7

Case Studies

7.1. INTRODUCTION

The purpose of this chapter is to show that improvements in safety, quality, and productivity are possible by applying some of the ideas and techniques described in this book. The fact that error reduction approaches have not yet been widely adopted in the CPI, together with questions of confidentiality, has meant that it has not been possible to provide examples of all the techniques described in the book. However, the examples provided in this chapter illustrate some of the most generally useful qualitative techniques. Case studies of quantitative techniques are provided separately in the quantification section (Chapter 5). The first two case studies illustrate the use of incident analysis techniques (Chapter 6).

The first case study describes the application of the sequentially timed event plotting (STEP) technique to the incident investigation of a hydrocarbon leak accident. Following the analysis of the event sequence using STEP, the critical event causes are then analyzed using the root cause tree.

In the second case study, variation tree analysis and the events and causal factors chart/root cause analysis method are applied to an incident in a resin plant. This case study illustrates the application of retrospective analysis methods to identify the underlying causes of an incident and to prescribe remedial actions. This approach is one of the recommended strategies in the overall error management framework described in Chapter 8.

Case study 3 illustrates the use of proactive techniques to analyze operator tasks, predict errors and develop methods to prevent an error occurring. Methods for the development of operating instructions and checklists are shown using the same chemical plant as in case study 2.

Case study 4 is based on the updating of information displays for refinery furnace control from traditional pneumatic panels to modern VDU-based display systems. In addition to illustrating the need for worker participation in the introduction of new technology, the case study also shows how task

analysis and error analysis techniques (Chapter 4) can be used in human–machine interface design.

Case study 5 provides an example from the offshore oil and gas production industry, and illustrates the fact that in solving a specific practical problem, a practitioner will utilize a wide variety of formal and informal methods. Table 7.1, which describes some of the methods used in the study, includes several techniques discussed in Chapter 4, including interviews, critical incident techniques, walk-throughs and task analysis.

7.2. CASE STUDY 1: INCIDENT ANALYSIS OF HYDROCARBON LEAK FROM PIPE

7.2.1. Introduction

This case study concerns the events leading up to the hydrocarbon explosion which was the starting point for the Piper Alpha offshore disaster. It describes the investigation of the incident using the sequentially timed events plotting (STEP) technique. Based on the STEP work sheet developed, the critical events involved in the incident are identified and analyzed in order to identify their root causes.

The following description is taken from Appendix D of CCPS (1992a). (The results of the public inquiry on the disaster are in Cullen, 1990.)

> An initial explosion occurred on the production deck of the Piper Alpha Offshore Platform in the North Sea at about 1:00 PM on July 6, 1988. The incident escalated into a tragedy that cost the lives of 165 of the 225 persons on the platform. Two additional fatalities occurred on a rescue boat. The Piper Alpha Platform was totally devastated.
>
> Immediately after this blast, a fire originated at the west end of B Module and erupted into a fireball along the west face. The fire spread quickly to neighboring portions of the platform. Approximately 20 minutes later, a major explosion happened due to the rupture of the Tartan gas riser. This occurrence caused a massive and prolonged high pressure jet of flames that generated intense heat. At about 10:50 PM, another immense blast occurred that was believed to be a result of the rupture of the MCP-01 gas riser. Debris from this explosion was projected up to 800 m. away from the platform. Structural deterioration at the level below Module B had begun. This failure was accelerated by a series of additional explosions. One of these eruptions was caused by the fracture of the Claymore gas riser. Eventually, the vast majority of the platform collapsed.

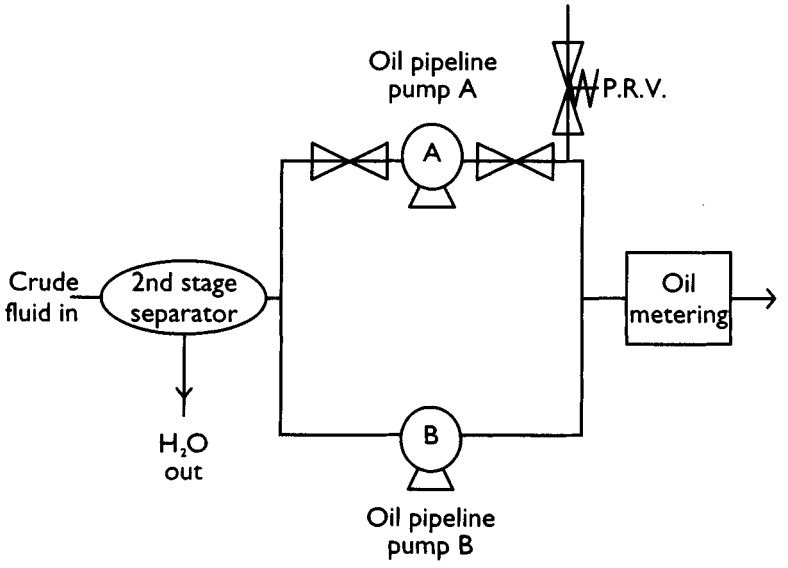

FIGURE 7.1. **Simplified Process Diagram: Hydrocarbon Leak From Pipe (from Cullen, 1990).**

7.2.2. Process Description

The process involved in the incident is concerned with the separation of crude into three phases. The crude is pumped into a two stage separation process where it is divided into three phases; oil, gas, and water. The water is cleaned up and dumped to drain. The remaining mixture of oil and gas is then pumped into the main oil line where it is metered and sent on for further processing. A simplified process diagram is shown in Figure 7.1. The case study described here is centered on a flange leak in one of the oil pipeline pumps (pump A) and its associated pressure relief valve piping.

7.2.3. Events Leading to the Explosion

The separation plant had been running smoothly for several weeks and the planned shutdown was some time away. On the day of the incident a number of unusual events occurred which contributed to its development. Shortly after the start of his day shift, the control room operator received a high vibration alarm from booster pump A in the crude fluid separation building. Following normal procedure, he switched over to the standby pump (pump B), switched off pump A, and told his supervisor of the alarm. The supervisor subsequently organized a work permit for work to be carried out on pump A by the day shift maintenance team. The permit was issued and repair work

started. Since pump A and its associated pipework was off-line, the supervisor took the opportunity to carry out scheduled maintenance on the pressure relief valve (PRV) downstream of pump A. The valve had been malfunctioning, and although the work was not scheduled to be done for some weeks, the specialist contractor team who maintain the PRVs had a team available to carry out the work immediately. The supervisor therefore now had two teams working on the pump A systems: the shift maintenance team working on the pump itself, and a two-man contractor team working on the PRV and its associated pipework. The PRV for pump A is not located immediately adjacent to the pump, and is above floor level, close to a number of other pipe runs. The following description represents a hypothetical sequence of events based on the inquiry findings, but embellished for the purposes of the case study.

During the course of the day, the shift maintenance team identified the cause of the vibration and rectified it. They rebuilt the pump and completed the work at about 17:30, before their shift ended. The permit was returned to the operations supervisor who duly signed it off. The contractor's work, however, did not go as smoothly. The team removed the PRV and the team leader took it to their workshop for maintenance and pressure testing. His partner remained behind in order to fit a blank to the pipeline, as required by site procedure. The contractor fitted the blank to the pipe, although the job was made difficult by its awkward position, and he returned to the workshop to help with the maintenance on the valve itself. Unknown to the workers, the blank had not been fitted correctly and did not seal the pipe. The PRV required a complete strip and overhaul but the contractors were unable to complete the work by the end of the day. They did not inform the operations supervisor, as they thought that the pump had been signed off for more than one day and that they would be able to complete the work the following morning. The day shift supervisor, having had no contact with the contractor team since signing on their permit, made the assumption that the contractors, as they were no longer on the job, would be working overtime to complete the job during the night shift.

At shift handover at 18:00, the incoming operations supervisor was briefed by the day supervisor. The conversation centered on the vibration fault and subsequent repair work carried out. However, no mention was made of the work on the PRV, so consequently none of the incoming shift were aware of it. The night shift supervisor, wanting to return pump A to standby as soon as possible, asked the plant operator to check the status of the pump, and together with the shift electrician, to reset it and put it back on stand-by. The operator, unaware of the work being done on the PRV, did not check this part of the system and, following inspection of the pump, returned it to stand-by.

Later in the night shift the control room operator received a pump trip alarm from pump B. Soon after, the second stage separator high oil level alarm sounded in the control room. The operator, needing to reduce the level,

switched on to the standby pump A. Monitoring the oil level in the separator, the operator saw the level fall. Unknown to the control room operator, switching to pump A resulted in high pressure oil and gas leaking from the incorrectly fitting blank. The control room operator's monitoring of the oil level was interrupted by the gas monitoring system giving an alarm. The operator accepted the alarm but was not unduly worried, thinking it was a false alarm, as often happens after work has been done on a pump. He decided to radio the plant operator and asked him to check it out. The oil level continued to fall in the separator, and the leaking flange continued to release oil and gas into the separation building. The plant operator, responding to the control room operator's request, went to investigate the low level alarm in the separation building. While the control room operator was waiting for the operator to report back, the high gas alarm sounded. He immediately started safety shutdown procedures. It was at this point that the oil and gas mixture ignited and exploded, and the next phase of the Piper Alpha disaster began.

7.2.4. Investigation Using the STEP Technique

A number of stages are used when applying the STEP technique. These will be illustrated with respect to the investigation carried out for the above incident.

The first stage involves documenting the beginning and the end state of the incident. This bounds the scope of the investigation from the first event that deviated from the planned process to the last harmful event in the incident. In this case study, these are the faulty PRV and pump vibration through to the explosion as a result of the ignition of the leaking hydrocarbon mixture. In documenting end states the intention is to identify the main agents (people and things) involved in the incident. This is achieved by recording, measuring, sketching, photographing, and videotaping the incident scene. For example, who were the last people present? What were they doing? Where were they? What plant was involved? Was it in operation? The start state indicates the state of the agents at the beginning of the incident, which shift personnel were on-site, the plant status, and how it was being run. Drawings, procedures, records, and personnel are the typical sources of such information.

The STEP work sheet shown in Figure 7.2 is developed during the analysis. It will obviously be simple and patchy at first, but serves as an important aid in guiding and structuring the data collection and representation. It is important to use a form of work sheet which is easy to construct and modify. Flip charts and add-on stickers are an ideal basis for the work sheet, and are also easy to change. The agents are placed on the vertical axis of the work sheet. This is the start state, the point at which the first deviation in the planned process which led to the incident is identified. In this incident this was found to be the vibrating pump A. The horizontal axis represents the time line on which events are fixed for each agent. The aim is to trace each agent's actions

from the start state to the end state This will picture the effect of each agent in the incident, the effect it had on other agents, and what influenced the agents. This can lead to new agents being considered which were not initially identified as being involved in the incident.

Taking the process control system (PCS) as an agent, for example, it can be identified as an agent at the start and end state of the incident. This provides objective information about the plant before, during, and after the event, and allows fixed time points on the work sheet to be established. Figure 7.5 contains the information available from the printout of the PCS alarm recorder. This locates a number of events for the PCS agent along the time-line, for example, when the vibrations in pump A were detected, when pump B was activated, and when the high oil level alarm was activated. This means that concrete data are available on events relating to the PCS from the start of the incident to its end. Similar data were also available for the gas monitoring system which indicate when both low and high alarms were activated.

A similar process was carried out for each of the agents identified. For agents that are people, however, the process can present problems. For example, in this case study the time period for the development of the incident crossed a shift boundary, another fixed point on the work sheet, and therefore involved different people. Each of these needs to be interviewed to establish their role in the incident. It is important to focus on the events involving the agents and to avoid introducing bias into the work sheet. In this case it was possible to use objective data to validate interview data. The PCS data confirms actions and indicates initiation times for the action taken by the control room operators on both the day and night shift. The interview data used to develop the STEP work sheet for this incident are contained in Figure 7.3 (note that these are hypothetical interview data generated for this case study). Data from the PCS gas monitoring systems was used to verify and help locate data gathered from interviews. Particular focus was paid to agent's actions which initiate changes in the other agents. For example, the control room's request for the plant operator to check out the low gas alarm, or the high oil level alarm leading to the control room operator switching to pump A and directing his attention to monitoring the oil level.

The logic tests for placing building blocks on the STEP diagram help to determine whether all the events for an agent were listed, and whether the relevant building block was placed correctly on the time sheet relative to that and other events. It is here that one of the strengths of the work sheet became apparent. Using the events for each agent and the simple logic tests quickly identified gaps in the analyst's knowledge. These gaps were further defined once the event elements were linked.

As the diagram develops, a necessary and sufficient test is applied to event pairs. For example, the event involving the night shift controller switching from pump B to pump A and the tripping of pump B are necessary for the

event, but not sufficient to cause this event. The process control system gave the high oil level alarm which reduced the time window for the operator to take other action, for example, investigating the cause of the trip. However, other events were also necessary. These were the confirmations by the plant operator and electrician that pump A had been placed back on standby. If this had not happened the option to switch to pump A would not have been available. The necessary and sufficient test led to both converging arrow links, as above, and also diverging links, for example where the gas/oil leaking from the flange leads to both high and high high gas alarms and is necessary for the ignition of the leak. In this way, the relationships among events were elicited and the investigator was forced to think about causal events one at a time instead of considering the incident as a whole. The process of data collection, with its conversion to events, building block positioning and logic testing, was an iterative one and this diagram went though several revisions.

The STEP procedure provides investigators with a well-structured, logical, and independently verifiable representation of the events involved in the incident. This, however, only represents the first stage in the investigation. The second stage was to identify the critical agents and events in the incident process.

7.2.5. Identification of Critical Agents/Events

This stage involved the identification of critical actions and events in the incident process. Three critical events were identified from the STEP diagram. These were

- Failure to fit the blank correctly
- Changeover between day and night supervisor
- Contractor fails to report status of work

It was these events which significantly influenced the course of events by triggering later problems.

7.2.6. Identification of Root Causes

Root causes for each of the critical events were then determined using the root cause tree (see Figure 6.8 and Chapter 6, Section 6.8.4). This six-level decision tree was used which, based on answers to general questions, leads through successive levels of the tree until the root cause is identified or the data limitations prevent further progress. These root causes specify the underlying reason for a given critical event. The analysis profiles for each of the critical events are presented below.

CRITICAL EVENT 1 **Failure to Fit Blank Correctly**	
ROOT CAUSE 1	**ROOT CAUSE 2**
A. Equipment difficulty B. Engineering department C. Corrective maintenance D. Human factors E. Human–machine interface F. Ergonomics poor	D. Immediate supervision E. Supervision during work F. Supervision less than adequate (LTA)

The problem manifested itself as an equipment problem, namely a leaking flange joint. The department broadly responsible for this area (but not for implementing, monitoring, and subsequent recommendations) is the engineering department, as the specialist contractors work for them. The critical event took place during a corrective maintenance operation. From here, two separate root causes were identified, based on the data from the investigation.

- **Root cause 1:** Supervision was less than adequate. The team leader should have stayed with his colleague and checked the work as he had responsibility for the team
- **Root cause 2:** The cramped, confined space available made it difficult to verify that the blank had been correctly fitted

The problem was an operational difficulty concerning the production department. Two root causes were identified based on the investigation.

- **Root cause 1:** Procedures for shift changeover were inconvenient for use. The prescribed changeover procedure was detailed and elaborate, so it was not used in practice, being seen as too inconvenient for practical purposes. Consequently, one important aspect was omitted. Supervisors are supposed to go through the work permit book at each shift changeover. This was not done.

CRITICAL EVENT 2 **Changeover between Day and Night Supervisor**	
ROOT CAUSE 1	**ROOT CAUSE 2**
A. Operations difficulty B. Production C. Not applicable D. Communication E. Shift changeover LTA F. Communication among shifts LTA	A. Operations difficulty B. Production C. Not applicable D. Procedures E. Not used F. Inconvenient for use

- **Root cause 2:** The informal method of shift changeover used on the plant meant that vital information relating to plant status was not communicated across shifts.

CRITICAL EVENT 3 **Contractor Fails to Report Status of Work**		
ROOT CAUSE 1	**ROOT CAUSE 2**	**ROOT CAUSE 3**
A. Operations difficulty	A. Services B. Contractor Maintenance	
D. Immediate supervision	D. Training	D. Procedure Not Use
E. Preparation	?	?
F. Instructions to operators LTA	?	F. Inconvenient

The root causes for this critical event both concern the operations department and the service department who ran the contractor maintenance team. The operations department (i.e., the day shift operations supervisor) failed to provide adequate supervision and instructions to the contractor team. Explanations of the nature of the permit-to-work systems (i.e., the need to report back at end of shift) should have been given, and the possibility and implications of work not being completed before the end of the shift should have been considered by both parties.

On the part of the contractor team, two root causes were identified, root cause 1 being insufficient training of the contractor team leader. He was uncertain of permit systems, specifically whether they should report in at the end of shift, and, if so, who should do it. The second root cause relates to the procedure used at the end of the shift for supervisors to sign back permits. Although according to procedure all workers should hand back permits to supervisors in person, in practice this did not occur. If no one is present, or they are busy, it had become common practice to either leave the permits on the supervisor's desk, or to sign them back in the morning.

7.2.7. Conclusion

The case study has documented the investigation and root cause analysis process applied to the hydrocarbon explosion that initiated the Piper Alpha incident. The case study serves to illustrate the use of the STEP technique, which provides a clear graphical representation of the agents and events involved in the incident process. The case study also demonstrates the identification of the critical events in the sequence which significantly influenced the outcome of the incident. Finally the root causes of these critical events were determined. This allows the analyst to evaluate why they occurred and indicated areas to be addressed in developing effective error reduction strategies.

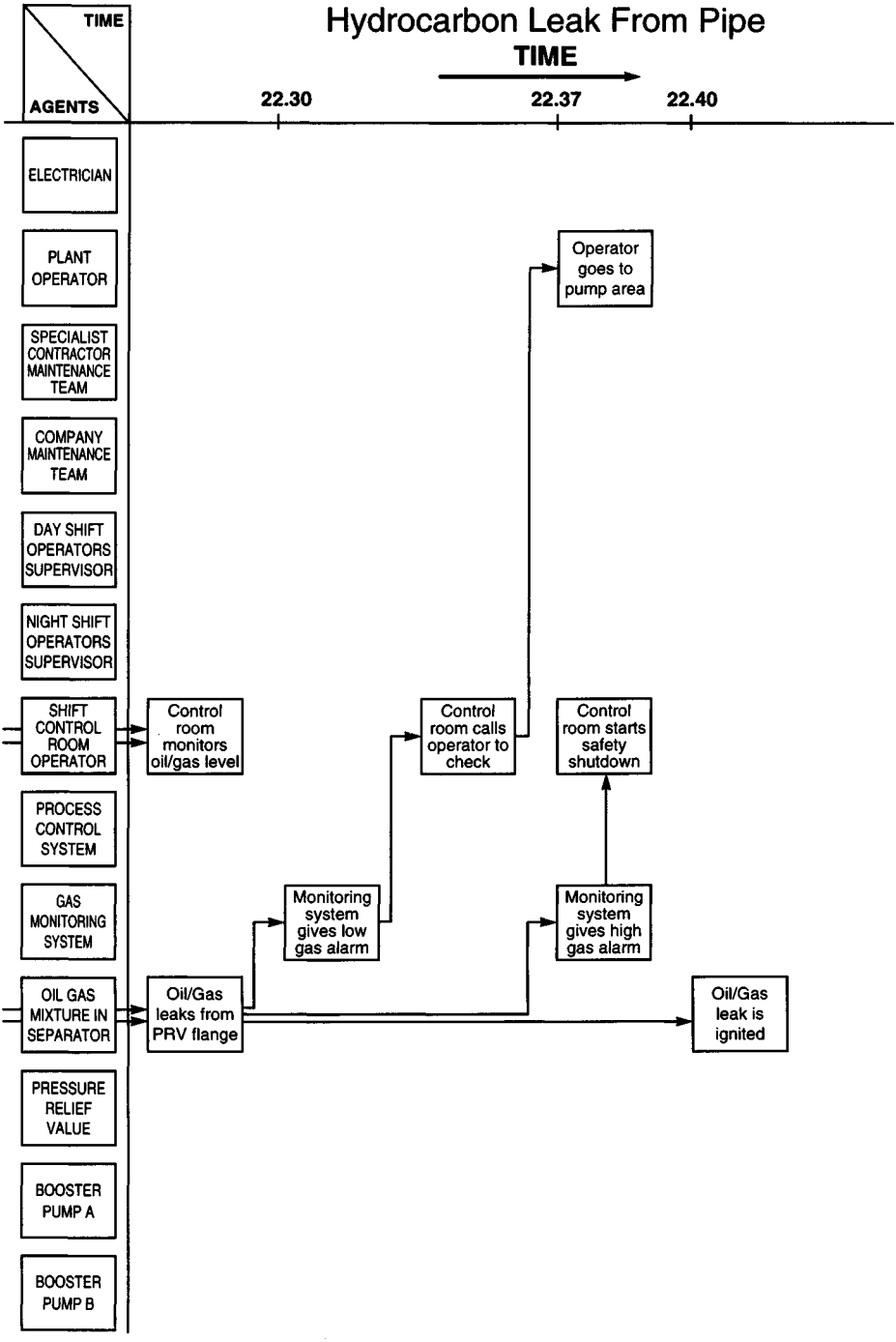

FIGURE 7.2 **STEP Diagram of Hydrocarbon Leak from Pipe, Page 1 of 4.**

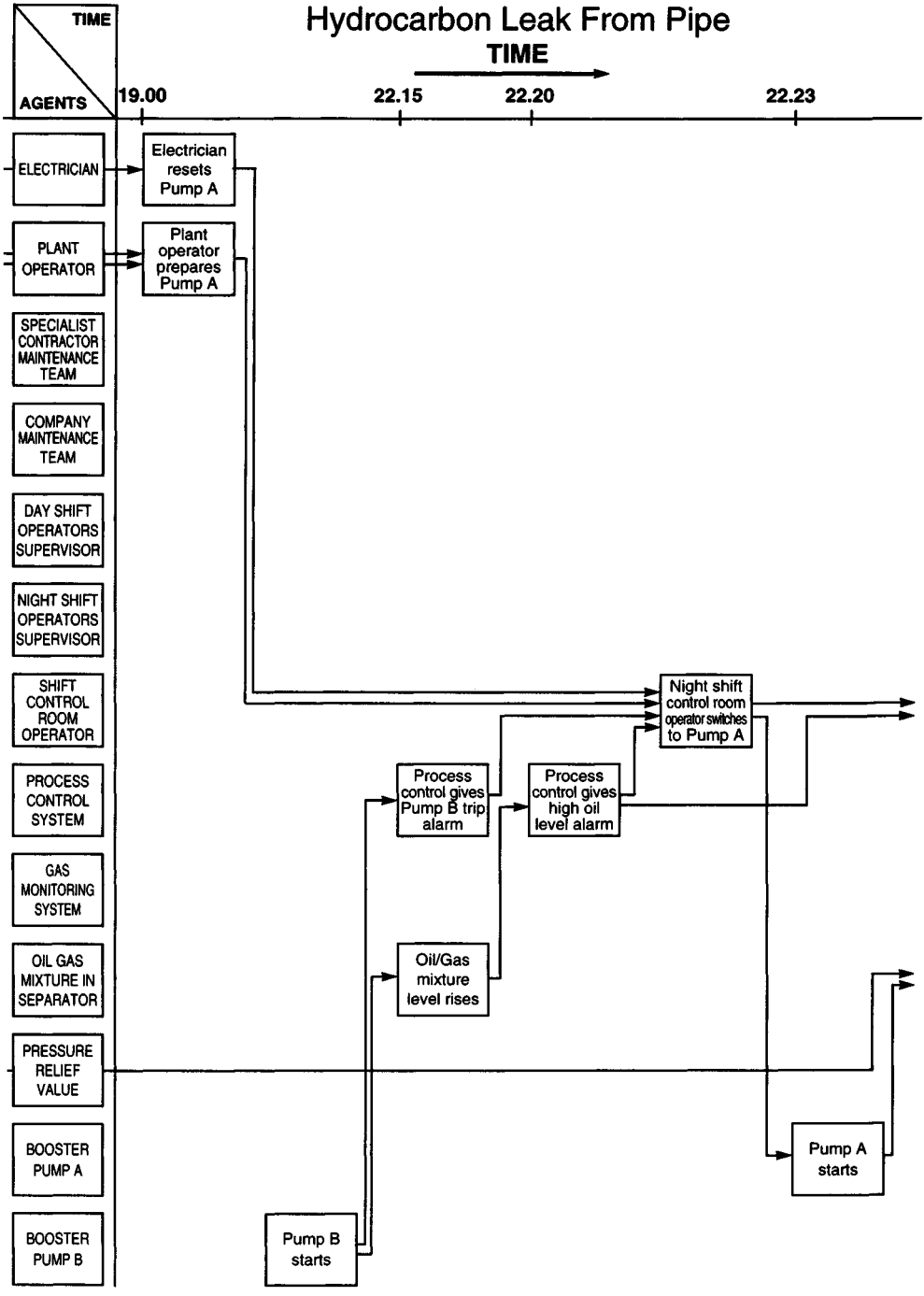

FIGURE 7.2 **STEP Diagram of Hydrocarbon Leak from Pipe, Page 2 of 4.**

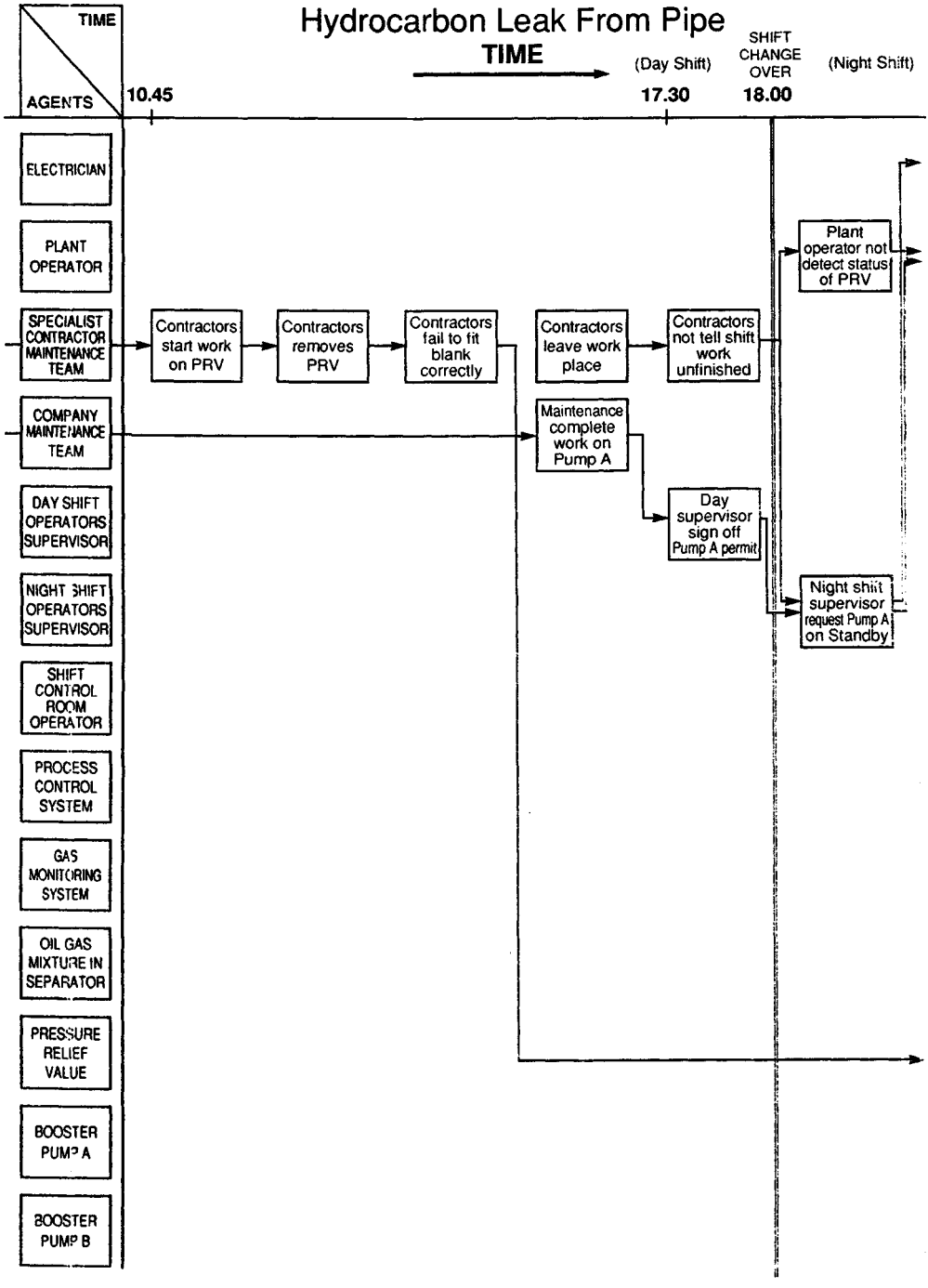

FIGURE 7.2 **STEP Diagram of Hydrocarbon Leak from Pipe, Page 3 of 4.**

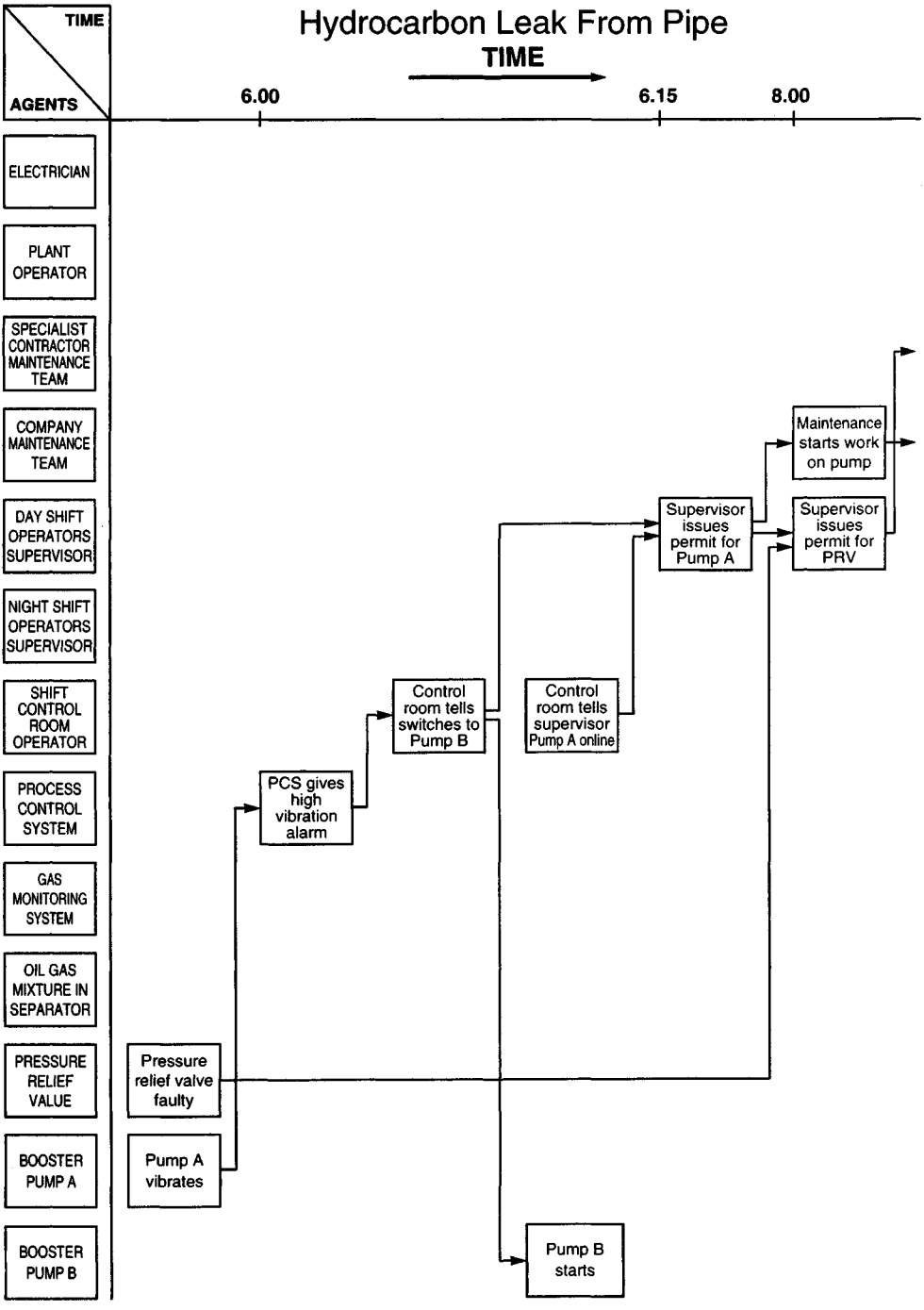

FIGURE 7.2 **STEP Diagram of Hydrocarbon Leak from Pipe, Page 4 of 4.**

Plant Operator (night shift)

1. Location: entering oil separation module.
2. Heard an explosion then thrown out of doorway.
3. Ran to phone and rang emergency services.
4. At start of his shift (18:00) had walked around plant, including oil separation module.
5. Supervisor had requested him to prepare pump A for restart. Operator was unaware pump A had been worked on during day shift.
6. Reported pump ready to control room operator. Unsure of time.
7. During break (approx. 22:30) had been called by control room operator to check separation room as gas alarm had gone off. Operator stated that false alarms are common.

Control Room Operator (night shift)

1. Location: Separation plant control room.
2. Heard explosion which was then followed by control room damage, including windows blowing in.
3. Immediately called emergency services followed by radioing plant operator—no reply. Then supervisor came into the control room and sounded plant alarm.
4. Started shift at 18:00, told by night supervisor pump A had been off-line and was to be brought back on standby.
5. Then received notice from plant operator and electrician that pump A was prepared. Unsure of time, approx. 19:15 for operator, 19:25 for electrician.
6. At about 22:10 received pump trip alarm. He then watched level increase in separators, then high oil level alarm sounded. Operator then switched to pump A and started it up.
7. He then monitored oil/gas level display. The oil level dropped.
8. When high gas alarm went off, he thought it was probably a false alarm, as has happened in the past, especially after work done on pump. Then requested plant operator to investigate.
9. While waiting for reply high high gas alarm went off (approx. 22:35) so he immediately started safety shutdown procedure. Explosion occurred while he was doing this.

FIGURE 7.3. **Statements of Witnesses, Page 1 of 2.**

Supervisor (night shift)

1. Location: Supervisor's office.
2. Heard loud explosion. Ran to control room and found that the windows had been blown in. Supervisor then sounded plant alarm. Then went to separation module and found it severely damaged and on fire.
3. Had come on shift at 18:00 and been briefed by day supervisor. Told pump A had been worked on but had just been signed back on by day supervisor. No mention of other work in separation module.
4. Supervisor had requested pump A to be prepared for standby. Did this by asking plant operator to prepare pump and electrician to reset pump. This request was made at about 19:00.

Supervisor (day shift)

1. Contacted at about 23:15 and told of explosion and fire in separation module.
2. During his day shift control room operator had told him pump A had given high vibration alarm and pump B was now in operation. The opportunity was taken to repair/rectify the pressure relief valve on pump A, while the pump was being repaired
3. After signing the permit for the works maintenance team, and seeing the job start (approx. 8:.00), he had contacted the specialist contractors and arranged for them to attend to the PRV. A permit to work had been prepared and the work started about 10:45. He had gone through the procedure for work with the contractor This included instructions for fitting a blank flange on the pipe.
4. Just prior to the end of the shift the works maintenance team reported that the work on pump A was completed, and he had signed off their permit.
5. The supervisor had no further contact with the contractors and had assumed they would be working overtime (after shift change at 18:00) to complete the job.

Contractor Maintenance Leader (days)

1. Had been contacted by oil separation day supervisor and worked to repair and rectify the PRV on pump A. Work started about 11:00 and then PRV had been removed and taken to the contractors workshop to be stripped.
2. One of the two contractors on the job had remained behind to fit a blank to the PRV pipe work.
3. The valve turned out to require a complete strip and overhaul and was unfinished by the end of the work day.
4. They had not informed the plant about this and assumed that the pump was "signed off" for more than one day.
5. The contractor team only work days and currently have no overtime policy in effect.

FIGURE 7.3. **Statements of Witnesses, Page 2 of 2.**

EXPLOSION IN SEPARATION BUILDING

Conclusions:

1. The explosion occurred just after 22:40 hours.
2. The explosion centered around the area of the separation plant holding pumps A and B.
3. The cause of this fire and explosion was ignition of hydrocarbon mixture.
4. The hydrocarbon leak probably resulted from a blank being incorrectly fitted to pump A PRV pipework and subsequent failure to provide a leak-tight seal.
5. The source of ignition is unknown.

FIGURE 7.4 **Investigating Engineer's Report**

GAS MONITORING SYSTEM:	ALARM REPORTS
00:00:00	
22:30:45	Low level alarm
22:31:30	Alarm accepted
22:37:50	High level alarm
PROCESS CONTROL SYSTEM:	**ALARM REPORTS**
00:00:00	
6:00:15	High vibration alarm: Pump A.
6:15:32	Pump B: activated.
22:15:47	Pump B: trip alarm.
22:20:01	High oil alarm: second stage separator.
22:23:17	Pump A: Activated.
22:37:53	Emergency shutdown sequence activated.

FIGURE 7.5 **Data for Process Data Recording System**

7.3. CASE STUDY 2: INCIDENT INVESTIGATION: MISCHARGING OF SOLVENT IN A BATCH PLANT

7.3.1. Introduction

This case study illustrates how the methodologies described in Chapter 6 can be used to analyze plant incidents and identify the root causes of the problems. Based on this information, specific error reduction strategies can be developed to prevent similar incidents from occurring in the future. Also, the findings of such an analysis can provide the basis for more general discussions about the prevalence of similar error inducing conditions in other plant areas.

The incident under consideration occurred in a batch processing plant in which batches of resins produced in various reactors are discharged into blenders to achieve the required viscosity by the addition of solvents. Solvent is charged into the blender via a valved pipeline which originates at the top floor of the building (see Figure 7.6). From the top floor the allocated worker is responsible for the pumping of solvents to the reactors or blenders via a metered solvent bank and a charging manifold.

The solvent bank consists of a number of metered pumps from the storage tanks which, by using flexible pipes (hoses) and quick fit couplings, the top floor man connects to the required pipeline. These pipelines are arranged in a charging manifold with each being labeled and having a valve adjacent to the coupling (see Figure 7.7).

One day, the lead operator gave verbal and written instructions, via a second worker, to the top floor man to pump solvent to 12A blender. The top floor man actually pumped the solvent to 21A blender, as a result of connecting the hose to the 21A blender pipe and not the 12A blender pipe. Consequently the solvent pumped to 21A blender was charged on top of another batch already in 21A blender. The contaminated batch had to be pumped back into a reactor where the mischarged solvent was removed by the application of vacuum.

Mischarging of solvents and oils was a recurrent problem in the plant and on many occasions batches were irrevocably contaminated because incorrect reactions had taken place. Additional problems were related to the unavailability of reactors due to reprocessing of contaminated batches, resulting in disruption of the process schedules. Management response to this problem had involved a number of actions including stressing the importance of checking communication; the issuing of standard operating procedures; and disciplinary action against the operators involved. The analysis of this incident revealed many error-inducing conditions not hitherto recognized by management.

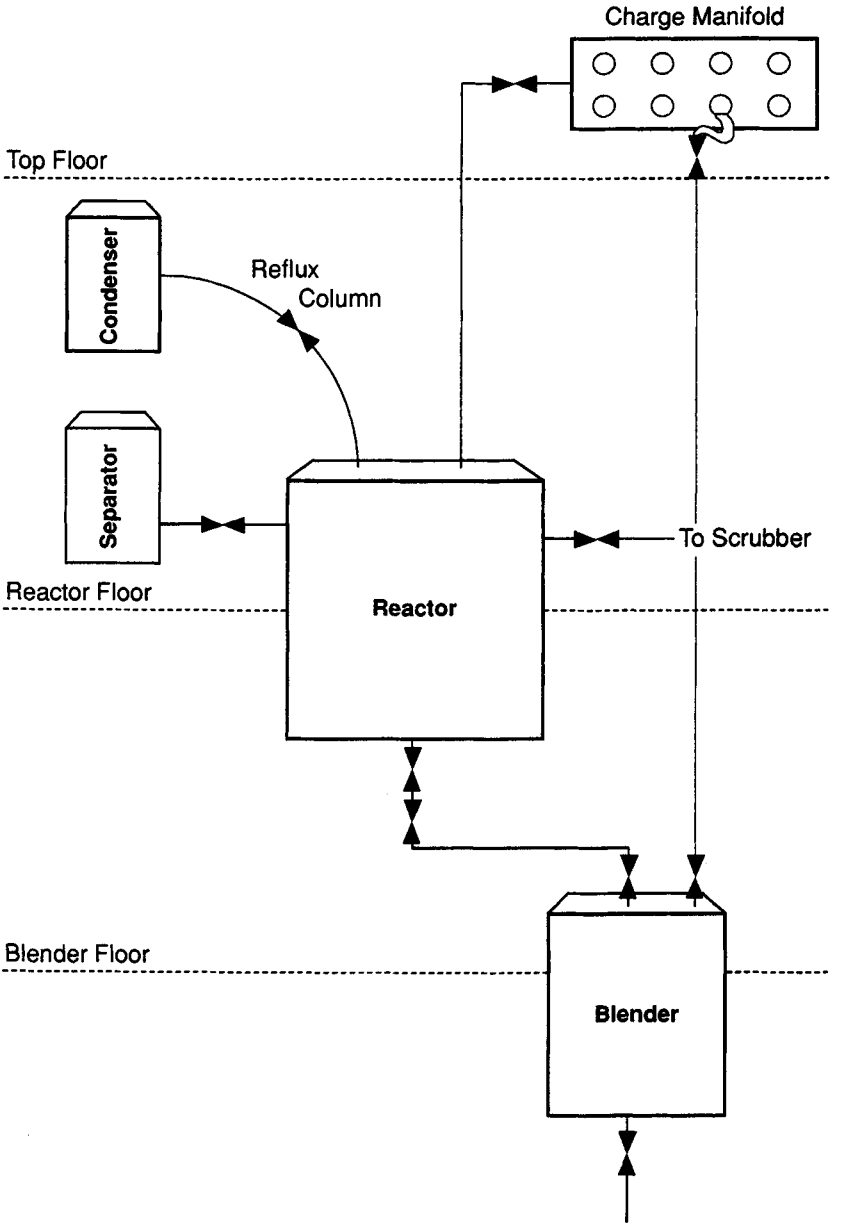

FIGURE 7.6 **Simplified Schematic Plant Diagram.**

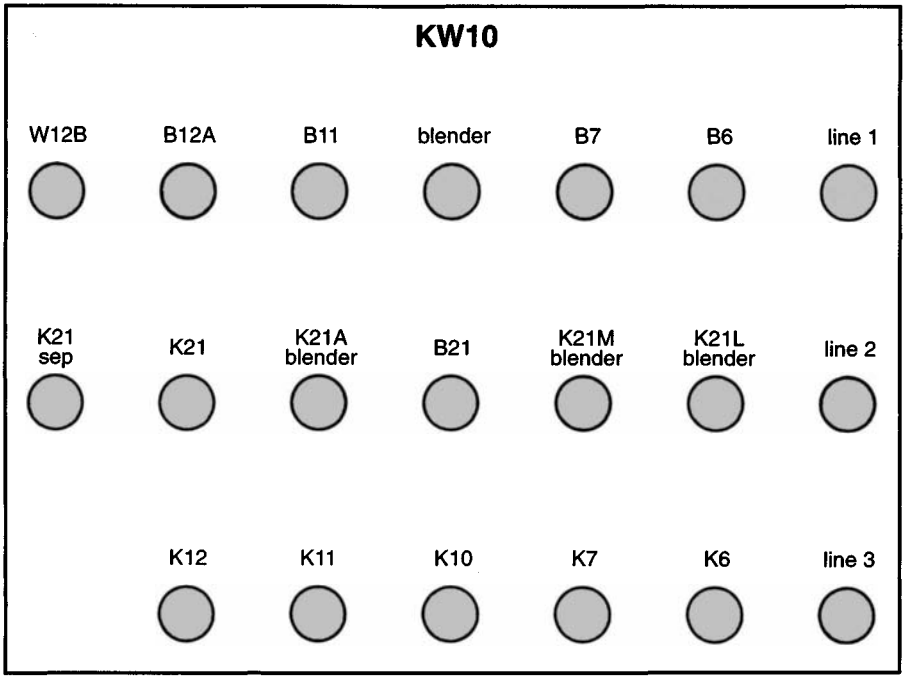

FIGURE 7.7 **Charging Manifold.**

7.3.2. The Application of Accident Investigation Techniques

To gather information about the factors which contributed to the above incident, interviews were held with the workers and their management. Relevant documentation such as standard operating procedures and documentation relating to the incident was also collected. A task analysis (see Case Study 3) of the job of the top floor person was carried out in order to examine the operations involved and the factors which could affect job performance. Two techniques were used for the analysis of this incident, namely variation tree analysis and root cause analysis.

7.3.3. Variation Tree Analysis

The information gathered relating to the incident was used to identify the sequence of causes and consequences which led to the mischarge. From the resulting variation tree (see Figure 7.8) two critical points and their contributory factors can be identified.

First, the selection of the wrong pipeline was influenced by a number of factors such as poor labeling and layout. A "spaghetti" of confusing pipework was already on the charging manifold as a result of a number of concurrent

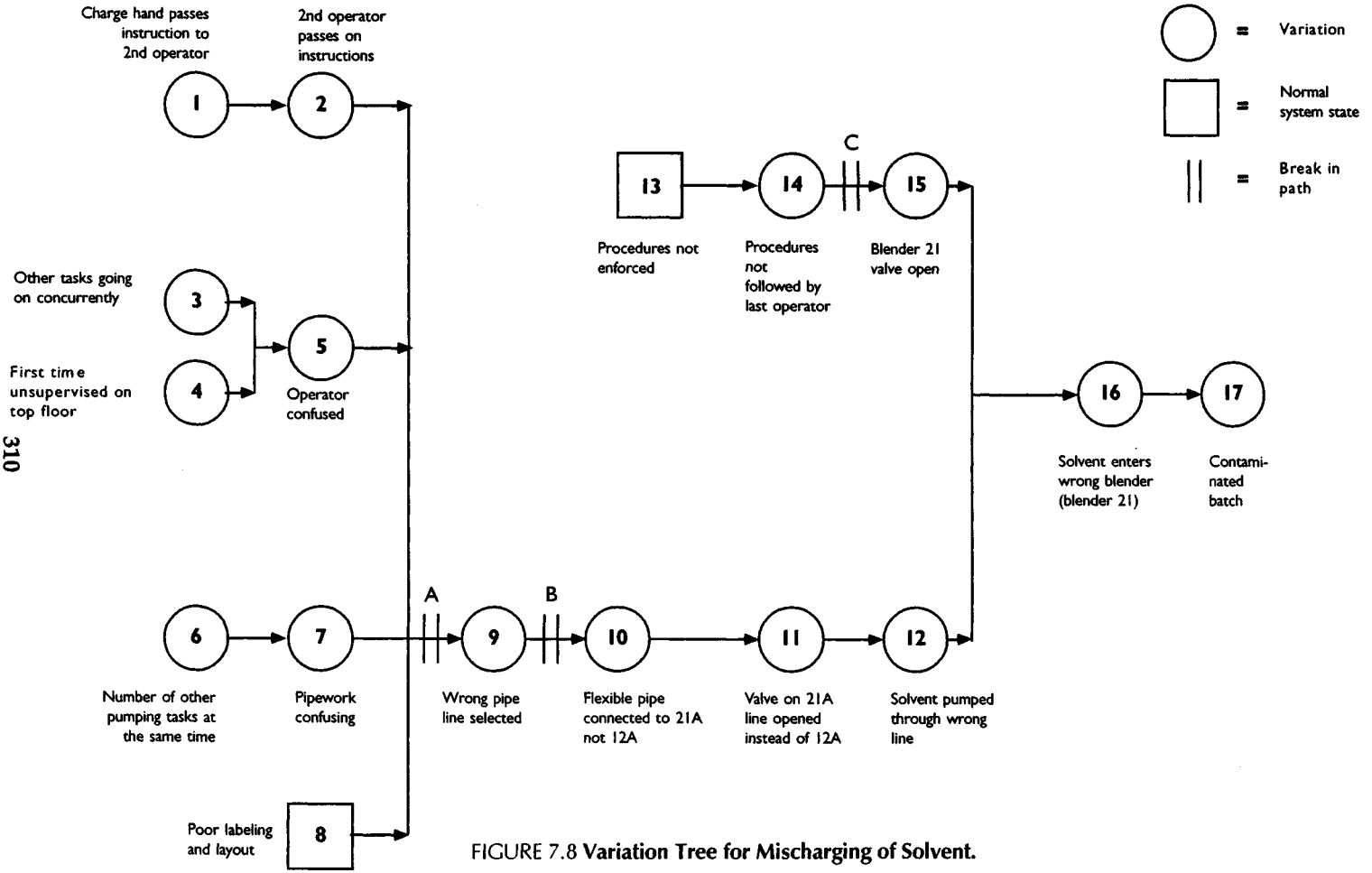

FIGURE 7.8 **Variation Tree for Mischarging of Solvent.**

pumping tasks. Also the worker was confused and possibly stressed due to inadequate training and the number of tasks being carried out at that time. Second, the charging of the solvent into the wrong blender could still have been avoided if the blender valve had been closed, as specified in the procedures. It was found that it was standard practice to leave this valve open in order to save the staff from having to open and close the valves with each charging. Also, there was no feedback to the worker with regard to the status of the valves.

To generate error reduction strategies, the incident sequence can be altered either by **canceling the variations** (the numbered nodes in Figure 7.8) or by **breaking the path** (shown by numbered vertical lines across the path). This is achieved by considering the cognitive processing level of the operation required at each stage, using Rasmussen's stepladder model (see Chapter 2 and Figure 4.11, Chapter 4), and addressing error reduction strategies at the levels which are specified in the model. A selection of possibilities follows.

Canceling the Variations (Nodes)

- **nodes 3, 4, 5, 6** (relate to the training and workload of the operator)
  Changes to remove some of these nodes could include:
  Identification level: too many jobs being done at once; limit work operator undertakes at one time.
  Observation level: some form of queuing system for jobs required.
  Evaluation level: management must outline explicit criteria for running concurrent tasks; train staff not only in normal work situations, but also in heavy work load situations; use valid training methods and provide procedures.
- **node 15**
  Activation level: install alarm system for indicating valve left open.
  Observation level: provide checklist to operators; make valve more accessible or remotely operable.
  Interpretation level: increase staff awareness of the consequences for safety, etc.
  Evaluation level: change operators' criteria for performance—enforce meaningful procedures—address work conditions and social content. Also it is necessary to change management's perception of the need for supervision and the importance of solvent charging. Obviously it is a failure of supervision to be unaware or to tolerate that valves were not reset after use.
  Execution Level: Enhance accessibility of valve or introduce remote operation.
- **nodes 5, 7, and 8** (relate to the design and ergonomic considerations of the situation). Designers need to acknowledge and address human–machine interface issues:

Observation and identification levels: ensure labeling is clear, consistent, and easily distinguished using color-coded pipework; improve work environment (e.g., lighting and general housekeeping).
Evaluation level: create a system, in accordance with ergonomic criteria, that is error tolerant and supports error recovery; redesign charging manifold (see Figure 7.7) using functional grouping corresponding to the actual layout of system.

Breaking the Paths

- At A, develop a method for facilitating selection of correct pipework such as a light system activated by the person giving the instruction, or a key system that requires a key from a specific valve to operate the coupling on the pipeline related to this valve
- At B, develop an alarm system indicating when a wrong connection is made
- At C, change procedures to reflect actual performance, provide checklists, alter worker's perception of the importance and consequences of leaving valves open, and improve the supervision of procedures. Some form of lock system would be of benefit

This selection gives an indication of the variety of error reduction strategies, suggested from a combination of the Variation Diagram and a consideration of the cognitive processes underlying either the worker's performance at a particular stage or those of the design and management of the system.

7.3.4 Root Cause Analysis

The events and causal factors chart for this incident is shown in Figure 7.9. The primary sequence of events is shown horizontally in bold boxes. Secondary events are shown in the other boxes, and conditions are in ovals. From the diagram three causal factors were identified and carried forward to the Root Cause Coding to establish the root causes of the causal factors.

Causal Factor 1: Operator A Connects Pump to 21A Pipe Not 12A Pipe
Root cause coding identified the following root causes:

- **Root cause 1.** Scheduling less than adequate; the excessive number of jobs required of the worker had a detrimental effect on his performance.
- **Root cause 2.** Incomplete training; the incident occurred during the worker's first time alone on the top floor. Training had been given but only in low task demand situations.
- **Root cause 3.** Corrective action not yet implemented; management had been aware of problems with the vessel and solvent banks but had done nothing about it.

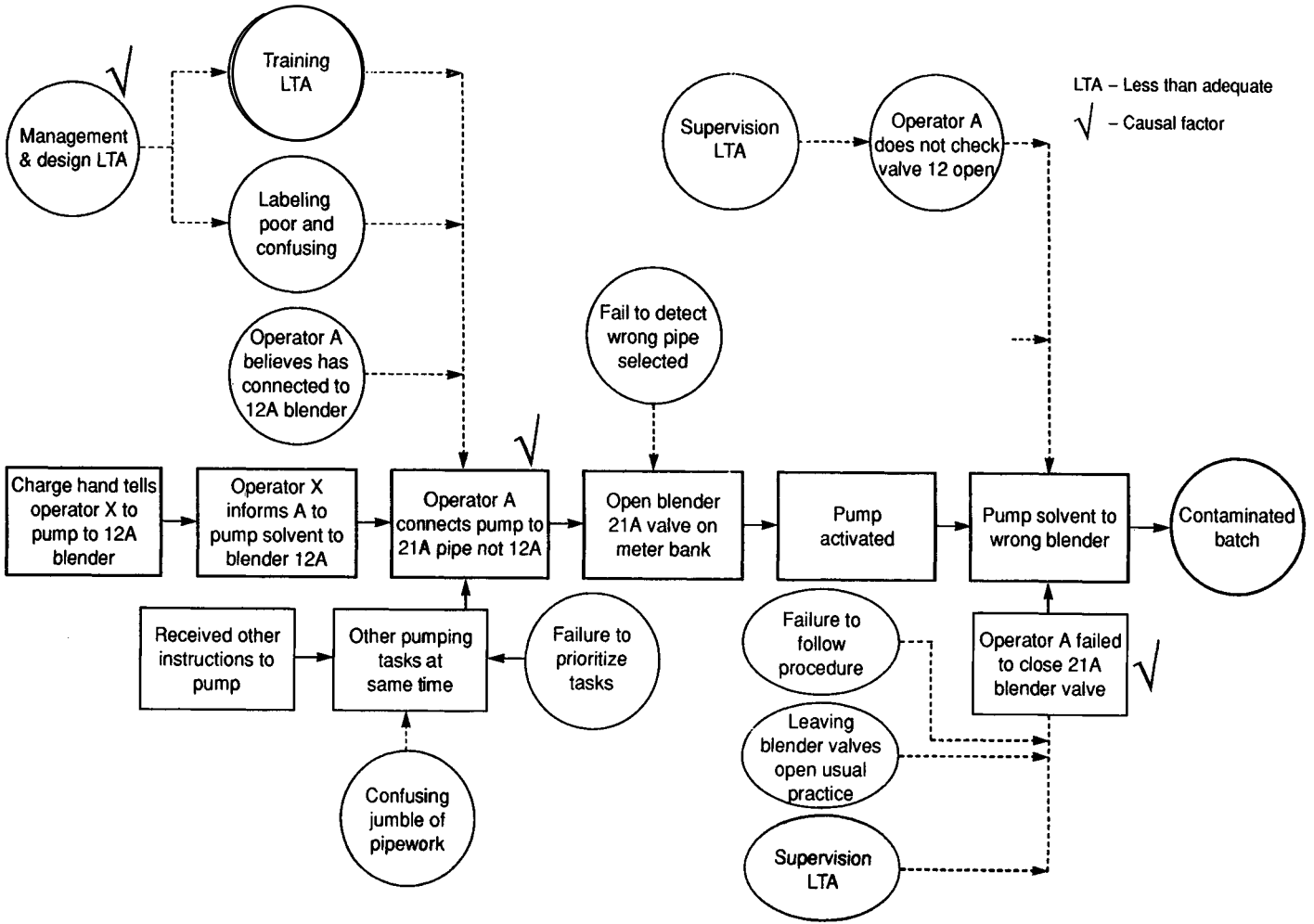

FIGURE 7.9. **Events and Causal Factors Chart.**

- **Root causes 4 and 5.** Human–machine interface less than adequate. The labeling of the pipe was poor and confusing, the general ergonomics of the work situation was poor.
- **Root cause 6.** The system was not error tolerant. The error made was not detectable.
- **Root cause 7.** Personal performance. Attention may have been less than adequate.

Causal Factor 2: Operator A Failed to Close 21A Blender Valve

Root cause coding identified the following root causes:

- **Root causes 1, 2, and 3.** Procedures were not followed. Procedures were not written down and in practice were inconvenient to use. No audit was made to verify the usability of the procedures.
- **Root causes 4 and 5.** There had been no supervision of the worker who should close the blender valves after completion of the job. No audit was made to verify that valves were routinely closed.
- **Root causes 6, 7, and 8.** Human factors aspects were inadequately addressed. Specifically, ergonomics of the plant was poor, there were differences in layout among different areas and the labeling was poor.
- **Root causes 9 and 10.** There may have been a communications problem in telling the worker to close the valve or the personal performance of the operator was less than adequate.

Causal Factor 3: Management and Design Less Than Adequate

This can apply to a number of areas in the sequence. Contributory root causes include: equipment design was poor with no human factors design for the vessel bank; supervision was poor; standards relating to design and training were poor with violations accepted as the norm. Communication among staff members was informal and unstructured.

7.4. CASE STUDY 3: DESIGN OF STANDARD OPERATING PROCEDURES FOR TASK IN CASE STUDY 2

7.4.1. Introduction

Standard operating procedures (SOPs) are step-by-step job instructions which can help workers perform their jobs safely and efficiently. When the end users are involved in their design, SOPs can provide a basis for arriving at a method of work agreed-to by different shifts. In this sense, SOPs can be used to develop training programs and specify measures of competence. Because of the importance of SOPs in the work situation, a systematic framework is needed to enable the design of reliable procedures which are acceptable by the workforce.

Next Page