the left of a basic event denoting the fact that the Foreman informed UGI's emergency number at 18:46 and so on. However, this left to right representation of time cannot be applied to components at different levels of the tree. For instance, an event that contributed to the separation of the gas pipeline, shown in the left-most branch, might occur *after* an event that impaired the emergency response, represented by the subtree on its right. This would, typically, occur if the inadequate response was influenced by events, such as inadequate training in emergency response procedures, that pre-dated the coupling failure.

A large proportion of the tree shown in Figure 9.10 relates to individual failures. The left-most sub-tree focuses on the excavation team's actions in exposing the gas line and in compromising the coupling. The next sub-tree deals with the Foreman's partial response to the initial separation of the gas line. However, the diagram also includes organisational factors. For example, the next sub-tree describes how UGI, the gas operating company, had only limited time to respond to the emergency. The right-most branch, in contrast, describes the environmental catalysts for two explosions. As can be seen, this sub-tree represents some of the uncertainty that inevitably arises during initial reconstructions. An inclusive OR gate shows that the explosion might have been triggered by a naked flame or by an arc from an electrical appliance.

The previous fault tree provides a graphical reconstruction of the events leading to the Allentown explosion. This offers a number of important benefits:

1. Fault trees provide an overview of the events that an analyst believes contributed to an incident. This is important because many secondary investigations gather evidence that reflects the complex nature of many safety-critical failures. It can often, therefore, be difficult to piece together evidence into a coherent account of the events that contribute to adverse incidents;

2. Fault trees also suggest alternative hypotheses and questions about the analysis that is presented in an accident report. Readers can further develop the events in a tree to develop further lines of investigation. For instance, it might be important to learn more about the problems that prevented the crew from successfully shutting off the gas flow with the tools that they had available.

Figure 9.11 introduces the events that led to the exposed gas line being supported by crossbucks. Figure 9.10 used the A1 continuation symbol to indicate the way in which these more detailed events contributed to the overall incident. In particular, it presents the more detailed events that were omitted It presents the events leading to the initial exposure of the pipeline that were denoted by the triangular extension symbol in the previous figure. The line was only supported by crossbucks

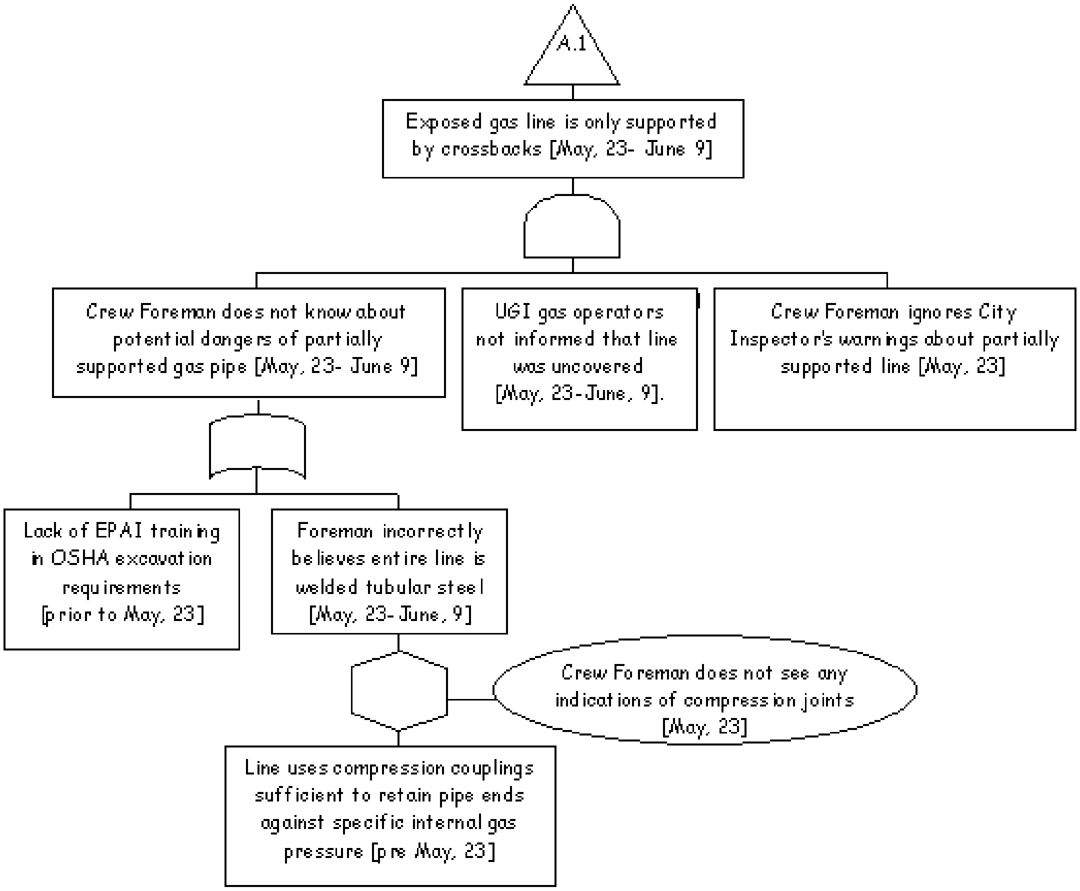

A.1
Exposed gas line is only supported by crossbacks [May, 23- June 9]
Crew Foreman does not know about potential dangers of partially supported gas pipe [May, 23- June 9]
UGI gas operators not informed that line was uncovered [May, 23-June, 9].
Crew Foreman ignores City Inspector's warnings about partially supported line [May, 23]
Lack of EPAI training in OSHA excavation requirements [prior to May, 23]
Foreman incorrectly believes entire line is welded tubular steel [May, 23- June, 9]
Crew Foreman does not see any indications of compression joints [May, 23]
Line uses compression couplings sufficient to retain pipe ends against specific internal gas pressure [pre May, 23]

Figure 9.11: Using Inhibit Gates to Represent Alternative Scenarios

because the Foreman did not appreciate the dangers of doing this, the gas supply operators, UGI, did not know that the line was uncovered and the Foreman ignored warnings from the Allentown Fire Inspectors. As can be seen, the fault tree uses an OR gate to represent a number of hypotheses about why the Foreman was unaware of the potential dangers associated with leaving the pipeline uncovered and partially supported:

> "Training–Before the accident, the workcrew had not had any formal training in excavation and trenching or in actions to take as a unit to protect lives and property in an emergency. The lack of training may account for why the crew did not shore the excavation site or tell the UGI that the gas line was unsupported. The crew foreman, despite not having any information about the construction of the gas line, said that he thought the entire line was welded tubular steel. His assumption may have led him to believe that the line could be adequately supported by crossbucks. In any event, he made a critical choice in assuming that it would be safe to leave the gas line uncovered and exposed for 2 weeks. A more prudent course of action would have been to immediately inform the UGI that the line was exposed." [589]

An OR gate is used because it is unclear what contributed most to the Foreman's lack of knowledge about the potential dangers associated with exposing the gas line. Their lack of training in appropriate OSHA standards for excavation or his incorrect belief about the pipeline construction could have affected his subsequent actions. It is important to emphasise that this decision to use an OR gate is not definitive. The construction of a fault tree is an iterative process. Subsequent discussions might discount the foreman's assumption. This might then be removed from the tree. Alternatively, it might be decided that both factors were required in order for the Foreman to behave in the way that he did. In such circumstances an AND gate might be introduced. This would have to be carefully justified because it implies that had the Foreman been trained in OSHA requirements then the incident would not have happened. Previous experience in incident and accident investigation has shown the dangers of making such assumptions about the efficacy of training as a primary protection mechanism.

In Figure 9.11 the left event of the OR gate represents the first line of analysis. It focuses on the Foreman's lack of training in applicable OSHA requirements. The second line of analysis is based on the Foreman's subsequent evidence that he believed the line to have been entirely constructed from welded tubular steel. This is developed using an INHIBIT gate, shown using a hexagon and an ellipse. The input event of an inhibit gate need not always lead to the output event. In this example, the fact that the line was constructed using compression couplings need not always lead the Foreman to incorrectly believe that an all-welded construction was used. The likelihood that the input event will lead to the output event is determined by the condition, shown in the ellipse. The Foreman did not see any indications of the compression joints and so believed that the tube was welded.

This ability to assign probabilities to representations of human error should not be underestimated. In particular, it provides a useful means of deriving simulations from a reconstruction of an incident or accident. Simulations enable analysts to replay or step through the course of an incident. Later sections will introduce automated tools for deriving simulations from incident reconstructions. For now, however, it is sufficient to observe that this can be done manually by inspecting a fault tree to trace the way in which particular combinations of events might lead to the high level failures shown in the upper levels of a figure. By introducing probabilistic information into a simulation it is possible for analysts to explore alternative scenarios during a reconstruction. For instance, Monte Carlo simulation techniques can be used to investigate probable and improbable, frequent or infrequent, traces of interaction. This approach involves the generation of random numbers typically in the range [0.0, 1.0]. This random number is then used to determine whether or not an event occurs during a particular run of the simulation. If the random number is less than the associated probability of the event then that event is assumed to happen. Conversely, if the number is greater then the event is assumed not to occur. For instance, it might be assumed that there is a 0.5 probability of anyone in the excavation team observing that compression couplings might have been used. Analysts might then begin to step through, or simulate, the events leading to the explosion. By generating a random number, it is possible to decide whether or not the couplings were observed during this particular simulation. In our example, they would be observed during approximately half of the run-throughs and would be overlooked during the rest.

Given our particular use of the fault tree notation, it might not at first appear that such simulation techniques are either appropriate or even useful. We know that the Foreman and their crew did not know that the pipe used compression couplings. However, the importance of simulation using Monte Carlo techniques is that it is possible to explore the consequences of small variations to the sequence of events that led to an incident. This is essential because incidents seldom recur in exactly the same way as previous failures. As we shall see, simulations can also be used to assess the potential impact of proposed improvements. For instance, improved training and amended site plans can be used to alert excavation crews to the construction techniques that are used by gas suppliers. These measures might increase the probability of correct observations being made to 0.8 or 0.9. It would then be correspondingly more likely that random numbers would fall below these thresholds and hence the detection of the compression joints would become more probable during any Monte Carlo simulation of a future incident. However, the obvious pitfall is that there must be some means of validating the statistics that are used to prime models such as that shown in Figure 9.11. The most appropriate means of obtaining these figures after an incident is through empirical tests with other operators. Of course, these studies are inevitably biased by the individual's knowledge that their performance is being monitored in the aftermath of an incident.

Figure 9.12 illustrates the iterative nature of incident reconstruction. This fault tree extends the diagram shown in Figure 9.11 to consider the events that contributed to the Foreman's decision

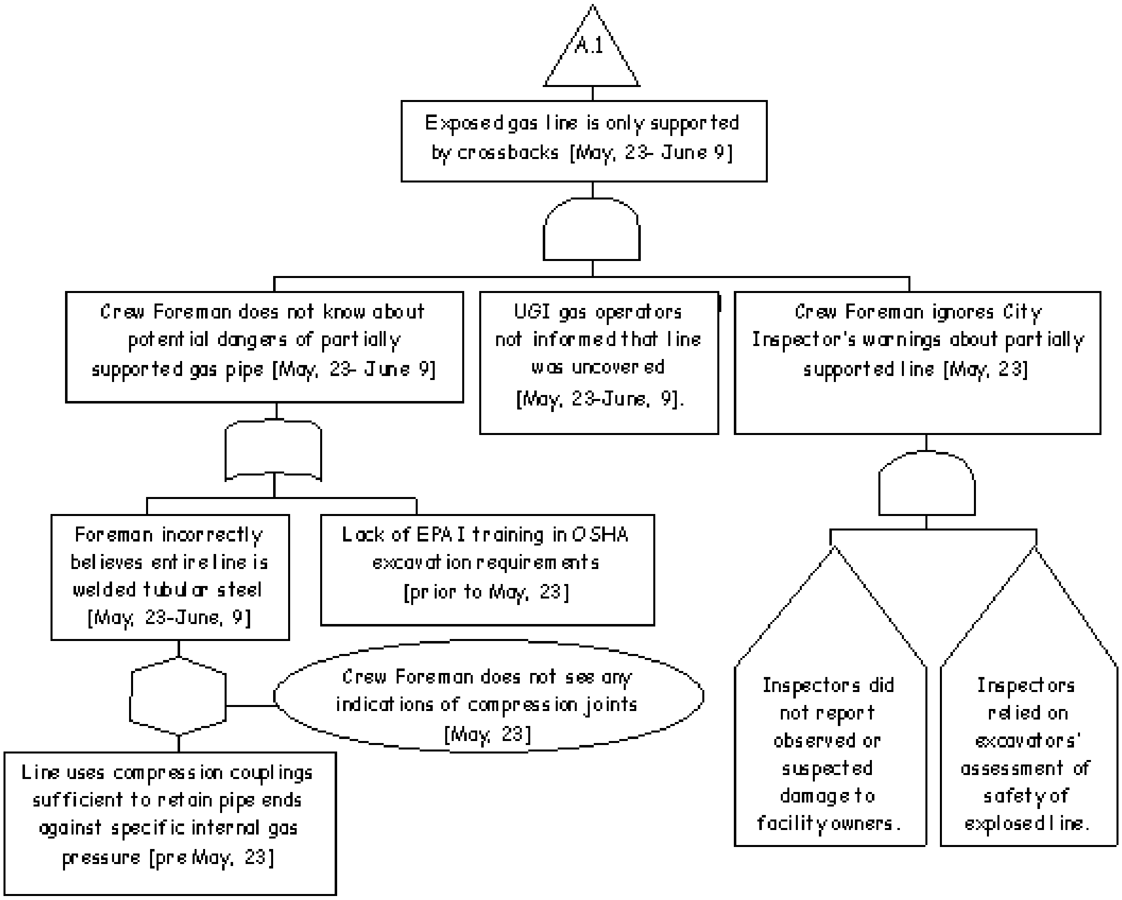

A.1
Exposed gas line is only supported by crossbacks [May, 23- June 9]
Crew Foreman does not know about potential dangers of partially supported gas pipe [May, 23- June 9]
UGI gas operators not informed that line was uncovered [May, 23-June, 9].
Crew Foreman ignores City Inspector's warnings about partially supported line [May, 23]
Foreman incorrectly believes entire line is welded tubular steel [May, 23-June, 9]
Lack of EPAI training in OSHA excavation requirements [prior to May, 23]
Crew Foreman does not see any indications of compression joints [May, 23]
Line uses compression couplings sufficient to retain pipe ends against specific internal gas pressure [pre May, 23]
Inspectors did not report observed or suspected damage to facility owners.
Inspectors relied on excavators' assessment of safety of explosed line.

Figure 9.12: Using House Events to Represent Alternative Scenarios

not to listen to the Fire Inspector's warnings. It does this by introducing HOUSE events. These are simplifications of the INHIBIT gates that were introduced in the previous chapter. HOUSE events support the simulation of alternative incident scenarios without the need to associate detailed probabilistic information with particular events. This is important because Chapter 2.3 has argued that it can be extremely difficult to validate human reliability statistics. In Figure 9.12, HOUSE events are used to show that the City Fire Inspectors did not report the damage to the pipeline to the facility owners and that they relied on the excavators assessment of the pipeline safety:

> "Because the citys fire inspectors saw on May 23 that the service line was unsupported, they could have prevented the accident. They showed proper concern about the safety of the line, especially after a piece of asphalt pavement fell on it and deformed it. However, not having been instructed to do otherwise, both inspectors relied on the EPAI foremen's assessment that the line was safe. It would have been more prudent of them to ask the pipeline owner for the assessment. The Safety Board concludes that the likely reason the fire inspectors did not tell the operator that its service line was damaged was because the inspectors did not understand the importance of notifying operators so the effects on a facility could be assessed by the operators and necessary action taken. Had the inspectors notified the UGI, it, the Safety Board believes, would have taken the necessary corrective actions, and the accident would not have happened." [589]

HOUSE events can either be "turned" on or off during the analysis of a fault tree. The NTSB investigation found that the Inspectors failed to report the damage and that they relied on the excavators. Technically, this can be represented by assigning a probability of 1 to the two house events in Figure9.12. However, the ability to switch events on and off also provides analysts with means of exploring alternative hypotheses about the course of an accident. For instance, a house event can be turned off if it is assigned a probability of 0. This can be used to explore what might have happened if the Inspector had reported the damage to the pipeline or had performed their own assessment of the pipeline safety. This might then have prevented the Foreman from ignoring their initial warnings about the unsupported line.

The previous paragraphs have argued that fault trees can be used to provide an overview of the immediate human errors that contribute to incidents. House events and inhibit gates can also be used to analyse the factors that did not play a part in past failures but which might lead to similar errors during the future operation of the system. In contrast, Figure 9.13 extends the previous analysis to look beyond the explosion at the emergency response. The continuation symbol, A2, is used to indicate that the events leading to the explosion, shown in Figure 9.10, also form part of this tree. In contrast, however, Figure 9.13 illustrates the events that contributed to an effective and well-co-ordinated response. This is an important illustration of how a graphical notation can provide a high-level overview of both the failures that contribute to an incident and the mitigating factors that help to reduce its potential consequences. Some of these events stem from successful training and management:

> "The fire department used the city's mass casualty incident plan, and the coordinator used the fire department's incident command system. The command post was established on the front lawn of Gross Towers at 7:03; and at 7:04, the emergency-response staging area and emergency shelter were established at the Allentown Fairgrounds, about 1/2 mile southwest of Gross Towers, where approximately 200 residents and 150 family members were helped. At 7:21, a MedEvac helicopter was requested to transport burn victims. Buses were requested at 7:40 to transport victims to the shelter at the fairgrounds, and by 7:49, the preliminary search of Gross Towers for victims was complete. The last injured resident was transported to a local hospital at 8:45." [589]

Other events that contributed to an effective and well-coordinated response were more due to chance than to planning. For example, the fact that many residents were not in the building at the time of the explosion helped to reduce the demands on those coordinating the initial evacuation. As can be seen from Figure 9.13, these 'chance' factors are not explored to the same level of detail as the organisational successes. This, in part, reflects the amount that can be gained from an improved understanding of these different aspects of the incident. It could also be argued that such 'chance' events ought to be denoted by HOUSE events so that analysts do not assume that they will always be true during any subsequent simulations of similar incidents.

Moving from Reconstructions to Conclusions

The previous fault trees, with the exception of Figure 9.9, illustrate the way in which the graphical notation can reconstruct the events leading to an incident. Fault trees provide a mid point between the evidence from any secondary investigation and the causal analysis that is the focus of the next chapter. The difference between reconstruction and causal analysis is often embodied in the structure of incident reports. For example, the NTSB report into the Allentown incident contained separate sections entitled 'Investigation', which includes the reconstruction of the events leading to the incident, and 'Analysis', which uses the reconstruction to support arguments about the underlying causes of the explosion. The findings of the analysis help to shape the conclusions that are to be drawn from any investigation. The following quotations illustrate these differences:

> "It took about 6 hours for the hydraulic hammer to break the concrete up. According to the EPAI employees, the impact of the hammer caused the ground to vibrate significantly. The backhoe bucket was used to remove the broken concrete and to load the pieces into a dump truck. The path of the backhoe bucket crossed over the pipe. The backhoe operator said that about 6:40 p.m. he moved the backhoe from a spot south of the

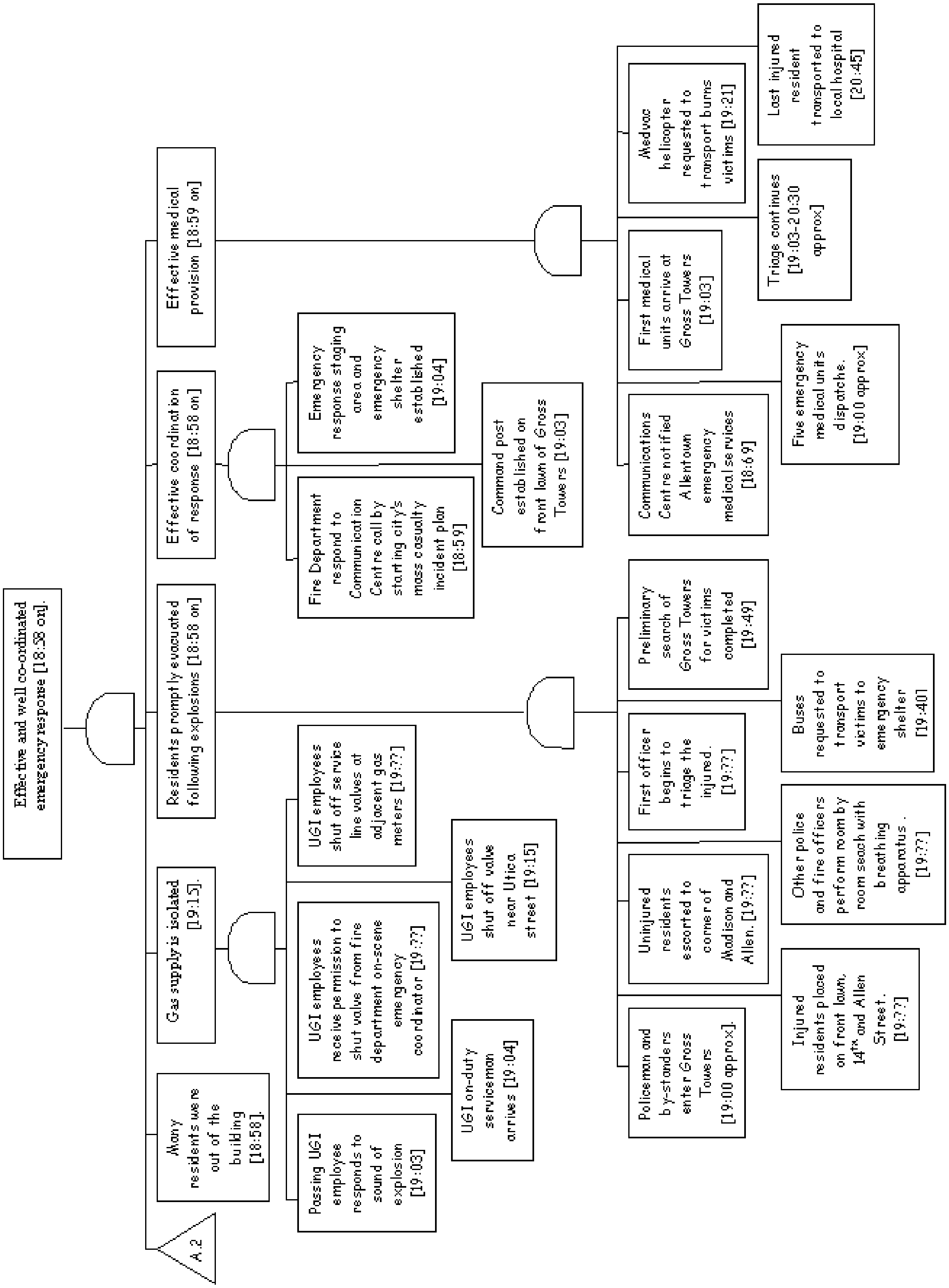

Effective and well co-ordinated emergency response [18:58 on].
A.2
Many residents were out of the building [18:58].
Gas supply is isolated [19:15].
Residents promptly evacuated following explosions [18:58 on]
Effective coordination of response [18:58 on]
Effective medical provision [18:59 on]
Passing UGI employee responds to sound of explosion [19:03]
UGI on-duty serviceman arrives [19:04]
UGI employees receive permission to shut valve from fire department on-scene emergency coordinator [19:??]
UGI employees shut off valve near Utica street [19:15]
UGI employees shut off service line valves at adjacent gas meters [19:??]
Fire Department respond to Communication Centre call by starting city's mass casualty incident plan [18:59]
Command post established on front lawn of Gross Towers [19:03]
Emergency response staging area and emergency shelter established [19:04]
Policeman and by-standers enter Gross Towers [19:00 approx].
Injured residents placed on front lawn, 14th and Allen Street. [19:??]
Uninjured residents escorted to corner of Madison and Allen. [19:??]
Other police and fire officers perform room by room seach with breathing apparatus . [19:??]
First officer begins to triage the injured. [19:??]
Buses requested to transport victims to emergency shelter [19:40]
Preliminary search of Gross Towers for victims completed [19:49]
Communications Centre notified Allentown emergency medical services [18:69]
Five emergency medical units dispatche. [19:00 approx]
First medical units arrive at Gross Towers [19:03]
Triage continues [19:03-20:30 approx]
Medvac helicopter requested to transport burns victims [19:21]
Last injured resident transported to local hospital [20:45]

Figure 9.13: Fault Tree Showing Post-Explosion Events

excavation to one on the west. In moving it, he crossed a buried section of pipeline that was between the excavation and the north wall of Gross Towers. The odour of gas was first detected about 6:45 p.m."
([589], Investigation, page 11).

"When the excavator resumed on June 9, its activities near the service line probably reduced the amount of restraint provided by the soil even more and increased the longitudinal force enough to cause the pipe to separate fully from the coupling. Using the impact tool to break the concrete tank support and moving the backhoe over the pipeline caused the soil to vibrate and probably further reduced the soils restriction of pipe movement. Also, the backhoe probably struck the line when being operated across it; the foreman's reports to both the UGI and the housing authority indicated that the pipe had been struck during recent excavation activities. Although the foreman denied after the accident that the backhoe had struck the line, the coating of the pipe showed evidence of mechanical damage, as did the pipe steel at one location. Also, the foreman's calls both to the housing authority and to the UGI show that at the time he believed his crew had hit the gas line while excavating."
([589], Analysis, page 32).

"By reducing the soils capacity to restrain the movement of the pipe and by exerting forces on the service line that resulted in excessive longitudinal stress, the excavator caused the line to separate at a compression coupling."
([589], Conclusion, page 47).

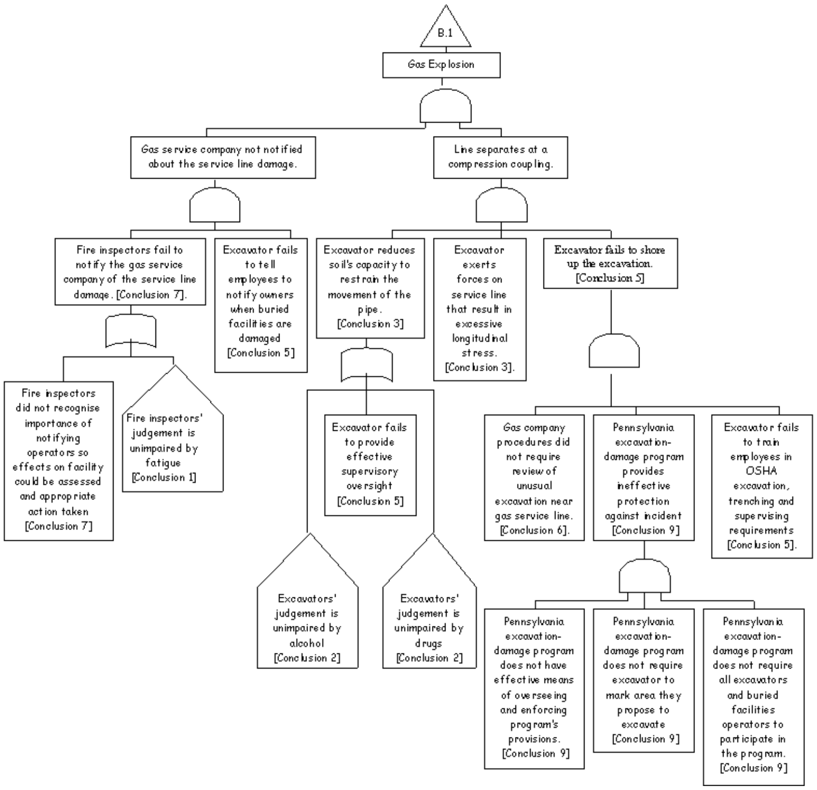

B.1
Gas Explosion
Gas service company not notified about the service line damage.
Line separates at a compression coupling.
Fire inspectors fail to notify the gas service company of the service line damage. [Conclusion 7].
Excavator fails to tell employees to notify owners when buried facilities are damaged [Conclusion 5]
Excavator reduces soil's capacity to restrain the movement of the pipe. [Conclusion 3]
Excavator exerts forces on service line that result in excessive longitudinal stress. [Conclusion 3].
Excavator fails to shore up the excavation. [Conclusion 5]
Fire inspectors did not recognise importance of notifying operators so effects on facility could be assessed and appropriate action taken [Conclusion 7]
Fire inspectors' judgement is unimpaired by fatigue [Conclusion 1]
Excavator fails to provide effective supervisory oversight [Conclusion 5]
Gas company procedures did not require review of unusual excavation near gas service line. [Conclusion 6].
Pennsylvania excavation-damage program provides ineffective protection against incident [Conclusion 9]
Excavator fails to train employees in OSHA excavation, trenching and supervising requirements [Conclusion 5].
Excavators' judgement is unimpaired by alcohol [Conclusion 2]
Excavators' judgement is unimpaired by drugs [Conclusion 2]
Pennsylvania excavation-damage program does not have effective means of overseeing and enforcing program's provisions. [Conclusion 9]
Pennsylvania excavation-damage program does not require excavator to mark area they propose to excavate [Conclusion 9]
Pennsylvania excavation-damage program does not require all excavators and buried facilities operators to participate in the program. [Conclusion 9]

Figure 9.14: Fault Tree Showing NTSB Conclusions about the Causes of the Explosion

The structure of the NTSB report separates the presentation of reconstruction, causal analysis and conclusions. We have, however, argued that these different activities often become blurred during the process of incident investigation. The reconstruction of an incident inevitably involves the formation and testing of causal hypotheses. Investigators include events in a reconstruction because they believe that those events have had some impact on the course of an incident. For example, if it were believed that the timing of the foreman's 911 call was critical for the analysis of the Allentown explosion then evidence would be sought so that this event could be explicitly included in any reconstruction. If the attempted call was not thought to have a significant, or potential, impact then it might be omitted. The generation and testing of such causal hypotheses against any reconstruction will inevitably affect the conclusions that can be drawn from an investigation. These links make it important that any tools, including time-lines and fault trees, do not impair the complementary activities of reconstructing an incident, generating causal hypotheses and forming conclusions.

Figure 9.14 shows how fault trees can be used to summarise the conclusions from the NTSB's investigation into the Allentown incident. Such high-level overviews are important because they help to determine whether the individual findings of an investigation form a coherent argument. For example, Figure 9.14 shows how the excavators' failure to shore-up the excavation was not simply due to individual failure on the part of the foreman and his team. The NTSB investigators also identified higher-level failures on the part of the gas company, on the excavations company and on the Pennsylvania excavation-damage program. Figure 9.14 shows how fault trees can be used to explicitly represent the relationships between these individual conclusions. The NTSB's organisational and managerial conclusions in Figure 9.14 contrast with OSHA's findings about the health and safety aspects of this incident. OSHA focuses more narrowly on the individual human errors that were represented in previous reconstructions, such as Figure 9.10:

> "OSHA determined that the EPAI foreman did not meet OSHAs definition of competence, as stated in 26 CFR 1926.650 (b). Among the failures OSHA attributed to the foreman were that he had classified the soil type incorrectly, had improperly supported the gas line, did not recognize the hazard of the gas line, did not know the lifting capacity of the chain used in the failed attempt to lift the fuel tank, did not know the lifting capacity of the backhoe, and did not keep spoil from the excavation from the top edge of the excavation." [589]

Before proposing further benefits that can be derived from using fault trees to reconstruct and summarise the conclusions of an incident investigation, it is important to acknowledge a number of weaknesses. Previous sections have argued that these is no automatic means of moving from the evidence of primary and secondary investigations to the reconstructions of Figures 9.10 and 9.11. Similarly, there is no automatic means of moving from incident reconstructions, such as Figures 9.10 and 9.11, to the conclusion overview presented in Figure 9.14. Both activities rely upon the skill and experience of individual analysts. Fault trees are, therefore, not a panacea. They simply provide a means of representing and reasoning about the products of different stages in an incident investigation.

The lack of any automated means of moving between fault tree reconstructions, illustrated in Figure 9.13, and conclusions, illustrated by Figure 9.14, should not be surprising. As we have seen, reconstructions tend to focus on the proximal events surrounding a particular incident. For example, Figure 9.10 traces the way in which initial failures on the 23rd May led to the eventual explosion in Allentown on June, 9th. However, many incident reports combine findings about specific causes with conclusions about wider failures in the managerial and regulatory system. For instance, Figure 9.14 considers problems at a State level, through the failure of the excavation damage program, and at a national level, through the lack of OSHA training for excavation workers. Hence the conclusions of an incident report are likely to draw on information that is not, typically, included within the reconstruction of a single incident.

There are further, more theoretical barriers to the automatic generation of conclusions from reconstructions. Previous chapters have argued that the interpretation and analysis of evidence is influenced by the goals and priorities of the organisations that are involved in an investigation.

Most often this is interpreted as a 'bad thing'. Organisations seek to influence or bias the findings of an investigation for commercial and even political ends. However, the social processes of incident investigation can also have a positive effect. For instance, regulators often increase the salience of particular pieces of evidence if they support the findings of previous incident reports. This is illustrated by the NTSB's emphasis on the importance of excess flow valves following the Allentown explosion. This was seen to be yet another example of an incident that might have been mitigated by the use of these devices. As a result the conclusions of the report places the Allentown incident in the context of many previous incidents that could not be explicitly considered within a reconstruction of this particular incident:

> "In the past 20 years, the Research and Special Programs Administration has failed to effectively assess the benefits of excess flow valves and has failed to promote their use." ([589], Conclusions, page 48).

Any system that attempted to generate conclusions from a reconstruction would also have to consider the wider commercial, political and regulatory environment in which it was operating. Although incident investigators must be independent from industry regulators, it is important that they work together to push through the recommendations of any enquiry. Ultimately, regulators are free to reject the findings of an investigation if they do not believe that they would lead to safety improvements. This need for independence and cooperation poses considerable social, organisational and technical challenges.

A more serious criticism of the fault tree notation, illustrated in Figure 9.14, is that it fails to distinguish between contextual and contributory factors and the root causes that were introduced in Chapter 6.4. Andrews and Moss maintain that fault trees are intended to record the "immediate, necessary and sufficient" events that contribute to any failure [27]. As a result, almost every conclusions represented in Figure 9.14 is elevated to the status of a root cause. There is no way of representing the observation that Pennsylvania's ineffective excavation damage program might have *contributed* to the incident but did not directly *cause* it. Such distinctions might be represented by introducing additional syntactic features into the basic fault tree notation. However, this would sacrifice many of the benefits associated with the use of an existing and well understood notation. Chapter 9.3 will explore these issues in greater detail. For now it is sufficient to observe that although it is possible to use fault trees to provide an overview both of the events leading to an incident and of the conclusions that can be drawn from an incident, there remain a number of theoretical and practical barriers to this application of the existing notation.

Figure 9.14 focussed on the failures that led from the damaged pipeline to the eventual explosion. In contrast, Figure 9.15 shows how the consequences of this incident were largely determined by the response *after* the pipeline was damaged. For example, the Allentown investigation found that the city's mounted an effective response to this incident. Careful preparation and training were guided by the lessons of previous incidents:

> "The executive director stated that the housing authority had procedures for evacuating the occupants and that the residents practiced the routines. For example, every 6 months the fire department conducted fire inspections and drills that also tested the evacuation procedures and emphasized how important it was for the residents to respond promptly. The drills included special precautions for the elderly and handicapped; and after a drill was held, all residents participated in a critique. Placards were posted on the windows and doors of apartments that had handicapped occupants and of rooms in which occupants were using pressurised oxygen." [589]

Figure 9.15 uses a HOUSE event to represent the finding that the housing association and the city's emergency response were appropriate. Previous sections have shown how these events can be 'turned' on or off during any walk-through of the causal model. As a result, analysts are encouraged to hypothesise about the potential impact of an ineffective response. In Figure 9.15, this would indicate a failure to learn from previous incidents and ultimately would have contributed to injury and a loss of life during the incident.

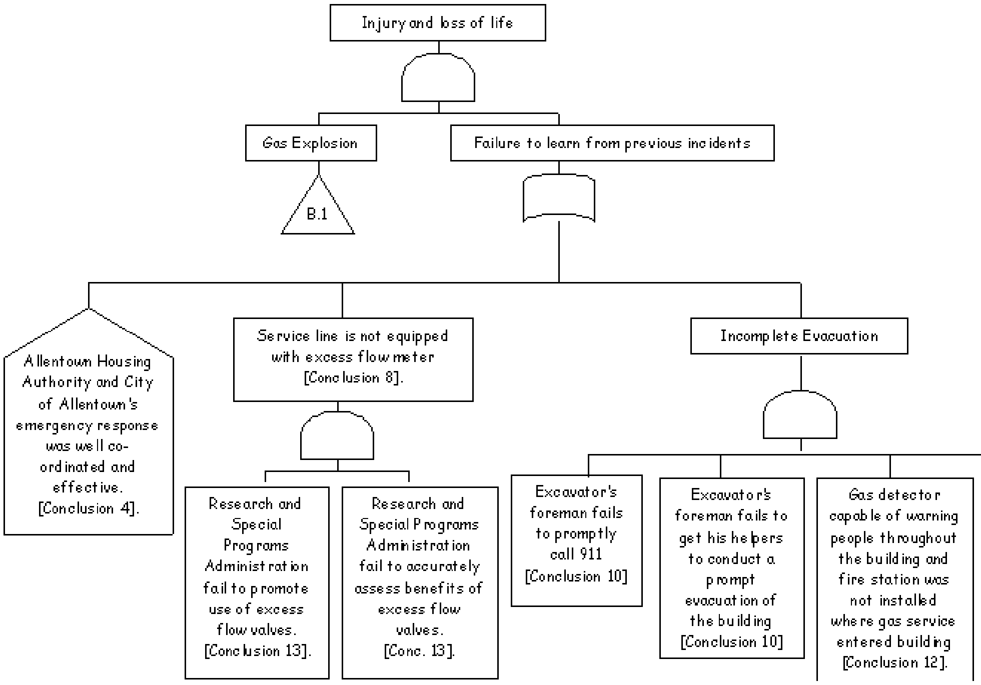

Injury and loss of life
Gas Explosion
B.1
Failure to learn from previous incidents
Allentown Housing Authority and City of Allentown's emergency response was well co-ordinated and effective. [Conclusion 4].
Service line is not equipped with excess flow meter [Conclusion 8].
Incomplete Evacuation
Research and Special Programs Administration fail to promote use of excess flow valves. [Conclusion 13].
Research and Special Programs Administration fail to accurately assess benefits of excess flow valves. [Conc. 13].
Excavator's foreman fails to promptly call 911 [Conclusion 10]
Excavator's foreman fails to get his helpers to conduct a prompt evacuation of the building [Conclusion 10]
Gas detector capable of warning people throughout the building and fire station was not installed where gas service entered building [Conclusion 12].
Excavation crew members are not trained in handling an emergency [Conclusion 11]

Figure 9.15: Fault Tree Showing Conclusions about Injuries and Loss of Life

The previous analysis raises many questions about the role of organisational failure in incidents and accidents. For instance, Figure 9.15 suggests that the lack of an excess flow valve or meter is an indication of a failure in organisational learning. As we have seen, the NTSB investigators argued that this stemmed from the Research and Special Programs Administration's failure to promote or to accurately assess the benefits of these devices. However, it is not certain that such devices will always prevent incidents such as the Allentown explosion. This objection can be represented by replacing the basic events in Figure 9.15 with an inhibit gate, as shown in Figure 9.16. Analysts could then assign a probability to the likelihood that an EFV would have cut the supply of gas either before or after the explosion. It might seem that it would be a trivial exercise to derive such reliability data given modern testing methods. Certainly, it ought to be easier to assess the reliability of such devices than it is to quantify human reliability assessments. As we have seen, however, the economic consequences of requiring the introduction of EFVs led to considerable debate about their reliability and utility between the supply industry and their regulators:

> "The two-accident sample RSPA (Research and Special Programs Administration within the Department of Transportation responsible for pipeline safety) used in its 1995 study to assess EFV effectiveness is statistically insignificant. Even so, RSPA incorrectly assessed what happened in the two accidents it did use. Although a life was saved when an EFV operated properly in one of the accidents, RSPA attributed its benefit as only one fifth of the \$ 2.6 million used by the study as the value of a life. That error was further compounded by using 57 percent as an assumed EFV effectiveness percentage. When Safety Board representatives met with RSPA on March 16, 1995, it questioned RSPA about the basis for the effectiveness percentage. A RSPA economist explained that 95 percent effectiveness was initially used, but that number was reduced because a National Highway Traffic Safety Administration (NHTSA) analyst, not knowledgeable about EFVs, said he believed the number was to high. RSPA stated that even though it had no justification for a different percentage, it offered 57 percent as the effectiveness percentage, and the NHTSA analyst accepted it, saying that it seemed about right.

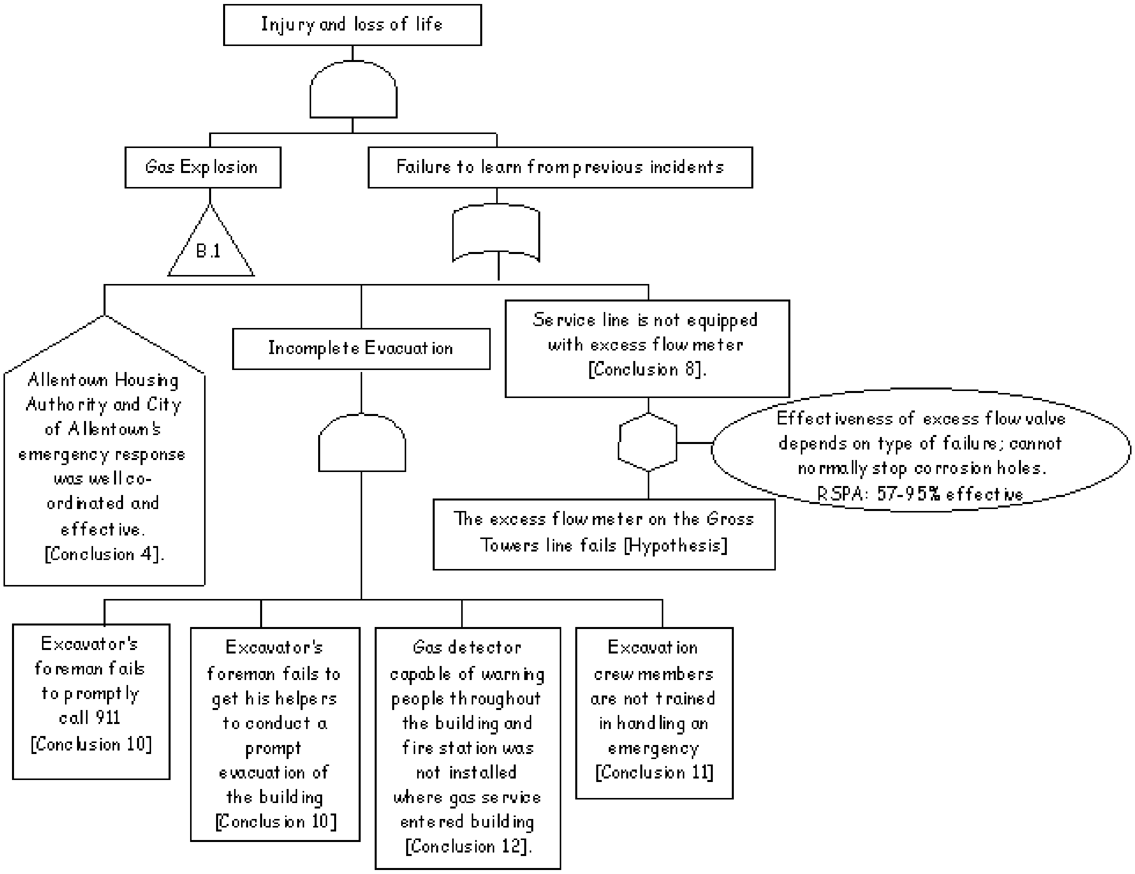

Injury and loss of life
Gas Explosion
Failure to learn from previous incidents
B.1
Allentown Housing Authority and City of Allentown's emergency response was well co-ordinated and effective. [Conclusion 4].
Incomplete Evacuation
Service line is not equipped with excess flow meter [Conclusion 8].
Effectiveness of excess flow valve depends on type of failure; cannot normally stop corrosion holes. RSPA: 57-95% effective
The excess flow meter on the Gross Towers line fails [Hypothesis]
Excavator's foreman fails to promptly call 911 [Conclusion 10]
Excavator's foreman fails to get his helpers to conduct a prompt evacuation of the building [Conclusion 10]
Gas detector capable of warning people throughout the building and fire station was not installed where gas service entered building [Conclusion 12].
Excavation crew members are not trained in handling an emergency [Conclusion 11]

Figure 9.16: Fault Tree Showing Conclusions about Reliability of Excess Flow Valves

> Other parts of RSPA's study appear to include similar insupportable numbers and assumptions." [589]

This quotation illustrates the way in which reliability data assumes a particular social and organisational significance in the aftermath of an incident. It is important to emphasise that quantitative reliability assessments are not always objective and that their true value is often questioned in the aftermath of an adverse occurrence.

9.1.3 Petri Nets

The previous section has shown how Fault-trees can be used to reconstruct the events that lead to incidents and accidents. We have also shown how they can be used to provide an overview of the conclusions that emerge from the subsequent analysis of those reconstructions. However, we have also noted a number of limitations in using this notation to distinguish between root causes and other contributory or contextual factors. The European Federation of Chemical Engineering's International Study Group On Risk Analysis also concludes:

> "Fault-trees have difficulties with event sequences... parts of systems where sequence is important are, therefore, usually modelled using techniques more adept at incorporating such considerations" [189].

We have tried to address this criticism by annotating events with real-time labels. However, this creates additional problems for analysts who must represent the way in which many failures emerge over a prolonged period of time. For example, the Allentown pipeline was left with inadequate support from the 23rd May until the 9th June. The following pages, therefore, introduce an alternative graphical notation that can be used to reconstruct the events that contribute to safety-critical incidents.

Petri Nets were developed to support the engineering of concurrent systems [460]. Chretienne shows how they can be used to represent and reason about timing properties of different systems designs [165]. Some notable attempts have been made to represent human factors requirements using this notation. For instance, Van Biljon exploits Petri Nets to derive formal specifications of interactive systems at a very high level of abstraction [81]. Bastide and Palanque have used this notation to represent the design of an interactive database [69, 665]. Hura and Attwood have used Petri Nets to support accident analysis from the perspective of hardware and software engineering engineering [379]. In contrast, this sections uses the same notation to reconstruct the more general systems failures that characterise safety-critical incidents.

A number of limitations complicate the application of Petri Nets to analyse accidents that involve interactive systems. In particular, they do not capture 'real' time. Various modifications have been applied to the classic model. Levi and Agrawala use 'time augmented' Petri Nets to introduce the concept of 'proving safety in the presence of time' [488]. Unfortunately, these enhancements are too complex to provide practicable tools for incident analysis. The following pages, therefore, retain a most basic form of the Petri Nets notation. It should be noted, however, that a range of modelling tools are significantly reducing the burdens associated with more advanced, time-augmented and stochastic extensions.

Petri Nets have been specifically developed to represent the complex sequencing and synchronisation constraints that cannot easily be captured by fault trees and time-lines. They can be used to reconstruct an incident in terms of the conditions that are satisfied at particular moments [679]. These conditions together help to represent the state of the various systems, individuals and groups that are involved in an adverse occurrence. The state of these diverse and distributed components will change during the course of an incident. Petri Nets model this by representing the way in which certain events can occur if particular conditions hold. If an event takes place then it can alter the state of the people, systems etc involved in the incident. Changes in state are represented by the new conditions that hold after an event has occurred. These new conditions enable further events to take place.

Places can be used to describe the conditions which hold for operators and their systems during the course of an incident. In our case study, investigators might use a place to represent the fact that the gas line is exposed. Another place can represent the fact that the excavation is undertaken on the incorrect assumption that the soil has a compression strength of 1.5 tons per square foot. Such places describe the causes of an incident at an extremely high level of abstraction. Places can also be used to represent causes which are specifically related to the human factors or systems engineering of an application. Places can be used to represent human factors observations about the behaviour of individual operators; the Allentown Fire Inspector is concerned about the consequences of the land slide. They can represent environmental attributes, such as the soil around the tank that is being extracted is contaminated with fuel. Places might also represent the behaviour of individual systems; the hydraulic hammer is breaking up the concrete base.

Transitions can be used to represent the events that trigger incidents and accidents. The initiating event leading to the Allentown explosion can be identified as the Foreman's over-estimate about the potential strength of the soil that he was excavating:

> "The foreman evaluated the soil being excavated as OSHA Type A, which is cohesive soil with an unconfined compressive strength of 1.5 tons per square foot. (OSHA's post-accident evaluation indicated that a visual evaluation of the soil should have shown that it was OSHA Type C, which is a cohesive soil with an unconfined compressive strength of 0.5 ton or less per square foot.) While an Allentown inspector was inspecting the EPAI's work, he saw the excavation's west sidewall slide into the excavation exposing the gas line, which was about 3 to 4 feet west of the tank. The collapsed sidewall removed the soil support from about 30 feet of the gas line, causing it to sag." [589]

The foreman's over-estimate of the soil strength can be represented as a transition that changes the state of the wider 'system' into one in which an excavation proceeds with inadequate precautions. This can be represented as a place that, if marked, can lead to a further transition, which triggers the land slip. Isolating these critical transitions provides a focus for subsequent analysis. In particular, the previous analysis might provoke greater discussion of the reasons why the foreman made an incorrect assessment of the soil strength.

Petri Nets have a formal syntax and semantics. The structure of valid networks and the meaning of those networks can be precisely defined using relatively simple mathematical concepts. Petri Nets are directed graphs; $PN = (P, T, E, M)$. They consist of a set of places, P, transitions, T, edges, E and markings, M. Edges connect places to transitions: $E \subseteq \{P \times T\} \cup \{T \times P\}$. They can be used to form the chains of events and conditions that lead to an accident. They can be described in terms of two functions. The function *Op* maps from each transition to its set of output places. The output places of a transition represent the conditions which hold after an event has occurred. For example, an output place can be used to represent the observation that the gas line is exposed after the land slip has occurred. An input place function, *Ip*, maps from each transition to the set of input places for that transition. The input places of a transitions specify the conditions which must hold for an event to occur. The input place of a transition can be used to represent the observation that the incorrect assumption about soil strength during the excavation led to the soil slip.

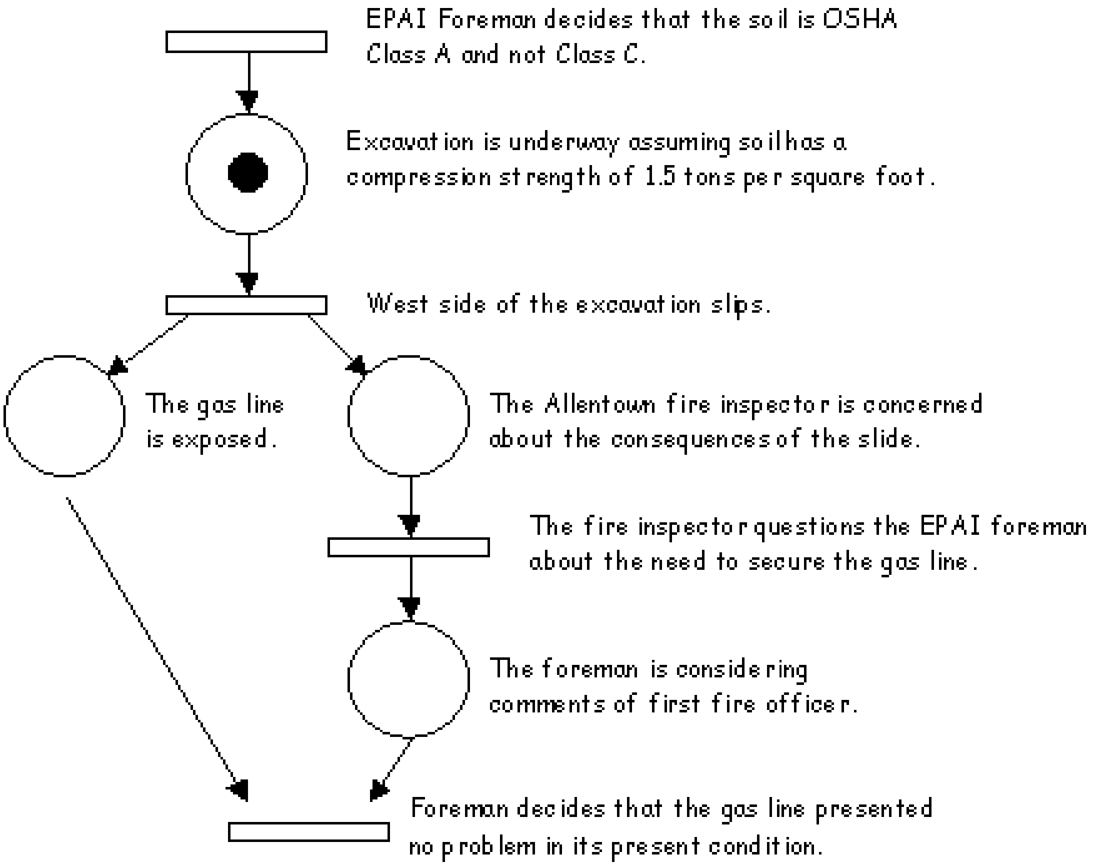

EPAI Foreman decides that the soil is OSHA Class A and not Class C.
Excavation is underway assuming soil has a compression strength of 1.5 tons per square foot.
West side of the excavation slips.
The gas line is exposed.
The Allentown fire inspector is concerned about the consequences of the slide.
The fire inspector questions the EPAI foreman about the need to secure the gas line.
The foreman is considering comments of first fire officer.
Foreman decides that the gas line presented no problem in its present condition.

Figure 9.17: Petri Net of Initial Events in the Allentown Incident

Fortunately for those who are more interested in the application than in the formal underpinnings of this notation, Petri Nets also have a graphical representation. Events, or transitions, are shown as bars (–). Conditions, or places, are denoted by unfilled circles (○). Edges are shown as arrows linking places and transitions. Figure 9.17 shows how a Petri net can represent the events leading up to the Allentown incident. The filled in circles represent tokens. These 'mark' the unfilled circles, or places, that represent assertions about th e state of the system. In this diagram, a place is marked to show that the excavation is underway assuming that the soil has a compression strength of 1.5 tons per square foot. An important benefit of the Petri Net notation is that analysts can simulate the flow of events in an accident model by altering the markings in a network. This is done through an iterative process of marking and firing. If all of the places leading to a transition, denoted by the rectangles, are marked then that transition can fire. In Figure 9.17, the transitions labelled West side of excavation slips can fire. All of the output places from this transition will then be marked. For example, if the place labelled West side of excavation slips were to fire then the places The gas line is exposed and The Allentown fire inspector is concerned about the consequences of the slide would be marked and the tokens in places that triggered this transition would be removed.

In order to simulate the dynamic events during an incident, tokens are used to mark those places in a Petri Net which are enabled. A place is enabled if its conditions hold. The tokens in a net are said to characterise a marking state and are denoted graphically by filled dots (•). For instance, Figure 9.18 is marked to show that the gas line is exposed and that both of the Allentown Fire Inspectors are concerned about the consequences of the slide. Analysts can alter the marking of a Petri Net to indicate the different conditions that hold for operators and their systems. These walk-throughs can be used to simulate the sequences of events and states that arise during accident scenarios. A transition can fire if all of its input places contain at least one token. After firing, a token is deposited in each of the output places of a transition. A single token is removed from all of the input places to that transition. In Figure 9.18 it is possible for the transition indicating that the first fire inspector questions the EPAI foreman about the need to secure the gas line to fire. The transition showing that the second fire inspector also questions the EPAI foreman about the need to secure the gas line can also fire. If these transitions fired then the places indicating that the Foreman is considering there comments would be marked. The transition showing that the Foreman decides to support the gas line can only fire if both of these places were marked together with the place indicating that the gas line is still exposed.

Incidents and accidents are often caused by the interaction between many different, concurrent users and systems [80, 279]. Figure 9.18 shows how Petri Nets can be used to represent one aspect of the interaction. In particular, this diagram shows how the first and second inspectors persuade the foreman to shore the gas line with saw horses. Although Figure 9.18 does not represent the real-time characteristics of the Allentown incident, it does accurately represent more abstract synchronisation properties. For instance, both the first and the second fire inspectors must question the need to support the pipeline before the Foreman considers supporting it. This is represented in Figure 9.18 by the places that lead to the transition labelled Foreman decides to shore the gas pipe with saw horses. This transition cannot fire until both of the places are marked to show that the Foreman is considering the implications of the inspectors' warning.

Figure 9.18 illustrates the common observation that initial failures seldom lead 'directly' to safety-critical incidents. The foreman had the opportunity to avert the Allentown explosion by correctly supporting the gas line. Indeed, the actions that he took in shoring-up the pipeline may have delayed its failure. Figure 9.18 also illustrates another important point about the reconstruction of complex failures. The resulting models often embody particular views and assumptions about the events leading to an incident. For example, the NTSB investigation obtained witness statements from Housing Association employees who:

> "...frequently passed the excavation between May 23 and June 9 stated they observed that the exposed pipe was not supported." [589]

This statement is ambiguous. It is difficult to be certain whether the employees could not see the supports, whether they saw the supports and believed them to be insufficient or whether there really were no supports there at all. Figure 9.18 does not consider such additional evidence and simply shows that the saw horses were in place throughout this period. However, Petri Nets can be used to develop alternative reconstructions that reflect these different interpretations of the available evidence. If the differences between these models were considered to be significantly important to

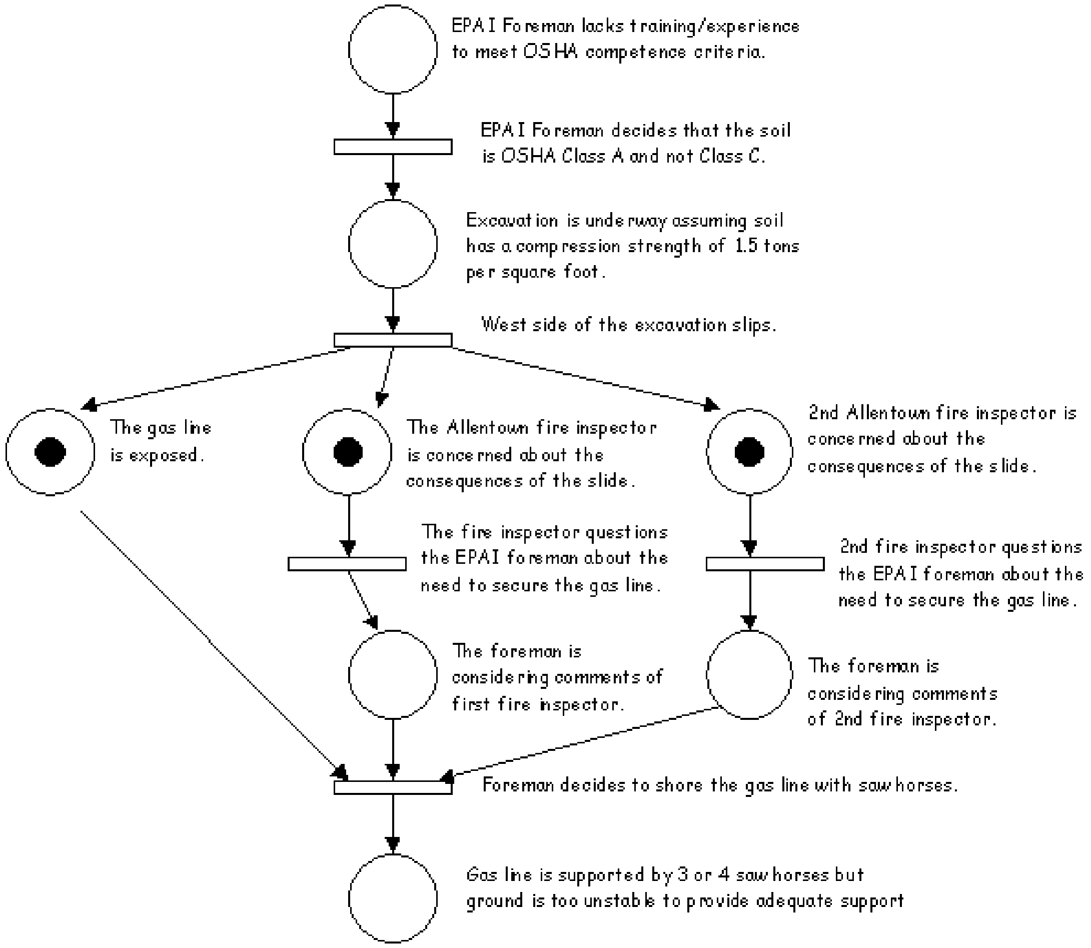

EPAI Foreman lacks training/experience to meet OSHA competence criteria.
EPAI Foreman decides that the soil is OSHA Class A and not Class C.
Excavation is underway assuming soil has a compression strength of 1.5 tons per square foot.
West side of the excavation slips.
The gas line is exposed.
The Allentown fire inspector is concerned about the consequences of the slide.
2nd Allentown fire inspector is concerned about the consequences of the slide.
The fire inspector questions the EPAI foreman about the need to secure the gas line.
2nd fire inspector questions the EPAI foreman about the need to secure the gas line.
The foreman is considering comments of first fire inspector.
The foreman is considering comments of 2nd fire inspector.
Foreman decides to shore the gas line with saw horses.
Gas line is supported by 3 or 4 saw horses but ground is too unstable to provide adequate support

Figure 9.18: A Petri Net With Multiple Tokens

any subsequent analysis then this should trigger further investigation. As we have seen, however, the supports were ultimately insufficient to protect the integrity of the pipeline. Figure 9.1.3, therefore, extends Figure 9.18 to show how the additional work, associated with removing the contaminated soil, placed undue stress on the exposed pipeline. It also shows how the Foreman's actions in attempting to shore-up the pipe with the saw horses can also, arguably, have helped to undermine a further defence. In particular, this partial remedy seems to have satisfied the concerns expressed by the inspectors. The first fire inspector's shift had ended by this point in the incident and so Figure 9.1.3 represents this important event by the transition labelled 2nd Fire Inspector and Foreman decide not to take any further action.

The upper components of the Petri Net in Figure 9.1.3 deal with the Foreman's decision to shore up the pipe in response to comments from the Allentown Fire Inspectors. The bottom right components deal with the catalytic events that stemmed from the decision to remove the concrete base and contaminated soil, which had surrounded the tank. The actions associated with the removal of this material placed the immediate stresses on the pipe that led to the failure of the compression coupling:

> "The tank was successfully removed from the excavation, and samples of soil were taken adjacent to the tank's concrete support, which remained in the excavation. The soil was to be tested to determine whether fuel had leaked from the tank and contaminated the surrounding soil. The EPAI foreman stated that before he and the other crewmembers left the site, they tried to support the pipe with saw horses, surrounded the excavation with orange plastic barrier fencing, put plastic sheeting over the excavation slopes, including the soil that lay beneath the pipe, and removed the equipment from the site... Fifteen days later, on June 9, after the EPAI received the test results, which showed that the soil around and beneath the concrete tank support had been contaminated, EPAI employees returned to remove the concrete support and contaminated soil... The backhoe (a track-mounted excavator) arrived about 12:30 p.m., and a hydraulic hammer was installed on the backhoe bucket to break up and remove the tank's concrete support. The foreman stated that he and his crewmembers removed the saw horses from beneath the pipe as the first step in removing the concrete support. He said they did not notice any movement of the pipe and did not smell any gas. The equipment operator, not the same person who had excavated the tank in May, used the backhoe to break up and remove the concrete and to excavate the fuel-contaminated soil. It took about 6 hours for the hydraulic hammer to break the concrete up. According to the EPAI employees, the impact of the hammer caused the ground to vibrate significantly. The backhoe bucket was used to remove the broken concrete and to load the pieces into a dump truck. The path of the backhoe bucket crossed over the pipe. The backhoe operator said that about 6:40 p.m. he moved the backhoe from a spot south of the excavation to one on the west. In moving it, he crossed a buried section of pipeline that was between the excavation and the north wall of Gross Towers. The odour of gas was first detected about 6:45 p.m." [589]

In Figure 9.1.3, this trigger event is represented by the transition labelled EPAI test results show the need to remove the concrete base and surrounding soil. This transition can fire because the place labelled Soil around the tank is contaminated with fuel is marked. If, however, the soil were not contaminated then this place would not have been marked and the transition could not have fired. However, as we know, the EPAI test result were positive. As a result, the associated transition can fire. This will deposit tokens in the output places that are connected to this transition in Figure 9.1.3. The new marking shows that the saw horses supports are removed to allow the access that is necessary for the work to commence. The marking will also show that a hydraulic hammer is used to break up the concrete base and that the backhoe's path crosses a buried portion of the pipeline.

It is important to note, however, that Figure 9.1.3 represents the events that led to the failure of the compression coupling. As with previous reconstructions in this chapter, it does not explicitly identify ways in which the incident could have been avoided. This illustrates an important point

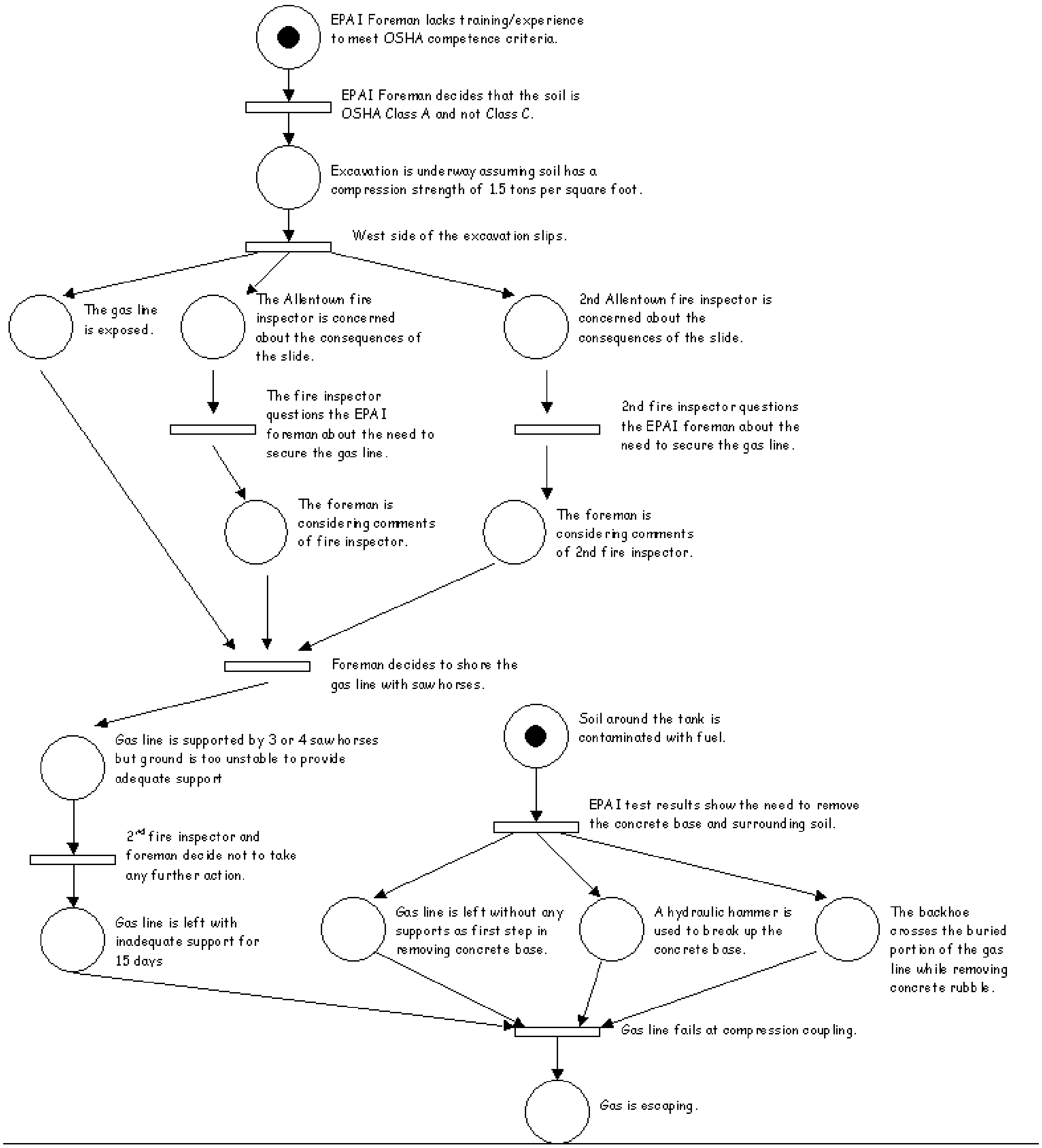

EPAI Foreman lacks training/experience to meet OSHA competence criteria.
EPAI Foreman decides that the soil is OSHA Class A and not Class C.
Excavation is underway assuming soil has a compression strength of 1.5 tons per square foot.
West side of the excavation slips.
The gas line is exposed.
The Allentown fire inspector is concerned about the consequences of the slide.
2nd Allentown fire inspector is concerned about the consequences of the slide.
The fire inspector questions the EPAI foreman about the need to secure the gas line.
2nd fire inspector questions the EPAI foreman about the need to secure the gas line.
The foreman is considering comments of fire inspector.
The foreman is considering comments of 2nd fire inspector.
Foreman decides to shore the gas line with saw horses.
Soil around the tank is contaminated with fuel.
Gas line is supported by 3 or 4 saw horses but ground is too unstable to provide adequate support
EPAI test results show the need to remove the concrete base and surrounding soil.
2nd fire inspector and foreman decide not to take any further action.
Gas line is left with inadequate support for 15 days
Gas line is left without any supports as first step in removing concrete base.
A hydraulic hammer is used to break up the concrete base.
The backhoe crosses the buried portion of the gas line while removing concrete rubble.
Gas line fails at compression coupling.
Gas is escaping.

Figure 9.19: A Petri Net Showing Catalytic Transition.

about the use of graphical notations, including time-lines, Fault trees and Petri Nets. They provide concise means of capturing the events that lead to incidents and accidents. They provide communications tools and can be shown to the other participants in an enquiry. They do not provide a panacea for the problems of incident analysis. In particular, they do not replace the judgemental skills that must be developed by human factors and systems engineers. In our scenario, there is no automatic means of moving between the Petri Net representation and the remedies that can prevent an incident from recurring.

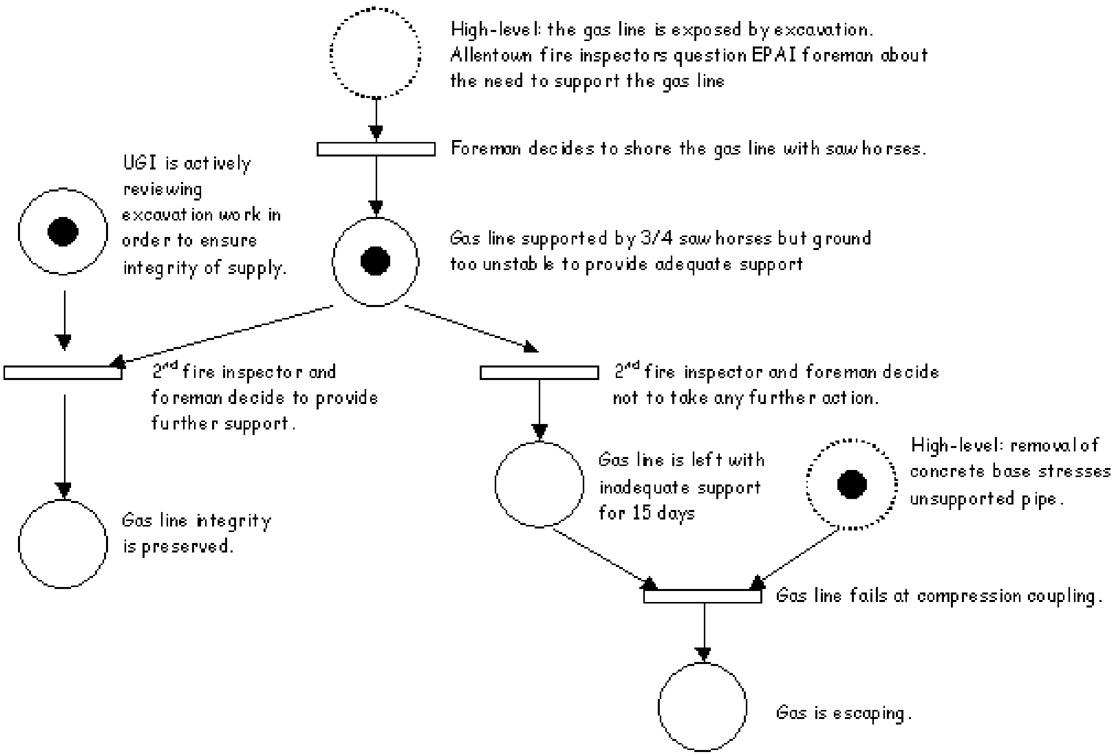

High-level: the gas line is exposed by excavation. Allentown fire inspectors question EPAI foreman about the need to support the gas line
Foreman decides to shore the gas line with saw horses.
UGI is actively reviewing excavation work in order to ensure integrity of supply.
Gas line supported by 3/4 saw horses but ground too unstable to provide adequate support
2rd fire inspector and foreman decide to provide further support.
2rd fire inspector and foreman decide not to take any further action.
Gas line is left with inadequate support for 15 days
High-level: removal of concrete base stresses unsupported pipe.
Gas line integrity is preserved.
Gas line fails at compression coupling.
Gas is escaping.

Figure 9.20: A Petri Net Showing Conflict

Previous paragraphs have shown how Petri Nets can be used to represent important events in the course of an incident. Investigators can also exploit this notation to hypothesise about alternative scenarios. Figure 9.1.3 represents two possible outcomes for the Allentown incident. One terminating place shows that gas is escaping. The other shows that the integrity of the supply is preserved. Analysts can use such networks to focus attention upon techniques that are intended to prevent future incidents. Human factors and systems engineering must be exploited so that the transition, labelled 2nd Fire Inspector and Foreman decide not to take further action, never fires. The reason we are concerned to disable this transition is that it is one possible outcome from what is known as a conflict situation. The place labelled Gas line is supported by 3 or 4 saw horses but ground is too unstable to provide adequate support is marked. As a result, it is possible to fire either the transition indicating no further action or the transition representing the decision to provide additional support. The network does not indicate which of these two possible transitions will fire. Given this marking we can, however, be sure that only one will fire and that they cannot occur simultaneously. Firing the transition indicating no further action would remove a token from the place labelled Gas line is supported by 3 or 4 horses but ground is too unstable to provide adequate support. This would disable the transition indicating that the 2nd Fire Inspector and the Foreman decide to provide further support. Conversely, firing the transition which indicates further actions would lead to a marking for the place labelled Gas line integrity is preserved. Petri Nets that include these conflict situations are non-deterministic. Any one of the transitions from a marked place can be selected for firing. In more conventional applications of the Petri Net notation it is, typically, important to detect and remove such non-determinism; it indicates an apparently random behaviour on the part of any proposed system. In incident reconstruction, however, this technique can be used to represent the non-determinism which is inherent in many complex multi-user, multi-system applications. This can, however, be problematic if investigators want to model the likely path of an incident rather than possible alternative behaviours.

Conflict situations represent critical stages in an incident reconstruction. Non-determinism indicates a loss of control over the behaviour of the ‘system’. It is, therefore, important that the recommendations from an incident report will remove conflict from the Petri Net reconstruction of an incident. For example, the NTSB enquiry recommended that the excavation contractor should:

> “Modify its excavation-damage prevention program to include the review and close monitoring of any proposed excavation near a gas service line, including any line with unanchored compression couplings, that is installed near a building and that, if damaged, might endanger public safety significantly. (Class II, Priority Action) (P-96- 5)” [589]

Inhibitor arks provide a means of representing the intended effect of such recommendations. Transitions which are linked by an inhibitor can only fire if the place from which the inhibitor comes is not marked. Inhibitors are represented graphically as an edge with a small empty circle on one end. In Figure 9.1.3 an inhibitor arc is shown running from the place labelled Foreman and employees trained in OSHA and company health and safety program for excavation and training to the transition marked 2nd Fire Inspector and Foreman decide not to take any further action. The input place to this inhibitor is marked. In consequence, Figure 9.1.3 can be interpreted as stating that any decision to reject further actions cannot be taken because the Foreman’s training ‘inhibits’ him from leaving the excavation partially supported.

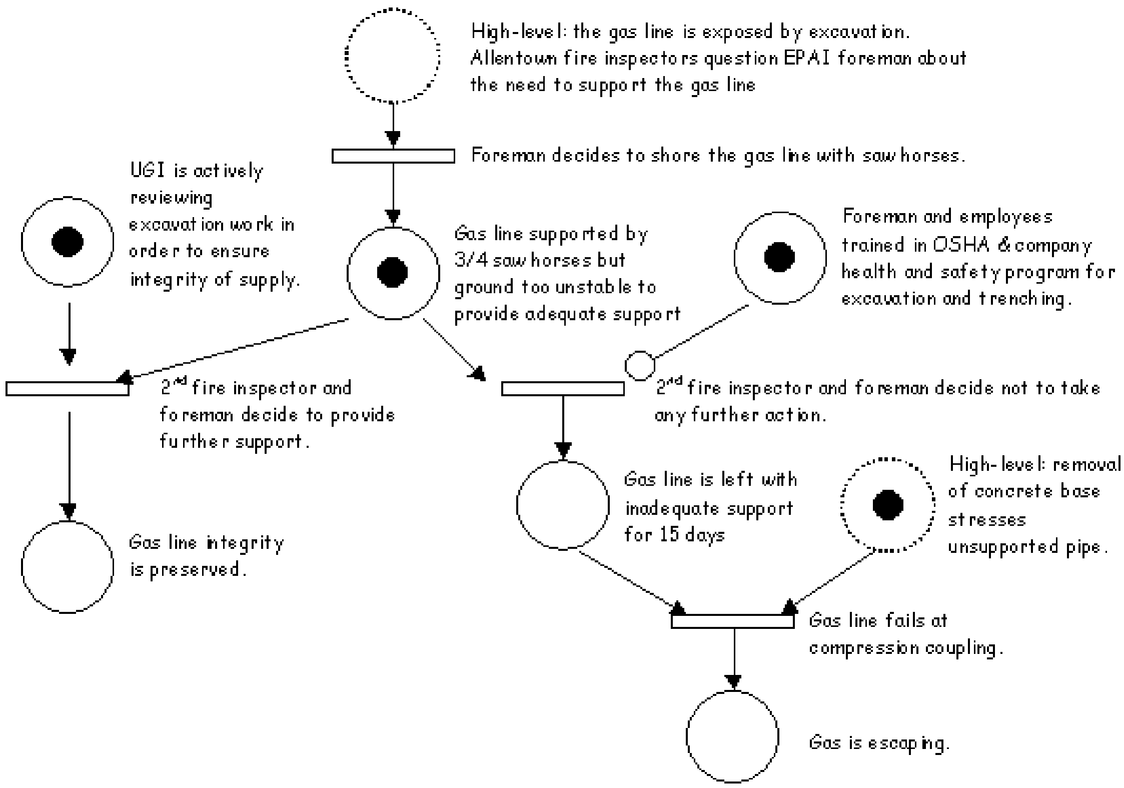

High-level: the gas line is exposed by excavation. Allentown fire inspectors question EPAI foreman about the need to support the gas line
Foreman decides to shore the gas line with saw horses.
UGI is actively reviewing excavation work in order to ensure integrity of supply.
Gas line supported by 3/4 saw horses but ground too unstable to provide adequate support
Foreman and employees trained in OSHA & company health and safety program for excavation and trenching.
2nd fire inspector and foreman decide to provide further support.
2nd fire inspector and foreman decide not to take any further action.
Gas line is left with inadequate support for 15 days
High-level: removal of concrete base stresses unsupported pipe.
Gas line integrity is preserved.
Gas line fails at compression coupling.
Gas is escaping.

Figure 9.21: A Petri Net With An Inhibitor Avoiding Conflict.

The recommendation represented by the inhibitor arc in Figure 9.1.3 is insufficient to guarantee the safety of the system. The transition labelled 2nd Fire Inspector and Foreman decide to provide further support cannot fire unless the place marked UGI is actively reviewing excavation work in order to ensure integrity of supply is also marked. In other words, improvements in the training of excavation teams might have encouraged the foreman not to leave the gas line partially supported by the saw horses. However, this need not have guaranteed that any eventual actions would have adequately addressed the risks posed by the exposed pipeline. The participation and oversight of the gas supply company might have provided increased confidence that positive actions would be taken to address any damage that had been sustained. The place labelled UGI is actively reviewing excavation work in order to ensure integrity of supply, therefore, represents the NTSB's additional recommendation that the gas supply company must:

> "Modify its excavation-damage prevention program to include the review and close monitoring of any proposed excavation near a gas service line, including any line with unanchored compression couplings, that is installed near a building and that, if damaged, might endanger public safety significantly. (Class II, Priority Action) (P-96- 5)" [589]

In Figure 9.1.3 this place is marked and so the transition labelled 2nd Fire Inspector and Foreman decide to provide further support can fire. This in turn will mark the place indicating that Gas line integrity is preserved.

Previous Petri Nets represent the Allentown incident at an extremely high level of abstraction. This is inappropriate for the later stages of incident reconstruction. For instance, it may be necessary to model the detailed gas flow into the Housing Association's building. In fact, this was done to determine that the gas flowed underground to Gross Towers. It then passed through openings in the buildings foundation into the space beneath the mechanical room, which served as a combustion air intake reservoir for boilers. The gas then passed through openings in the floor of the building's mechanical room from where it migrated to other floors through the adjacent boiler exhaust tower, through a rubbish chute and through floor openings for electrical and other building services. It may also be important to reconstruct the more detailed cognitive and perceptual factors that influence an individual's response to potential accidents. For instance, the NTSB interviews revealed that the Foreman did not share the First Fire Inspector's concerns because he believed that the pipe did not use compression joints:

> "The fire inspector said that he questioned the EPAI foreman about the need to secure the gas line. He said that the foreman told him the condition presented no problem because the gas line was an all welded system. (The foreman later stated that based on his experience he believed all gas systems were welded)." [589]

This reconstruction is revealing because it implies that the inspector was prepared to accept the foreman's judgement. He assumed that the foreman had greater technical competence than, in fact, he did. Petri Nets can also be used to model these details. Places and transitions can be replaced by sub-networks to provide finer grained representations. The transition labelled High-level: The Fire Inspector questions the EPAI foreman about the need to secure the gas line can be refined into the sub-network shown in Figure 9.1.3.

Ths more detailed reconstruction of the incident can help to generate further hypotheses and questions. For instance, the previous paragraphs have focussed on the NTSB's recommendations about the need to improve the training of excavation crews. They have also incorporated the recommendations for improved monitoring by service suppliers into Figure 9.1.3. However, experience has shown that improved training and manual surveillance cannot be relied upon to guarantee the safety of future systems. In consequence, the NTSB investigators focussed most of their attention on the potential benefits of EFV's. These were discussed in the section on graphical time-lines. However, the Petri Net reconstruction of Figure 9.1.3 also suggests questions about the nature and origin of the disrepancy between the Foreman's mental model of the pipeline construction and the actual techniques that were used to build it. In particular, subsequent analysis might focus on why compression joints are not routinely anchored to provide increased protection against longitudinal

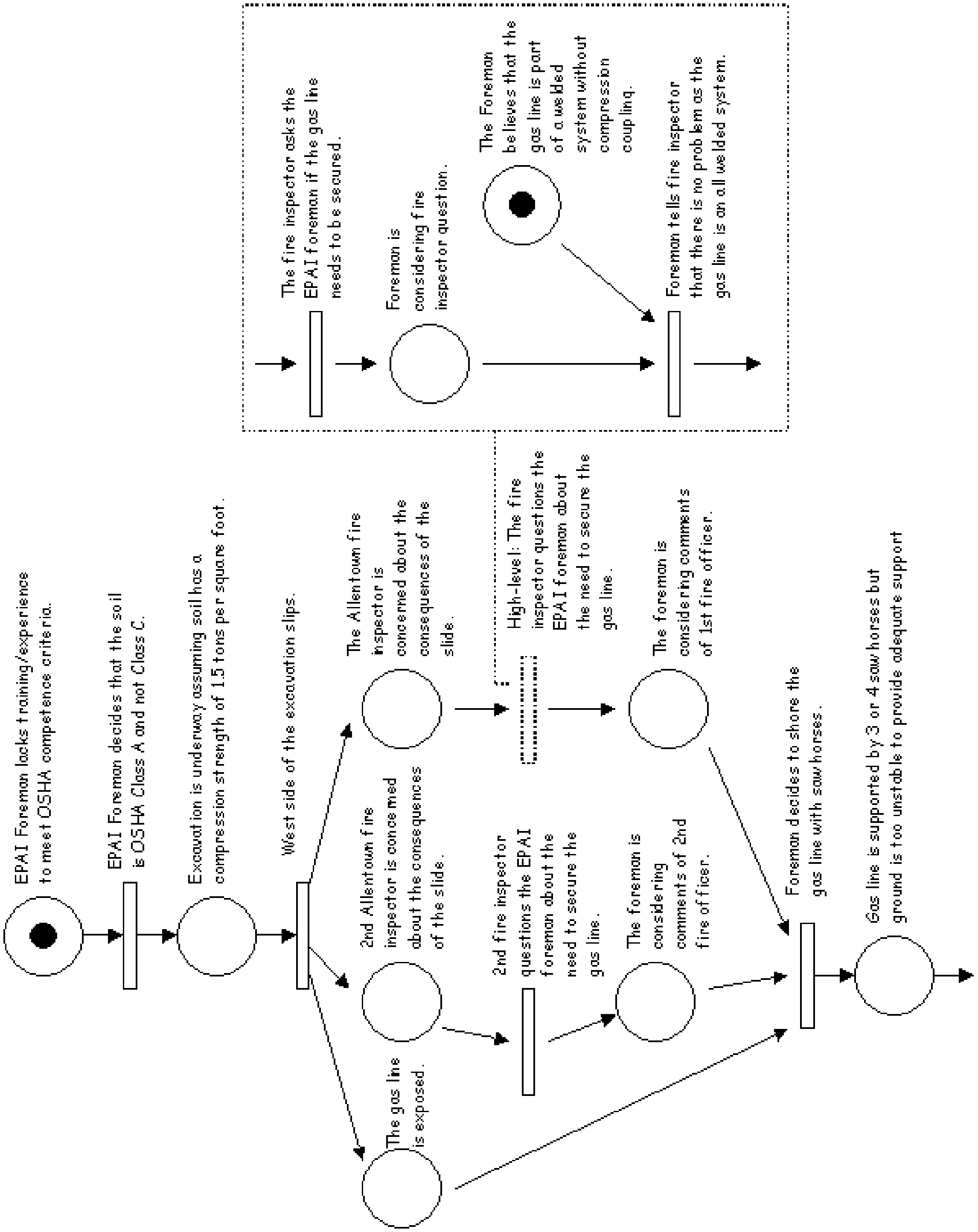

EPAI Foreman lacks training/experience to meet OSHA competence criteria.
EPAI Foreman decides that the soil is OSHA Class A and not Class C.
Excavation is underway assuming soil has a compression strength of 1.5 tons per square foot.
West side of the excavation slips.
The Allentown fire inspector is concerned about the consequences of the slide.
2nd Allentown fire inspector is concerned about the consequences of the slide.
The gas line is exposed.
High-level: The fire inspector questions the EPAI foreman about the need to secure the gas line.
2nd fire inspector questions the EPAI foreman about the need to secure the gas line.
The foreman is considering comments of 1st fire officer.
The foreman is considering comments of 2nd fire officer.
Foreman decides to shore the gas line with saw horses.
Gas line is supported by 3 or 4 saw horses but ground is too unstable to provide adequate support
The fire inspector asks the EPAI foreman if the gas line needs to be secured.
Foreman is considering fire inspector question.
The Foreman believes that the gas line is part of a welded system without compression coupling.
Foreman tells fire inspector that there is no problem as the gas line is an all welded system.

Figure 9.22: A Sub-Net Showing Crew Interaction.

pressures. The NTSB investigators considered introduced this issue but never took it any further in either their reconstruction or analysis of the incident:

> "A note on the UGI's original service record stated that the line was 'Tied in Solid,' meaning that the pipe lengths were welded. However, to comply with 1971 Federal requirements on protecting steel pipelines against corrosion, the UGI began installing corrosion-protection systems on segments of its pipeline systems that had been installed before the requirements were adopted. The UGI's records show that on September 27, 1973, an electrically insulating compression coupling 9 was installed in the service line. Although there is no documentation of the instructions given the crewmembers about the work, records and physical evidence show that they installed an insulating compression coupling in the service line north of the wall next to the boiler room. That coupling was installed just inches south of a noninsulating compression coupling for which there are no records and which was apparently installed at the same time as the insulating coupling to obtain adequate space to install the insulating coupling. Neither compression coupling was anchored or otherwise protected against movement relative to the service pipe, nor were there any requirements for doing so." [589]

Given that the Foreman believed that the pipe was of welded construction and that it had greater longitudinal strength than it actually did, it seems important to consider the reasons why he eventually decided that the line should be support. The Petri Net in Figure 9.18 shows that this was the result of the combined comments of two of Allentown's Fire Inspectors. This reconstruction emphasizes the importance of providing confirmatory advice to support a colleague's concerns about the safety of such situations. It arguably illustrates the Inspectors' success in forcing the Foreman to reconsider the situation. However, this is a flawed interpretation of the model. If the Inspectors had been sufficiently concerned then they ought to have notified the gas supplier and halter the excavation. Instead, they acquiesced in the Foreman's view that the gas line could adequately be supported by the saw horses.

Figure 9.1.3 provides an alternative view of the reason why the Foreman reconsidered his decision not to support the pipeline. His eventual decision was partly due to the intervention of the inspectors but also to a chance incident involving asphalt from the excavation:

> "The fire inspector, the EPAI crewmembers and an EPAI management representative saw a piece of asphalt paving fall about 4 feet and strike the gas pipe. The piece was large (3 by 5 feet and 3 to 4 inches thick), and the pipe was not supported. The fire inspector said that the paving permanently deflected the pipe by about a foot. He stated that before the paving hit it, the pipe was sagging, but still fairly straight." [589]

In Figure 9.1.3, the place showing that the Asphalt is close to the exposed pipeline is marked. The transition labelled Asphalt hits gas pipe can then fire. This marks a place denoting that the gas pipe is deflected by about a foot. If the place denoting the Foreman's initial judgement is also marked then the transition labelled Foreman starts to have second thought about supporting the gas pipe can fire. Clearly this reconstruction has profound safety implications; the Inspectors intervention was not sufficient to cause the Foreman to reconsider his actions. The chance event of the asphalt deflecting the pipe was, arguably just as significant. The NTSB investigators found that:

> "Because the city's fire inspectors saw on May 23 that the service line was unsupported, they could have prevented the accident. They showed proper concern about the safety of the line, especially after a piece of asphalt pavement fell on it and deformed it. However, not having been instructed to do otherwise, both inspectors relied on the EPAI foremen's assessment that the line was safe. It would have been more prudent of them to ask the pipeline owner for the assessment. The Safety Board concludes that the likely reason the fire inspectors did not tell the operator that its service line was damaged was because the inspectors did not understand the importance of notifying operators so the effects on a facility could be assessed by the operators and necessary action taken. Had the inspectors notified the UGI, it, the Safety Board believes, would have taken the necessary corrective actions, and the accident would not have happened." [589].

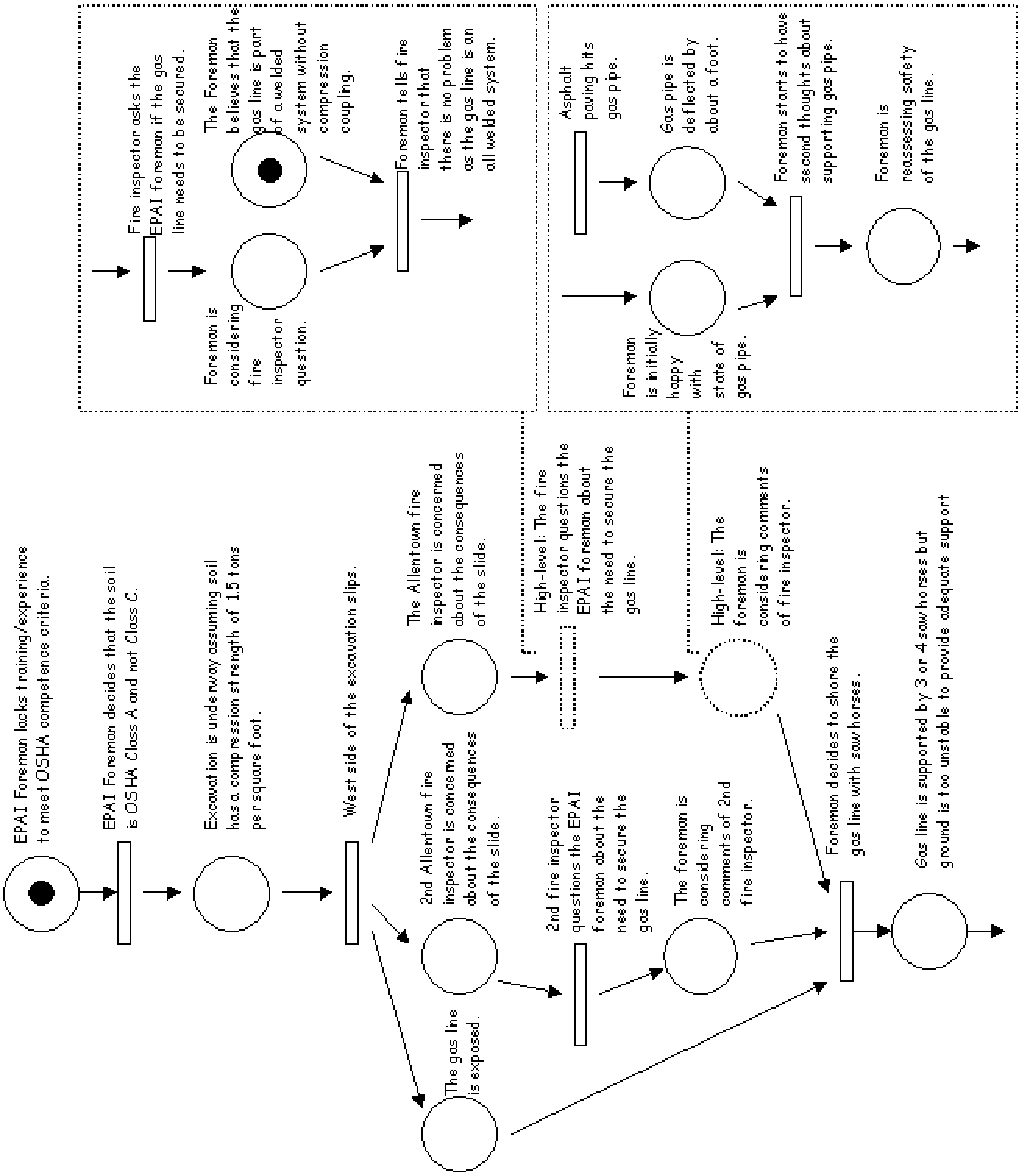

EPAI Foreman lacks training/experience to meet OSHA competence criteria.
EPAI Foreman decides that the soil is OSHA Class A and not Class C.
Excavation is underway assuming soil has a compression strength of 1.5 tons per square foot.
West side of the excavation slips.
The Allentown fire inspector is concerned about the consequences of the slide.
2nd Allentown fire inspector is concerned about the consequences of the slide.
The gas line is exposed.
High-level: The fire inspector questions the EPAI foreman about the need to secure the gas line.
2nd fire inspector questions the EPAI foreman about the need to secure the gas line.
High-level: The foreman is considering comments of fire inspector.
The foreman is considering comments of 2nd fire inspector.
Foreman decides to shore the gas line with saw horses.
Gas line is supported by 3 or 4 saw horses but ground is too unstable to provide adequate support
Fire inspector asks the EPAI foreman if the gas line needs to be secured.
Foreman is considering fire inspector question.
The Foreman believes that the gas line is part of a welded system without compression coupling.
Foreman tells fire inspector that there is no problem as the gas line is an all welded system.
Asphalt paving hits gas pipe.
Foreman is initially happy with state of gas pipe.
Gas pipe is deflected by about a foot.
Foreman starts to have second thoughts about supporting gas pipe.
Foreman is reassessing safety of the gas line.

Figure 9.23: A Sub-Net Showing Alternative Reasons for the Foreman's Decision.

Previous sections have argued that the reconstruction of an adverse occurrence forms part of an iterative process. Secondary investigations provide evidence that is used to reconstruct an incident. These reconstructions help to generate causal hypotheses. The hypotheses that emerge during the analysis of a reconstruction can force investigators to continue their search for evidence. For example, the process of using Petri Nets, such as Figure 9.1.3, to reconstruct the Allentown incident leads to further hypotheses about the reasons why the Foreman did not inform the gas supplier or provide additional support for the pipeline. In particular, the Foreman did not receive any feedback to indicate that his actions had had an adverse impact upon the pipeline. There was no smell of gas and the pipe appeared to be stable:

> "The pipe deformation caused by the asphalt pavement striking the line probably caused the pipe to be pulled out partially from the coupling because of the reduction in the effective length of the pipe. However, because there was no evidence that gas was escaping from the pipe/coupling connection before June 9, it is apparent that the activities of May 23 did not cause the pipe and coupling to separate completely." [589]

The Petri net in Figure 9.1.3 can be refined to explicitly model these observations. It is important, however, to emphasise that the successive accretion of more and more details can ultimately sacrifice the tractability of this graphical notation. Investigators must have a clear understanding of the behaviour of the incident reconstructions that are represented by a Petri Net. This task can be impaired by the additional complexity that is introduced through the use of sub-networks. It can be difficult to trace the likely passage of tokens through the many places and transitions that might used to represent the cognitive, perceptual and environmental details that contribute to a complex failure. Fortunately, this task can be eased by tools that animate the enabling and firing of transitions as tokens pass from place to place in a Petri Net. For instance, Chiola's GreatSPN can be used to view tokens as they pass through a network [164]. Investigators can record which places are marked and which transitions are enabled. The ability to play these token games greatly simplifies the development of correct models. By correct here, we mean that the model reflects the investigator's view of the incident rather than that the model correctly reflects the events leading to an incident. In contrast, this latter form of correctness depends on individual investigatory skills and on the accuracy of automated logs, mentioned in previous chapters. A further advantage of Petri Net modelling tools is that the resulting animations provide powerful means of communication. They can be shown to the many different teams that must collaborate during investigations into more serious incidents.

9.1.4 Logic

Graphical notations, such as Fault trees and Petri Nets, are not the only class of analytical tools that can be used to support incident reconstruction. A number of text based formalisms can model the events that contribute to adverse occurrences. In particular, a range of logics have been used to represent and reason about incidents and accidents [118, 415, 470]. These notations have a number of important benefits for the reconstruction of safety-critical systems:

- *formally defined syntax.* Logics, typically, have well-defined syntactic rules. These rules provide a grammar that specifies how the symbols in the logic can be combined in order to form valid sentences. These rules exist for graphical notations as well. For example, places must be connected to transitions in order to form a valid Petri Net. It would make little sense to connect a place to another place.

- *clearly defined semantics.* Logics also, typically, provide procedures for deriving the intended meaning of any sentence that obeys the syntactic rules, mentioned above. This is important because considerable confusion can arise if two different analysts can derive multiple interpretations of the same sentence. It is worth mentioned, however, that the notion of a formal semantics refers only to the information that can be directly derived or proved from the sentence itself and not to any additional, subjective judgements that might be derived from subsequent analysis.

- *proof procedures.* Logics are also supported by a set of rules that define what inferences can be made from a set of sentences. These are intended to have a close relation to the informal proof procedures that we recruit in everyday life. These 'everyday' inferences can be illustrated by the following example. If we know that 'the excavation crew at Allentown work for EPAI' and that 'the Foreman is a member of the excavation crew at Allentown' then we can conclude that the 'Foreman works for EPAI'. Proof procedures are intended to codify such inferences in order to avoid the paradoxes and fallacies that often weaken informal arguments. A paradox is a sentence that obeys the grammatical syntax rules of the language and yet is self contradictory. A good example, is the liar paradox that often frustrates the interpretation of eye witness statements. If someone says 'I am lying' then if what is said is true then it is false. If what they have said is false then it is true! Proof procedures help to identify such situations by providing rules that can demonstrate the self-contradictory nature of some grammatically valid sentences.

- *tractability.* The proof procedures, mentioned above, provide rules for manipulating the sentences of a logic to derive particular implications. There are corresponding procedures for the manipulation of textual representations for the Petri Net notation, illustrated in previous paragraphs. These techniques acknowledge that for anything but the simplest procedures it is more tractable to manipulate a textual rather than a graphical formalism. Unfortunately, it can be more difficult for non-mathematicians to interpret the meaning of textual representations than their graphical counterparts. As a result, tool support is often a necessary prerequisite for the commercial application of these techniques.

- *tool support.* Logic is an example of what have become know as 'formal methods'. These are mathematically based notations that possess the syntax, semantics and proof procedures, mentioned above. The precision and rigour provided by these features is argued to provide the increased assurance that is necessary when safety is at stake. As mentioned above, however, these benefits are often achieved at the cost of comprehension. It can be extremely difficult, even for skilled specialists, to perform the manual manipulation of mathematical sentences that are required by complex design tasks. Paradoxically, this can be an extremely error-prone activity. As a result a number of automated tools, theorem provers and model checkers, have been developed to support these tasks. Work is just beginning to improve our understanding of the errors that emerge even with this tool support [20, 21] .

- *application to both human factors and systems engineering problems.* As mentioned above, logic has been used to support the systems engineering of a range of safety-critical systems. It is also being applied to a range of human-system interaction problems. Most noticeably, a number of authors are using formal specification techniques to analyse the sources of mode confusion problems within the aviation industry [193]. Their work identifies areas in which the autopilot behaviour does not support the users' model of how the automation behaves. Ths commercial up-take of these ideas support the application of mathematically-based techniques to other forms of 'break down' during the operation of safety-critical systems.

The previous list provides some of the reasons that justify the application of logic to help reconstruct the events leading to incidents and accidents. As mentioned, however, it can initially be difficult to interpret the meaning of these formal notations. In consequence, the following pages will also provide informal readings for any notation that is presented.

Critical Components

A limitation with natural language approaches to incident reconstruction is that it can be difficult to identify critical information from a mass of background detail. For example, the NTSB's investigation into the Allentown explosion produced the following observations:

> "Post-accident surveys of 115 residents show that three Towers East occupants, in units 108, 408, and 902, had smelled gas immediately before the explosion and that two

> other occupants had smelled gas shortly before the explosion while they were in the mail room on the first floor. The occupant of unit 108 stated that he had reported the gas odour to '911,' but after the explosion." [589]

The results of this survey helped to form a more complete picture of the incident. Investigators must, however, determine whether such details are relevant to their subsequent analysis. This is important because hundreds and even thousands of items of evidence can be collected in the aftermath of a major incident. In fact, this survey were only mentioned as a parenthesis within the NTSB's final report. It might, therefore, be decided that such details could justifiably be omitted from any high-level reconstruction of the incident. The development of a logic-based model helps this process because investigators must identify significant categories of components that were involved in an adverse occurrence. The following list indicates some of the categories that have been identified from previous incidents:

- people. It is necessary to represent the people involved in an incident so that investigators can follow the way in which operator intervention affects the course of system failures;
- physical locations. It is necessary to represent the place in which an incident occurs because the location of a failure can have a profound impact upon an operator's ability to respond to that incident [406];
- warning systems. Investigators must also record the role that particular warning systems did or did not play in the course of an incident. For example, excess flow valves and gas detection equipment might have provided additional warnings about the Allentown incident;
- utterances. It is vital to represent communication between the operators that are involved in an incident. Misunderstandings have a profound impact upon the safety of many applications;
- tasks. It is necessary to identify the tasks that operators were or should have been performing during an incident if investigators are to understand the ways in which human intervention safeguarded the system or exacerbated any key failures.

For example, the following except is taken from the NTSB investigation into the Allentown incident. This quotation identifies important physical locations, such as the parking lot that the Foreman later attempted to call 911 from. It is also possible to identify key individuals, such as the Foreman, the Backhoe operator and the loader. We can also identify items of equipment such as the excavator's tools that failed to operate the valve:

> "While he was making the calls, the foreman said, he instructed the operator and the loader to trace the gas line back toward Utica Street until they found the shutoff valve. They found the valve near the north edge of the parking lot, but were unable to close it. They lacked the necessary tools to operate the below-ground valve. (Later, when the fire department representatives arrived, the EPAI workmen did not tell them they had been unable to close the valve.)" [589]

Table 9.1.4 summarises the entities that will be used in the logic-based reconstruction of the Allentown incident. It is incomplete in that the elements in the list can be expanded to enlarge the scope of the reconstruction. The identification of key individuals, locations, tasks etc is a manual, skill-based activity. It involves the subjective judgement of individual investigators. However, the outcome of this process is subject to debate and review because it can be explicitly represented in this tabular format. In formal terms, the elements of this table define the types that model the Allentown incident. The process of building such a table helps to strip out 'irrelevant' detail that can obscure critical properties of any reconstruction.

Axiom for the Accident System

The identification of people, physical locations, communication systems, equipment, utterances and tasks is of little benefit if analysts cannot represent and reason about the manner in which these components influence the course of an incident. The following section uses a simple form of temporal logic to demonstrate how this might be done for the Allentown case study.

People/Agents	Physical Locations	Warning Systems
backhoe_operator	utica_parking_lot	gas_detector
foreman	gross_towers_valve	
ugi	gross_towers	
fire_dept		
loader		
answer_service		
house_engineer		
housing_authority		
residents		
third_floor_resident		

Utterances/Messages	Tasks
gas_leak	initiate_evacuation
gas_line_hit	ventilate_building
trace_to_valve	shut_off_gas

Table 9.1: Critical Entity Table for the Allentown Incident

Operators and Locations

It is important to consider the physical location of system operators during major incidents. For instance, it is important to trace the movements of the foreman and the excavation crew after the gas was detected and before the explosion because it their locations provide valuable insights into their response to the incident. As we shall see, an appropriate response would have been to send workers to evacuate Gross Towers. Instead, the foremen sent his workers to turn off the gas supply with tools that could not achieve this goal. We can reconstruct the movements of these individuals from witness testimonies and the observations of NTSB investigators:

> "The foreman said that he then went to his pickup truck and, using his cellular phone,2 called the gas company and the housing authority, telling them that he was excavating near the gas line and smelled gas. He stated that he next made three attempts to phone 911. He said that each time he called, there was no answer. He said he then moved his truck to another spot in the parking lot in case the phone signal to his cellular phone was being blocked. He said that at the new location he again tried unsuccessfully to call 911."

It was during these telephone calls that the foreman asked the backhoe operator and the loader to trace the gas line back to Utica Street. We do not know the exact time at which the foreman made this request but the NTSB investigators suggest that it was after the first telephone call that was logged by UGI at 18:48. The backhoe operator must, therefore, have been within earshot of the foreman in order to respond to his instruction to trace the line. The operator then left the parking lot at the request of the foreman. It may be assumed that he reached the cut-off valve at some time after the request was issued, although there is no independent verification for the exact timing. The following clauses reconstruct these observations. They exploit a simple form of temporal logic in which the binary *at* operator takes a proposition and a term denoting a time such that $at(p, t)$ is true if and only if p is true at t. The existential, $\exists$ quantifier (read as 'there exists') can be used to capture the uncertainty about the timing of the operators movements. The first clause states that the backhoe operator is at the Utica Street parking lot at 18:48. The second clause states that at some time, t, after 18:48, the backhoe operator is not at the gas valve for Gross Towers:

$$at(position(backhoe\_operator, utica\_parking\_lot), 1848). \tag{9.2}$$

$$\begin{aligned}\exists\, t : & \; at(position(backhoe\_operator, gross\_towers\_valve), t) \wedge \\ & \; after(1848, t). \end{aligned} \tag{9.3}$$

A number of technical problems surround the general application of this simple extension to propositional logic. In particular, the philosophical issue of reification forces analysts to clearly state the relationship between particular terms and objects over time. This theoretical problem is less of an issue for our purposes because we are always referring to definite entities at specific times during an accident. We, therefore, retain this simple temporal framework rather than the more elaborate temporal languages in our previous work [404, 427].

It might appear that such clauses add little to the information that is provided in the prose accounts of eye witness testimonies. The process of constructing such representations does, however, encourage investigators to re-examine all of the evidence supporting such location and timing information. To illustrate the importance of this cross-checking, the final NTSB report into the Allentown explosion states that UGI logged the first phone call at 18:48, cited on page 3 [589]. The investigators' time-line in appendix C of the report, on page 81, records the initial connection to the UGI switch board at 18:46 and the telephone call itself taking place at 18:47. By 18:48, the foreman was logged as calling the home of the vice president of his company to report the incident. The fact that such inconsistencies can be propagated into a final report reflects the importance of developing accurate reconstructions.

There are further reasons for reconstructing location information. The subsequent investigation into the Allentown incident was heavily critical of the Foreman's decision to send his crew members to shut off the valve. The NTSB inspectors argued that he should have asked them to evacuate anyone inside Gross Towers. Prompt action to safeguard the people inside the building would have mitigated the consequences of any explosion that they were ill-equipped to prevent. Further insights can be derived from the process of formalising the positional information in the clauses shown above. For instance, this reconstruction says remarkably little about the precise time at which the crew member left the Foreman. This is significant because it leaves open the possibility that the request was made shortly after 18:48. In which case, the Foreman would potentially have been left without sufficient staff to respond to an evacuation request:

> "Although it was after normal business hours, the foreman first called the UGI's Lehigh Division business office (the EPAI had not obtained and provided the foreman with the UGIs 24-hour emergency telephone number). Even after contacting the UGI, he did not say, and the UGI did not question, whether the odour of gas had been detected within the building. Had the UGI known that gas was already in the building, it probably would have told him to evacuate the occupants, which he could have done with the help of his crew and the bystanders. The UGI probably also would have notified the fire department, thus giving it more time to respond." [589]

UGI never issued the instructions to evacuate the building were never issued. Hence, the precise timings in clauses (9.2) and (9.3) are not significant for the reconstruction of the events leading to this particular incident. They are, however, significant for the wider recommendations about site evacuation procedures that may be drawn from this incident. Clearly those procedures should advise against allocating personnel before contacting the relevant supply company or the emergency services.

The previous clauses do not specify the relative position of the shut-off valve outside Gross Towers or of the Foreman's truck inside the Utica Street parking lot. Such information can be introduced by formalising a three-dimensional co-ordinate scheme [406]. This was not done because clauses (9.2) and (9.3) reflect the level of detail recorded after the incident investigation. However, such details can be represented in a logic-based notation, for example to support the analysis of tyre marks in road traffic incidents. These techniques can be directly derived from formal notations that underpin many CAD-CAM systems. This example illustrates a more general benefit of using a formal language. Logic provides an explicit representation of the level of abstraction that is considered appropriate for each stage of the reconstruction process. Investigators do not need to record the relative positions of the parking lot and the shut-off valve in order to model or represent the events leading to the explosion. Such decisions are extremely important. Too much detail and important properties of a reconstruction can become obscured by a mass of contextual information. Too little detail and it will be difficult to reconstruct the specific events that contribute to an incident. Clauses, such as (9.2) and (9.3), can be left at this high level of abstract or can be refined using the detailed coordinate systems introduced in [406]. This helps to avoid the ad hoc decisions that frequently seem to be made about the amount of location information that is included in incident reconstructions [426].

Operators and Communications

Communications problems exacerbate many major incidents. They also contribute to the emergency response and to any mitigating actions that may be performed. It is, therefore, important such utterances are explicitly represented within any reconstruction. For example, the investigation into the Allentown incident identified the following communications between the Foreman and the gas pipeline operator:

> "According to the UGIs records, the foreman's call was answered at 6:48 p.m. by UGI's Central Gas Control at Reading, Pennsylvania. According to the UGIs records, the foreman said that there was a gas leak at 1337 (Allen Street) Gross Towers in Allentown and that the gas line had been hit during digging. (The foreman acknowledged telling the UGI that he was digging near the gas line and had detected the odour of gas, but said that he did not tell the UGI that he had 'hit' the gas line.) At 6:52, the UGI received a second call, which was apparently from the foreman. The call was recorded as 'Cust [customer] just called back, said they definitely hit gas line and broke it.' The UGI's procedures did not require Gas Control to notify the Allentown fire department or any other emergency-response agency of either report about the release of gas because the caller did not indicate there was an imminent threat; consequently the fire department was not called." [589]

The following clauses reconstruct aspects of this quotation.

$$at(message(foreman, ugi, gas\_leak), 1848). \tag{9.4}$$

$$at(message(foreman, ugi, gas\_line\_hit), 1852). \tag{9.5}$$

An important benefit of temporal logic notations is that analysts can go beyond the previous clauses to specify persistent properties of incident reconstructions. For example, the $\forall$ (read as 'for all') quantifier can be used to specify that at no time did UGI pass on the foreman's messages to the Fire Department. $\neg$ stands for negation. The first of the following clauses can, therefore, be read as stating that at all times during the incident, UGI did not tell the Fire Department that there was a gas leak at Gross Towers. The seconds clauses states that at all times during the incident, UGI did not tell the Fire Department that the foreman had hit a gas line:

$$\forall\, t : \neg\; at(message(ugi, fire\_dept, gas\_leak), t). \tag{9.6}$$

$$\forall\, t : \neg\; at(message(ugi, fire\_dept, gas\_line\_hit), t). \tag{9.7}$$

Similar techniques can be used to reconstruct events for which the precise time is not known. For example, we do not know the exact time when the Foreman told the operator of the Backhoe and the loader to trace the gas line back to the shut off valve. The first of the following clauses states that there exists some time, t, when the foreman told the backhoe operator to trace back the gas line to the shut-off valve. The second clauses states that there exists some time, t, when the foreman told the loader to trace back the gas line to the shut-off valve:

$$\exists\, t : at(message(foreman, backhoe\_operator, trace\_to\_valve), t). \tag{9.8}$$

$$\exists\, t : at(message(foreman, loader, trace\_to\_valve), t). \tag{9.9}$$

Additional clauses can be introduced to narrow down the time when such an order could have been given. For instance, the investigators' statements record that it was issued *while* the foreman was making the phonecalls. The initial call to UGI was made at 18:48. Additional evidence must be found to identify the timing of foreman's final call by which time the order must have been given:

> "According to the housing authoritys records, the foreman called the housing authority at 6:55 and was connected to the after-hours answering service. The answering services records show that the foreman advised that 'they [the EPAI] were digging and they think they got the gas line.' At 7:06, according to the answering service, the foreman's message was relayed to one of the housing authority's maintenance employees, who promptly went to Gross Towers. The records of both the UGI and the housing authority of the foremans calls do not show that he said anything about detecting a strong odour of gas within the building." [589]

The following clause, therefore, states that the order to trace the gas line to the shut-off valve was made between the start of the first UGI call at 18:48 and the end of the call to the Housing Association at 19:06:

$$\begin{aligned}\exists\, t : &\ at(message(foreman, backhoe\_operator, trace\_to\_valve), t) \land \\ &\ after(1848, t) \land after(t, 1906).\end{aligned} \tag{9.10}$$

It is possible to impose stricter timing constraints than those shown in the previous clause because we know that the first explosion occurred at 18:58. It seems likely that the foreman directed his men to isolate the supply before the explosion. However, this is not explicitly indicated in the NTSB reconstruction which simply notes that the request was made at "6:??pm". These same logic-based techniques can be used to reconstruct more complex verbal exchanges, such as the transfer of messages between the Foreman, the Housing Authority answering service and the maintenance employee:

$$\begin{aligned}\exists\, t : &\ at(message(foreman, answer\_service, gas\_leak, 1855) \land \\ &\ at(message(answer\_service, house\_engineer, gas\_leak), t) \land \\ &\ after(1855, t)\end{aligned} \tag{9.11}$$

It is important to note that the preceding clauses do not represent the precise verbal components of each utterance. This information could be introduced if it were available, for instance through studying cockpit voice recordings in the aviation and shipping domains. In the case of the Allentown incident there was no such record. We only have the second-hand account of the answering service that the foreman had said "they [the EPAI] were digging and they think they got the gas line". After the incident, the Foreman denied saying that the backhoe had actually hit the line. However, the housing authority and UGI employees believed that this had been stated in his calls to them. Place holders, such as *gas_leak*, are used to capture the recollected sense of the communication without specifying its exact form.

Reasoning About Incidents

The previous section focussed on the flow of communication between the individuals and groups who were involved in an incident. This enables analysts to trace the way in which operators helped to exacerbate or mitigate the consequences of an incident. The same techniques can also be used to represent and reason more narrowly about the failure of particular system components. For instance, the emergency lighting failed during the Allentown incident:

> "Gross Towers, like all other housing complexes operated by the housing authority , had an internal fire alarm system that had alarm bells on each floor. When the system was activated, the company that monitored it promptly called the Allentown Communications Center. Gross Towers had a gas-powered emergency generator that started automatically whenever the flow of electricity to the building was interrupted. As long as the buildings gas supply was uninterrupted, the generator provided emergency lighting in the stair wells and exit lights. During this emergency, however, the generator did not operate because th e gas supply had been interrupted when the service line separated." [589]

This illustrates the point made in Chapter 2.3 that many incidents involve complex dependent system failures. The explosion that damaged the electrical power supply was caused by a gas leak that, in turn, prevented the emergency generators from working:

$$\neg\ \mathit{at}(\mathit{electricity\_supply}(\mathit{gross\_towers}), 1858). \tag{9.12}$$

$$\neg\ \mathit{at}(\mathit{gas\_supply}(\mathit{gross\_towers}), 1858). \tag{9.13}$$

$$\begin{aligned} \forall\, t :\ & \neg\ \mathit{at}(\mathit{electricity\_supply}(\mathit{gross\_towers}), t) \wedge \\ & \mathit{at}(\mathit{gas\_supply}(\mathit{gross\_towers}), t) \Rightarrow \\ & \mathit{at}(\mathit{emergency\_lighting}(\mathit{gross\_towers}, t). \end{aligned} \tag{9.14}$$

$$\begin{aligned} \forall\, t :\ & \neg\ \mathit{at}(\mathit{gas\_supply}(\mathit{gross\_towers}), t) \wedge \\ & \neg\ \mathit{at}(\mathit{electricity\_supply}(\mathit{gross\_towers}), t)) \Rightarrow \\ & \neg\ \mathit{at}(\mathit{emergency\_lighting}(\mathit{gross\_towers}), t) \end{aligned} \tag{9.15}$$

Previous paragraphs have used temporal logic to formalise the events leading to an accident. This formalisation process helps to strip out the contextual detail that hides critical observations in the many hundreds of pages that form conventional reports. We have not, however, shown that this approach can be used to reason about the events that lead to an incident. Rules of inference can be used to direct reasoning about an incident reconstruction. These rules are intended to increase the precision and rigour that is used when investigators draw particular conclusions from the events that they model. The general idea behind logical proof can be illustrated by the simple example that was presented in the previous paragraph. This provided a number of implications. For example, it was stated that the emergency lighting comes on if the electricity supply has failed but the gas supply is still working. It was also stated that if the gas system has failed then the emergency lighting would fail as well. We can use these assertions to make several inference if we have a proof rule of the following form. This states that if we know that some formula p is true at all times t and we know that if p is true at t then q is true at t then given we already know p is true then we can safety conclude that q is true at t as well:

$$\forall\, t, p(t), p(t) \Rightarrow q(t) \vdash q(t) \tag{9.16}$$

Given this rule we can begin to construct a formal proof to show that the emergency lighting failed in our reconstruction as a logical consequence of the gas leak. The proof begins by instantiating the particular moment of failure into the clauses introduced in the previous section:

$$\begin{aligned} & \neg\ \mathit{at}(\mathit{gas\_supply}(\mathit{gross\_towers}), 1858) \wedge \\ & \quad \neg\ \mathit{at}(\mathit{electricity\_supply}(\mathit{gross\_towers}), 1858) \Rightarrow \\ & \quad \neg\ \mathit{at}(\mathit{emergency\_lighting}(\mathit{gross\_towers}, 1858) \\ & \qquad \mathit{Instantiate\ t\ in}\ (9.15)\ \mathit{with}\ 1858 \end{aligned} \tag{9.17}$$

Given the previous proof rule and the fact that we know from clause (9.13) that the gas and electricity did fail at 18:58, it can now be concluded that the emergency lighting did not come on at that time.

$$\begin{aligned} & \neg\ \mathit{at}(\mathit{emergency\_lighting}(\mathit{gross\_towers}, 1859) \\ & \qquad \mathit{Application\ of}\ (9.16)\ \mathit{to}\ (9.17)\ \mathit{given}\ (9.13)\ \mathit{and}\ (9.12). \end{aligned} \tag{9.18}$$

We might like to argue that there was some time after the explosion when there was still a sufficient supply within the emergency generators to drive the emergency lighting. The same procedures cannot, however, be used to prove this. Recall that clause (9.14) specified that the emergency lights came on if the electricity failed and the gas system was functioning. We know from (9.12) that the electricity failed at 18:58. However, we cannot prove from our reconstruction that the gas system was functioning at 18:58. Hence we cannot apply rule (9.16). If an investigator wished to establish that the generators were able to function for some initial time then additional evidence would have to be found. This might then support the following inference:

$$\begin{array}{l} \mathit{at}(\mathit{gas\_supply}(\mathit{gross\_towers}), 1858)). \\ \mathit{Assumption} \end{array} \tag{9.19}$$

$$\begin{array}{l} \neg\ \mathit{at}(\mathit{electricity\_supply}(\mathit{gross\_towers}), 1858) \wedge \\ \mathit{at}(\mathit{gas\_supply}(\mathit{gross\_towers}), 1858) \Rightarrow \\ \quad \mathit{at}(\mathit{emergency\_lighting}(\mathit{gross\_towers}, 1858) \\ \qquad \mathit{Instantiate}\ t\ \mathit{in}\ (9.14)\ \mathit{with}\ 1858 \end{array} \tag{9.20}$$

$$\begin{array}{l} \mathit{at}(\mathit{emergency\_lighting}(\mathit{gross\_towers}, 1858) \\ \qquad \mathit{Application\ of}\ (9.16)\ \mathit{to}\ (9.20)\ \mathit{given}\ (9.12)\ \mathit{and}\ (9.19) \end{array} \tag{9.21}$$

The Allentown investigators argued that:

> “Once the line and coupling separated, the EPAI could have limited the consequences. When the EPAI foreman was told about the strong odour of gas within the building, he should have immediately called 911. Contrary to his post-accident statement, telephone records show that he did not attempt to call 911 until after the explosion. Had he immediately reported the emergency to the fire department, it would have known almost 15 minutes before the explosion, giving it enough time to respond, notify the UGI, initiate evacuations and building ventilation, and, using the UGI responders, shut off the flow of gas into the building, which would have either prevented the explosion or reduced its force. The Safety Board concludes that the consequences of this accident could have been significantly reduced had the foreman promptly called 911 and had his helper promptly told the occupants of the building to evacuate.” [589]

It is possible to use this statement together with the timing information that was provided in an NTSB inspector’s time-line to reconstruct a number of important observations about the Allentown incident. The smell of gas was first reported by an EPAI employee to the foreman at 18:45. A statement from a passing policeman recorded the time of the explosion at 18:58. Between these two times, the foreman managed to call both UGI and the Housing Association but did not succeed in reaching the emergency services on 911.

$$\begin{array}{l} \exists\, t, t', \forall\, t'' : \\ \quad \mathit{at}(\mathit{message}(\mathit{foreman}, \mathit{ugi}, \mathit{gas\_leak}), t) \wedge \\ \quad \mathit{at}(\mathit{message}(\mathit{foreman}, \mathit{housing\_authority}, \mathit{gas\_leak}), t') \wedge \\ \quad \neg\ \mathit{message}(\mathit{foreman}, \mathit{fire\_dept}, \mathit{gas\_leak}), t'') \wedge \\ \quad \mathit{before}(1845, t) \wedge \mathit{before}(1845, t') \wedge \mathit{before}(1845, t'') \wedge \\ \quad \mathit{before}(t, 1858) \wedge \mathit{before}(t', 1858) \wedge \mathit{before}(t'', 1858) \end{array} \tag{9.22}$$

The term ‘task’ is typically used in the human-computer interaction literature to describe a collection of activities that are intended to achieve particular goals. Chapter 2.3 has argued that many incidents occur because individuals fail to perform particular tasks or because they select tasks whose goals are inappropriate for the context in which they are performed. It is, therefore, important that reconstructions trace the manner in which different tasks are allocated or imposed by the flow of information during an incident. Had the foreman completed a 911 call to the emergency services then the Fire Department would have been informed of the need to evacuate the building. Logic can be used to model the way in which such communications notify other people of the tasks they must perform. This could, equally, be done by using a conventional task analysis technique from the human factors literature, such as task analysis for knowledge description (TAKD) [428]. Later sections will, however, argue that formal reasoning techniques provide additional means of proving properties of incident reconstructions.

The previous quotation also stressed that had the Fire Department been notified by the Foreman then they, in turn, would have contacted UGI. Their responders would then have had time to 'shut off the flow of gas into the building, which would have either prevented the explosion or reduced its force'. This assertion can be modelled as follows. It should be noted that unlike the previous clause we do not bind the timing for t and t' to particular intervals. It is assumed that UGI shut off the supply whenever they are notified of a gas leak by the Fire Department. The *perform* predicate is used to represent an individual or group's attempt to achieve a particular task at a particular time:

$$\begin{aligned}\forall\, t : & \; at(message(fire\_dept, ugi, gas\_leak), t) \Rightarrow \\ & \exists\, t' : perform(ugi, shut\_off\_gas), t') \wedge after(t, t'). \end{aligned} \tag{9.23}$$

Incidents often act as a catalyst that provokes investigators to hypothesise about the introduction of particular pieces of equipment. Such alternative scenarios introduce a certain amount of additional complexity into the reconstruction process. Analysts and investigators must keep track of which clauses are being used to model any particular scenario. In particular, a contradiction would occur if clauses were introduced to simultaneously denote that gas detection equipment did and did not generate a warning. Brevity prevents a more detailed introduction to this issue, however, Burns' recent thesis identifies many of the technical problems that can arise from this aspect of formal reconstruction [118]. With these caveats in mind, it is possible to formalise alternative scenarios such as those suggested by the NTSB investigators in the previous quotation. It is important to repeat that these formalisations model or reconstruct certain aspects of an adverse occurrence. They do not capture every aspect of the prose descriptions produced by investigators, just as those prose descriptions to not capture every event that occurred during the incident itself. For example, the previous clauses do not capture the idea that had UGI and the Fire Department intervened, in the manner described above, then the explosion would either have been avoided or its energy reduced. Such notions can be formalised as properties of possible future states of the system using modal logics [118]. Such notations have the same foundations as the causal logics exploited by Ladkin's accident analysis techniques [469]. These notations provide elegant means of distinguishing between, for example, degrees of risk or notions of cause from notions of time. However, these approaches greatly increase the degree of mathematical sophistication that is necessary to reconstruct an incident. McDermid summarises many of the issues that are raised by the use of these techniques when he argues that increased expressiveness is often sacrificed at the cost of tractability and complexity [528].

The entities that were identified in Table 9.1.4 are generic in the sense that operators, tasks, utterances, physical locations etc. are central to a wide range of incidents reports [410, 426, 427]. This does not mean that the list is exhaustive. Some incidents require new types of entities to be introduced in order to model important aspects of an adverse occurrence. The significance of individual entities will also vary from incident to incident. For example, automated systems played a relatively minor role in the Allentown incident:

> "...the consequences of the accident might have been significantly reduced had the room in which the service line entered the building had a gas detector capable of alerting the occupants and the fire department. Had there been a gas detector in the room in which the service line entered, the occupants of the building and the fire department would have had 15 extra minutes in which to react. The fire department would have had time to communicate with the UGI, which might have been able to close the gas line valve soon after the separation occurred, thus preventing the accident. More likely, the accident would have happened, but much less gas would have been available to fuel the explosion, which might have substantially reduced the number of casualties and extent of the damage... contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building."[589]

Such findings create a number of problems for organisations that must prevent the recurrence of future accidents. It does not explain the impact that such devices might have had upon the course of the Allentown explosion. This ambiguity has serious consequences. Different readers might form very different conclusions about whether or not such systems would have had a significant impact upon the course of the incident [845, 700]. Formal proof techniques can be used to reason about the impact that such findings might have for any reconstruction. For instance, a gas detector warning might have prompted the evacuation of the building. The following clause does not specify that a gas leak must actually have occurred in order for an evacuation to be initiated:

$$\begin{aligned}&\forall\, t : at(message(gas\_detector, residents, gas\_leak), t) \Rightarrow \\ &\qquad at(perform(residents, initiate\_evacuation), t)\end{aligned} \tag{9.24}$$

Formal reasoning techniques can be used to determine whether such assertions are supported by the evidence from a reconstruction. We can use the laws of our logic system to determine whether or not such a warning would actually have prompted the residents to leave the building. One way of doing this is to look for a situation that contradicts the previous assertion. This involves looking through the clauses of our model or reconstruction to find evidence of a situation in which the residents failed to evacuate their building in spite of a warning about the presence of gas. Ideally, the detection equipment should have identified the presence of gas almost immediately after the line had separated from the coupling at 18:45:

$$\begin{aligned}&at(message(gas\_detector, residents, gas\_leak), 1845) \Rightarrow \\ &\quad at(perform(residents, initiate\_evacuation), 1845). \\ &\quad \mathit{Instantiate}\ 1845\ \mathit{for}\ t\ \mathit{in}\ (9.24)\end{aligned} \tag{9.25}$$

$$\begin{aligned}&\neg\ at(message(gas\_detector, residents, gas\_leak), 1845) \vee \\ &at(perform(residents, initiate\_evacuation), 1845) \\ &\mathit{Implication\ Law\ applied\ to}\ (9.25)\end{aligned} \tag{9.26}$$

Looking at the first part of this disjunction, we know that the residents did not initiate any evacuation.

$$\forall\, t : \neg\ \ at(perform(residents, initiate\_evacuation), t) \tag{9.27}$$

A passing police officer started clearing the building after he had heard the sound of the first explosion after 1858. We, therefore, have a contradiction with part of the previous clause:

$$\begin{aligned}&at(perform(residents, initiate\_evacuation), 1845) \\ &\mathit{Assumption\ from}\ (9.26)\end{aligned} \tag{9.28}$$

$$\begin{aligned}&\neg\ at(perform(residents, initiate\_evacuation), 1845) \\ &\mathit{Instantiate}\ 1845\ \mathit{for}\ t\ \mathit{in}\ (9.27)\end{aligned} \tag{9.29}$$

$$\begin{aligned}&\neg\ at(perform(residents, initiate\_evacuation), 1845) \wedge \\ &at(perform(residents, initiate\_evacuation), 1845) \\ &\wedge\ \mathit{Introduction\ for}\ (9.28)\ \mathit{and}\ (9.29)\end{aligned} \tag{9.30}$$

As mentioned, formal reasoning is being used to reconstruct a situation that contradicts previous assertions about the potential role of gas detection equipment. The residents did not initiate an evacuation at 18:45. In order to derive the necessary contradiction we must also show that they were alerted to the presence of gas at this time. We know from the NTSB report that several of the residents had smelt gas by 18:45, almost immediately after the line had separated from the coupling. No evacuation was started. They only called 911 after the first explosion had occurred:

> "Post-accident surveys of 115 residents show that three Towers East occupants, in units 108, 408, and 902, had smelled gas immediately before the explosion and that two other occupants had smelled gas shortly before the explosion while they were in the mail room on the first floor. The occupant of unit 108 stated that he had reported the gas odour to '911,' but after the explosion." [589]

An EPAI employee is recorded on page 81 of the report as stating that a woman on the third floor shouted that she smelled a "heavy odour of gas' at 18:45. It is not possible to resolve this reference against the room numbers mentioned in the previous citation. We do, however, know that this person did try to alert the other residents:

$$at(message(third\_floor\_resident, residents, gas\_leak), 1845). \tag{9.31}$$

This element of the reconstruction does not support the contradiction that was initially intended. We cannot show a situation in which the residents failed to respond to a detection *system.* However, the formal modelling does emphasise that residents were not alerted by their neighbours' warnings and that even those who smelled gas did not take immediate action to evacuate the building:

$$\begin{array}{l} \neg\ at(message(gas\_detector, residents, gas\_leak), 1845). \\ \textit{Assumption from } (9.26) \end{array} \tag{9.32}$$

$$\begin{array}{l} at(message(third\_floor\_resident, residents, gas\_leak), 1845) \wedge \\ \neg\ at(message(gas\_detector, residents, gas\_leak), 1845). \\ \wedge\ \textit{Introduction for } (9.31) \textit{ and } (9.32) \end{array} \tag{9.33}$$

The previous clause illustrates the important point that formal modelling does not provide a panacea for the problems of incident reconstruction. The same insights can also be derived by careful inspection of the evidence that is gathered during a secondary investigation. However, such formal analysis introduces a discipline and rigour that can help investigators to reassess the assumptions that might otherwise be made about the course of an incident. For instance, as the previous clauses have shown, there is no guarantee that residents will respond to either automated or human warnings. It is for this reason that most institutions, including the Gross Towers retirement home, practice fire drills. It is pertinent to ask why these procedures are cued by the detection of fire rather than the presence of gas:

> "The executive director stated that the housing authority had procedures for evacuating the occupants and that the residents practiced the routines. For example, every 6 months the fire department conducted fire inspections and drills that also tested the evacuation procedures and emphasized how important it was for the residents to respond promptly. The drills included special precautions for the elderly and handicapped; and after a drill was held, all residents participated in a critique." [589]

The previous paragraphs used formal reasoning to drive an analysis of the NTSB's assertion that the lack of a gas detection system exacerbated the consequences of the incident by failing to alert the residents to the potential danger. This mirrors the observation that the fire brigade could have used the additional warning to notify the gas supply company:

$$\begin{array}{l} at(message(gas\_detector, fire\_dept, gas\_leak), 1845) \Rightarrow \\ \quad \exists\, t, t', t'' : at(perform(fire\_dept, initiate\_evacuation), t) \wedge \\ \quad at(perform(fire\_dept, ventilate\_building), t') \wedge \\ \quad at(message(fire\_dept, ugi, gas\_leak)), t'') \wedge \\ \quad after(1845, t) \wedge after(1845, t') \wedge after(1845, t'') \wedge \\ \quad after(t, 1858) \wedge after(t', 1858) \wedge after(t'', 1858). \end{array} \tag{9.34}$$

A warning from the gas detector results in a message being sent to UGI, at t'', between the moment when the gas is detected and when the moment when the explosion actually occurred. If we assume that a gas detection system had been installed:

$$\begin{array}{l} at(message(gas\_detector, fire\_dept, gas\_leak), 1845). \\ \textit{Assumption.} \end{array} \tag{9.35}$$

$$\begin{array}{l} \exists\, t, t', t'' : at(perform(fire\_dept, initiate\_evacuation), t) \wedge \\ \quad at(perform(fire\_dept, ventilate\_building), t') \wedge \\ \quad at(message(fire\_dept, ugi, gas\_leak)), t'') \wedge \\ \quad after(1845, t) \wedge after(1845, t') \wedge after(1845, t'') \wedge \\ \quad after(t, 1858) \wedge after(t', 1858) \wedge after(t'', 1858). \\ \quad \textit{Application of Modus Ponens to } (9.34) \textit{ given } (9.35) \end{array} \tag{9.36}$$

$$\begin{array}{l} \exists\, t'' : at(message(fire\_dept, ugi, gas\_leak)), t'') \wedge \\ \quad after(1845, t'') \wedge after(t'', 1858). \\ \quad \textit{Elimination of } \wedge \textit{ from } (9.36) \end{array} \tag{9.37}$$

As before, this formalisation suggests directions for further analysis. In particular, the previous clause would be satisfied if the fire service issued a warning at any time between 18:45 and 18:58. Clearly, information at the start of this interval might have had a greater impact upon the outcome that a warning that arrived only seconds before the explosion at 18:58. The gas supply company would have had a greater opportunity to cut off the supply before it built up within Gross Towers. The following clause assumes that the message was passed to UGI at 18:46; immediately after it was received by the fire service:

$$\begin{array}{l} \forall\, t : at(message(fire\_dept, ugi, gas\_leak), t) \Rightarrow \\ \quad \exists\, t' : perform(ugi, shut\_off\_gas), t') \wedge after(t, t'). \qquad (9.23) \end{array}$$

$$\begin{array}{l} at(message(fire\_dept, ugi, gas\_leak), 1846) \wedge \\ after(1845, 1846) \wedge after(1846, 1858). \\ \textit{Instantiation of } t'' \textit{ for } 1846 \textit{ in } (9.37). \end{array} \tag{9.38}$$

$$\begin{array}{l} at(message(fire\_dept, ugi, gas\_leak), 1846). \\ \textit{Elimination of } \wedge \textit{ in } (9.38). \end{array} \tag{9.39}$$

$$\begin{array}{l} \exists\, t' : perform(ugi, shut\_off\_gas), t') \wedge after(1846, t'). \\ \textit{Application of } (9.16) \textit{ to } (9.23) \textit{ given } (9.39) \end{array} \tag{9.40}$$

One means of assessing the potential benefit of such an early warning is to compare the possible impact of a warning system with what actually happened during this incident. This follows what was done by the previous proof in which we compared the impact of an automated alarm with the warning that was issued by individual residents in Gross Towers. In this case, however, we know form page 3 of the NTSB report that UGI was informed of the gas leak in a telephone call by the EPAI foreman at 18:48. We also know from page 5 of the NTSB report that the UGI operators eventually cut off the gas supply to the building at 19:15. In other words, it took approximately twenty-seven minutes for UGI employees to reach the scene of the gas leak, to trace the damaged pipe back to the Utica Street supply and then to isolate the line to Gross Towers. we can use this information to instantiate t' in (9.40) by adding the twenty-seven minute delay to the best case estimate for the fire brigade passing the gas detector's warning to UGI:

$$\begin{aligned}&\mathit{perform}(\mathit{ugi}, \mathit{shut\_off\_gas}), 1913) \wedge \mathit{after}(1846, 1913).\\&\mathit{Instantiation\ of}\ 1913\ \mathit{for}\ t'\ \mathit{in}\ (9.40).\end{aligned} \tag{9.41}$$

The implications of this analysis are clear. The additional time gained by an automated gas detection system would only have bought an additional two minutes during this incident. This confirms the argument put forward by the NTSB's investigators. The warning would not have provided sufficient time in order to avoid the explosion. However, it does not necessarily confirm their analysis that the additional time might have enabled respondents to mitigate the consequences of the incident. The validity of such an assertion cannot be directly assessed from the reconstruction that has been presented in this chapter. Nor can it be directly assessed from any of the evidence in the final report into this incident.

Unfortunately, mathematical analysis provides non-formalists with an extremely poor idea of the argumentation processes that support particular conclusions. It is difficult for people without some mathematical background to understand the various proof rules that are applied during our formal analysis. The consequences of this should not be underestimated. The use of a mathematical notation does not guarantee that any analysis will be free from error. Formal proof rules are simply intended to explicitly represent the mechanisms that support particular inferences. They expose the reasoning that is implicit within an informal analysis of an incident or accident. The intention is that other investigators can use those proof rules to challenge the basis for particular arguments about an adverse occurrence. However, if those proof rules cannot easily be understood by other investigators then there is little likelihood that they will be able to challenge the inferences and arguments of their peers. Automated reasoning tools provide means of increasing confidence in such proofs even when they may not be accessible to all parties in an investigation. Some initial work has applied these theorem provers and model checkers to support incident investigation [421, 415]. More work remains to be done. The insights provided by these systems must still be communicated to many different domain experts. The following pages, therefore, present techniques that have been developed to address the communications problems that affect the formal analysis of incident reports.

Conclusion, Analysis and Evidence (CAE) Diagrams

Conclusion, Analysis and Evidence (CAE) diagrams provide a high level overview of the argument that investigators construct to support the findings of an incident investigation. They build on the products of any reconstruction to support the causal reasoning that will be the focus of the next chapter. It is appropriate to briefly introduce this technique here because we have already stressed the close links between investigation, reconstruction and causal analysis. This decision is also justified by the way in which CAE diagrams illustrate the products of formal reasoning. They can be used to overcome some of the problems of communicating these reconstruction techniques to domain experts who may not have any background in mathematical logic.

Figure 9.24 presents an initial CAE diagram for the Allentown incident. The nodes of this graph are annotated with direct quotations from the NTSB investigators. As can be seen, CAE diagrams are formed around particular conclusions about the adverse occurrence. Here C1 denotes the argument made on page 48 of the NTSB incident report that the lack of a gas detector contributed to the severity of this incident. This represents a particular instance of the counterfactual arguments, mentioned in previous sections. The incident would have been less severe if a gas detector had been installed. The consequences of the failure were exacerbated because such a device had not been installed. The conclusion that forms the root of a CAE diagram is, in turn, supported by a number of lines of analysis. In this instance, A1.1 argues that a gas detector might have enabled the fire department to communicate with UGI in order to ensure a more prompt response. The line of analysis represented by A1.2 denotes the argument that a gas detector might have provided the residents with an extra fifteen minutes in which to react.

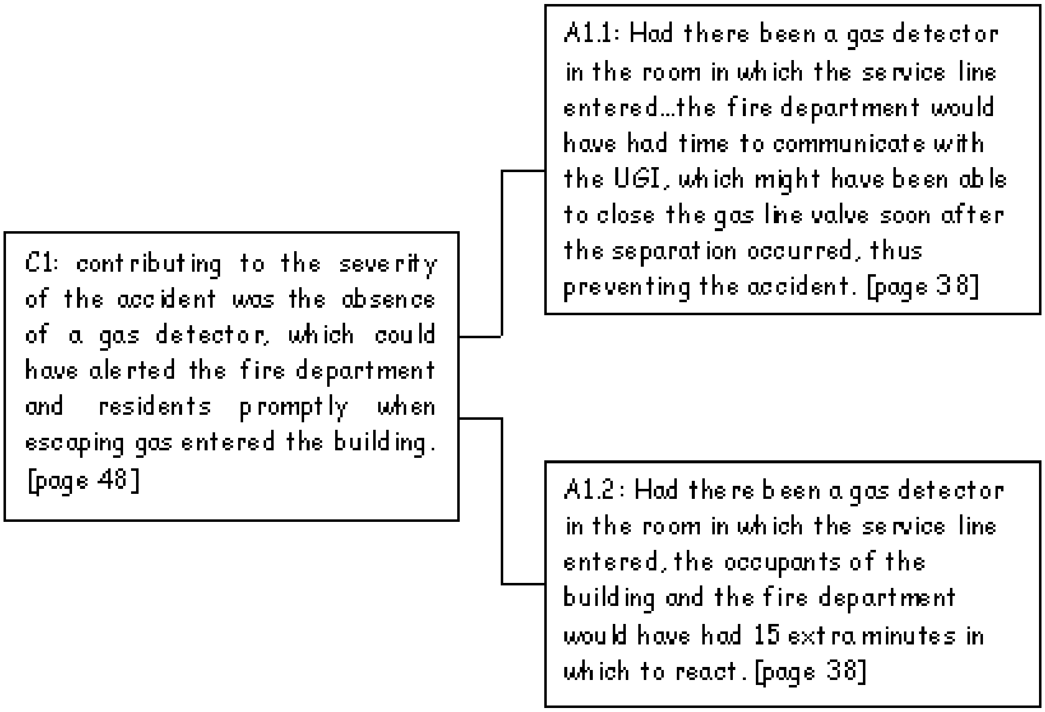

A1.1: Had there been a gas detector in the room in which the service line entered...the fire department would have had time to communicate with the UGI, which might have been able to close the gas line valve soon after the separation occurred, thus preventing the accident. [page 38]
C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]
A1.2: Had there been a gas detector in the room in which the service line entered, the occupants of the building and the fire department would have had 15 extra minutes in which to react. [page 38]

Figure 9.24: High-Level CAE Diagram for the Allentown Incident

CAE diagrams can be used to trace the arguments that both support and weaken particular conclusions. For instance, Figure 9.25 extends Figure 9.24 to show an objection to the NTSB conclusion. This is denoted by the dotted line between A1.1 and A1.1.1. Figure 9.25 counters the argument that a gas detector might have prevented the incident. The analysis in A1.1.1 argues that a gas detector would not have provided a warning soon enough for UGI to avert the explosion. This analysis is based on the assumption that it took 27 minutes to cut the supply from the time at which UGI were first notified at 18:48. Even if the gas detector had issued a warning immediately after the line was cut this could only have gained two minutes from the time at which the foreman made his first call. This line of argument is supported by two items of evidence. The node E1.1.1.1 shows that according to UGI records, the Foreman's initial call was answered at 18:48. The evidence denoted by E1.1.1.2 shows that the UGI employee only succeeded in shutting down the gas line by 19:15.

Figure 9.26 provides a further illustration of the way in which CAE diagrams sketch the arguments for an against particular conclusions. Rather than focusing on the response of the Fire Service and UGI to any automated warning, this CAE diagram illustrates a counter argument to the theory that a gas detector might have encouraged the residents to evacuate Gross Towers. This is based on the observation that some residents did know about the gas leak and yet still did not initiate an evacuation. As can be seen, two further items of evidence support this counter argument. E1.2.1.1 denotes that a resident did smell gas almost as soon as the pipeline failed. This is recorded at 18:45 on page 81 of the NTSB report. E1.2.1.2 shows that at least three other residents had first-hand knowledge of a potential gas leak but nobody rang '911' until after the first explosion. The evacuation was, in fact, initiated by a passing police officer.

Many investigators recruit extremely complex arguments both for and against particular conclusions. As can be seen, it is possible to identify a number of competing positions within the NTSB reports into the Allentown incident. CAE diagrams provide a high-level means of mapping out these positions to ensure that analysts demonstrate that their analysis is well-founded in the events that are represented within a reconstruction. This is important because there causal arguments or arguments about the mitigation of an incident can become 'detached' from the evidence that is

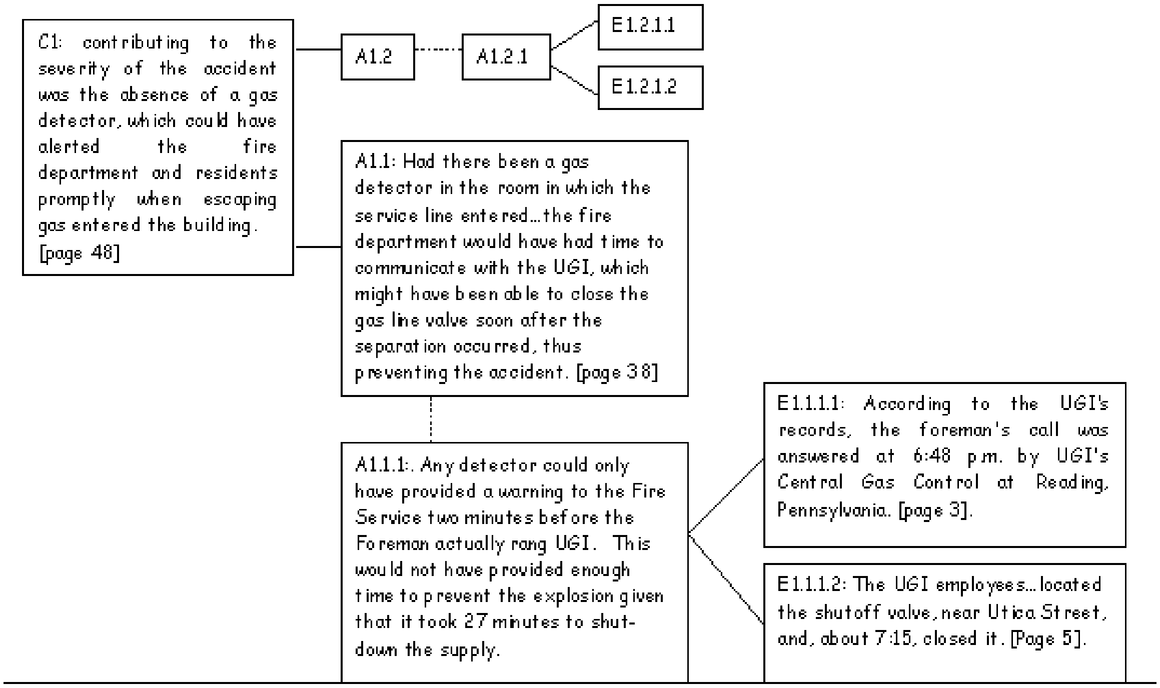

C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]
A1.2
A1.2.1
E1.2.1.1
E1.2.1.2
A1.1: Had there been a gas detector in the room in which the service line entered...the fire department would have had time to communicate with the UGI, which might have been able to close the gas line valve soon after the separation occurred, thus preventing the accident. [page 38]
A1.1.1:. Any detector could only have provided a warning to the Fire Service two minutes before the Foreman actually rang UGI. This would not have provided enough time to prevent the explosion given that it took 27 minutes to shut-down the supply.
E1.1.1.1: According to the UGI's records, the foreman's call was answered at 6:48 p.m. by UGI's Central Gas Control at Reading, Pennsylvania. [page 3].
E1.1.1.2: The UGI employees...located the shutoff valve, near Utica Street, and, about 7:15, closed it. [Page 5].

Figure 9.25: Representing Counter Arguments in a CAE Diagram (1)

gathered during a primary and secondary investigation. This need not, however, be malicious. It can simply stem from the logistical problems created by the increasing complexity of many technological failures. This is illustrated by the way in which Figure 9.26 cites evidence from page 3 to analyse arguments that were proposed on page 38 in support of a conclusion that is presented on page 48 of the NTSB report. Without such diagrammatic support, there is a danger that important evidence may be overlooked when analysing any reconstruction.

Figure 9.26 is not unusual in the complexity of the argument that it presents. For example, Figure 9.27 extends the previous analysis. It represents a line of argument that supports the assertion that a gas detector might have helped the gas supplier, UGI, to prevent the explosion. As can be seen, A.1.1.2 argues that UGI would have responded differently if a warning had been raised by the Fire Service rather than from the EPAI foreman. This line of argument is supported by two additional items of evidence. E.1.1.2.1 emphasizes the point that the foreman's calls to UGI did not emphasise the degree of threat posed by the initial gas leak. In E.1.1.2.2, UGI's records indicate that the foreman did not report the smell of gas within Gross Towers. Both items of evidence help to explain why UGI personnel might not have understood the implications of the foreman's report. The NTSB investigators argue that if the suppliers had been notified by the fire service, in response to an automated alarm, then the warning would have been less ambiguous. This would also have avoided the communications problems, noted in previous chapters, that often arise when individuals must report adverse events that they are themselves implicated in.

The previous diagrams have shown how CAE diagrams can be used to map out the arguments and counter arguments that are constructed using the evidence provided in reconstructions. This is important if analysts are to consider not simply the arguments that they favour but also the competing views that might be raised in the aftermath of an investigation. We have not, however, shown how this techniques might also be used to communicate the products of any formal reconstruction using logic or other mathematical notations. In contrast, Figure 9.28 presents a relatively simplistic means of achieving this aim. Textual annotations to the nodes in a CAE diagram are extended to include clauses derived from the formal reconstruction of an adverse occurrence. In this case, A1.1 shows that if the fire department had alerted UGI to the gas leak then they would have shut it off

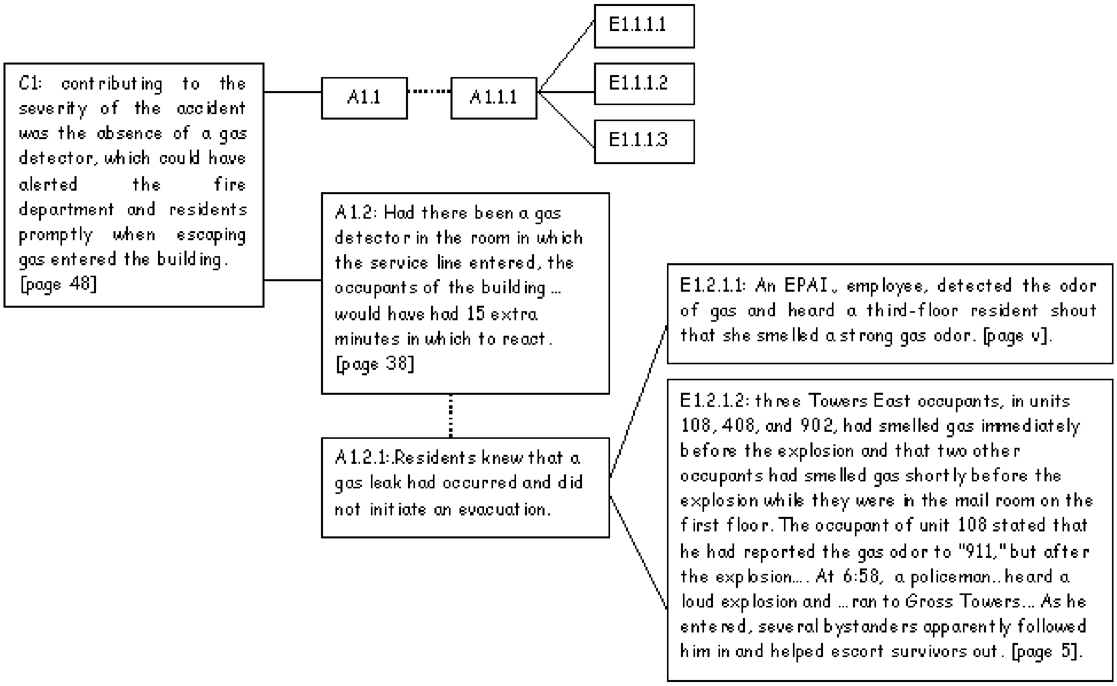

C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]
A1.1
A1.1.1
E1.1.1.1
E1.1.1.2
E1.1.1.3
A1.2: Had there been a gas detector in the room in which the service line entered, the occupants of the building ... would have had 15 extra minutes in which to react. [page 38]
A1.2.1:Residents knew that a gas leak had occurred and did not initiate an evacuation.
E1.2.1.1: An EPAI. employee, detected the odor of gas and heard a third-floor resident shout that she smelled a strong gas odor. [page v].
E1.2.1.2: three Towers East occupants, in units 108, 408, and 902, had smelled gas immediately before the explosion and that two other occupants had smelled gas shortly before the explosion while they were in the mail room on the first floor. The occupant of unit 108 stated that he had reported the gas odor to "911," but after the explosion.... At 6:58, a policeman..heard a loud explosion and ... ran to Gross Towers... As he entered, several bystanders apparently followed him in and helped escort survivors out. [page 5].

Figure 9.26: Representing Counter Arguments in a CAE Diagram (2)

before the explosion at 18:58. A1.2 states that the residents would have initiated an evacuation if a detection system had identified the gas leak when it first started at 18:45. These formalisations represent strong requirements. For instance, A1.1 states that UGI would shut off the gas before 18:58 irrespective of the time at which the Fire Service contacted them. This seems unreallistic and, as we have seen, additional clauses may be introduced to reflect the minimum time necessary between any notification and a successful intervention by UGI. CAE diagrams, such as Figure 9.28, can help to expose such unwarranted assumptions that might otherwise be embodied within a formal analysis.

Figure 9.29 presents part of the formal reasoning that was used to assess whether or not the assumptions, embodied in Figure 9.28, might be sustained. Elements of the mathematical model constructed in the previous section are linked to the natural language evidence that was identified by the NTSB investigators. This is then used to create a conjunction which shows that the foreman alerted UGI to the gas leak at 18:48 and that their representatives did not shut the supply until 19:15, after the explosion at 18:58. As we have seen, this is not a direct contradiction of the argument put forward by the investigation team. However, it does use the evidence about what actually happened in this incident to construct a counter-case against the hypothesis about the effectiveness of an automated gas detector.

The CAE in Figure 9.30 shows how elements of the formal analysis can be used to counter the argument that a gas detector might have encouraged the resident to initiate an evacuation. Elements of the reconstruction are again linked to the natural language evidence on page v and page 5 of the investigators' report. This evidence is then used to develop a counter case. We can establish that residents did know about the gas leak almost as soon as it occurred, they smelt gas at 18:45. However, they did not initiate an evacuation in spite of this direct physical evidence of the potential danger. Human factors research into the efficacy of alarms suggests that many automated warnings have little effect on such a response, especially given that the residents had already received evacuation training [638].

It is important to emphasise that we have only shown one means of using CAE diagrams to represent the insights that can be gained from the formal reconstruction of adverse occurrences. In the previous examples, we have constructed models of the incident and then used those models to

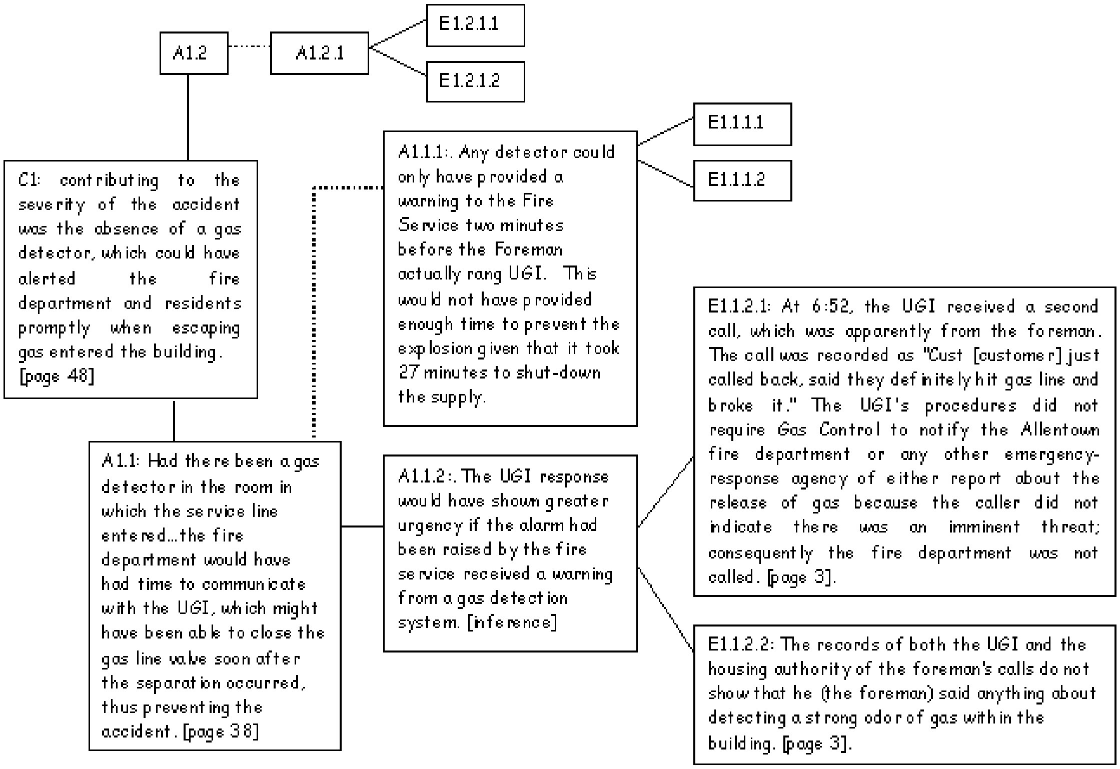

A1.2
A1.2.1
E1.2.1.1
E1.2.1.2
E1.1.1.1
E1.1.1.2
C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]
A1.1.1:. Any detector could only have provided a warning to the Fire Service two minutes before the Foreman actually rang UGI. This would not have provided enough time to prevent the explosion given that it took 27 minutes to shut-down the supply.
E1.1.2.1: At 6:52, the UGI received a second call, which was apparently from the foreman. The call was recorded as "Cust [customer] just called back, said they definitely hit gas line and broke it." The UGI's procedures did not require Gas Control to notify the Allentown fire department or any other emergency-response agency of either report about the release of gas because the caller did not indicate there was an imminent threat; consequently the fire department was not called. [page 3].
A1.1: Had there been a gas detector in the room in which the service line entered...the fire department would have had time to communicate with the UGI, which might have been able to close the gas line valve soon after the separation occurred, thus preventing the accident. [page 38]
A1.1.2:. The UGI response would have shown greater urgency if the alarm had been raised by the fire service received a warning from a gas detection system. [inference]
E1.1.2.2: The records of both the UGI and the housing authority of the foreman's calls do not show that he (the foreman) said anything about detecting a strong odor of gas within the building. [page 3].

Figure 9.27: Representing Counter Arguments in a CAE Diagram (3)

develop counter cases that raise questions about some of the investigators' findings. Elsewhere this technique has been used more directly to identify inconsistencies, errors and omissions in incident reports [415]. For instance, we have shown that investigators have placed the same individual in two different locations at the same time. The resulting CAE diagrams have much in common with other techniques for communication formal reasoning, such as tableaux or proof trees.

9.2 Requirements for Reconstructive Modelling

Previous sections have introduced a number of abstract notations that can be used to reconstruct the events that contribute to adverse occurrences. The intention has been to provide a broad overview of techniques that avoid some of the current limitations that affect the simulation environments introduced in Chapter 7.3. In particular, these more abstract notations can, typically, capture both catalytic failures but also the more latent and managerial failures that contribute to major incidents. There are, however, a number of problems that frustrate the application of these techniques to support the reconstruction of adverse occurrences. For instance, a considerable amount of training may be required before domain specialists and incident investigators can exploit the formal proof techniques that were introduced in the previous section. In contrast, temporal extensions to Fault Trees can initially be easier to understand. However, the lack of any formal semantic can lead to disagreement about the interpretation of these informal annotations. The following pages, therefore, address some of these limitations and derive requirements that investigators should consider when selecting an appropriate reconstruction technique.

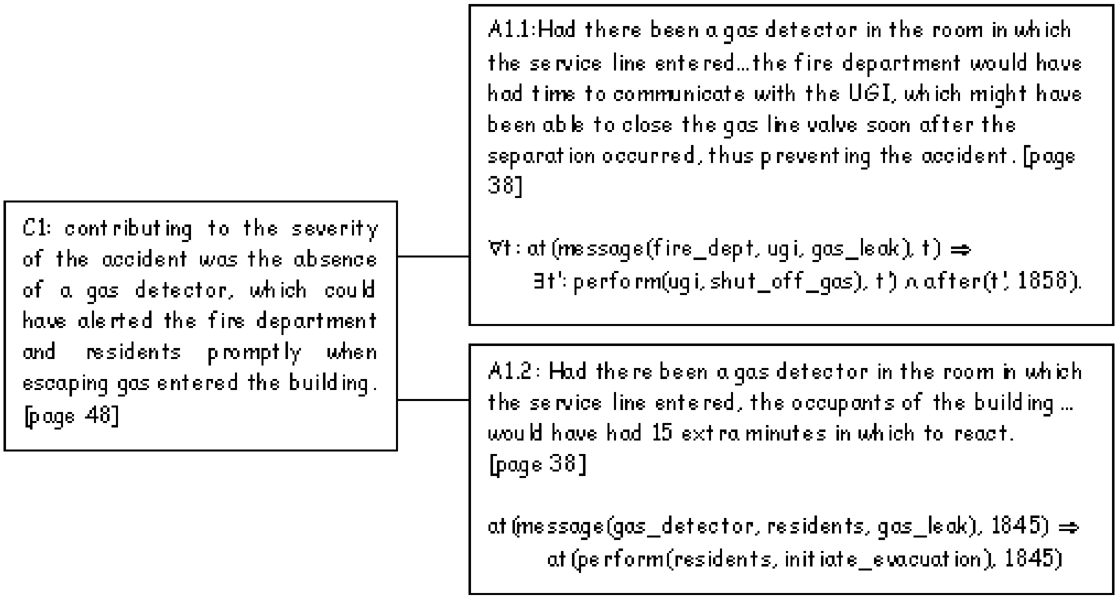

C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]
A1.1:Had there been a gas detector in the room in which the service line entered...the fire department would have had time to communicate with the UGI, which might have been able to close the gas line valve soon after the separation occurred, thus preventing the accident. [page 38]
∀t : at(message(fire_dept, ugi, gas_leak), t) ⇒
∃t': perform(ugi, shut_off_gas), t') ∧ after(t', 1858).
A1.2: Had there been a gas detector in the room in which the service line entered, the occupants of the building ... would have had 15 extra minutes in which to react. [page 38]
at(message(gas_detector, residents, gas_leak), 1845) ⇒
at(perform(residents, initiate_evacuation), 1845)

Figure 9.28: High-Level CAE Diagram Integrating Formal and Informal Material

9.2.1 Usability

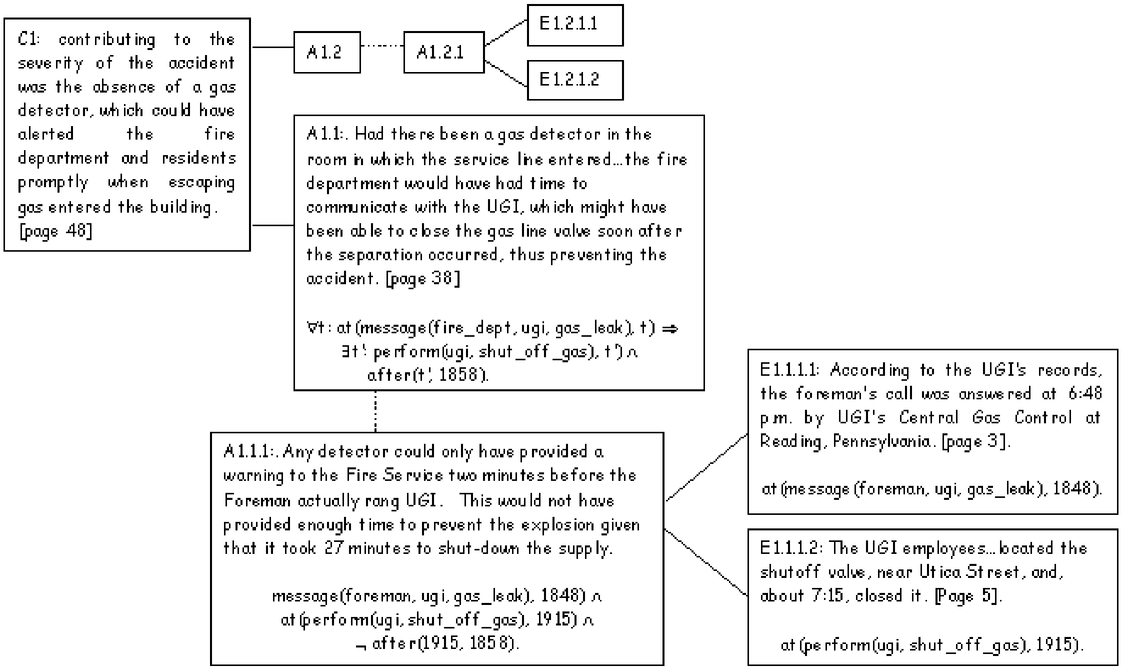
Modelling notations must satisfy two different sets of requirements if they are to support incident reconstruction. The first centers on the usability of the technique; can investigators learn to apply the approach to quickly and accurately reconstruct the events leading to an incident? The second set of requirements focuses on expressiveness; does the notation enable designers to represent salient aspects of the incident?

Proportionate Effort and Ease of Learning

Different notations offer different degrees of support to various stages of the learning process. For instance, graphical notations may be easier for novices to understand than textual notations. Features such as a simple linear relationship between time and the position of annotations on a time-line can help people at the lower ends of the learning curve to focus upon key concepts rather than underlying mechanisms. Conversely the features of more advanced temporal logics, such as model based semantics and Kripke proof techniques, help more experienced analysts to exploit the full power of the language.

It is important to emphasise, however, that investigators will not invest the time necessary to gain additional expertise in complex modelling notations unless that are persuaded of the benefits. The rewards from using a notation must be perceived to be in proportion to the time taken to learn that notation [151]. This has significant consequences for some of the notations that have been introduced in this chapter. It has not been demonstrated that formal logics and semi-formal notations, included extended fault trees, offer significant benefits over less formal approaches, including graphical and textual time-lines. Unfortunately, this creates a paradox. More formal notations are rejected because they are not perceived to offer significant benefits. However, it is difficult to determine whether these approaches will offer significant benefits because they have not been widely adopted.

There have been a number of attempts to validate the potential benefits of semi-formal and formal notations both as tools for incident reconstruction and, more generally, to support the design of safety-critical systems. These studies yielded a number of interesting insights. For example, in one study we investigated whether engineers could learn to read and analyse complex reconstructions of safety-critical applications. The studies focussed on a number of different applications with complex



C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]

A1.1:. Had there been a gas detector in the room in which the service line entered...the fire department would have had time to communicate with the UGI, which might have been able to close the gas line valve soon after the separation occurred, thus preventing the accident. [page 38]

$\forall t: at(message(fire\_dept, ugi, gas\_leak), t) \Rightarrow \exists t': perform(ugi, shut\_off\_gas), t') \wedge after(t', 1858).$

A1.1.1:. Any detector could only have provided a warning to the Fire Service two minutes before the Foreman actually rang UGI. This would not have provided enough time to prevent the explosion given that it took 27 minutes to shut-down the supply.

$message(foreman, ugi, gas\_leak), 1848) \wedge at(perform(ugi, shut\_off\_gas), 1915) \wedge \neg after(1915, 1858).$

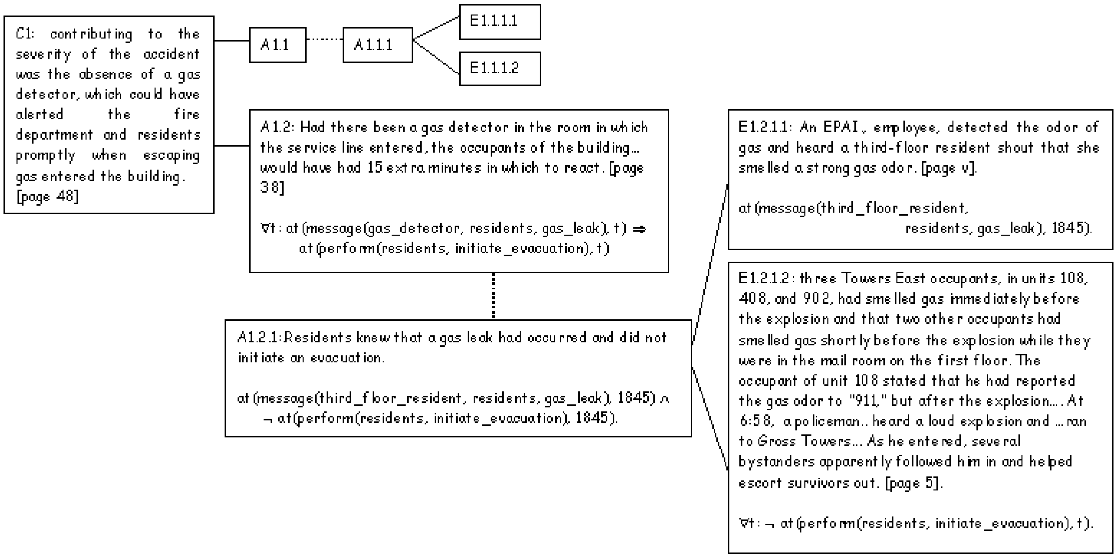
E1.1.1.1: According to the UGI's records, the foreman's call was answered at 6:48 p.m. by UGI's Central Gas Control at Reading, Pennsylvania. [page 3].

$at(message(foreman, ugi, gas\_leak), 1848).$

E1.1.1.2: The UGI employees...located the shutoff valve, near Utica Street, and, about 7:15, closed it. [Page 5].

$at(perform(ugi, shut\_off\_gas), 1915).$

Figure 9.29: Extended CAE Diagram Integrating Formal and Informal Material (1)



C1: contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building. [page 48]

A1.2: Had there been a gas detector in the room in which the service line entered, the occupants of the building... would have had 15 extra minutes in which to react. [page 38]

$\forall t: at(message(gas\_detector, residents, gas\_leak), t) \Rightarrow at(perform(residents, initiate\_evacuation), t)$

A1.2.1: Residents knew that a gas leak had occurred and did not initiate an evacuation.

$at(message(third\_floor\_resident, residents, gas\_leak), 1845) \wedge \neg at(perform(residents, initiate\_evacuation), 1845).$

E1.2.1.1: An EPAI., employee, detected the odor of gas and heard a third-floor resident shout that she smelled a strong gas odor. [page v].

$at(message(third\_floor\_resident, residents, gas\_leak), 1845).$

E1.2.1.2: three Towers East occupants, in units 108, 408, and 902, had smelled gas immediately before the explosion and that two other occupants had smelled gas shortly before the explosion while they were in the mail room on the first floor. The occupant of unit 108 stated that he had reported the gas odor to "911," but after the explosion.... At 6:58, a policeman.. heard a loud explosion and ... ran to Gross Towers... As he entered, several bystanders apparently followed him in and helped escort survivors out. [page 5].

$\forall t: \neg at(perform(residents, initiate\_evacuation), t).$

Figure 9.30: Extended CAE Diagram Integrating Formal and Informal Material (2)

failure models. These were modelled using temporal logic and a simplified Petri Net notation. This differed from the more convention notation introduced in this chapter because only one place was marked at any stage of a reconstruction. It was, therefore, very similar to state transition networks [405]. For instance, one study looked at the behaviour of a gas turbine controller. The participants were engineers stationed on rigs off the United States and Norwegian coasts. We faxed them example models and a number of associated questions. They were encouraged to take as long as they needed to answer the questions but to report the amount of time that they required to complete the questionnaires. They were expected to respond to two different types of question. The first tested their comprehension of the reconstruction. For instance, they were asked 'does the model describe any possible error condition after the application was loaded?' and 'was the application active after the error was acknowledged?'. The comprehension questions were counter-balanced so that subjects could not re-use their answers from the graphical reconstruction to answer questions about the logic model or vice versa. We also asked more qualitative questions about their impressions from using the formal and semi-formal notations. For instance, we asked them whether or not they would have preferred the reconstructions to have been expressed in natural language rather than the logic or the graphical notation.

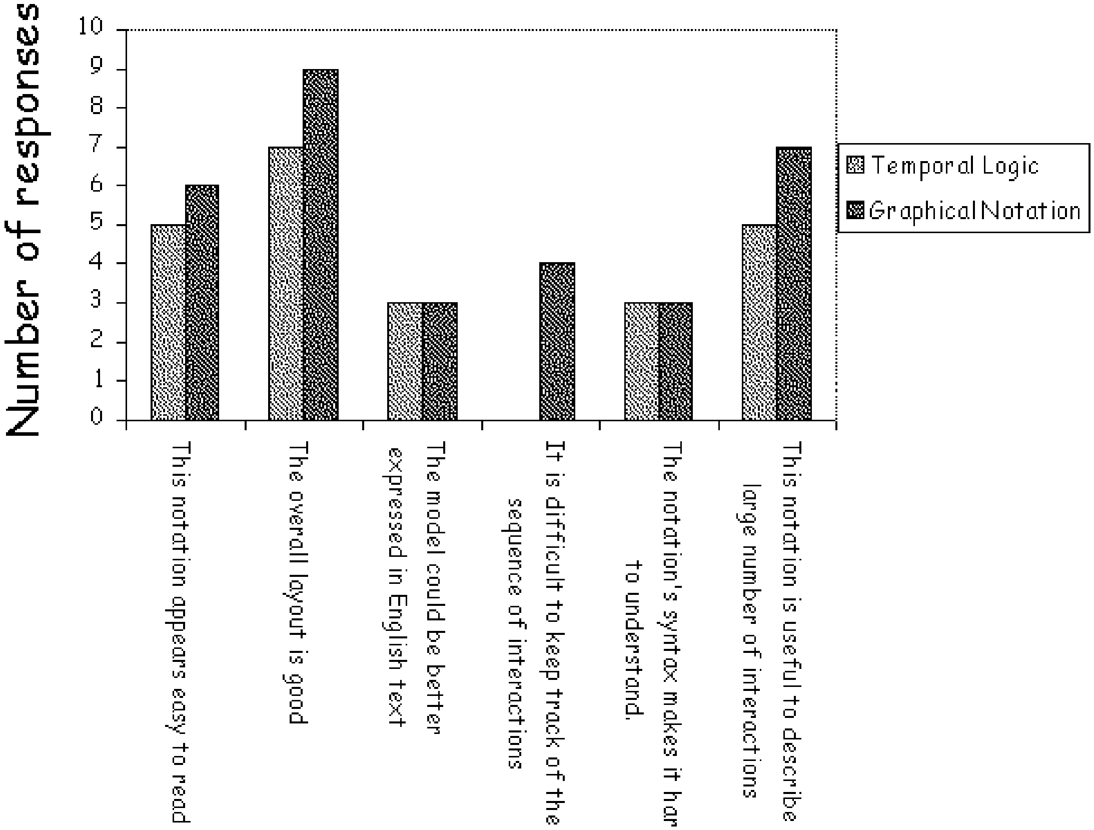


Figure 9.31: Subjective Responses to Modelling Notations.

The results confirmed many of our intuitions about the application of formal and semi-formal reconstruction techniques. For instance, the first set of fifteen US and Norwegian engineers only provided correct answers to 60 per cent of the comprehension questions using the graphical notation. The same group achieved a 55% success rate with the logic notation. Although these results seem disappointing, they were achieved without any formal training in the use of the notations. There were large deviations in individual scores. For instance, one engineer scored 100% in both conditions whilst another did not better than 30% correct. There were also some surprises. This group of engineers took an average of 8.2 seconds to answer the comprehension questions using the graphical notation and 8.7 seconds to answer using the logic-based reconstruction. Again, there were considerable deviations in individual performance. Figure 9.31 provides an overview of the responses to the modelling notations. Each individual had to tick a box stating that they agreed or disagreed with the statement. Each column, therefore, has a maximum value of 15. Perhaps the most surprising result here is that so few of the engineers believed that the model could be better expressed in natural language rather than either the graphical or logic based notation. This is interesting because it suggests that our limited sample of qualified engineers have a certain tolerance for the use of formal and semi-formal notations. Follow-up interviews revealed that similar techniques, for example fault trees, formed a common ingredient in their education and training.

There are a number of caveats that must be raised about such attempts to assess the usability of incident reconstructions. Previous chapters have argued that questionnaires and self-reporting techniques both raise a host of methodological questions about the reliability of the data that they yield. In particular, this initial study focussed on individual responses to a single set of tasks. It did not study the effectiveness of a reconstruction technique for the team-based tasks that typify incident investigations. Nor did it assess whether the long-term benefits of using either the graphical or logic-based technique were perceived to outweight any training overheads. In other words, it provided a single snap-shot of engineers' attitudes at a relatively early stage on the learning curve. It should also be stressed that our findings are not statistically significant, with limited exceptions [405]. Further studies are required to replicate these findings for other incident reconstructions and for greater numbers of potential users. The sample used in this study was relatively small. This was a consequence of our decision to use practicing engineers with similar skills and backgrounds. A number of practical reasons motivate the decision to restrict our sample in this way. Incident reconstructions must account for the technical causes of systems failure. It is, therefore, important that potential participants understand the potential causes of these systems failures. Otherwise, any results might stem from the participants ignorance about the application domain rather than from attributes of the reconstruction. However, this decision raised further issues. In particular, we could not obtain access to enough individuals with experience as incident investigators. Hence the exercise relied upon the participants' experience as design engineers attempting to diagnose potential problems that they had observed in a system rather than as incident investigators responding to reports from others within their organisation. Some of these caveats can be addressed by recruiting a larger group of participants. For example, a cohort of undergraduate students might have been used. However, the findings of such a study cannot easily be generalised to account for the attitudes of individuals who are likely to participate in incident investigations. Ultimately such studies probably require the financial backing and administrative support of regulatory authorities if they are to produce satisfactory results. We are, however, unaware of any field trials or studies that are specifically intended to validate potential techniques for incident reconstruction and modelling.

Visual Appeal

The previous section has argued that investigators must be persuaded of the practical benefits of reconstruction techniques if they are to invest time and money in learning to exploit them. The initial 'visual appeal' of a notation has a profound impact upon whether or not such investments will be made. For instance, logics are often rejected as being unnecessarily complex [427]. They lack the visual appeal of many graphical notations. However, this initial assessment can be very misleading. It can be difficult to maintain fault trees that extend to several hundred events. In contrast, mathematical abstraction techniques can be used to support the maintenance of large scale logic reconstructions [118]. It can be argued that the visual appeal of graphical notations must be weighed against the reasoning power of textual notations. This would, however, be too simplistic an analysis. For instance, there are strong text-based reasoning techniques associated with Petri Net reconstructions [679]. There are also well-established techniques for moving between these different representations. For example, Hura and Attwood demonstrate that the gates of a fault-tree can be represented by the places and transitions of a Petri Net [379]. Alternatively, the findings of formal proof techniques can be presented using semi-formal approaches that include the CAE diagrams and proof trees of previous sections.

There are additional costs associated with hybrid techniques that move between textual and graphical approaches or between formal and semi-formal notations. For example, it can be difficult to ensure that these multiple representations remain consistent during the course of an investigation. It is, therefore, again important to demonstrate the 'real-world' benefits of such hybrid techniques. We have conducted a number of studies to determine whether engineers can use semi-formal argumentation structures, similar to CAE diagrams, to address the usability problems that are often perceived to jeopardise the use of logic-based notations. For instance, a week-long trial was conducted with a group of software engineers from a range of industries. During this period the subjects were trained from 'scratch' to a level where they could both read and write logic-based models of complex, safety-critical systems. The first four days included an intensive course on discrete mathematics. On the fifth day, they were presented with a logic-based model of a control application for a chlorine recovery system. Elements of this model were then used to reconstruct the events leading to a previous incident involving this application. The engineers were asked a number of qualitative questions about the usability of the formalisation. The results of this are shown as Figure 9.32. As can be seen, our subjects found the model to be either impossible or hard to understand even after a week's intensive training.

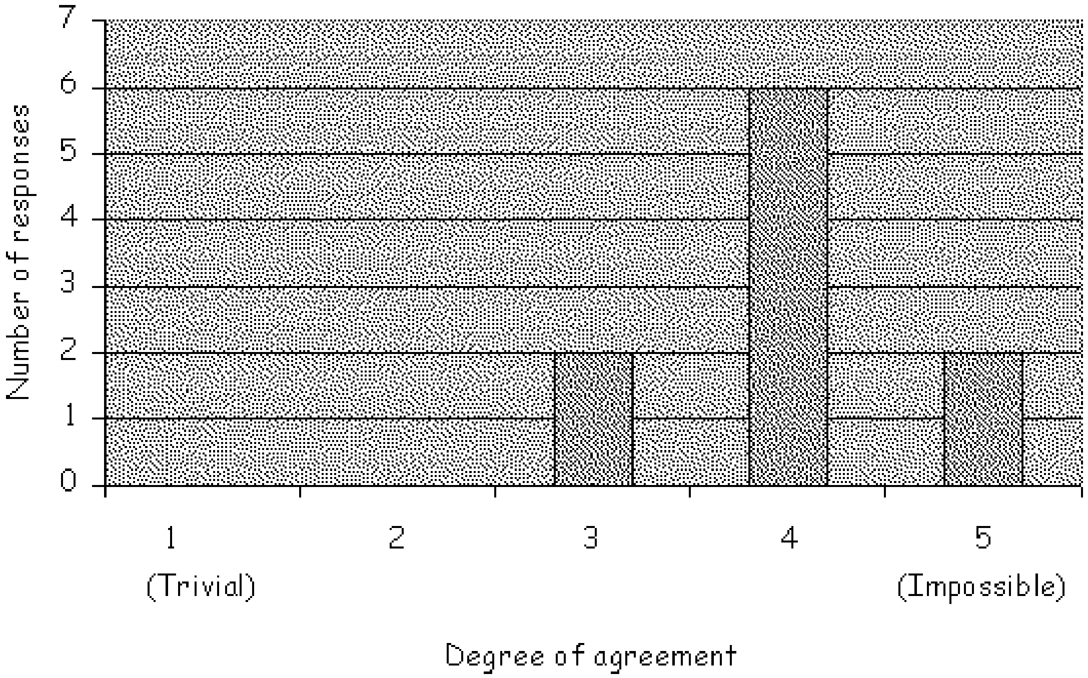


Figure 9.32: Subjective Responses to Logic-Based Reconstruction
How Easy did you find it to understand the logic-based model?

Such results are not particularly surprising. The application of logic is a skill based activity. The example used was of 'industrial strength'; it was based around the failure of a real system One week provides insufficient training to develop the expertise that is necessary to become confident in the use of formal reconstructions. Perhaps, more surprising are the qualitative responses for the semi-formal diagrams. After being asked to analyse the logic model, our subjects were shown a CAE-based diagram for another area of the chlorine recovery system. The ratings for this are shown in Figure 9.33. It should be noted that the logic-based reconstruction provided a detailed explanation of the events leading to an incident. In contrast, the graphical representation sketched the arguments for and against two competing explanations for a failure elsewhere in the recovery application.

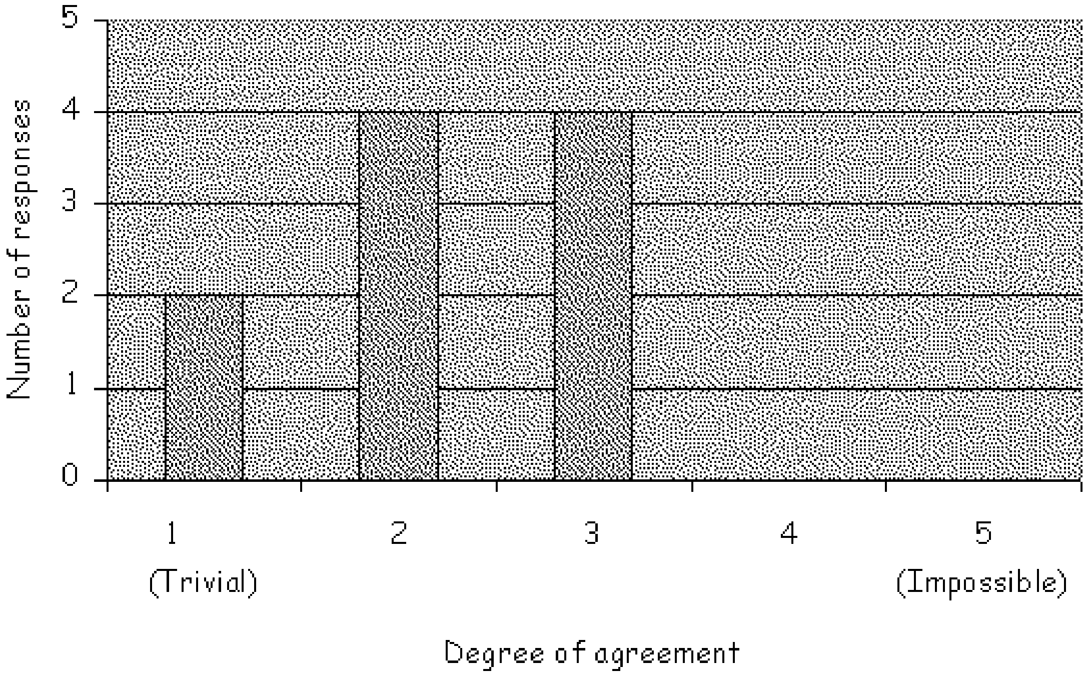


Figure 9.33: Qualitative Assessments Of CAE-Based Diagrams
How Easy Did You Find It to Understand the CAE Diagram?

In contrast to the formal specification, the subjects found it far easier to understand the graphical notation. It is important to emphasise, however, that no direct comparisons can be made between the attitude statements in Figures 9.32 and 9.33. Clearly, the information content is quite different. We then presented the participants with a more integrated reconstruction that that included logic clauses within a CAE diagram. The resulting diagram was similar to that presented in Figures 9.29 and 9.30. The participants' responses to this hybrid approach are shown in Figure 9.34. This provide some encouragement, especially considering the antipathy to logic-based reconstructions and that the participants had not any previous training in discrete mathematics.

As with the previous validation, these findings are suggestive rather than conclusive. we have not, to date, been able to guarantee the participation of a reasonable sample of trained incident investigators. As a result, we have been forced to rely upon the support of practicing engineers who have participated in incident investigations but who are not specifically trained in the investigatory techniques mentioned in previous chapters. There rae many reasons for this. One is that there are still relatively few trained investigators within even large-scale commercial organisations. They tend to be senior staff. In consequence, it can be difficult to secure their participation in such validation exercises. This study proved to be particularly difficult because it did not simply rely upon the one-off questionnaires that were described in the previous study. We had to train our subjects over a significant period of time; this involved a high degree of commitment from both the individuals concerned and from their companies. We are currently attempting to replicate our results with

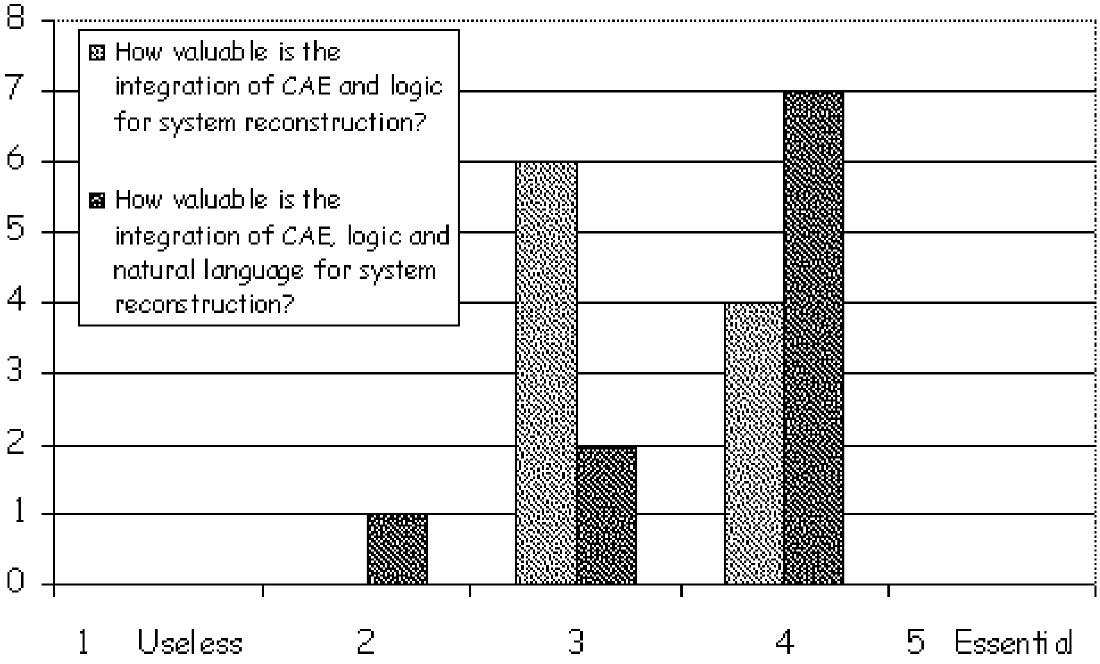


Figure 9.34: Qualitative Assessments of Hybrid Approach

larger groups of engineers and investigators. Again, however, it is difficult to foresee how many of the practical barriers will be resolved without greater regulatory commitment and support.

Tool Support

Previous sections have argued that semi-formal and formal notations provide investigators with means of focusing on critical properties of incidents and accidents. Irrelevant details can be stripped out to represent those events that contribute to an adverse occurrence. However, we have also demonstrated that these models can also become difficult to develop and maintain. For instance, there are significant overheads involved in constructing Petri Nets such as that shown in Figure 9.1.3. It can also be difficult to prove that the introduction of clauses, such as (9.2) and (9.3), does not contradict previous assertions about the course of an incident. It can be argued that this complexity is an inevitable consequence of our increasing desire to adopt a 'systems' approach to incident investigation. As we have seen, reconstructions must capture both the proximal and the distal causes of adverse occurrences. This inherent complexity helps to increase the importance of tool support during incident reconstruction. Tools can help in a number of ways. They can provide electronic support for the problems of constructing, navigating and typesetting complex graphical structures that might otherwise extend over many printed pages. Tool support can also implement syntactic checks to ensure that designers have constructed valid sentences from the lexical tokens in a formal language. They can partially automate reasoning about critical properties of incident reconstructions. As we have seen in the previous chapter, they can also be used to develop interactive simulations of adverse occurrences. Some tools enable these simulations to be directly derived from the abstract models that we have presented in this chapter.

The use of a formal or semi-formal notation does not guarantee the error-free development of an incident reconstruction. In Chapter 2.3 we defined a mistake to 'stem from a failure to select appropriate objectives irrespective of whether or not the actions taken to achieve those objectives are successful'. It is entirely possible that other analysts will conclude that investigators are mistaken in those aspects of an incident that they choose to reconstruct. We defined slips and lapses to 'result from some failure in the execution of a plan or well understood sequence of actions regardless of whether that plan was or was not appropriate'. By extension, it is also possible for investigators to develop a reconstruction that does not model an incident in the manner that they intended. For example, the structure of a Petri Net may make it impossible for places to be marked in the sequence that was intended by the investigator. Alternatively, a fault tree might have a minimal cut set that was not intended by the analyst and which could not have led to the incident given the available evidence.

At a higher level, it is possible for analysts to combine the tokens of a language to construct a model that has no meaningful interpretation. For instance, the places of a Petri Net must be connected to transitions. It is unclear what it would mean for one place to be connected directly to another place in such a graph. However, it can be difficult to avoid such errors when reconstructions can grow to include several hundred nodes or clauses. As a result, it is important to provide as much support as possible during the development of incident models. Type checking tools can ensure that relations hold between variables of the correct sort within the clauses of a logic model. Similar tools exist for the construction of both Petri Nets and Fault Trees. Without such support, it is difficult to conceive of large teams of designers constructing and maintaining detailed models of complex incidents. Computer-based tools can also conduct syntax checks. For instance, structure editors enable analysts to automatically insert syntactically correct components into a reconstruction. This raises a number of further usability issues. Some tools force analysts to *always* construct valid models. This can lead to considerable frustration. For example, it is frequently the case that investigators will have identified an important transition within an incident reconstruction. However, it may not be clear where it fits within the developing model. A tool that ensures continual correctness would force the analyst to link the transition to the rest of the network even if they did not feel confident about this placement. Incremental checking tools avoid this problem. They enable analysts to construct syntactically incorrect models. Places may initially be unconnected to any transitions and vice versa. However, these tools typically enable their users to periodically check the syntax of their structure once they feel confident that they have achieved a satisfactory placement of a node or that they have correctly constructed the axioms of their model. The meta-level issue is that not all tools provide equal degrees of support for incident reconstruction. Poorly designed tools may do little to address the usability problems that affect formal and semi-formal notations.

As mentioned, there are many different tools that can be recruited to support the reconstruction of complex incidents. The previous paragraph focussed on syntax editors and type checkers. However, other systems can be used to 'directly' develop prototype implementations from formal models [720, 721]. Chapter 7.3 included an example of a datalink air traffic control system that was simulated using this approach in Figure 8.15. This is important because formal and semi-formal notations can provide an extremely poor impression of the events leading to an accident. Interactive simulations can be shown to other analysts in order to validate the assumptions that are contained within accident models.

9.2.2 Expressiveness

A principle requirement for any incident reconstruction is that it should be capable of representing the diverse events that contribute to adverse occurrences. This creates problems because the temporal properties of control systems are very different from those of their operators. Similarly, the catalytic failures occur on a very different timescale to the period over which management and regulatory changes can be effected. For example, the NTSB investigators recorded the EPAI's foreman's recollections that:

> "The foreman said that he then went to his pickup truck and, using his cellular phone,2 called the gas company and the housing authority, telling them that he was excavating near the gas line and smelled gas. He stated that he next made three attempts to phone '911'. He said that each time he called, there was no answer. He said he then moved his truck to another spot in the parking lot in case the phone signal to his cellular

> phone was being blocked. He said that at the new location he again tried unsuccessfully to call '911'." [589].

This can be contrasted with the level of detail in the following observations about systems behaviour within the Cullen report into the Piper Alpha incident [194]. Here the focus is upon the observable behaviour of a gas detection system during the disaster:

> "It became apparent that only the larger leaks could give a flammable gas cloud containing the quantity of fuel evidently necessary to cause the observed explosion effects. Interest centred therefore particularly on series 42, which was the only test at a leak rate of 100 kg/min. In this test the low level alarms occurred first for C3 in 5 seconds, then for C2, C4 and C5 in 15, 20 and 25 seconds respectively..." (page 77).

The first quotation is based around an individual's recollections. The timings are vague and, in this case, difficult to substantiate. The second quotation provides clear and precise timings for alarms that have been validated by empirical studies on replicas of the system. These examples illustrate how the range of temporal properties that must be captured in any reconstruction is determined by the nature of the incident that is being considered. For example, the NTSB investigators did not consider it necessary to model the flow of gas within Gross Towers to the same level of detail as the enquiry team did for the Piper Alpha accident. However, the nature of the temporal properties being represented within any reconstruction is also determined by the evidence that is available from any primary or secondary investigation. Some timings can be grounded while other temporal information may be vague and imprecise. For instance, table 9.2 shows how the Foreman's recollections can be measured against the records of his cellular operator.

Time	In/Out/ Complete	Duration (secs.)	Connected (secs.)	Time Between Calls (secs)	Location
18:46:41	Out Complete	13	25	9	UGI Switchboard
18:47:15	Out Complete	87	95	5	UGI Emergency Number
6:48:55	Out Complete	70	82	15	Home, EPAI V.P.
18:50:32	Out Complete	39	47	173	UGI Emergency Number.
18:54:10	Out Complete	84	121	170	Housing Authority Answer Service
18:59:01	Out Incomplete	0	55	2	911 (Allentown)
19:00:02	Out Complete	162	175	3	Home, EPAI V.P.
19:03	In Complete	120	120	40	Not Recorded
19:05:40	Out		540		Private No.
19:14	In Complete	180	180		Not Recorded

Table 9.2: Cellular Phone Records for Allentown Foreman

The Beginning and the End

When does an incident actually begin? Previous sections have argued that this is a non-trivial question and it is worth reviewing the issue in the light of our case study. For instance, we have shown how the catalytic events centre around the operation of the backhoe and other heavy equipment during the removal of the soil. However, the incident could not have occurred if the pipeline had not been left relatively unsupported after the initial operation to remove the tank. Alternatively, the incident might have started when the EPAI foreman and crew were briefed for this particular operation or when their training missed necessary information about OSHA excavation requirements. At a more general level, this incident might have stemmed from the long-running discussions about Excess Flow Valves that were chronicled in Figure 9.1. The key point here is that the starting point for an incident is often a subjective decision that reflects the analyst's view of its causes. Incident modelling notations must, therefore, represent this subjective decision. It must be possible for readers to clearly identify the moment at which an analyst considers an incident to begin.

A related question is 'when does an incident end?'. As we have seen, many conventional risk analysis techniques stop with an undesired event. This is illustrated by the fault tree in Figure 9.8. As we have seen, however, incident reconstructions must also consider what happens after such an event. In particular, they must represent the way in which people and systems either exacerbate or mitigate the consequences of any failure. For example, the Police Officer played a key role in evacuating the survivors after the initial explosion. Similarly, the prompt response of the Fire Service and the medical agencies helped to ensure that the injured were swiftly evacuated from the scene of the incident. These actions did not *cause* the accident but they did contributed to the saving of lives. They reduced the consequences of the failure itself.

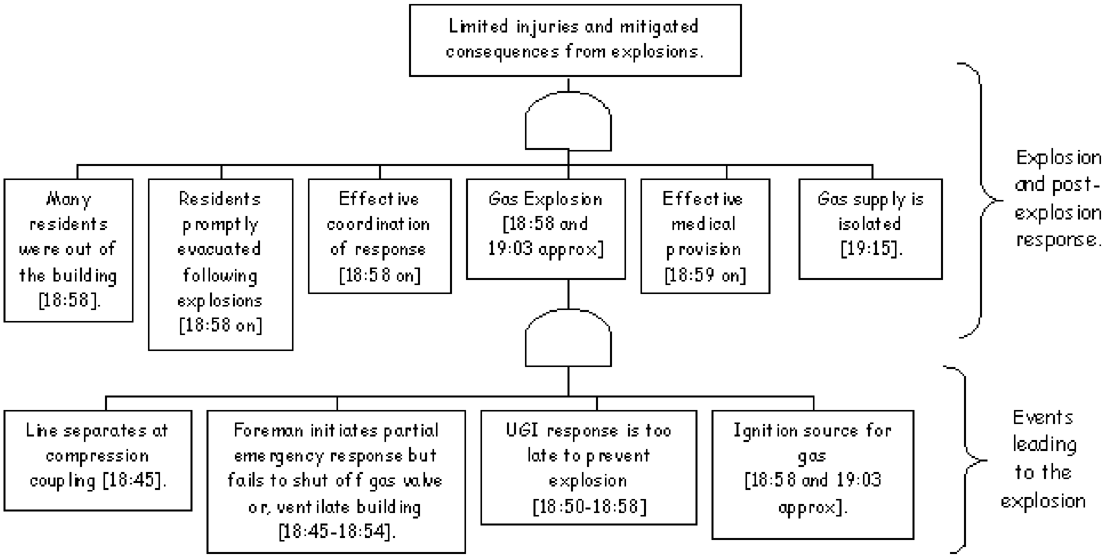

Limited injuries and mitigated consequences from explosions.
Many residents were out of the building [18:58].
Residents promptly evacuated following explosions [18:58 on]
Effective coordination of response [18:58 on]
Gas Explosion [18:58 and 19:03 approx]
Effective medical provision [18:59 on]
Gas supply is isolated [19:15].
Explosion and post-explosion response.
Line separates at compression coupling [18:45].
Foreman initiates partial emergency response but fails to shut off gas valve or, ventilate building [18:45-18:54].
UGI response is too late to prevent explosion [18:50-18:58]
Ignition source for gas [18:58 and 19:03 approx].
Events leading to the explosion

Figure 9.35: Allentown Fault Tree Showing Pre- and Post-Incident Events

Figure 9.35 uses elements of the Fault Trees that were constructed in previous sections of this chapter to show how modelling notations can be used to reconstruct events leading to, and stemming from, an adverse occurrence. The analyst's view of the start and finish of the accident are explicitly bounded by the extent of the tree. In this case we have not expanded the events that, for instance, contributed to Foreman's response. If investigators considered that such details fell within the scope of any analysis then they could be introduced as shown in Figure 9.10. Nor does it expand on the events that contributed to the effective coordination of the Emergency Services' response from 18:58 on, illustrated in Figure 9.13. These details can, of course, be introduced to explicitly indicate that they fall within the scope of the investigation. The development of the incident fault tree, therefore, encourages analysts to represent the extent of their enquiries. This can help to avoid the implicit decisions and misunderstandings that may threaten any subsequent causal analysis.

Figure 9.35 illustrates the strengths and the weaknesses of fault trees as a reconstruction notation. Te scope or extend of incident is explicitly represented. However, the lines between nodes represent a mixture of causal, temporal and logical relationships. This overloading provides considerable expressive power. It can also be misleading. For instance, previous sections have argued that incident fault trees can be formatted to preserve a left to right temporal ordering. Events and gates that occur during the early stages of an incident should be drawn to the left of components that occur later on. However, this convention does not form any part of the syntax or semantics of the fault tree notation. We have also shown the problems that arise when attempting to satisfy such a requirement. Events at one level in a tree can occur after or before events at another level. The best example of this is where some event in the aftermath of an incident is influenced by another, organisational or managerial, event that occurred long before the incident took place. In this case, the organisational event that contributed to the response would be shown higher-up the tree because its relevance is not to the pre-incident events but to the consequences of that failure.

Concurrency

Figure 9.36 illustrates the structure of many incident reports. Each chapter presents a chronology of events from a different perspective. A synopsis or overview chapter is followed by an analysis of any systems failure. The systems analysis is followed by an investigation of operational and management issues. This, in turn, is followed by an interpretation of any emergency response and so on. As a result, if a reader wants to build up a coherent view of all of the events in an incident at a particular point in time then they are forced to cross-reference many different sections of the report. For example, the events occurring at times T1 and T2 are described in each of the chapters represented in Figure 9.36. These problems also affect investigators during the stages of reconstruction and analysis that precede the drafting of an incident report. They must piece together information about the many different aspects of complex systems failures. This implies that there must be some means of representing and reasoning about concurrent interaction between the simultaneous failures that contribute to many incidents and accidents.

As we have seen, there are a range of graphical and textual notations that can be used to address these concerns. They provide explicit means of representing the concurrent events that occur in different areas of a system. They can also be used to represent the way in system failures and human error combine, at critical moments, to create the circumstances for an accident. To illustrate the importance of this, consider the following excerpts provided by the NTSB investigators into the Allentown incident:

> “When an Allentown fire inspector was inspecting the EPAI’s work, he saw the excavation’s west sidewall slide into the excavation, exposing the gas line, which was 3 to 4 feet west of the tank. The collapsed sidewall removed the soil support from about 30 feet of gas line causing it to sag.” ([589], page 10).
>
> “Neither the EPAI employees nor the fire inspectors notified the UGI that the service line was unsupported and damaged. Later on May 23, the EPAI crew placed a cable sling around the tank and attached it to a chain that was attached to the backhoe. When the crew tried to lift the tank, the chain broke. Those who witnessed the event, including the second fire inspector, stated that they did not believe the tank struck the gas line”. ([589], page 11),
>
> “Because the citys fire inspectors saw on May 23 that the service line was unsupported, they could have prevented the accident. They showed proper concern about the safety of the line, especially after a piece of asphalt pavement fell on it and deformed it. However, not having been instructed to do otherwise, both inspectors relied on the EPAI foremen’s assessment that the line was safe”. ([589], page 36).

These quotations illustrate how it can often be difficult for readers to form a coherent model of the events that are identified during incident investigations. for instance, these different accounts

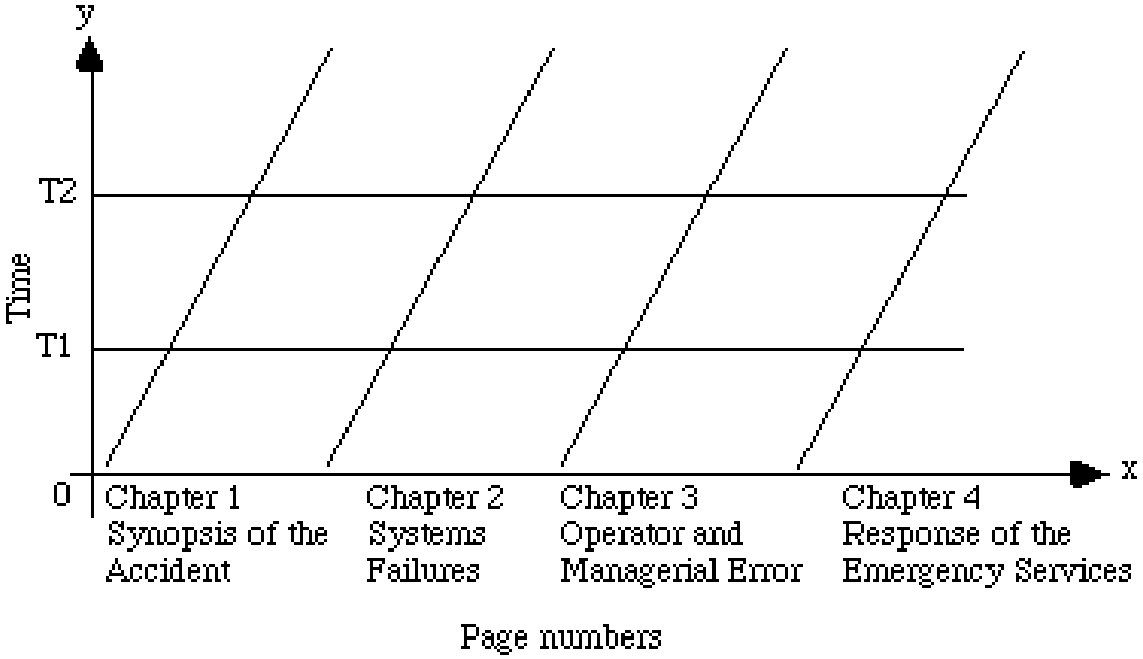


Figure 9.36: Cross-Referencing Problems in Incident Reports

do not state the order in which the wall collapsed, the chain broke or the asphalt struck the gas pipe. This ordering has to be inferred from evidence presented elsewhere in the report. Similarly, it can be difficult to determine how these different events affected the different people who were involved in the incident. Figure 9.37 builds on the Petri Nets that were introduced in previous sections to reconstruct a more coherent model of some of these events. As can be seen, the marking in this diagram denotes that the foreman is initially happy with the safety of the line, in spite of the inspector's concerns, and that asphalt is being lifted over the gas supply. The diagram, therefore, simultaneously captures human factors observations, derived from eye witness statements, together with information about the observable sequence of events leading to the incident.

There are a number of limitations with the previous diagram. There is little direct evidence to show that the asphalt strike triggered the Foreman's decision to support the pipe although this implied by the NTSB investigators. More significantly, however, Figure 9.37 only captures the relative timings of various events. The excavation slip occurred before the inspector questioned the Foreman about the safety of the gas line. The asphalt was being moved across the gas line before it was deflected and so on. What the previous diagram does not represent is the real-time at which these different events occurred. This is a significant limitation. For instance, there might have been seconds, minutes or even hours between the deflection of the pipeline and the Foreman's decision to reconsider the safety of their system.

Figure 9.37 illustrates the strengths and weaknesses of Petri Nets for incident reconstruction. This diagram shows how the notation can be used to generalise beyond the specific circumstances of a particular incident. Previous sections have argued that the temporal characteristics of previous incidents are unlikely to be exactly replicated in future failures. For example, there was a considerable delay between the failure of the excavation wall and the physical damage that separated the exposed pipeline to Gross Towers. In future, however, there might only be a matter of seconds between the excavation failure and direct physical damage to an exposed gas supply. The Petri Net illustrated in Figure 9.37 clearly avoids any commitment to such absolute timings that might not be replicated in future incidents. This ambiguity is, however, a significant weakness if investigators are concerned to accurately represent key properties of this particular incident. For instance, previous sections shown

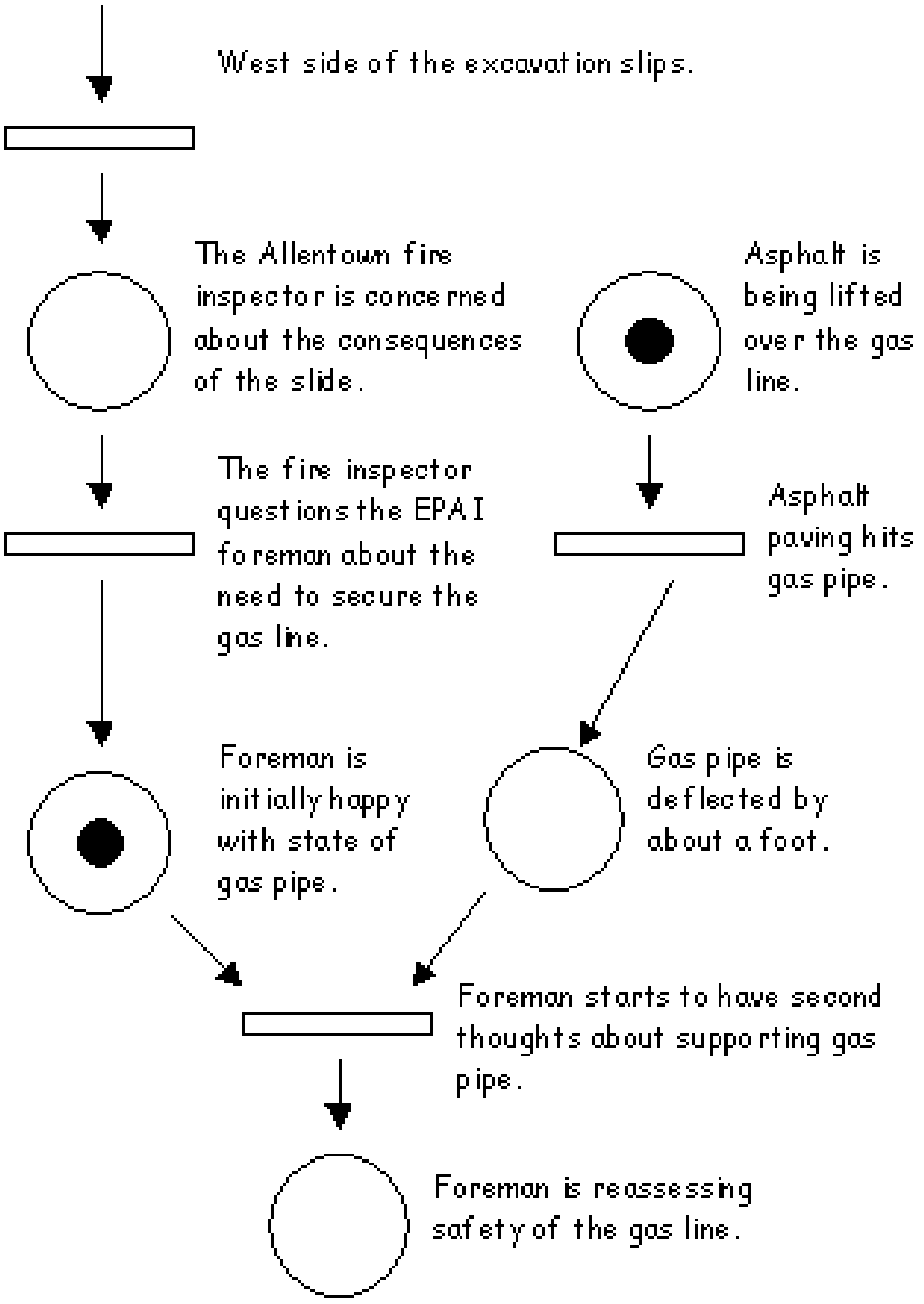

West side of the excavation slips.
The Allentown fire inspector is concerned about the consequences of the slide.
Asphalt is being lifted over the gas line.
The fire inspector questions the EPAI foreman about the need to secure the gas line.
Asphalt paving hits gas pipe.
Foreman is initially happy with state of gas pipe.
Gas pipe is deflected by about a foot.
Foreman starts to have second thoughts about supporting gas pipe.
Foreman is reassessing safety of the gas line.

Figure 9.37: Using a Petri Net to Build a Coherent Model of Concurrent Events

how investigators can temporal logics to examine the real-time characteristics of this incident. In particular, we have demonstrated that warnings from an automated gas detection system might not have prevented an explosion. Such an analysis cannot easily be performed using the relative sequences provided by the Petri Net in Figure 9.37.

Lack of Evidence

The previous section has made the case that incident modelling notations must be capable of representing real and interval time properties of adverse events. It is important, however, to emphasise that this must not force analysts into undue commitment when the exact timing for an event is unknown. For example, the NTSB investigators concluded that:

> "...the backhoe probably struck the line when being operated across it; the foreman's reports to both the UGI and the housing authority indicated that the pipe had been struck during recent excavation activities. Although the foreman denied after the accident that the backhoe had struck the line, the coating of the pipe showed evidence of mechanical damage, as did the pipe steel at one location. Also, the foreman's calls both to the housing authority and to the UGI show that at the time he believed his crew had hit the gas line while excavating." [589]

The use of terms such as 'probably' re-iterate the point that uncertainty often remains within models and reconstruction of safety-critical incidents. This uncertainty has many causes. For example, it may not be possible to obtain direct evidence to support the investigators' hypotheses. Alternatively, physical evidence can be contradicted by eye-witness testimony. In this case, the physical evidence of damage to the pipeline is contradicted by the foreman's recollections. Such contradictions can occur when witnesses do not observe key events during an incident. They can also result from the cognitive effects of stress, anxiety and guilt that have been discussed in previous chapters. This uncertainty can take many forms. For instance, the previous quotation centres on whether or not the backhoe struck the gas line when it was being operated across it. Even if we assume that the physical evidence does indicate that such damage was incurred then we cannot be certain of exactly when this happened. In consequence, even with sophisticated logging techniques it may not be possible to associate particular events with particular moment in time. Some notations provide more support for the representation of this lack of evidence than others. For example, time-lines may be extended with informal annotations as shown in Figure 9.38.

The annotations below the time-line are used to indicate the position of events whose time is known, either through corroborated eye witness statements or through external monitoring of the event. In contrast, the annotations above the line are used to indicate imprecise timings or events for which there is contradictory evidence. The horizontal parentheses under the label Backhoe probably strikes the gas line while being operated over it is used to indicate that the event occurred one or more times between 13.30-18.40. We do not know exactly when this occurred during this interval. Such annotations do not form part of the conventional time-line notation. This is important because analysts would have to learn to exploit a number of further extensions if such an approach were to represent the differing forms of temporal uncertainty that arise during many investigations. These can be summarised as follows:

- *a certain event with uncertain timing.* The event is known to have taken place but there is no clear evidence for when it occurred;

- *an uncertain event with uncertain timing.* It is not clear whether this event actually occurred or, if it did, when it actually took place. In some respects, this is the pathological case for incident reconstruction;

- *a certain event with certain timing.* This is the ideal case. There is clear evidence that an event occurred and there is evidence for when it took place.

- *an uncertain event with certain timing.* It is unclear whether the event actually occurred but, if it did, there is evidence for when it must have taken place.

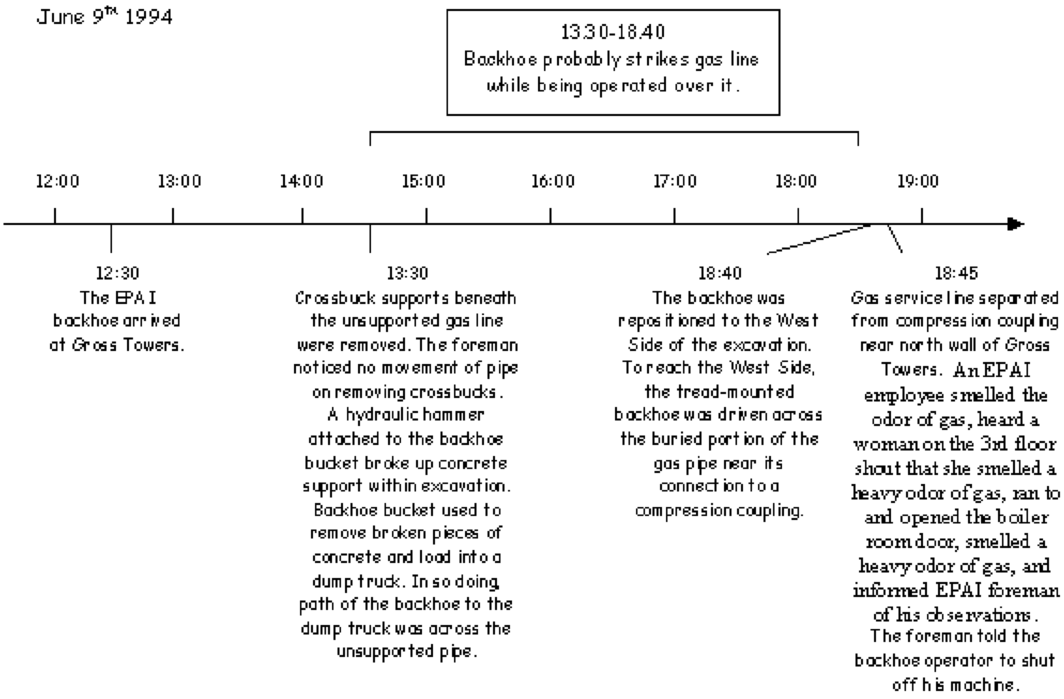

June 9th 1994
13:30-18.40
Backhoe probably strikes gas line while being operated over it.
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
12:30
The EPAI backhoe arrived at Gross Towers.
13:30
Crossbuck supports beneath the unsupported gas line were removed. The foreman noticed no movement of pipe on removing crossbucks. A hydraulic hammer attached to the backhoe bucket broke up concrete support within excavation. Backhoe bucket used to remove broken pieces of concrete and load into a dump truck. In so doing, path of the backhoe to the dump truck was across the unsupported pipe.
18:40
The backhoe was repositioned to the West Side of the excavation. To reach the West Side, the tread-mounted backhoe was driven across the buried portion of the gas pipe near its connection to a compression coupling.
18:45
Gas service line separated from compression coupling near north wall of Gross Towers. An EPAI employee smelled the odor of gas, heard a woman on the 3rd floor shout that she smelled a heavy odor of gas, ran to and opened the boiler room door, smelled a heavy odor of gas, and informed EPAI foreman of his observations. The foreman told the backhoe operator to shut off his machine.

Figure 9.38: Lack of Evidence, Imprecise Timings and Time-lines

Even this list is a simplification. For instance, investigators may have evidence that an event did occur and that it happened at a particular moment during an incident. However, there may not be any evidence about the duration of an event or if it occurred more than once. There are further complexities. For instance, it is important to distinguish between instantaneous events and more gradual changes that influence the underlying state of any system. There is an important distinction between this sort of information and that shown above the time-line in Figure 9.38. In the former case the event is instantaneous but it's timing is not known, in the latter case the property is continuous and its duration is well known. This distinction could be supported by introducing further annotations within the time-line notation.

Figure 9.39 illustrates the way in which additional syntactic features must be introduced to represent gradual changes in the underlying state of the system. In this instance, a different form of horizontal parentheses denote a continuous change over an interval rather than a discrete event at a particular point in the time-line. This diagram also illustrates the use of previous annotations to denote imprecise information. The text above the time-line is used to represent the lack of information about when exactly the foreman ordered his crew to trace the line back towards Utica Street. It is important to emphasise that the degree of uncertainty that is represented in diagrams such as Figure 9.39 will change over time. There is a strong motivation for investigators to resolve ambiguity as more evidence becomes available. Techniques, such as time-lines, that can be used to represent an event without commitment to whether it occurred or when it occurred are, therefore, more appropriate to the early stages of reconstruction. Other techniques, including computer-based simulation, that force greater commitment to particular timings are used more often in the later stages of an investigation.

Figure 9.39 shows how investigators must extend the basic time-line notation if they are to distinguish between different forms of uncertainty or between discrete events and continuous change. This illustrates the flexibility of this informal notation. The absence of strong syntactic rules enables designers to introduce novel features without worrying about whether or not the resulting diagrams

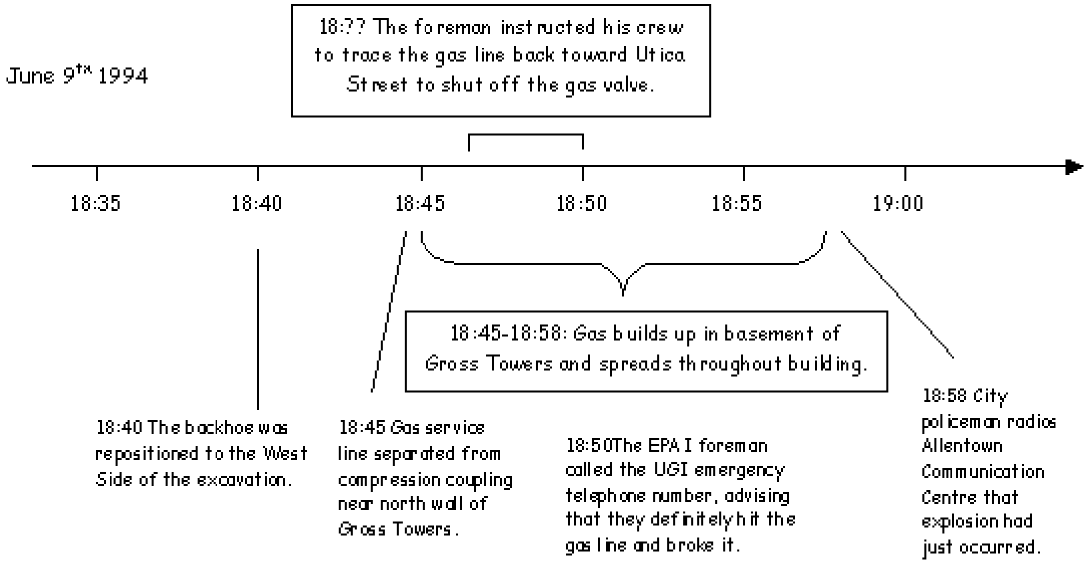

June 9th 1994
18:?? The foreman instructed his crew to trace the gas line back toward Utica Street to shut off the gas valve.
18:35
18:40
18:45
18:50
18:55
19:00
18:45-18:58: Gas builds up in basement of Gross Towers and spreads throughout building.
18:40 The backhoe was repositioned to the West Side of the excavation.
18:45 Gas service line separated from compression coupling near north wall of Gross Towers.
18:50The EPA I foreman called the UGI emergency telephone number, advising that they definitely hit the gas line and broke it.
18:58 City policeman radios Allentown Communication Centre that explosion had just occurred.

Figure 9.39: Continuous changes and Time-lines

will represent 'valid' or well formed time-lines. However, this freedom also results in a proliferation of ad hoc annotations within different investigation teams. During the prepartion of this book, I witnessed different investigators use the same annotation to represent different types of temporal properties. One used an asterisk to represent an uncertain event with a known time whilst their colleague used it to represent multiple occurrences of a known event at a known time. As a result, other members of the team had to recognise who had drawn any particular asterisk in order to know what it meant!

Inconsistencies

It is a frequent observation in incident reports that the evidence of one witness does not agree with that of another. Most often, these disagreements focus upon the sequence and timing of critical events. Alternatively, as we have seen in the previous section, they may disagree about whether or not those events ever took place at all. The following citation provides a further example of such contradictions. The foreman stated that he and other crewmembers supported the pipeline before they left the site. In contrast, housing authority employees testified that the line was unsupported:

> "The tank was successfully removed from the excavation, and samples of soil were taken adjacent to the tank's concrete support, which remained in the excavation. The soil was to be tested to determine whether fuel had leaked from the tank and contaminated the surrounding soil. The EPAI foreman stated that before he and the other crewmembers left the site, they tried to support the pipe with saw horses, surrounded the excavation with orange plastic barrier fencing, put plastic sheeting over the excavation slopes, including the soil that lay beneath the pipe, and removed the equipment from the site. They left the excavation open to await the result of the tests. Housing authority employees who frequently passed the excavation between May 23 and June 9 stated they observed that the exposed pipe was not supported." [589]

Analysts must consider the different scenarios that are created by such uncertainty. The following Petri Nets illustrate this point. The diagram on the left of Figure 9.40 presents an extract from the Petri Net previously introduced in Figure 9.1.3. This represents the view that the saw horses were left providing partial support for the exposed gas line after the excavation team left the site. In contrast, the Petri net on the right represents an alternative version of events based on the House

Association employees' testimony. This extends the previous networks by hypothesising that the unstable soil and adverse weather conditions contributed to the collapse of the supports that had previously been placed under the gas line. The main conflict arises between the Housing Association employees' observations and the testimony of the Foreman and his crew, confirmed by the two Inspectors.

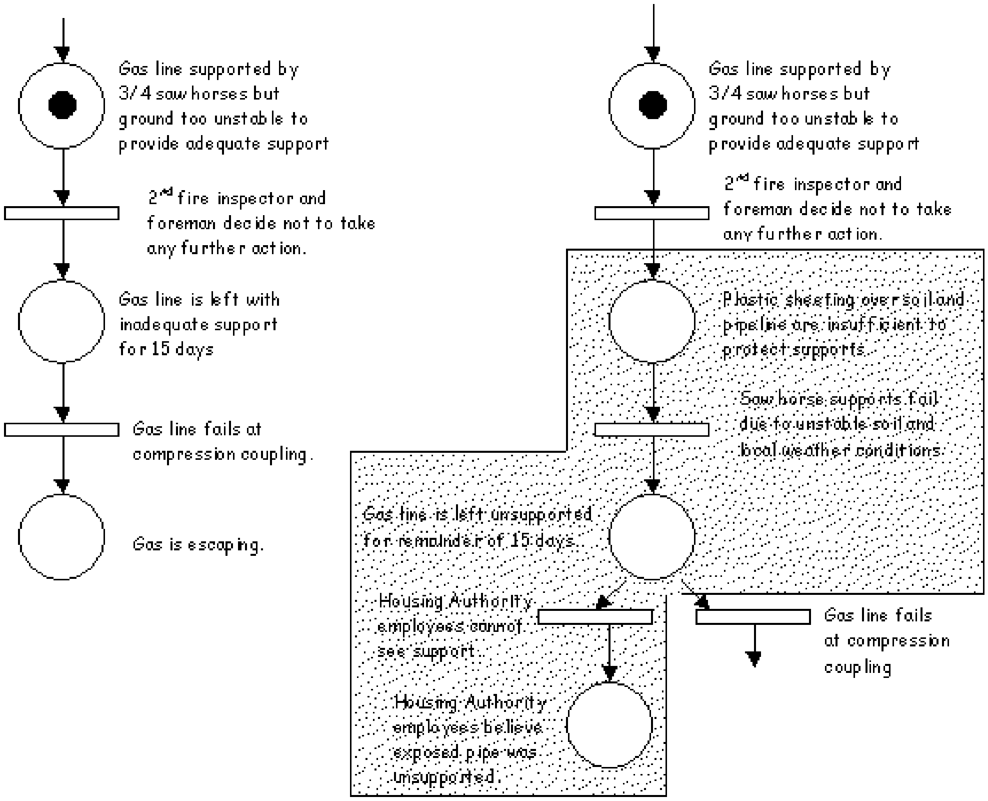

Gas line supported by 3/4 saw horses but ground too unstable to provide adequate support
2nd fire inspector and foreman decide not to take any further action.
Gas line is left with inadequate support for 15 days
Gas line fails at compression coupling.
Gas is escaping.
Gas line supported by 3/4 saw horses but ground too unstable to provide adequate support
2nd fire inspector and foreman decide not to take any further action.
Plastic sheeting over soil and pipeline are insufficient to protect supports.
Saw horse supports fail due to unstable soil and local weather conditions.
Gas line is left unsupported for remainder of 15 days.
Housing Authority employees cannot see support.
Housing Authority employees believe exposed pipe was unsupported.
Gas line fails at compression coupling

Figure 9.40: Using Petri Nets to Represent Different Versions of Events

Petri Nets have not previously been used to represent and reason about such inconsistency. This approach does not, however, provide an ideal solution. As we have seen, these networks can become extremely complex even for relatively simple behaviours. The problems associated with constructing and maintaining these diagrams can be exacerbated if they are used to represent multiple, alternative accounts of the same failures. Analysts must manually inspect the different networks in order to identify the differences that exist between these individual accounts. Figure 9.40 provides partial support by shading the area of the network to denote potential disagreement over the course of events. This is not, however, a general solution. For example, subtle differences of interpretation about the initial causes of an incident might have consequences that extend throughout any model or reconstruction. As a result, almost every node within a network might be shaded [408]. A more pragmatic solution is to find evidence that can be used to resolve any apparent contradictions.

Figure 9.41 shows how analysts can use the Petri Net notation to construct a third version of event that resolves the previous inconsistency. The Petri Net on the left shows that from certain positions around the excavation, the pipe might have appeared to be unsupported even though the saw horses were still in place. This can be compared with the Petri Net on the right of Figure 9.41. This network was introduced in Figure 9.40; supports failed at some point after the excavation team left the site. The key point is that the explicit reconstruction of an incident encourages investigators to identify and resolve potential inconsistencies. Additional evidence must be sought to determine which hypothesis is correct. Where there is contradictory evidence, the skill and

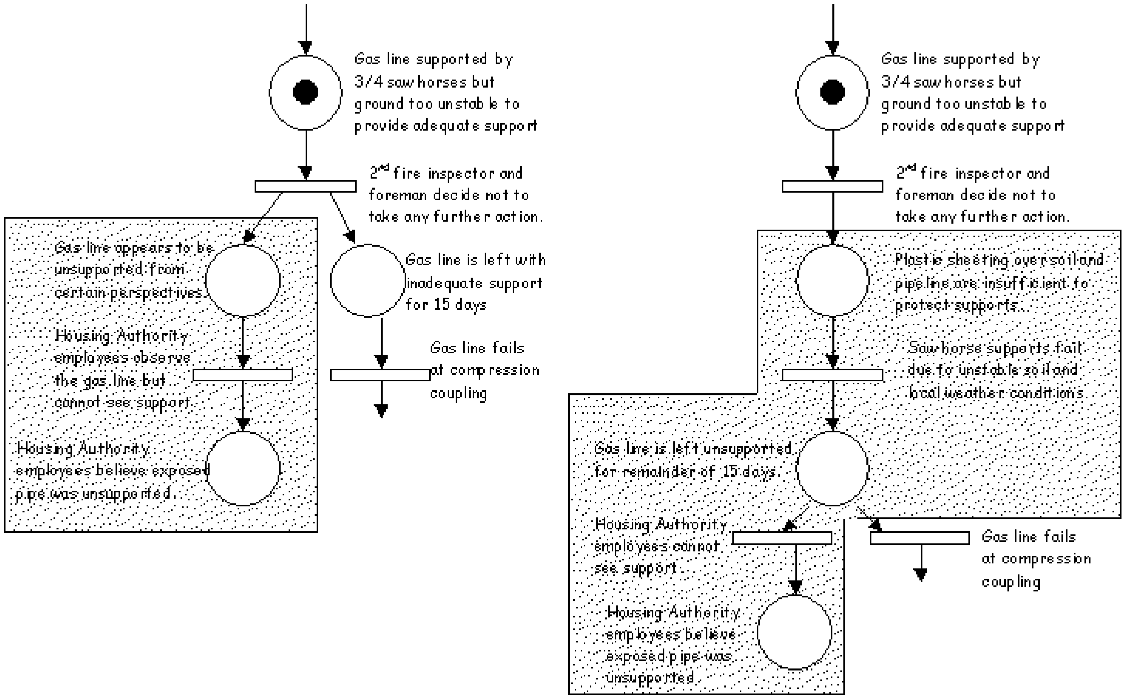


Figure 9.41: Annotating Petri Nets to Resolve Apparent Contradictions

judgement of the investigator must identify a 'probable' version of events. Ideally, such a resolution must also account for any apparent contradiction. If this is not done then individual investigators will construct radically different interpretations of the course of an incident. For instance, the NTSB report documents the Housing Authority employees' observations without attempting to resolve the apparent contradiction. As a result, it is impossible for readers to accurately assess whether or not a cursory visual inspection of the site should have identified the need for further support. In our example, some people will choose to follow the first account shown on the left of Figure 9.41. Others will choose to believe the alternative version of events shown on the right.

It is often impossible to entirely avoid ambiguity and inconsistency within an incident report. Many failures have complex organisational and managerial causes. These cannot easily be associated with discrete events that can be logged or recorded using automated equipment. Even when these devices are available, they often fail to provide unambiguous evidence. For example, many modern devices cannot record data at the same rate at which it is used by application processes [223]. Similarly, Chapter 4.3 has shown that the information provided by many of these recorders has been corrupted by reliability problems and design flaws. Even when accurate data is available, there can be genuine disagreement about the interpretation of that evidence. All of these factors make it unlikely that we shall have complete and unambiguous evidence for the events that contribute to major incidents. The key point, therefore, is not that the techniques in this chapter will entirely avoid ambiguity and inconsistency. They can, however, identify and address inconsistency *if investigators believe that it plays a significant role in our understanding of the incident.* In our example, the NTSB investigators did not further investigate the apparent contradiction between the Housing Authority employees and the other witnesses because even if the saw horses had remained in position they still failed to provide sufficient support for the exposed gas line.

Impact

The previous sections in this chapter have shown how a range of textual and graphical notations can be used to map out the events that contribute to safety-critical incidents. It has been argued that this form of modelling inevitably involves a process of selection or filtration. Secondary and primary investigations, typically, yield a mass of evidence about the course of an incident. Some of this evidence helps to establish the context in which a failure occurred. Other information provides more significant insights into the root causes of an incident. However, there will also be a mass of circumstantial data that has little apparent significance for the course of events. Investigators must, therefore, select which information is to be propagated into any reconstruction. For instance, the NTSB investigators gathered evidence about the excavation crews shift patterns immediately prior to the Allentown explosion. These were not found to have had any influence on this incident and so the information was not included in the time-lines and other reconstructions that were developed during the subsequent investigation.

The use of Petri Nets, of logic, or of Fault Trees only provides a crude indication of the salience of a particular event. The decision whether or not to include an event does not reflect the more detailed distinctions between root causes, contributory factors and contextual factors that were introduced in Chapter 6.4. This is a significant limitation. For instance, the NTSB summarised the outcome of their incident investigation in the following terms:

> "The National Transportation Safety Board determines that the probable cause of the natural gas explosion and fire at Gross Towers in Allentown, Pennsylvania, was the failure of the management of Environmental Preservation Associates, Inc., to ensure compliance with OSHA's and its own excavation requirements through project oversight. Contributing to the accident was the failure of the workmen from Environmental Preservation Associates, Inc., to notify UGI Utilities, Inc., that the line had been damaged and was unsupported.
>
> Contributing to the severity of the accident was the absence of an excess flow valve or a similar device, which could have rapidly stopped the flow of gas once the service line was ruptured. Also contributing to the severity of the accident was the absence of a gas detector, which could have alerted the fire department and residents promptly when escaping gas entered the building." [589]

Previous sections have not shown how such detailed assessments might be represented amongst the mass of events that we have represented in the previous Fault Trees, time-lines, Petri Nets and logic clauses. Before presenting one means of addressing this limitation, it is first important to clarify what we mean by terms such as 'root cause' or 'contributory factor'. The following list summarises the distinctions introduced in Chapter 6.4 but also introduces the term 'exacerbating factor'. This is identified in the NTSB conclusions and extends any impact analysis to consider events that occur in the immediate aftermath of an incident:

- *Contextual Factor.* Contextual factors are events or conditions that did not directly contribute to an incident.
- *Contributory Factor.* Contributory factors are events or conditions that collectively increase the likelihood of an accident but that individually would not lead to an adverse occurrence.
- *Root Cause.* Root causes capture Lewis' notion of causation established by counterfactual reasoning [491]. If a root cause had not occurred in the singular, particular causes of an incident then the incident would not have occurred.
- *Exacerbating factor.* Exacerbating factors do not contribute to the likelihood of an event but they can act to increase the consequences of an incident.

Figure 9.42 builds on Figure 9.11 to show how some of these distinctions might be represented within the fault tree notation. As can be seen, this embodies some of the NTSB investigators' findings, cited in the previous paragraph. This lack of training in OSHA excavation requirements is identified as a root cause for the incident. The fact that UGI were not informed that the line was uncovered is represented as a contributory factor.

Figure 9.42 again reflects the way in which simple syntactic extensions can be used to extend what can be represented in a modelling notation. However, it should be noted that we have only

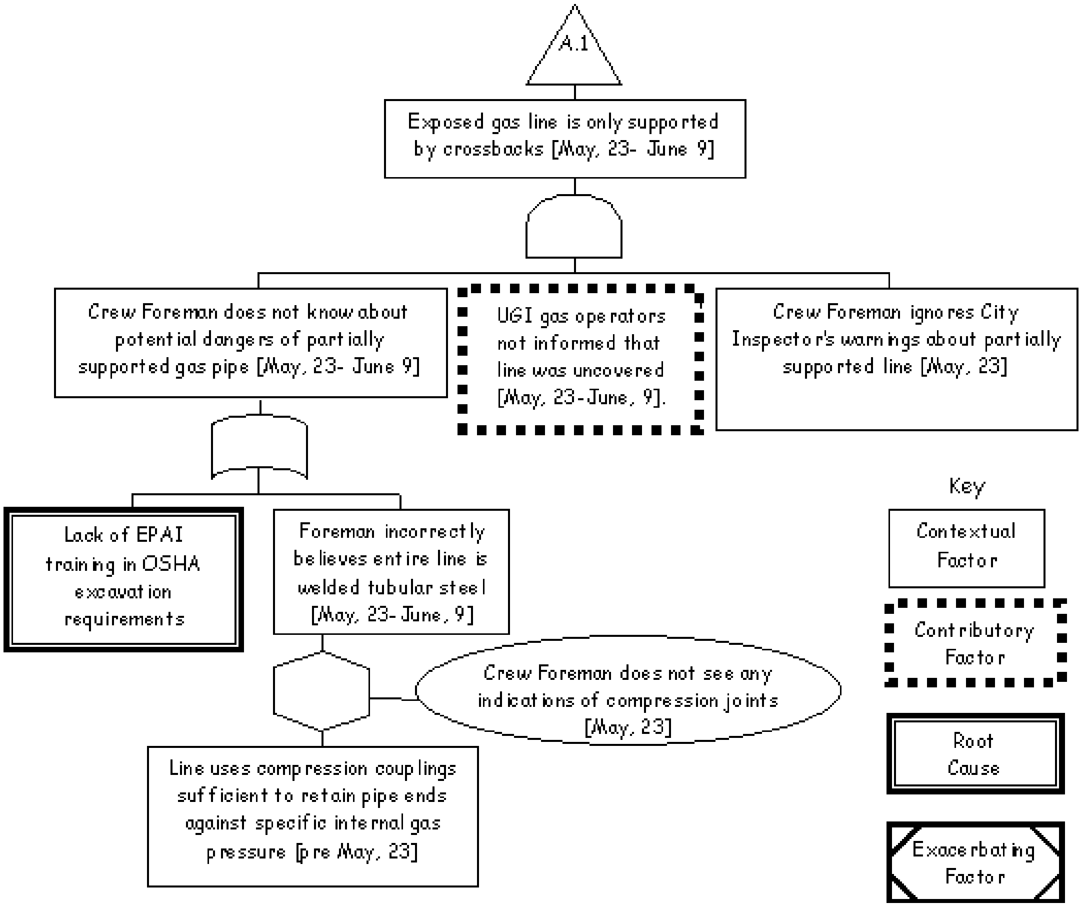

A.1
Exposed gas line is only supported by crossbacks [May, 23- June 9]
Crew Foreman does not know about potential dangers of partially supported gas pipe [May, 23- June 9]
UGI gas operators not informed that line was uncovered [May, 23-June, 9].
Crew Foreman ignores City Inspector's warnings about partially supported line [May, 23]
Lack of EPAI training in OSHA excavation requirements
Foreman incorrectly believes entire line is welded tubular steel [May, 23- June, 9]
Crew Foreman does not see any indications of compression joints [May, 23]
Line uses compression couplings sufficient to retain pipe ends against specific internal gas pressure [pre May, 23]
Key
Contextual Factor
Contributory Factor
Root Cause
Exacerbating Factor

Figure 9.42: Representing the Criticality of Distal Causes

provided an informal semantics for the different impact assessments that are represented in this picture. Similarly, we have not provided any grammatical rules that can be used to determine whether or not Figure 9.42 is well formed. For example, it might be argued that if a root cause is identified in a child event then that criticality should be propagated up the fault tree. By this argument, the intermediate event labelled Crew Foreman does not know about potential dangers of partially supported gas pipe should be denoted as a root cause that is inherited from the basic event labelled Lack of EPAI training in OSHA excavation requirements. We have chosen not to do this in order to keep Figure 9.42 as simple as possible. The ad hoc nature of these extensions re-iterates the point that we have used fault trees in a semi-formal manner. It would, of course, be possible to introduce mathematically defined rules to govern the representation of criticality within a fault tree. We have chosen not to do this. This decision is justified partly, as mentioned above, for the sake of simplicity. This decision is also justified by the relative lack of information that we have about the nature of criticality in incident investigations. We shall return to this theme in the next chapter. For now it is sufficient to observe that, in practice, it can be far harder to distinguish between root causes and contributory factors than might, at first, appear from Lewis' counterfactual definition.

Figure 9.42 is interesting for a number of reasons. Not only does it illustrate that impact or criticality assessments can be introduces as syntactic extensions to a semi-formal modelling notation, it also provides some insights into the Allentown incident. As can be seen, both the root cause and the contributory factor are identified as distal factors. In other words, they relate to events that occurred well before the gas leak or the explosion. In this respect, the NTSB investigators provide a good example of the 'systems' approach to incident investigation. They go beyond the immediate failures of individual staff to look at the longer term causes of the incident. This analysis can also be explained in terms of Mackie's ideas on particular and general causation. When attempting to assess criticality, there is a tendency for investigators to consider the general causes of an incident. In other words, the most significant or critical failures tend to be those that might threaten the safety of other applications rather than the particular failures associated with the incident under consideration.

The previous diagrams in this section have shown how impact assessments can be introduced into fault tree models. By denoting particular nodes as contributory factors or root causes, we have begun to indicate those events that might jeopardise the safety of future systems. It is important to emphasise that this involves a subjective classification. It reflects investigators' view of the relative criticality of key events during the course of an accident. However, it is important not to underestimate the importance of diagrams such as Figure 9.42. Too often these assessments are left as implicit judgements during the investigation process [427].

Figure 9.43 builds on the previous analysis by presenting an impact analysis of the proximal events that led to the Allentown incident. This diagram is based on the Fault Tree that was introduced in Figure 9.10. There are, however, two additions. The impact analysis was guided by the NTSB's findings, quoted above. As a result two additional events were incorporated into Figure 9.43. The first is labelled Excess flow valve not installed in Gross Towers. The second is labelled Gas detector capable of warning UGI was not installed in Gross Towers. These were identified as contributory factors by the NTSB but were not introduced into our model of the proximal events leading to the Allentown incident. This omission is very revealing. It emphasizes the way in which our initial model, represented by the Fault Tree in Figure 9.43, was initially constructed around those events that we knew to have taken place immediately before the explosion. The impact analysis, denoted by the fault tree in Figure 9.43, forced us to consider the way in which those events were affected by omissions or actions that did not take place. Several authors have noted that our bias in Figure 9.10 is symptomatic of a more general tendency to consider errors of commission rather than errors of omission [365].

Further biases affect the modelling and analysis of safety-critical incidents. We have already argued that there is a tendency to focus on contributory factors or root causes rather than the mitigating factors that help to reduce the consequences of an incident. This point can be illustrated by Figure 9.44, which is the same as Figure 9.13. The NTSB investigators focussed their analysis on the root causes and contributory factors that led to the incident. They did not devote the same amount of attention to the mitigating factors that contributed to the effective response after the Allentown explosion. In Mackie's terms, the investigation focuses on the general causes of failure. The investigators identified the particular events that occurred after this incident. In consequence, it can be difficult to identify the wider lessons that might be drawn from the successful response. This is worrying. Perrow and Sagan point to the difficulties of predicting future failures. We often fail to identify the general causes of particular incidents until a large number of similar failures have occurred. We might, therefore, learn more by studying an effective response than by trying to derive the general form of a particular failure.

This chapter has argued that primary and secondary investigations gather evidence about the events that are contribute to major failures. This evidence is then filtered to identify the key events that must be represented in any incident reconstruction. These models can then be used to distinguish root causes from other contributory and contextual factors. It is important to stress, however, that this only represents the first stage of analysis in any incident investigation. Previous paragraphs have re-iterated the problems that arise when attempting to derive general conclusions from the specific events that characterise a particular failure. It is, therefore, important that investigators can examine the products of such a generalisation to determine whether the wider conclusions accurately reflect their interpretation of the salient events that took place during an incident. Figure 9.45 represents one means of achieving this. The same fault tree notation is used to map out the conclusions of the NTSB report into the Allentown incident. As can be seen, this diagram avoids the timing information that was important in reconstructing the event-based models. Similarly, it omits some of the incidents that were considered to be significant in explaining the course of the Allentown incident but which are unlikely to recur in future failures. The detailed communications between the

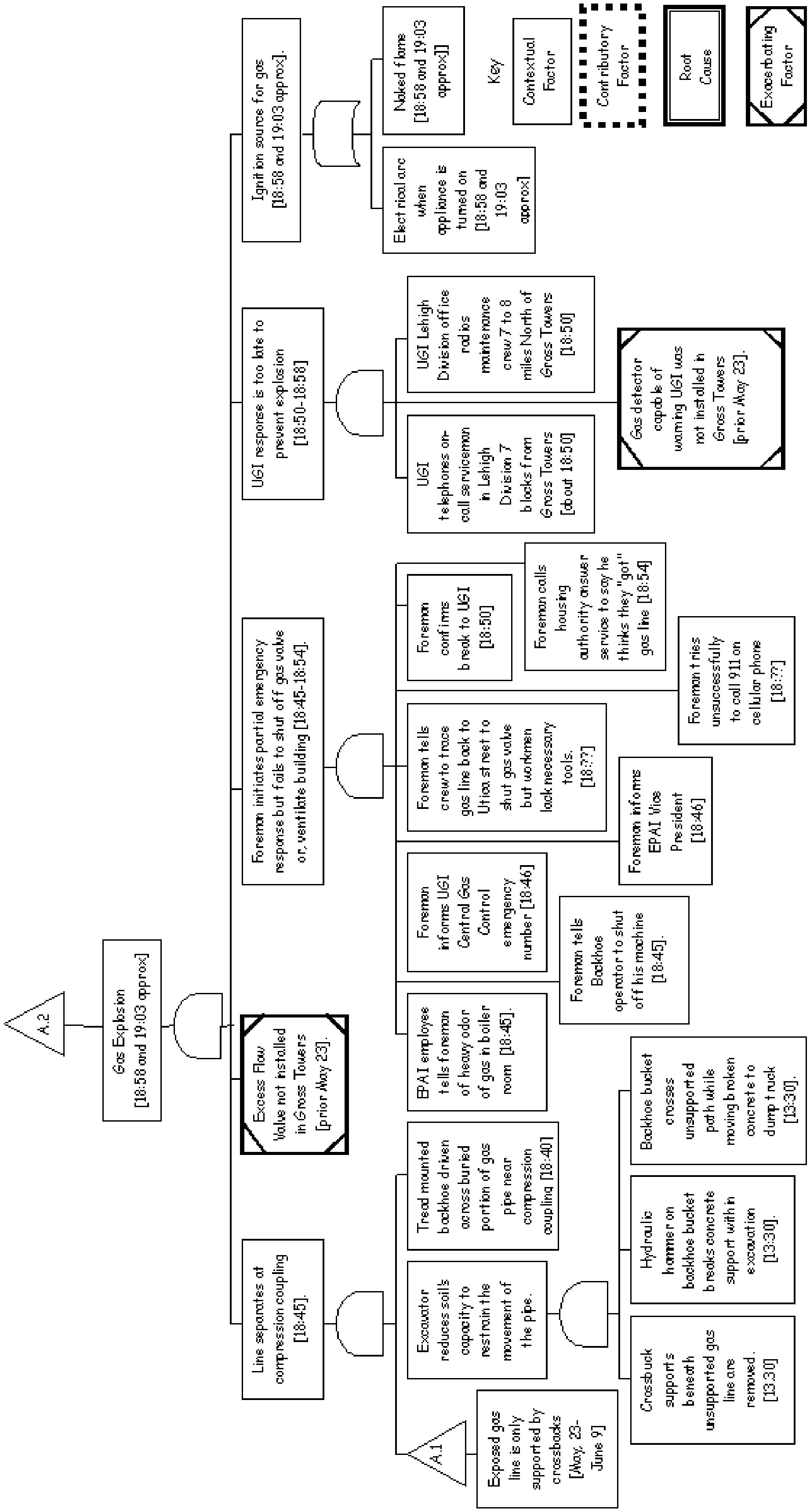

A.2
Gas Explosion [18:58 and 19:03 approx]
Line separates at compression coupling [18:45].
Excess Flow Valve not installed in Gross Towers [prior May 23].
Foreman initiates partial emergency response but fails to shut off gas valve or, ventilate building [18:45-18:54].
UGI response is too late to prevent explosion [18:50-18:58]
Ignition source for gas [18:58 and 19:03 approx].
A.1
Exposed gas line is only supported by crossbacks [May, 23- June 9]
Excavator reduces soils capacity to restrain the movement of the pipe.
Tread mounted backhoe driven across buried portion of gas pipe near compression coupling [18:40]
Crossbuck supports beneath unsupported gas line are removed. [13:30]
Hydraulic hammer on backhoe bucket breaks concrete support within excavation [13:30].
Backhoe bucket crosses unsupported path while moving broken concrete to dump truck [13:30].
EPAI employee tells foreman of heavy odor of gas in boiler room [18:45].
Foreman tells Backhoe operator to shut off his machine [18:45].
Foreman informs UGI Central Gas Control emergency number [18:46]
Foreman informs EPAI Vice President [18:46]
Foreman tells crew to trace gas line back to Utica street to shut gas valve but workmen lack necessary tools. [18:??]
Foreman tries unsuccessfully to call 911 on cellular phone [18:??]
Foreman confirms break to UGI [18:50]
Foreman calls housing authority answer service to say he thinks they "got" gas line [18:54]
UGI telephones on-call serviceman in Lehigh Division 7 blocks from Gross Towers [about 18:50]
UGI Lehigh Division office radios maintenance crew 7 to 8 miles North of Gross Towers [18:50]
Gas detector capable of warning UGI was not installed in Gross Towers [prior May 23].
Electrical arc when appliance is turned on [18:58 and 19:03 approx]
Naked flame [18:58 and 19:03 approx]]
Key
Contextual Factor
Contributory Factor
Root Cause
Exacerbating Factor

Figure 9.43: Representing the Impact of Proximal Causes

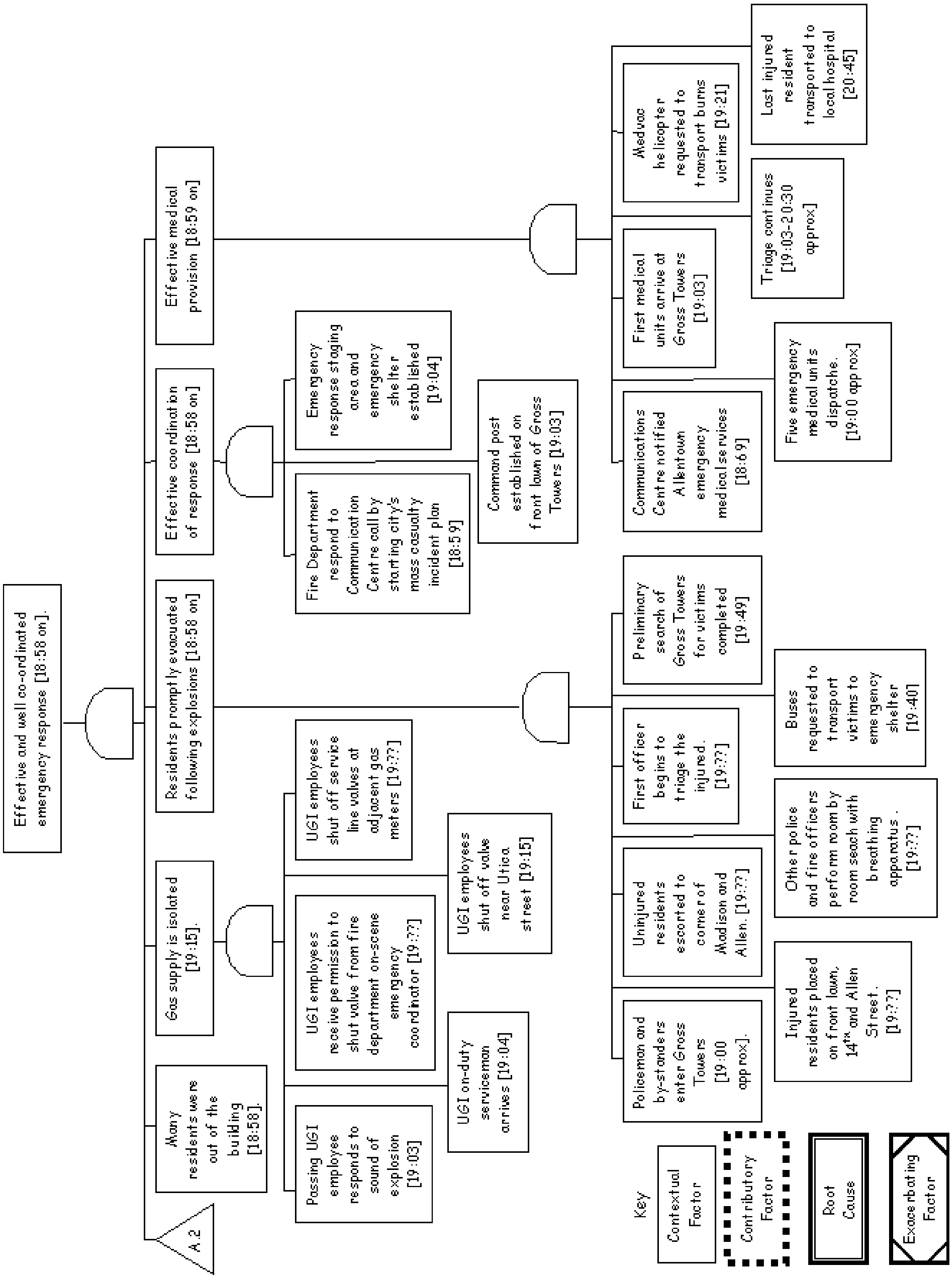

Effective and well co-ordinated emergency response [18:58 on].
A.2
Many residents were out of the building [18:58].
Gas supply is isolated [19:15].
Residents promptly evacuated following explosions [18:58 on]
Effective coordination of response [18:58 on]
Effective medical provision [18:59 on]
Passing UGI employee responds to sound of explosion [19:03]
UGI on-duty serviceman arrives [19:04]
UGI employees receive permission to shut valve from fire department on-scene emergency coordinator [19:??]
UGI employees shut off valve near Utica street [19:15]
UGI employees shut off service line valves at adjacent gas meters [19:??]
Fire Department respond to Communication Centre call by starting city's mass casualty incident plan [18:59]
Command post established on front lawn of Gross Towers [19:03]
Emergency response staging area and emergency shelter established [19:04]
Policeman and by-standers enter Gross Towers [19:00 approx].
Injured residents placed on front lawn, 14th and Allen Street. [19:??]
Uninjured residents escorted to corner of Madison and Allen. [19:??]
Other police and fire officers perform room by room seach with breathing apparatus. [19:??]
First officer begins to triage the injured. [19:??]
Buses requested to transport victims to emergency shelter [19:40]
Preliminary search of Gross Towers for victims completed [19:49]
Communications Centre notified Allentown emergency medical services [18:69]
Five emergency medical units dispatche. [19:00 approx]
First medical units arrive at Gross Towers [19:03]
Triage continues [19:03-20:30 approx]
Medvac helicopter requested to transport burns victims [19:21]
Last injured resident transported to local hospital [20:45]
Key
Contextual Factor
Contributory Factor
Root Cause
Exacerbating Factor

Figure 9.44: Representing the Impact of Mitigating Factors

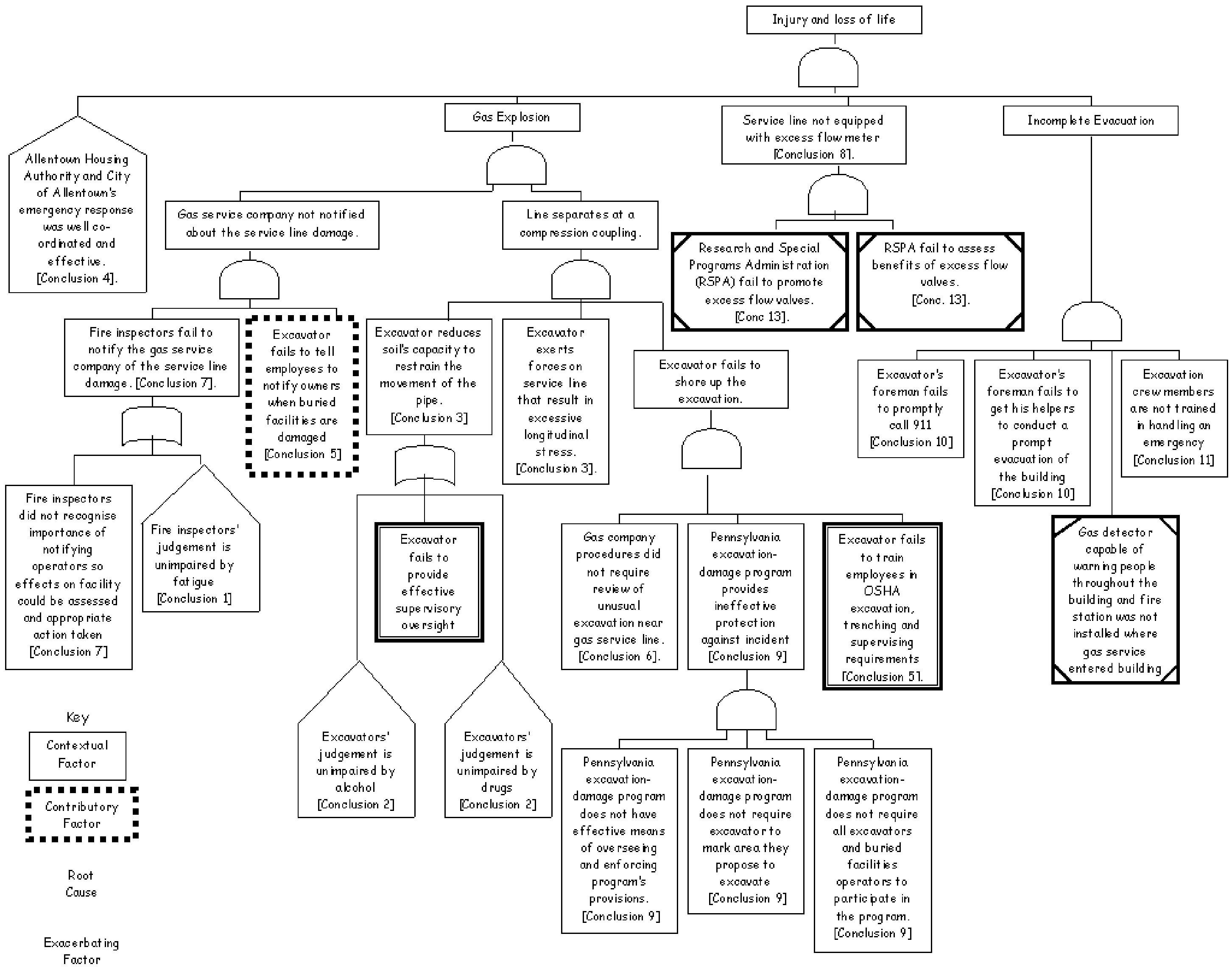

Injury and loss of life
Gas Explosion
Service line not equipped with excess flow meter [Conclusion 8].
Incomplete Evacuation
Allentown Housing Authority and City of Allentown's emergency response was well co-ordinated and effective. [Conclusion 4].
Gas service company not notified about the service line damage.
Line separates at a compression coupling.
Research and Special Programs Administration (RSPA) fail to promote excess flow valves. [Conc 13].
RSPA fail to assess benefits of excess flow valves. [Conc. 13].
Fire inspectors fail to notify the gas service company of the service line damage. [Conclusion 7].
Excavator fails to tell employees to notify owners when buried facilities are damaged [Conclusion 5]
Excavator reduces soil's capacity to restrain the movement of the pipe. [Conclusion 3]
Excavator exerts forces on service line that result in excessive longitudinal stress. [Conclusion 3].
Excavator fails to shore up the excavation.
Excavator's foreman fails to promptly call 911 [Conclusion 10]
Excavator's foreman fails to get his helpers to conduct a prompt evacuation of the building [Conclusion 10]
Excavation crew members are not trained in handling an emergency [Conclusion 11]
Fire inspectors did not recognise importance of notifying operators so effects on facility could be assessed and appropriate action taken [Conclusion 7]
Fire inspectors' judgement is unimpaired by fatigue [Conclusion 1]
Excavator fails to provide effective supervisory oversight
Gas company procedures did not require review of unusual excavation near gas service line. [Conclusion 6].
Pennsylvania excavation-damage program provides ineffective protection against incident [Conclusion 9]
Excavator fails to train employees in OSHA excavation, trenching and supervising requirements [Conclusion 5].
Gas detector capable of warning people throughout the building and fire station was not installed where gas service entered building
Excavators' judgement is unimpaired by alcohol [Conclusion 2]
Excavators' judgement is unimpaired by drugs [Conclusion 2]
Pennsylvania excavation-damage program does not have effective means of overseeing and enforcing program's provisions. [Conclusion 9]
Pennsylvania excavation-damage program does not require excavator to mark area they propose to excavate [Conclusion 9]
Pennsylvania excavation-damage program does not require all excavators and buried facilities operators to participate in the program. [Conclusion 9]
Key
Contextual Factor
Contributory Factor
Root Cause
Exacerbating Factor

Figure 9.45: Representing Impact in a Causal Analysis

Fire Service coordinator and the UGI employees is an example of such a particular event. Although this Fault Tree captures the more general conclusions about this incident, it is still possible to distinguish those findings that relate to the root cause from those that relate to contributory factors and findings that relate to the contextual factors from those that relate to exacerbating/mitigating factors. This illustrates how the same graphical notation can be adapted to support the transition between incident modelling, which was the focus of this chapter, and causal analysis, which is the focus of the next chapter.

9.3 Summary

This chapter has introduced a number of modelling notations, which can be used to reconstruct the events that lead to safety-related incidents. These languages help to strip out the clutter of contextual information that threatens to obscure important information about adverse occurrences. They can chart proximal and distal failures so that investigators can establish both the immediate and longer term events that contribute to an incident. They provide an overview of the interaction between human, technical and organisational failures. This is important because this diverse range of events cannot easily be represented within many of the simulation environments introduced in Chapter 7.3. Reasoning and proof techniques can also be used to check for the consistency and completeness of the resulting models. Reconstruction techniques, therefore, help to develop coherent accounts from the diverse evidence that is elicited during primary and secondary investigations. These reconstructions of the events leading to an incident can, in turn, be used to support hypotheses about the causes of incidents and accidents.

We have focussed on reconstructing events that contribute to an incident. It is important, however, to represent both the commission of undesirable events as well as the omission of necessary actions. The dual nature of any reconstruction has not been stressed enough in the preceding discussion. This is partly due to the nature of the Allentown incident. The NTSB team focussed on those actions that actively contributed to the explosion. OSHA conducted a separate investigation into those procedures and guidelines that were ignored during the EPAI excavations. This ultimately led to a Citation and Notification Penalty for approximately $54,000. If we had focussed on reconstructing the incident from OSHA's viewpoint then these omissions would have formed a far more significant component of the model. This illustrates another important point. Reconstructions focus on critical events during an adverse occurrence. The exact definition of what does and what does not constitute a 'critical' event is determined by the person building the model. The focus of the NTSB investigation was clearly different from that conducted by OSHA's employees and hence we would expect some important differences between the reconstructions that they might develop. However, if we could develop some common tools and techniques these is the possibility that future investigations might share reconstructions to support these different forms of analysis.

The development of an incident reconstruction is not an end in itself. The utility of any notation is determined by whether or not groups of individuals can use that notation to cooperate on the development of a natural language, accident report. This raises a number of further issues. The first set of problems relate to the difficulty of constructing coherent temporal models for safety-related incidents. It is a non-trivial task to resolve the contradictory timings that often appear in eye-witness evidence and automated logs. It can also be difficult to integrate imprecise temporal information about operator behaviour with the more precise temporal schemas that are available for process components. It is important to stress that the development of coherent temporal models must not force analysts into arbitrary decisions or commitments to timings that are not supported by the available evidence.

It is not simply important that a reconstruction notation is capable of representing the course of events, it is also important that investigators can learn to exploit those capabilities. We have argued that there is often a trade-off between the visual appeal of formal and semi-formal notations and the reasoning power that those notations offer to analysts and investigators. This is significant because formal proof techniques provide a powerful means of identifying the temporal ambiguities that have been criticised in the previous paragraph. Tool support has been identified as one means of improving the 'usability' of notations with a relatively low visual appeal. However, further work is urgently required to determine whether similar tools, that have been developed in other areas of engineering, can be applied to analyse incident reconstructions.

The final set of problems stem from the difficulties of managing cooperative work between heterogenous groups of experts. Rather than focusing on modelling capabilities or visual appeal, these problems relate to aspects of control. For example, what are the consequences of allowing more than one author to simultaneously work on a formal or semi-formal description of an incident? No research has been done into these issues. This is an important omission. Without some understanding of the group processes involved in incident reconstruction, it is unlikely that adequate tool support can be developed. This may explain why many existing systems, such as Fault-Tree editors, often only support specific areas of an investigation. They are frequently restricted to systems or control flow analysis. Few attempts have been made to support human factors investigations or the analysis of managerial decision making.

We have focussed on graphical and textual time-lines, on fault trees and Petri Nets and on temporal extensions to first order logic. It is important to emphasise that these represent a very small subset of the range of notations that are currently being applied to this area. For example, we have cited work into more complex logics that include explicit notions of causation [470] or obligation and permission [118]. Others have used state-based techniques that are amenable to model checking [193]. It is too early to judge which, if any, of these approaches will be accepted by practitioners. However, the increasing complexity of many technological failures makes it highly likely that the incident investigators of the future will have to exploit more formal techniques for incident reconstruction.