error (e.g., domino effect on nearby equipment). Independent review of final event
trees is the best method to identify such faults (Step 7, Figure 3.9).

Errors can arise in the conditional probability data leading to major errors in the
predicted final outcome frequencies. The analyst should document sources of data
employed to allow for subsequent checking.

Utility. Event trees are a straightforward technique to use. They are a graphical form of
a logic table and are easier to understand by nonspecialists than fault trees. Provided the
assumptions of no dependency and total success and failure are met, the calculations are
easy. They are useful for both preincident and postincident analyses, and are especially
helpful in the analysis of sequential systems or in human error problems.

Resources Needed. Except for unusually complicated problems, event trees tend not
to require significant resources. Because protective system designs tend to be very com-
plex (Section 6.2), postincident analyses tend to be easier to apply than preincident
analyses.

Computer Codes Available.
ETA II, Science Applications International Corp., 5150 El Camino Real, Los Altos,
CA 94022
RISKMAN, Pickard, Lowe and Garrick, Newport Beach, CA
SUPER, Westinghouse Risk Management, P.O. Box 355, Pittsburgh, PA 15230.

3.3. Complementary Plant-Modeling Techniques

The previous section (3.2) discusses the analysis of fault trees and event trees, by using
frequency and probability data. For ease of presentation in that section, some factors
that influence the quality of the analysis were deferred. In this section (3.3) we discuss
common-cause failure analysis (3.3.1), human reliability analysis (3.3.2), and external

---

**TABLE 3.6. Sample Event Tree Outcomes and Frequencies**

<table>
<thead>
<tr>
<th>Outcome</th>
<th>Sequences leading to outcome</th>
<th>Frequency (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLEVE</td>
<td>ABF</td>
<td>$2.0 \times 10^{-6}$ = $2.0 \times 10^{-6}$</td>
</tr>
<tr>
<td>Flash Fire</td>
<td>ABCDEF + ABCDEF</td>
<td>$4.9 \times 10^{-6} + 27.5 \times 10^{-6} = 32.4 \times 10^{-6}$</td>
</tr>
<tr>
<td>Flash fire and BLEVE</td>
<td>ABCDEF + ABCDE</td>
<td>$1.2 \times 10^{-6} + 6.9 \times 10^{-6} = 8.1 \times 10^{-6}$</td>
</tr>
<tr>
<td>UVCE</td>
<td>ABCDE + ABCDE</td>
<td>$6.1 \times 10^{-6} + 34.5 \times 10^{-6} = 40.5 \times 10^{-6}$</td>
</tr>
<tr>
<td>Local thermal hazard</td>
<td>ABF</td>
<td>$8.0 \times 10^{-6} = 8.0 \times 10^{-6}$</td>
</tr>
<tr>
<td>Safe dispersal</td>
<td>ABCD + ACD</td>
<td>$1.4 \times 10^{-6} + 7.6 \times 10^{-6} = 9.0 \times 10^{-6}$</td>
</tr>
<tr>
<td>Total all outcomes</td>
<td></td>
<td>$= 100 \times 10^{-6}$</td>
</tr>
</tbody>
</table>
events analysis (3.3.3). The results of any of these analyses can be used in the frequency modeling techniques of Section 3.2, and may have a major effect on the results of those techniques.

3.3.1. Common Cause Failure Analysis

Functional redundancy and diversity are used throughout many industries to improve the reliability and/or safety of selected systems. There is an increasing trend toward the use of redundancy and diversity in the CPI-particularly in instrumentation and control applications. Specifically, companies in the CPI have provided multiple layers of protection (multiple safeguards) to help ensure adequate protection against process hazards. Safeguards include both engineering and administrative controls that help prevent or mitigate process upsets (e.g., releases) that can threaten employees, the public, the environment, equipment, and/or facilities. Examples of safeguards include (1) process alarms, (2) shutdown interlocks, (3) relief systems, (4) hydrocarbon detectors, (5) fire protection systems, and (6) plant process safety policies and procedures.

Using multiple safeguards often reduces risk. However, the very high reliability theoretically achievable through the use of multiple safeguards, particularly through the use of redundant components, can sometimes be compromised by single events that can fail multiple safeguards. For example, all temperature sensors in an emergency shutdown system can fail because of a miscalibration error during maintenance activities. The events that defeat multiple safeguards and are attributed to a single cause of failure are often called dependent failures, and they have consistently been shown to be important contributors to risk. These events are generally referred to as dependent failure events. Normally, in a CPQRA, several types of dependent failure events are addressed explicitly in the failure logic models used to estimate accident frequencies (e.g., failure of a support system such as instrument air). The causes of dependent failures that are not addressed explicitly, if judged to be important, should be addressed in a common cause failure (CCF) analysis.

The importance of dependent failures and CCFs in systems analysis has long been recognized. When multiple safeguards are used to help ensure adequate protection against process hazards, accidents cannot occur unless multiple failures occur. Multiple failures can happen as the result of the independent failure of each safeguard; however, operational experience shows that multiple independent failures are rare. This is easily understood with the simple, numerical example by Paula et al. (1997b). Consider a shutdown interlock that consists of three redundant temperature switches—A, B, and C. Each switch is designed to individually shut down the system upon high temperature. Also, assume that the probabilities that the switches will fail on demand ($P(A)$, $P(B)$, and $P(C)$) are constant and equal to 0.01 (1 in 100 demands). If it is further assumed that failures of these three switches are independent, then the total probability that all switches will fail, $P(S)$, is given by

$$P(S) = P(A) \times P(B) \times P(C) = (0.01)^3 = 10^{-6}$/demand

That is, the system is expected to fail once in every one million demands. Further, if we had assumed that the probabilities of switch failure on demand ($P(A)$, $P(B)$, and $P(C)$) were equal to 0.001 (1 in 1000 demands), which may be difficult but possible to
obtain in practical applications, then the system would be expected to fail *once in every one trillion demands*. These are rather unbelievable numbers because, as exemplified later, systems with two, three, four, or even higher levels of redundancy have failed often in commercial and industrial applications, including CPI facilities, aircraft, and nuclear power plants. That is, the assumption of independence among redundant safeguards results in unrealistic, very low estimates for the probability of loss of all safeguards; it gives too much credit for multiple safeguards, potentially causing a gross underestimation of risk.

But what makes the simple probabilistic evaluations presented above unrealistic? As more complex designs evolved in the 1950s, engineers and reliability specialists discovered that multiple safeguards can also fail because of a single event (a dependent failure event) (Epler, 1969; Laurence, 1960; Siddall, 1957). In the previous example, all three switches in the high temperature shutdown interlock could be miscalibrated during maintenance, resulting in the functional unavailability of the entire system. Because they are attributable to a single cause of failure, these dependent failure events are often called CCF events. Many authors have used different terminology to describe this class of events, including “cross-linked failure,” “systematic failure,” “common disaster,” and “common mode failure” (Edwards, 1979; Watson and Edwards, 1979; Paula, 1995). This section defines and exemplifies dependent failures and CCFs, and it provides guidance and quantitative data to account for CCFs when assessing risk for CPI facilities. Examples where CCF played a major role in accidents are

- **Engineering Construction.** Hagen (1980) quotes a case of a CCF when a package of 4-year-old diodes in a rod drive system failed during a required trip of a nuclear reactor, defeating all redundant systems.
- **External Environment.** Hoyle (1982) reports a silicon tetrachloride incident due to common cause failure.
- **Operation Procedure.** Hagen (1980) discusses the Browns Ferry fire incident. A fire induced by human error defeated several systems.

Other incidents, mainly from the nuclear industry, have been reported by Epler (1969). More recent reviews are given by Edwards et al. (1979), Fleming et al. (1986), and Paula et al. (1985).

There are numerous possible sources of dependencies among redundant equipment. Figure 3.11 presents a comprehensive categorization scheme for the causes of dependent failures, including events external to the chemical process plant (e.g., earthquakes, fires, floods, high winds, aircraft collisions) and events internal to the plant (e.g., fires and explosions). Some of these events can be treated in a CPQRA by developing specific event tree and fault tree logic models (Budnitz 1984; NUREG, 1983). Other causes of dependency include failure of common support systems (common power supply, common lube oil, common instrument air system, etc.) and functional dependencies (e.g., loss of raw water system booster pumps on loss of suction from the discharge of the upstream low-lift pump). Again, most CPQRAs incorporate these dependencies explicitly in the analysis (i.e., in the event tree and fault tree logic models).

There are still other important causes of dependent failures in Figure 3.11 that are generally not explicitly addressed in a CPQRA. They result from harsh environments
FIGURE 3.11. Classification system for dependent failures (Edwards et al., 1979).
(high temperature, humidity, corrosion, vibration and impact, etc.), inadequate design, manufacturing deficiencies, installation and commissioning errors, maintenance errors, and other causes. These causes are, in general, so numerous that explicitly representing them in the quantitative risk analysis models (event trees or fault trees) greatly increases the size of the CPQRA and can overwhelm the analyst. This group of dependent failures and any other known dependencies that are not, for whatever reason, explicitly modeled are denoted residual CCFs.

3.3.1.1. BACKGROUND

Early CCF techniques and studies were mostly either qualitative (Epler, 1969, 1977; Putney, 1981; Rasmussen et al., 1976, 1982; Rooney et al., 1978; Wagner et al., 1977; Worrell, 1985) or quantitative (Apostolakis, 1976; Apostolakis et al., 1983; Atwood, 1983a; Fleming, 1974; Fleming et al., 1978; Stamatelatos, 1982; Vaurio, 1981). A qualitative CCF analysis investigates the factors that create dependencies among redundant components (Paula et al., 1990, 1991). It often includes analysis of the causes of dependent failures, and attempts to identify those causes most likely to lead to a CCF. The insights provided by the qualitative analysis are useful in developing recommendations regarding defenses against CCFs.

A quantitative CCF analysis evaluates the probability of occurrence of each postulated CCF event. These probabilities can then be used in the CPQRA. Recent quantitative CCF analyses have also included detailed analyses of available data (e.g., failure occurrence reports) to help identify CCF events and to estimate parameters for quantitative CCF models (Battle et al., 1983; Edwards et al., 1979; Mosleh et al., 1988; NUS Corporation, 1983; Paula, 1988; Poucet et al., 1987).

Several models are available for evaluating CCF probabilities. These models are often referred to as parametric models and include the Beta Factor (Fleming, 1975), the Multiple Greek Letter (Mosleh, 1988), the Binomial Failure Rate (Atwood, 1980) and several others. Although there are theoretical differences between these models, practical applications indicate that model selection is not critical in a CCF analysis. Analysis results are much more sensitive to the qualitative and data analysis portions of the CCF analysis (Mosleh et al., 1988; Poucet et al., 1987).

The current consensus of risk assessment experts is that an adequate CCF analysis should rely on both qualitative and quantitative techniques. The integrated CCF procedure described in this section emphasizes both of these.

**Purpose.** CCF analysis objectives include the following: (1) identification of relevant CCF events, (2) quantification of CCF contributors, and (3) formulation of defense alternatives and stipulation of recommendations to prevent CCFs. The first objective includes identifying the most relevant causes of CCF events, the second permits comparisons to be made with other contributors to system unavailability and plant risk, and the third relies extensively on the first two objectives.

**Philosophy.** The underlying philosophy is to recognize the potential for CCFs (i.e., accept that they might exist in the system) and to account for CCFs by making the best use of available historical experience (including plant-specific and generic data) based on a thorough understanding of the nature of CCF events.
To understand CCF events and to model them, it is necessary to answer questions such as the following (Paula et al., 1990): Why do components fail or why are they unavailable? What is it that can lead to multiple failures? Is there anything at a particular facility that could prevent the occurrence of such multiple failures?

These questions lead to the consideration of three factors. The first is the root cause of component failure or unavailability. The root cause is the specific event or factor that may lead to a CCF. A detailed CCF analysis requires proper identification of the root cause. The degree of detail in specifying the root cause is dictated by how specific an analysis needs to be, but it is clear that a thorough understanding of CCF events and how they can be prevented can only come from a detailed specification of the types of root causes.

Given the existence of the root cause, the second factor is the presence of a linking or coupling mechanism, which is what leads to multiple equipment failures. The coupling mechanism explains why a particular root cause impacts several components. Obviously, each component fails because of its susceptibility to the conditions created by the root cause; the role of the link or coupling mechanism is that it makes those conditions common to several components. CCFs therefore, can be thought of as resulting from the coexistence of two factors: (1) a susceptibility for components to fail or to be unavailable because of a particular root cause and (2) a coupling mechanism that creates the conditions for multiple components to be affected by the same cause.

The third factor increases the potential for CCFs. This is the lack of engineered or operational defenses against unanticipated equipment failures. Typical tactics adopted in a defensive scheme include design control, segregation of equipment, well-designed test and inspection procedures, maintenance procedures, review of procedures, training of personnel, manufacturing quality control, and installation and commissioning quality control. These tactics may be particularly effective for mitigating specific types of dependent or CCFs.

As an example of a defensive strategy, physical separation of redundant equipment reduces the chance of simultaneous failure caused by exposure of the equipment to certain environmental conditions. In this case, the defense acts to eliminate the coupling mechanism. Other defensive tactics may be effective in reducing the likelihood of independent failures as well as dependent failures by reducing the susceptibility of components to certain types of root causes. Thus, it can be argued that a complete treatment of CCFs should not be performed independently of an analysis of the independent failures; rather, the treatment of all failures should be integrated.

**CCF Definition.** For CPI applications, a CCF event is defined as multiple safeguards failing or otherwise being disabled simultaneously, or within a short time, from the same cause of failure (Paula et al., 1997b). Thus, three important conditions for an actual CCF are that (1) multiple safeguards must be failed or disabled (not simply degraded), (2) the failures must be simultaneous (or nearly simultaneous as discussed next), and (3) the cause of the failure for each safeguard must be the same.

Within this definition, multiple failures occurring “simultaneously” (or nearly simultaneously) does not necessarily mean occurring at the same instant in time. “Simultaneously” means sufficiently close in time to result in failure to perform the safety function required of the multiple safeguards (i.e., preventing and/or mitigating
the consequences of an accident). For instance, if emergency cooling water is required from one of two, continuously running, redundant pumps for 2 hours to safely shut down a reactor, “nearly simultaneous” means “within 2 hours.” That is, both pumps failing any time within the 2-hour mission results in a CCF. For interlock systems that use redundancy (e.g., the high temperature shutdown interlock discussed earlier), “nearly simultaneous” often means “within the time between testing of the redundant equipment.” (This assumes that once they occur, failures are detected and corrected during the next test.)

Note that the essence of a CCF event is not the cause of failure, which could be equipment failure, human error, or external damage (e.g., fire or external impact). In fact, the available literature shows that the causes of CCF events are generally no different from the causes of single, independent failures. The only difference is the existence of CCF coupling factors that are responsible for the occurrence of multiple instead of single failures (Mosleh et al., 1988; Paula et al., 1990, 1991, 1995). For example, the spurious operation of a deluge system can result in the (single) failure of an electronic component, A, in a certain location of the CPI facility. The same deluge system failure would probably have resulted in the failure of both redundant components, A and B, if they were in the same location. The cause of component failure (water damage to electronic equipment) is the same in both cases; CCF coupling (same location in this example) is what separates CCF events from single failure events. Other CCF couplings include common support system, common hardware, equipment similarity, common internal environment, and common operating/maintenance staff and procedures. These CCF couplings are discussed later.

Thus, the essence of a CCF event is the coupling in the failure times of multiple safeguards. This is illustrated in Figure 3.12, which shows the failure times for three redundant safeguards over a period of about 20 years. In case (a), each safeguard has failed four times, and the times of failure are random (not linked or coupled). The pattern in Figure 3.12a should be expected if no CCF coupling exists. Figure 3.12b shows the failure times for three other safeguards. Just like the safeguards in case (a), each safeguard in Figure 3.12b has failed four times over about 20 years. However, the failure times are completely coupled in time (i.e., the safeguards always fail at the same time). The pattern in Figure 3.12b is hypothetical because complete coupling in the failure times does not occur even if all CCF couplings exist, but Figure 3.12b does illustrate the essence of a CCF event.

**CCF Coupling.** Six CCF coupling types act alone or (more often) in combination to create a CCF event. Each CCF coupling is discussed and exemplified in the following paragraphs.

**CCF coupling 1: common support system.** Several types of safeguards have a functional dependency on support systems, including control systems [distributed control systems (DCS), programmable logic controller (PLC), etc.] and utilities (instrument air, electric power, steam, etc.). Although safeguards are often designed to “fail safe” upon loss of support systems (e.g., isolation valve closing upon loss of control signal or loss of instrument air), these are not the only failure modes. In fact, intentionally or unintentionally, loss or degradation of support systems can defeat safeguards in some
applications. This can be a source of coupling if the support systems are common to multiple safeguards.

For example, if two electric-driven firewater pumps are supplied electric power from the same motor control center (MCC), they will both be disabled if the MCC fails. Also, there may still be coupling even when the safeguards rely on separate support systems. For example, it may appear no coupling should exist if pump A gets electric power from MCC A and pump B gets electric power from MCC B. However, it is possible that coupling factors exist between MCC A and MCC B (e.g., a common offsite electric feeder to both MCCs A and B). Therefore, it is not enough to provide separate support systems for multiple safeguards; it must be ensured that CCF couplings within the separate support systems have also been eliminated or reduced.

Note that the common support system coupling factor refers to coupling that results from safeguards being disabled because of loss or degradation of the support system. It is also possible that the support system will malfunction in a way that damages the safeguards. For example, a power surge in the electric supply to the two firewater pumps A
and B could damage the electric motor on each pump. This type of coupling is considered with the common internal environment coupling, and thus is excluded from the common support system coupling.

**CCF coupling 2: common hardware.** This coupling is similar to the common support system coupling, but the coupling is the failure of hardware that is common (shared) by multiple safeguards. A typical example of multiple safeguards with common hardware is two (or more) firewater pumps that take suction from a common header. All pumps would fail if the header were inadvertently blocked, plugged, or ruptured. As another example, several pumps were used to help ensure an adequate and continuous supply of feedwater to steam boilers at the powerhouse for an oil refinery. However, the inadvertent operation of a single low-level switch in the feedwater surge tank caused simultaneous tripping of all boiler feedwater pumps.

The common hardware coupling factor has also been observed between redundant instrumentation, control/data acquisition equipment, and (to a lesser degree) protection systems. For example, Paula et al. (1993) discuss four “one-out-of-two” redundant systems that failed a total of 23 times because of hardware failures in shared equipment (bus, bus switching, wiring, etc.). In fact, Paula et al. (1993) concluded that failures within common or shared equipment (e.g., output modules) are one of the most important contributors to the frequency of failure of fault-tolerant DCS typically used in CPI facilities.

**CCF coupling 3: equipment similarity.** Most CCFs observed in several industries have involved similar equipment. This is primarily due to similar equipment being affected by common design and manufacturing processes, the same installation and commissioning procedures, the same operating policies and procedures, the same maintenance programs. These commonalities allow for multiple failures that are due to systematically repeated human errors or other deficiencies. For example, two redundant circuit breakers in the reactor protection system at a nuclear power plant in Germany failed to open. Investigation of the event revealed that, because of a deficiency in the manufacturing of the breaker contacts, the coating on the contacts melted during reactor operation and fused the contacts together. Both redundant breakers were manufactured following the same process and procedures, and obviously they were both susceptible to (and failed from) the same deficiency.

Equipment similarity has also been an important factor to maintenance-related failure events. For instance, during routine maintenance of a commercial aircraft, a maintenance mechanic failed to install an O-ring seal in each of the three jet engines. Shortly after takeoff, all three engines shut down after the lubricating oil was consumed because of the missing seal. Fortunately, one engine restarted, allowing the pilot to land. The cause of this incident was that, unknown to the mechanic, the storeroom had changed the normal stocking procedure and now stocked the O-ring seal separate from the other components in the lube oil seal replacement kit. (They changed the procedure because of a packaging change from the part’s manufacturer.) The similarity of the piece-parts (and maintenance procedures) resulted in the mistake being systematically made on all three engines.

**CCF coupling 4: common location.** Equipment in the same location may be susceptible to failure from the same external environmental conditions, including sudden, energetic events (earthquake, fire, flood, missile impact, etc.) and abnormal environments.
(excessive dust, vibration, high temperature, moisture, etc.). For example, redundant electronic equipment in a room could fail because of a fire in that location or from high temperature if the air-conditioning system for that room fails.

Regarding sudden, energetic events, Stephenson (1991) discusses two unrelated air tragedies (a Japan Air Lines Boeing 747 and a United Airlines DC10) that resulted from the loss of redundant hydraulic systems. These systems failed because of damage to the redundant hydraulic lines in the rudder of each aircraft; in both cases, all hydraulic lines were close together (common location). According to documents from the National Transportation Safety Board and the Federal Aviation Administration, the DC-10 accident resulted in 111 fatalities and many injuries when the plane crashed during an emergency landing in Sioux Gateway Airport, Iowa. It was caused by catastrophic failure of the tail-mounted engine during cruise flight. The separation, fragmentation, and forceful discharge of the stage one fan rotor assembly led to severing or loosening the hydraulic lines in the rudder of the aircraft. This in turn disabled all three redundant hydraulic systems that powered the flight controls.

Regarding abnormal environments, operational experience in CPI and other industrial facilities shows that the common location coupling factor is often strengthened by the equipment similarity coupling factor. This may be from similar equipment having the same (or similar) stress-resisting capacity (strength) to environmental causes. Thus, similar components are more likely to fail simultaneously if the environments-induced stress exceeds the strength of the components. Dissimilar components generally have different strengths regarding environmental causes, and the weakest component is likely to fail first, allowing the operating/maintenance staff to detect and correct the problem before additional failures occur.

**CCF coupling 5: common internal environment.** The internal environment sometimes causes or contributes to safeguard failures. Examples of internal environments include air in an instrument air system, electric current in an electrical distribution system, water in an emergency cooling system, and fluid in a hydraulic system. These events can fail multiple safeguards if the internal environment is the same or similar for these safeguards. An example mentioned earlier is a power surge in the electric supply to two firewater pumps A and B that could damage the electric motor on each pump. A more common example in CPI facilities is grass and other debris causing strainers in river water pumps to plug, resulting in loss of suction to redundant pumps. Redundant river water pumps have also failed because of accelerated internal erosion from abnormally high concentrations of sand in the water.

Obviously, any set of components subjected to a common internal environment is susceptible to the CCF coupling common internal environment. In fact, operational experience shows that pneumatically operated valves have often been involved in CCFs from the internal environment (e.g., moisture in the air supply). Heat exchangers, pump strainers, and trash racks used in river water systems have also been involved in CCFs from the internal environment (e.g., sand contamination). However, this coupling is only weakly associated with other types of environments. For example, check valves used in clean water service have been less susceptible to this coupling. Also, CCFs involving electrical equipment is only occasionally associated with the internal environment (electrical supply). This may be due to better
controls (e.g., fault and surge protection in electrical distribution systems) of some internal environments.

**CCF coupling 6: common operating/maintenance staff and procedure.** Some catastrophic accidents were the result of human or procedural errors such as misoperation, misalignment, and miscalibration of multiple safeguards. Theoretically, all safeguards (similar or dissimilar) operated or maintained by the same staff or addressed by the same procedure (written or otherwise) are susceptible to failure from a CCF. In the well-publicized accident at the Three Mile Island (TMI) nuclear power plant in the United States, the plant operators (acting on inadequate and misleading information) shut down the redundant trains of the emergency core cooling system (ECCS). The ECCS had started automatically to respond to a small loss of coolant event, and the operator action eventually led to uncovering the reactor core and core damage.

Operational experience suggests that when misalignment, miscalibration, and other types of staff/procedural errors result in multiple failures, they often involve similar equipment. That is, this CCF coupling is often strengthened by the equipment similarity coupling (or vice-versa). This is understandable because multiple misalignment and miscalibration errors are more likely to occur when the equipment involved is similar. For example, the likelihood of inadvertently closing a redundant set of valves A and B while attempting to close another set of valves C and D is much higher if these two sets of valves look the same. Also, the common location and equipment similarity couplings together can strengthen the common operating/maintenance staff and procedure coupling. For example, if an operator misaligns valves in one train of equipment, the likelihood of misaligning the valves on the redundant equipment increases if the redundant equipment is similar and is in the same location; the operator could rely on the incorrect alignment of one train to align the other train.

As another example of this coupling, on April 26, 1986, the worst accident in the nuclear power industry occurred at Chernobyl Unit 4 (Chernobyl-4). It happened during a test designed to assess the reactor's safety margin in a particular set of circumstances. Descriptions of the details of the incident are somewhat inconsistent, but it has been established that the automatic trip systems on the steam separators were deactivated by the operators to allow the test. That is, multiple safeguards were disabled by the operators. (The ECCS was also isolated before the test, but experts now believe this had little impact on the outcome of the accident.) Because this type of reactor has a positive void coefficient [i.e., water turning into steam in the core increases the reaction rate (and power generation)], controlling pressure and temperature in the core is particularly critical; the misoperation of safeguards (deactivation of the trip systems) disabled the protection against inadvertent steam generation in the core. Subsequent actions by the operators while conducting the test resulted in an uncontrolled generation of steam in the core, causing the reactor power to peak about 100 times above the design power.

**Applications.** CCFs should be considered in chemical process industry applications that rely on redundancy or diversity to achieve high levels of system reliability and process safety. A CCF analysis is likely to be needed for studies of process systems in which the accident frequency estimates derived from an analysis of independent failures are
very low. This is often the case when a system design makes extensive use of redundancy, voting logic, and so forth. These applications often involve instrumentation and control systems and redundant mechanical equipment configurations. Normally, if a CCF analysis is necessary, the emphasis should be on safety systems. Experience indicates that most CCF events have involved standby equipment.

### 3.3.1.2. DESCRIPTION

This section describes an integrated framework for a CCF analysis (Mosleh et al., 1988). There are four stages in this framework, as illustrated in Figure 3.13.

We will present an overview of each of the four stages, and then discuss the following portions of the framework in more detail:

- Identification of the groups of components to be included in the CCF analysis
- Identification of the defenses against CCF coupling
- CCF quantification approaches
- Incorporation of CCF events in the fault tree
- Selection of the CCF model
- Estimation of CCF model parameters
- Quantification of CCFs using the simple method by Paula and Daggett (1997b)

**Overview of the framework.** The integrated framework for a CCF analysis has four stages:

![Diagram of the integrated framework for a CCF analysis](image.png)

**FIGURE 3.13. Framework for Common Cause Analysis (Mosleh et al., 1988).**
Stage 1. System Logic Model Development. The objective of this stage, which includes system familiarization and problem definition, is to construct a logic model that identifies the contributions of basic events that lead to the Top event. Section 3.2 describes methods for developing these logic models.

Stage 2. Identification of Common Cause Component Groups. The objectives of this stage include:

- Identifying the groups of system components to be included in or eliminated from the CCF analysis
- Prioritizing the groups of system components identified for further analysis, so that time and resources can best be allocated during the CCF analysis
- Providing engineering arguments to aid in the data analysis step (Step 3)
- Providing engineering insights for later formulation of defense alternatives and stipulation of recommendations in Step 4 (System Quantification and Interpretation of Results)

These objectives are accomplished through the qualitative analysis and quantitative screening steps.

In the qualitative analysis, a search is made for common attributes of components within a minimal cut set and mechanisms of failure that can lead to common cause events. Past experience and understanding of the engineering environment are used to identify signs of potential dependence among redundant components (e.g., component similarity). Experience is also used to identify the effectiveness of defenses that may exist to preclude or reduce the probability of certain CCF events. The result of this search is the identification of initial groups of system components to be included in the analysis. An analysis of the root causes of equipment failure is then performed to substantiate and improve the initial identification. This root cause analysis involves reviewing failure occurrence reports for the plant as well as reports for similar facilities. The information from the qualitative analysis is used to define CCF events (e.g., CCF or redundant valves).

Quantitative screening is used to assign generic (and usually conservative) values to the probability of each CCF event. The system unavailability is evaluated using these values, and the potential dominant contributors to system unavailability are identified.

Stage 3. Common Cause Modeling and Data Analysis. The objectives of this stage are (1) to modify the logic model developed in Stage 1 to incorporate common cause events and (2) to analyze available data for quantifying these events. This modification and analysis are accomplished in a four-step procedure.

- Stage 3.1. Incorporation of Common Cause Basic Events. To model CCFs, it is convenient to define common cause basic events in the logic models (e.g., fault trees). Common cause basic events are those that represent multiple failures of components from shared root causes. Figure 3.14 illustrates this step for systems consisting of two redundant components.

- Stage 3.2. Data Classification and Screening. The purpose of this step is to evaluate and classify event reports to provide input to parameter estimation of the CCF basic events added to the logic model. This involves distinguishing between failure causes that are explicitly modeled in the event and fault trees and those that
are to be included in the residual common cause basic events. The sources of data necessary for this step are event reports on both single and multiple equipment failures at the plant under analysis as well as similar plants. This review of the data concentrates on root causes, coupling mechanisms, and defensive strategies in place at the plant of interest.

• **Stage 3.3. Parameter Estimation.** Typically, CCF models are used to estimate the probabilities of CCF events. The analyst can use the information obtained in Step 3.2 to estimate the parameters of such CCF models. Only the beta-factor model will be illustrated in this overview. Descriptions and estimators for one other model are presented later in this section and additional models are presented by Mosleh et al. (1988). The beta-factor model is the most commonly used parametric model. This model assumes that the failure rate (assumed constant) for each component in a system can be expanded into additive independent and CCF contributions.

\[
\lambda = \lambda_i + \lambda_c
\]

where \( \lambda \) = component failure rate

\( \lambda_i \) = component failure rate for independent failures

\( \lambda_c \) = component failure rate for CCFs

The beta-factor is

\[
\beta = \frac{\lambda_c}{\lambda_c + \lambda_i}
\]
If the system consists of identical redundant units, the system CCF rate is $\beta \lambda$. The following estimator is generally used for $\beta$:

$$\beta = \frac{n_c}{n_c + n_i} \quad (3.3.3)$$

where $n_c$ = total number of component failures that are due to CCF events and $n_i$ = total number of component failures that are due to independent causes.

A basic assumption of the beta-factor model is that a CCF event will result in the failure of all redundant components in the group being considered. This assumption often leads to conservative predictions since, for example, a given CCF event may fail only two out of three components in a group. Some other CCF models [e.g., the multiple greek letter (MGL) model presented later in this section] and do not incorporate this assumption.

**Stage 4. System Quantification and Interpretation of Results.** The purpose of this stage is to synthesize the key outputs of the previous stages for the purpose of quantifying system failure probability. The event probabilities obtained for the common cause events (as a result of Step 3 of the analysis) are incorporated into the solution for the unavailability of the systems or, alternatively, into accident sequence frequencies in the usual way fault tree and event tree models are quantified (Sections 3.2.1, 3.2.2, and Appendix D). The outputs of this stage include the numerical results and the identification of key unavailability contributors. The key contributors are generally the focus of recommendations for better defending against CCFs.

**Identification of the Groups of Components to be Included in the CCF Analysis.** An important objective of Stage 2 in Figure 3.13 is to identify the groups of components that are susceptible to CCFs. Most CCF analyses consider each group of identical, redundant components (e.g., redundant shutdown valves, redundant pressure transmitters) as a group of components that are susceptible to CCFs. This is consistent with operational experience in several industries, which has shown that most CCF events have affected similar equipment operated and maintained in the same way (Edwards and Watson 1979; Fleming et al., 1985; Paula et al., 1985; Watson et al., 1979). For the same reason, most CCF analyses assume that CCF events will not affect dissimilar or diverse equipment. (One exception is an external event such as earthquakes and hurricanes, but external events are typically outside the scope of CCF analyses.)

However, when diverse equipment has piece-parts that are nondiverse (similar), the equipment should not be assumed to be fully diverse. For example, two redundant, motor-driven pumps may be from different manufacturers (and thus “dissimilar”). However, the motor starter (or other piece-parts of the pumps’ electrical and control circuit) for these pumps could be from the same manufacturer. The typical approach here is to redefine the equipment boundary in the fault tree, and model the similar piece-parts (a motor starter in this example) separately from the pumps. The portions of the equipment that are similar (motor starts) are susceptible to CCFs, and the portions that are diverse (pump bodies and motor drivers) are not.

The simple guidelines provided in the two previous paragraphs are often adequate for developing the initial groups of basic events that are susceptible to CCFs. However, when operational data and resources are available, it is recommended that a detailed
qualitative analysis be done of the system under consideration to support the initial groupings. Detailed qualitative analysis also helps ensure that no important CCF events have been overlooked. The scope and depth of the analysis will depend on the (1) information available (particularly operational data for the equipment of interest), (2) experience of the analysis team (CCF analysis experience and design, operations, and maintenance experience), and (3) resources available for the study.

Mosleh et al. (1988) and Paula (1988) present examples of detailed qualitative analyses of CCFs. (These references also exemplify how the results of the qualitative analyses can be used to support quantitative analyses.) Next, we discuss what should be considered in a detailed qualitative analysis. CCFs have occurred because of many different causes. Extensive analyses of several hundred CCF events show that these events can be grouped into a few classes of causes of failure (Edwards et al., 1979; Paula et al., 1985 and 1990):

- Design, manufacturing, installation, and commissioning deficiencies
- Human and procedural errors during maintenance, testing, and operation of the equipment
- Internal (e.g., erosion of valve internals) and external (e.g., excessively high temperature) environment for the equipment
- Energetic external events

Energetic external events can be external to the facility (earthquake, hurricane, aircraft collision, etc.) or internal to the facility (fire, explosion, etc.). Energetic external events are listed above for completeness, but they are often the subject of special studies and are not addressed in CCF analyses. The reason for considering external events separately from the CCF analysis is simple: the approaches best suited for an analysis of external events (e.g., an earthquake) are different from the approaches best suited for the analysis of other types of CCF events. Also, the type of expertise required to analyze external events is different from the expertise required in CCF analysis; the analysis team composition may be different when dealing with external events.

By starting with the comprehensive set of causes of CCFs listed above and analyzing operational data for the system of interest, the qualitative CCF analysis considers:

- The causes of failures applicable to the equipment of interest
- The group of components that could be affected by the occurrence of each cause
- The CCF potential (degree of dependence of CCF coupling) associated with each cause/component group of interest

The last item above (CCF coupling) is critical because the causes of CCF events are generally no different from the causes of single component failures; coupling is the real factor that separates single and multiple failure events. Table 3.7 illustrates this point by presenting six actual failure occurrences and corrective actions taken at different plants. The first two events represent identical problems (at the same plant) resulting in single and multiple failures. The next two events are examples of personnel failing to restore redundant equipment following maintenance, again resulting in single and multiple failures.

Examples such as those in Table 3.7 show that the reason a particular cause affects several components is often associated with one or more conditions (or CCF coupling
<table>
<thead>
<tr>
<th>Plant</th>
<th>Event Description</th>
<th>Failure Mechanism/Cause</th>
<th>Defense/Corrective Action</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>One circuit breaker (CB) to a valve tripped during a test on a room ventilation system</td>
<td>The thermal overload setting on the CB was set too low for the abnormally hot environment</td>
<td>The thermal overload setting was increased in the tripped CB and in the CB to a redundant valve</td>
<td>The untrippe CB to the redundant valve is in the same room as the tripped CB (Room 104)</td>
</tr>
<tr>
<td>A</td>
<td>Two CBs to two redundant valves tripped during a test on a room ventilation system</td>
<td>The thermal overload settings on the CBs were set too low for the abnormally hot environment</td>
<td>The thermal overload settings were increased in both of the CBs</td>
<td>Both CBs are in Room 149</td>
</tr>
<tr>
<td>B</td>
<td>Auxiliary feed pump A was not delivering an adequate flow of feedwater</td>
<td>An in-line conical strainer was found in the pump suction line. The strainer was 95% plugged. This event resulted from an installation error (the strainer should have been removed before operation). Strainers were found in the suction line for three other feedwater pumps</td>
<td>The strainers were removed</td>
<td>The three other strainers were not plugged and did not result in failures</td>
</tr>
<tr>
<td>C</td>
<td>Both emergency service water trains were inoperable</td>
<td>Strainers became plugged in both trains because of contamination. Because of maintenance oversight, they had not been cleaned often enough</td>
<td>Self-cleaning strainers were installed</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>The turbine bypass valve alarm would not clear. An investigation revealed a relay was closed, making the reactor protection system (RPS) subchannel B1 for load reject and turbine valve closure signals inoperable</td>
<td>During a recent maintenance outage, a pressure switch that operates the relay was isolated. The switch was not returned to its proper position before startup</td>
<td>The condition was corrected, and the occurrence was discussed with maintenance and operating personnel</td>
<td>The other RPS subchannels were operable</td>
</tr>
<tr>
<td>E</td>
<td>The main control board indication for feedwater flow was discovered to be reading zero</td>
<td>Personnel left the equalizing valves on the three transmitters open</td>
<td>The valves were closed. Personnel were indoctrinated on the removal and restoration of instruments and the observance of indications</td>
<td></td>
</tr>
</tbody>
</table>

TABLE 3.7. Actual Failure Occurrences and Corrective Actions (Paula et al., 1990)
3.3. Complementary Plant-Modeling Techniques

factors) that were the same for all components that failed. Thus, the CCF coupling factors previously defined provide the basis for identifying CCF potential among multiple safeguards; every set of multiple safeguards applicable to a potential accident scenario must be reviewed for the existence of CCF coupling. Table 3.8 summarizes key points in the identification of CCF coupling.

The coupling factors **common support system** and **common hardware** are usually apparent on piping and instrumentation diagrams (P&IDs), logic diagrams for interlock and shutdown systems, and other process safety information (PSI). CPQRA analysts generally review these diagrams and PSI documents as part of the CPQRA, and the review should reveal these types of dependencies.

However, CCF analysts should review all of this information in sufficient detail to identify subtle support system dependencies or hardware dependencies. For example, a detailed analysis of a fault-tolerant distributed control system (F-T DCS) was performed with instrumentation and control (I&C) specialists and a technician from Honeywell—the DCS manufacturer. This F-T DCS is a Honeywell TDC 3000 that controls a fluidized catalytic cracking (FCC) unit in a large refinery. The analysis involved an in-depth review of the DCS logic diagrams and associated instrumentation, and it revealed some shared instrumentation for interlock systems. Also, the analysis team identified a few shutdown interlocks that were not “fail safe.” In addition, some redundant equipment in the F-T DCS was in the same location, making it susceptible to failure caused by loss of the heating, ventilating, and air-conditioning system.

Any set of similar safeguards (e.g., three identical temperature switches) is susceptible to the coupling factor **equipment similarity**. However, this coupling factor is not limited to identical, redundant components. As previously discussed, some “dissimilar” equipment (e.g., two pumps from different manufacturers) may have piece-parts (e.g., motor starter and IN&C devices) that are similar, being susceptible to this coupling factor. Also, any set of safeguards that (1) are physically in the same location, (2) have the same or similar internal environment, or (3) are operated or maintained by the same staff or addressed by the same procedure (written or otherwise), is susceptible to the following coupling factors: **common location**, **common internal environment**, and **common operating/maintenance staff and procedure**, respectively.

**Identification of the Defenses against CCF Coupling.** An important consideration in the identification of CCFs is the existence or lack of defenses against CCF coupling. It is obvious from the previous discussion of CCF coupling that a search for coupling is primarily a search for similarities in the design, manufacture, construction, installation, commissioning, maintenance, operation, environment, and location of multiple safeguards. A search for defenses against coupling, on the other hand, is primarily a search for dissimilarities among safeguards. Dissimilarities include differences in the safeguards themselves (diversity); differences in the way they are installed, operated, and maintained; and differences in their environment and location.

Paula et al. (1990, pages 21–26, and 1997a, Appendix A) discuss defenses against CCFs in more detail. For example, excellent defenses against the **equipment similarity** coupling include functional diversity (the use of totally different approaches to achieve roughly the same result) and equipment diversity (the use of different types of equipment to perform the same function). Spatial separation and physical protection (e.g.,
### TABLE 3.8. Key Points in the Identification and Quantification of Coupling
(Paula et al., 1977a)

<table>
<thead>
<tr>
<th>Coupling Factor</th>
<th>CCF Identification</th>
<th>CCF Quantification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common support system</td>
<td>Support system dependencies and common hardware dependencies are usually not of interest if the safeguards “fail safe” upon loss of the support system or common hardware. These CCF couplings are identified by reviewing P&amp;IDs, logic diagrams for interlock and shutdown systems, and other PSI documents associated with the set of multiple safeguards. Additional reviews may be required with specialists on each support system (e.g., D.S. specialists, including a representative from the manufacturer)</td>
<td>These coupling factors are highly plant-specific, and plant personnel usually know the frequency of loss of support systems such as electric power and other utility systems. Plant data should be used to evaluate the probability of loss of multiple safeguards resulting from the unavailability of a common support system. Standard CPQRA techniques (e.g., fault tree analysis) and generic failure rate data can be used when plant data are not available (e.g., to evaluate the probability of failure of common hardware).</td>
</tr>
<tr>
<td>Common hardware</td>
<td>Any set of similar safeguards or safeguards that have similar piece parts is susceptible to this coupling factor</td>
<td>Parametric models (based on empirical data) provide an estimate of the probability of CCF events resulting from this coupling factor. This estimate typically includes the contribution from this coupling factor and contributions from at least some causes considered in the coupling factors common location, common internal environment, and common operating/maintenance staff and procedure.</td>
</tr>
<tr>
<td>Equipment similarity</td>
<td>Any set of safeguards that are physically in the same location is susceptible to this coupling factor</td>
<td>All CCFs caused by sudden, energetic events (earthquake, fire, flood, hurricane, tornado, etc.) should be analyzed using techniques specially designed for the analysis of each type of event. Parametric models are used to analyze CCF events resulting from the other causes (abnormal environments) associated with this coupling factor, including excessive dust, vibration, high temperature, moisture, etc.</td>
</tr>
<tr>
<td>Common location</td>
<td>Any set of safeguards that have the same or similar internal environment is susceptible to this coupling factor</td>
<td>Parametric models are used to analyze CCF events associated with this coupling factor.</td>
</tr>
<tr>
<td>Common internal environment</td>
<td>Any set of safeguards (similar or dissimilar) operated or maintained by the same staff or addressed by the same procedure (written or otherwise) is susceptible to this coupling factor</td>
<td>Operator errors during accidents (i.e., misoperation actions) should be analyzed using human reliability analysis techniques. Parametric models are used to analyze CCF events resulting from the other causes (misalignment and miscalibration) associated with this coupling factor.</td>
</tr>
</tbody>
</table>
barriers) are often used to reduce the susceptibility of multiple safeguards to the **common location** coupling.

As another example of defense against CCF coupling, *staggering* test and maintenance activities offers some advantages over doing these activities simultaneously or sequentially. First, it reduces the coupling associated with certain human-related failures—those introduced during test and maintenance activities. The probability that an operator or technician will repeat an incorrect action is lower when test or maintenance activities are performed months, weeks, or even days apart than when they are performed a few minutes or a few hours apart. A second potential advantage of staggering test and maintenance activities relates to the maximum exposure time for CCF events. If multiple safeguards fail because of a CCF event, then evenly staggering these activities reduces the maximum time that the multiple safeguards would be failed because of that CCF event. (This is true if we assume that this type of failure is detectable by testing and inspecting.)

**CCF quantification approaches.** Table 3.8 summarizes key points in the quantification of CCFs. Three ways are available to quantify CCF events:

- Use CPQRA techniques specially designed for the analysis of the specific causes of interest
- Use a parametric model (e.g., the Beta factor or the MGL model) (Mosleh et al., 1988)
- Use a simple method specifically designed to account for CCFs involving safeguards in CPI facilities (Paula et al., 1997b)

The first two CCF couplings in Table 3.8 (**common support system** and **common hardware**) are highly plant-specific, and they can be quantified using standard CPQRA techniques specially designed for the analysis of the specific causes of interest. These techniques include generic failure rate data (CCPS, 1989) and fault tree analysis. However, plant personnel usually know the frequency of loss of support systems (instrument air, steam, etc.) and this information should be used to evaluate the probability of loss of multiple safeguards resulting from the unavailability of a common support system.

Selected causes associated with the CCF coupling **common location** should also be quantified using standard CPQRA techniques specially designed for the analysis of these causes. Specifically, all CCFs caused by sudden, energetic events (earthquake, fire, flood, etc.) should be analyzed using techniques specially designed for the analysis of each type of event. The reason for considering these causes individually is that the techniques best suited for one type of event (e.g., estimating the frequency of an earthquake) are generally different from the techniques best suited for the other types of events (e.g., estimating the frequency of a hurricane or tornado). Section 3.3.3, External Event Analysis, presents these techniques in some detail and provides additional references.

Selected causes associated with the CCF coupling **common operating maintenance staff and procedure** should also be quantified using standard CPQRA techniques specially designed for the analysis of these causes. Specifically, operator errors
during accidents (i.e., misoperation actions) should be analyzed using human reliability analysis techniques. This type of human error includes the actions taken during the TMI and Chernobyl-4 accidents previously discussed. Section 3.3.2, Human Reliability Analysis, presents these techniques in some detail and provides additional references.

Parametric models use empirical data, and they are typically used to quantify the remaining CCF coupling (and the causes associated with a coupling that is not analyzed using standard CPQRA techniques). Specifically, parametric models are typically used to quantify:

1. all causes (inadequate design, manufacturing deficiencies, installation and commissioning errors, environmental stresses, etc.) associated with the CCF couplings equipment similarity and common internal environment,
2. the causes related to abnormal environments (excessive dust, vibration, high temperature, moisture, etc.) associated with the common location CCF coupling, and
3. the causes related to misalignment and miscalibration associated with the common operating/maintenance staff and procedure CCF coupling.

Parametric models are discussed in more detail later in this section. Although parametric models have been used in CPQRAs, the detailed and complete quantifications provided by these models are not always required or cost-effective. Paula et al. (1997b) developed a new, simplified method that can be used instead of the more complicated parametric models. The simplified method is also presented later in this section.

Incorporation of CCF Events in the Fault Tree. After CCF events have been identified in Stage 2, they must be incorporated into the fault tree. We will present two approaches for accomplishing this.¹ The first approach consists of replacing each basic event that represents the failure of a component from a CCF component group with a small fault tree. The small fault tree that will be used depends on the number of components, n, in the CCF component group.

Figures 3.15 through 3.17 present the fault tree logics for n = 2, 3, and 4. For two components (A and B) in the CCF component group (n = 2), the logic is an OR gate with two inputs. The first input represents the independent failure of the component, and the second input represents both components failing because of a CCF event. If n = 3, the logic represents the independent failure of the component, the CCF of the component with one (and only one) of the other two components, and the CCF of all three components. For n = 4, the logic represents the independent failure of the component, the CCF of the component with one (and only one) of the other three components, the CCF of the component with each set of two (and only two) of the other three components, and the CCF of all four components. (Similar logics can be developed for n > 4.)

¹ Some analysts believe that both approaches for incorporating CCF events in the fault tree are approximate, and they slightly overestimate the contribution of CCFs because of double counting of certain types of CCF events. This potential overestimation is discussed in detail by Mosleh et al. (1989, pages C-1, C-2, and C-3), and it has negligible impact in practical applications.
Figures 3.15 through 3.17 also show the probabilities \( Q_1, Q_2, Q_3, \) and \( Q_4 \) for each event in the fault trees. \( Q_j \) is the probability of a CCF resulting in a specific set of \( k \) failures. For example, \( Q_2 \) is the probability of a CCF of components A and B. Later in this section, we discuss how to calculate the values of \( Q_1, Q_2, Q_3, \) and \( Q_4 \), which is typically accomplished using sets of parameters \( (\beta, \gamma, \delta, \text{etc.}) \) specifically defined for quantification of CCFs.

The fault tree logic substitution procedure described above is conceptually simple. Nonetheless, the incorporation of many pieces of fault tree into the fault tree for the system of interest can result in a large fault tree. This is often not a problem because most fault tree software packages can easily analyze the large fault trees that may result after the incorporation of CCF events. However, some analysts may not have access to fault tree software packages or may find it more convenient to analyze the fault tree by hand. Therefore, an alternative approach for incorporating CCF events in the fault trees may be useful.

The alternative approach for incorporating CCF events in the fault trees is called the “pattern recognition” approach (Mosleh et al., 1989). (The simplified method for quantification of CCFs, presented later in this section, uses this approach.) In the pattern recognition approach, the analyst evaluates the total probability that a redundant set of components (e.g., three pressure transmitters) will fail according to a success criterion (e.g., two-out-of-three), and then incorporates this total probability directly into the fault tree. That is, the specific combinations (e.g., components A and B, components A and C) of failures that will cause the set of redundant components to fail are not modeled explicitly in the fault tree; the fault tree has a single event that represents the failure of the redundant system from all possible combinations (independent failures, CCFs, and any combination of these). The reader is referred to the work of Mosleh et al. (1989) for additional information on the pattern recognition approach.

\[
\begin{align*}
Q_r &= P(A) \\
Q_1 &= (1 - \beta) Q_r \\
Q_2 &= \beta Q_r 
\end{align*}
\]

**FIGURE 3.15.** Fault tree modification to account for CCFs \( (n = 2) \).
FIGURE 3.16. Fault tree modification to account for CCFs ($n = 3$).

Number of redundant components ($n = 3$)

$$Q_T = P(A)$$
$$Q_1 = (1 - \beta) Q_T$$
$$Q_2 = \frac{1}{2} \beta (1 - \gamma) Q_T$$
$$Q_3 = \beta \gamma Q_T$$

FIGURE 3.17. Fault tree modification to account for CCFs ($n = 4$).

Number of redundant components ($n = 4$)

$$Q_T = P(A)$$
$$Q_1 = (1 - \beta) Q_T$$
$$Q_2 = \frac{1}{3} \beta (1 - \gamma) Q_T$$
$$Q_3 = \frac{1}{3} \beta \gamma (1 - \delta) Q_T$$
$$Q_4 = \beta \gamma \delta Q_T$$
Selection of the CCF Model. The previous paragraphs show how to incorporate CCF events in the fault trees. Also, formulas were introduced in Figures 3.15, 3.16, and 3.17 for the evaluation of the CCF event probabilities as a function of $Q_1, Q_2, Q_3,$ and $Q_4$. $Q_k$ can be evaluated in several ways. Perhaps the simplest conceptual approach is to evaluate CCF probabilities directly from field data in the same way equipment failure rates and equipment failure probabilities are evaluated from field data. For example, if a system with two redundant trains of equipment experienced two CCFs in approximately 120 system demands, the following CCF probability, $Q_2$, can be estimated directly from these field data using standard reliability techniques:

$$Q_2 = \frac{2 \text{ CCFs}}{120 \text{ demands}} = 0.017/\text{demand}$$

Because of simplicity and consistency with the quantification of the other basic events in a fault tree, direct evaluation is probably the best approach for quantifying CCFs whenever statistically significant data are available for the redundant system of interest or similar systems. However, CCFs are rare, and the analyst typically does not have sufficient data to estimate failure rates and probabilities directly as illustrated above. Thus, the analyst must rely on generic data (i.e., combined data from several systems in different facilities). Generic data are often from systems and equipment that are not identical to the system/equipment considered in the analysis and/or from systems/equipment used in other industries (e.g., nuclear power plants). Obviously, this creates uncertainty in the CCF probability estimates.

Another source of uncertainty was first recognized by Fleming (1974 and 1975) in the early attempts to collect and analyze generic CCF data, and it is still a source of uncertainty today. Some equipment failure databases do not provide all the information needed in estimating failure rates and/or probabilities of failure on demand. [The databases available at the time were based on licensee event reports (LERs), which are submitted to the U.S. Nuclear Regulatory Commission (NRC) by nuclear power plants (LER, 1987). LERs are still valuable sources of CCF data.] Specifically, some databases contain information about system/equipment failures attributable to CCFs and independent failures, but they do not provide the operating time and the total number of demands for the systems/equipment. That is, most databases provide information to estimate the numerator in the equations for evaluating $Q_k$, but not sufficient information to evaluate the denominator.

Based on this realization, Fleming (1974) evaluated CCFs indirectly; instead of attempting to evaluate $Q_k$, he evaluated the ratio of component failures from CCFs to the total number of failures for the component. This ratio is called the “beta factor.” Then, for $n = 2$, $Q_2$ can be obtained by multiplying the beta factor by the total probability of failure for the component. Specifically, the Beta Factor Model assumes that the failure rate (or probability of failure) for a component in a redundant system can be separated into independent and CCF contributions [Eq. (3.3.1)]:

$$\lambda = \lambda_i + \lambda_c$$

(3.3.4)

2 The Beta Factor Model and other parametric CCF models can be defined in terms of failure rates or probabilities of failure on demand. We will assume the former for the sake of discussion. Defining the CCF model in terms of failure rates or probabilities of failure on demand may result in differences in the parameter estimation (e.g., different values of the beta factor).
where \( \lambda_i \equiv \) component failure rate for independent failures
\( \lambda_c \equiv \) component failure rate for CCFs

The beta factor is \( \beta = \lambda_i/(\lambda_i + \lambda_c) \) [Eq. (3.3.2)]. Note that the beta factor is defined at the component level, not at the system level. That is, the beta factor is the fraction of a component's (not the system's) failure rate that results in simultaneous failure of a redundant component from the same cause. Other models [e.g., the alpha-factor (Mosleh et al., 1988) and the \( p \)-factor models (Bodsberg et al.)] are defined at the system level, and alpha/\( p \) factors represent fractions of the system's failure rate that result in multiple failures.

Fleming and Raabe (1978) also observed that despite the type of equipment (valve, pump, instrumentation, etc.) and the value of the failure rate, the values of the beta factors were relatively constant. They postulated that the nearly constant beta factors "may be an inherent characteristic, perhaps directly associated with the current state of technology." If so, the uncertainty associated with indirect models (beta factor, alpha factor, \( p \)-factor, etc.) may be relatively low, even when using generic data derived from other industries. This assertion has not been formally proven. However, the relatively constant values of generic beta factors [and other factors (alpha, etc.)] have been verified by several authors (Edwards and Watson, 1979; Montague et al., 1984). Also, indirect models have been used in nearly all CCF analyses of real systems (versus the analysis of a sample problem to demonstrate a method). These observations (relatively constant values of factors and wide use of indirect models) suggest some acceptability of the contention that there is lower uncertainty associated with indirect models than with direct models.

Since its publication in 1974, the Beta-Factor Model was the most frequently used CCF model in reliability and risk assessments in several industries (Montague et al., 1984). Simplicity of application and availability of operational data to estimate the beta factor values were certainly important reasons for the popularity of this model. Also, the Beta-Factor Model was the first CCF model that used operational data; the empirical nature of the model provided a relatively high confidence on the final quantitative results. However, this model has limitations. Specifically, this is a single-parameter model that does not accurately model redundant systems with three or more trains. The usual assumption for systems with three or more levels of redundancy is that all redundant trains fail when a CCF event occurs; this results in over prediction of the system failure probability.

To address this limitation, several other models have been developed for quantification of CCF probabilities, including the binomial failure rate (BFR), alpha factor, basic parameter, \( p \)-factor, and MGL models (Bodsberg et al.; Fleming et al., 1984; Mosleh et al., 1989). For considerable time, there was debate about the best model for quantitative CCF analysis. This debate was resolved during the Common Cause Failure Reliability Benchmark Exercise (CCF-RBE) (Poucet et al., 1986). The CCF-RBE was conducted over a 2-year period with 10 teams participating from eight countries. Each team analyzed the same system using models and data deemed appropriate by the team. One of the most important conclusions was that "once the qualitative analysis and system logic model are fixed and the available data are interpreted consistently, the selection of a parametric model among a relatively large set of tested and tried models is not particularly important and does not introduce an appreciable level of uncertainty."
Therefore, the use of any one of several models is adequate and should provide analysis results that are consistent with the results that would be obtained using the other models.

Because it is the most straightforward and widely used extension of the Beta-Factor Model, we suggest using the MGL model (Fleming et al., 1984). In this model, other parameters are introduced to account for each additional level of redundancy. For example, for a system with four redundant trains of equipment, the MGL parameters are defined as follows:

\[
\beta = \text{Conditional probability of a CCF event that fails at least two components, given that a specific component has failed}
\]

\[
\gamma = \text{Conditional probability of a CCF event that fails at least three components, given that a CCF has occurred and affected at least two components}
\]

\[
\delta = \text{Conditional probability of a CCF event that fails all four components, given that a CCF has occurred and affected at least three components}
\]

Additional parameters [\(\epsilon\), \(\mu\), etc.] are defined similarly for systems with higher levels of redundancy. Figures 3.15 through 3.17 show the equations for evaluating the probabilities of CCFs \((Q_1, Q_2, Q_3,\) and \(Q_4)\) as a function of the values of the MGL parameters (for up to \(n = 4\)). Estimation of the MGL parameters is addressed next.

**Estimation of CCF Model Parameters.** An important step in the CCF analysis procedure is the estimation of the CCF model parameters (\(\beta, \gamma, \delta,\) etc.). Mosleh et al. (1988, page 3-49, and 1989, Appendix C) provide statistical estimators for the MGL parameters. These references also

- provide guidelines for review, evaluation, and classification of operational data;
- discuss data sources;
- present a procedure for adjusting data from systems of different size (e.g., using CCF data from systems with four redundant trains to estimate parameters for a system with three redundant trains); and
- discuss the impact of different testing strategies (i.e., staggered versus nonstaggered) on the estimators.

These references should be consulted if plant-specific data are available and the analyst wishes to estimate the MGL parameters from field data. However, plant-specific data are not available for most CPI applications. In this case, CCF analysts often use generic data. Montague et al. (1984) and PSI (1997) present more than 80 generic beta factor values published in the late 1970s and early 1980s for a variety of component types (pump, diesel generator, air-operated valve, etc.). Many of these values were derived from actual CCF data from safety systems at nuclear power plants, but these references also include several beta factor values from other industries (chemical, aircraft, computer applications, and a conventional power plant at an oil refinery). These references do not include data for the other MGL parameters (\(\gamma, \delta,\) etc.) because insufficient information was available in the 1970s and 1980s to estimate these parameters.
A CCF database developed recently at the Idaho National Engineering Laboratory (INEL) (Kvarfordt et al., 1995) contains statistically significant data to evaluate MGL parameters for systems with up to six redundant trains. INEL's database contains more than 17,000 failure occurrences involving safety-related components in more than 100 nuclear power plants in the United States. Of these, about 1700 involved CCF events in a variety of safety-related components. Paula (1997c) used these data to estimate the MGL parameters presented in Tables 3.9 and 3.10.

As mentioned before, CCF models can be defined in terms of failure rates or probabilities of failure on demand, and the parameter estimators may be different in each case. Specifically, the estimators depend on the testing strategy (staggered versus nonstaggered) when the CCF model is defined in terms of probabilities of failure on demand. Another important variable in estimating parameters is system size (n = 2, 3, 4, etc.). Table 3.9 presents the estimators for the MGL parameters for selected component types, testing strategies, and value of n. These estimators apply in either of two cases (1) CCF model defined in terms of failure rates and (2) CCF model defined in terms of probabilities of failure on demand, assuming that the testing strategy for the equipment in redundant systems is nonstaggered. Table 3.10 presents the estimators for CCF models defined in terms of probabilities of failure on demand, assuming staggered testing strategy.

The values of the MGL parameters in each of the Tables 3.9 or 3.10 are remarkably similar for a variety of component types. For example, the values of the beta factors in each table are within a factor of about three; the values of the gamma factors and delta factors are within a factor of less than two. Also, with a few possible exceptions, the small differences that we do observe in the MGL parameters for different component types are difficult to explain.

That is, we see no strong engineering argument that would have allowed us to postulate these differences before seeing the data in the tables. These differences are not from statistical uncertainty because the number of independent and CCF events used to derive the MGL parameters is very large.

The few exceptions are the MGL parameters, particularly the beta factor values, for air/gas operated valves and "other equipment" (heat exchanger, pump strainer, and trash rack). For example, the beta factors for these component types are about three times higher than the beta factor values for check valves and motor-operated valves in Table 3.9. A review of the actual CCF events involving air/gas operated valves, heat exchangers, pump strainers, and trash racks revealed that many of these events were associated with the coupling factor common internal environment.

The data in Tables 3.9 and 3.10 suggest that the use of combined data (e.g., "all valves" or "all equipment") to estimate parameters for equipment that is not in these

---

3 CCF events involve multiple equipment failing simultaneously, or within a short period of time, from the same cause of failure (e.g., maintenance error, design deficiency). Thus, three important conditions for an actual CCF event are that multiple equipment must be failed (not simply degraded), the failures must be simultaneous (or nearly simultaneous), and the cause of failure for each redundant component must be the same. However, there is uncertainty about these conditions for several events in any CCF database. In these cases, weighting factors are used to reflect the analyst's confidence about these events being actual CCF events. The 1,700 events include the actual CCF events as well as the CCF events that involved some uncertainty concerning these three conditions.
## TABLE 3.9. Generic MGL Parameters for Models that Use (1) Failure Rates or (2) Probabilities of Failure on Demand with Nonstaggered Testing (Paula, 1997c)

<table>
<thead>
<tr>
<th>Equipment</th>
<th>$n$</th>
<th>$\beta$</th>
<th>$\gamma$</th>
<th>$\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air/gas-operated valve</td>
<td>2</td>
<td>0.21</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.27</td>
<td>0.60</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.31</td>
<td>0.67</td>
<td>0.74</td>
</tr>
<tr>
<td>Check valve</td>
<td>2</td>
<td>0.076</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.11</td>
<td>0.49</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.13</td>
<td>0.67</td>
<td>0.59</td>
</tr>
<tr>
<td>Motor-operated valve</td>
<td>2</td>
<td>0.056</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.078</td>
<td>0.50</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.089</td>
<td>0.71</td>
<td>0.70</td>
</tr>
<tr>
<td>Relief (remotely operated) valve</td>
<td>2</td>
<td>0.12</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.18</td>
<td>0.54</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.21</td>
<td>0.79</td>
<td>0.59</td>
</tr>
<tr>
<td>Safety valve</td>
<td>2</td>
<td>0.11</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.14</td>
<td>0.53</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.17</td>
<td>0.69</td>
<td>0.57</td>
</tr>
<tr>
<td>Combined data for all valve types listed in this table</td>
<td>2</td>
<td>0.10</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.14</td>
<td>0.56</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.16</td>
<td>0.72</td>
<td>0.66</td>
</tr>
<tr>
<td>Equipment, Electrical (battery, battery charger, circuit breaker, and motor)</td>
<td>2</td>
<td>0.13</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.16</td>
<td>0.69</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.18</td>
<td>0.75</td>
<td>0.80</td>
</tr>
<tr>
<td>Equipment, Rotating (diesel generator, pump, and turbine)</td>
<td>2</td>
<td>0.067</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.096</td>
<td>0.62</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.11</td>
<td>0.82</td>
<td>0.68</td>
</tr>
<tr>
<td>Equipment, Other (heat exchanger, pump strainer, and trash rack)</td>
<td>2</td>
<td>0.20</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.25</td>
<td>0.76</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.27</td>
<td>0.82</td>
<td>0.85</td>
</tr>
<tr>
<td>Combined data for all equipment, including some equipment not listed in this table</td>
<td>2</td>
<td>0.11</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.14</td>
<td>0.63</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.16</td>
<td>0.76</td>
<td>0.71</td>
</tr>
</tbody>
</table>

Tables should not result in significant uncertainty in reliability analyses and risk assessments. That is, the estimates based on combined data seem representative of the estimates for most types of components. For example, the estimates for "all valves" in Tables 3.9 and 3.10 are probably representative of the MGL parameters for hydraulic-operated valves, which are not shown in the tables. Also, it appears that it is not pos-
TABLE 3.10. Generic MGL Parameters for Models That Use Probabilities of Failure on Demand with Staggered Testing

<table>
<thead>
<tr>
<th>Equipment</th>
<th>$n$</th>
<th>$\beta$</th>
<th>$\gamma$</th>
<th>$\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air/gas-operated valve</td>
<td>2</td>
<td>0.12</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.13</td>
<td>0.51</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.13</td>
<td>0.53</td>
<td>0.68</td>
</tr>
<tr>
<td>Check valve</td>
<td>2</td>
<td>0.039</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.050</td>
<td>0.39</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.050</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td>Motor-operated valve</td>
<td>2</td>
<td>0.029</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.033</td>
<td>0.50</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.032</td>
<td>0.58</td>
<td>0.64</td>
</tr>
<tr>
<td>Relief (remotely operated) valve</td>
<td>2</td>
<td>0.066</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.084</td>
<td>0.44</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.079</td>
<td>0.68</td>
<td>0.52</td>
</tr>
<tr>
<td>Safety valve</td>
<td>2</td>
<td>0.056</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.065</td>
<td>0.43</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.068</td>
<td>0.56</td>
<td>0.50</td>
</tr>
<tr>
<td>Combined data for all valve types listed in</td>
<td>2</td>
<td>0.053</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>this table</td>
<td>3</td>
<td>0.062</td>
<td>0.46</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.061</td>
<td>0.58</td>
<td>0.59</td>
</tr>
<tr>
<td>Equipment, Electrical (battery, battery charger, circuit breaker, and motor)</td>
<td>2</td>
<td>0.071</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.070</td>
<td>0.60</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.069</td>
<td>0.61</td>
<td>0.75</td>
</tr>
<tr>
<td>Equipment, Rotating (diesel generator, pump, and turbine)</td>
<td>2</td>
<td>0.035</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.041</td>
<td>0.52</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.036</td>
<td>0.71</td>
<td>0.61</td>
</tr>
<tr>
<td>Equipment, Other (heat exchanger, pump strainer, and trash rack)</td>
<td>2</td>
<td>0.11</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.11</td>
<td>0.68</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.10</td>
<td>0.70</td>
<td>0.81</td>
</tr>
<tr>
<td>Combined data for all equipment, including some equipment not listed in this table</td>
<td>2</td>
<td>0.057</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0.063</td>
<td>0.53</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0.060</td>
<td>0.64</td>
<td>0.65</td>
</tr>
</tbody>
</table>

It is possible to use judgment to justify estimates other than those from the "combined data" for any equipment that is not in Tables 3.9 and 3.10. This is because, with the few exceptions noted, we cannot explain the individual departures from the estimates obtained from "combined" data. Unless field data exist for a specific type of equipment, the estimates obtained from "combined" data may be the best estimates for reliability analyses and risk assessments.
Quantifications of CCFs Using the Simple Method by Paula and Daggett (1997b). The quantification procedures available for CCFs have been briefly described. These methods are often used as part of CPQRAs for CPI facilities. However, the detailed and complete quantification of CCF events is not always required or cost-effective; in some applications approximate numbers are adequate to support decisions about safeguards. This section presents a simple method that provides probability estimates in the right “ballpark.” The simple method consists of a three-step procedure, which is done separately for each set of multiple safeguards

• **Step 1**—Review the set of multiple safeguards to identify the CCF couplings and defenses that are in place against coupling. Previous discussions in this section provide guidance for this identification step, and Table 3.8 shows the key points in the identification of couplings

• **Step 2**—Establish the “strength” of the CCF coupling as **High, Moderate to High, Low to Moderate,** or **Low.** Table 3.11 provides guidelines for establishing the coupling strength as a function of the CCF couplings and defenses identified in Step 1

• **Step 3**—Evaluate the probability of failure for the set of multiple safeguards using Table 3.12. This probability depends on the level of redundancy and success logic (one-out-of-two, one-out-of-three, etc.), the probability of failure on demand (PFOD) for a single safeguard, the testing/maintenance strategy (staggered versus nonstaggered), and the coupling strength (**High, Moderate to High, Low to Moderate,** or **Low)**

For example, if PFOD = 0.01, the coupling strength is **Moderate to High** for a set of three safeguards configured as two-out-of-three success logic, and safeguards are tested/maintained on a nonstaggered basis, the probability of at least two-out-of-three safeguards failing on demand is 0.003. That is, the probability that at least two safeguards would fail on demand is about one-third of the probability of failure for a single safeguard.

3.3.1.3. **SAMPLE PROBLEM**

This example considers the design of a continuous, stirred-tank reactor (CSTR) that uses a highly exothermic reaction to produce a chemical compound. The CSTR will be operated continuously throughout the year and will shut down annually for 2 weeks of preventive maintenance. It is shown schematically in Figure 3.18.

**Stage 1. System Logic Model Development**

• **System Description.** The accident or concern is an upset condition resulting in a runaway exothermic reaction in the CSTR. The protection against this undesirable event is provided by two CSTR dump valves (V1 and V2) that should open and quench the reaction mixture in a water-filled sump if the temperature inside the CSTR rises above a preset limit. The valve actuators are pneumatic and are controlled by a voting logic unit (VLU). The VLU commands the valves to open when at least two of three temperature channels indicate a high-high condition. Each channel has a temperature transmitter (TT), and a temperature switch
Although any set of components subjected to a common internal environment is susceptible to the CCF coupling common internal environment, operational experience shows that the equipment most affected by this coupling are pneumatically operated valves, heat exchangers, pump strainers, and trash racks. This coupling has been less significant for other component types such as check valves, electrical equipment (including motor-operated valves), and rotating equipment (diesel generator, pump, and turbine).

(TSHH). The temperature switches are all set to trip at the same temperature (high–high).

Every quarter, all the temperature channels will be tested and calibrated on the same day. In addition, a temperature indicator in the control room allows detection of sensor and transmitter failures (the operators will be required to check and record these temperatures every 8-hour shift). However, failures of the temperature switches will likely go undetected until the next quarterly test. The valves and the VLU are tested during the annual maintenance by simulating a signal from all three temperature channels.

- **Problem Definition.** Only the vessel, the temperature channels, the VLU, the valves, and valve operators are addressed in this example. The instrument air (IA) system supplies both pneumatic valve actuators and is assumed to fail on

<table>
<thead>
<tr>
<th>CCF Couplings</th>
<th>CCF Coupling Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>If one or more of the following CCF couplings exist: common support system, common hardware, and common location (sudden, energetic events only) AND the probability of occurrence of the event (support system failure, failure of common hardware, or occurrence of a sudden, energetic event) in the same order of magnitude as the probability of failure for a single safeguard (Note: If the probability of occurrence of the event [support system failure, failure of common hardware, or occurrence of a sudden, energetic event] is higher than the probability of failure of a single safeguard, the probability of occurrence of the event dominates and safeguard redundancy is irrelevant)</td>
<td>High</td>
</tr>
<tr>
<td>For pneumatically operated valves, heat exchangers, pump strainers, and trash racks, if the equipment similarity and common internal environment CCF couplings exist</td>
<td>Moderate to High</td>
</tr>
<tr>
<td>If one or more of the following CCF couplings exist: common support system, common hardware, and common location (sudden, energetic events only) AND the probability of occurrence of the event (support system failure, failure of common hardware, or occurrence of a sudden, energetic event) is about one order of magnitude lower than the probability of failure for a single safeguard</td>
<td>Low to Moderate</td>
</tr>
<tr>
<td>If the equipment similarity and at least one of the following CCF couplings exist: (1) common location (abnormal events only), (2) common operating/maintenance staff and procedure, or (3) common internal environment (except for pneumatically operated valves, heat exchangers, pump strainers, and trash racks)</td>
<td>Low</td>
</tr>
<tr>
<td>If none of the conditions for High, Moderate to High, or Low to Moderate apply</td>
<td>Low</td>
</tr>
</tbody>
</table>

*Although any set of components subjected to a common internal environment is susceptible to the CCF coupling common internal environment, operational experience shows that the equipment most affected by this coupling are pneumatically operated valves, heat exchangers, pump strainers, and trash racks. This coupling has been less significant for other component types such as check valves, electrical equipment (including motor-operated valves), and rotating equipment (diesel generator, pump, and turbine).
<table>
<thead>
<tr>
<th>Level of Redundancy and Success Logic</th>
<th>Testing/Maintenance Strategy</th>
<th>Coupling Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Staggered</td>
<td>Nonstaggered</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Moderate to High</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>One-out-of-two</td>
<td>5e-02*</td>
<td>3e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.03</td>
<td>2e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.01</td>
<td>5e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.003</td>
<td>2e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.0003</td>
<td>2e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-05</td>
</tr>
<tr>
<td>One-out-of-three</td>
<td>5e-02*</td>
<td>2e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.03</td>
<td>2e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.01</td>
<td>5e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.003</td>
<td>2e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.0003</td>
<td>2e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-05</td>
</tr>
<tr>
<td>Two-out-of-three</td>
<td>6e-02</td>
<td>5e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.03</td>
<td>2e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.01</td>
<td>5e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.003</td>
<td>5e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>2e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.0003</td>
<td>5e-05</td>
</tr>
<tr>
<td>Two-out-of-four</td>
<td>5e-02</td>
<td>3e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.03</td>
<td>2e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.01</td>
<td>5e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.003</td>
<td>2e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.0003</td>
<td>2e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-05</td>
</tr>
<tr>
<td>Three-out-of-four</td>
<td>7e-02</td>
<td>7e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.03</td>
<td>2e-02</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.01</td>
<td>5e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.003</td>
<td>2e-03</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.0003</td>
<td>2e-04</td>
</tr>
<tr>
<td></td>
<td>PFOD = 0.001</td>
<td>5e-05</td>
</tr>
</tbody>
</table>

*Scientific notation: \(5e-02 = 5 \times 10^{-2} = 0.05\).
demand with a probability of 0.001 (this system is not analyzed in detail in this example). Other support systems are not required for successful operation of the protection system. (The VLU is designed to open the valves on loss of electric power.)

The top event of interest is "CSTR Fails to Dump following a High Temperature Upset." Successful operation of the protection systems requires operation of at least two of the temperature channels, the VLU, and at least one of the valves (including the respective actuator and the instrument air system). External events such as earthquakes, fires, and floods are beyond the scope of this example.

• **Logic Model Development.** Figure 3.19 presents a fault tree for this problem. The data for this example are presented in Table 3.13. These data were derived from plants operated by the same company, as part of the previous effort to collect reliability data. This effort was made a few years earlier and did not include an attempt to collect CCF data.

**Stage 2. Identification of Common Cause Component Groups.**

• **Qualitative Analysis.** There are two CCF events of concern in this example: (1) the CCF of the redundant dump valves and (2) the CCF of the redundant temperature channels. As previously mentioned, the reliability data obtained from a
previous effort did not address CCFs explicitly. However, the following observations from the data collection study are useful for CCF considerations:

- About 70% of all failures of valves used in this type of service involved blockage of flow caused by process material plugging the valve inlet or the valve internals.
- The majority of failures involving temperature switches in other plants were associated with maintenance activities (e.g., maladjusted set-points)

- **Quantitative Screening.** This step is important when performing an analysis of a complete chemical process plant. In that case, the number of CCF events could be high and some prioritization would be useful. In this problem, the Beta-Factor Model will be used to develop preliminary CCF probabilities. Generic experience indicates that a beta-factor for temperature channels is about 0.1 to 0.2 (Lydell, 1979; Meachum et al., 1983) and that the beta-factor for pneumatic valves is about 0.2 (Stevenson and Atwood, 1983). Thus, the following preliminary CCF rates and probabilities are derived in connection with the data in Table 3.13:
CCF rate for valves \( = \beta_{VALVE} \times \lambda_{VALVE} = 0.2 \times 0.1/\text{year} = 0.02/\text{year} \)
CCF rate for temperature sensing element \( = 0.2 \times 0.3/\text{year} = 0.06/\text{year} \)
CCF rate for temperature transmitters \( = 0.2 \times 0.1/\text{year} = 0.02/\text{year} \)
CCF probability of failure on demand for temperature switches
\( = 0.2 \times 0.025 = 5 \times 10^{-3} \)

Table 3.14 presents a preliminary evaluation of the protection system unavailability. For example, the results of “CCF of valves V1 and V2 to open” (third row of Table 3.14) were calculated as follows:

\[
\text{Failure rate} = \beta_{VALVE} \times \lambda_{VALVE} \\
(\text{CCF of both valves}) = 0.2 \times 0.1/\text{year} = 0.02/\text{year} \\
\text{Maximum exposure time} = 1 \text{ year (valves are tested annually)} \\
\text{Probability of failure} = \text{failure rate} \times \text{maximum exposure time} \\
\times 0.5 \text{ on demand (PFOD)} \\
= 0.02/\text{year} \times 1 \text{ year} \times 0.5 \\
= 0.01 \\
\text{Contribution to system unavailability} = 0.01 \text{ (the CCF of both valves is a minimal cut unavailability set)} \\
\text{Percentage contribution} = \frac{\text{minimal cut set PFOD}}{\text{system PFOD}} \times 100 \\
= \frac{0.01}{0.023} \times 100 = 44\% 
\]

The results for other Table 3.14 entries were calculated similarly. According to Table 3.14, CCFs involving valves contribute 44% to the system unavailability, and CCFs involving the temperature switches contribute 22%. CCFs involving sensing elements and transmitters contribute negligibly to system unavailability and are not considered further in this analysis.
TABLE 3.14. Preliminary Evaluation of Protection System Unavailability

<table>
<thead>
<tr>
<th>Contributor to system unavailability</th>
<th>Failure rate (per year)</th>
<th>Maximum exposure time (years)</th>
<th>Probability of failure on demand</th>
<th>Contribution to system unavailability ($10^{-3}$)</th>
<th>Percentage contribution to system unavailability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valve V1 or V2 fails to open</td>
<td>0.1</td>
<td>1</td>
<td>0.05</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Both valves V1 or V2 fail to open (independently)</td>
<td>—</td>
<td>—</td>
<td>(0.05)$^2$</td>
<td>2.5</td>
<td>11</td>
</tr>
<tr>
<td>CCF of valves V1 and V2 to open</td>
<td>0.02</td>
<td>1</td>
<td>0.01</td>
<td>10</td>
<td>44</td>
</tr>
<tr>
<td>Voting logic unit—failure to output shutdown signal when commanded</td>
<td>0.005</td>
<td>1</td>
<td>0.0025</td>
<td>2.5</td>
<td>11</td>
</tr>
<tr>
<td>Instrument air—loss of air pressure</td>
<td>—</td>
<td>—</td>
<td>0.001</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Temperature channel:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensing element</td>
<td>0.3</td>
<td>8 hr</td>
<td>b</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Transmitter</td>
<td>0.1</td>
<td>8 hr</td>
<td>b</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Switch—low</td>
<td>—</td>
<td>—</td>
<td>0.0025</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Two temperature channels fail to trip (independently)</td>
<td>—</td>
<td>—</td>
<td>$3 \times (0.025)^2$</td>
<td>1.9</td>
<td>8</td>
</tr>
<tr>
<td>CCF of temperature channels to trip</td>
<td>—</td>
<td>—</td>
<td>0.005</td>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>Total system unavailability</td>
<td>—</td>
<td>—</td>
<td></td>
<td>22.9</td>
<td>100</td>
</tr>
</tbody>
</table>

*Some cells are intentionally left blank; not all parameters are applicable to all equipment.

*Negligible contribution.

Stage 3. Common Cause Modeling and Data Analysis.

* Step 3.1. Incorporation of Common Cause Basic Events. Figure 3.20 shows a modified fault tree for the sample problem. Two CCF events have been added to the original fault tree.

* Step 3.2. Data Classification and Screening. When failure event reports are available, the analyst should review previous occurrences of failures and postulate how they could have occurred in the system of interest. This review involves identifying events whose causes are explicitly modeled in the fault tree. For example, a failure report may describe a loss of two valves because of the loss of instrument air, this event is already addressed in the fault tree (Figures 3.19 and 3.20) and should not be considered in evaluating CCFs of valves.

Another aspect that should be investigated is whether there are conditions (e.g., a different maintenance program) that would make the failures that occurred at other plants more (or less) likely to occur at the plant being studied. If
FIGURE 3.20. Fault tree for sample problem modified for common cause failure events.
so, the generic data must be adjusted to accommodate those differences. This topic is discussed in detail in NUREG/CR-4780 (Mosleh et al., 1988).

• **Step 3.3 Parameter Estimation.** When failure event reports are available to perform Step 3.2, the analyst develops a set of pseudodata, that is, generic data specialized for a particular process plant. NUREG/CR-4780 (Mosleh et al., 1988) provides guidance on how to develop the pseudodata. These pseudodata can be used to estimate parameters of any of the available parametric models (e.g., the beta-factor).

### Stage 4. System Quantification and Interpretation of Results

The CCF analysis results are shown in Table 3.14. This table indicates that two CCF events are important contributors to system unavailability: (1) the CCF of the valves and (2) the CCF of the temperature switches.

Consider the CCF of the valves first. One possible alternative to reduce the likelihood of this event is to institute a periodic test (e.g., quarterly) of the valves. The test could involve momentarily opening and then closing each valve and verifying the proper flow to the sump. The benefit associated with this test is that the exposure time for the CCF event is reduced. That is, if both valves were indeed failed, this condition would be detected within, at most, one quarter. This benefit can be evaluated quantitatively by reducing the maximum exposure time for the valve CCF event from 1 to 0.25 years (a quarter) in Table 3.14. The probability of occurrence of the valve CCF event would be reduced to $2.5 \times 10^{-3}$, which is a factor of four lower than the probability value without the test. Obviously, possible detrimental effects associated with instituting the test (e.g., excessive valve wear) must be analyzed and compared with the benefits.

Consider now the CCF of the temperature switches. One possible alternative to reduce the likelihood of this event is to stagger the (quarterly) test and adjust the temperature channels. That is, each channel will still be tested and adjusted every 3 months, but these activities will be conducted about 1 month apart (rather than sequentially). The benefit associated with this alternative is that the chances of maintenance-related errors affecting multiple channels are reduced. This reduction is attained because similar human errors in each task are less likely to occur if the tasks are performed about 1 month apart than if the tasks are performed sequentially (a few minutes apart). Again, possible detrimental effects associated with the modified testing and adjustment policy (e.g., increased cost) must be compared with the benefits.

### 3.3.1.4. DISCUSSION

**Strengths and Weaknesses.** The main strength of the technique is that it acknowledges the historical evidence of CCF occurrences in redundancy applications. Although CCF data are sparse (this is the main weakness of the CCF analysis), there are sufficient data to indicate that CCF events tend to dominate system unavailability in those applications where redundancy is used to improve system reliability performance.

Using multiple safeguards in CPI facilities often reduces risk. However, the very high reliability theoretically achievable by multiple safeguards, particularly with redundant components, can sometimes be compromised by CCF events. CCF events have
consistently been shown to be important contributors to risk, and the frequency of accident scenarios in CPI facilities may be grossly underestimated if CCFs affecting multiple safeguards are not taken into account.

An important observation regarding CCFs is that the potential for the occurrence of CCFs does not imply that using multiple safeguards is ineffective. On the contrary, the use of multiple safeguards has been shown to reduce risks, and the information presented in this section supports this contention. However, it is important to recognize that CCFs may limit the theoretical benefits achievable through the use of multiple safeguards, particularly through the use of redundant components. A good understanding of CCFs provides a more realistic appreciation of risk in CPI facilities by allowing better decisions to be made about the use of safeguards.

**Identification and Treatment of Possible Errors.** CCF analysis is limited by the lack of plant-specific data. Thus, the analysis must rely extensively on generic experience. There is judgment involved in using generic data for a specific plant. This problem can be alleviated by using systematic procedures for analyzing generic data (Mosleh et al., 1988) and by developing high-quality CCF databases.

**Utility.** A complete CCF analysis offers both quantitative and qualitative insights that are helpful in establishing defense alternatives to improve availability and safety.

**Resources.** The CCD analyst should be an engineer experienced in risk assessment techniques and in the analysis of failure reports. The CCF analysis should be peer reviewed by CCF experts.

**Available Computer Codes.** There are several computer codes available for CCF analysis. The recently developed computer program CCF evaluates CCF parameters (e.g., MGL parameters) and CCF probabilities (Kvarford et al., 1995). The codes COMCAN (Rasmuson et al., 1982), SETS (Worrell, 1985), WAMCOM (Putney, 1981), and BACKFIRE (Rooney et al., 1978) are useful when performing qualitative CCF analyses of large, complex systems. The computer code BFR evaluates CCF rates according to the binomial failure rate (quantitative) model (Atwood et al., 1983b).

3.3.2. Human Reliability Analysis

3.3.2.1. BACKGROUND

**Purpose.** The primary purpose of human reliability analysis (HRA) in a CPQRA is to provide quantitative values of human error for inclusion in fault tree analysis (Section 3.2.1) and event tree analysis (Section 3.2.2). HRA techniques can also be valuable in identifying potential recommendations for error reduction.

**Technology.** A human error is an action that fails to meet some limit of acceptability as defined for a system. This may be a physical action (e.g., closing a valve) or a cognitive action (e.g., fault diagnosis or decision making). Some examples where human error can increase risk from a process plant are

- errors in operations or maintenance procedures that lead to increased demands on protective systems